Ricardo Ferraro de Souza

UMA PROPOSTA DE INFRAESTRUTURA COM SEGURANÇA PARA PACS EM NUVEM ATRAVÉS DE IDENTIDADE FEDERADA

Dissertação submetida ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina para a obtenção do Grau de mestre em Ciência da Computação.
Orientador: Prof. Dr. Carlos Becker Westphall.

Florianópolis
2013

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Souza, Ricardo Ferraro de
Uma proposta de infraestrutura com segurança para PACS em nuvem através de identidade federada / Ricardo Ferraro de Souza ; orientador, Carlos Becker Westphall - Florianópolis, SC, 2013.
65 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro Tecnológico. Programa de Pós-Graduação em Ciência da Computação.

Inclui referências

1. Ciência da Computação. 2. Cloud Computing. 3. PACS. 4. Healthcare Systems. 5. Security. I. Westphall, Carlos Becker. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Computação. III. Título.

Ricardo Ferraro de Souza

UMA PROPOSTA DE INFRAESTRUTURA COM SEGURANÇA PARA PACS EM NUVEM ATRAVÉS DE IDENTIDADE FEDERADA

Esta Dissertação foi julgada adequada para obtenção do Título de "Mestre em Ciência da Computação", e aprovada em sua forma final pelo Programa Pós-Graduação em Ciência da Computação.

Florianópolis, 2 de agosto de 2013.

_____
Prof. Ronaldo dos Santos Mello, Dr.
Coordenador do Curso

Banca Examinadora:

_____
Prof. Carlos Becker Westphall, Dr.
Presidente - Universidade Federal de Santa Catarina

_____
Prof.ª Carla Merkle Westphall, Dra.
Universidade Federal de Santa Catarina

_____
Prof. Mario Antônio Ribeiro Dantas, Dr.
Universidade Federal de Santa Catarina

_____
Prof. Elias Procópio Duarte Jr., Dr.
Universidade Federal do Paraná

Este trabalho é dedicado aos meus queridos pais e minha amada esposa, que nunca deixaram de acreditar em mim, mesmo em momentos difíceis. Também o dedico aos amigos que me deram apoio e aos professores, que sempre estiveram aconselhando.

AGRADECIMENTOS

Agradeço a Deus, primeiramente, pela oportunidade concedida para estudar, conseguir realizar um sonho e fazer amizades.

Agradeço aos familiares mais próximos, Ademir Luiz de Souza e Jane Ferraro de Souza, meus pais, que sempre estiveram presentes, apoiando-me, à disposição para qualquer eventualidade, incentivando-me nos momentos difíceis. A minha tia Jaqueline Ferraro pela colaboração.

Agradeço a minha esposa Flora Eliane Willrich Ferreira de Souza por estar sempre ao meu lado nas horas em que nada parecia dar certo, pela paciência nestes meses de turbulência, pelo afeto e carinho em momentos difíceis, pelas palavras de incentivo quando o entusiasmo não era mais o mesmo do início.

Agradeço aos professores Carlos Westphall e Carla Westphall, que se mostraram compreensivos e sempre dispostos a ajudar no que fosse possível, além de terem acreditado no trabalho e contribuído muito para a sua realização. Também gostaria de agradecer ao professor Mario Dantas pelas críticas feitas durante a defesa e pela ajuda fornecida para o aperfeiçoamento do trabalho. O professor Elias Procópio Duarte Jr. também contribuiu significativamente para o aperfeiçoamento deste trabalho, merecendo meus sinceros agradecimentos. Estendo estes agradecimentos aos colaboradores do Laboratório de Redes e Gerência (LRG), em especial ao mestrando Rafael Weingartner, pela amizade demonstrada ao longo deste período de convivência, ensinamentos e troca de experiências realizadas.

Agradeço ao meu grande amigo Malcus Otávio Quinoto Imhof pelo apoio e colaboração durante esta jornada.

Nossa maior fraqueza está em desistir. O caminho mais certo de vencer é tentar mais uma vez.

(Thomas Edison)

RESUMO

Clínicas e hospitais vêm adquirindo cada vez mais recursos tecnológicos que auxiliam em um diagnóstico mais rápido e preciso, a fim de torná-lo mais dinâmico e eficaz. Isso vem fazendo com que entidades de saúde busquem equipamentos mais modernos e com recursos tecnológicos avançados. Os exames chegam aos médicos com muitas informações processadas em diferentes softwares e hardwares. Com o elevado número de informações contidas no exame, aumenta-se o tamanho e a quantidade de imagens presentes no exame do paciente. Com o passar do tempo, o volume de imagens cresce exponencialmente, saturando a capacidade de retenção de informações contidas nos dispositivos de armazenamento. A aquisição de novos hardwares para suportar tamanho acúmulo de informações tem-se mostrado um problema grave nestas instituições.

Os sistemas PACS (Picture Archive and Communications System) podem adquirir, transmitir, armazenar e exibir informações de imagens médicas. O dcm4chee é um projeto de código aberto muito usado por provedores de sistemas de saúde, projetos de pesquisa e aplicações comerciais que fornece um conjunto de aplicações e bibliotecas usadas para implementar sistemas PACS. Normalmente, os sistemas PACS desenvolvidos são executados localmente em cada uma das instituições, nos seus servidores locais. Os médicos devem se cadastrar localmente em cada sistema PACS de cada uma das instituições de saúde nas quais exerçam sua profissão, para poder ter acesso às imagens médicas.

Este trabalho propõe a implantação de sistemas PACS em ambientes de nuvem usando identidades federadas. Ambientes de nuvem auxiliam na eficiência do armazenamento de imagens médicas, possibilitando o acesso ao exame/laudo do paciente a partir de qualquer localidade, sendo independente a plataforma utilizada para o acesso. O acesso aos exames na nuvem é garantido e seguro através do conceito de federação que garante a confiança e segurança entre as partes. Foi desenvolvida a integração do sistema Shibboleth, que provê identidades federadas, com o sistema dcm4chee. Esta integração demonstra a utilização de PACS em nuvem através de identidades federadas.

Palavras-chave: Cloud Computing. PACS. Healthcare Systems. Security.

ABSTRACT

Clinics and hospitals are acquiring increasingly technological resources that improve the diagnosis, turning it quicker, more accurate and effective. This way, the exams come to doctors with information that is processed on different software and hardware across the datacenter. With the large number of information required to make an exam, increases the size and number of images present on the examination file of the patient. The volume of images grows exponentially out of the storage devices. Then, the acquisition of new hardware to support increase on information has been a serious problem in these institutions.

The PACS (Picture Archive and Communications System) may acquire, transmit, store and display information from medical images. The dcm4chee is an open source project used by providers of health systems, research projects and commercial applications that provides a set of applications and libraries used to implement PACS. Normally, developed systems PACS run locally in each of the institutions on local servers. Doctors must register locally on each system PACS of each health institutions in which they exercise their profession in order to have access to medical images.

This paper proposes the implementation of PACS systems on cloud environments using federated identities. Cloud environments assist the efficient storage of medical images, enabling access to the report of the patient from any location, anywhere at any time. It was extended the dcm4chee application to integrate with the Shibboleth System, which provides federated identity. This integration demonstrates the use of cloud based PACS through the federated identity. This way the is secured and safe through the concept of federation that ensures trust and confidence between the involved parties.

Keywords: Cloud Computing. PACS. Healthcare Systems. Security.

LISTA DE FIGURAS

Figura 1 - Modelo tradicional. 16
Figura 2 – Modelos de serviços para *Cloud Computing*. 21
Figura 3 - Divisão em camadas da teleradiologia. 23
Figura 4 - Visão Geral do PACS. 24
Figura 5 - Arquitetura tradicional para PACS. 26
Figura 6 - Exemplo de imagem DICOM. 27
Figura 7 - Modelo de identidade federada [GERENCIAMENTO DE IDENTIDADES, 2013]. 35
Figura 8 – Nuvem para instituições com PACS. 38
Figura 9 – Componentes da nuvem SaaS utilizando PACS. 39
Figura 10 - Estrutura LDAP. 40
Figura 11 - Tela principal do PACS. 42
Figura 12 – Implementação do Shibboleth para PACS em nuvem. 45
Figura 13 - Acesso ao PACS com JAAS. 48
Figura 14 - Acesso ao PACS com Shibboleth. 49
Figura 15 - Tela inicial *login tablet*. 50
Figura 16 - Tela principal PACS *tablet*. 51
Figura 17 - Tela de *logout* Shibboleth *tablet*. 52
Figura 18 - Tela inicial Shibboleth computador. 53
Figura 19 - Tela principal PACS computador. 53
Figura 20 – Tela *logout* Shibboleth computador. 54
Figura 21 – Processo de autenticação com IDP. 55

LISTA DE ABREVIATURAS E SIGLAS

DICOM – *Digital Imaging and Communications in Medicine*
FBI – *Federal Bureau of Investigation*
GPRS – *General Packet Radio Services*
HIS – *Hospital Information Systems*
HTTP – *Hypertext Transfer Protocol*
IDP – *Identity Provider* ou Provedor de Identidades
IAM - *Identify and Access Management*
ISO – *International Organization for Standardization*
JAAS – *Java Authentication and Authorization Service*
LDAP – *Lightweight Directory Access Protocol*
NIST – *National Institute of Standards and Technology*
ONU – Organização das Nações Unidas
OWASP – *Open Web Application Security Project*
PACS – *Picture Archive and Communications Systems*
RIS – *Radiology Information Systems*
SAML – *Security Assertion Markup Language*
SP – *Service Provider*
SSO – *Single Sign On*
TI – Tecnologia da Informação
URL – *Uniform Resource Locator*
XML – *Extensible Markup Language*

SUMÁRIO

1 INTRODUÇÃO 13
1.1 MOTIVAÇÃO E JUSTIFICATIVA 13
1.2 OBJETIVOS 15
1.2.1 Objetivo Geral 16
1.2.2 Objetivos Específicos 17
1.3 ORGANIZAÇÃO DO TRABALHO 18
2 FUNDAMENTAÇÃO TEÓRICA 19
2.1 COMPUTAÇÃO EM NUVEM 19
2.1.1 Modelos de serviços 20
2.2 PACS (*PICTURE ARCHIVE AND COMMUNICATIONS SYSTEM*) 22
2.2.1 Arquitetura para PACS no modelo tradicional 24
2.2.2 DICOM (*Digital Imaging and Communications in Medicine*) 26
2.3 PACS NO CONTEXTO DAS NUVENS COMPUTACIONAIS 28
2.4 SUSTENTABILIDADE 29
3 CONCEITOS DE SEGURANÇA CONSIDERADOS NA PROPOSTA 30
3.1 AMEAÇAS 30
3.2 MECANISMOS DE SEGURANÇA 31
3.3 SEGURANÇA EM SAÚDE 33
3.4 FEDERAÇÃO 34
3.5 IDENTIDADE FEDERADA 34
4 MODELO DE SEGURANÇA PARA PACS EM NUVEM 37
4.1 PACS COM SEGURANÇA EM NUVEM 37
4.2 NUVEM COMPUTACIONAL PARA INSTITUIÇÕES COM PACS 38
4.3 FERRAMENTAS UTILIZADAS NA NUVEM COM PACS 39
4.3.1 *OpenLdap* 39
4.3.2 *Shibboleth* 40
4.3.3 Dcm4chee 41
4.4 PRINCIPAIS CONTRIBUIÇÕES E TRABALHOS CORRELATOS 42

5 VALIDAÇÃO DA SEGURANÇA PARA PACS EM NUVEM COM IDENTIDADE FEDERADA 44
5.1 DESCRIÇÃO DA IMPLEMENTAÇÃO REALIZADA 45
5.2 RESULTADOS OBTIDOS 49
5.2.1 Caso 1 49
5.2.2 Caso 2 52
5.3 DIFICULDADES ENCONTRADAS NO DESENVOLVIMENTO E VALIDAÇÃO DA PROPOSTA 54
5.4 DESENVOLVIMENTO DA INTEGRAÇÃO DO SHIBBOLETH COM PACS EM NUVEM 55
6 CONCLUSÕES E TRABALHOS FUTUROS 57
6.1 PRINCIPAIS CONTRIBUIÇÕES 57
6.2 TRABALHOS FUTUROS 58
REFERÊNCIAS 59
APÊNDICE A – handle.xml modificado 64

1 INTRODUÇÃO

1.1 MOTIVAÇÃO E JUSTIFICATIVA

A tecnologia da informação vem revolucionando todas as áreas e melhorando significativamente os modelos de negócios. A medicina é aperfeiçoada através de soluções tecnológicas inovadoras em inúmeros equipamentos com as mais diversas funções, como os radiológicos para processamento de imagens, para análise de sangue, para auxiliar em cirurgias e para controle do paciente a distância. A necessidade da busca por um diagnóstico mais preciso, que permita um tratamento eficaz para os pacientes, faz com que exista uma constante evolução tecnológica.

Dentro dos hospitais e clínicas de diagnóstico por imagem é comum encontrarmos *Picture Archive and Communications Systems* (PACS), que tem a finalidade de gerenciar o armazenamento e a exibição de imagens médicas. Através de estações de trabalho, os médicos conseguem acesso ao sistema PACS, onde fazem a manipulação das imagens independentemente do local físico onde o médico se encontra.

O diagnóstico médico é realizado mediante a análise das imagens ou leitura de laudo por médicos especialistas, que nem sempre estão presentes no local em que o exame foi realizado, principalmente quando há necessidade da participação de um segundo médico no diagnóstico, ou em casos de treinamento de médicos residentes. O envolvimento desses médicos pode ocorrer através de teleconferências, telelaudo ou qualquer outra tecnologia que possibilite a comunicação de um médico que não se encontra fisicamente no local, desde que ele consiga ter acesso às imagens do exame e/ou o laudo. Esta prática é conhecida como *e-health*.

E-health compreende a oferta de serviços ligados aos cuidados de saúde nos casos em que a distância é um fator crítico. Estes serviços são realizados por profissionais de saúde utilizando tecnologias de informação e comunicação para o intercâmbio de informações válidas para diagnósticos, prevenção e tratamento de doenças e a contínua educação de prestadores de serviços de saúde, bem como a pesquisa (WHO, 2008).

Imagens provenientes de exames radiológicos são utilizadas em clínicas e hospitais para o diagnóstico médico. A inter-relação entre clínicas, hospitais e departamentos de radiologia depende cada vez mais da acessibilidade dessas imagens, a partir de qualquer localização física dentro ou fora da unidade de atendimento (BARROS JUNIOR, 2010).

A prática da *e-health* só é possível por causa dos avanços significativos em sistemas de comunicação. A possibilidade de conectividade com a *World Wide Web* a partir de dispositivos móveis, uma tecnologia em constante

evolução, permite aos pacientes obterem cuidados médicos adequados em regiões menos favorecidas onde não há médicos ou ligação com a Internet com fio disponível. Redes *Wi-Fi*, 3G, 4G, dentre outras, são constantemente melhoradas com taxas de transmissão mais altas, permitindo acesso a conteúdos não explorados antes, que visam melhorar, simplificar e complementar os serviços relacionados com o atendimento ao paciente para imprimir mais eficiência a tais serviços.

Médicos de hospitais e clínicas necessitam de um recurso que possibilite acesso às informações e ao histórico de cada paciente, tendo em vista que no serviço público, é comum um paciente trocar de médico várias vezes durante um diagnóstico ou tratamento. Desta forma, muitos dados importantes como os diagnósticos, exames, e prescrições feitas por cada médico não são arquivados. Essa situação pode gerar duplicidade em solicitações de exames e em prescrições de medicamentos, pois são recorrentes os casos em que os pacientes, talvez por ingenuidade, não sabem o nome do medicamento que estão tomando ou qual a finalidade do mesmo, atitude que gera aumento do consumo de medicamentos e dos recursos de diagnóstico. Isso poderia ser minimizado se todos os profissionais, ao prestarem serviço ao cliente, tivessem acesso ao seu perfil de saúde e histórico de diagnósticos e tratamentos. Por fim, os médicos, farmacêuticos, bioquímicos, entre outros profissionais, poderiam ter acesso a qualquer exame, consulta, laudo ou medicamento que o paciente tenha em seu histórico.

Em se tratando de diagnósticos por imagens, Ultrassom, Ressonância Magnética, Tomografia Computadorizada, Raios-X, entre outros, o paciente leva os laudos anteriores para o médico usar como referência no atual diagnóstico. Frequentemente tais laudos não são recebidos pelo hospital digitalizados ou possuem um amplo histórico contendo inúmeras digitalizações a serem inseridas no servidor local, o que dificulta o acesso do médico a informações fundamentais, atrasando o procedimento clínico.

A necessidade de investimento em processamento e armazenamento de dados é cada vez maior, quase que insustentável para grande parte dos hospitais e clínicas que não dispõem de muitos recursos para investimento em equipamentos modernos ou infraestrutura de tecnologia da informação. Armazenar imagens de exames médicos vem se tornando um grave problema. Exames complexos significam maior número de imagens a serem armazenadas, exigindo maior capacidade de processamento e infraestrutura necessária para o estabelecimento que disponibiliza os serviços.

Cloud Computing ou computação nas nuvens vem sendo tema central de várias pesquisas em tecnologia da informação. A possibilidade de compartilhar recursos através de *clusters*, a virtualização e a facilidade de acesso à informação atraem cada vez mais pesquisadores de tecnologia da informação.

As empresas estão buscando este novo paradigma como uma forma de baixar custos, contratando recursos computacionais e evitando a aquisição de *hardware* e *software*, obtendo maior escalabilidade, acessibilidade, disponibilidade e recuperação de desastres.

Há, no entanto, preocupação com a privacidade dos dados, uma vez que eles estão fora do domínio do cliente, isto é, por um lado, temos as vantagens dos serviços disponíveis; por outro, existe a preocupação com a segurança. Para que esses serviços sejam efetivamente desfrutados pelas organizações, é necessário fornecer controle de acesso através de mecanismos que gerenciam identidade e acesso *Identify and Access Management* (IAM) protegido por federações. Federações são grupos de organizações que estabelecem a confiança entre si para cooperar. O uso de federações garante a segurança na troca de informações (LEANDRO, 2012).

Há, também, a necessidade de certificação de qualidade nos hospitais e clínicas a fim de atender aos requisitos mínimos de qualidade pré-estabelecidos exigidos por convênios e legislações. Informações armazenadas eletronicamente e de fácil acesso não precisam ser impressas, evitando-se a geração de resíduos (películas, papéis, cartuchos) e poluentes ambientais, um requisito que deve ser cumprido pelas empresas que almejam alguma certificação *International Standard Organization* (ISO) ou que pretendem atingir os objetivos do milênio estipulados pela Organização das Nações Unidas (ONU), dentre os quais a qualidade de vida e o respeito ao meio ambiente, relacionado à preservação ambiental (OBJETIVOS DO MILÊNIO, 2011).

1.2 OBJETIVOS

Ficha de atendimento, consultas, laudos médicos e laboratoriais, imagens médicas e medicamentos são alguns dos itens do histórico médico do paciente, que fica cada vez mais complexo, contendo importantes dados que crescem exponencialmente. Este histórico é de cuidado total do paciente, que além de cuidar da saúde e de outros afazeres, necessita manter em local seguro todas estas informações. É crescente o número de casos de pacientes que se submetem a consulta sem os laudos de exames e outros documentos necessários, dificultando e atrasando um diagnóstico preciso e eficaz.

Todos os dias, pacientes em situação de emergência são atendidos em postos de saúde, farmácias e pronto-socorro de hospitais, havendo necessidade de intervenção cirúrgica ou qualquer outro procedimento clínico que requer atenção às condições e históricos de saúde do paciente. Nem sempre tais informações chegam às mãos do médico.

Muitos médicos atendem em diversas clínicas e/ou hospitais e têm pacientes em vários locais, muitas vezes em outras cidades. Precisam, frequentemente, acompanhar os exames, dando suporte a todos os pacientes. Em casos de urgência, em que o paciente necessita de um procedimento imediato, a distância pode interferir no tempo do laudo e na tomada de decisão do médico. Para suprir essa necessidade, clínicas e hospitais investem grandes valores na infraestrutura de comunicação, no processamento e no armazenamento desses exames. A figura 1 mostra um escopo do processo descrito para hospitais e clínicas atualmente.

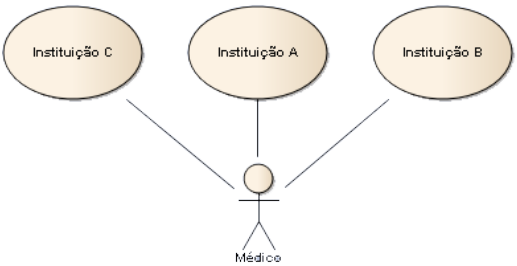

Figura 1 - Modelo tradicional.

Tendo em vista esses problemas, o trabalho apresenta uma solução para alguns deles.

1.2.1 Objetivo Geral

O objetivo geral deste trabalho é propor uma infraestrutura segura para sistemas PACS em ambientes de nuvem que tenha suporte para identidades federadas. A ideia é usar nuvem como um modelo para aplicativos a serem entregues como serviços através da Internet. Como o serviço funciona sob demanda, gráficos e relatórios de utilização podem ser gerados para justificar os valores a serem pagos pelos clientes.

Serviços de nuvem são construídos de tal forma que se uma máquina falhar, o sistema reajustar-se-á para evitar que o serviço deixe de funcionar ou que o contratante saiba que houve algum tipo de problema.

A abordagem de computação em nuvem viabiliza o crescimento de infraestrutura de armazenamento e processamento para hospitais e clínicas sem causar muito impacto. Acesso à Internet e dispositivos de computação estão disponíveis em qualquer lugar ou área, criando novas oportunidades de compartilhamento e utilização de recursos *on line*. Um número inexplicável de recursos e serviços de Internet, como *e-mail* e armazenamento, é utilizado diariamente como uma espécie de mercadoria. Aliando-se conceitos de

telemedicina e tecnologia, pacientes são continuamente monitorados sem serem perturbados durante suas atividades diárias (BERNDT, 2012).

Em um ambiente hospitalar, pacientes podem usar sensores que ficam conectados a equipamentos médicos que são interconectados a fim de trocar informações. Esses dados tornam-se disponíveis na "nuvem", onde podem ser processados por um sistema inteligente e/ou distribuído para a equipe médica para análise (ROLIM, 2010).

1.2.2 Objetivos Específicos

Uma solução de PACS em nuvem deve conceder acesso ao servidor de arquivo a partir de qualquer lugar ou plataforma. Utilizando o conceito de identidade federada, o trabalho expõe um método de acesso ao PACS na nuvem com segurança. Os serviços da nuvem são autenticados usando um sistema de gerenciamento de identidades que é responsável por estabelecer a federação e lidar com as identidades de forma segura.

Os objetivos específicos deste trabalho que podem ser listados são:

- Adaptar o sistema PACS para executar em nuvem, garantindo acesso ao servidor de arquivo a partir de qualquer lugar ou plataforma; e,
- Prover segurança no sistema PACS na nuvem através da integração de um sistema de gerenciamento de identidades com o sistema PACS. O sistema de gerenciamento de identidades será responsável pelas seguintes tarefas: construção da federação (que é a relação de confiança entre as partes) e autenticação (usando identidades federadas).

Usar identidades federadas no ambiente PACS significa ter uma relação de confiança entre as partes, isto é, previamente foram definidas chaves criptográficas para as trocas de mensagens e também formatos padronizados para a semântica e sintaxe das identidades. Por exemplo, caso as várias instituições de saúde nas quais um médico trabalha façam parte de uma mesma federação, este médico pode, depois de se autenticar no sistema, ter acesso aos vários sistemas PACS nas diferentes instituições.

Através de PACS em nuvem, espera-se que o paciente possa realizar exame de imagem em qualquer lugar do mundo e receber um diagnóstico médico mais específico e de qualidade. O paciente não precisará mais levar o histórico clínico quando for procurar um profissional da saúde.

Para os médicos, o PACS em nuvem permite acesso a um histórico de imagens e laudo, a seleção de "imagem chave", que por definição, resume-se a imagens que apresentam uma suposta variação nos padrões de normalidade, *teaching files,* que se refere a arquivos de aprendizagem que o médico destaca, colocando seu parecer no exame, o que resulta na disponibilidade desse caso

clínico para que outros médicos possam utilizá-lo como parâmetro ou como continuidade de pesquisas.

1.3 ORGANIZAÇÃO DO TRABALHO

Este trabalho está organizado da seguinte forma: o capítulo 2 apresenta conceitos sobre computação em nuvem, PACS, PACS em nuvem, além de comentar sobre sustentabilidade, envolvendo computação; o capítulo 3 aborda conteúdos sobre segurança, federação e segurança através de identidades federadas; o capítulo 4 mostra o modelo de segurança proposto para PACS em nuvem, utilizando identidade federada para acesso aos exames médicos; o capítulo 5 apresenta o ambiente, os resultados e experimentos realizados, validando o modelo proposto; o capítulo 6 descreve as conclusões e trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 COMPUTAÇÃO EM NUVEM

A tecnologia vem proporcionando avanços significativos no universo da computação: serviços antes dedicados a supercomputadores são substituídos por estruturas virtuais mais confiáveis e eficientes. A utilização de recursos de *hardware* e *software* compartilhados torna-se presente em diversos segmentos e categorias, fazendo com que ambientes computacionais complexos fiquem flexíveis e transparentes para o usuário.

Capitais antes destinados à compra de *hardware* e *software* têm sido substituídos por economia, comprando-se serviços sob demanda. Empresas que investem maciçamente em *datacenters* a fim de manter serviços disponíveis todas as horas do dia, todos os dias do ano sem que seus usuários percebam a troca de servidores ou a inutilização de algum destes, tendem a possuir recursos de *hardware* em demasia. Tal sobra de recursos fez com que referidas empresas iniciassem um processo de utilização dos mesmos na forma de prestação de serviços sob demanda.

O termo computação nas nuvens apareceu para o mundo neste período onde grandes empresas como Amazon, Google e Microsoft começaram a prestar serviços sob demanda, através da utilização de seus *hardwares* na forma de empréstimo para terceiros, os quais precisavam de processamento e armazenamento. Junto a este novo modelo de negócios, estavam usuários avançados de computação que já compartilhavam processamento através da rede, além de produtos de *software* aparecerem como soluções para os usuários, sem que estes precisassem instalá-los em seus computadores pessoais.

O *National Institute of Standards and Technology* (NIST) define computação em nuvem como um modelo para acesso conveniente, sob demanda, e de qualquer localização, a uma rede compartilhada de recursos de computação (isto é, redes, servidores, armazenamento, aplicativos e serviços) que possam ser prontamente disponibilizados e liberados com um esforço mínimo de gestão ou de interação com o provedor de serviços (BROWN, 2011).

Pode-se dizer que computação em nuvem é o resultado da união de paradigmas computacionais tais como: virtualização, acordo de níveis de serviço e computação em grade, direcionados a disponibilizar serviço sob demanda baseados em modelos de negócios de computação utilitária (CHAVES, 2012).

A computação em nuvem oferece a capacidade de virtualizar os recursos, aliviando as organizações do fardo de investimentos pesados sobre o

software, *hardware*, plataforma e infraestruturas de recursos (CHOWDHARY, 2011). Estes investimentos são minimizados para pequenas quantias destinadas aos provedores de serviços da nuvem, que fornecem a possibilidade de acessar conteúdos e executar tarefas. Esta prática tornou-se simples e acessível para todos os níveis de usuários, bastando estar conectado à rede para desfrutar de opções como utilizar planilhas, necessitar de um servidor com um processamento maior, até mesmo jogar sem a necessidade de instalar o programa no computador.

2.1.1 Modelos de serviços

A computação em nuvem pode ser classificada através de três modelos de serviços (BROWN, 2011) e (SCHUBERT, 2011):

- *Software* como serviço (SaaS) : restringe o cliente ao uso de *software*, sem poder ter controle sobre a infraestrutura. Pode ser acessado de através de um navegador *web* ou acessando diretamente a interface de um programa;
- Plataforma como serviço (PaaS): o cliente tem controle sobre aplicativos implementados e as configurações para o ambiente de hospedagem de aplicativos na nuvem;
- Infraestrutura como serviço (IaaS): o cliente pode implementar e executar *softwares* arbitrários, tendo controle sobre sistemas operacionais, armazenamento e aplicativos implementados.

A figura 2 apresenta exemplos de aplicações de cada um dos modelos de nuvem.

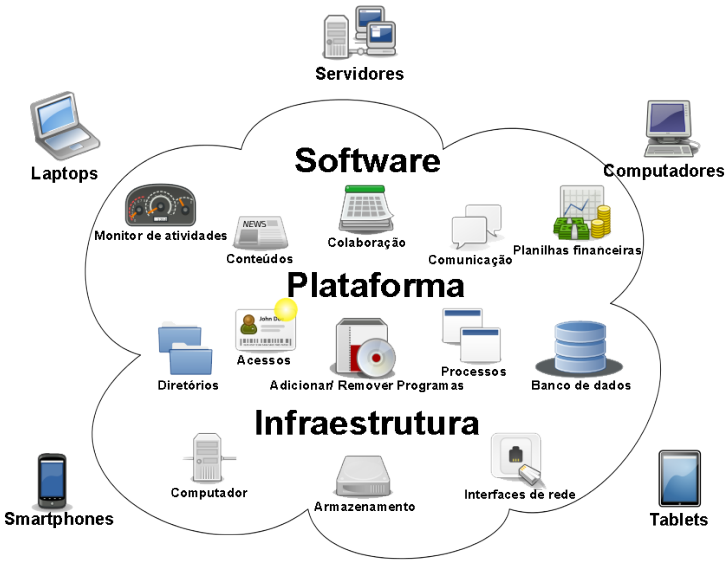

Figura 2 – Modelos de serviços para *Cloud Computing*.

Além desta classificação, as nuvens possuem formas variadas de implementação. As nuvens computacionais podem ser implementadas de quatro formas, e a política de segurança depende do processo de negócios, do tipo de informação e do nível de visão desejado (CHAVES, 2012):

- Nuvem Privada: Administrada pela própria empresa ou por terceiros, esta nuvem é acessada somente por uma organização. Para Sotomayor (2009) o principal objetivo da uma nuvem privada é proporcionar aos usuários uma infraestrutura ágil e flexível para suportar cargas de trabalho de serviços dentro do seu próprio domínio administrativo;
- Nuvem Pública: Disponível ao público em geral ou a um grande grupo empresarial, de acordo com Mell (2013), além de poder ser fornecida por uma organização que explora o serviço;
- Nuvem Comunitária: compartilhada por empresas com interesse em comum. Segundo Mell (2013), esta nuvem pode ser administrada por alguma das empresas que fazem parte da comunidade ou por terceiros; sendo assim, ela pode existir local ou remotamente;

- Nuvem Híbrida: Para Sotomayor (2009), é a composição entre a nuvem privada e a nuvem pública.

2.2 PACS (*PICTURE ARCHIVE AND COMMUNICATIONS SYSTEM*)

Em meados dos anos 80, surgiu a ideia de gerenciar o armazenamento das imagens digitais de diferentes modalidades em um banco de dados central. Este banco de dados é um sistema de arquivos que gerencia o armazenamento e responde a consultas às imagens e dados clínicos relacionados (BAKKER, 1991).

O sistema de banco de dados central é chamado de PACS. PACS pode adquirir, transmitir, armazenar e exibir informações de imagens médicas (ARENSON, 1992). Adquire imagens diretamente das modalidades, ou seja, equipamentos que geram imagens médicas; armazena as imagens em seu banco de dados central para que os hospitais e clínicas não precisem mais apresentar filmes radiológicos, resultando na redução de custos, ajudando na preservação da natureza; e além disso, PACS pode transmitir e exibir imagens médicas através de estações de trabalho. As estações de trabalho permitem manipular e processar imagens médicas. PACS aparece dentro da radiologia médica como solução para teleradiologia, que é uma parte da *e-health*.

Para Gondo (2002), uma forma de organizar teleradiologia é dividir em três camadas: geração de imagens, gerenciamento das informações e análise de imagens, em que uma camada depende da outra. A figura 3 mostra a dependência dessas três camadas: a geração de imagens é feita logo que o paciente vai ao hospital ou à clínica e realiza um exame de imagem. O gerenciamento das informações do exame acontece quando as imagens e dados do paciente são armazenadas no sistema de gestão da entidade de saúde. Esses sistemas são conhecidos como *Radiology Information System* (RIS) e/ou *Hospital Information System* (HIS), tendo a finalidade de gerenciar a distribuição das informações, a utilização dos recursos disponíveis, a localização dos dados adquiridos e os procedimentos de funcionamento da radiologia. Nota-se o PACS na análise de imagens quando médicos e outros profissionais da equipe técnica utilizam a ferramenta para manipular as imagens médicas através de técnicas de aperfeiçoamento de imagens, extração de medidas e transformações geométricas, além da mineração de dados em conjunto com informações simbólicas.

Figura 3 - Divisão em camadas da teleradiologia.

Sistemas PACS permitem realizar consultas através de textos vinculados às imagens, no entanto as consultas realizadas através de atributos da própria imagem podem facilitar o diagnóstico (BUENO, 2002). Também permite que o trabalho de radiologia seja realizado sem filmes, ou seja, *filmless*. O termo *filmless* refere-se a um ambiente médico com uma rede ampla e integrada, no qual os filmes são substituídos por sistemas eletrônicos que adquirem, arquivam, disponibilizam e exibem imagens médicas (SIEGEL, 2006).

Um servidor PACS tradicional é composto pelos seguintes componentes: repositório *Digital Imaging and Communications in Medicine* (DICOM) e sistema de banco de dados. O repositório de objetos solicita uma infraestrutura com capacidade de armazenamento para suportar todos os exames DICOM. O módulo de banco de dados suporta o modelo de informação DICOM, que contém informações de metadados relacionados aos pacientes, às séries dos exames e às imagens. Quando um PACS recebe exames das modalidades, ele armazena as imagens no repositório DICOM e atualiza o banco de dados com elementos extraídos do exame.

Além desses componentes citados, PACS possui outros três que englobam seu conceito: interfaces para dispositivos de geração de imagens digitais; estações de trabalho para acesso visual às imagens armazenadas e uma rede de comunicação para integração de todos os componentes. A figura 4 mostra o funcionamento de um sistema PACS.

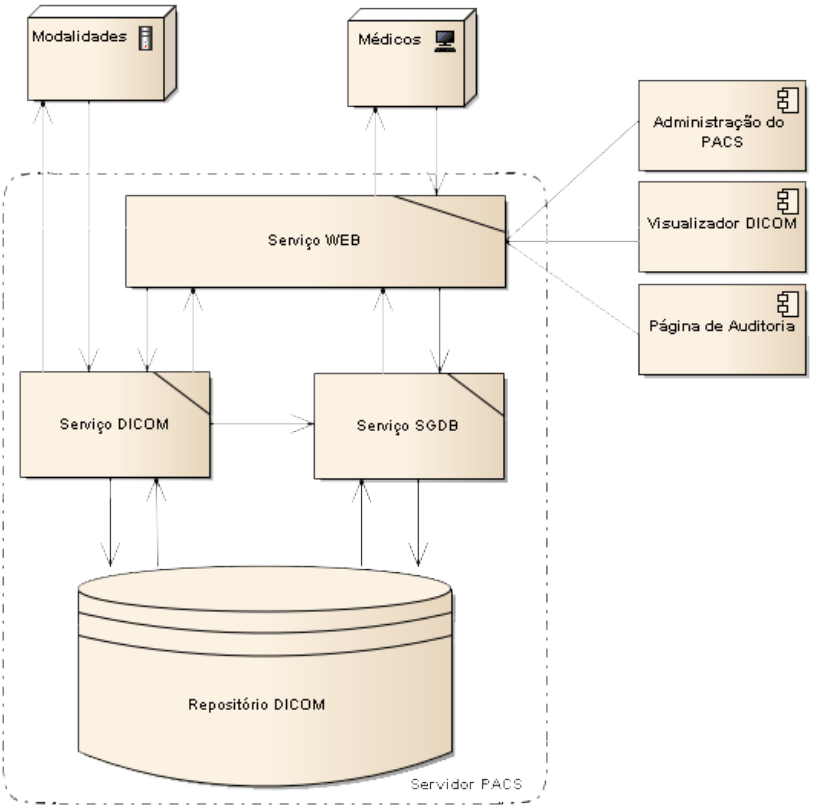

Figura 4 - Visão Geral do PACS.

Para Azevedo-Marques (2001), PACS é um sistema de arquivamento e comunicação que permite o pronto acesso, em qualquer setor do hospital ou clínica, de imagens médicas em formato digital, sendo caracterizado por quatro subsistemas: aquisição, exibição, disponibilização e armazenamento de imagens.

2.2.1 Arquitetura para PACS no modelo tradicional

Hospitais e clínicas possuem PACS implementado através de uma arquitetura tradicional, em que as modalidades após a realização do exame por parte do paciente enviam as imagens para o servidor localizado dentro da própria instituição. Os médicos têm acesso a esses exames por estações de trabalho que através de consultas, buscam as imagens do paciente e exibem-nas

em monitores. Com o PACS, os médicos também podem realizar impressões de imagens e laudos que serão entregues aos pacientes. A figura 5 exemplifica esta arquitetura tradicional descrita.

A figura 5 ainda mostra o processo de um médico que atende a mais de um hospital ou clínica. As instituições de saúde disponibilizam acesso ao PACS através da Internet para médicos que não ficam integralmente em suas dependências.

As imagens do exame do paciente, adquiridas nas modalidades, seguem o padrão DICOM. Modalidades, PACS, estações de trabalho e centrais de impressão de imagens comunicam-se através do protocolo DICOM, formando a rede DICOM. Esta rede é composta por equipamentos e sistemas que trocam mensagens neste padrão, facilitando o envio e o recebimento de arquivos por estes, mesmo que sejam de diferentes marcas, modelos ou versões.

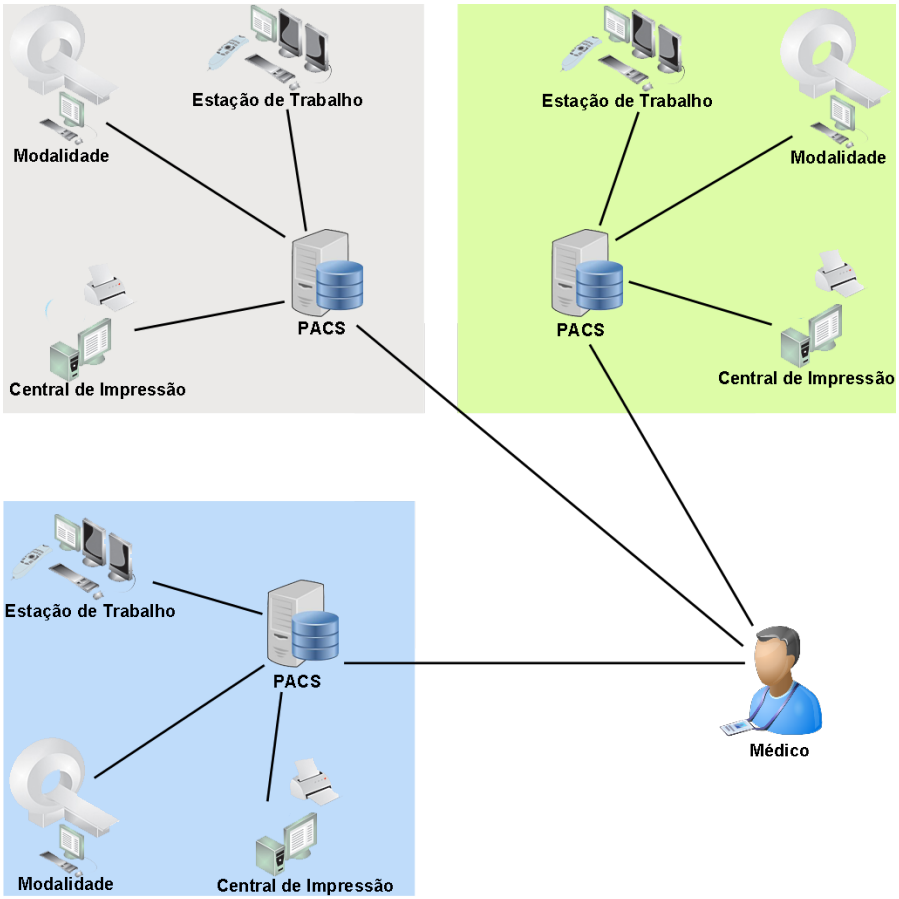

Figura 5 - Arquitetura tradicional para PACS.

2.2.2 DICOM (*Digital Imaging and Communications in Medicine*)

Equipamentos de diferentes áreas médicas devem possuir meios para representar informações sobre exames variados, realizados por pacientes em locais distintos. O *Digital Imaging and Communications Medicine* (DICOM) é um padrão na área de informática médica, elaborado pela associação *National Electrical Manufacturers Association* (NEMA).

As imagens armazenadas em PACS seguem o formato DICOM, sendo o padrão mais conhecido e fundamental quando se trata de imagens médicas (SOARES, 2013). É um padrão estabelecido em 1993 que revolucionou a prática da radiologia, permitindo a substituição da película de raios-X por um

fluxo de trabalho totalmente digital (NEMA, 2013). Representa um conjunto de normas para tratamento, armazenamento e transmissão de imagens médicas no formato eletrônico, que se encontra em sua terceira versão. O padrão DICOM surgiu como forma de tornar as imagens médicas digitais independentes dos dispositivos de fábrica, estabelecendo um método único para dispositivos médicos e facilitando a expansão de imagens médicas digitais (PIANYKH, 2011).

Este protocolo, não proprietário, de troca de dados no formato digital de imagem e estrutura de arquivo para imagens médicas, além de informações relacionadas à imagem, define a forma e o fluxo das mensagens eletrônicas que transmitem imagens e informações relacionadas entre equipamentos médicos e computadores. A figura 6 mostra um exemplo de uma imagem DICOM. A padronização das imagens médicas permite que dados possam ser trocados entre vários equipamentos de diferentes áreas médicas.

Figura 6 - Exemplo de imagem DICOM.

DICOM suporta diversas modalidades de imagens médicas sendo que todos os itens que compõem o padrão são divididos em grupos numerados, com base na similaridade do conteúdo (SOARES, 2013). Cada grupo numerado, por sua vez, é organizado por elementos individuais que são numerados da mesma forma; a esses números dá-se o nome de *tag*. A *tag* DICOM é constituída por um par de números que utilizam estrutura hexadecimal e representam grupo e elemento, como por exemplo, a *tag* "Modalidade" de aquisição do exame, que é representada por "0008,0060".

Através deste formato sempre que uma aplicação DICOM precisar fazer referência à modalidade ou equipamento que o paciente adquiriu, as imagens do exame, a *tag* a ser consultada, será a que possuir a identificação "0008,0060".

Pode-se notar que na figura 6 existem elementos que compõem a imagem, os quais representam informações referentes à imagem apresentada. Essas informações fazem parte das *tags* DICOM, onde cada informação está inserida em uma *tag*. Através dessas tags, o médico pode visualizar qualquer dado referente ao exame ou à imagem que está na tela.

2.3 PACS NO CONTEXTO DAS NUVENS COMPUTACIONAIS

A quantidade de imagens médicas aumentou significativamente ao longo dos últimos anos (TENG, 2010). O aumento no número de imagens do exame médico significa que o PACS terá de armazenar um enorme volume de dados e estes repositórios normalmente ficam dentro dos hospitais e clínicas. Devido ao aumento do número de imagens médicas, o sistema PACS precisa ser escalável, elevando, gradualmente, os custos com manutenção e infraestrutura.

Para Silva (2011), empresas e indústrias tendem a utilizar computação em nuvem, sendo, o mercado de saúde, um ótimo potencial de consumo devido à elasticidade e à escalabilidade da rede. Da aplicação de computação nas nuvens às soluções existentes surge o conceito PACS em nuvem. O acesso universal à informação a partir de qualquer lugar e hora, ainda enfatizando o poder de processamento e armazenamento a um custo inferior daquele praticado, faz com que PACS em nuvem seja uma solução adequada para médicos, pacientes e instituições de saúde.

A possibilidade de médicos utilizarem PACS em nuvem para acesso a exames realizados em cidades antes distantes geograficamente, mas próximas virtualmente; a prestação de serviços a hospitais e clínicas ao mesmo tempo com a mesma agilidade e eficiência que a ferramenta PACS disponibiliza; o atendimento aos exames a partir de qualquer lugar e momento utilizando computadores ou dispositivos conectados à Internet, são alguns dos benefícios que o conceito de utilização de PACS em nuvem permite.

Aos pacientes, esse conceito permite: que seus exames estejam disponíveis a médicos especialistas em pouco de tempo depois de realizados; o parecer médico com eficiência devido ao fato de o histórico estar disponível; a vantagem de não precisarem guardar seu histórico de exames e/ou transportar todos os laudos anteriores impressos.

Para instituições de saúde, utilizar PACS em nuvem a fim de minimizar os problemas de processamento e principalmente de armazenamento representa

a solução para os desafios enfrentados na implentação de PACS no modelo tradicional, em que as instituições possuem seu *hardware* e sistema de PACS local, como mostra a figura 1.

2.4 SUSTENTABILIDADE

A utilização do PACS em nuvem, vem de encontro com a filosofia da padronização da área de tecnologia da informação (TI) das empresas de saúde que visam à certificação ou à adequação aos cuidados com o meio ambiente, já que esse recurso proporcionará redução do consumo de papel e insumos necessários para a impressão de laudos, bem como a economia de energia elétrica e a redução de sucatas eletrônicas, gerando também menor custo financeiro à organização.

Para Werner (2012) e Geronimo (2013), na nuvem, os valores gastos com energia elétrica acontecem em níveis diferenciados, tais como: troca de dados entre usuário e nuvem, processamento dos dados na nuvem, sistemas de refrigeração e de manutenção dos datacenters. Para diminuir esses gastos e tornar as nuvens mais sustentáveis, deve haver um controle dos recursos com o objetivo de criar um equilíbrio entre rendimento e consumo de energia.

Com o auxílio de ferramentas que monitoram a nuvem, é possível gerenciar os recursos computacionais de modo que possam atender a um grande número de usuários em uma única infraestrutura distribuída. A utilização de servidores de alto desempenho possibilita que haja troca de tarefas entre servidores a fim de se economizar energia e controle de datacenters de modo que os ajustes na refrigeração sejam automáticos e os gastos com manutenção sejam mínimos.

3 CONCEITOS DE SEGURANÇA CONSIDERADOS NA PROPOSTA

Os sistemas vêm evoluindo ao longo dos anos e apresentam mudanças constantes. O número de vulnerabilidades em *softwares* cresce nas estatísticas, causando erros e danos na segurança dos ambientes computacionais (CSI, 2013).

Ao longo de 15 anos, o *Federal Bureau of Investigation* (FBI) busca, de várias formas, compreender os crimes cibernéticos com a finalidade de tornar o ambiente virtual mais atrativo e seguro para os usuários. Os crimes cibernéticos crescem a cada ano e empresas perdem muitos dólares com esses ataques, que em parte, poderiam ser evitados caso houvesse um investimento (CSI, 2013).

Computação em nuvem é um modelo que utiliza a Internet para disponibilizar serviços, tornando o ambiente que sustenta a estrutura da nuvem distribuído devido à utilização de diferentes domínios, sistemas operacionais, *softwares*, políticas de segurança, criptografia, dentre outros. A segurança deve prover a autenticidade, a confidencialidade, a integridade, a disponibilidade e o não-repúdio. Essas características devem garantir a proteção de um conjunto de informações, preservando o valor que possuem para cada pessoa ou organização (BELAPURKAR, 2009) e (GOLLMANN, 2011).

Pela forma como é oferecida, a computação nas nuvens torna-se alvo de usuários que procuram possíveis vulnerabilidades em sistemas distribuídos, a fim de terem acesso a informações privilegiadas sem autorização. O combate a esses intrusos nem sempre é uma tarefa simples, pois os mecanismos utilizados para invasão estão cada vez mais silenciosos, dificultando a percepção dos administradores de rede e sistemas especialistas em tomadas de decisão que monitoram a rede.

A seleção da quantidade apropriada de controles e recursos de segurança em um ambiente distribuído requer uma precisa avaliação de riscos. Os riscos levam a mudanças na forma de administrar a segurança conforme o tempo passa, devido à quantidade de dados armazenados e serviços oferecidos na nuvem. Toda a agilidade e o dinamismo que a nuvem oferece estão sujeitos a ataques discretos e variados, do mesmo modo como o domínio, que é implementado localmente, disponibilizando dados e serviços através da Internet.

3.1 AMEAÇAS

A preocupação com a segurança está presente nos momentos em que uma pessoa sente-se desconfortável, seja com uma situação financeira, pessoal, profissional e/ou utilizando alguma tecnologia. A tecnologia que causa

desconforto ao ser manipulada tende a deixar o usuário inseguro, preocupado, com medo e receoso quanto a sua aceitação. Desta forma, o usuário que vem ao longo do tempo absorvendo a necessidade de obter seguro a bens materiais e saúde recebe as mudanças tecnológicas preocupado com as ameaças que podem causar danos a ele.

Ao comentar sobre danos aos usuários, no que se refere à tecnologia, a atenção é voltada para os dados e serviços que estão compartilhados através da Internet, quando essas pessoas dependem, dia após dia, desses recursos. As soluções de melhoria em serviços apresentadas atualmente requerem um usuário cada vez mais enriquecido de conhecimento não voltado à praticidade na utilização, mas atento aos riscos expostos através das ferramentas disponíveis. Os riscos representam ameaças significativas quanto ao uso de informações privadas para alguma prática maliciosa, por parte das pessoas as quais fazem deste meio uma forma de tirarem proveito da situação.

Sendo assim, aproveitando as mudanças de tecnologias que ocorrem de tempos em tempos e aliadas aos erros que ferramentas apresentam ao longo de seu desenvolvimento, segundo Owasp (2013), as ameaças à segurança são provocadas por atacantes que utilizam vulnerabilidades, fraquezas que podem ser exploradas para colocar em risco ou causar danos a um recurso informacional, existentes nas aplicações, a fim de realizarem ataques. Ainda de acordo com Owasp (2013), os dez ataques mais praticados podem ser evitados tomando-se medidas de segurança com relação à configuração e à implementação dos sistemas. Sendo assim, ameaça é qualquer ato que possa causar danos ao sistema.

Burges (2006), comenta que essas ameaças podem ser físicas através de desastres naturais, falta de energia e guerras, dentre outras. Também podem ser humanas através de invasão, roubo, suborno, sabotagem, espionagem e acidentes, dentre outros; e ainda podem ser provocadas por *software*, através de vírus, cavalos de troia ou recusas de serviço.

3.2 MECANISMOS DE SEGURANÇA

Medidas podem ser tomadas a fim de se evitar ataques indesejáveis, devendo-se sacrificar um certo nível de conveniência para que medidas de disciplina sejam colocadas em prática (JONAS, 1987). Tal prática gerará sistemas com comportamento previsível, passível de proteção a ocorrências indesejadas, uma vez que o controle sobre o ambiente será rigoroso (BURGES, 2006). A proteção contra as ameaças requer medidas preventivas de identificação do conteúdo a ser protegido, avaliando-se as fontes de riscos para o desenvolvimento de contramedidas possíveis e eficazes.

Para Belapurkar (2009) e Gollmann (2011), os requisitos fundamentais para a segurança de um ambiente ou sistema são os seguintes:

- confidencialidade: garantir que as informações serão disponíveis somente aos usuários autorizados às mesmas;
- integridade: está ligada à capacidade do sistema de impedir a corrupção das informações por faltas intencionais ou acidentais; e,
- disponibilidade: deve garantir sempre o acesso autorizado às informações. O serviço de um sistema não pode ser interrompido por ações ou conhecimento de indivíduos não autorizados.

Para garantir esses requisitos, foram adaptados e desenvolvidos mecanismos de segurança, que quando corretamente configurados e utilizados, podem auxiliar na proteção contra os riscos envolvendo a Internet. Tais mecanismos devem garantir acesso e privilégio para restringir acesso aos dados de forma que somente pessoas autorizadas possam fazê-lo. Todo esse relacionamento de acesso e privilégio é baseado na confiança do usuário, para que a pessoa não tenha a intenção de causar algum dano ao sistema, seja na forma de ataque ou por roubo de informação. Os mecanismos de segurança desenvolvidos por sistemas contemporâneos passam a adotar algumas regras que visam proteger tanto as empresas quanto os usuários. Alguns desses mecanismos são abordados a seguir:

- Política de segurança: sempre há um nível de risco associado a qualquer sistema, mas a política de segurança define os direitos e responsabilidades de cada um, a segurança dos recursos computacionais que utiliza e as penalidades às quais se está sujeito. É um mecanismo que deixa claro para usuários o comportamento esperado de cada um, além de demonstrar o compromisso da organização com a eficácia da sua segurança. Deve assegurar que compromissos legais e contratuais sejam atendidos e que as ramificações econômicas de falha na segurança sejam conhecidas;
- Notificação de incidentes e abusos: um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, como uma tentativa de uso ou acesso não autorizado a sistemas ou dados, tentativa de tornar serviços indisponíveis, modificação em sistemas e o desrespeito à política de segurança. Todos os incidentes devem ser notificados a fim de se contribuir para a segurança com a intenção de ajudar na detecção de falhas. Esses incidentes são registrados através de relatórios completos contendo informações de data, hora, dados relacionados ao incidente e qualquer outra informação extraída no incidente;

- Criptografia: Através da criptografia, os dados são mascarados através de cifras com a intenção de evitar acessos indevidos a dados privados;
- *Backups*: Um dos mecanismos de segurança mais utilizados atualmente, o *backup* tem a finalidade de garantir ao usuário uma cópia de segurança. Proteção, recuperação e arquivamento são algumas das vantagens oferecidas pelo *backup* que o usuário deve manter atualizado e em local seguro e bem condicionado. Pode ser realizado de maneira *on line*, ou seja, na própria Internet;
- Registro de eventos: É a atividade realizada por sistemas de computador, que armazena arquivos no computador para serem analisados. Essas análises têm vários objetivos, entre eles: detectar o uso indevido do computador, monitorando as ações dos usuários; detectar algum tipo de ataque, monitorando o comportamento e as ações do sistema; auditar ações executadas pelos usuários para garantir a performance do sistema; detectar problemas em *hardware* ou programas e serviços executados pelo computador;
- Contas e senhas: o uso de contas e senhas é um mecanismo de autenticação comum usado nos serviços oferecidos na Internet. O conhecimento das senhas envolve apenas um dos fatores da autenticação, que é algo que o usuário sabe. Outros fatores possíveis a serem usados na autenticação são: algo que o usuário tem posse (como um cartão físico) ou algo que o usuário tem como característica biométrica (impressão digital, retina).

3.3 SEGURANÇA EM SAÚDE

A relação médico/paciente é restrita, cabendo ao médico o sigilo e ao paciente, a publicidade das informações envolvidas nesta relação. Com a adoção de mecanismos que se interpõem nesta relação, torna o conteúdo da informação passível de falhas que estão diretamente ligadas às ameaças encontradas em sistemas distribuídos, pois a área de *e-health* está multiplicando-se para abranger todas as pessoas. Com a utilização de *e-health*, toda informação privada referente ao paciente fica disponível na rede, cabendo à instituição de saúde a garantia da segurança da informação.

A segurança desta relação é tema central em debates envolvendo a evolução da *e-health* nos principais países do mundo. Para Peyton (2007), a União Europeia e o Canadá possuem as legislações mais rígidas quando se trata de controle de privacidade de informações médicas. A implementação dos mecanismos de segurança para combater as ameaças que exploram as

vulnerabilidades existentes em serviços oferecidos via Internet torna a *e-health* complexa.

Mesmo com a adoção destes mecanismos por parte das instituições de saúde, novos estudos e soluções são desenvolvidos e implementados para que os pacientes sintam confiança ao utilizar a *e-health* e os médicos sintam-se à vontade para experimentar essas soluções. Uma das maneiras propostas para segurança em *e-health* aparece no uso de federações.

3.4 FEDERAÇÃO

O termo federação aparece na história do Brasil como diversas entidades territoriais autônomas dotadas de um governo próprio, mas que quando unidas, tornam-se uma federação. O Brasil é um país federativo, pois possui estados autônomos de governo próprio mas unidos através de uma constituição.

A evolução da tecnologia é parte integrante do processo de como fazer negócios, pois torna-se chave do compartilhamento de informações e serviços entre organizações. Esta capacidade de compartilhar informações traz a responsabilidade de protegê-las para que perdas de negócios, responsabilidade civil e regulamentos governamentais sejam motivos para não serem acessados por pessoas não autorizadas.

Negócios exigem o compartilhamento de informações entre organizações, sendo necessário determinar o volume de informações a serem compartilhadas para se atingir a meta do negócio. Desafios aparentes podem tornar essa troca de informações complicada, baseados em tecnologia. As consequências da divulgação de informações sigilosas, bem como o acesso ilegal à informação, e o compartilhamento de informações excedentes ao acordado, são desafios com os quais as empresas se deparam quando fazem negócios baseados na confiança (CHONG, 2013).

Segurança baseada em federação utiliza o conceito de confiança, pois uma estrutura de autenticação e autorização federada é constituída por dois elementos principais: provedores de identidades - que são responsáveis pela manutenção das informações sobre usuários e sua autenticação - e os provedores de serviço, que oferecem acesso a um recurso ou serviço específico. Há relação de confiança entre os provedores de serviço e os provedores de identidades (REDE NACIONAL DE ENSINO E PESQUISA, 2013).

3.5 IDENTIDADE FEDERADA

A identidade de uma pessoa é composta por uma quantidade de informações pessoais que a caracterizam em diferentes contextos dos quais

essa faz parte (CLAUß, 2001). No contexto da saúde, as características podem ser nome, idade, tipo sanguíneo, peso, altura, CPF, identidade, número do plano de saúde, exames realizados, laudos médicos, dentre outras. Essas informações são utilizadas para identificar um paciente no ambiente de saúde e no mundo digital.

Assim que iniciam uma conversa, as pessoas podem escolher que informações suas vão passar para outras. No ambiente virtual, o responsável pela troca de informações é o gerenciador de identidades (WANGHAM, 2010). O gerenciador de identidades filtra as informações e durante a troca de mensagens, envia somente aquelas necessárias ao requisitante. Para Bhargav-Spantzel (2007) e Wangham (2010), um gerenciador de identidades deve apresentar as seguintes características:

- Usuário: pessoa que deseja acessar algum serviço;
- Identidade: conjunto de características do usuário;
- Provedor de Identidades (IdP): responsável por emitir a identidade de um usuário;
- Provedor de Serviços (SP): oferece recursos aos usuários autorizados.

Os gerenciadores de identidades podem ser classificados de acordo com as diferentes formas de interação e disposição de suas características. O modelo apresentado neste projeto é o federado, que consiste na distribuição da tarefa de autenticação dos usuários por múltiplos provedores de identidade, estando, estes dispositivos, em diferentes domínios. A figura 7 mostra um esboço do modelo federado.

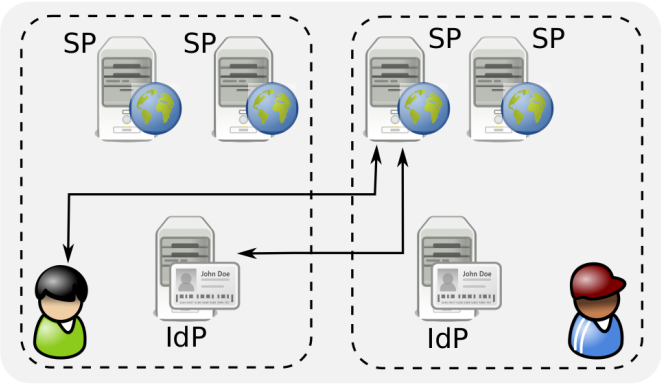

Figura 7 - Modelo de identidade federada [GERENCIAMENTO DE IDENTIDADES, 2013].

O conceito de identidade federada é utilizado para fornecer confiabilidade entre as instituições de saúde através da implementação do acesso seguro. Os usuários são representados por identidades as quais são uma representação de uma entidade (ou grupo de identidades) sob a forma de um ou mais elementos de informação (atributos), que permitem à entidade ser reconhecida apenas dentro de um contexto (LEANDRO, 2012).

A identidade federada visa facilitar a partilha de bens digitais entre instituições e organizações, ligando os seus serviços de autenticação, possibilitando acesso aos recursos digitais para uma população identificada sem ter de administrar localmente os usuários (LAYOUNI, 2009).

Sendo assim, médicos, através de suas identidades federadas, podem ter acesso a diversos serviços de hospitais e clínicas que fizerem parte de uma federação.

4 MODELO DE SEGURANÇA PARA PACS EM NUVEM

Neste capítulo é apresentada uma proposta de modelo e arquitetura abrangendo a utilização de PACS em nuvem a fim de se organizar o arquivamento dos exames de diferentes locais em um repositório centralizado, diminuindo os investimentos em infraestrutura de armazenamento e processamento por parte dos hospitais ou clínicas para futuras leituras ou até mesmo futuros diagnósticos em qualquer instituição da saúde. Além disso, o modelo contempla a utilização de identidade federada como método de acesso ao sistema PACS em nuvem, que possibilita ao médico autenticar-se na nuvem que utiliza identidade federada para fornecer confiabilidade entre as instituições de saúde, através da implementação do acesso seguro. Também são mostradas as ferramentas que dão suporte ao modelo e arquitetura apresentados.

4.1 PACS COM SEGURANÇA EM NUVEM

Como médicos atendem em diversas clínicas ou hospitais, ou em ambos, precisam acompanhar, com frequência, muitos pacientes através de exames de imagem, além das instituições de saúde terem a possibilidade de investirem pequenos valores na infraestrutura de processamento e armazenamento de exames. Este trabalho propõe um novo modelo para utilização segura de PACS. O sistema é disponibilizado na nuvem como SaaS e os médicos têm acesso ao serviço através de dispositivos conectados à Internet, conforme mostrado na figura 8.

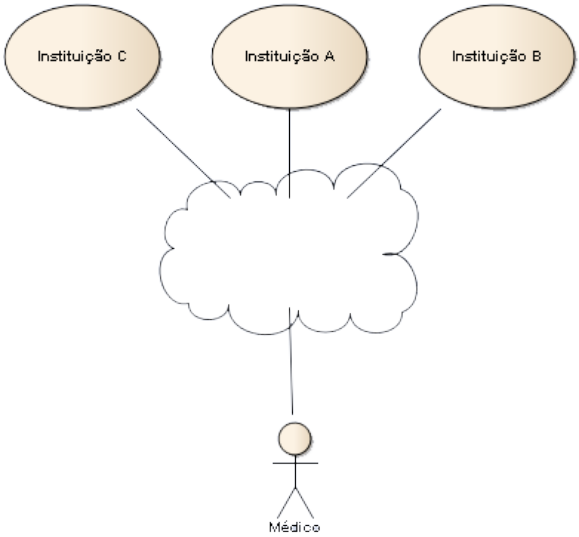

Figura 8 – Nuvem para instituições com PACS.

4.2 NUVEM COMPUTACIONAL PARA INSTITUIÇÕES COM PACS

Hospitais e clínicas têm a possibilidade de ter PACS implementado através de uma nuvem SaaS, em que as modalidades, após a realização do exame por parte do paciente, enviam as imagens para a nuvem diretamente com o auxílio de um roteador. Os médicos têm acesso a esses exames através de um dispositivo que faz acesso à nuvem, para buscar e exibir imagens de pacientes com exames realizados em cidades distantes ou anteriormente. A figura 9 exemplifica a arquitetura descrita mostrando dinamismo para o médico realizar um diagnóstico mais eficiente e preciso, bem como hospitais e clínicas distantes de grandes centros contarem com o apoio de médicos especialistas e economizarem com estrutura de armazenamento e processamento.

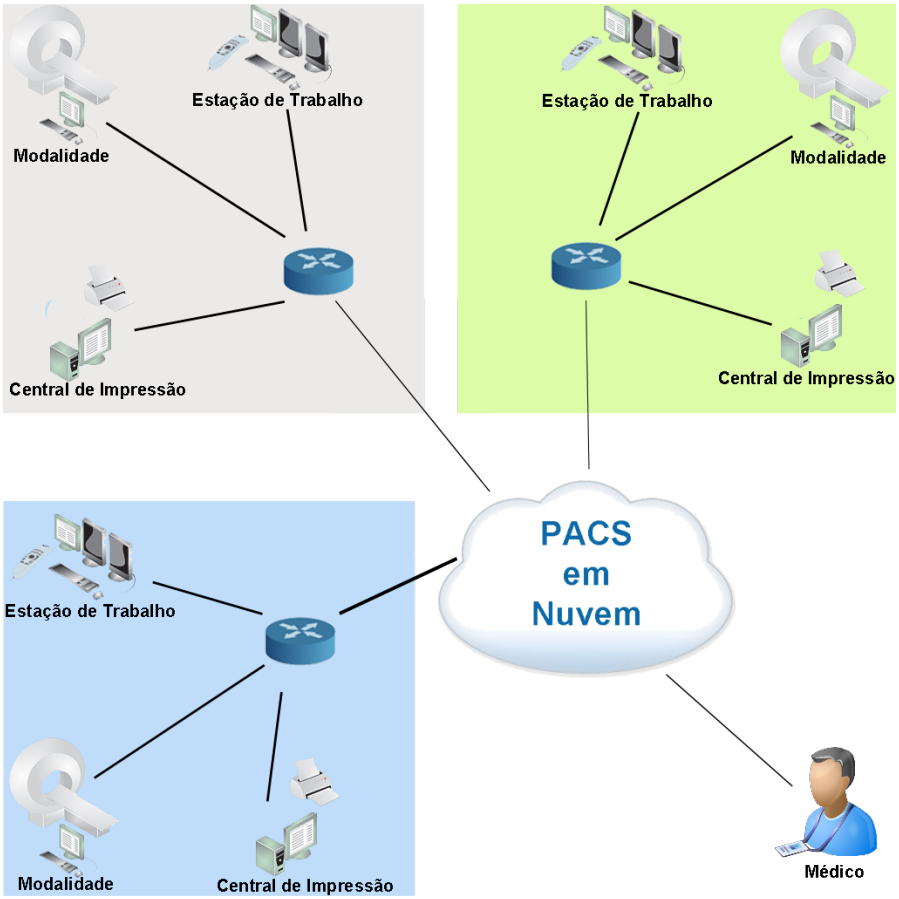

Figura 9 – Componentes da nuvem SaaS utilizando PACS.

4.3 FERRAMENTAS UTILIZADAS NA NUVEM COM PACS

4.3.1 *OpenLdap*

OpenLdap é um uma ferramenta de licença gratuita implementada com *Lightweight Directory Access Protocol* (LDAP) e desenvolvido pelo projeto *OpenLdap*. Iniciado em 1998 por Kurt Zeilenga, que clonou a referência *Ldap* da Universidade de Michigan, é liberado sob licença BSD, chamada de licença pública *OpenLdap*, sendo um protocolo independente de plataforma.

O LDAP é um protocolo baseado em diretório que funciona sobre TCP/IP, que segue o modelo de árvore de nós X500. Seu dinamismo desponta

como um ótimo modelo de representação para dados organizacionais e limítes políticos.

Com o suporte destes modelos pôde-se desenvolver uma estrutura que representasse a hierarquia para usuários de PACS em nuvem. Desta forma, o LDAP dá suporte à base de dados onde estão armazenados os usuários e suas informações. A figura 10 mostra a estrutura criada, em que usuários fazem parte do grupo pessoas, que por sua vez possuem atributos, tais como: *uid*, que representa o usuário; *cn*, que é o primeiro nome do usuário; *sn*, o sobrenome do usuário; e *userPassword,* atributo que contém a senha criptografada do usuário.

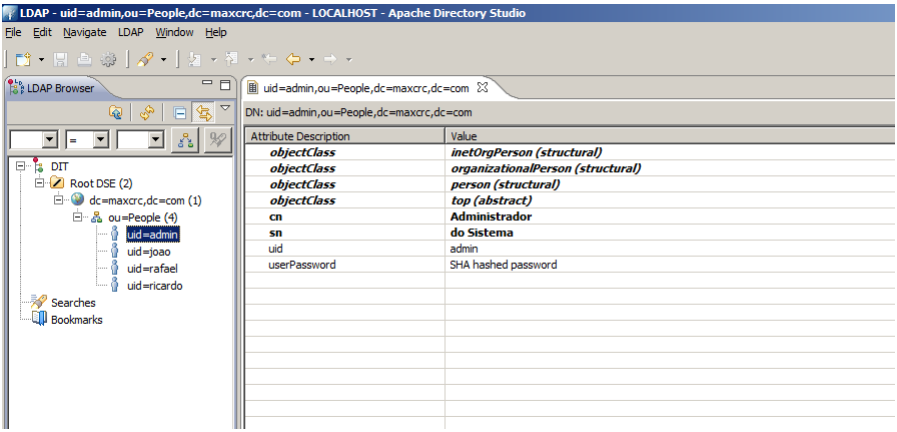

Figura 10 - Estrutura LDAP.

4.3.2 Shibboleth

A palavra *Shibboleth* teve seus primórdios em uma aparição no livro bíblico, o livro dos Juízes, e conta que duas tribos, os Eframitas e os Gileaditas, na época, travavam grandes batalhas. Certa vez, às margens do Rio Jordão, quando Eframitas tentaram atravessá-lo em direção ao seu território, sentinelas Gileaditas abordaram todas as pessoas pedindo para pronunciarem a palavra Shibboleth. Devido aos dialetos existentes naquela época, Eframitas e Gileaditas pronunciavam de maneira diferente esta palavra: enquanto os Gileaditas falavam com som sh, os Eframitas pronunciavam com som de s. Os sentinelas Gileaditas deixavam passar somente quem conseguisse pronunciar Shibboleth com som sh.

A ferramenta Shibboleth é utilizada para formar uma federação através do estabelecimento de uma relação de confiança entre partes: previamente são definidas chaves criptográficas para as trocas de mensagens e também

formatos padronizados para a semântica e sintaxe das identidades e atributos. Em uma federação, como uma parte confia na outra, os usuários podem se autenticar uma única vez, *Single Sign On* (SSO) e ter acesso a vários serviços de diferentes provedores da federação. As informações trocadas entre os provedores de serviço e provedores de identidade segue o acordo de segurança estabelecido pela federação (GHAZIZADEH, 2012) e (KHATTAK, 2010).

A troca de informações utilizada no Shibboleth é semelhante à troca de informações exercida pelos sentinelas Gileaditas com as pessoas que tentavam atravessar o rio Jordão. Existiam regras distintas naquela época quando comparadas às atuais, mas ambas pelo mesmo motivo: o acesso. Desta forma, a Internet2 criou uma arquitetura e implementação de código aberto para gerenciamento de identidades e autenticação baseada em identidade federada e infraestrutura de autorização, ou controle de acesso, baseado em *Security Assertion Markup Language* (SAML).

Para Oasis (2013), SAML é um padrão que define formas de se usar o *Extensible Markup Language* (XML) para representação de informações de autenticação e de atributos, definindo um protocolo para requisição e recebimento de credenciais de uma autoridade SAML.

O Shibboleth permite criar uma estrutura segura que simplifica o gerenciamento de identidades e fornece ao usuário SSO, eliminando a necessidade de manter nomes de usuário e senhas em cada um dos provedores de serviço. Pode-se dividir o Shibboleth em duas entidades: IDP - responsável pela autenticação dos usuários, mantendo o controle de suas credenciais e atributos, divulgando esta informação aos pedidos das organizações parceiras - e SPs - onde os recursos são armazenados e acessados pelo usuário, aplicando o controle de acesso aos recursos com base em informações enviadas pelo IDP, sendo que um único SP pode ser composto de várias aplicações, mas continuará a ser tratado como entidade única por um IDP.

4.3.3 Dcm4chee

Em 2013, de acordo com dcm4che, a ferramenta PACS disponibilizada teve início no ano 2000 quando Gunter Zeilinger escreveu o JDicom utilizando o Java DICOM *Toolkit* (JDT). Após essa experiência, desenvolveu seu DICOM *Toolkit* com a intenção de enviar para Sun uma API baseada em Java DICOM. Mas a popularidade alcançada do Toolkit entre os desenvolvedores DICOM fez com que a ferramenta evoluísse para uma plataforma mais robusta e estável para o gerenciamento de estudos de imagem e relatórios. Assim nasceu a ferramenta dcm4chee.

Por ser um projeto *open source* de simples implementação em ambientes como OSx da Apple, Linux e Windows, além de ser utilizado por muitos

profissionais na área da saúde, projetos de pesquisa, aplicações de código aberto, bem como aplicações comerciais, é que foi escolhida esta ferramenta.

A implantação do dcm4chee versão 2.17 mostra-se simples e flexível. A ferramenta PACS é instalada em um ambiente Ubuntu Sun JDK e o banco de dados PostgreSQL Server. A figura 13 mostra a tela principal do PACS em que são listados os exames contidos na base de dados.

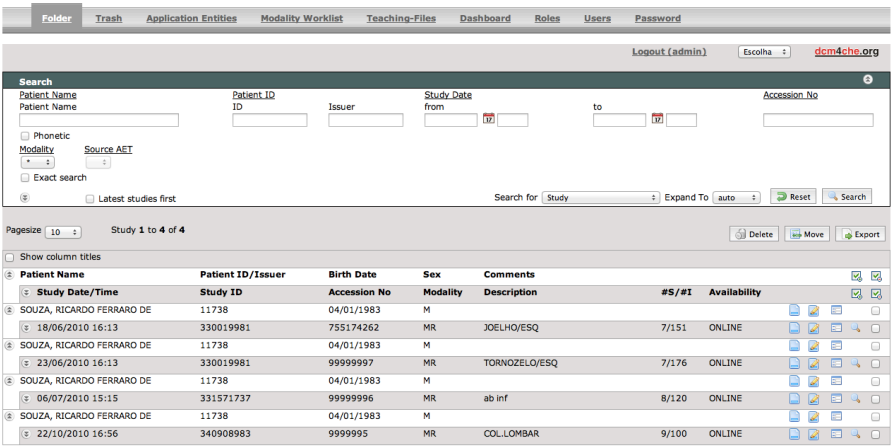

Figura 11 - Tela principal do PACS.

4.4 PRINCIPAIS CONTRIBUIÇÕES E TRABALHOS CORRELATOS

Em Chen (2000), é descrito um processo que transfere dados do PACS através de uma rede *General Packet Radio Services* (GPRS), em que o recurso inclui alocação de canal de pacotes dinâmicos e a de largura de banda variável. Prevê-se que a aplicação fornecerá informações sobre o funcionamento do protocolo e o desempenho, além de estimular revisões dos procedimentos básicos. Seu foco não é diretamente os exames médicos, mas dados do PACS que serão enviados através da comunicação GPRS para monitorar a transferência e explorar o protocolo, comparando-se com protocolos de redes sem fio existentes.

Em Silva (2011), é descrito um componente cujo foco é transcrever um comando DICOM em não-DICOM, bem como não-DICOM em DICOM. O componente filtra informações que o PACS recebe e envia, além de monitorar o *storage* onde ficam armazenados os exames. O componente é implementado através de regras definidas na arquitetura do PACS em nuvem, provendo alto nível de segurança que respeita a privacidade das três entidades envolvidas: hospitais, médicos e pacientes. O módulo ainda oferece a possibilidade de

gravar em múltiplos *storages*. Comenta as vantagens de utilizar PACS em nuvem, a economia que a instituição passa a ter com redução de processamento e armazenamento de imagens, bem como a diminuição da quantidade de dados que entram e saem da instituição, dominuido a manutenção da infraestrutura.

Em Ni (2007), são descritas algumas aplicações de PACS usando *grids* computacionais, alguns federados. O foco do trabalho é monitorar recursos e dados em diferentes *grids*, com ênfase no gerenciamento total do *grid*. Os resultados mostram que as abordagens garantem a transmissão confiável, melhor seleção, recuperação de desastres e otimização de custos pelo sistema de gestão de recursos baseado em políticas.

Em Tohme (2006), é descrito um estudo para uso de *grid* computacional para auxliar diagnósticos a distância, em que o foco é um amplo estudo de um *middleware* técnico. A utilização do *grid* serve para distribuir imagens médicas, armazenamento e processamento de exames médicos entre hospitais que estejam conectados e compartilhando recursos através da Internet. Exames realizados nos hospitais ficam armazenados, disponibilizando-se o acesso aos recursos de processamento para manipulação deste exame. O processamento pode ser compartilhado através do *grid* computacional. O processo não é desmonstrado, somente comentado.

Este trabalho descreve e apresenta um modelo e uma arquitetura para hospitais e clínicas armazenarem e disponibilizarem exames médicos com segurança na nuvem. Este modelo proposto no estudo para a área médica pode ser utilizado em diversos segmentos da telemedicina e adaptado às demais áreas de atuação. Demonstra a implementação e o funcionamento do processo envolvendo o acesso a PACS em nuvem federada, além de mostrar que através de PACS baseado em nuvem, as instituições de saúde possuem uma solução para telerradiologia, utilizando conceitos de segurança, escalabilidade e confiança. Os trabalhos estudados apresentam sistemas PACS federados e não federados, porém sem abranger profundamente o tema, sem demonstrar a federação implementada com PACS baseado em nuvem, como é apresentado e descrito neste trabalho.

5 VALIDAÇÃO DA SEGURANÇA PARA PACS EM NUVEM COM IDENTIDADE FEDERADA

Neste capítulo, é apresentado o ambiente implementado para representar a infraestrutura de acesso ao PACS em nuvem através de identidade federada, bem como os resultados obtidos na implementação desta infraestrutura.

Para o desenvolvimento da infraestrutura, são utilizadas as ferramentas apresentadas no capítulo anterior, que fornecem suporte ao ambiente visando estabelecer uma federação para o acesso ao sistema PACS. Para estabelecer a federação, é utilizado o Shibboleth IDP e SP; o dcm4chee, que é um sistema PACS, contemplando os principais componentes como aquisição, exibição, disponibilização e armazenamento de imagens DICOM. O repositório contendo os usuários é gerenciado pelo OpenLdap.

A representação do acesso ao PACS é mostrada na figura 12, em que as setas numeradas indicam a ordem dos acontecimentos dentro do ambiente e interação do usuário. O número 1 indica que o usuário faz o acesso no Shibboleth SP, quando verifica as configurações dos metadados com o o Shibboleth IDP em 2 e 3; e sendo válidas as configurações, retorna ao usuário a tela de login da federação em 4. Em 5, o usuário preenche com as informações solicitadas e esta requisição vai diretamente ao Shibboleth IDP, que verifica as credenciais do usuário na base de dados LDAP em 6 e 7, em que retorna ao Shibboleth SP solicitando acesso ao serviço do usuário em 8 caso os dados sejam validados. O Shibboleth SP verifica se o serviço está disponível em 9 e redireciona o usuário à tela principal da aplicação em 10. Em 11, o usuário pode interagir diretamente com o serviço disponibilizado.

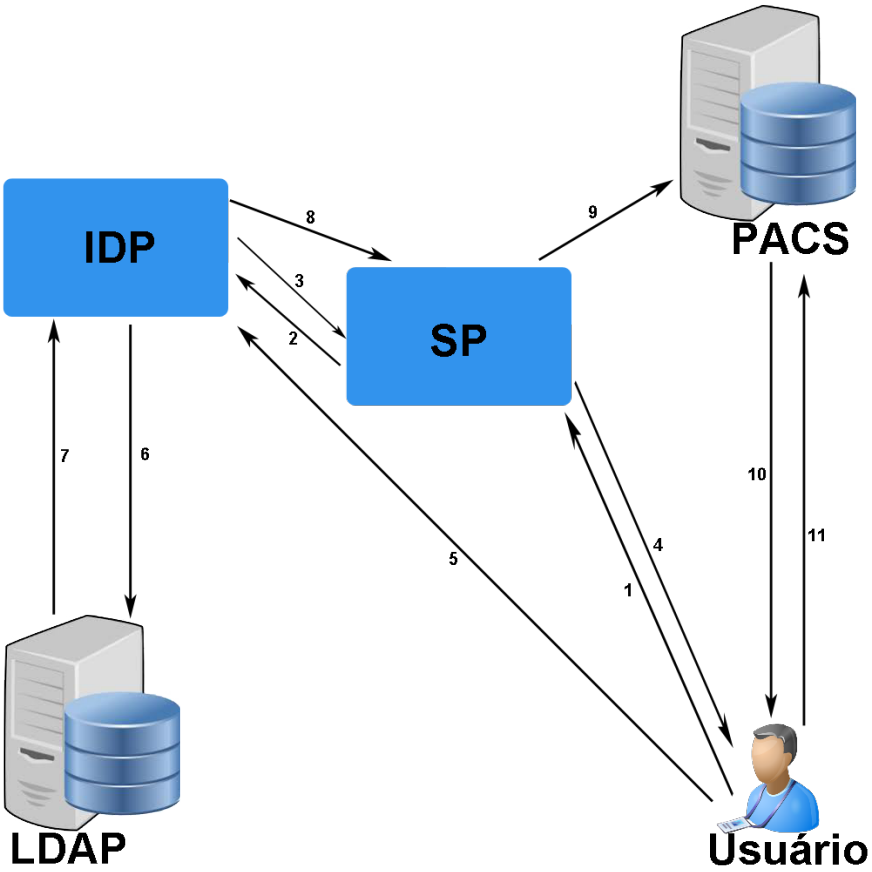

Figura 12 – Implementação do Shibboleth para PACS em nuvem.

5.1 DESCRIÇÃO DA IMPLEMENTAÇÃO REALIZADA

A nuvem é implementada através de máquinas virtuais criadas a partir da ferramenta Oracle Virtual Box. O sistema operacional utilizado para implementação do Shibboleth IDP e o OpenLDAP é o Windows Server 2008, escolhido devido a sua flexibilidade. O Shibboleth SP é implementado em uma plataforma Windows 7. A outra máquina virtual escolhida está implementada em plataforma Linux com Ubuntu, suportando a ferramenta PACS. Três computadores são utilizados para dar suporte à virtualização do ambiente descrito.

O processo que cria a federação passa pela troca de informações entre o IDP e o SP, sendo, o Shibboleth, a ferramenta que implementa e contempla estes dois módulos para formar a federação. O Shibboleth IDP é configurado para validar o metadata do Shibboleth SP através do arquivo *relaying-party.xml*. Além disso, esse arquivo possui as informações sobre o metadata do gerenciador de identidades. Esta validação sendo configurada, disponibilizará um módulo para realizar a autenticação na federação.

Os arquivos *Metadata.xml e idp-metadata.xml* são os que contêm as chaves públicas responsáveis pela validação do SP e do IDP respectivamente. Além disso, os metadatas possuem informações que a federação utiliza durante os acessos realizados, que inclui redirecionamentos a ações a serem tomadas durante a autenticação e também durante a saída do usuário.

Obtida a validação do IDP e SP por parte da federação, é apresentada uma forma de autenticação do usuário, através de *login,* com a informação de usuário e senha. Para validar as informações que o usuário insere, a federação troca dados entre o IDP e o SP através dos arquivos *attribute-filter.xml* e *attribute.xml* respectivamente. Esses arquivos contêm informações referentes à declaração dos atributos configurados na federação e disponíveis para o usuário que realiza o *login*, além de possuírem estrutura de classes *inetOrgPerson*. As informações da estrutura de classes verifica-se no arquivo *atribute-resolver.xml*. Além do mais, os atributos configurados para a autenticação na federação são *uid* e *userPassword,* que representam respectivamente usuário e senha da pessoa.

Durante a autenticação, o Shibboleth verifica os valores inseridos nos atributos na base OpenLdap, que estão configuradas nos arquivos *atribute-resolver.xml* e *loging.config*, que ficam no IDP. Tais arquivos contêm informações referentes de acesso à base de dados LDAP. Após autenticar o usuário, de modo que faça a autenticação uma única vez, o provedor de identidades repassa o resultado dessa autenticação ao provedor de serviços e cria uma sessão de uso associada ao usuário, de forma que acessos a novos serviços dentro de um determinado intervalo de tempo não gerem novas requisições de autenticação.

Além da garantia de autenticação, o provedor de serviço poderá requisitar ao provedor de identidade informações adicionais (atributos) sobre o usuário. Esses atributos podem ser utilizados para estabelecer as autorizações do usuário com respeito ao recurso ou serviço acessado.

Realizada a autenticação através do Shibboleth, é o momento de fazer com que a sessão do Shibboleth tenha validade no PACS. Para que o dcm4chee funcione com o Shibboleth, é alterado o código fonte do sistema e compilado novamente.

Então, é criado um filtro na aplicacão para interceptar todas as requisições *Hypertext Transfer Protocol* (HTTP) e verificar se elas estão passando pelo controle de acesso no Shibboleth SP, que é executada em um sevidor apache.

O nome do filtro é "*ShibbolethSingleSignInFilter*". É criado em um componente fora da aplicação para que este filtro possa ser reutilizado para outras aplicações.

Caso a requisição HTTP não possua as variáveis que o Shibboleth SP insere no cabeçalho da requisição, o filtro redireciona o usuário para o Shibboleth SP configurado.

Após a conclusão do filtro, é alterado na aplicação o ponto onde ela carrega os dados do usuário, que vêm do *Java Authentication and Authorization Service* (JAAS), para ler os dados que o filtro coloca no *principal* da *request*. O filtro obtém o ID do usuário, que vem do Shibboleth, e insere no objeto principal que está na requisição HTTP.

Sendo assim, é alterado o método "*mapSwarmSubject*" da classe *LoginContextSecurityHelper*, que é responsável por carregar os dados do usuário que o JAAS armazena. O *org.dcm4chee.web.common.login.LoginContextSecurityHelper.mapSwarmSubject*(*ApplicationSubject, SecureSession*) é alterado para que a aplicação obtenha o identificador do usuário que vem no *principal* pelo *ShibbolethSingleSignInFilter*. Depois de obter esta informação, a aplicação carrega as *roles* deste usuário, que estão no banco de dados do PACS. Realizado esse procedimento, a aplicação continua em seu fluxo normal.

Ainda no dcm4chee, é alterado o arquivo *web.xml* para remover as configurações de segurança, que agora não são mais realizadas diretamente na aplicação, mas no Shibboleth SP. Após a adição do filtro, que verifica as variáveis do SP, o usuário é redirecionado novamente ao processo de autenticação caso elas não existam.

Também são removidas por completo as configurações de segurança com JAAS no *jboss-web.xml*, que identifica um contexto protegido para o jboss gerenciar. Com essa configuração removida, a aplicação não gerencia mais a segurança diretamente.

Para realizar o *logout,* em vez de invalidar a sessão do usuário, como é praticado pela aplicação, uma alteração se faz necessária para que depois que invalide a sessão do usuário, redirecione-o para uma *Uniform Resource Locator* (URL) no SP, que faz o invalidamento da sessão do usuário no IDP também.

A destruição da sessão do usuário no IDP, realizada pelo SP, tem de ser configurada no arquivo *handle.xml* no IDP. São adicionadas *tags* XML para dar suporte à destruição da sessão do usuário no IDP, como mostra o Apêndice

A. No SP, é configurado no arquivo *shibboleth2.xml* uma *tag* XML para chamar uma página de *logout* padrão do Shibboleth SP, que invalida a sessão no SP. Esta página de *logout* é alterada para realizar uma chamada ao IDP, com a intenção de acionar a função de *logout* no IDP ao mesmo tempo que no SP. Sendo assim, fica garantido que as sessões do usuário no IDP e no SP se tornaram inválidas.

Sem a adoção do filtro criado, o acesso ao PACS é realizado através da tela de *login* do dcm4chee, que é configurada e segura pelo JAAS como mostra a figura 13.

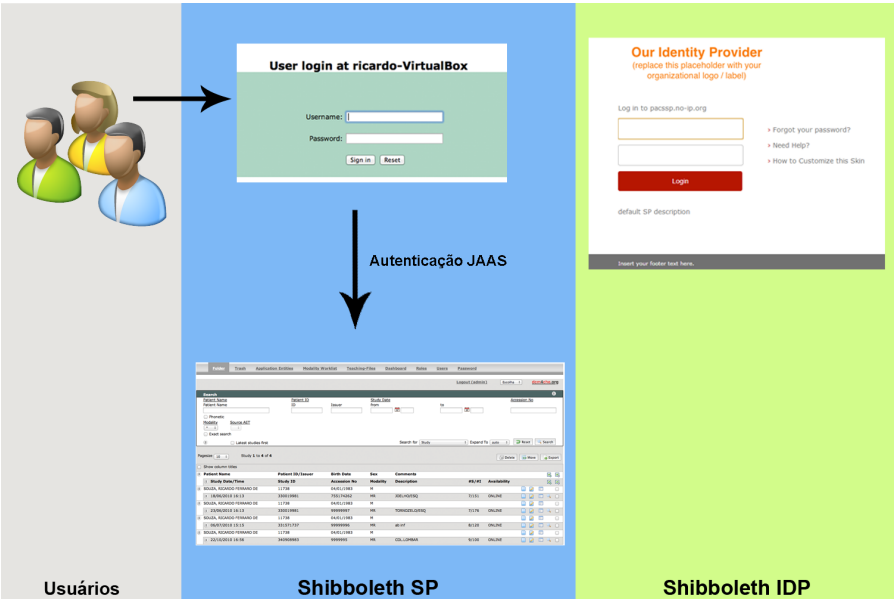

Figura 13 - Acesso ao PACS com JAAS.

Com a adoção do filtro, o acesso ao PACS é realizado através da tela de *login* do Shibboleth, que é configurada e segura por uma federação como mostra a figura 14. O novo modo de acesso ao PACS através do Shibboleth possibilita ao usuário a autenticação utilizando o conceito de identidade federada.

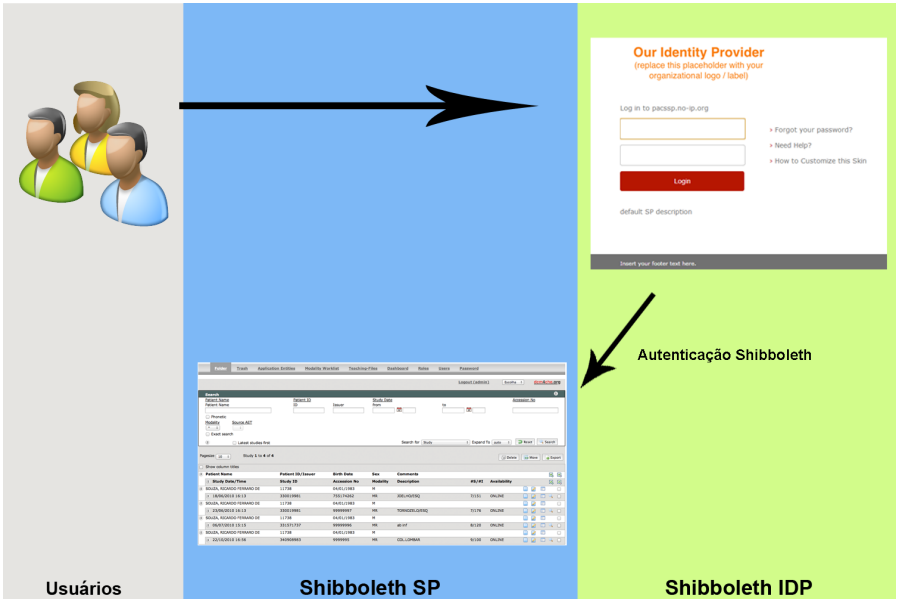

Figura 14 - Acesso ao PACS com Shibboleth.

5.2 RESULTADOS OBTIDOS

O funcionamento da solução apresentada neste trabalho é obtido através de dois casos de uso. No primeiro caso, é descrito o acesso ao PACS em nuvem através de um *tablet*.

No segundo, é descrito o acesso ao PACS em nuvem através de um computador.

5.2.1 Caso 1

Nesta abordagem, o PACS em nuvem é acessado através de um *tablet* utilizando uma rede 3G de dados. Há necessidade de alterar as configurações do navegador do *tablet* e habilitar a opção para gravar *cookies*. O tempo para realizar o processo de autenticação na rede 3G foi de aproximadamente 5 minutos.

A figura 15 mostra a tela apresentada ao usuário quando é realizado o acesso ao Shibboleth SP no *link* https://pacssp.no-ip.org/secure. Nesta página, são informadas as credenciais do usuário para acesso à federação.

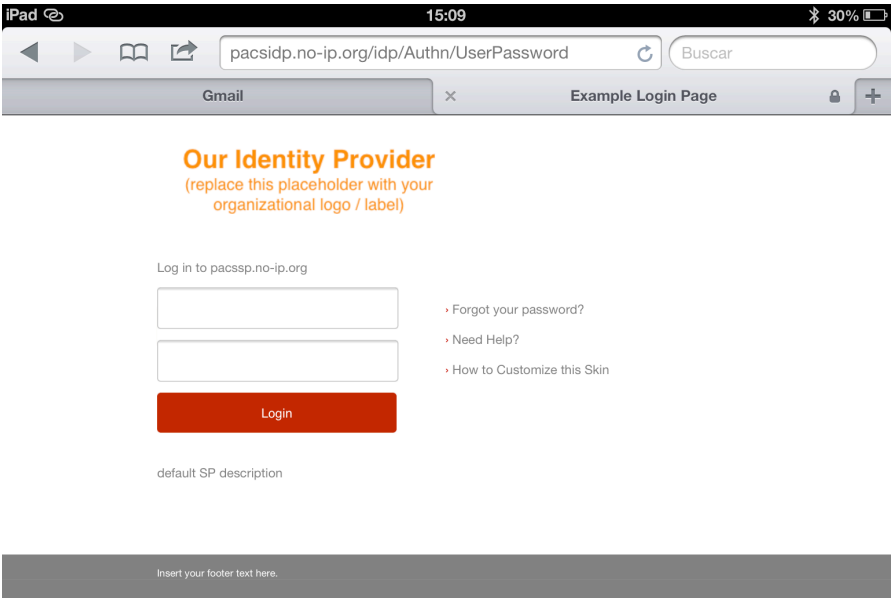

Figura 15 - Tela inicial *login tablet*.

Após o Shibboleth validar e criar as sessões do usuário, a página é redirecionada ao PACS na nuvem, onde é apresentada a página principal do dcm4chee como mostra a figura 16.

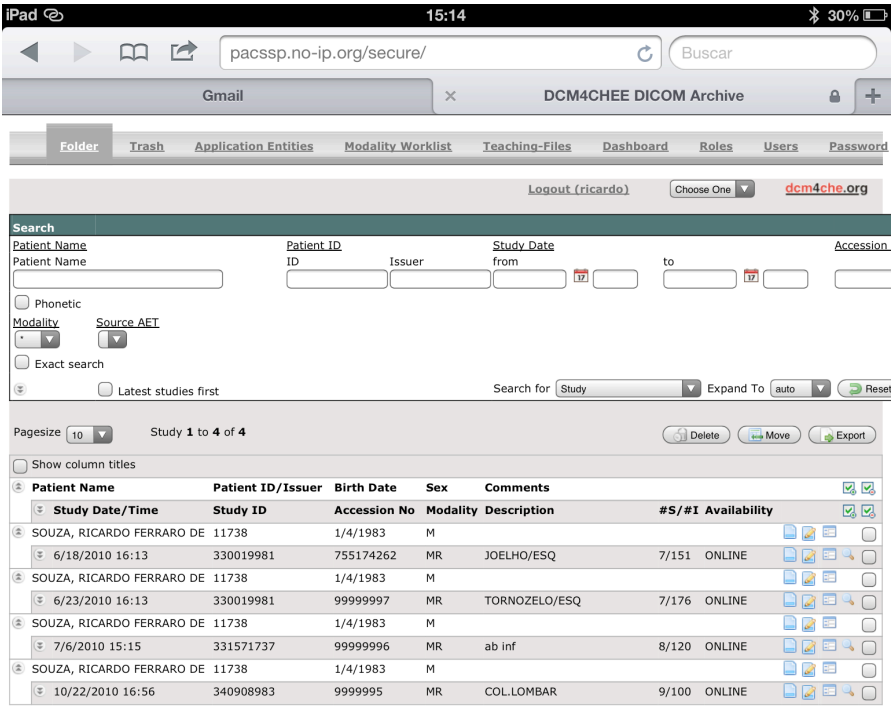

Figura 16 - Tela principal PACS *tablet*.

Despois do usuário ver as imagens dos exames, realiza o *logoff* no dcm4chee e automaticamente o Shibboleth encerra as sessões do usuário. A figura 17 mostra a tela onde é apresentada a mensagem de *logout* do Shibboleth contendo a informações que identificam de qual SP foi realizada a saída e a destruição dos *cookies*.

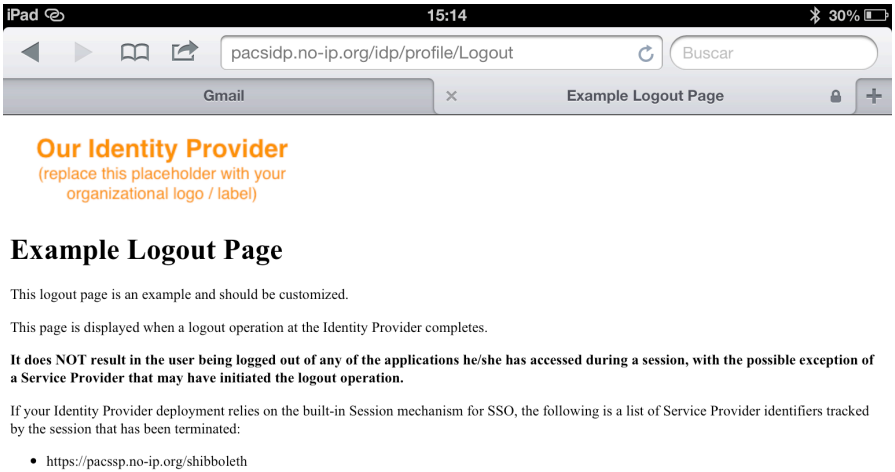

Figura 17 - Tela de *logout* Shibboleth *tablet*.

5.2.2 Caso 2

Nesta abordagem, o PACS em nuvem é acessado através de um notebook, utilizando Internet banda larga disponibilizada por uma empresa de telefonia. O tempo para realizar a autenticação através do computador foi de menos de 5 segundos.

A figura 18 mostra a tela apresentada ao usuário quando é realizado o acesso ao Shibboleth SP no *link* https://pacssp.no-ip.org/secure. Nesta página, o usuário informa suas credenciais para acesso à federação.

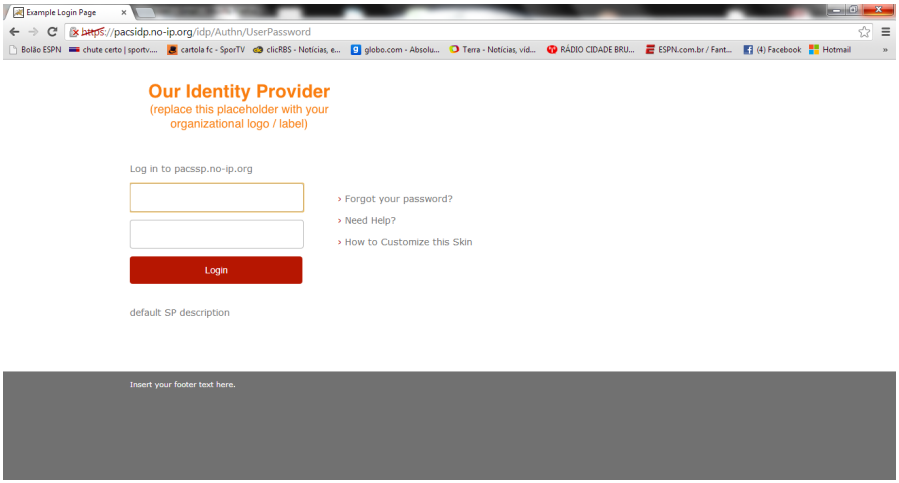

Figura 18 - Tela inicial Shibboleth computador.

Após o Shibboleth validar e criar as sessões do usuário, a página é redirecionada ao PACS na nuvem, onde é apresentada a página principal do dcm4chee como mostra a figura 19.

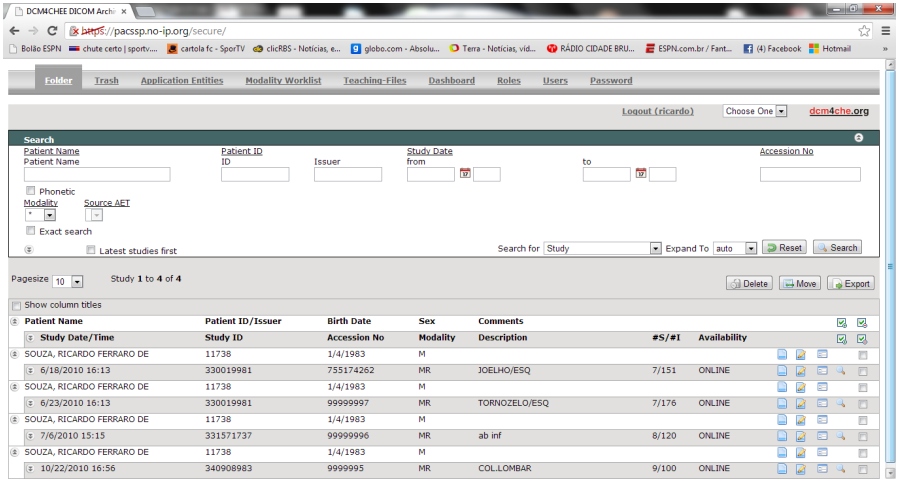

Figura 19 - Tela principal PACS computador.

Depois do usuário ver as imagens dos exames, realiza o *logoff* no dcm4chee e automaticamente o Shibboleth encerra as sessões do usuário. A figura 20 mostra a tela que apresenta a mensagem de *logout* do Shibboleth

contendo a informações que identificam de qual SP foi realizada a saída e a destruição dos *cookies*.

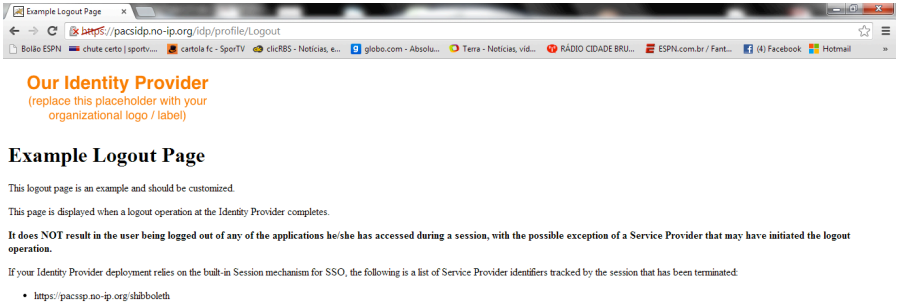

Figura 20 – Tela *logout* Shibboleth computador.

5.3 DIFICULDADES ENCONTRADAS NO DESENVOLVIMENTO E VALIDAÇÃO DA PROPOSTA

Antes de iniciar as implementações da nuvem para receber a autenticação através de identidade federada e utilizar o PACS como um serviço, foram coletados materiais tais como: artigos científicos voltados ao tema de *e-health*, *e-health* federada, identidades federadas e PACS implementando a nuvem. Após a coleta do material, foram realizados estudos para poder dar início ao processo de implementação do ambiente com máquinas virtuais baseadas em Linux.

Os sistemas operacionais utilizados virtualmente receberam o Shibboleth IDP e Shibboleth SP. Para o início da implementação do Shibboleth IDP, foram seguidos os passos descritos no endereço https://wiki.shibboleth.net/confluence/display/SHIB2/Home. Este documento online foi elaborado e disponibilizado pela Internet2, que é uma comunidade virtual vinculada a pesquisas acadêmicas, industriais e governamentais que desenvolve e colabora com pesquisas tecnológicas. Para o Shibboleth SP também foi utilizada a mesma base de informações. Ambas as ferramentas foram instaladas com sucesso, apresentando resultados desejados e sugeridos como testes a serem feitos, com a intenção de verificar o seu funcionamento.

O próximo passo foi realizar a integração dos serviços e a partir desse ponto, vários problemas foram encontrados, pois as mensagens de testes sugeridos nunca foram satisfatórias. A fonte de informações, que antes se mostrava rica e cheia de recursos, agora se apresentava muito confusa e pouco objetiva. A solução foi partir para outras fontes de pesquisa, que se mostraram mais completas e cheias de ideias de implementação da federação.

Durante este processo, optou-se por mudar os sistemas operacionais utilizados na implementação do Shibboleth IDP e SP para *windows server* e *seven* respectivamente. Depois de um tempo de pesquisa e vários testes, a federação ficou pronta.

5.4 DESENVOLVIMENTO DA INTEGRAÇÃO DO SHIBBOLETH COM PACS EM NUVEM

Após a instalação e a configuração do Shibboleth IDP, SP e OpenLdap, chegou o momento de continuar a pesquisa para demonstrar a entrada no sistema PACS através da autenticação Shibboleth. Inicialmente havia a intenção de realizar o procedimento de autenticação para gerar uma sessão em que estariam as variáveis necessárias para autenticar no servidor PACS, como mostra a figura 21.

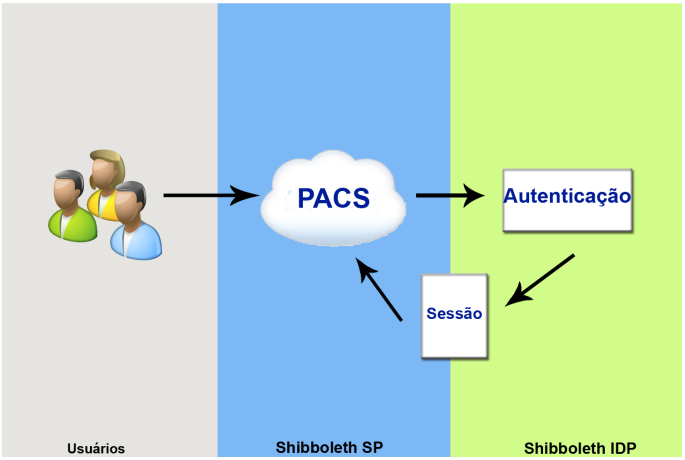

Figura 21 – Processo de autenticação com IDP.

O processo foi descartado após a percepção de que a sessão somente poderia ser implementada no servidor PACS. Sendo assim, optou-se por alterar o código da ferramenta, havendo, então, a necessidade de aprimorar os estudos no dcm4chee.

Houve necessidade de alterar o modo com que é realizado o gerenciamento de identidade e segurança do sistema PACS, sendo preciso investigar a obtenção de identificação do usuário logado através do JAAS. O identificador é utilizado pelo sistema para verificação do usuário que efetuou o *login,* e através deste, também carregar as informações referentes a ele. A alteração, neste ponto, é obrigatória para integração do sistema, pois de acordo

com documentos da Internet2, o sistema a ser adaptado deve deixar de gerenciar os usuários, passando tal função para o Shibboleth.

Após verificar o código fonte da ferramenta e deparar-se com o grau de complexidade envolvido, verificou-se a necessidade de dar mais ênfase nos estudos na linguagem JAVA, além do *framework* Jboss. Sendo assim, codificou-se a ferramenta de modo que o cabeçalho vindo do Shibboleth SP seja filtrado para a retirada de algumas informações necessárias à realização do *login* no PACS.

6 CONCLUSÕES E TRABALHOS FUTUROS

O modo como PACS está implementado em hospitais e clínicas vem se tornando um grave problema, pois a necessidade de investimentos é cada vez maior e a receita, menor. Exames mais complexos necessitam maior processamento e capacidade de armazenamento, exigindo uma infraestrutura mais adequada para disponibilizar serviços diferenciados e de qualidade.

A utilização do PACS em nuvem possibilita a centralização do serviço de TI empresarial, gerando economia em mão-de-obra, serviços, infraestrutura de armazenamento e processamento, além de manutenção em equipamentos e sistemas.

A criação da nuvem para utilização de PACS como serviço tem o intuito de organizar o armazenamento dos exames de diferentes locais em um repositório centralizado, diminuindo os investimentos em infraestrutura de armazenamento e processamento por parte dos hospitais ou clínicas. Na nuvem, médico e paciente poderão visualizar o exame através de qualquer dispositivo que tenha acesso à mesma.

A utilização de identidade federada para acesso ao repositório de imagens na nuvem mostra-se dinâmica e segura para os usuários. Médicos que trabalham em mais de um hospital podem ter acesso a todos os serviços de telemedicina através de uma conexão, utilizando o conceito SSO.

A função de prover serviços com segurança utilizando o conceito SSO faz com que uma federação digital seja uma solução ideal para o problema apresentado, pois através de uma identidade federada, os médicos têm acesso ao sistema PACS em nuvem protegido por uma federação.

O modelo e a arquitetura para as instituições de saúde armazenarem e disponibilizarem exames médicos com segurança na nuvem, apresentado neste trabalho, demonstra a implementação e o funcionamento do processo envolvendo o acesso a PACS em nuvem federada, além de mostrar que através de PACS baseado em nuvem, as instituições de saúde possuem uma solução para telerradiologia, utilizando conceitos de segurança, escalabilidade e confiança.

6.1 PRINCIPAIS CONTRIBUIÇÕES

O trabalho de Silva (2011), descreve um componente cuja idéia é transcrever um comando DICOM em não-DICOM, bem como não-DICOM em DICOM; em Chen (2000), o foco é a transferência de dados através de uma rede GPRS; Tohme (2006) faz um estudo para uso de *grid* computacional para auxiliar diagnósticos a distância; e Ni (2007) relata um monitor de recursos e dados em diferentes *grids* computacionais, com ênfase no gerenciamento total

do *grid*. Os estudos descrevem sistemas PACS sem demonstrar qualquer tipo de federação implementada com PACS baseado em nuvem. De forma distinta, este trabalho contribui na elaboração de uma solução de infraestrutura com segurança para PACS em nuvem utilizando identidade federada.

A ferramenta dcm4chee não possui suporte a federação, sendo que a autenticação é realizada pelo sistema JAAS, disponibilizado pela mesma. Para implementar esta solução, precisou-se codificar a ferramenta de modo que o cabeçalho vindo do Shibboleth SP fosse filtrado para a retirada de algumas informações necessárias à realização do *login* no PACS. O filtro intercepta as requisições HTTP enviadas pela federação e desabilita a autenticação JAAS, passando esta função para o Shibboleth.

O filtro desenvolvido para a ferramenta dcm4chee mostra-se eficaz para autenticação em PACS na nuvem através da federação. Quando a sessão do usuário é criada na federação, o filtro colhe informações do protocolo HTTP e repassa para o PACS, para que tais informações sejam utilizadas para criar uma sessão no serviço oferecido pela nuvem. No *logout*, a sessão é destruída no IDP e no SP. As implementações realizadas na ferramenta dcm4chee impedem que ela continue, utilizando o JASS como forma de autenticação. O conhecimento de JBoss e Java permitiu a adaptação da ferramenta ao modelo proposto e possibilitou a alteração no código fonte da ferramenta, de modo que o módulo de gerência de identidade e segurança fosse transferido para o Shibboleth.

6.2 TRABALHOS FUTUROS

Este trabalho objetivou apresentar a utilização de PACS em nuvem com identidade federada, o que foi possível através dos métodos e procedimentos demonstrados. É necessária a criação de uma biblioteca que auxilie a adaptação do Shibboleth com outras aplicações, de modo que não sejam realizadas alterações significativas na implementação disponibilizada pela dcm4che.org. Sugere-se o estudo do *framework* JBoss e Java para promover a integração entre a ferramenta dcm4chee e o Shibboleth. Também faz se necessário desenvolver metodologias para monitorar o PACS na nuvem, afim de obter medidas mais eficientes a respeito da economia de recursos da nuvem, além da energia utilizada pela mesma.

REFERÊNCIAS

ARENSON, R. L.. **Picture Archiving and Communications Systems.** San Francisco: Western Journal Of Medicine, pp. 298-299, 1992.

AZEVEDO-MARQUES, P. M.. **Implantação de um Mini-PACS (Sistema de Arquivamento e Distribuição de Imagens) em Hospital Universitário.** São Paulo: Radiol Bras, pp. 221-224, 2001.

BAKKER, A. R.. **HIS and RIS and PACS.** Berlin: Picture Archiving And Communication Systems (PACS) In Medicine, v. 74, pp.157-162, 1991.

BARROS JUNIOR, E. M.. **Teleradiologia: Central Remota de Diagnóstico por Imagem Digital Integrada a um Portal de Informações Médicas Distribuídas:** Aplicação da rede pública. 2010. 81 f. Tese (Doutorado) - Curso de Ciências, Universidade Federal de São Paulo, São Paulo, 2010.

BELAPURKAR, A. et al. **Distributed Systems Security: Issues, Processes and Solutions.** Chicester: John Wiley And Sons Ltd, 334 pp., 2009.

BERNDT, R-D.; TAKENGA, M. C.; KUEHN, S; PREIK P.; SOMMER G.; BERNDT S.. **SaaS-platform for mobile health applications.** Chemnitz: Systems, Signals And Devices (ssd), 2012 9th International Multi-conference, pp.1-4, 2012.

BHARGAV-SPANTZEL, A.; CAMENISCH, J.; GROSS, T.; SOMMER, D.. **User centricity: A taxonomy and open issues.** Amsterdam: Journal Of Computer Security - The Second Acm Workshop On Digital Identity Management, pp. 493-527. 2007.

BROWN, E. **Publicada definição final de Computação em Nuvem**. Disponível em: <http://www.inovacaotecnologica.com.br/noticias/noticia.php?artigo=definicao-computacao-em-nuvem&id=010150111128>. Acesso em: Dezembro 2011.

BUENO, J. M.; CHINO, F.; TRAINA, A. J. M.; JUNIOR, C. T.; AZEVEDO-MARQUES, P. M.. **How to add content-based image retrieval capability in a PACS.** Maribor: Computer-based Medical Systems, 2002. (CBMS 2002). Proceedings Of The 15th IEEE Symposium, pp. 321-326, 2002.

BURGES, M.. **Princípios de administração de redes e sistemas.** 2. ed. Rio de Janeiro: LTC, 468 pp., 2006.

CHAVES, S.; URIARTE, R.; WESTPHALL, C.. **Toward an architecture for monitoring private clouds.** Hollis: Communications Magazine, IEEE, pp. 130-137, 2012.

CHEN, P-C.; VARMA, V.; POLLINI, G.P.; SHERRY, H.. **GPRS-PACS: evolution of T-PACS towards third generation wireless services.** Londres: Personal, Indoor And Mobile Radio Communications, 2000. Pimrc 2000. The 11th Ieee International Symposium, pp. 994-998. 2000.

CHONG, F., TAYLOR, D.. **Federated Identity: Scenarios, Archetecture, and Implementation.** Disponível em: <http://msdn.microsoft.com/en-us/library/aa479079.aspx>. Acesso em: Maio 2013.

CHOWDHARY, S. K.; YADAV, A.; GARG, N.. **Cloud computing: Future prospect for e-health.** Kanyakumari: Electronics Computer Technology (ICECT), 2011 3rd International Conference, pp. 297-299, 2011.

CLAUß, S.; KÖHNTOPP, M.. **Identity management and its support of multilateral security.** [S.l.]: Computer Networks, v. 37, pp. 205-219, 2001.

CSI. **2010/2011 Computer Crime and Security Survey.** [S.l]: 15th annual Computer Crime and Security Survey. Disponível em: <http://www.go.com/Survey_2010>. Acesso em: Maio de 2013.

DCM4CHE. **Open Source Clinical Image and Object Management.** Disponível em: <http:// www.dcm4che.org>. Acesso em: Setembro, 2013.

GERENCIAMENTO DE IDENTIDADES. **SGI.** Disponível em: <http://www.gta.ufrj.br/grad/11_1/geren-id/index.php?file=kop5.php>. Acesso em: Julho 2013.

GERONIMO, G. A.; WERNER, J.; WESTPHALL, C. B.; DEFENTI, L.; WESTPHALL, C. M.. **Provisioning and Resource Allocation for Green Clouds.** Sevilla: The Twelfth International Conference On Networks, pp. 81-86, 2013.

GHAZIZADEH, E., ZAMANI, M., MANAN, J., PASHANG, A.. **A survey on security issues of federated identity in the cloud computing.** Taipei: Cloud

Computing Technology And Science (cloudcom), 2012 IEEE 4th International Conference, pp. 532-565, 2012.

GOLLMANN, D.. **Computer Security.** 3. ed. Reino Unido: John Wiley & Sons, Inc., 456 pp., 2011.

GONDO, M. K.. **Teleradiologia.** São Paulo: Jornal da Imagem, pp. 32, 2002.

JONAS, V., SCHRODEL, D. **Balancing security and convenience.** Berkley: Large Installation System Administration Workshop, pp. 5, 1987.

KHATTAK, Z., SULAIMAN, S., MANAN, J.. **A study on threat model for federated identities in federated identity management system.** Kuala Lumpur: Information Technology (ITSIM), 2010 International Symposium, pp. 618-623, 2010.

LAYOUNI, F.; POLLET, Y.. **Mobile Agents and Their Ontology Serving a Federated Identity Platform.** Gosier, Guadeloupe: Systems, 2009. Icons '09. Fourth International Conference, pp. 1-6, 2009.

LEANDRO, M., et al.. **Multi-Tenacy Authorization System with Federated Identity for Cloud-Based Environments Using Shibboleth.** Saint Gilles, Reunion: Icn 2012 : The Eleventh International Conference On Networks., p. 88-93, 2012.

MELL, P., GRANCE, T. **The NIST Definition of Cloud Computing.** Disponível em: < http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>. Acesso em: Maio 2013.

NEMA, **Digital Imaging and Communications in Medicine**. Disponível em: <http://dicom.nema.org>. Acesso em: Agosto, 2013.

NI, Y.-J.; YOUN, C-H; SONG, H.; KIM, B-J; HAN, Y.. **A PACS-Grid for Advanced Medical Services based on PQRM.** Melbourne, Qld.: Intelligent Sensors, Sensor Networks And Information, 2007. Issnip 2007. 3rd International Conference, pp. 625-630, 2007.

OASIS, **Security Assertion Markup Language (SAML) 2.0 Technical Overview.** Disponível em: <https://www.oasis-open.org/committees/download.php/11511/sstc-saml-tech-overview-2.0-draft-03.pdf >. Acesso em: Junho, 2013.

OBJETIVOS DO MILENIO. Disponível em: <http://www.objetivosdomilenio.org.br>. Acesso em: Dezembro, 2011.

OWASP. **Open Web Application Security Project.** Disponível em: <https://www.owasp.org/index.php/Main_Page>. Acesso em: Agosto, 2013.

PEYTON, L., JUN HU, DOSHI, C., SEGUIN, P.. **Addressing Privacy in a Federated Identity Management Network for EHealth.** Toronto, Ont.: Management Of Ebusiness, 2007. Wcmeb 2007. Eighth World Congress, pp. 12, 2007.

PIANYKH, O. S.. **Digital Imaging and Communications in Medicine (DICOM): A Practical Introduction and Survival Guide.** 2. ed. [S.l.]: Springer-Verlag Berlin Heidelberg, 420 pp., 2011.

REDE NACIONAL DE ENSINO E PESQUISA. **Infraestrutura de autenticação e autorização federada.** Disponível em: <http://portal.rnp.br/web/servicos/como-funciona>. Acesso em: Maio, 2013.

ROLIM, C. O. et al. **A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions.** St. Maarten: Ehealth, Telemedicine, And Social Medicine, 2010. Etelemed '10. Second International Conference, pp. 95-99, 2010.

SCHUBERT, F.; ROLIM, D. O.; WESTPHALL, C. B.. **Aplicação de Algoritmos de Provisionamento Baseados em Contratos de Nível de Serviço para Computação em Nuvem.** Campo Grande: XXIX Simposio Brasileiro de Redes de Computadores-IX Workshop em Clouds, Grids e Aplicações (WCGA 11), pp. 175-187, 2011.

SIEGEL, E. L.; KOLODNER, R. M.. **Filmless Radiology.** New York: Springer Science+business Media, LLC, 441 pp., 2006.

SILVA, L. A. B., COSTA, C., SILVA, A., O. J. L.. **A PACS Gateway to the Cloud.** Chaves: Information Systems And Technologies (cisti), 2011 6th Iberian Conference, pp. 1-6, 2011.

SOARES, T. S.. **Uma arquitetura paralela para o armazenamento de imagens médicas em sistemas de arquivos distribuídos.** 2013. 118 f. Dissertação (Mestrado) - Curso de Ciências da Computação, Universidade

Federal de Santa Catarina, Florianópolis, 2013. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/100420/311578.pdf?sequence=1>. Acesso em: Agosto 2013.

SOTOMAYOR, B. et al. **Virtual Infrastructure Management in Private and Hybrid Clouds.** [S.l]: Internet Computing, IEEE, pp. 14-22, 2009.

TENG, C. et al. **A medical image archive solution in the cloud.** Beijing: Software Engineering And Service Sciences (ICSESS), 2010 IEEE International Conference, pp. 431-434, 2010.

TOHME, W.G.; CHOI, I.; VASILESCU, E.; MUN, S.K.. **The Evolution of Distributed Diagnosis: Teleradiology As a Case Study.** Arlington, Va: Distributed Diagnosis And Home Healthcare, 2006. D2h2. 1st Transdisciplinary Conference, pp. 113-115, 2006.

WANGHAM, M. S.; MELLO, E. R.; BÖGER, D. S.; GUEIROS, M.; FRAGA, J. S. **Gerenciamento de Identidades.** Porto Alegre: X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, minicurso, pp. 3-52, 2010.

WERNER, J.; GERONIMO, G. A.; WESTPHALL, C. B.; KOCH, F.; FREITAS, R. R.; WESTPHALL, C. M.. **Environment, Services and Network Management for Green Clouds.** Quito: Clei Eletronic Journal, pp. 1-12, 2012.

WHO, **World Health Organization.** Disponível em: < http://www.who.int/en/ >. Acesso em: Junho, 2008.

APÊNDICE A – handle.xml modificado

```
        .
        .
        .
        <ph:ProfileHandler                    xsi:type="ph:SAML2SLO"
inboundBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
outboundBindingEnumeration="urn:oasis:names:tc:SAML:2.0:bindings:HTTP
-Redirect
                              urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POSTSimpleSign
                              urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
                              urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Artifact">

          <ph:RequestPath>/SAML2/Redirect/SLO</ph:RequestPath>
        </ph:ProfileHandler>

        <ph:ProfileHandler                    xsi:type="ph:SAML2SLO"
inboundBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
        outboundBindingEnumeration="urn:oasis:names:tc:SAML:2.0:bindings:
HTTP-Redirect
                              urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST-SimpleSign
                              urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
                              urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Artifact">
          <ph:RequestPath>/SAML2/POST/SLO</ph:RequestPath>
        </ph:ProfileHandler>

        <ph:ProfileHandler                    xsi:type="ph:SAML2SLO"
inboundBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-
SimpleSign"
        outboundBindingEnumeration="urn:oasis:names:tc:SAML:2.0:bindings:
HTTP-Redirect
                              urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST-SimpleSign
                              urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
                              urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Artifact">
```

```
        <ph:RequestPath>/SAML2/POST-
SimpleSign/SLO</ph:RequestPath>
    </ph:ProfileHandler>

    <ph:ProfileHandler                    xsi:type="ph:SAML2SLO"
inboundBinding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
outboundBindingEnumeration="urn:oasis:names:tc:SAML:2.0:bindings:SOAP
">
        <ph:RequestPath>/SAML2/SOAP/SLO</ph:RequestPath>
    </ph:ProfileHandler>

    <ph:ProfileHandler                    xsi:type="ph:SAML2SLO"
inboundBinding="urn:mace:shibboleth:2.0:profiles:LocalLogout">
        <ph:RequestPath>/Logout</ph:RequestPath>
    </ph:ProfileHandler>
    .
    .
    .
```