UNIVERSIDADE DA BEIRA INTERIOR
Covilhã | Portugal

Telemedicina e Telecuidados

Flávio André Barreto Amorim

Submetido para a Universidade da Beira Interior em candidatura para o Grau de Mestre em Engenharia informática

Orientador
Professor Doutor Pedro Araújo
Co-Orientador
Professor Doutor Miguel C.Branco

Departamento de Informática
Universidade da Beira Interior
Covilhã, 27 de Junho de 2011
http://www.di.ubi.pt

Agradecimentos

Desde o início do mestrado, contei com a confiança e o apoio de inúmeras pessoas. Sem aqueles contributos, a realização deste projeto teria sido mais difícil. Ao Professor Doutor Pedro Araújo, orientador do mestrado, agradeço o apoio, a partilha do saber e as valiosas contribuições para o trabalho. Acima de tudo, por ajudar a potenciar as minhas capacidades de inovação, para criar algo de novo e com valor para a sociedade. Ao Professor Doutor Pedro Inácio, por ter apoiado incondicionalmente o meu trabalho desenvolvido. Contribuiu ativamente para uma boa implementação da segurança informática das aplicações desenvolvidas por mim. Ao Professor Doutor João Cordeiro, pela sua disponibilidade para avaliar e ajudar no desenvolvimento do interface das minhas aplicações. A Universidade Da Beira interior por disponibilizar um bom local de trabalho para desenvolver a tese e a todos os seus docentes que acompanharam ao longo do meu percurso académico. Um agradecimento especial ao Filipe Quinaz e Fábio Campos pela sua amizade, companheirismo e partilha de saber. Por ultima quero agradecer á minha família e em especial à minha namorada.

Resumo

Este documento apresenta todo o processo de criação de uma infraestrutura tecnológica para um sistema de telemedicina.

Este sistema permite a transferência de informação médica entre o paciente que está em casa e os profissionais de saúde que estão no seu respetivo local de trabalho.

Para a criação desta infraestrutura foi tida em conta políticas de segurança de dados, controlo da sobrecarga dos servidores, interface amigável para o utilizador e criação de um mecanismo de automatização de aplicações.

O meio de comunicação escolhido foi a internet, porque hoje em dia grande maioria dos lares tem um serviço de acesso à internet e com uma capacidade razoável de transmissão de dados. E com aparecimento da internet por fibra as aplicações vão poder dispor de ainda mais recursos, aumentando assim a potencialidade do uso deste serviço.

Para o armazenamento da informação utilizamos um sistema de gestão de dados. Toda a informação dos utentes é automaticamente armazenada numa base de dados, isto de forma a facilitar o uso do sistema e diminuir o número de possíveis erros do utilizador.

Na automatização foram tidos em conta vários aspectos, como a redução do número de erros de utilização, e a notificação bilateral instantânea de anomalias nos exames médicos.

Foi desenvolvido um protocolo de comunicação para possibilitar a integração de vários sistemas de telemedicina e a comunicação entre si.

A interface do utilizador foi desenvolvida para monitores tácteis e para permitir uma facilitada interação com os pacientes.

O modo de funcionamento visa permitir a utilização do sistema por utilizadores sem formação ou prática no uso de meios informáticos.

Abstract

This document presents all the process to create a technological infrastructure for a telemedicine system. This system allows the medical information transference between the patient that is in his home, and the health professionals that are in their respective workplace.

For the creation of this infrastructure we had in consideration several policies of data security, control of the servers overload, friendly interface for the user and creation of a mechanism of automation for the applications.

The chosen communication mode was the internet, because nowadays the majority of all houses have an access to the internet service and with a reasonable capacity to transmit all data, and with the fiber internet emergence, the applications will dispose of even more resources, increasing that way the potentiality for the use of this service.

For the information storage we use a data management system. All user information is automatically stored into a data base that will facilitate the use of the system and reduce the number for possible mistakes.

For this automation it was taken in consideration several aspects such as the reduction the number of mistakes created by using it, and the instant bilateral notification for anomalies in the medical exams.

It was developed a communication protocol to enable integration for several systems of telemedicine and communication.

The user interface was developed for tactile monitors and to allow an easier interaction with the patients.

The use mode has the objective to facilitate the use of these electronic means especially for those without formation or practice.

Palavras-chave

Saúde, Telemedicina, e-Saúde, Segurança Informática, Automatização

Conteúdo

Lista de Figuras

Lista de Tabelas

Acrónimos

DDos - Distributed Denial Of Service

STS- Station-To-Station

IP - Internet Protocol

AES - Advanced Encryption Standard

CA - Certificate Authority

ECG - Electrocardiograma

UML - Unified Modeling Language

Voip - Voz sobre Ip

Capítulo 1

Introdução

Atualmente verifica-se que a esperança média de vida nos países desenvolvidos é elevada e tem vindo a aumentar. Este fator contribui para o aumento dos números de população idosa. Esta faixa etária possui características peculiares no que toca à exigência de cuidados especiais no seu dia-a-dia. Com esta exigência advém um aumento do custo individual relacionado com a prestação de cuidados de saúde. No entanto, existem pequenas populações que devido ao isolamento geográfico continuam sem acesso apropriado aos serviços de saúde. Este isolamento traduz-se também num afastamento relativo em relação aos cuidados de saúde. A contenção da despesa estatal inibe a possibilidade da criação de centros de saúde em localização apropriada para a sua utilização por parte dos elementos destas pequenas comunidades. Esta situação constituí uma problema relevante na sociedade atual para o qual uma resolução ou melhoria representa um aumento na qualidade de vida da população afetada. Hoje em dia podemos assistir a uma grande aposta em sistemas integrados de telemedicina. Ao longo do período do desenvolvimento desta tese presenciou-se um aumento relevante no número de sistemas comerciais disponíveis neste setor. A maioria das soluções oferecem serviços para todas as faixas etárias, pretendendo a redução dos custos de saúde, melhoria na prestação dos mesmos e aumento da população abrangida.

Uma característica comum aos sistemas presentes no mercado consiste na sua restrição da utilização por parte das outras empresas. O objetivo desta tese consiste na implementação de novos conceitos no âmbito da telemedicina, criando um serviço universal. Este serviço fornece a possibilidade de comunicação entre os pacientes e médicos a todos serviço e sistemas de forma aberta.

A segurança informática das aplicações foi também tida em conta como aspecto fundamental. Atualmente tem havido um incremento da consciência da sociedade relativamente a problemas adjacentes a falhas de segurança, aumentando também o interesse na verificação da autenticidade e confidencialidade da informação. Estas preocupações estão também latentes na informação crítica inerente à área médica. O perigo relacionado com informações pessoais e sua possível má utilização constituí uma barreira no uso de sistemas de telemedicina.

1.1 Conceito de Telemedicina

A Telemedicina é a aplicação das ciências médicas à distância sem que haja contacto físico direto para criação, manutenção ou complementação da relação médico-paciente, utilizando para a sua concretização um meio de comunicação entre os pontos interessados. Essa é uma definição extremamente abrangente que começa relacionando a ciência médica que envolve contato com o paciente, diagnóstico, tratamento ou até intervenção cirúrgica com qualquer meio de comunicação que possa unir dois ou mais pontos distantes fisicamente.

1.2 História da Telemedicina

A aplicação de tecnologias de comunicação ao exercício da medicina começa a ser aplicada no início do século XX. Foi demonstrado em 1910 na Inglaterra o primeiro estetoscópio eléctrico que funciona por telefone. Durante a 1ª guerra mundial, nos anos de 1916 o rádio foi utilizado para comunicar com médicos em estações costeiras ou frente de batalhas, com hospitais de campanha ou navios em busca de apoio e informações logísticas. Em 1950, imagens de radiologia foram transmitidas pela primeira vez entre West Chester e Philadelphia. No fim dos anos 50 faziam-se experiências com consultas de telepsiquiatria. No fim dos anos 60, ocorreram as primeiras aplicações com o uso de vídeo, com um projeto de demonstração de teledermatologia ligava uma clínica a um hospital central nos Estados Unidos. As duas alavancas maiores da telemedicina foram a conquista do espaço [1] e a guerra. O Departamento de Defesa dos Estados Unidos desenvolveu e ainda desenvolve enormes projetos utilizados, por exemplo, pelos porta-aviões da Marinha. Cada um desses navios possui 10.000 tripulantes, cujo atendimento médico, em grande parte, é feito em tempo real por um hospital militar localizado em Bethesda, Estados Unidos [2]. Na última guerra na Bósnia, houve um projeto ambicioso com o nome de Primetime III3 [3]. O resultado dessas experiências serve como modelo para grandes sistemas integrados de telemedicina pelo mundo, e, entre estes, muitas aplicações de atendimento de emergências médicas. A telemedicina iniciou com as primeiras aplicações na exploração espacial pelos americanos (Projeto Mercury), entre 1960 e 1964, através da telemetria fisiológica, ou seja, o envio de dados contínuos de monitorização dos astronautas em órbita [4]. Estas aplicações provaram que a telemedicina podia ser muito útil, pois as viagens espaciais sempre tiveram apoio

médico à distância e os progressos foram imensos. Atualmente, a NASA, prevê viagens interplanetárias e o próximo alvo é Marte, está a construir o projeto do Médico Virtual, ou seja, desenvolvendo sistemas inteligentes.

1.3 Benefícios da Telemedicina

A telemedicina é vista algo capaz de potenciar, promover e agregar benefícios socioeconómicos para a sociedade na medida que[5] [6]:

- Promove o acesso aos serviços de saúde
- Pode funcionar como uma ferramenta para a pedagógica dos profissionais de saúde ou como um método para obter uma segunda opinião
- Melhora o atendimento e qualidade de vida da população
- Pode funcionar como um recurso valioso para uma emergência, isto porque alguns hospitais não têm dimensão para ter todos os especialistas
- Prevenção e avaliação precoce de problemas de saúde
- Diminuir a despesa pública

Existe vários casos de sucesso em hospitais na aplicação desta tecnologia, no entanto ainda não há um caso de sucesso de aplicação massiva da telemedicina, isto é, um ou vários países que tenha adotado uma solução tecnológica e esta tenha sido aplicada massivamente com sucesso. Neste momento ainda não há uma solução que seja líder, mas sim várias soluções à procura de um modelo de negócio e de um modelo tecnológico.

Capítulo 2

Aplicações da Telemedicina

Neste capítulo serão abordadas algumas das aplicações típicas de telemedicina existentes atualmente.

2.1 Teleambulância

Figura 2.1: Teleambulância

É uma ambulância (ver figura:2.1) equipada com vários sistemas de telemedicina, tais como tele-EEG, tele-ECG, teleconsulta e teleanálise, para assistência local a grandes eventos, emergências médicas, acidentes, campanhas de medicina preventiva, bem como para comunidades necessitam de assistência especializada. Com a instalação de comunicação interativa visual e auditiva com o Centro de Coordenação, os Postos e os Hospitais. Munidos com redes 3G integradas nas aplicações de telemedicina que permitem ter um sistema funcional e a baixo custo.

2.2 Telediagnostico

São realizadas consultas para obter um diagnóstico, geralmente ocorrem por troca de textos, imagens estáticas de Raio-X, ECG, áudio e vídeo. Entre os sinais biológicos implementados com sucesso em telediagnóstico estão: eletrocardiograma, eletroencefalograma, eletromiograma, eletro-oculograma, eletrogastrograma, medidor tensão, temperatura corporal, ritmo respiratório e frequência cardíaca. A neurologia e a cardiologia estão entre as especialidades que mais tem beneficiado da telemedicina, pois as tecnologias desenvolvidas proporcionam um suporte confiável para emergências, monitorização de pacientes de alto risco, monitorização ao domicílio e em áreas isoladas ou carentes, bem como para a redução da hospitalização de pacientes com doenças cardíacas e nervosas. Entre os diversos sistemas telemedicina de sucesso desenvolvidos para essas especialidades estão o tele-EEG e o tele-ECG(ver figura: 2.2). Este último, que já foi objeto de imensos testes e uso prático em diversos países, como na Itália. Consiste num transmissor digital de 12 canais por via telefónica normal (terrestre ou telemóvel), que angaria e envia o ECG, em tempo real, para um centro especializado de análise. Este, por sua vez, dispõe também de um equipamento especializado, com computador, internet, vídeo e um sistema de registo ECG. A transmissão dispõe de um canal de voz bidirecional por telefone, que permite ao centro orientar o diagnóstico e a conduta ao paciente.

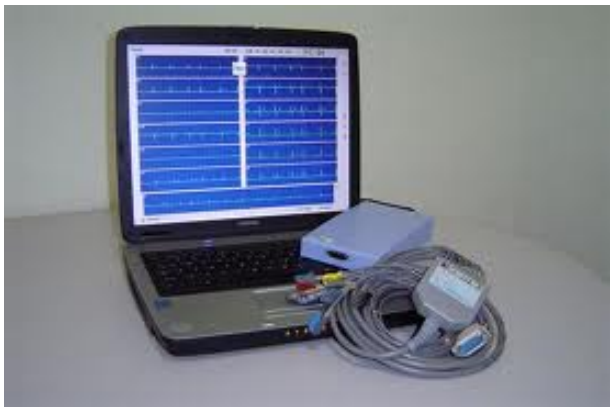

Figura 2.2: Tele-ECG portátil de 12 canais.

2.3 Telemonitorização

Utilizam-se equipamentos especiais para registar dados vitais de pacientes e enviá-los continuamente a um centro de análise, interpretação e alerta. Exemplos desse tipo de aplicação são os de monitorização cardíaca, controlo de pacientes com gravidez de risco, pacientes deficientes ou imobilizados em casa. Baseia-se no conceito de digitalização e envio de sinais biológicos por um canal de comunicação (ex. Internet), desde o local onde o paciente se encontra, a um centro especializado de interpretação e análise. A diferença em relação ao telediagnóstico de sinais é que a monitorização geralmente faz-se de forma contínua, periódica ou sob pedido, mas geralmente envolvendo um período de tempo longo, principalmente em pacientes com doenças crônico-degenerativas. A obstetrícia é uma das especialidades também beneficiam da telemedicina, através do desenvolvimento de um sistema que tem por objetivo a prevenção da mortalidade perinatal e a morbilidade de mulheres de gravidez de risco(ver figura:2.3). O sistema monitoriza os batimentos cardíacos do feto e as contrações uterinas até duas vezes por dia, na própria residência da paciente, enviando os dados através de um canal de comunicação para uma central de interpretação e análise, inteiramente automática. Esta processa alarmes em caso de apneia perinatal, sofrimento cardiofetal e contrações precoces. Permitindo o rápido atendimento à grávida, sem necessidade de internações prolongadas e com um histórico que ajuda os médicos a tomar decisões mais acertadas.

Figura 2.3: Dispositivo de ecografia

2.3.1 Equipamentos mais usados

Quando se fala de telemonitorização referem-se frequentemente uma série de diferentes equipamentos que desempenham diversas funções. Nesta seção iremos abordar alguns dos equipamentos mais comuns, explicitando para cada um o seu objetivo e respetivas caraterísticas.

2.3.1.1 Medidor de Tensão

Existe uma grande variedade de medidores de tensão para a telemedicina, mas nem todos são mundialmente conhecidos ou comercializados. O aparelho consiste num pequeno medidor electrónico muito parecido com os tradicionais medidores. No entanto estes aparelhos não precisam de um médico para fazer o exame, isto porque estão munidos de um sensor capaz de obter toda a informação necessária para a realização do exame e com algoritmos capazes de avaliar os dados obtidos. Como exemplo temos o "Omron USB 790 serie"(ver figura: 2.4), com um simples premir de um botão o exame inicia, a informação é obtida, um algoritmo trata os dados e devolve o resultado do exame para um pequeno monitor LCD. Se desejarmos podemos ligar ao dispositivo pela porta USB ou porta SERIE e descarregar os dados para o computador num formato texto ou em PDF. O utilizador pode assim criar um histórico de exames e mais tarde ou na hora enviar os dados para um profissional de saúde para que sejam analisados. Caso tenha algumas bases médicas, pode consultar o histórico e saber como tem evoluído ou deteriorado a sua saúde ao longo dos exames que foi efetuando. Isto pode incentivar o paciente a ter mais cuidado com a sua saúde ou a dirigir-se a um centro de saúde.

Figura 2.4: Medidor de Tensão Arterial

2.3.1.2 Electrocardiograma

O cardiobip [7](ver figura: 2.5) é um dos sistemas especializados desenvolvidos para a telemedicina. Consiste num pequeno aparelho portátil de ECG mono canal, sem fios, cabe no bolso e utiliza três sensores para captar sinais cardíacos. Quando o paciente deseja realizar um exame para verificar o seu estado de saúde, pega no dispositivo e encosta ao peito e pressiona um botão para recolher alguns segundos de ECG. E em seguida pode enviar os dados utilizando o método "transtelephoni"[6] para o centro remoto ou o aparelho pode alertar o paciente caso esteja em perigo de vida. Este tipo de aparelhos são muito úteis para pacientes que sofrem de problemas cardíacos, isto porque podem alertar o paciente antecipadamente para perigo de ataque cardíaco e incentivar a dirigir-se a um centro de saúde. Existe um grande número de fabricantes deste tipo de equipamentos. A informação pode ser descarregada para o computador e proceder à criação de um histórico ou enviar pela Internet os exames efectuados para um profissional de saúde analisar.

Figura 2.5: Electrocardiograma

2.3.1.3 Balança Multifunções

Hoje em dia com este tipo de balanças podemos fazer muito mais do que apenas obter o nosso peso corporal. O normal é termos em casa uma simples balança electrónica em que quando é pressionada pelo nosso peso corporal, liga-se e mostra o peso. Mas agora com as balanças multifunções (ver figura: 2.6) podemos obter muitos dados relevantes. O processo é simples, basta estarmos descalços em cima da balança e elevar à altura do peito um pequeno medidor. Os dados são recolhidos e de seguida tratados por vários algoritmos e em poucos segundos fica-se a saber o peso, massa gorda, em que índice de peso está e quantidade de água no corpo. Os dados podem ser descarregados para o computador e proceder à criação de um histórico ou enviar para um profissional de saúde. Hoje em dia muitos ginásios começam a utilizar este tipo de equipamentos para os ajudar a saber mais sobre a pessoa que está a ser avaliada fisicamente. Uma boa avaliação do cliente pode ajudar o avaliador a criar um plano de treino adequado e evitar casos em que o plano de treino seja demasiadamente puxado para o cliente, fazendo com que este deseja de frequentar o ginásio ou fique desmotivado.

Figura 2.6: Balança Multifunções

2.3.1.4 Oxímetro

O oxímetro de pulso(ver figura: 2.7) mede os níveis de saturação do oxigênio no sangue (SpO2) bem como o batimento cardíaco por minuto. O paciente prende ao dedo um sensor confortável e pressiona um único botão para ativar o aparelho. O oxímetro é usado no combate à hipoxemia (nível baixo de oxigénio no sangue arterial), mostrando as mudanças da saturação de oxigénio na hemoglobina. A hipoxemia pode acorrer a qualquer momento em pacientes com um quadro clínico que necessita de cuidados especiais com a ventilação. O princípio de leitura destes valores leva em conta o comportamento da hemoglobina quando incide uma luz de comprimentos de onda diferentes (vermelho e infravermelho), e a relação de energia luminosa absorvida pela hemoglobina que é distinta quando está saturada (oxigemoglobina) e quando está insaturada (ausência de moléculas de O2). A relação entre a energia luminosa absorvida dos comprimentos de onda vermelha e infravermelho, obtemos o valor da saturação da hemoglobina no sangue arterial.

Figura 2.7: Oxímetro

2.3.1.5 Medidor de Glicose

Essencial para os portadores de diabetes, o medidor de glicemia é a única forma eficiente de detectar a quantidade anormal de glicose no fluxo sanguíneo para tomar as precauções necessárias. A análise instantânea permite que sejam feitos os ajustes necessários na alimentação, na dosagem da medicação e no nível de atividade física corretamente, permitindo que o utilizador tenha um maior controle sobre a sua vida. O controlo da diabetes depende de uma frequente monitorização. Mesmo para pessoas cuja rotina raramente se altera, factores como stress, doenças, medicamentos e álcool pode afectar na oscilação da glicose. Há diversas marcas e fabricantes de medidores de glicose no mercado que analisam o nível de glicose através de variados métodos, cabe ao utilizador escolher o aparelho ideal ao seu estilo de vida. O medidor da figura 2.8, permite gravar para um iphone ou ipad os exames efectuados. Para isso utiliza uma aplicação que pode ser descarregada da loja online de software da Apple e mais tarde consultar ou enviar para um profissional de saúde.

Figura 2.8: Medidor de Glicose

2.3.2 Sistemas Integrados de Telemonitorização

Estes sistemas são compostos por vários medidores explicitados anteriormente e entre outros, tudo depende da quantidade de serviços que cada um oferece. O seu aparecimento surge porque é uma necessidade do mercado, ter um sistema que facilite o acondicionamento automático da informação, barato e que não seja necessário ter um profissional de saúde a monitorizar a realização do exame médico. Como a telemedicina é para toda a população e grande maioria não sabe ou não tem tempo para tratar a informação, este facto pode gerar vários problemas na utilização dos vários equipamentos. Assim surge estes sistemas integrados de telemedicina quem vem facilitar a vida dos seus utilizadores e cuidar eficientemente dos exames realizados. São criados históricos locais e históricos em bases de dados centralizadas que retêm a informação para mais tarde ser consultada por profissionais de saúde. Uma grande potencialidade destes sistemas é, informar automaticamente o utilizador ou um profissional de saúde indicado para o exame em questão sobre um problema de saúde que o paciente possa ter ou estar em risco iminente. Sendo assim vou exemplificar alguns sistemas de grandes marcas que começam aparecer no mercado. A tese que está a ser desenvolvida é uma alternativa a estes sistemas, é também um meio de como integrar estes vários serviços, ou seja, ter um sistema que promova a comunicação entre todos os sistemas existentes.

2.3.2.1 Philips TeleStation

Figura 2.9: TeleStation da Philips

O "TeleStation"(ver figura:2.9) é a sistema desenvolvido pela Philips para a monitorização remota de pacientes com doenças crónicas. Esta solução tecnológica permite o fluxo seguro e bidirecional de informações entre as pessoas responsáveis pelo atendimento médico, os profissionais de saúde remotos e os pacientes portadores de doenças crônicas. Funciona como um distribuidor que transmite dados de sinais vitais (obtidos automaticamente dos dispositivos sem fio de medição ou inseridos manualmente) e também é uma forma de comunicação interativa entre os profissionais de saúde e os pacientes em casa. O "TeleStation"pede aos pacientes que respondam a perguntas para avaliação da sua saúde, estes pode ser personalizados para gerir qualquer doença e envia automaticamente as respostas do questionário (Autochek) a um profissional de saúde para haver um acompanhamento sobre leituras anormais. Os médicos podem adaptar as interações diárias dos pacientes para ajudar a reforçar tópicos específicos: sinais e sintomas, medicação e efeitos secundários, dieta e estilo de vida. Essas interações automatizadas podem agilizar o fluxo de trabalho médico, reduzir o número de chamadas telefônicas desnecessárias e ainda permitir que os médicos estejam em contacto com o maior número de pacientes crónicos, tendo em mãos os dados de que precisam para intervenções mais oportunas. A "TeleStation"permite interligar vários dispositivos como:

- Electrocardiograma
- Medidor de Tensão Arterial
- Balança
- Oxímetro de Pulso
- Medidor de Glicose

Tem também um interface que permite ligar medidores de glicose de outras marcas. Os pacientes usam estes dispositivos sem fio de medição para controlar seus próprios sinais vitais e responder a um questionário personalizado, orientado pelos médicos, usando a TeleStation. A plataforma de comunicação que transmite automaticamente as respostas subjetivas do questionário e os resultados obtidos da medição. Os dados são guardados num servidor seguro e remoto da Philips. Os médicos podem utilizar o Clinical Review Application (Aplicação de Análise Clínica) por um browser, para visualizar os dados do paciente e usar ferramentas de suporte às decisões que garantem e facilitam a gestão do atendimento para casos crônicos.

2.3.2.2 Bosch Healthcare

Figura 2.10: Health Buddy

A Bosch criou o "Health Buddy"(ver figura: 2.10), um sistema a nível físico muito parecido com a solução apresentada pela Philips, mas com um cuidado especial ao nível da segurança. O sistema "Health Buddy"interliga os pacientes que estão em suas

casas ao seu provedor de serviços de saúde. O que se destaca mais nesta solução não é só a sua habilidade para transmitir a informação sobre o histórico do paciente, mas é também ajudar na instrução do paciente para saber lidar confortavelmente com o condicionamento que a sua saúde lhe implica. Todos os dias, os utilizadores deste sistema respondem a uma série de questões sobre a sua saúde e bem-estar, usando a aplicação do "Health Buddy". Os dados são enviados(ver figura: 2.11) por um canal de comunicação para um centro de dados seguro (Data Center), assim os dados ficam automaticamente disponíveis para ser revistos através de uma aplicação baseada na Web fornecida pela Bosch.

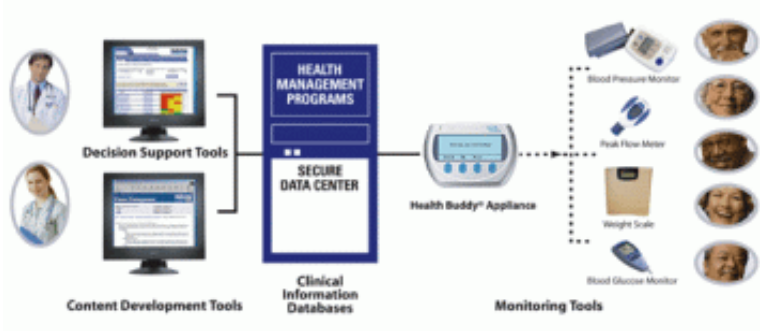

Figura 2.11: Sistema Health Buddy

A aplicação está desenhada para automaticamente e precocemente verificar riscos iminentes que possam estar a surgir, apresenta esta informação cuidada aos utilizadores e também avisa o seu prestador de serviços de saúde para intervir antes que a situação do paciente agrave. Os pacientes respondem a um sistema codificado por um nível de cores em que o vermelho é o mais elevado, amarelo moderado e verde um risco baixo, baseado nos seus sintomas, comportamento do paciente e o seu nível de conhecimento sobre a saúde.

A solução apresentada permite ligar vários aparelhos ao dispositivo central "Health Buddy"tais como(ver figura: 2.11):

Figura 2.12: Diagrama do Sistema de Dispositivos

- Medidor de Glicose no sangue
- Medidor de Tensão Arterial
- Oxímetro
- Medidor de Picos do Fluxo
- Balança

Os aparelhos não têm de ser obrigatoriamente todos da marca Bosch, os consumidores tem a opção de utilizar vários componentes compatíveis com o componente principal "Health Buddy". Toda a informação gerada por este sistema recebe um tratamento especial a nível de segurança. Os dados que são transmitidos são cifrados com um cifra RSA de 128 bits e os apresentados no browser. Utilizam o protocolo SSL para garantir a confidencialidade e autenticidade da informação na troca online de informação.

2.4 TeleCirurgia

Figura 2.13: Telecirurgia

Um dos aspectos mais importantes, arrojados e inovadores da telemedicina é a telecirurgia (ver figura: 2.13). Este conceito consiste em realizar vários tipos de operações cirúrgicas à distância usando para isso robôs e técnicas computacionais avançadas. O cirurgião tem assim a possibilidade de controlar o robô à distância e ter uma total percepção da operação que está a realizar no quarto do paciente. Este sistema tem de possuir algumas características essenciais sem as quais não pode funcionar:

- Precisão
- Segurança informática do sistema
- Segurança em relação ao paciente
- Capaz de realizar operação em tempo real
- Portabilidade
- Qualidade e fiabilidade dos canais de comunicação
- Fiabilidade de todo o sistema

2.5 Teleconsulta

A teleconsulta é um desenvolvimento com o qual é possível transmitir, a qualquer distância, vários tipos de imagens médicas e biológicas, tais como radiografias, to-

mografias, ecografias e fotos de pacientes. Deste modo, médicos situados em centros geograficamente distantes podem trocar entre si os dados de imagem sobre casos de pacientes, e consultar colegas mais especializados quanto ao diagnóstico e conduta para os mesmos. A maioria dos sistemas é constituída por um sistema de transmissão de vídeo (câmara de vídeo, desktop) e de um canal de comunicação de banda larga. As características técnicas dos sistemas de teleconsulta disponíveis no mercado permitem a transmissão rápida de imagens de alta qualidade, com pouca ou nenhuma perda de definição. Por exemplo, um sistema desenvolvido por uma empresa italiana, permite a transmissão de imagens com resolução de até 1024 x 1024 pixéis, 16 milhões de cores por pixel ou 256 níveis de cinza. Usando uma técnica de compressão da imagem antes da transmissão, que pode reduzir seu tamanho em até 30 vezes.

Capítulo 3

Segurança Informática

Neste capítulo vamos falar sobre alguns aspectos de segurança informática utilizados na construção da solução apresentada nesta tese[8].

3.1 Introdução

Hoje em dia cada vez mais a sociedade está informatizada e grande parte dos serviços públicos e privados são o reflexo disso, assim torna-se cada vez mais urgente proteger a privacidade da população. Estamos assistir a um crescimento substancial da quantidade de serviços principalmente disponíveis na Internet. E no entanto apenas os bancos estão a proteger devidamente aspectos importantes relativamente à informação, como a confidencialidade, autenticidade, não repúdio, anonimato, integridade e Identificação.

- Confidencialidade: garantir que a informação trespassada apenas é conhecida por quem envia e a recebe.

- Integridade: garantir que o receptor não aceita informação adulterada.

- Autenticidade: ter a certeza de que um objeto (em análise) provém das fontes anunciadas e que não foi alvo de mutações ao longo de um processo.

- Não repúdio: demonstrar quem emitiu a mensagem de forma que não possa negar que o fez.

- Anonimato: não fornecer qualquer informação relativa ao autor da mensagem.

- Identificação: garantir a identidade dos intervenientes na comunicação.

Uma realidade cada vez mais urgente é garantir estes aspectos explicitados, isto porque, a população no geral não tem conhecimentos suficientes para lidar com estas situações e geram em si um clima de medo de serem expostos ao utilizar todos estes serviços que lhes são fornecidos. No desenvolvimento da solução tecnológica aqui apresentada, a segurança informática foi um aspecto muito importante tido em conta. Com o objectivo de deixar os seus utilizadores descansados em relação à sua privacidade e também para acrescentar valor a este sistema implementado. No entanto não foi apenas implementado sistemas de segurança para proteger a informação, houve também uma necessidade de desenvolver algoritmos para garantir a qualidade e disponibilidade do serviço.

3.1.1 Definições

Definem-se a seguir alguns termos comuns em segurança informática:

- Ataque - comprometimento dos objectivos da técnica criptográfica (ex. conseguir obter o texto limpo sem conhecimento da chave ou descobrir a chave utilizada na cifragem)

- Cifra - algoritmo criptográfico que efetua transformações entre o texto limpo e o criptograma. Operação que transforma o texto limpo numa mensagem obscurecida.

- Chave - parâmetro de segurança da operação de cifra, ou seja elemento principal utilizado na cifragem e decifragem da informação alvo.

- Intruso/Inimigo - entidade que personifica quem pretende comprometer o sistema alvo ou técnica criptográfica utilizada

- Texto limpo - mensagem a transmitir

3.2 Reflexão Sobre Problemas De Segurança

Ao projetar a solução apresentada foram detectadas duas potenciais ameaças:

- Qualidade, disponibilidade e escalabilidade do serviço
- Segurança das comunicações e todas as questões relacionadas com a mesma

Isto, porque hoje em dia o principal canal de comunicação é a internet e como tal este sistema utiliza esses canais de comunicação. Assim, surge uma necessidade de proteger a informação que é transmitida por canais inseguros. No entanto os alvos favoritos de organizações mal-intencionadas não são as pessoas em si mas sim as entidades que oferecem os serviços, isto porque há um grande fluxo de informação de todos os utilizadores que estão conectados a esse serviço, logo torna um alvo muito apetecível. Contudo a maior parte dos ataques destinam-se a tornar os serviços indisponíveis e um muito conhecido é o ataque DDos (Distributed Denial of service) [9], que pode deixar por horas ou dias um serviço inoperacional. O sistema construído nesta tese está vulnerável a este tipo de ataques, isto porque está assente na internet para realizar as suas comunicações. No entanto podemos ter um problema muito parecido com o "DDos", que chama-se "Unintentional denial of service", isto é, em alturas do dia pode haver um grande número de pedidos ao servidor que presta o serviço de telemedicina. Um exemplo teórico que pode acontecer é: muitas pessoas entrarem ao trabalho à mesma hora. Há uma grande probabilidade de todos acordarem no mesmo intervalo de tempo, efetuar exames de rotina e como consequência haver um número excessivo de pedidos ao prestador de serviços. Este acontecimento pode levar a que o serviço entre em ruptura ou até fique inoperacional.

Grandes empresas como a Google e Twitter sofreram de problemas idênticos como o apresentado anteriormente [10]. Aconteceu em 2009. Quando Michael Jackson morreu, houve uma quantidade excessiva de pedidos a estes serviços e a consequência disso foi os serviços ficarem muito lentos ou até ficarem inoperacionais. Os sistemas de defesa destes servidores reagiram pensando que estavam perante um ataque "DDos".

Quanto à segurança das comunicações, houve uma necessidade de garantir vários aspectos referidos na introdução deste capítulo, como confidencialidade, autenticidade, não repúdio, anonimato, integridade e identificação. Uma das potenciais ameaças é o processo de identificação (Login), que é efetuado a partir a aplicação de gestão (SaudeGest) desenvolvida para as entidades que prestam os serviços de telemedicina (ver capitulo:4).

Isto porque assumimos que as comunicações da rede interna não é segura, logo há um risco de alguém estar a espiar a rede e apoderar-se dos dados para efetuar

"Login"não autorizado e ter acesso total a toda a informação contida na base de dados.

Um segundo potencial problema é alguém estar a escutar o canal de comunicação do servidor e assim apoderar-se ilegalmente de informação.

Um terceiro problema ligado também ao anterior é existir alguém no meio da comunicação a adulterar a informação ou a fazer-se passar por uma entidade ou pessoa. A este tipo é chamado de ataque "man in the middle"[11] (literalmente "ataque do homem no meio "ou "ataque do interceptor"), é um cenário de ataque no qual um intruso escuta uma comunicação entre dois interlocutores e falsifica as trocas a fim de fazer-se passar por uma das partes.

O objectivo inicial foi resolver estes problemas, isto porque apresentam um grande risco para o bom funcionamento do sistema. No entanto há outros problemas como não repúdio e identificação que foram resolvidos ao tratar dos problemas anteriores, isto porque foi implementado o protocolo STS (station-to-station)[12] como solução e outros sistemas que serão explicitados no decorrer deste documento.

3.3 Mecanismos Implementados

Aqui vão ser explicitados vários mecanismos implementados para resolver os problemas mais graves de segurança. Contudo para proteger de ataques "DDos"não poderá ser feito diretamente nesta aplicação, será utilizado aplicações externas como firewalls.

3.3.1 Anunciador e Servidor de Telemedicina

Foram implementados alguns mecanismos para mitigar problemas como excesso de pedidos. Na aplicação "Anunciador"(ver Capítulo 4), foi construído vários algoritmos para controlar o excesso de pedidos ao serviço tais como:

- Algoritmo para banir temporariamente um endereço (IP), caso este efetue mais do que cinco pedidos em menos de dois minutos e evitando assim que alguém maliciosamente tente sobrecarregar o servidor. No entanto ao fim de 5 minutos o IP é removido da lista negra (lista de IP's banidos) e esse utilizador poderá voltar a comunicar com o servidor.

- Foi também implementado no protocolo, algoritmos para controlar a sobrecarga de ligações, com recurso a um contador de ligações ativas. Uma vez atingindo

o limite de ligações o servidor nega o pedido de serviço a nível protocolar. No entanto o utilizador está programado para voltar a tentar ligar-se ao fim de cinco minutos, assim podemos arrastar ao longo do tempo a sobrecarga até que o sistema consiga processar todos os pedidos.

No servidor da entidade prestadora de serviços de telemedicina (Servidor de Telemedicina ver capitulo 4) foi implementado também algoritmos iguais ao do anunciador. Contudo estes mecanismos podem não ser suficientes para garantir a qualidade, disponibilidade e escalabilidade máxima dos serviços. Seria necessário realizar teste de stress aos serviços para saber até onde os serviços conseguem escalar em conjunto com o hardware e largura de banda atribuída aos servidores.

3.3.2 Aplicação SaudeGest

Para a aplicação de gestão (SaudeGest) explicitada no capítulo 4, foi desenvolvido um mecanismo de autenticação (Login) seguro, isto é, com o auxílio de vários algoritmos é possível fazer identificação do utilizador sem que a palavra-chave seja transmitida pelo canal de comunicação em texto claro. O segredo para a criação deste método seguro de "login"é utilizar um "Hash sha1"[13]:

- Hash - um hash é uma sequência de bits gerados por um algoritmo de dispersão. O conceito teórico diz que um "hash"é uma transformação de uma grande quantidade de informação em uma pequena quantidade de informação. A finalidade do hash é identificar um conjunto de dados com uma pequena sequência de dados únicos. Assim a partir dessa sequência podemos garantir quase a 100% que os dados não foram adulterados.

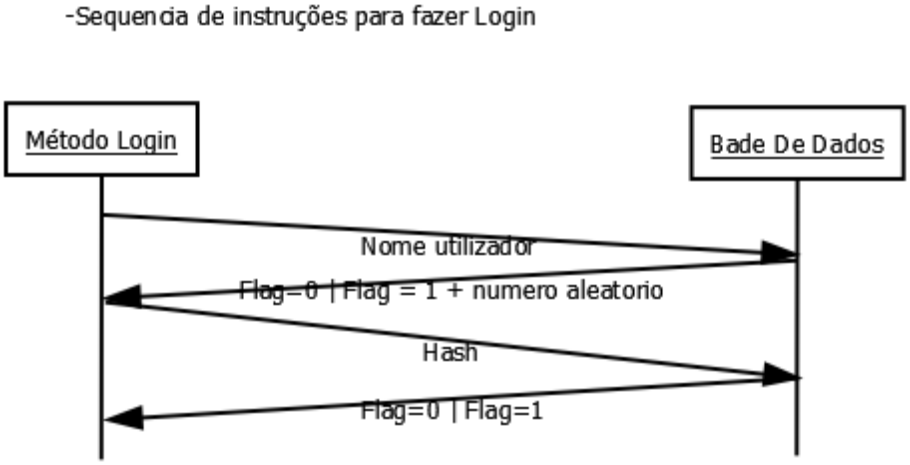

Figura 3.1: Sequência de instruções para fazer Login

Como podemos ver na figura 3.1, o processo de autenticação começa pelo método login, que envia o nome de utilizador para a base de dados. A base de dados tem um procedimento que recebe o nome e faz uma pesquisa para verificar se realmente existe este utilizador, caso seja falso devolve "Flag = 0"e termina aqui o processo todo. Caso seja verdade, o procedimento da base de dados gera um número pseudoaleatório com um tamanho de 14 dígitos, associa o número ao utilizador em questão e devolve verdade ("Flag=1") mais o número gerado e informações relativas ao utilizador como "ID"e permissões. O método login concatena o número à palavra-chave e utiliza a função de hash sha1 para criar um hash dos dados concatenados e envia para a base da de dados o hash criado, chamando um dos seus procedimentos. Este procedimento recebe a informação o "ID"e o hash enviado pelo login, de seguida procura pelo "ID"do utilizador na base de dados e uma vez encontrado colhe a sua palavra-chave e o numero aleatório criado anteriormente e cria um hash destes dados. O passo final é comparar os dois hash, caso seja falso devolve "Flag=0", isto é não são iguais, caso seja verdade devolve "Flag=1", ou seja a autenticação foi um sucesso. Como podemos concluir, a palavra-chave nunca é enviada em texto claro pela rede, e mesmo que alguém escute o canal de comunicação e memorize o hash enviado pelo utilizador para tentar fazer-se passar pelo utilizador não terá sucesso. Isto porque sempre que se tenta fazer autenticação é gerado um novo número aleatório. No entanto a forma mais segura de fazer autenticação seria criar um canal seguro o que implicaria criar uma aplicação no servidor onde a base de dados está alojada para servir de interlocutor entre o emissor (Utilizador) e o receptor (Base de Dados).

3.3.3 Comunicação Utilizando Protocolo Station-to-Station

O último mecanismo desenvolvido e mais complexo, foi para a comunicação entre o servidor/serviço de telemedicina e a aplicação "HomeStation"(aplicação para os pacientes) explicitados no capítulo 5 .

3.3.3.1 Conceitos

No entanto antes de falar sobre este processo precisamos conhecer melhor os conceitos usados na implementação deste protocolo.

1. Cifra simétrica - utiliza uma chave exclusivamente partilhada entre duas entidades ou mais para cifrar e decifrar os dados. Num sistema de cifra de chaves simétricas é necessário que os intervenientes tenham conhecimento das chaves simétricas. A chave tem de ser enviada por um canal seguro ou entregar em mão à entidade receptora dos dados cifrados para que os possa decifrar.

2. Cifra assimétrica - cifra assimétrica ou algoritmo assimétrico é aquele onde a chave de cifragem é diferente da chave de decifragem. Isto é, usa-se uma chave para cifrar o texto e no momento de decifra-la usa-se ma outra chave que é inversa da primeira. Desta forma não fala-se mais de uma chave de cifragem e sim de um par de chaves únicos e inversas usadas no processo. Na literatura técnica costuma-se chamar as cifras assimétricas de cifras de chave pública e chave privada. Isso porque na maioria dos casos uma das chaves do par é tornada pública e a outra é mantido em segredo pelo proprietário da mesma. Isso propicia que este tipo de cifra possa ser usada para outros fins que não o sigilo dos dados. Essas cifras, como será mostrado mais à frente, poderão ser usadas para implementar os serviços de autenticação e certificação. Porém, conceptualmente existe uma diferença entre cifra assimétrica e de chave pública e privada. O primeiro conceito é mais amplo que o segundo. Isto é, toda cifra de chave pública é uma cifra assimétrica porém a recíproca não é verdadeira. Isso porque uma cifra para ser assimétrica basta que a chave de cifragem seja distinta da chave de decifragem, porém nada é garantido que a partir de uma chave não se deriva a outro.

3. Algoritmo AES - é um algoritmo de cifra simétrica por blocos, usa princípios de

difusão e confusão recorrendo a operações de permutação, substituição expansão e compressão para realizar a cifragem dos dados.

4. Certificado X.509 [14] - é um ficheiro de dados que contem informações referentes à entidade para qual o certificado foi emitido. Essa entidade pode ser uma pessoa, organização ou um computador. Acredita-se que este certificado pode identificar unicamente a entidade para qual foi emitido. No entanto é preciso entidades extra que validem o certificado, isto porque o certificado em si não é o rosto de uma organização ou pessoa. É necessário que haja uma entidade para validar que o certificado é válido e que podemos utilizar a sua chave pública, sabendo que só a entidade que queremos irá poder decifrar esses dados. A anatomia do certificado X.5009 (ver figura 3.2) é a seguinte:

   - Versão - Contem a versão do certificado X.509.
   - Número de serie - Todo certificado possui um, não é globalmente único, mas único no âmbito de uma CA (Certificate authority.
   - Tipo de algoritmo - Contem um identificador do algoritmo criptográfico usado pela CA para assinar o certificado juntamente com o tipo (ex. sha1).
   - Nome do titular - Nome da entidade para o qual o certificado foi emitido.
   - Nome do emitente - Autoridade Certificadora (CA) que emitiu/assinou o certificado.
   - Período de validade - Mostra o período de validade do certificado no formato "Não antes"e "Não depois"(Ex. "Não antes de 05/03/2010 - 14:35:02Não depois de 05/03/2012 - 14:03:20")
   - Informações de chave pública da entidade:

     Algoritmo de chave pública.

     Chave Publica.
   - Assinatura da Ca - A garantia que a CA valida a veracidade das informações contidas neste certificado de acordo com as políticas da CA.
   - Identificador da chave do titular - É uma extensão do X.509 que possui um identificador numérico para a chave pública contida neste certificado, especialmente útil para que programas de computador possam se referir a ela.

- Identificador da chave do emissor - A mesma ideia explicitada anteriormente, só que se referindo a chave pública da CA que emitiu o certificado.
- Atributos ou extensões - A vasta maioria dos certificados X.509 possui campos chamados extensão (OID) que contem algumas informações extra.

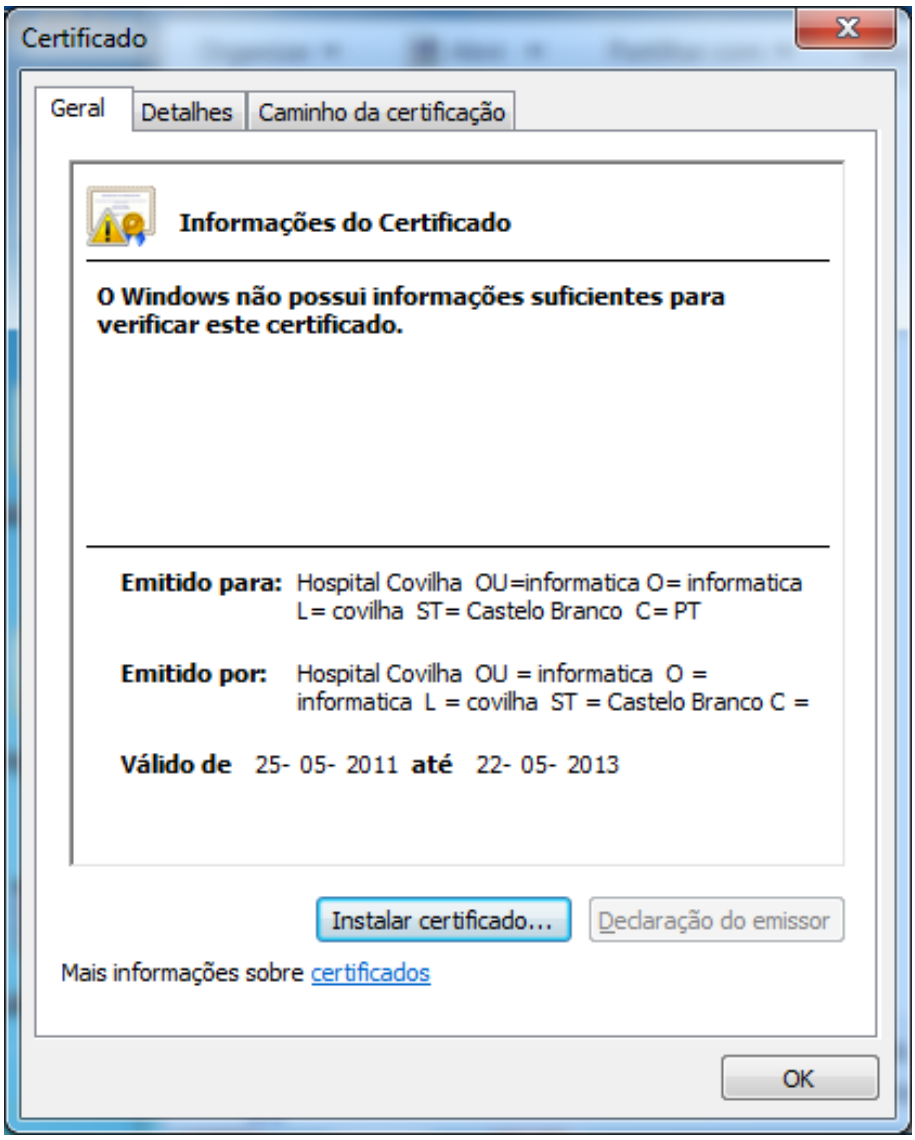

Figura 3.2: Exemplo de um Certificado

5. Chave publica - é uma chave utilizada para cifrar dados com algoritmos assimétricos. Esta chave pode ser publicada na Internet ou ser enviada pelo correio electrónico, isto é, se a pessoa que publicou a chave deseja que alguém envie algo cifrado com a sua chave pública. Sobre o ponto de vista matemático, o processo da criptografia de chave pública é baseado em funções de "one way"[15].

Estas funções têm a característica de serem fáceis de calcular e praticamente impossíveis de serem retrocedidas. Na criptografia de chave pública a cifragem do texto é a parte fácil. Qualquer pessoa pode cifrar o texto porque as instruções estão na chave pública. Mas decifrar é a parte difícil: sem conhecer o segredo, abrir a mensagem cifrada pode levar milhares de anos mesmo se for usado super computadores. O segredo é a chave privada, só com esta chave podemos rapidamente chegar ao texto claro.

6. Chave privada - é uma chave utilizada para decifrar os dados cifrados, explicitado anteriormente.

3.3.3.2 Solução Implementada

Nesta subsecção vamos explicar como foi implementado o protocolo STS (Station-to-Station). Vamos assumir que o "Bob"é o servidor de telemedicina e a "Alice"o utilizador comum que está em sua casa a utilizar a aplicação "Homestation". Também vamos assumir que o Bob tem a chave pública da Alice e a sua própria chave privada e a Alice tem a sua chave privada e a chave pública do Bob.

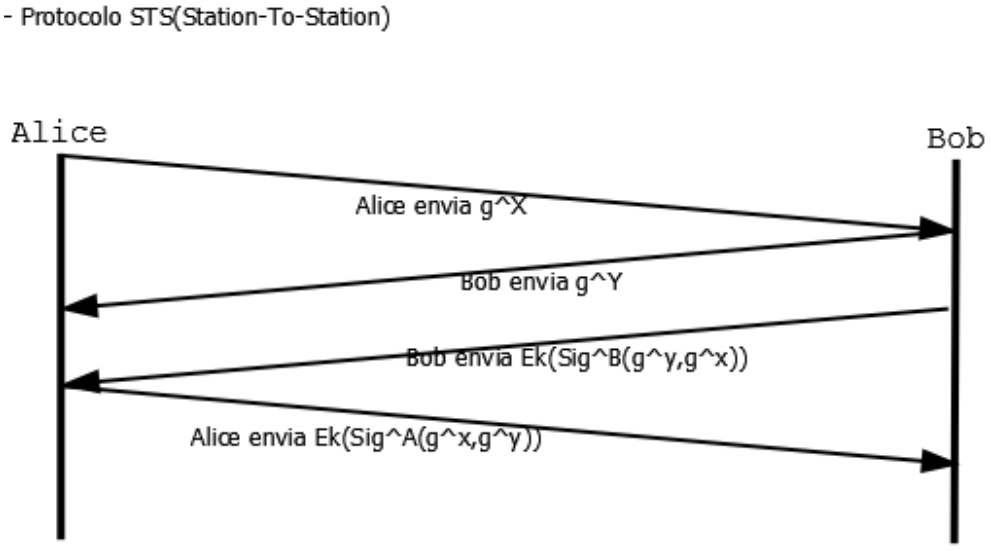

Figura 3.3: Diagrama do protocolo station-to-station

O protocolo (ver figura 3.3) começa pela "Alice"que equivale ao "HomeStation", carregando para a memória a sua chave privada e a chave pública do Bob, de seguida calcula dois parâmetros p e g. O parâmetro p é um número primo e o g é um número

inteiro menor do que p, com as seguintes propriedades: para cada numero n, entre 1 e p-1 inclusive, há uma potencia de K^g tal que $n = g^k mod p$. Depois do passo anterior é gerado um numero aleatório e privado X, de seguida é calculado g^x e a Alice envia este valor ao Bob. O Bob (servidor telemedicina) recebe o valor g^x e começa por carregar a sua chave privada e a chave publica da Alice para a memoria, cria os parâmetros p e g, cria um numero aleatório e privado Y, calcula o valor g^y, , envia à Alice este valor e depois concatena obrigatoriamente pela seguinte forma o valor g^y com g^x (g^y, g^x). Depois Bob assina digitalmente com a sua chave pública o valor g^x (g^y, g^x) que resulta em $SigB(g^y, g^x)$. Agora é preciso cifrar a mensagem anterior, para isso Bob calcula a chave partilhada k da seguinte forma: $k = (g^x)^y mod ep$ e cifra $SigB(g^y, g^x)$ com a chave k recorrendo ao algoritmo de cifra simétrica AES e o resultado é:$Ek(SigB(g^y, g^x))$ que por sua vez é enviado à Alice. A Alice recebe os dois valores anteriores enviados pelo Bob e calcula a chave secreta partilhada k da seguinte forma: $k = (g^y)^x mod ep$, depois utiliza esta chave para decifrar $Ek(SigB(g^y, g^x))$ e verifica se é válida a assinatura criada pelo Bob. Agora Alice vai concatenar os exponenciais (g^x, g^y) obrigatoriamente por esta ordem e assina usando a sua chave pública que resulta em $SigA(g^x, g^y)$. De seguida cifra utilizando a sua chave k: $Ek(SigA(g^x, g^y))$ e envia este valor para o Bob. O Bob recebe $Ek(SigA(g^x, g^y))$ e decifra utilizando a chave partilhada k criada anteriormente e verifica se a assinatura da Alice é válida. Agora o sistema está pronto para comunicar de forma segura entre os dois intervenientes. A troca de assinaturas permite verificar a autenticidade dos intervenientes, a não repudiação, integridade e a origem das mensagem assinadas, isto é, que a mensagem foi validada pelos dois que pretendem comunicar em segredo.

3.3.4 Conclusão

Foram aplicados diversos mecanismos para revolver vários problemas de segurança, que o sistema podia sofrer caso não fossem implementados. No entanto não podemos afirmar que o sistema está completamente seguro, mas podemos afirmar que os problemas mais graves de segurança foram resolvidos. Contudo será preciso contratar uma autoridade de certificação (CA) de certificados e todos os serviços inerentes para validar os certificados, além da aplicação SaudeGest ter algoritmos já implementados para criar e assinar certificados.

Capítulo 4

Engenharia do Software

Este capítulo refere os princípios de engenharia de software utilizados na criação do sistema de telemedicina[16].

4.1 Introdução

No desenvolvimento de aplicações informáticas complexas, para as organizações, tornou-se um factor muito importante criar métodos capazes de explicitar e facilitar a compressão de sistemas complexos. Isto para que o seu crescimento e posição perante as demais organizações seja competitivo e não seja afectado pela dinâmica de colaboradores que pode existir na criação e manutenção de um sistema. A Internet tornou-se um meio primordial para acompanhar todo o processo de uma organização, pelo que é um bom canal de partilha de recursos e transmissão de informação. Assim, com neste capítulo, pretende-se elaborar um conjunto de "esquemas"que possam retratar todo o processo de criação deste sistema complexo, composto por quatro aplicações que interagem entre si. A linguagem utilizada para modelar toda a informação é a UML (Unified Modelling Language[17]). A ferramenta utilizada para a elaboração dos diagramas designa-se por Astah Professional[18].

4.2 Identificação e análise de requisitos

Neste capítulo vamos identificar e analisar todos os requisitos para a construção do sistema de informação[16].

4.2.1 Anunciador

Aqui vamos expor a identificação e análise de requisitos para a aplicação Anunciador.

4.2.1.1 Ator

Um ator representa uma entidade externa que interage com o sistema. Foi identificado apenas um ator para esta aplicação.

- Gestor - A pessoa que regista e remove entidades da aplicação

4.2.1.2 Identificação dos Casos de Uso e Análise de Requisitos

Para este ator procedeu-se à identificação dos Casos de uso em que estes interagem com a aplicação como se pode ver na tabela 4.1.

Ator	Casos de Uso
Gestor	Registar Entidade
	Remover Entidade
	Consultar Entidade
	Actualizar Entidade
	Iniciar Serviço

Tabela 4.1: Tabela De Identificação dos Casos De Uso para o Anunciador

4.2.2 Servidor de Telemedicina

Aqui vamos expor a identificação e análise de requisitos para a aplicação Servidor de Telemedicina.

4.2.2.1 Ator

Um ator representa uma entidade externa que interage com o sistema. Foi identificado apenas um ator para esta aplicação e ator é o processo de automação em si no entanto identificado como servidor.

- Servidor Telemedicina - O processo de automatização que recebe exames médicos dos utentes e envia mensagens de aviso, recomendação e datas de consulta para o paciente que está utilizar a aplicação Anunciador. No entanto também gere o envio de mensagens dentro da entidade de saúde para avisar os profissionais de saúde sobre anomalia/problemas nos exames médicos recebidos.

4.2.2.2 Identificação dos Casos de Uso e Análise de Requisitos

Para este ator procedeu-se à identificação dos Casos de uso como se pode ver na tabela 4.2.

Ator	Casos de Uso
Servidor Telemedicina	Gerir recepção de dados Gerir envio de dados Gerir envio de mensagens

Tabela 4.2: Tabela De Identificação dos Casos De Uso para o Servidor Telemedicina

4.2.3 SaudeGest

Aqui vamos expor a identificação e análise de requisitos para a aplicação Servidor de Telemedicina.

4.2.3.1 Atores

Foi identificado dois atores para a aplicação SaudeGest.

- Administrador - É a pessoa que configura toda a aplicação, desde de configurar o acesso à base de dados, cria o primeiro registo de administrador e o certificado que assina os novos certificados emitidos para a entidade em questão. Depois tem a possibilidade de registar novos administradores ou utilizadores e os remover, pode também registar ou remover pacientes e consultar toda a informação da base de dados.

- Utilizador - É a pessoa que pode registar ou remover pacientes, bem como consultar toda a sua informação que está gravada na base de dados.

4.2.3.2 Identificação dos Casos de Uso e Análise de requisitos

Para estes atores procedeu-se à identificação dos Casos de uso em que estes interagem com a aplicação como se pode ver na tabela 4.3.

Ator	Casos de Uso
Administrador	Configurar e Registar a aplicação Consultar Registar Administrador ou Utilizador Remover Administrador ou Utilizador Registar Pacientes Remover Pacientes
Utilizador	Registar Utilizador Remover Utilizador Consultar

Tabela 4.3: Tabela De Identificação dos Casos De Uso para a aplicação SaudeGest

4.2.4 HomeStation

Aqui vamos expor a identificação e análise de requisitos para a aplicação Servidor de HomeStation.

4.2.4.1 Atores

Foi identificado dois atores para a aplicação HomeStation.

- Utilizador - É o paciente que inicialmente precisa de registar-se na aplicação com a devida credencial, pode efetuar quatro exames médicos tais como: tensão arterial, oximetro, electrocardiograma e balança. Podem também após fazer login remover-se a si mesmo como utilizador da aplicação.

- HomeStation - É a aplicação em si que pode gerir o envio de exames médicos para a central de telemedicina predefinida, pode também gerir a recepção de mensagens do serviço e reportar este avisos ao utilizador

4.2.4.2 Identificação dos Casos de Uso e Análise de requisitos

Para estes atores procedeu-se à identificação dos Casos de uso em que estes interagem com a aplicação como se pode ver na tabela 4.4.

Ator	**Casos de Uso**
Utilizador	Registar-se na aplicação Efetuar exame de rotina Remover utilizador
HomeStation	Gerir envio de dados Gerir recepção de dados Gerir envio de mensagens

Tabela 4.4: Tabela De Identificação dos Casos De Uso para a aplicação HomeStation

4.3 Casos de Uso

Os diagramas Casos De Uso permitem descrever um cenário que mostra as principais funcionalidades do sistema[16].

4.3.1 Diagrama casos de Uso para Anunciador

Na figura 4.1 podemos visualizar o diagrama casos de usos criado para representar as principais funcionalidade da aplicação Anunciador.

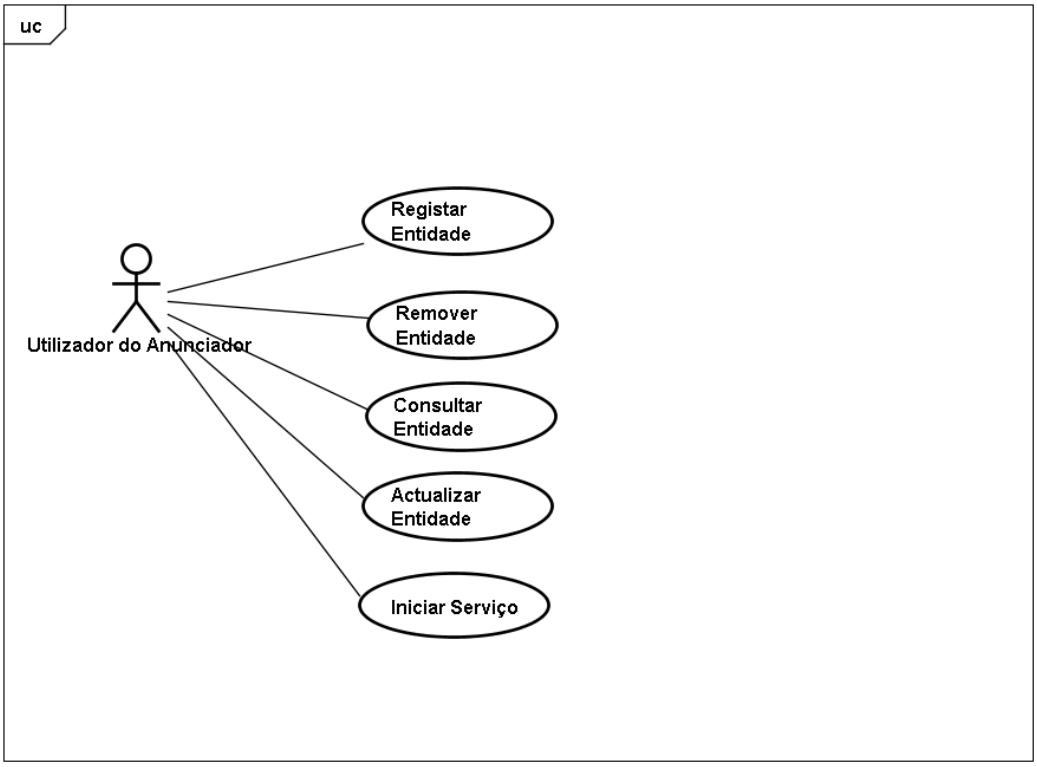

Figura 4.1: Diagrama Casos de Uso para Annunciador

4.3.2 Diagrama casos de Uso para Servidor de Telemedicina

Na figura 4.2 podemos visualizar o diagrama casos de usos criado para representar as principais funcionalidade da aplicação Anunciador

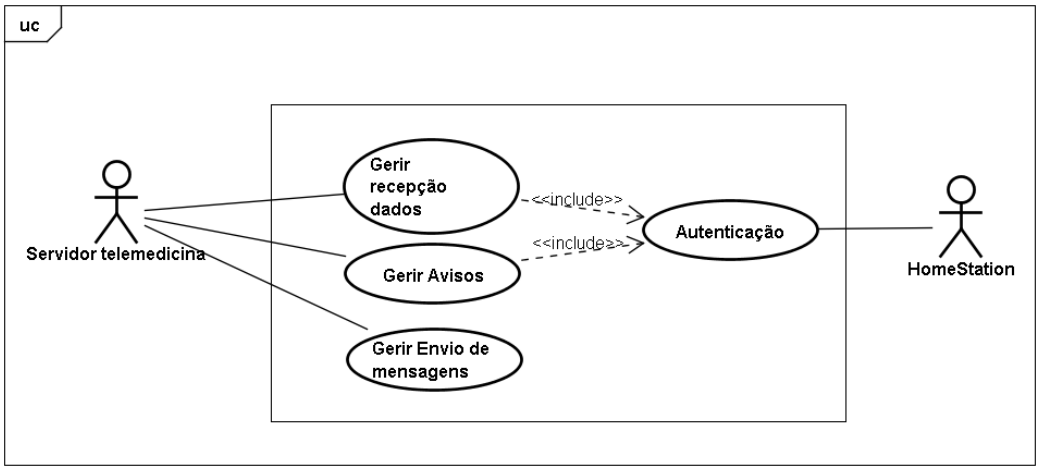

Figura 4.2: Diagrama Casos de Uso para Servidor de Telemedicina

4.3.3 Diagrama casos de Uso para SaudeGest

Neste secção vamos expor os diagramas caso de uso para o administrador e para o utilizador da aplicação SaudeGest.

4.3.3.1 Administrador

Na figura 4.3 podemos visualizar o diagrama casos de usos criado para representar as principais funcionalidades do administrador na aplicação SaudeGest

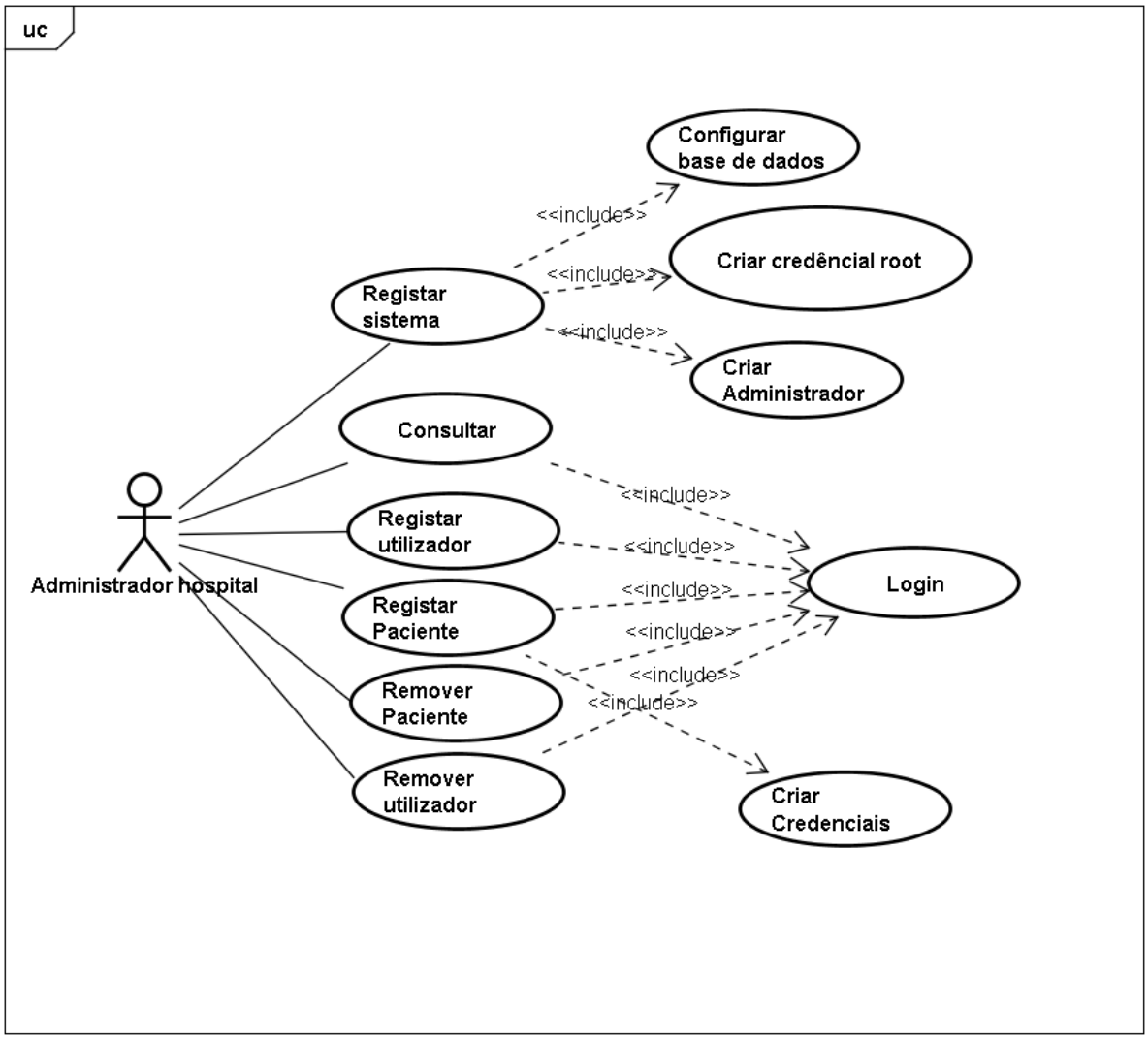

Figura 4.3: Diagrama Casos de Uso do administrador para aplicação SaudeGest

4.3.3.2 Utilizador

Na figura 4.4 podemos visualizar o diagrama casos de usos criado para representar as principais funcionalidades do utilizador na aplicação SaudeGest

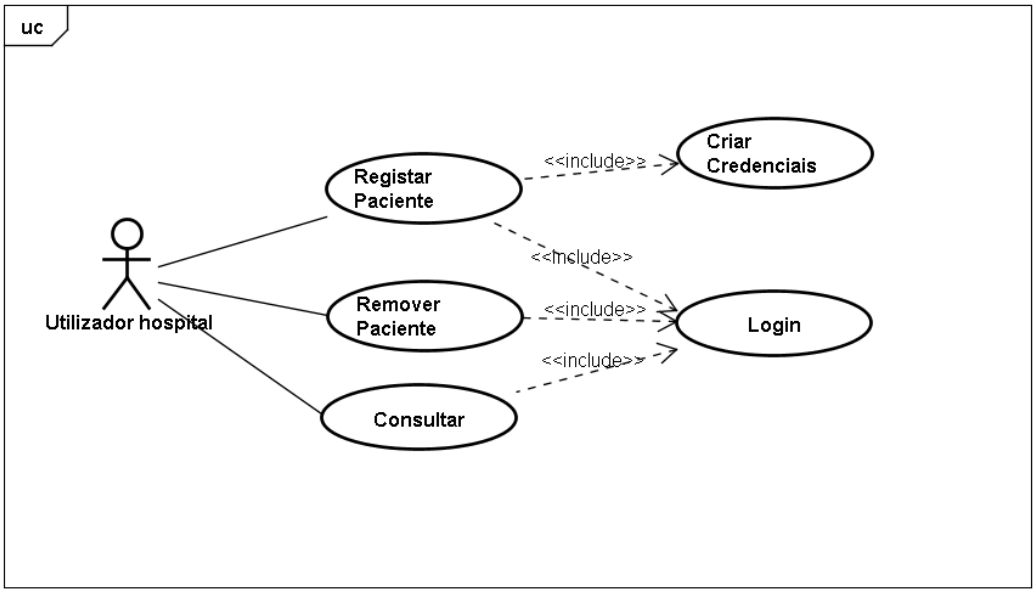

Figura 4.4: Diagrama Casos de Uso do utilizador para aplicação SaudeGest

4.3.4 Diagrama casos de Uso para HomeStation

Neste secção vamos expor os diagramas caso de uso para o utilizador e para o processo de automatização da aplicação HomeStation.

4.3.4.1 Utilizador da aplicação HomeStation

Na figura 4.5 podemos visualizar o diagrama casos de usos criado para representar as principais funcionalidades do utilizador da aplicação HomeStation.

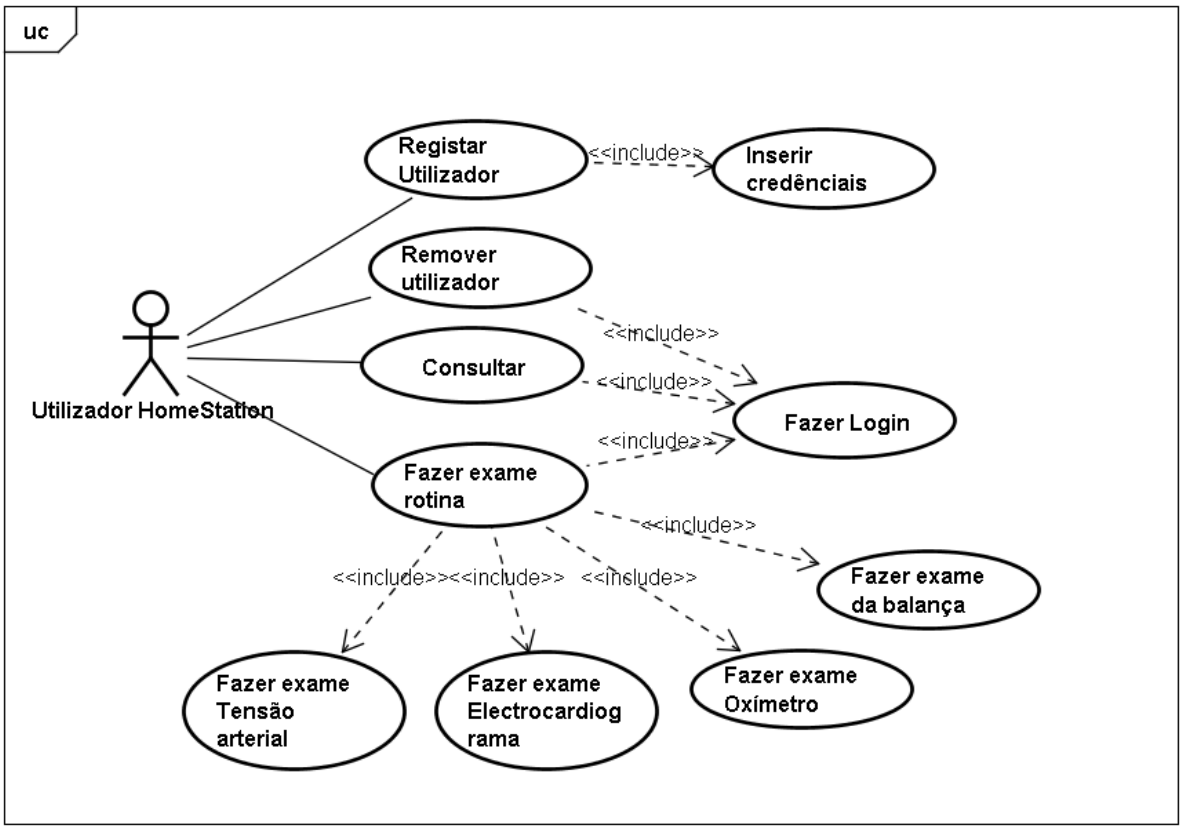

Figura 4.5: Diagrama Casos de Uso do paciente para aplicação HomeStation

4.3.4.2 Processo automatizado da HomeStation

Na figura 4.6 podemos visualizar o diagrama casos de usos criado para representar as principais funcionalidades do processo automatizado da aplicação HomeStation.

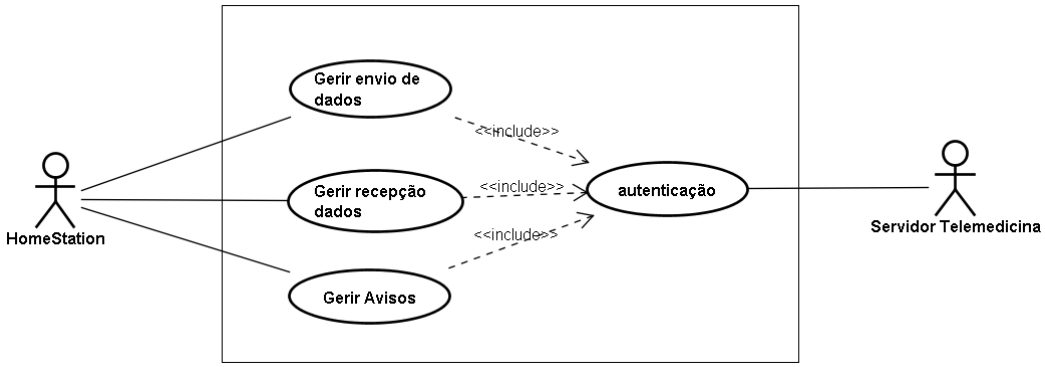

Figura 4.6: Diagrama Casos de Uso do processo automatizado da aplicação HomeStation

4.4 Diagramas de Sequência

Os diagramas de sequência apresentam as interações entre objectos a partir do encadeamento temporal das mensagens. Para elaboração dos diagramas de sequência, foram tidos em consideração os casos de usos previamente explicitados.

4.4.1 Anunciador

Aqui serão expostos os diferentes diagramas de sequência elaborados para o utilizador do anunciador.

4.4.1.1 Utilizador do Anunciador

Para este ator foram tidos em consideração os seguintes Casos de Uso:

- Registar Entidade

- Remover Entidade

- Consultar Entidade

- Actualizar Entidade

O diagrama de sequência para o caso de uso "Registar Entidade"é o seguinte que se pode visualizar na figura 4.7.

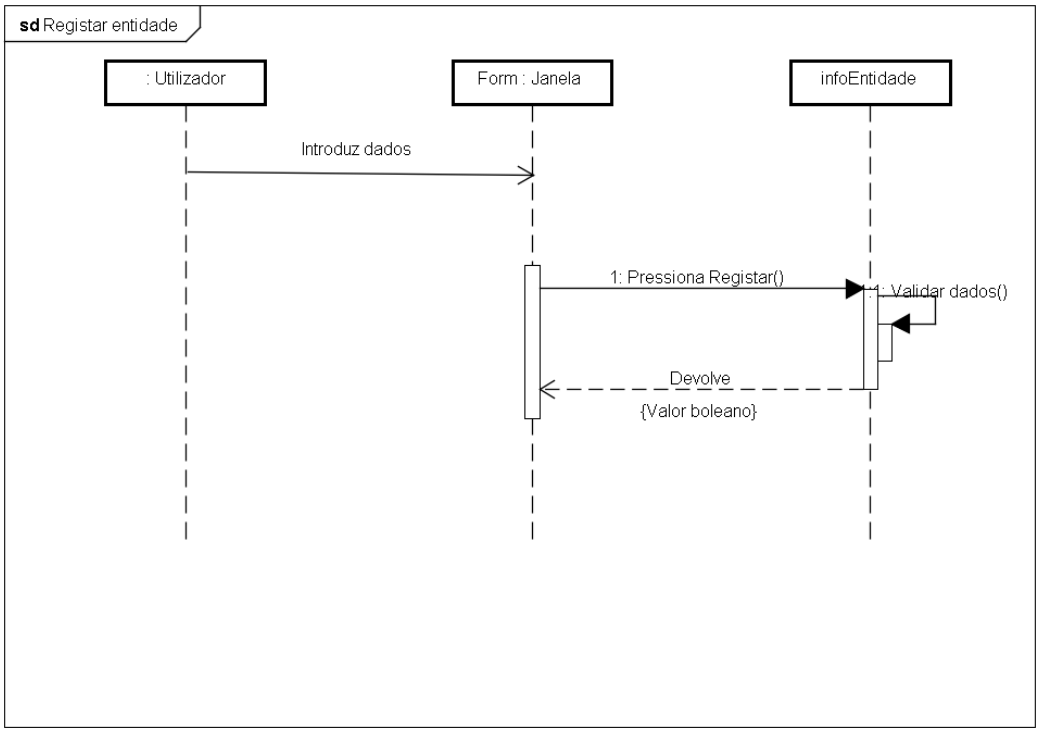

Figura 4.7: Diagrama sequência Registar Entidade

O diagrama de sequência para o caso de uso "Remover Entidade"é o seguinte que se pode visualizar na figura 4.8.

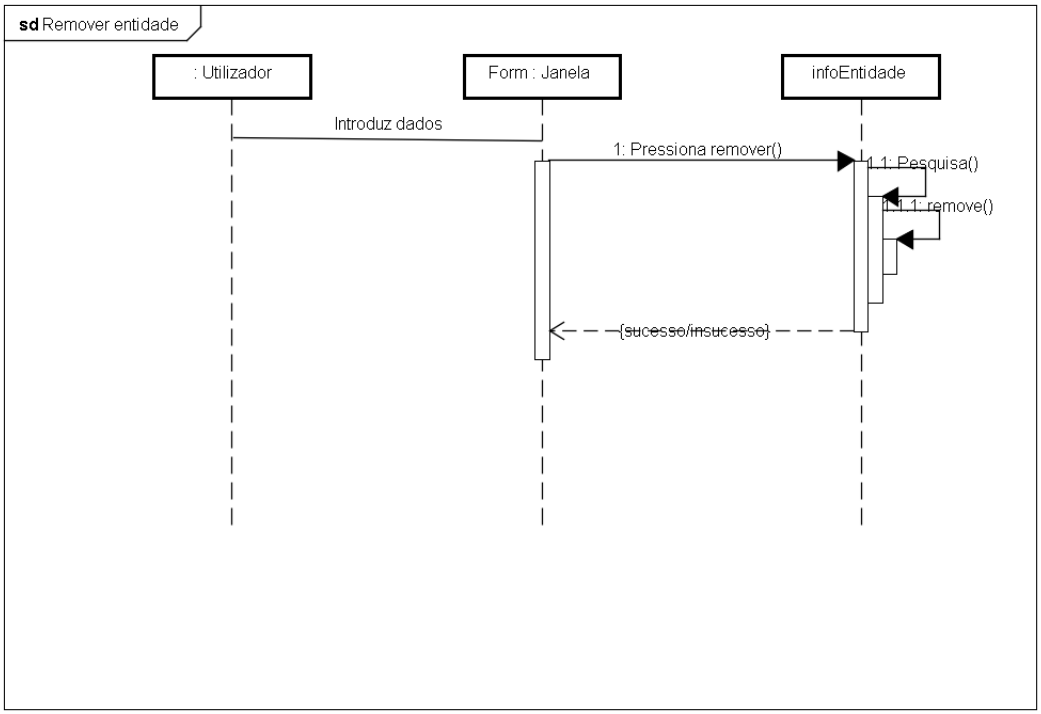

Figura 4.8: Diagrama sequência Remover Entidade

O diagrama de sequência para o caso de uso "Consultar Entidade"é o seguinte que se pode visualizar na figura 4.9.

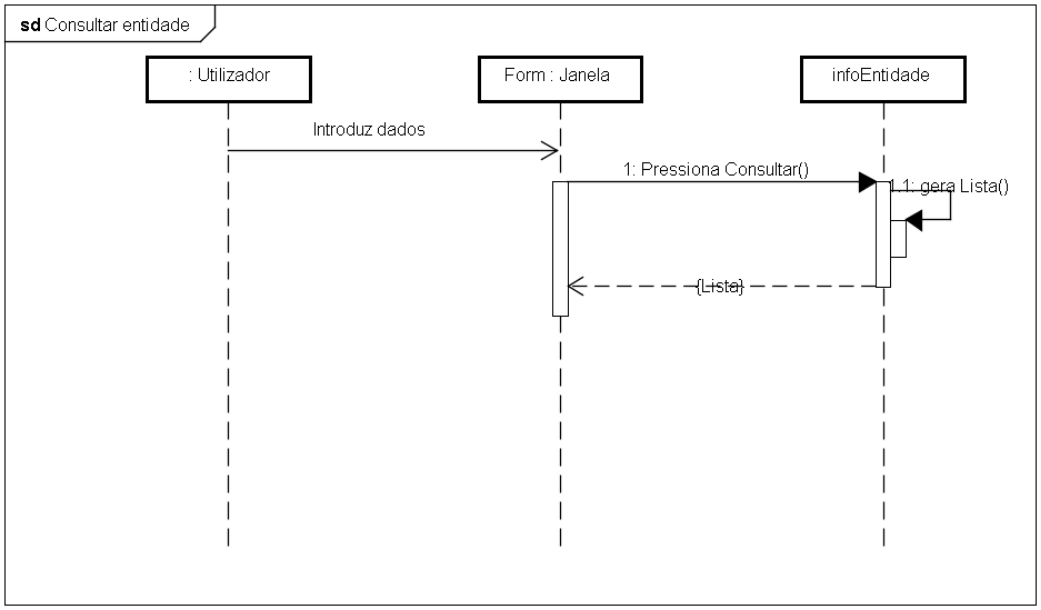

Figura 4.9: Diagrama sequência Consultar Entidade

O diagrama de sequência para o caso de uso "Actualizar Entidade"é o seguinte que se pode visualizar na figura 4.10.

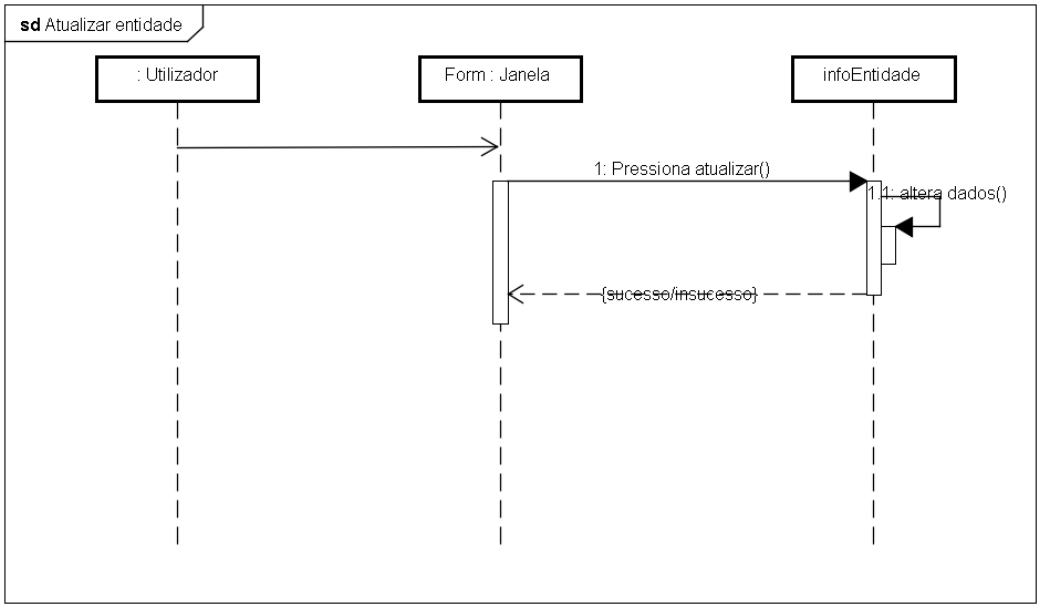

Figura 4.10: Diagrama sequência Actualizar Entidade

4.4.2 Servidor de Telemedicina

Aqui serão expostos os diferentes diagramas de sequência elaborados para o processo automatizado do servidor de telemedicina. No entanto como se pode ponto 4.3.2, temos o caso de uso autenticação e o seu funcionamento foi explicitado previamente no capitulo 3

4.4.2.1 Servidor de Telemedicina

Para este ator foram tidos em consideração os seguintes Casos de Uso:

- Gerir recepção de dados
- Gerir envio de dados
- Gerir envio de mensagens

O diagrama de sequência para o caso de uso "Gerir recepção de dados"é o seguinte que se pode visualizar na figura 4.11.

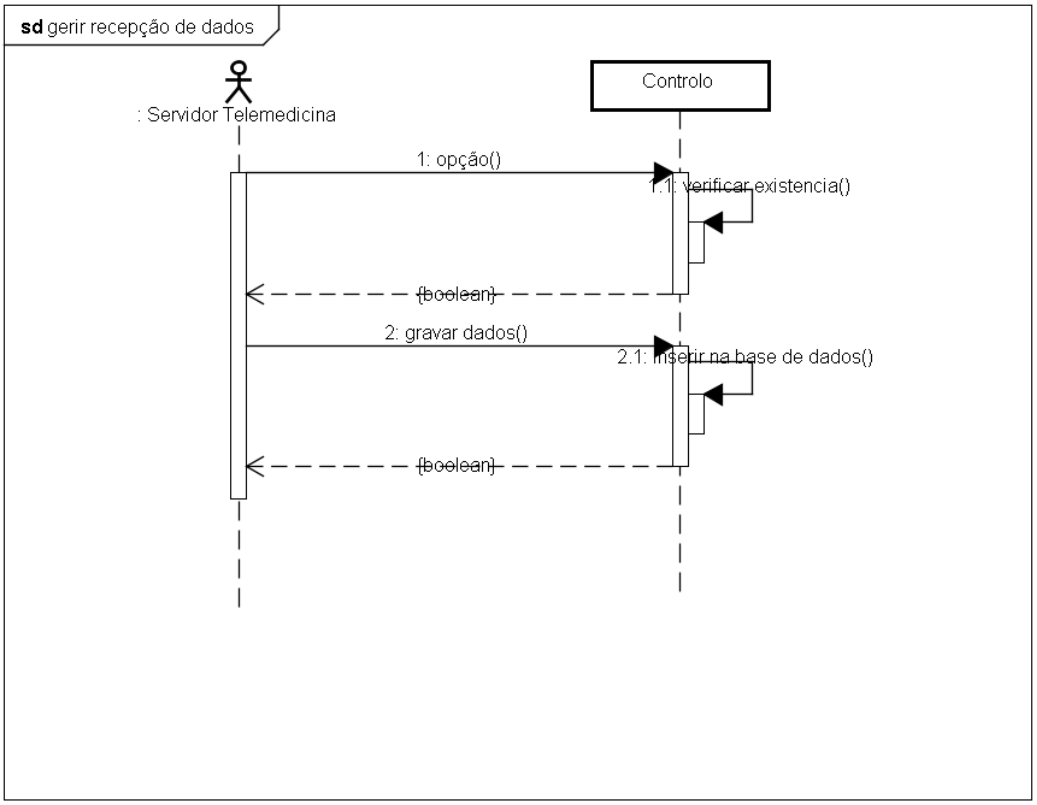

Figura 4.11: Diagrama sequência gerir recepção de dados

O diagrama de sequência para o caso de uso "Gerir envio de dados"é o seguinte que se pode visualizar na figura 4.12.

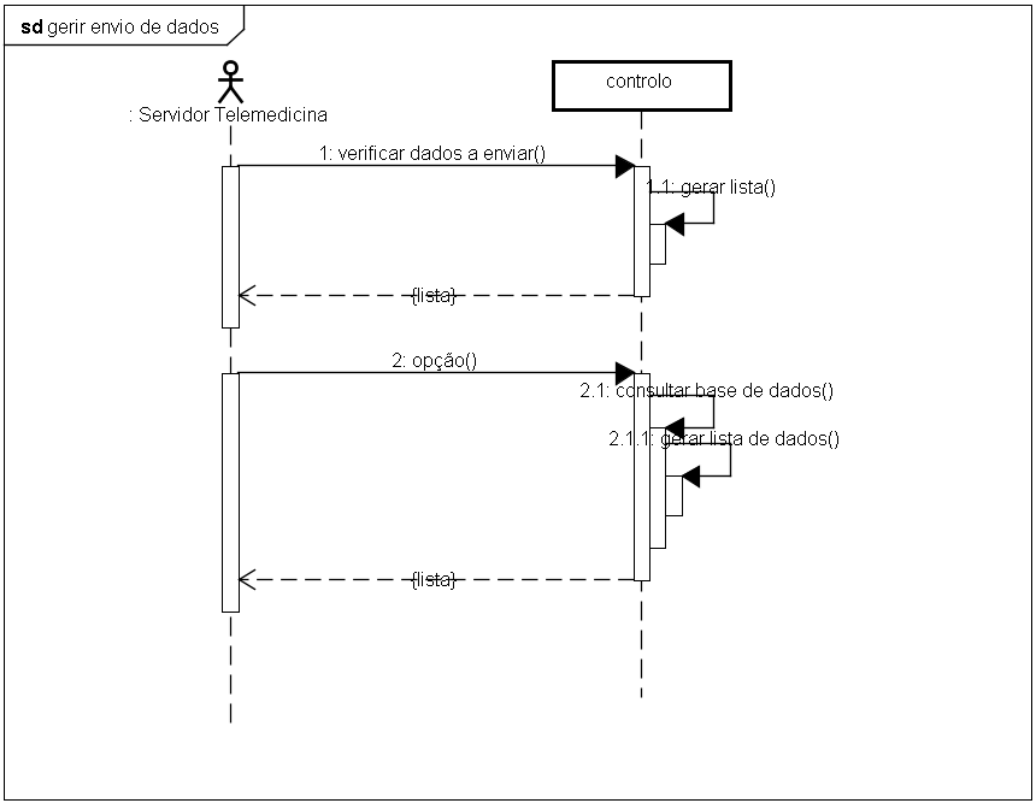

Figura 4.12: Diagrama sequência gerir envio de dados

O diagrama de sequência para o caso de uso "Gerir envio de mensagens"é o seguinte que se pode visualizar na figura 4.13.

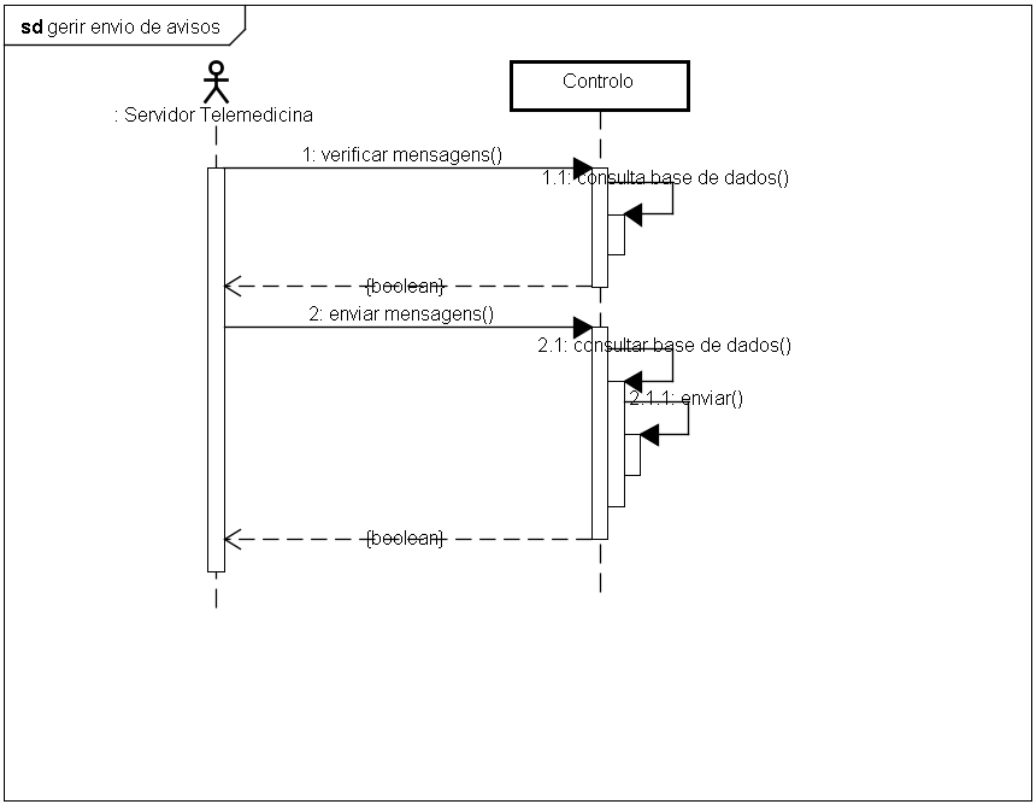

Figura 4.13: Diagrama sequência gerir envio de mensagens

4.4.3 SaudeGest

Aqui serão expostos os diferentes diagramas de sequência elaborados para a realização do software SaudeGest. Não foi realizado diagramas de sequência para o utilizador porque são idênticos ao do Administrador apenas com menos funcionalidades. O mecanismo de "Login"já foi explicitado no capitulo 3.

4.4.3.1 Administrador

Para este ator foram tidos em consideração os seguintes Casos de Uso:

- Registar Sistema
- Consultar

- Registar utilizador

- Remover utilizador

- Registar paciente

- Remover paciente

O diagrama de sequência para o caso de uso "Registar Sistema"é o seguinte que se pode visualizar na figura 4.14.

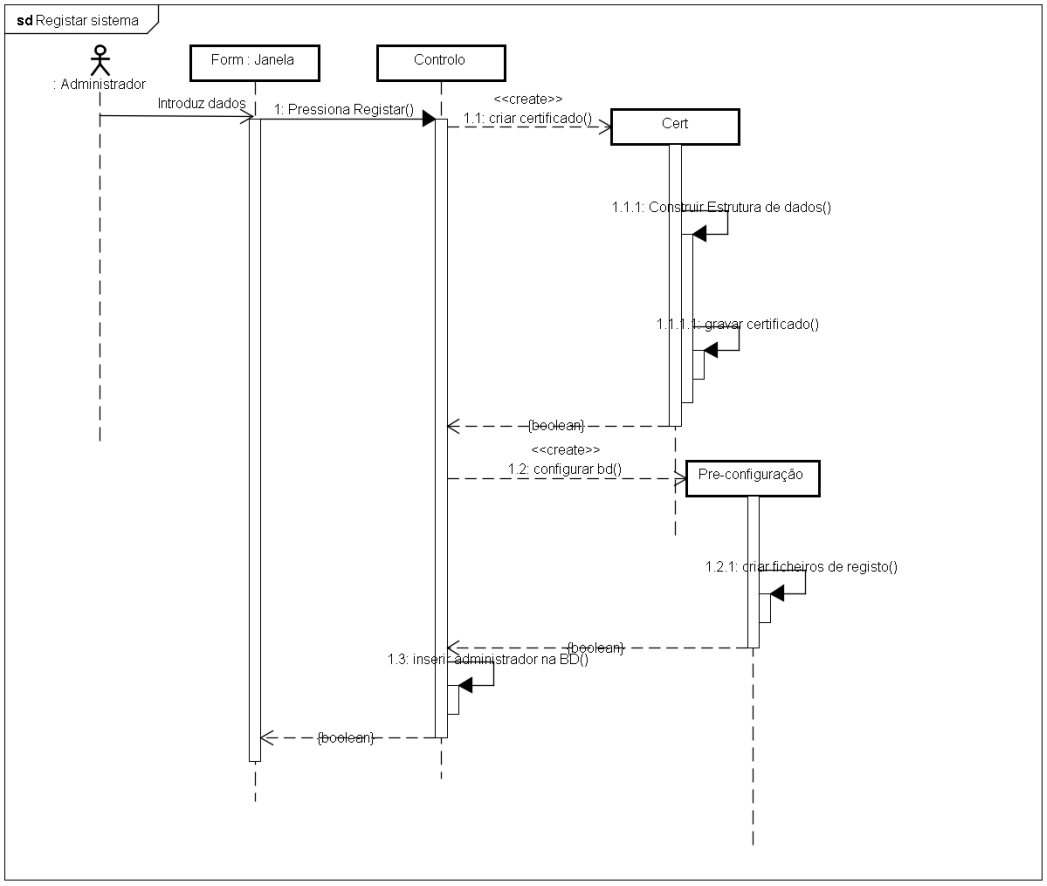

Figura 4.14: Diagrama sequência Registar Sistema

O diagrama de sequência para o caso de uso "Consultar"é o seguinte que se pode visualizar na figura 4.15.

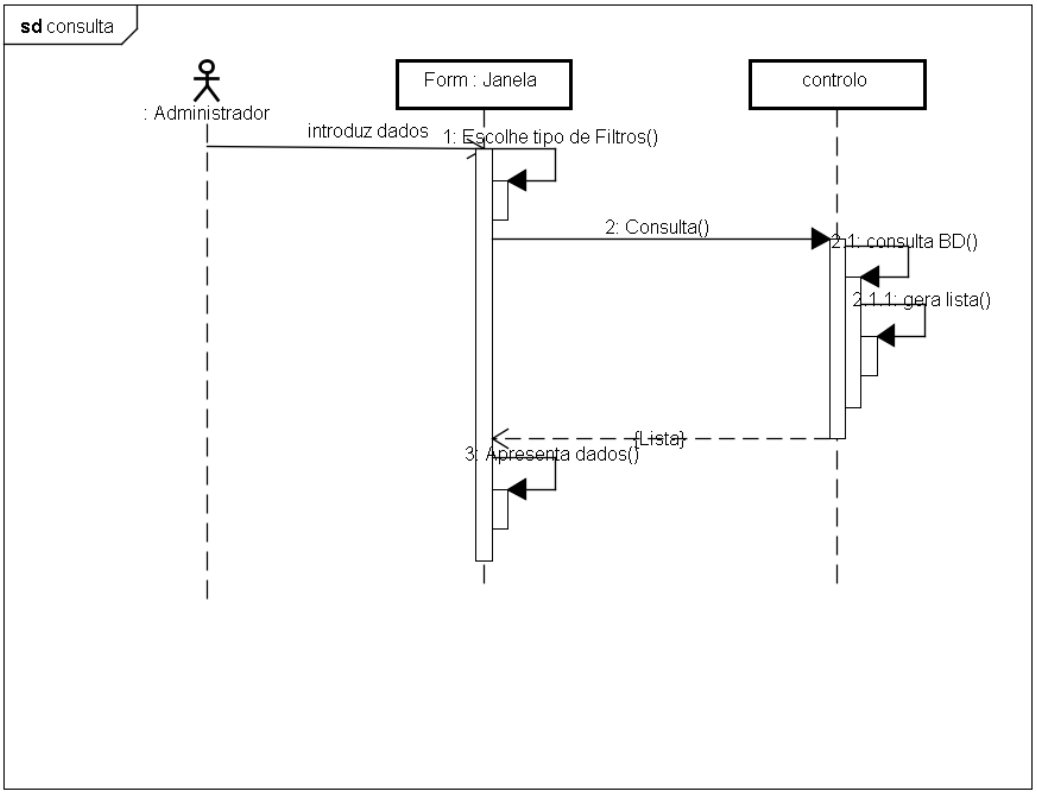

Figura 4.15: Diagrama sequência Consultar

O diagrama de sequência para o caso de uso "Registar utilizador"é o seguinte que se pode visualizar na figura 4.16.

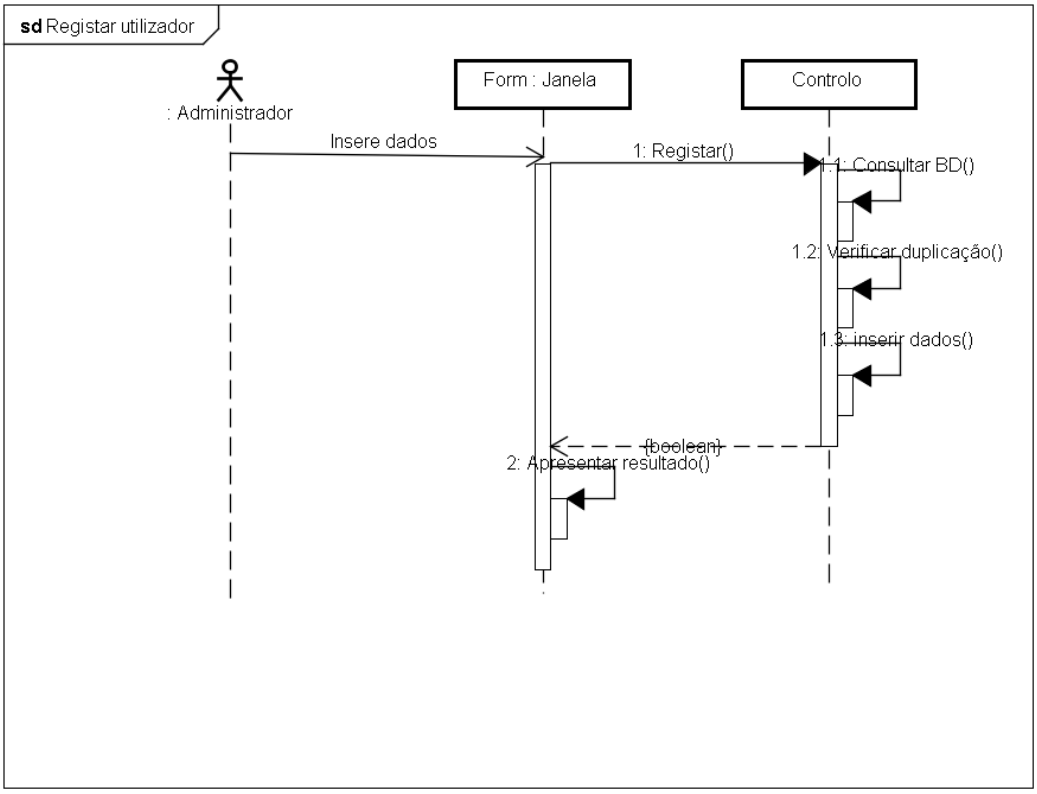

Figura 4.16: Diagrama sequência Registar utilizador

O diagrama de sequência para o caso de uso "Remover utilizador"é o seguinte que se pode visualizar na figura 4.17.

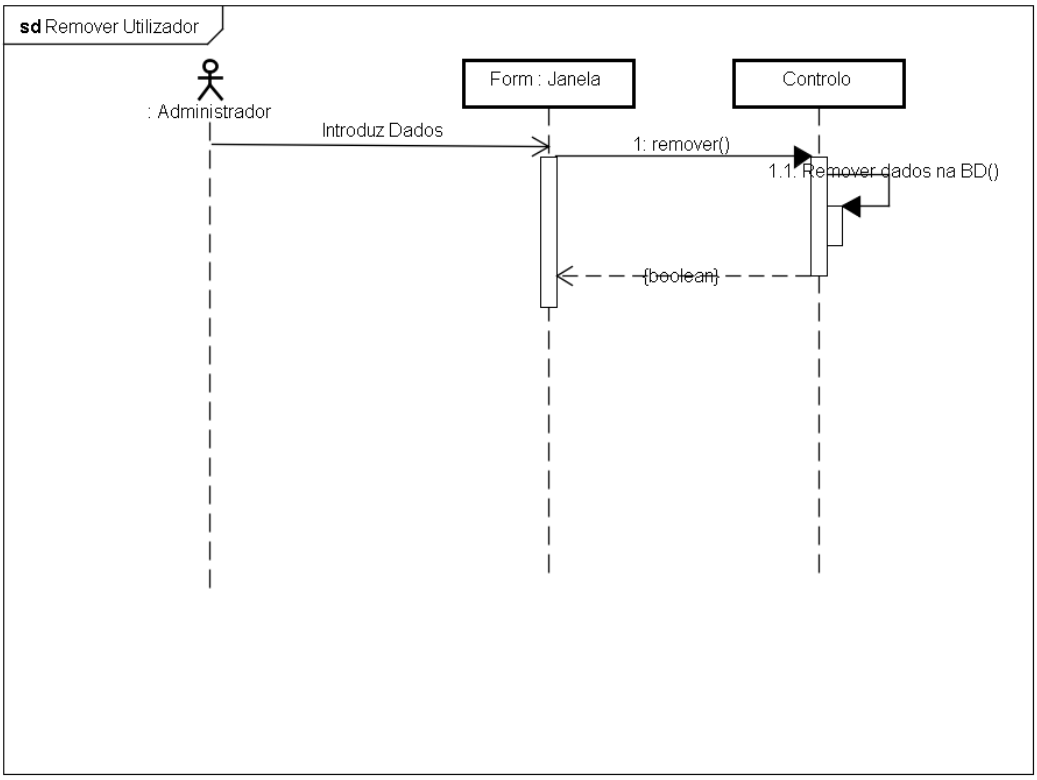

Figura 4.17: Diagrama sequência Remover utilizador

O diagrama de sequência para o caso de uso "Registar paciente"é o seguinte que se pode visualizar na figura 4.18.

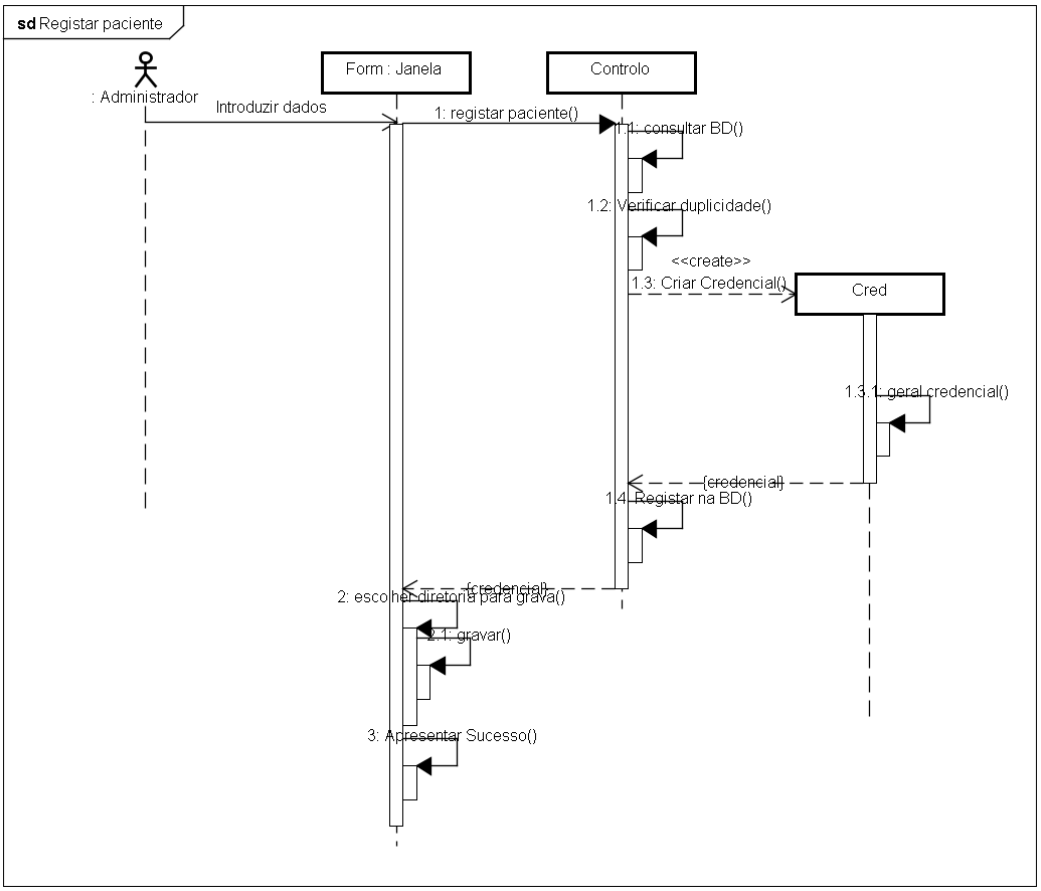

Figura 4.18: Diagrama sequência Registar paciente

O diagrama de sequência para o caso de uso "Remover paciente"é o seguinte que se pode visualizar na figura 4.19.

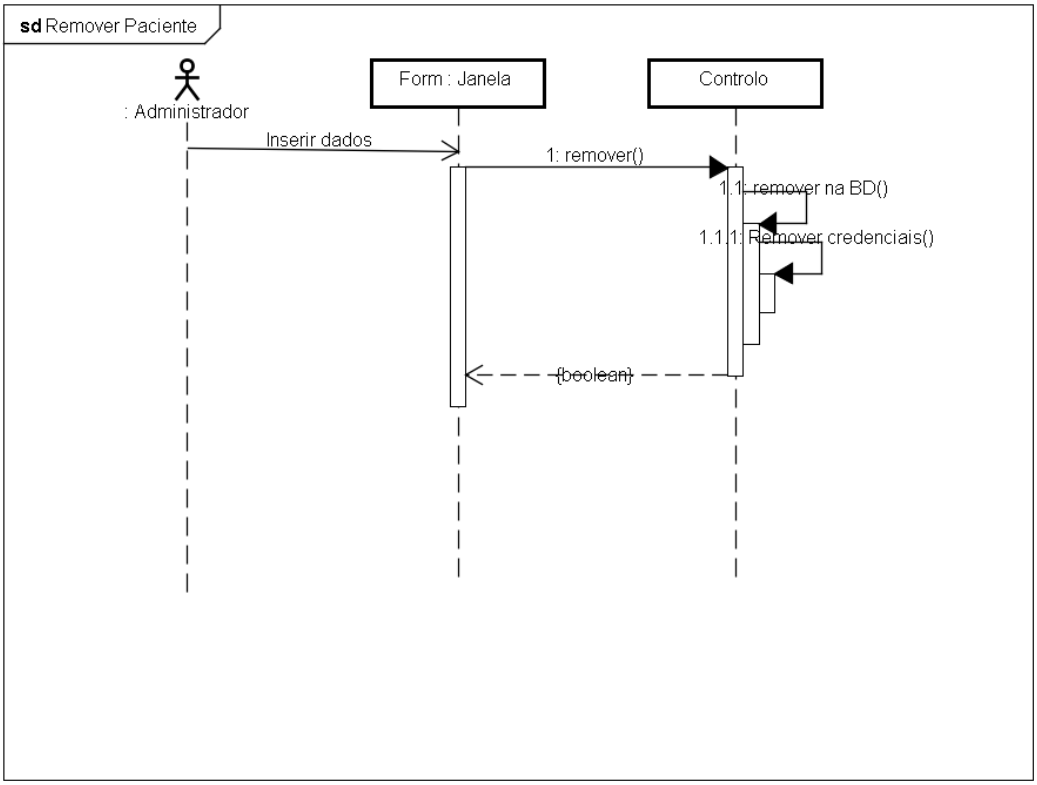

Figura 4.19: Diagrama sequência Remover paciente

4.4.4 HomeStation

Aqui serão expostos os diferentes diagramas de sequência elaborados para realização da aplicação "HomeStation", no entanto o processo de automatização não vai ser demonstrado em diagrama de sequência porque é idêntico ao do servidor de telemedicina.

4.4.4.1 Utilizador HomeStation

Para este ator foram tidos em consideração os seguintes Casos de Uso:

- Registar Utilizador
- Remover Utilizador
- Fazer exame rotina

- Consulta

O diagrama de sequência para o caso de uso "Consulta"não foi elaborado porque não foi implementada essa funcionalidade.

O diagrama de sequência para o caso de uso "Registar Utilizador"é o seguinte que se pode visualizar na figura 4.20.

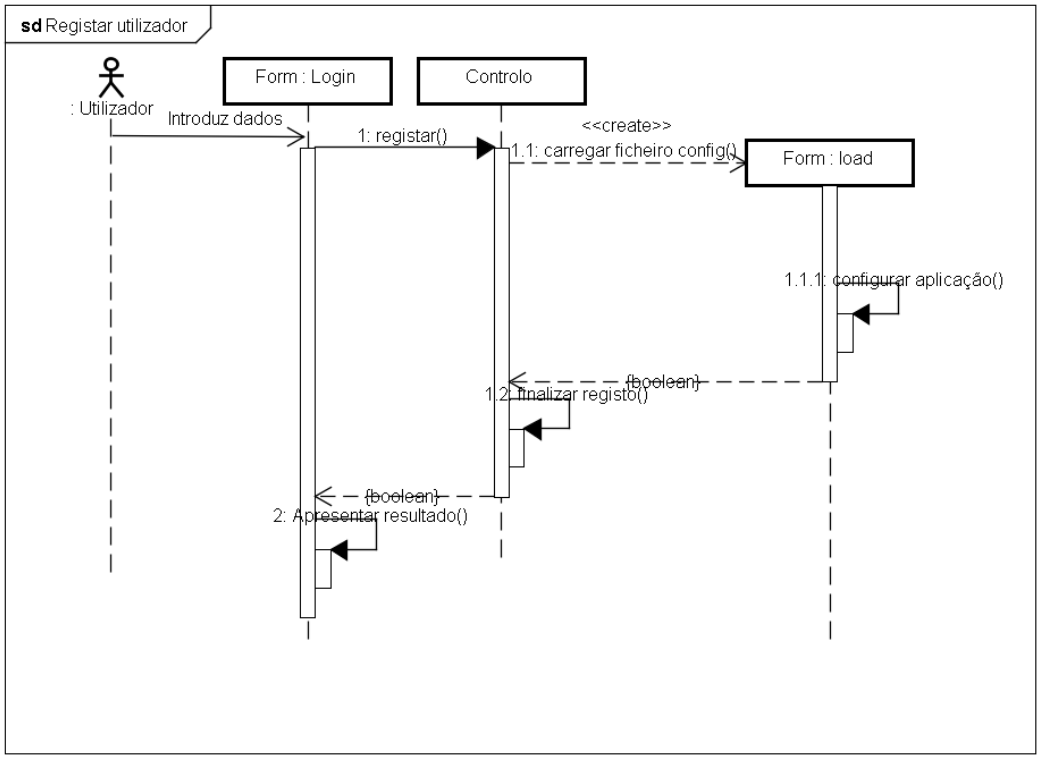

Figura 4.20: Diagrama sequência Registar Utilizador

O diagrama de sequência para o caso de uso "Remover Utilizador"é o seguinte que se pode visualizar na figura 4.21.

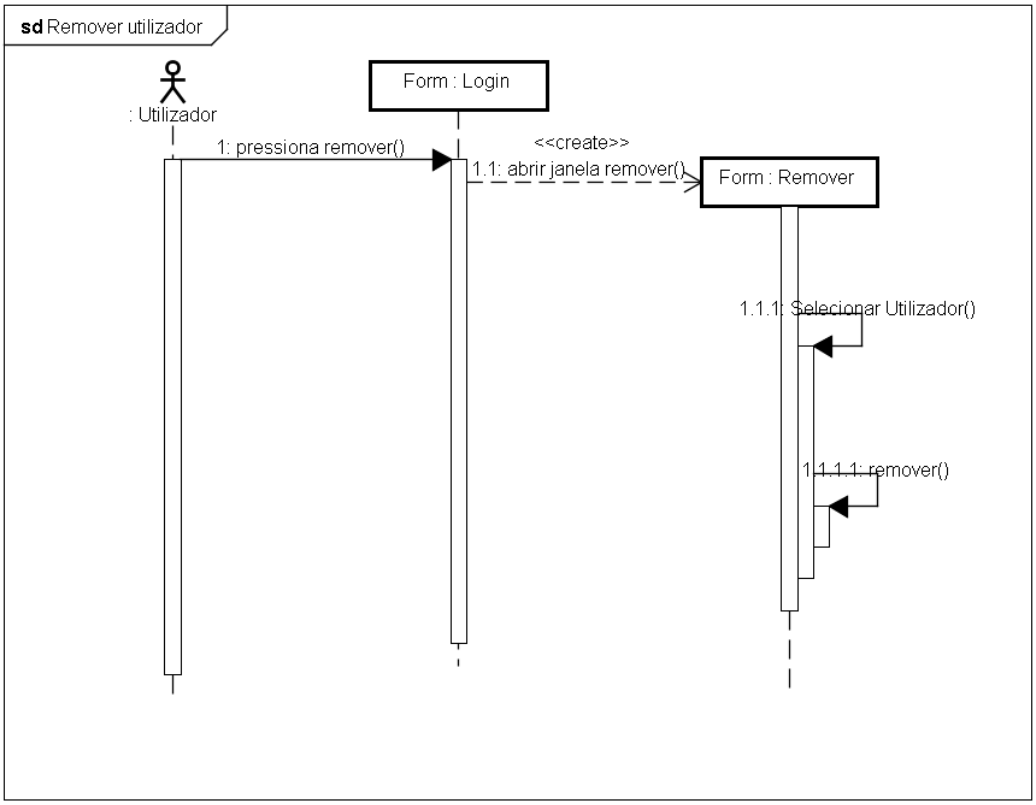

Figura 4.21: Diagrama sequência Remover Utilizador

O diagrama de sequência para o caso de uso "Fazer exame rotina"é o seguinte que se pode visualizar na figura 4.22. Este diagrama está muito simplificado porque os módulos para realizar exames médicos foram desenvolvidos pelo Fábio Campos para o seu projecto de mestrado.

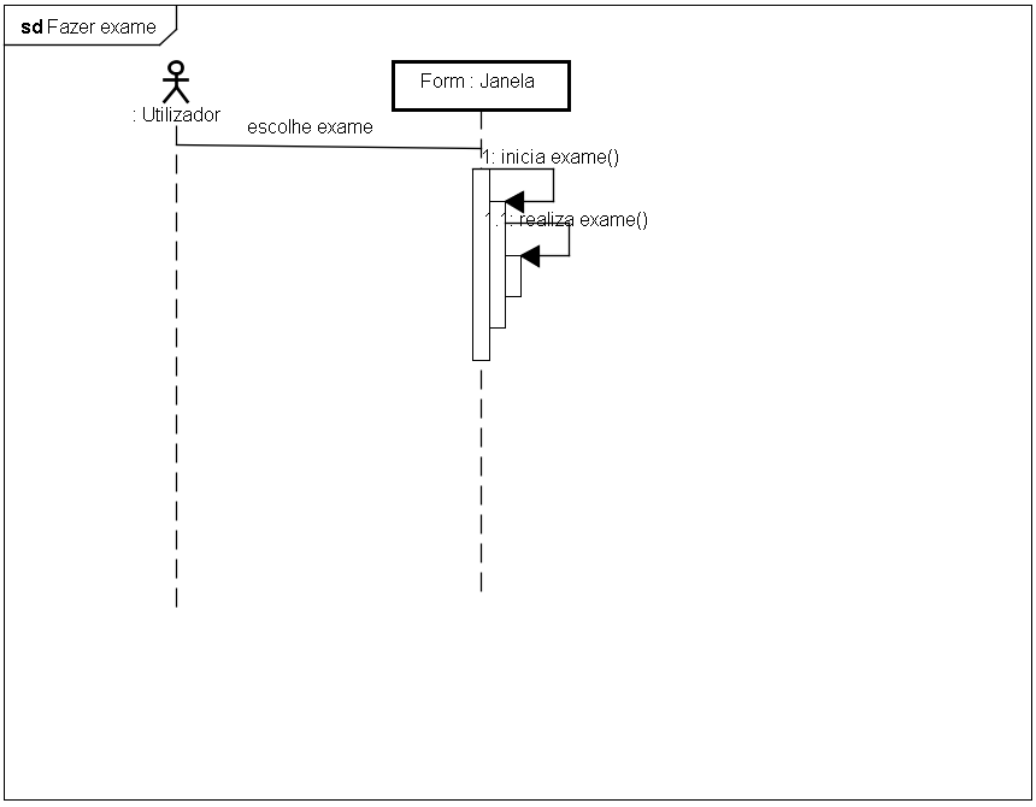

Figura 4.22: Diagrama sequência Fazer exame rotina

4.5 Diagrama de Instalação

Como se pode ver na figura 4.23 temos o diagrama de instalação com todos os relacionamentos físicos entre os componentes de software e hardware para o sistema distribuído desenvolvido.

O diagrama ilustra a arquitectura do sistema distribuído em termos de nós que efetuam o processamento dos componentes:

- Nó - representa um parte de hardware do sistema
- Componente - representa uma aplicação (software)

O diagrama da figura 4.23 está representado todo o hardware e aplicações necessárias para construir o sistema de telemedicina desenvolvido nesta tese, bem como a localização de cada componente. O nó "Servidor de Telemedicina"contem dois componentes "Thread: servidor"que representam os vários processos que o servidor cria para cada novo utilizador que se liga ao servidor, este processos tratam do todo o processo de automatização das comunicações entre servidor e o cliente. O mesmo se aplica para o nó "Servidor Anunciador", no entanto o nó "Tablet pc", a sua aplicação apenas cria um processo "Thread: cerebro".

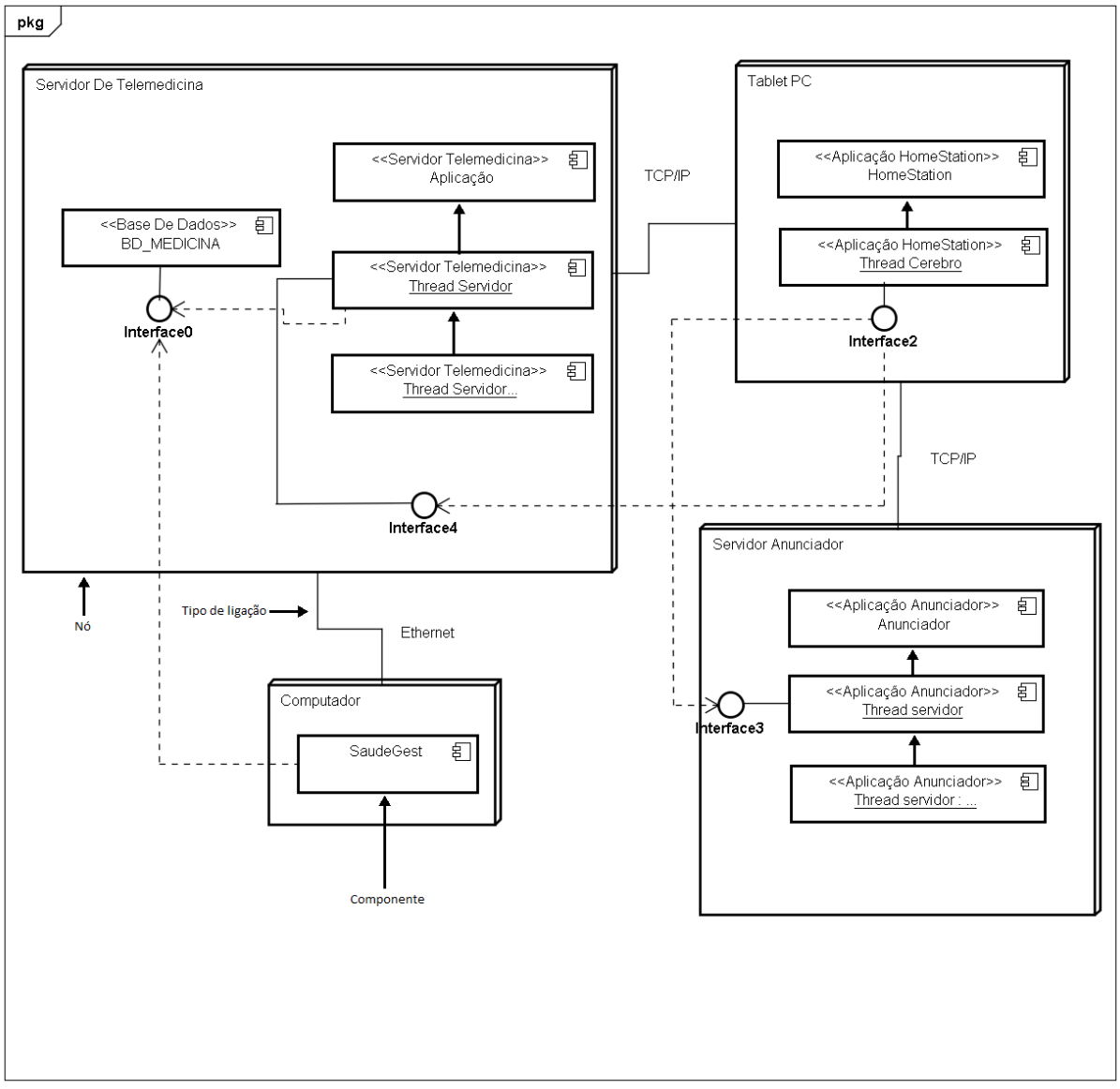

Figura 4.23: Diagrama de Instalação

4.6 Conclusão

Os diagramas mais importantes foram elaborados para o desenvolvimento deste sistema distribuído. No entanto só foi detalhado as operações mais importantes.

Capítulo 5

Solução Desenvolvida

5.1 Introdução

Neste capítulo vamos explicitar todo o sistema desenvolvido para criar a solução de telemedicina. Vamos poder observar ao longo deste capítulo, que o sistema é composto por várias aplicações que desempenham diferentes papéis no funcionamento do sistema. Para o suposto fornecedor de serviços de telemedicina foi desenvolvido duas aplicações, uma para gerir, outra será o serviço em si prestado ao paciente. Foi criado também uma aplicação que se chama "Anunciador", o seu papel será aclarado posteriormente. Uma última aplicação criada foi a "HomeStation", é uma aplicação para os pacientes que estão em casa. O sistema é composto por quatro aplicações e duas delas funcionam como serviço prestado ao público. No desenrolar deste documento será exposto o papel de cada uma delas.

5.2 Visão Geral Do Sistema

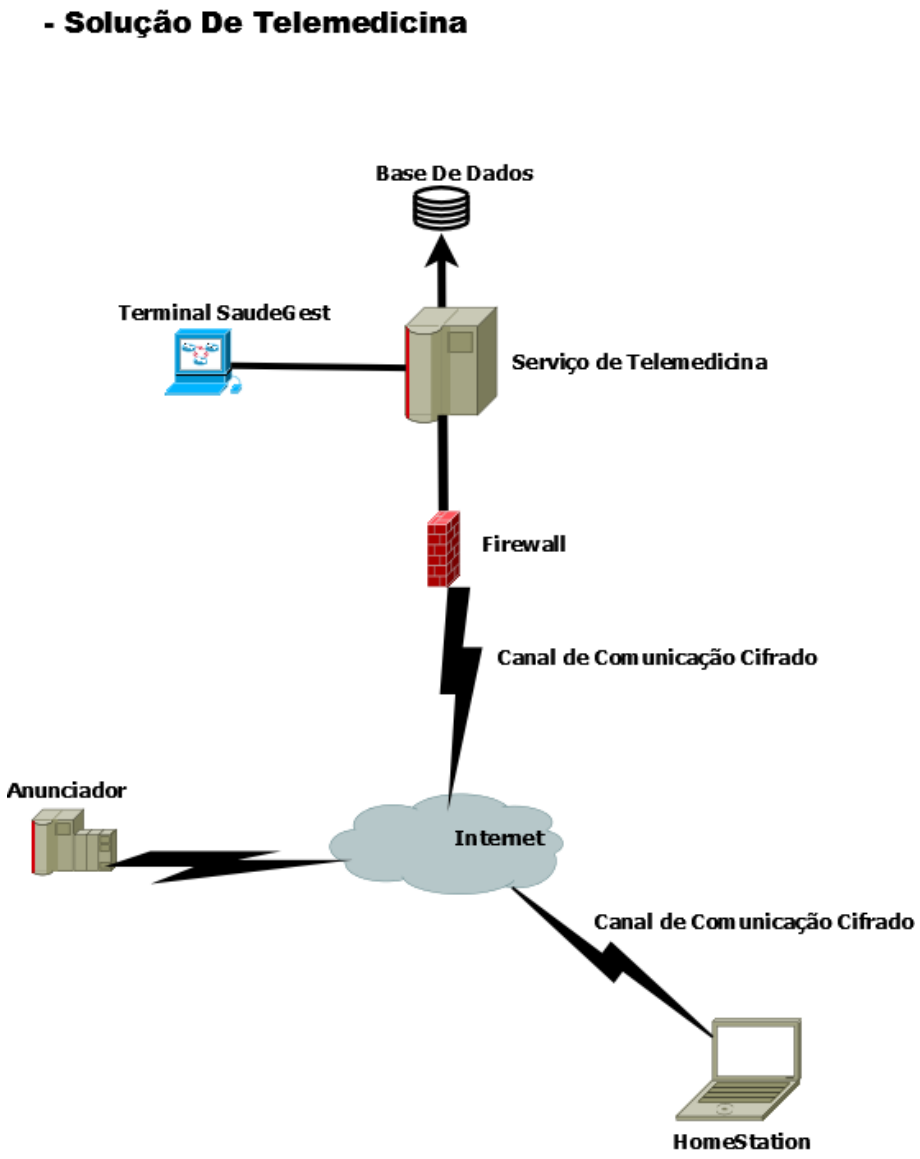

Figura 5.1: Diagrama Geral Do Sistema de Telemedicina

Como podemos observar na figura 5.1, o sistema é composto por quatro aplicações e uma base de dados, desenvolvidos para esta tese. A Firewall será um serviço adicional à solução implementada, mas muito importante para o bom funcionamento deste sistema distribuído. Mais detalhadamente o sistema é composto por uma aplicação "Anunciador", fornece um serviço que será explicado mais à frente. Temos também o "HomeStation", é a aplicação para os pacientes utilizarem em casa, onde se faz exames e automaticamente envia dados para os respectivos repositórios ou serviços de

telemedicina. Uma terceira aplicação é o serviço de telemedicina em si, um servidor que quando recebe um pedido de comunicação do HomeStation executa uma série de operações para receber e enviar dados dos pacientes. Todos estes dados tratados no serviço de telemedicina são guardados numa base de dados para posteriormente serem consultados. A ultima aplicação desenvolvida é o "SaudeGest", um software que tem muitas funcionalidades, desde configurar o serviço telemedicina, criar credenciais, gerir pacientes, gerir utilizadores e consultar a informação armazenada na base de dados. Para o desenvolvimento de todo o software apresentado nesta tese foi utilizado a linguagem Java e o IDE de desenvolvimento foi o NetBeans IDE 6.9.1 [19] . O sistema de gestão de base de dados é o Mysql 5.5 [20] . Para a segurança foi utilizado a plataforma de desenvolvimento do Bouncy Castle Crypto [21].

5.3 Protocolo de Comunicação

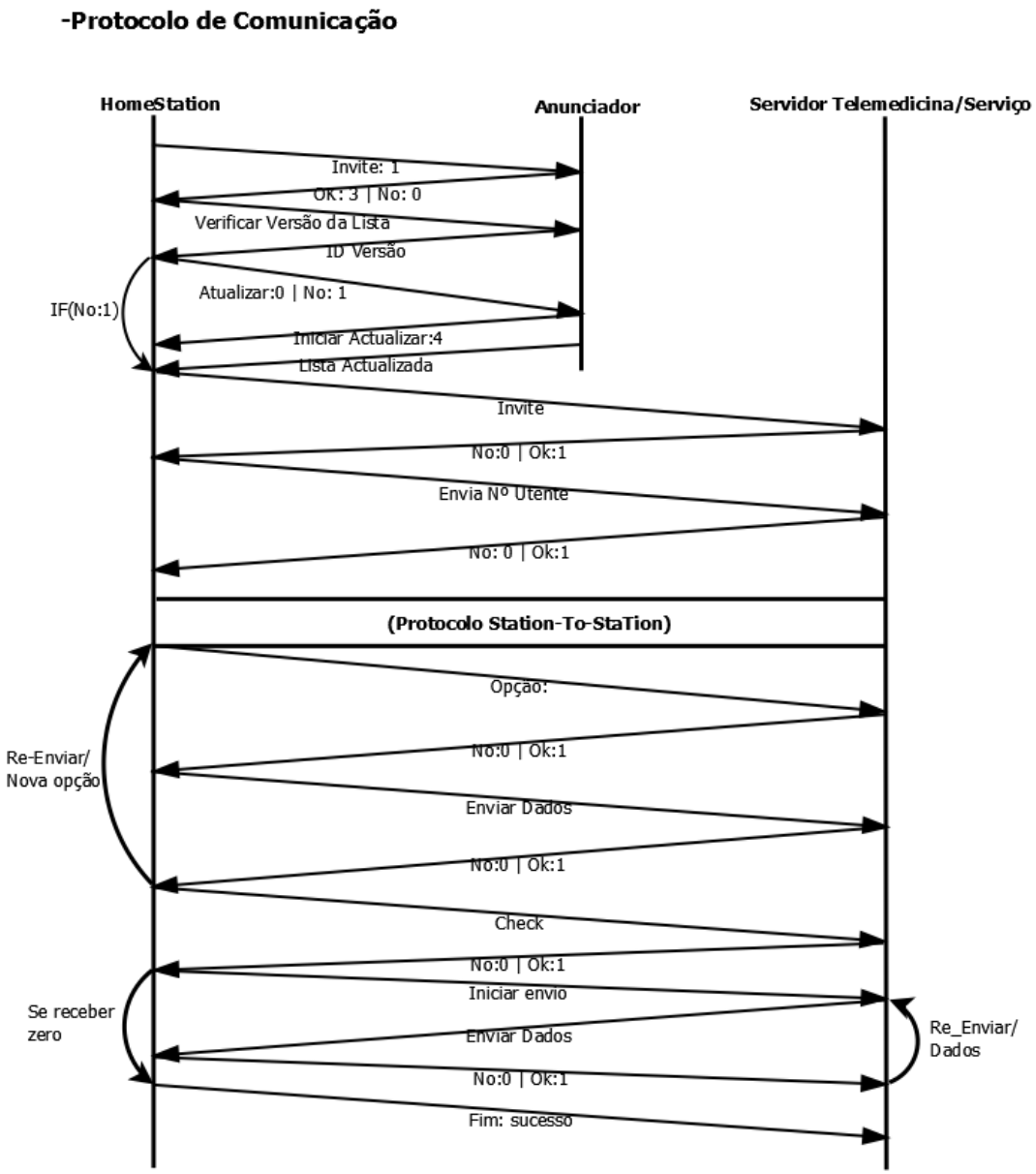

Figura 5.2: Protocolo De comunicação

O protocolo de comunicação (ver figura 5.2)começa por a aplicação HomeStation (HS) enviar um convite para comunicar ao Anunciador e este responde com valor zero se estiver em sobrecarga ou o IP em questão estiver banido temporariamente. De seguida a aplicação HS envia um pedido ao Anunciador para enviar o ID (identificação da versão atual) da versão atual, o HS verifica se precisa de atualizar, caso precise envia zero senão envia um. Se for preciso atualizar o Anunciador responde que vai enviar

dados e enviar a lista atualizada, senão o HS simplesmente termina a ligação e conecta ao Serviço de Telemedicina (ST). A comunicação com ST começa por receber um convite do HS, responde com zero se o serviço estiver no seu limite máximo de capacidade e a ligação é terminada, caso contrário envia um, dizendo ao HS que está disponível para comunicar. De seguida o HS envia o número de utente do utilizador predefinido, o ST recebe e verifica se é um número válido e responde com zero caso seja falso e termina a comunicação, ou com um se o número for encontrado na base de dados e não estiver suspenso por outros motivos. Uma vez que o ST tenha o suposto numero do utente é iniciado o protocolo STS (Station-To-Station) explicitado no capítulo 3. Se o protocolo STS concluir com sucesso o utilizador está autenticado e o canal cifrado, e HS envia um número correspondente ao tipo de dados que vai enviar (ex. numero um para "Dados da Tensão"). De seguida o ST responde com zero caso seja impossível receber esses dados, isto porque pode haver a possibilidade de o ST não ter o serviço pedido disponível, caso resposta seja um o HS envia um conjunto de dados. O ST responde com zero caso tenha recebido dados corruptos ou responde com um caso tenha sido um sucesso a comunicação e fica à espera de receber mais pedidos. Caso o ST receba um pedido para receber mais dados o processo de envio explicado anteriormente é repetido. Quando o HS não tiver mais dados médicos para enviar, passa para uma nova etapa e envia um pedido ao ST para saber se há mensagens para receber. Caso HS receba zero(Não há mensagens para enviar) avança no protocolo e envia uma mensagem ao ST para finalizar a comunicação com sucesso. Caso HS receba um, envia uma mensagem ao ST para iniciar o envio dos dados e assim fazem a transferência das mensagens e para finalizar envia mensagem de fim e acaba a comunicação com sucesso.

5.4 Anunciador

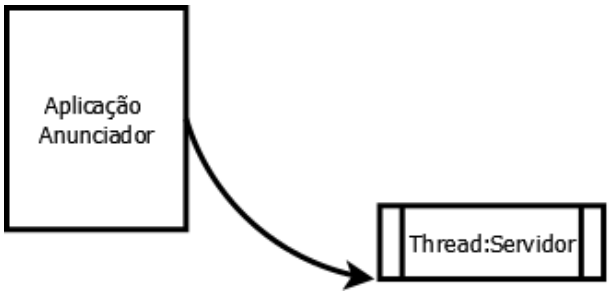

Figura 5.3: Anunciador cria um novo processo servidor

O Anunciador (ver figura 5.3) é uma aplicação/serviço em que a ideia é baseada nas redes peer-to-peer, um componente chamado "Announcer"[22]. A ideia da construção deste serviço surgiu da necessidade de saber automaticamente que serviços de telemedicina estão disponíveis para contactar na internet. Isto para saber informação relevante sobre os serviços de telemedicina, como o Nome, ID (Número de identificação) e o mais importante IP. A ideia centra-se no princípio de que o utilizador que está em casa, não tem grandes conhecimentos informáticos, logo não sabe o que é um IP nem o que fazer com ele e tem grande dificuldades em configurar a aplicação que vai utilizar. Logo há uma necessidade de ter este serviço com uma lista de todos os serviços de telemedicina, para que os utilizadores da aplicação HomeStation recebam esta lista atualizada e toda a informação associada automaticamente. Em casa o utilizador apenas precisa de escolher a entidade que pretende ligar-se através do nome ou ID. Uma segunda potencialidade deste sistema é, aplicações de outras marcas poderem implementar o protocolo deste sistema, ou seja qualquer equipamento que siga o protocolo explicitado anteriormente poderá comunicar com o sistema e utilizar os seus serviços. Uma terceira potencialidade é por exemplo: o caso em que efetuamos análises numa clínica e esta enviou o objecto em análise para um laboratório. Ao fim de alguns dias pretendemos receber os resultados e para isso basta ter previamente as credenciais do laboratório e utilizar o Anunciador para encontrar a laboratório que pretendemos para descarregar as análises ou saber se ainda está pendente. No entanto, para esta tese só foi testado o processo de um utilizador comunicar com uma entidade de saúde que tem o serviço de tensão arterial ativado, mas como podemos ver o Anunciador e todo o protocolo associado tem muita potencialidade para ser explorado de várias formas, integrar vários serviços e equipamentos.

5.4.1 Explicação e Manual de Utilizador

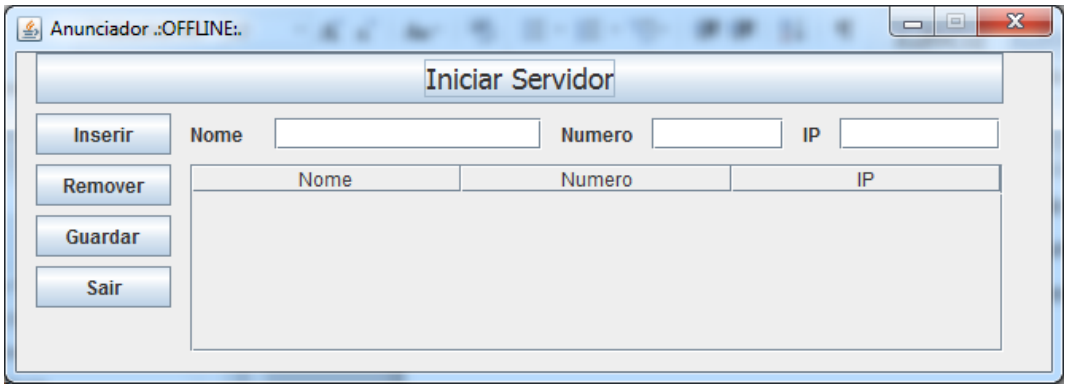

Figura 5.4: Estado inicial do Anunciador

Na figura 5.4, podemos observar a janela principal do "Anunciador"e o seu estado após arranque da aplicação. De seguida vamos explicitar todas as funcionalidades desta aplicação. Para arrancar o serviço é preciso pressionar o botão "Iniciar Servidor"e neste momento é criado uma Thread servidor que ficara encarregue de tratar toda a informação com o exterior (ver figura:5.3).

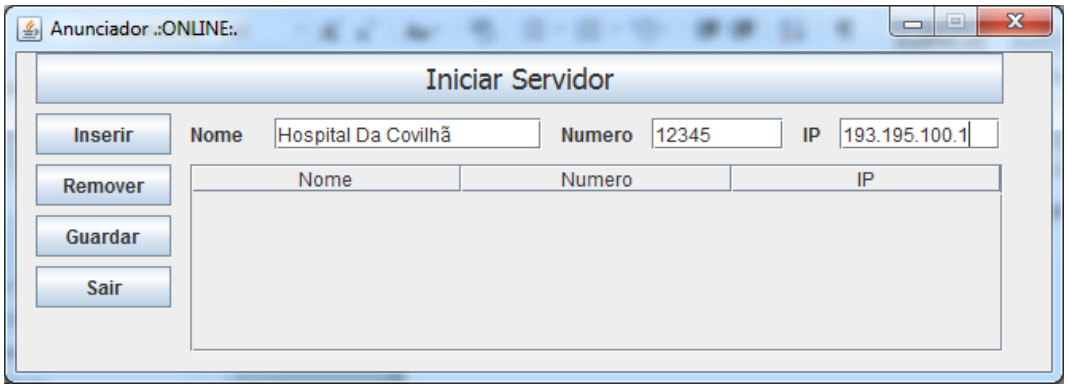

Figura 5.5: Inserir Entidade

Para inserir uma nova entidade/serviço de telemedicina, é preciso preencher os campos como podemos ver na figura 5.5 e de seguida pressionar no botão "Inserir". O campo "Nome"corresponde ao nome da entidade, o campo "Numero"é o identificador único da entidade e o campo IP é o endereço de internet da entidade/serviço. A nova entidade é adicionada à lista do servidor como se pode ver na figura 5.6 e para ficar gravado definitivamente é preciso pressionar o botão "Guardar". Após guardar,

o número de versão é atualizado e todos os utilizadores da aplicação HomeStation receberam automaticamente a nova lista, basta ligaram as suas aplicações.

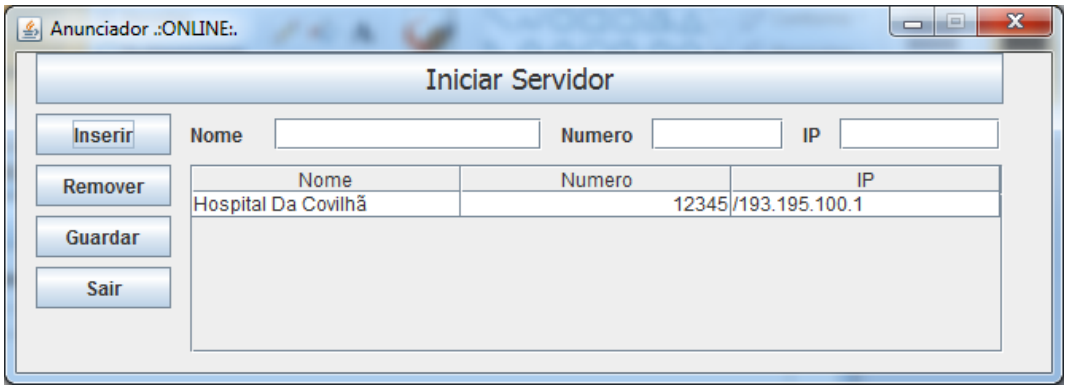

Figura 5.6: Exemplo de entidade inserida

Para terminar a aplicação basta pressionar o botão "Sair"ou pressionar o botão "X".

5.5 Servidor Telemedicina/Serviço

O servidor de telemedicina é uma aplicação que trata todas as comunicações e pedidos com os utilizadores que pretendem ligar e utilizar este serviço. No entanto o servidor nunca sabe quem são os utentes antes de se autenticarem, mas os utentes sabem quem é o servidor através do "Anunciador", contudo só tem a certeza depois de completar a autenticação. Para esta tese apenas existe um tipo de utilizadores, os que tem a aplicação HomeStation e é fornecido apenas um serviço guardar informação relativa à tensão arterial numa base de dados interna e enviar avisos aos utilizadores. Os avisos podem lembranças para tomar medicamentos, data de consultas ou pedidos para se apresentar na entidade de saúde a que está ligado. Não existe padrão nas mensagens, pode ser enviado qualquer tipo de mensagem ao critério do profissional de saúde. Quando é feito um pedido de comunicação, esta aplicação pede ao utilizador para se identificar e caso seja um utente válido o programa procura pelas suas credenciais e inicia todo um processo para cifrar a comunicação que já foi previamente explicitado. Todo este processo é feito automaticamente e cifrado sem precisar interação humana.

5.6 HomeStation

A aplicação HomeStation é o software que os utentes/pacientes irão utilizar em casa para conectar os seus dispositivos e realizar exames médicos, bem como para submeter automaticamente esses exames para o serviço de telemedicina predefinido. Esta aplicação está projetada para ligar quatro dispositivos diferentes para quatro exames distintos tais como:

- Medidor Tensão Arterial
- ECG- Electrocardiograma
- Oxímetro
- Balança

No entanto só foi possível ter disponível o medidor de tensão arterial, mas para testar o sistema é o suficiente, visto que o cerne desta tese é criar o sistema em si capaz de integrar vários tipos de serviços, aplicações e dispositivos diferentes.

Os algoritmos utilizados para medir a tensão arterial foram desenvolvidos pelo meu colega Fábio Campos [23] para a sua tese de mestrado e todo o processo de medição, interface aplicacional para o medidor foi feito por si.

Como já foi explicitado anteriormente esta aplicação obedece a um protocolo para comunicar com o serviço de telemedicina. Contudo no desenvolvimento desta aplicação foi tido em conta vários aspectos tais como:

- Interface adaptado para ecrãs tácteis
- Interface o mais básico possível
- Numero muito reduzido de operações que o utilizador tem de efetuar
- A configuração ser o mais simples possível
- Mostrar o essencial

Isto porque o software funcionará num "Tablet Pc"ou em algo muito idêntico, como portáteis com monitores tacteis. Estes aspectos expostos anteriormente trazem alguns

custos, o sistema fica menos personalizável, foi necessário criar um serviço extra "Anunciador"previamente explicitado e desenvolver mecanismo de automação para comunicar com o serviço de telemedicina automaticamente. A automação foi conseguida através de vários mecanismos que verificam se a configuração da aplicação foi concluída, e caso seja verdade a aplicação Homestation lança um processo adicional chamado de "ThreadCerebro"que vai tratar de comunicar automaticamente com o serviço de telemedicina. Este processo quando arranca fica adormecido por cinco minutos e depois começa a trabalhar, verificando se há dados para enviar e mesmo que não haja ele liga-se ao serviço para ver se há alguma coisa para receber (ex. avisos ou datas de consultas). Quando não há mais trabalho a realizar o processo volta adormecer por um período de cinco minutos. Este valor pode ser personalizado e o tempo que escolhemos para o processo ficar adormecido foi escolhido ao acaso, isto porque seria necessário realizar testes de stress e chegar a um consenso sobre o tempo ideal. Os exames efetuados são guardados numa pasta predefinida na raiz do programa com o nome "data". Quando a processo "ThreadCerebro"acorda vai procurar na pasta predefinida ficheiros com a extensão ".hspa"para a tensão arterial, se encontrar um ou mais ficheiros vai abrir um a um e enviar toda a informação para o serviço de telemedicina e se tudo correr bem estes ficheiros são apagados. Uma das dificuldades na gestão destes ficheiros, foi nomear sempre com nomes diferentes o nos ficheiros criados, para não haver o caso de escrever por cima de outro ficheiro. A solução para este problema foi criar um nome para o ficheiro a partir da data atual, que é convertida para um valor em milissegundos e o ficheiro é nomeado com esse valor. Este valor é obtido pela conversão do tempo que passou desde 1 Janeiro de 1970 até à data atual para milissegundos. A ideia central da automatização é facilitar o processo de pós realização de exames de rotina e receber algum feedback da entidade que está a prestar o serviço (ex. dirija-se a uma entidade de saúde porque tem a tensão arterial com valores anormais).

Os exames são encaminhados automaticamente e de forma segura para a entidade predefinida e o paciente apenas precisa de perder alguns minutos realizar o exame e depois pode ir à sua vida sem ter de preocupar se os dados estão seguros ou de os enviar a uma entidade responsável por os mesmos. Ainda podemos acrescentar outras vantagens de os dados serem automaticamente enviados para o médico como:

- A entidade que recebe os dados pode fazer uma pré-triagem e avisar o médico se detetar alguma anormalidade.

- O médico depois de receber o aviso pode consultar o exame e caso seja grave contactar o paciente e pedir dirigir ao centro de saúde por telefone ou pelo sistema interno de avisos.
- Não há risco de perder exames.
- É criado um histórico do utente consistente.
- Possibilidade de consultar o histórico e ajudar o médico a tomar decisões.

5.6.1 Explicação e Manual de Utilizador

Aqui vamos explicitar todo o processo necessário fazer para configurar e utilizar esta aplicação.

5.6.1.1 Registo e Configuração

Antes de arrancar esta aplicação precisamos de efetuar o registo na entidade que nos vai fornecer o serviço de telemedicina, para obter as credenciais e ficheiros para autoconfiguração desta aplicação. Os ficheiros necessários são os seguintes:

- Certificado do serviço de telemedicina
- Certificado do Cliente
- Chave Privada do Cliente
- Ficheiro com instruções de configuração

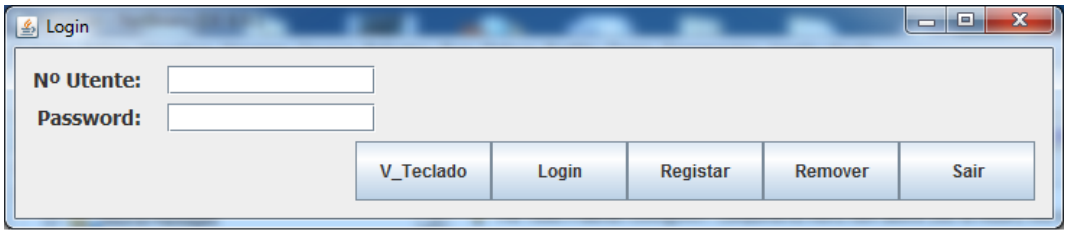

Figura 5.7: Janela de Login HomeStation

Assumindo que temos estes ficheiros podemos executar a aplicação HomeStation. Vai aparecer uma janela (ver figura:5.7), que nos permite registar, remover ou efetuar

identificação (Login). Como esta aplicação foi desenhada para idealmente funcionar com ecrãs tácteis, foi acrescentado a funcionalidade de abrir o teclado virtual como se pode ver o botão"V_ teclado", para ser possível efetuar login. No entanto se a ferramenta que estivermos a usar for um "Tablet Pc", esta funcionalidade deixa de fazer sentido. Contudo o abrir o teclado virtual do win7 (sistema operativo Windows 7) foi impossível, isto porque o sistema operativo tem um sistema que nos obriga a escalar as permissões para o fazer. Não foi possível encontrar uma solução para este problema, mas se o sistema operativo for o windowxp não há qualquer problema.

Tendo conhecimento do que foi explicitado, agora vamos registar um utilizador, para isso temos de pressionar o botão "Registar"que irá abrir uma janela como podemos ver na figura 5.8.

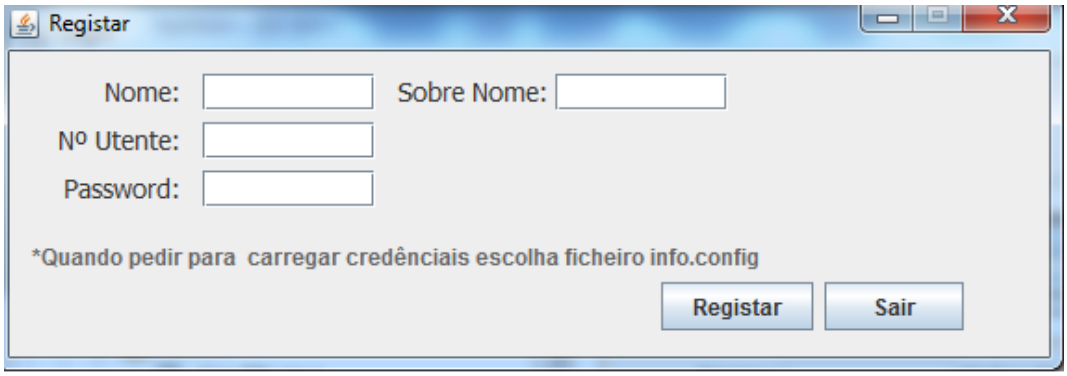

Figura 5.8: Janela de Registo Utilizador

O utilizador precisa de preencher os campos com os seus dados pessoais, escolher uma palavra-chave (Password) e utilizar o mesmo numero de utente que usou para se registar na entidade que lhe está a fornecer o serviço. Ao fim de preencher os campos o utilizador tem de pressionar o botão registar e ai irá abrir uma nova janela (ver figura: 5.9), que irá pedir o ficheiro de configuração automática fornecido pela entidade de saúde e os certificados.

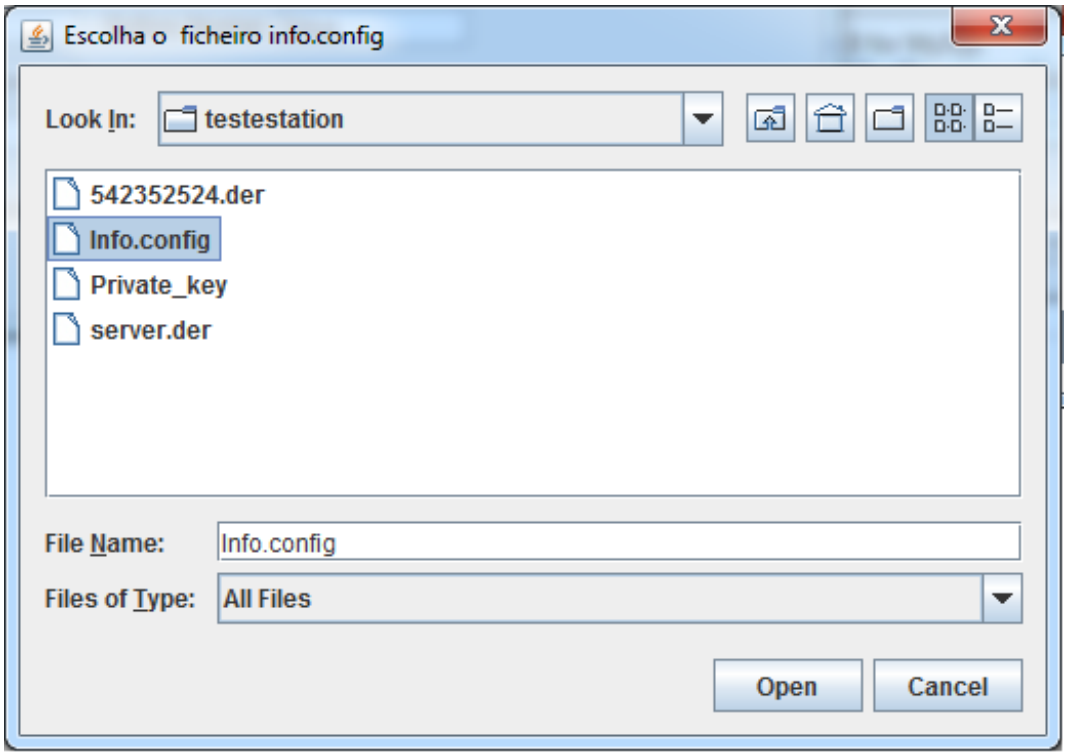

Figura 5.9: Selecionar ficheiro de configuração

No entanto basta escolher o ficheiro com o nome "info.config"e aplicação irá ler instruções escrita no ficheiro e proceder à correta configuração do software, se tudo correr bem vai aparecer uma janela de diálogo a dizer que foi um sucesso.

5.6.1.2 Remover Utilizador

Para remover um utilizador precisamos de estar na janela de autenticação (ver figura: 5.7) e pressionar o botão "Remover", que fará aparecer uma nova janela (ver figura: 5.10). Temos de selecionar o utilizador que queremos remover e pressionar o botão "Remover"para concluir a remoção.

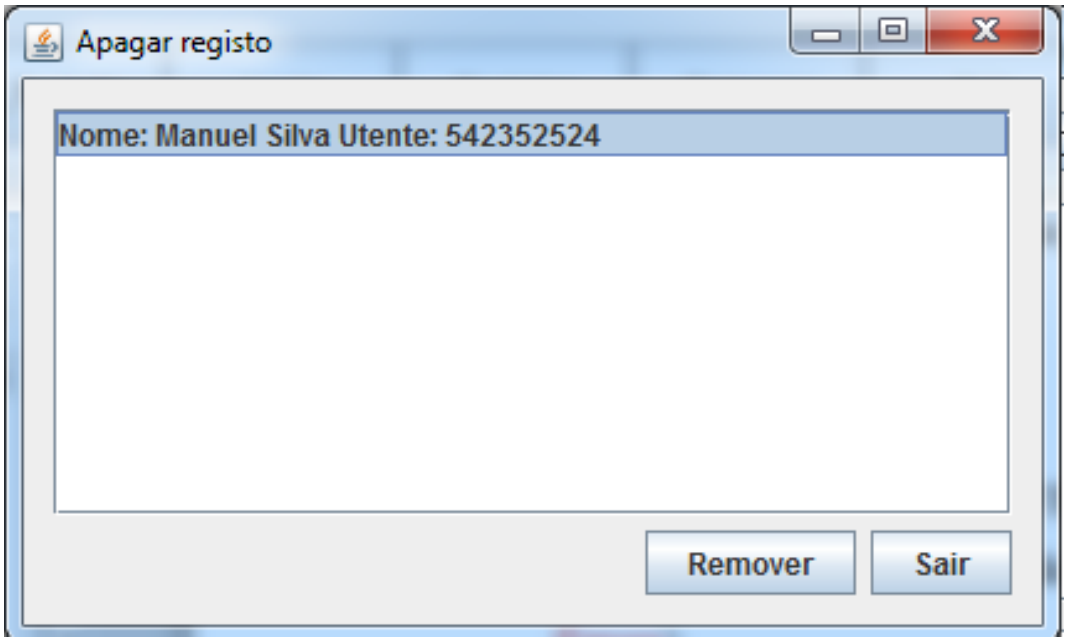

Figura 5.10: Janela para remover utilizador

5.6.1.3 Operar

Assumindo que todos os passos anteriores foram concluídos com sucesso, agora precisamos de efetuar autenticação com a conta criada. Se a autenticação for feita com sucesso, irá aparecer uma mensagem de diálogo a dizer que precisa de concluir a configuração, isto é, verificar se a entidade existe na lista fornecida pelo Anunciador e predefinir a entidade escolhida. Assim que a janela principal aparece, escolhemos visionar o painel de configuração (ver figura:5.11).

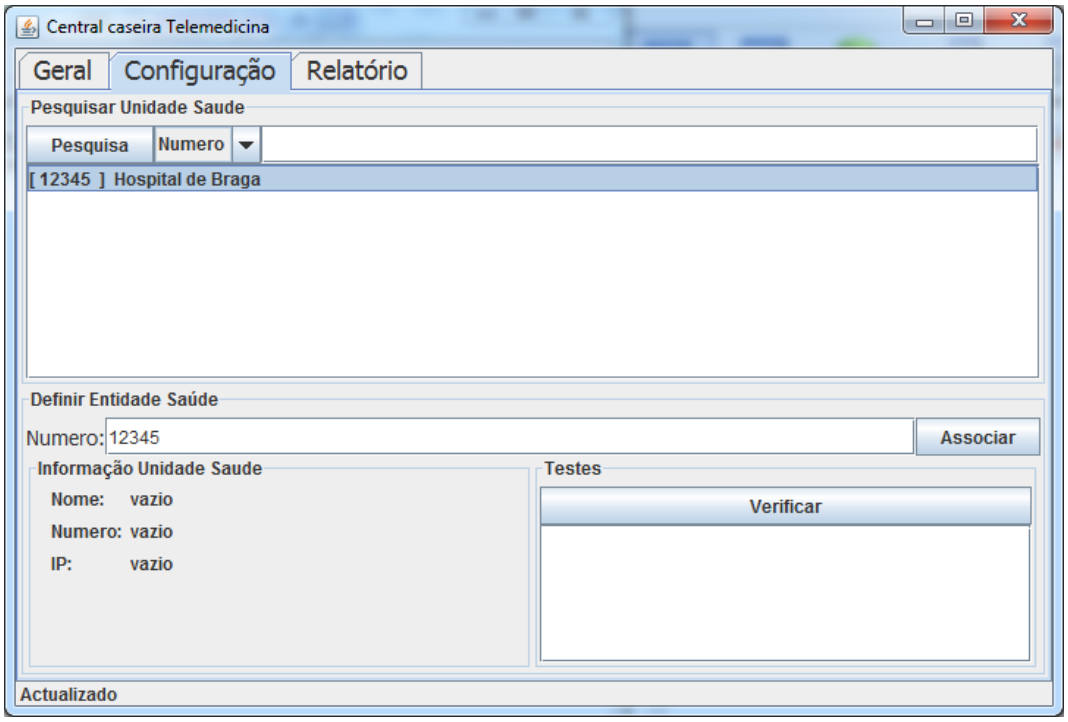

Figura 5.11: Janela de Configuração

A lista de serviços disponíveis é atualizada automaticamente através de um pedido ao Anunciador e depois basta selecionar ou pesquisar o serviço que desenhamos predefinir e pressionar o botão "Associar". Assim que seja definido o serviço o painel "Definir Entidade Sáude"irá mostrar informação relativa ao serviço que predefinimos. Temos um painel à direita para fazer um teste de disponibilidade do serviço, para isso temos de pressionar o botão "Verificar"e aparecerá na caixa de texto mais abaixo o resultado (ver figura: 5.12), como se pode observar o servidor está em baixo.

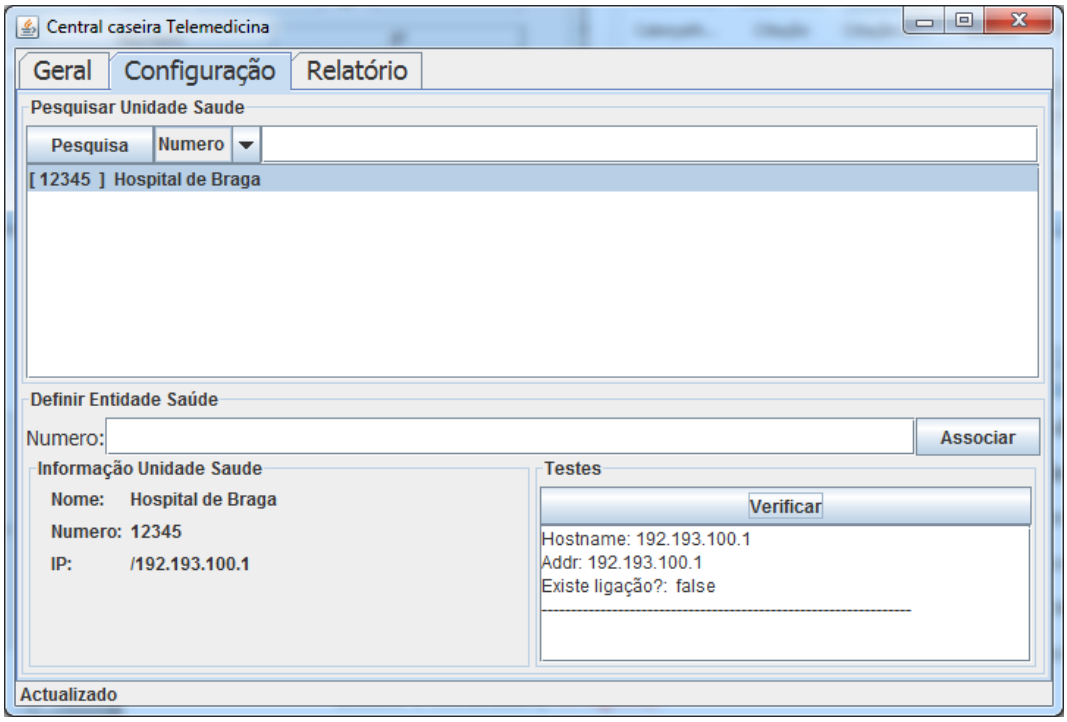

Figura 5.12: Janela de Configuração opção de teste

Mais à direita do painel de configuração temos o painel relatório, este mostrará se a aplicação está a conseguir conectar com o serviço e todos os problemas relevantes que podem acontecer (ver imagem:5.13).

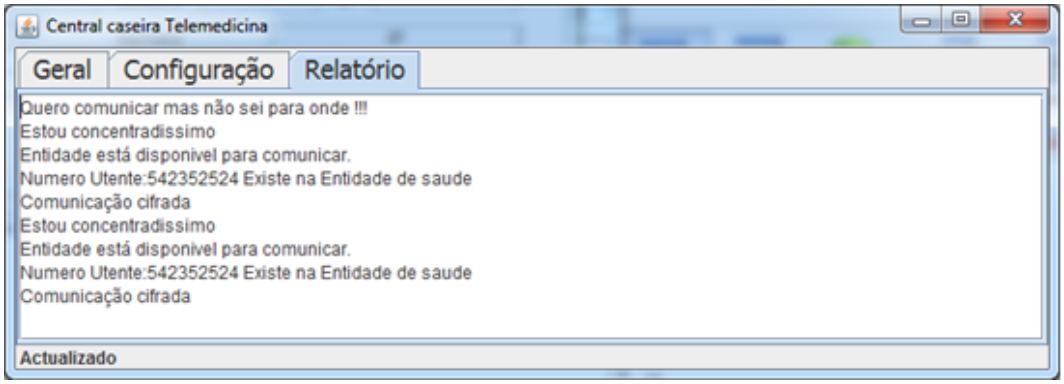

Figura 5.13: Janela de Relatório

Ao fim de todas as configurações serem concluídas a aplicação está pronta para realizar exames. Para iniciar o exame de tensão arterial pressionamos o botão "Tensão Arterial"e no painel inferior irá iniciar as funcionalidades para executar o exame (ver figura:5.14).

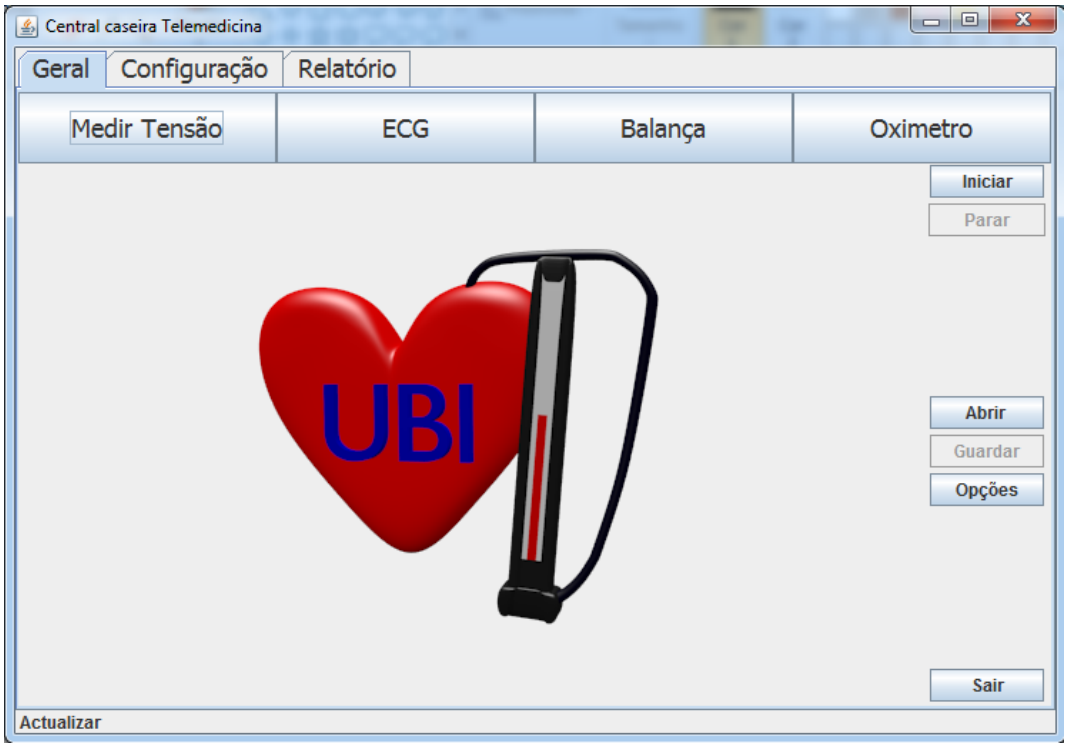

Figura 5.14: Janela de exame à tensão arterial

Agora o utilizador precisará de colocar a manga para medir a tensão arterial corretamente e pressionar o botão "Iniciar", para dar início ao exame e começar a recolher informação. Uma vez concluído a medição a aplicação mostra a informação recolhida (ver figura:5.15). Agora podemos descartar o exame pressionando o botão "Fechar"ou submeter o exame pressionando o botão "Guardar". Caso a opção escolhida seja guardar, será criado duas cópias, uma para o processo "ThreatCerebro"e outra cópia para o utilizador mais tarde poder consultar. A copia feita para o processo tem um tempo de vida pequeno, isto é, no máximo se tudo correr bem os dados serão enviados para o serviço de telemedicina e esta copia será eliminada. No entanto o ficheiro depositado para o processo anteriormente referido apenas contém três dados, pressão mínima, pressão máxima e pulsação por minuto.

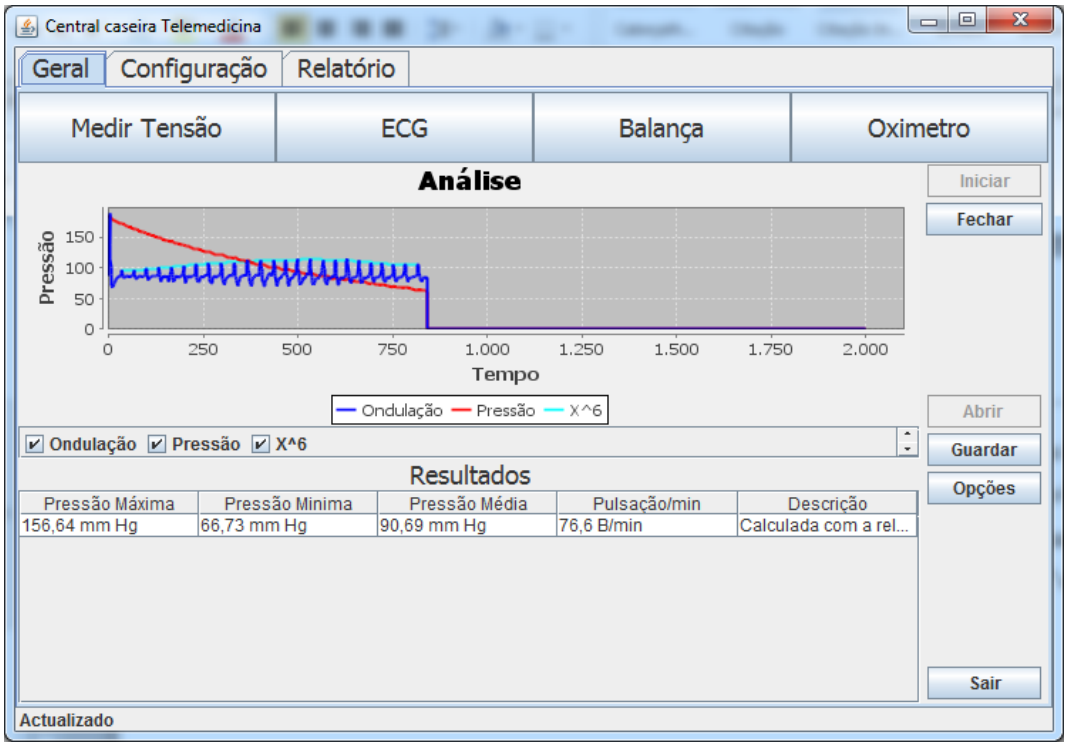

Figura 5.15: Informação do exame de tensão arterial

5.7 SaudeGest

A aplicação SaudeGest foi criada para gerir o serviço de telemedicina e emitir certificados. Esta aplicação vai gerir todos os utilizadores, utentes e permitir consultar toda a informação gerada pelos utentes e utilizadores. No entanto esta aplicação também funciona como uma Autoridade de Certificação. Consegue criar o certificado "root", isto é o certificado que vai assinar todos os certificados gerados para os utentes, mas não fornece o serviço de validação de certificados e revogação dos mesmos. Esta aplicação serve-se de uma base de dados, para guardar e consultar a informação. No entanto esta base de dados é partilhada também com o servidor de telemedicina, isto porque, é este servidor que faz todas as comunicações com o utente que está em casa e por sua vez recebe todos os dados referentes aos exames médicos efectuados.

5.7.1 Explicação e Manual de Utilizador

Quando se executa pela primeira vez o SaudeGest é iniciado um mecanismo para configurar de raíz a aplicação como se pode ver na figura 5.16.

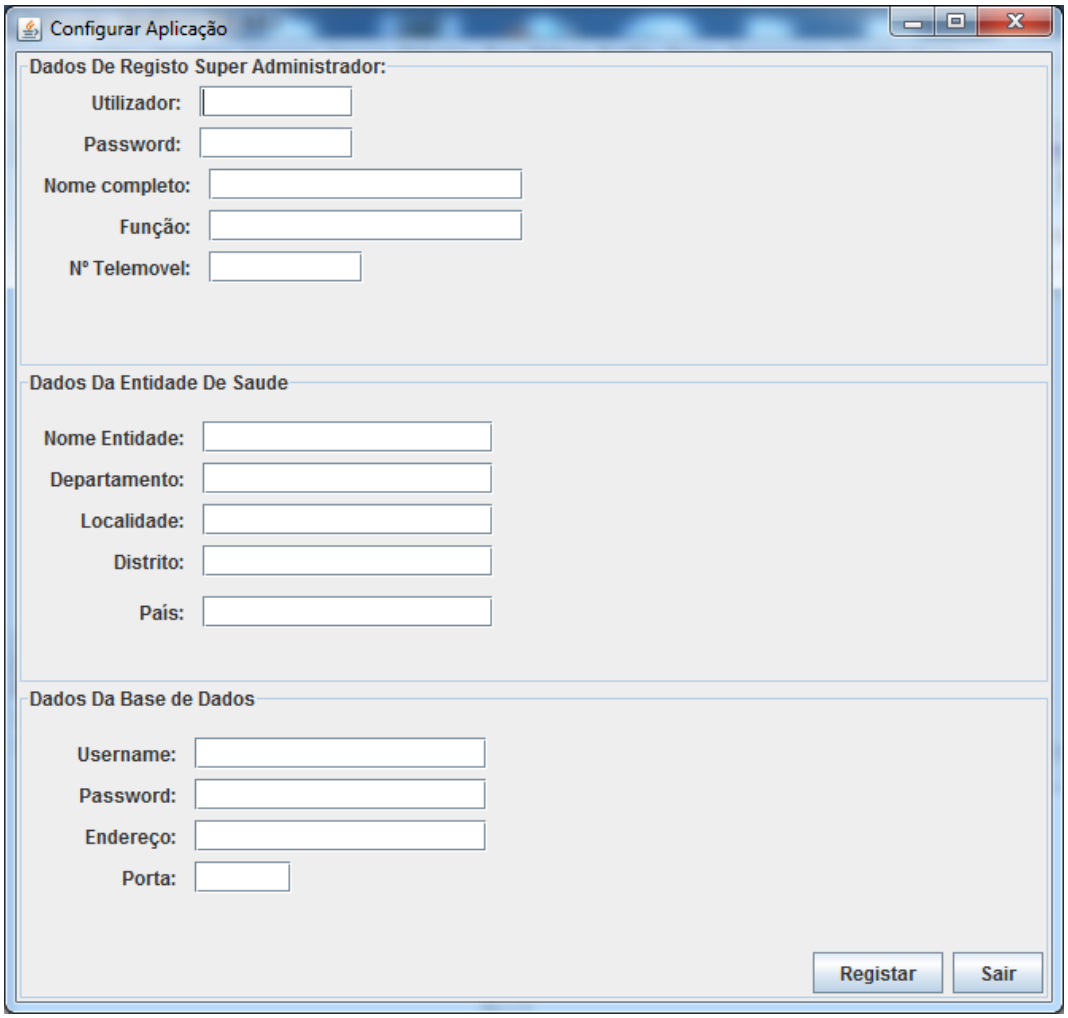

Figura 5.16: Primeira execução do SaudeGest

Onde diz "Dados De Registo Super Administrador", os cinco campos abaixo são para introduzir informação referente à pessoa que será o responsável máximo pela gestão do serviço de telemedicina. Os dados colocados no campo "Utilizador"e "Password", serão utilizados no processo de identificação (Login) para aceder à janela principal, os restantes campos é informação pessoal relativa a essa pessoa. Onde diz "Dados Da Entidade De Saude", temos cinco campos para preencher com informação relativa à entidade prestadora do serviço e estes dados serão utilizados para criar o certificado raíz do serviço.

Por ultimo onde diz "Dados Da Base De Dados", temos quatro campos que para preencher com informação relativa à base de dados que vai conter toda a informação do sistema. Um conjunto de dados exemplo para a configuração da aplicação pode se verificar na figura 5.17.

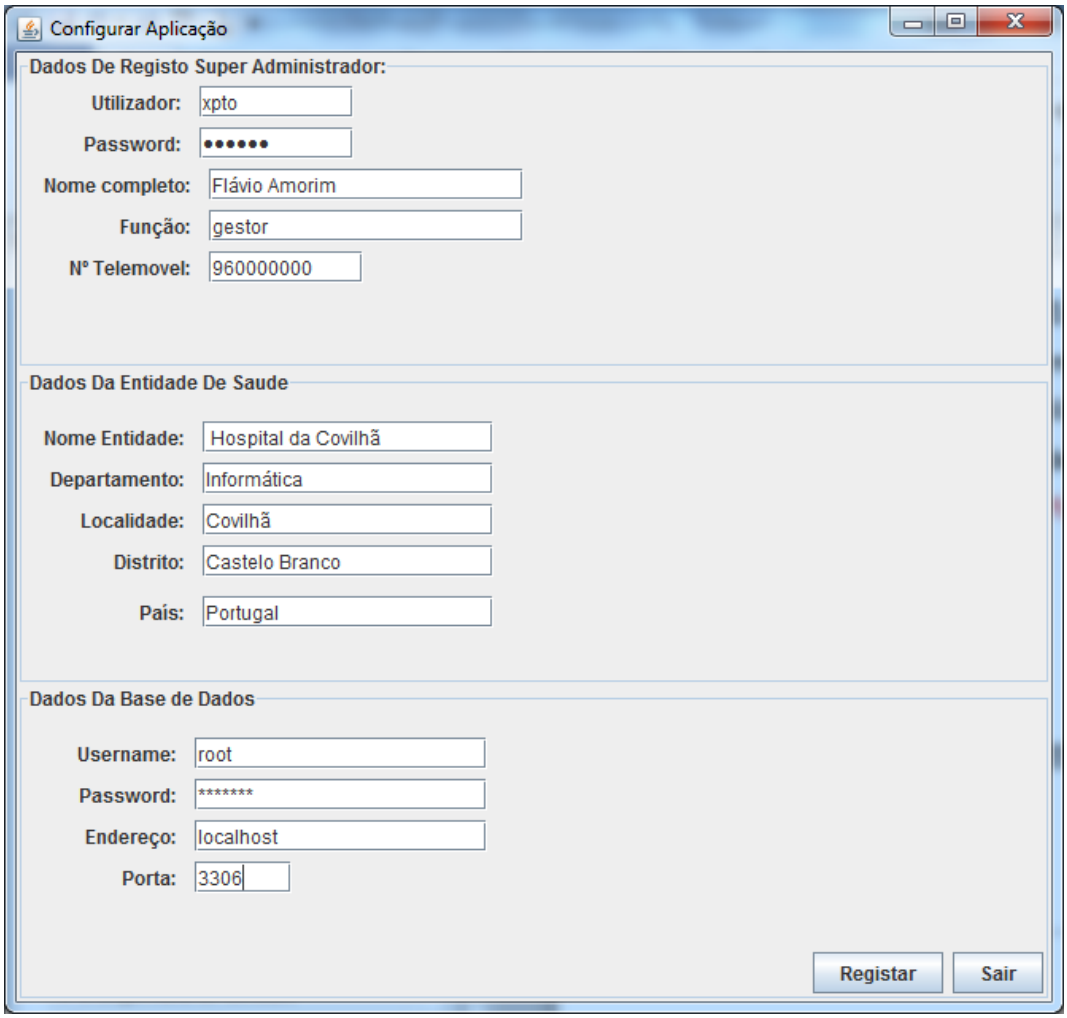

Figura 5.17: Exemplo de preenchimento dos campos

Assim que toda a informação esteja inserida, temos pressionar o botão "Registar", que irá despoletar uma série de mecanismos internos para configurar toda aplicação. Será também criado uma pasta na raíz do programa com o nome "CA", que contem a chave privada e a chave pública do serviço. É também criado uma pasta com o nome "Certificados", que contem o certificado raíz do servidor e também todos os certificados criados para os utentes. Se o registo concluir com sucesso aparecerá uma mensagem como se pode ver na figura 5.18, senão irá aparecer mensagens de erro que indicam

o que possivelmente está mal, como por exemplo campos vazios ou um número de telemóvel com menos de 9 dígitos ou problemas relativos com a base de dados.

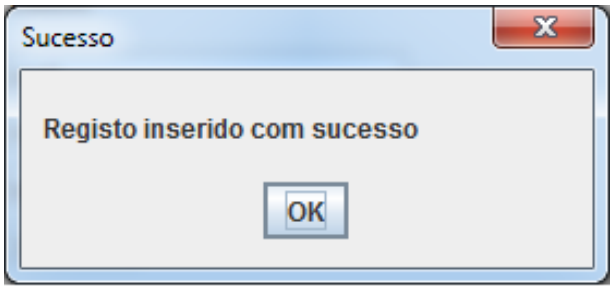

Figura 5.18: Mensagem de registo com sucesso

Agora temos a aplicação configurada, fechamos as janelas e procedemos ao "Login"como se pode ver na figura 5.19. Os dados inseridos nestes campos, são os que foram introduzidos no processo de configurar a aplicação mencionados acima e depois pressionamos o botão Login. Como já foi explicitado no capítulo de segurança 3 este processo de identificação tem alguns mecanismos de segurança.

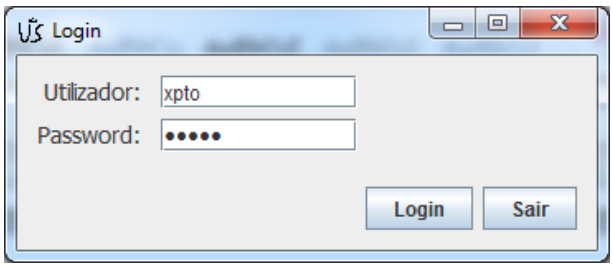

Figura 5.19: Janela de Login da entidade de saúde

Depois de efetuada a identificação aparece a seguinte janela (ver figura:5.20).

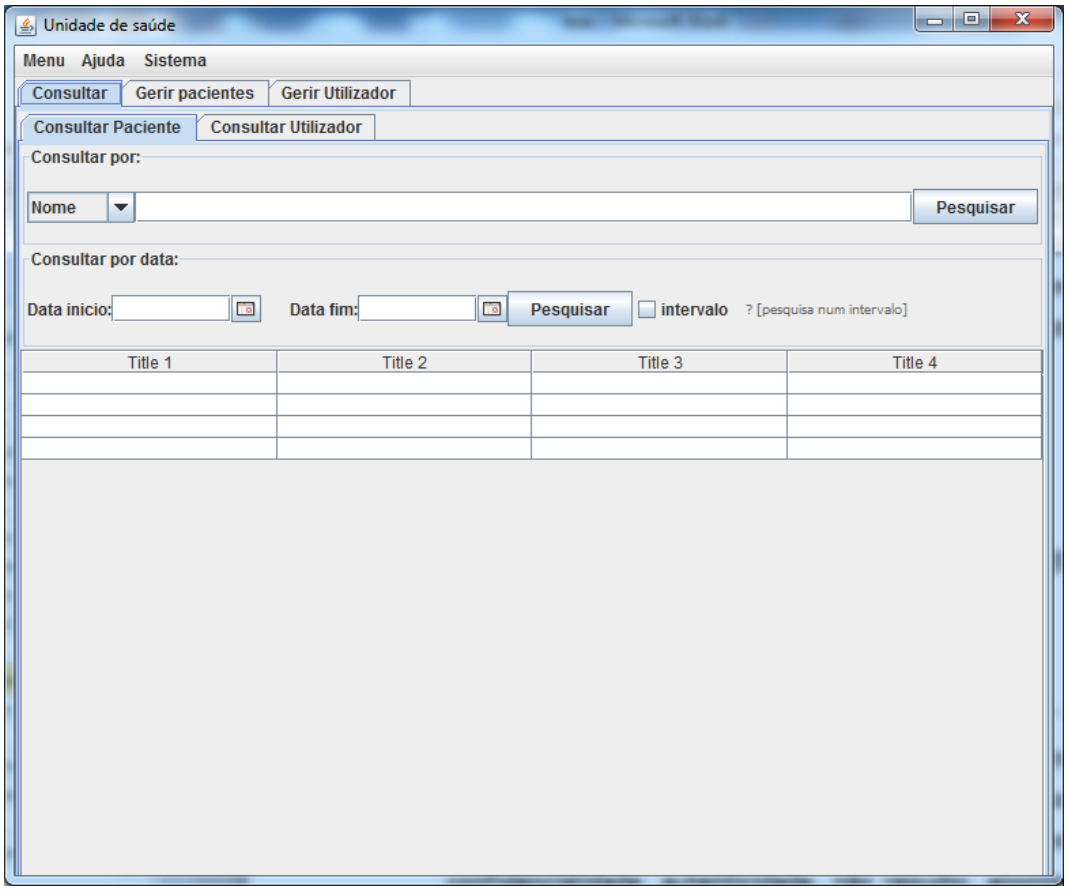

Figura 5.20: Janela principal do software SaudeGest

Como se pode ver na figura 5.20, temos três paneis principais tabulados , "Consultar", "Gerir Pacientes", "Gerir Utilizador"e estes contem cada um dois sub-painéis. No entanto quando um utilizador faz "Login"o numero de funcionalidades é reduzido, ou seja, o utilizador não pode registar/remover novos administradores ou utilizadores, logo o painel "Gerir Utilizador"fica invisível. Apenas o super administrador (Criado no processo de configuração da aplicação) pode criar o primeiro administrador. Após isto os novos administradores podem criar outros administradores ou utilizadores.

5.7.1.1 Gerir Utilizador

Vamos começar por explicitar o painel "Gerir Utilizador", que contem dois sub-painéis para registar e remover utilizadores. Para registar um utilizador, temos de preencher os campos que podemos ver na figura 5.21 , só existe dois tipos de utilizador o adminis-

trador e o utilizador normal. Assim que os campos estejam preenchidos, pressionamos o botão registar e se não houver um utilizador com o mesmo nome de "Utilizador"ou dados que o sistema considere errados, o registo é concluído com sucesso.

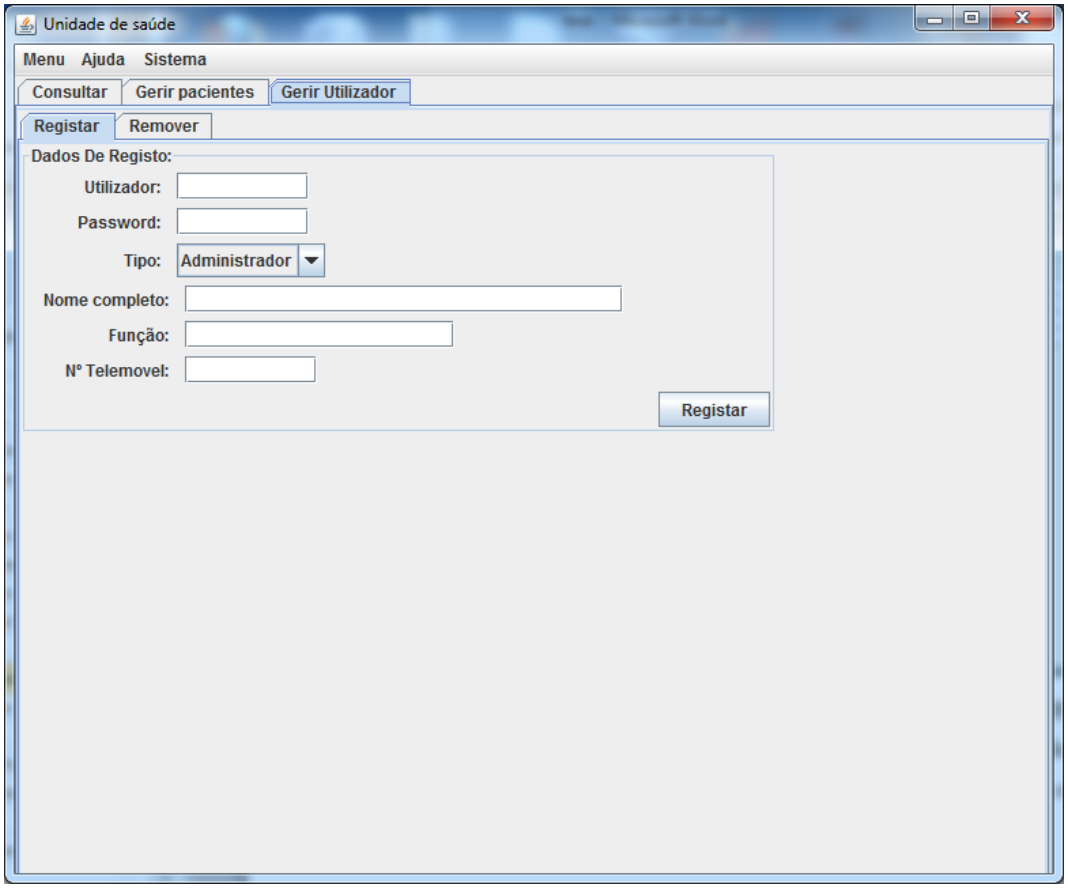

Figura 5.21: Janela registar utilizador

Para remover utilizador escolhemos o painel "Remover"(ver figura: 5.22) e no painel mais abaixo com o nome "Remover Utilizador", preenchemos o campo "Código de utilizador"com o código referente ao utilizador que desejamos apagar do sistema. No entanto podemos observar nessa figura que tem outro painel para remover um "Login", a ideia é um utilizador poder ter várias contas para efetuar "Login"como por exemplo uma conta de administrador e uma de utilizador normal sem ter de estar a introduzir novamente os seus dados pessoais. Contudo esta opção está inativa.

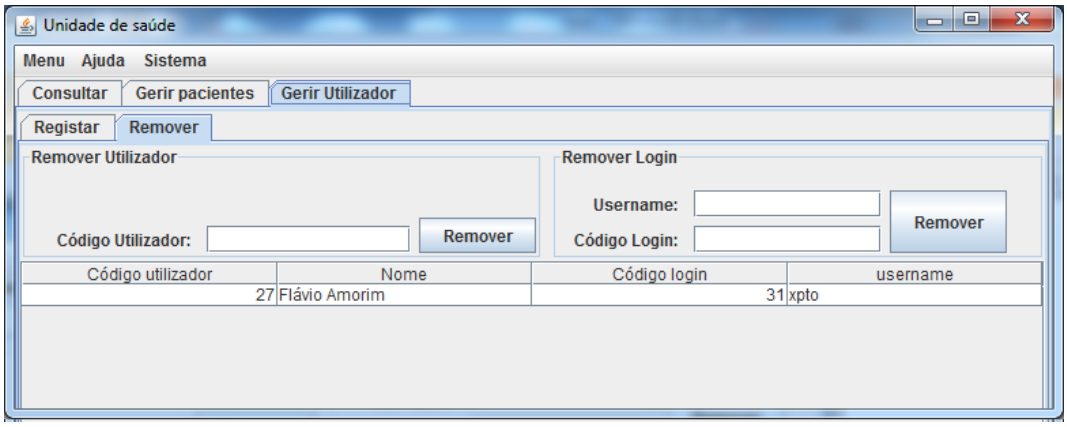

Figura 5.22: Janela remover Utilizador

5.7.1.2 Gerir Pacientes

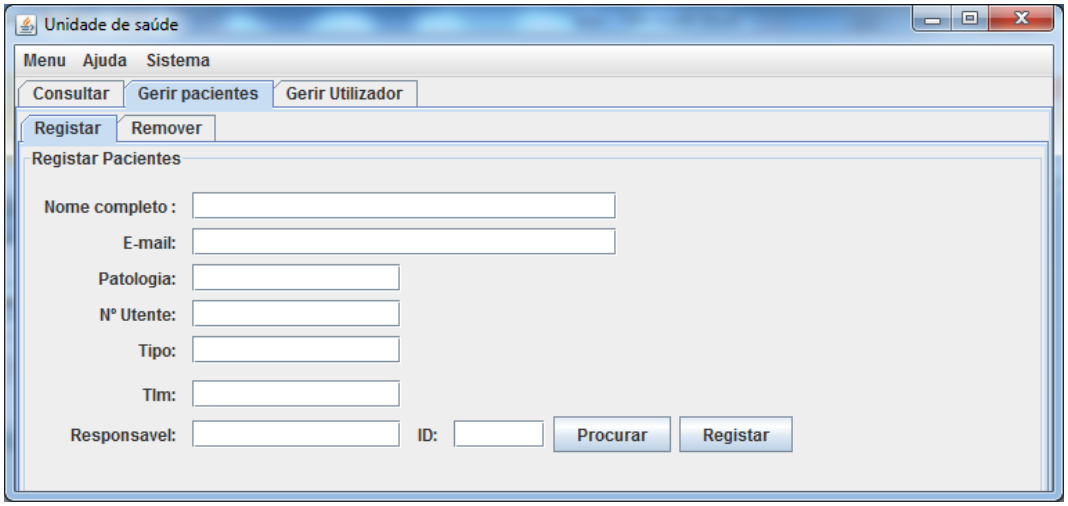

Figura 5.23: Janela gerir pacientes

Vamos começar por explicitar o processo de registar um paciente no sistema para que mais tarde e em casa o paciente possa usufruir do serviço de telemedicina. Como podemos ver na figura 5.23 do registo, temos de preencher os seis primeiros campos com informação referente ao utente, note-se que o número de utente é o que atualmente se usa no serviço nacional de saúde, logo o número é único e tem de ser fornecido pelo titular.

Para preencher o ultimo campo "Responsável", temos de pressionar o botão "Procurar", que por sua vez abrirá uma janela com todos os utilizadores registados na base de dados (ver figura:5.24). Está pessoa será a alguém que ficará responsável pelo paciente e possivelmente será um médico, isto porque só a eles interessa saber como está o doente.

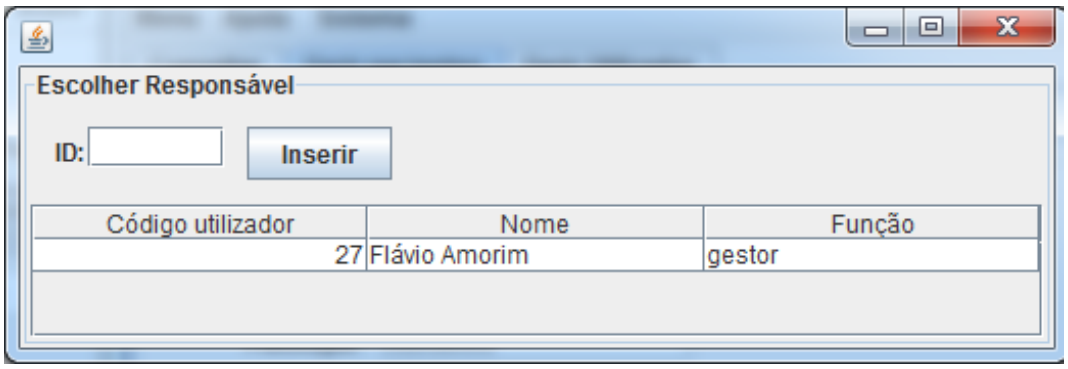

Figura 5.24: Janela procura responsável

Depois de os campos estarem preenchidos pressionamos o botão "Registar", que automaticamente valida todos os campos e verifica se o utente não foi previamente registado. Caso o utilizador seja registado com sucesso, será despoletado um processo para criar as credenciais do utilizador assinadas pela respectiva entidade e um ficheiro com informação de como a aplicação "HomeStation"deve se auto-configurar para este utente. Ao fim da validações anteriores abre-se uma janela (ver figura: 5.25) e depois escolhemos o local onde queremos gravar, que pode ser por exemplo uma "Pen disk". Estes dados gravados são fornecidos ao utente para conseguir registar em casa no sistema de telemedicina. Agora no local que escolhemos para guardar contem quatro ficheiros, a credencial da entidade de saúde, credencial do utente, chave privada do utente e o ficheiro de auto-configuração.

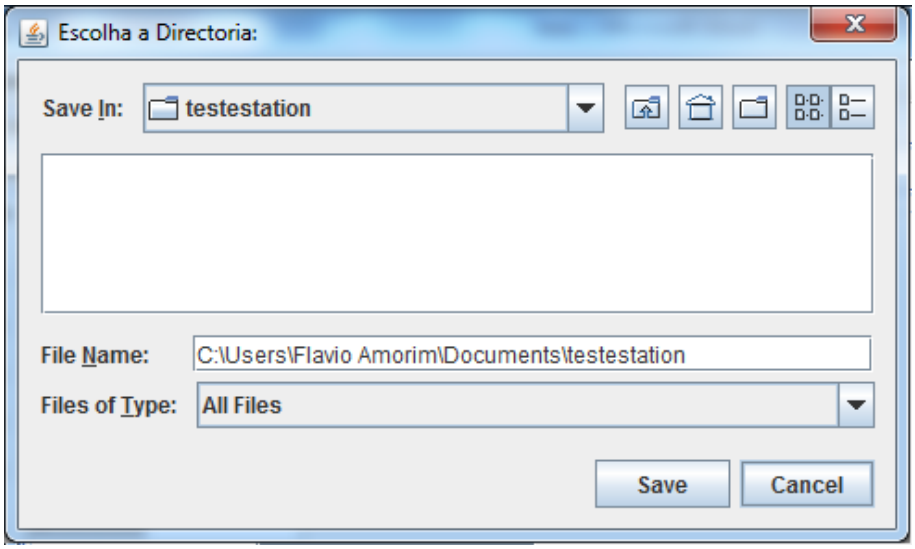

Figura 5.25: Guardar ficheiros

Para remover este paciente escolhemos o painel "Remover"(ver figura:5.26) e escrevemos no campo "N Utente"o respectivo número do utente e pressionamos o botão "Remover".

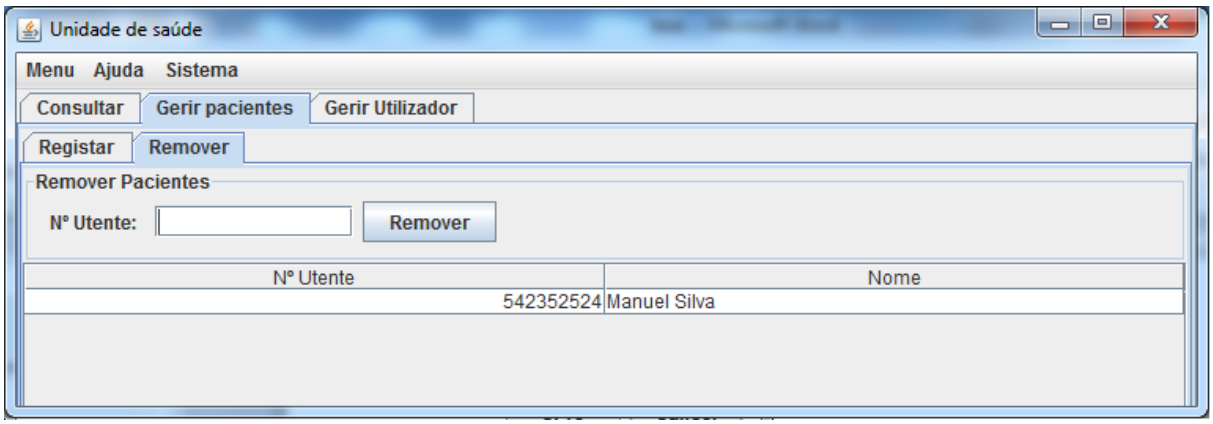

Figura 5.26: Remover utente

5.7.1.3 Consultar

No painel consultar podemos escolher dois sub-painéis, um para consultar informação acerca dos utilizadores e outro acerca dos utentes. No painel de consulta de utilizador (ver figura:5.27) é carregado automaticamente toda a informação relativa aos utilizadores da aplicação para uma tabela. Depois temos opções de pesquisa, como consultar por nome ou por um código único (ID) de utilizador.

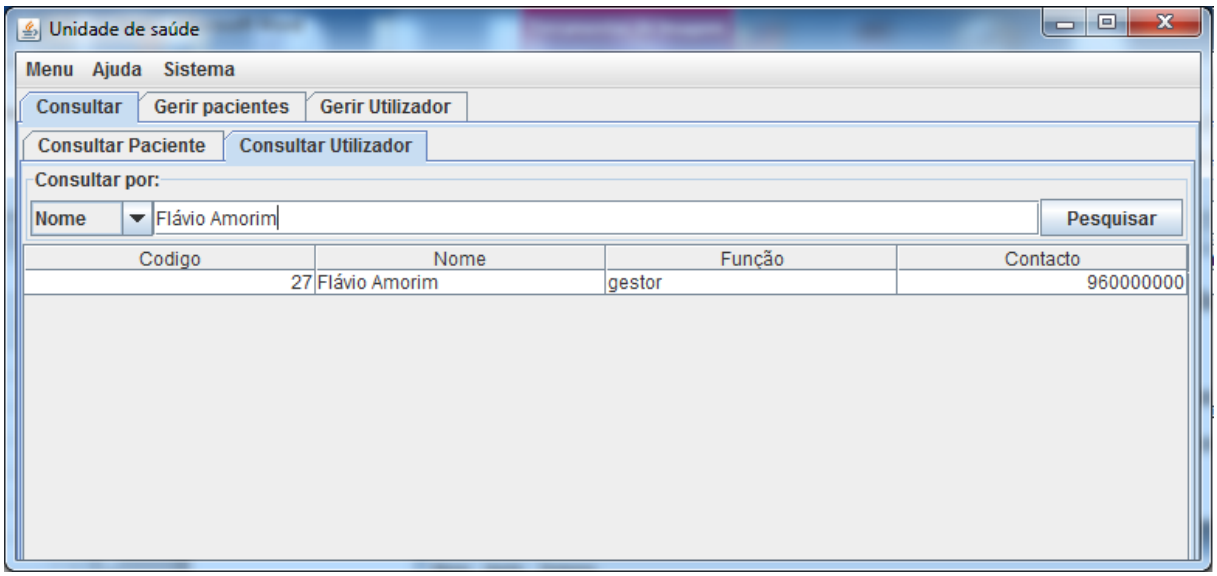

Figura 5.27: Consultar utilizador

Por último no painel consultar paciente (ver figura:5.28), podemos consultar informação relativa aos exames dos pacientes que foram depositados na base de dados através da sua aplicação HomeStation. No sub-painel "Consultar por:"podemos efetuar pesquisas aos dados dos pacientes, se simplesmente pressionarem o botão "Pesquisar", é mostrado todos os dados existentes na base de dados. Mas podemos aplicar filtros, temos uma "combobox"para escolher se pretendemos pesquisar por nome ou por número de utente e à frente colocamos dados referentes à escolha feita, de seguida temos outra "combobox"para escolhermos o tipo de exame (ex. tensão ou electrocardiograma). Como só temos exames à tensão arterial, só é possível escolher essa opção. Agora podemos pressionar o botão "Pesquisar"e a informação será filtrada com os filtros escolhidos anteriormente. Por último ainda podemos aplicar o filtro (ver figura:5.29) da data em que o exame foi realizado, no sub-painel "Consultar por data:", podemos utilizar este filtro de duas formas: se desejarmos pesquisar exames efetuados num dia à escolha, basta preencher o campo "Data inicio"e pressionar o botão "Pesquisa". Caso pretendam pesquisar exames num intervalo de datas, temos preencher o campo "Data Inicio", o campo "Data fim:"e clicar no visto "Intervalo", e pressionar o botão "Pesquisa"e o resultado será como se pode ver na figura.

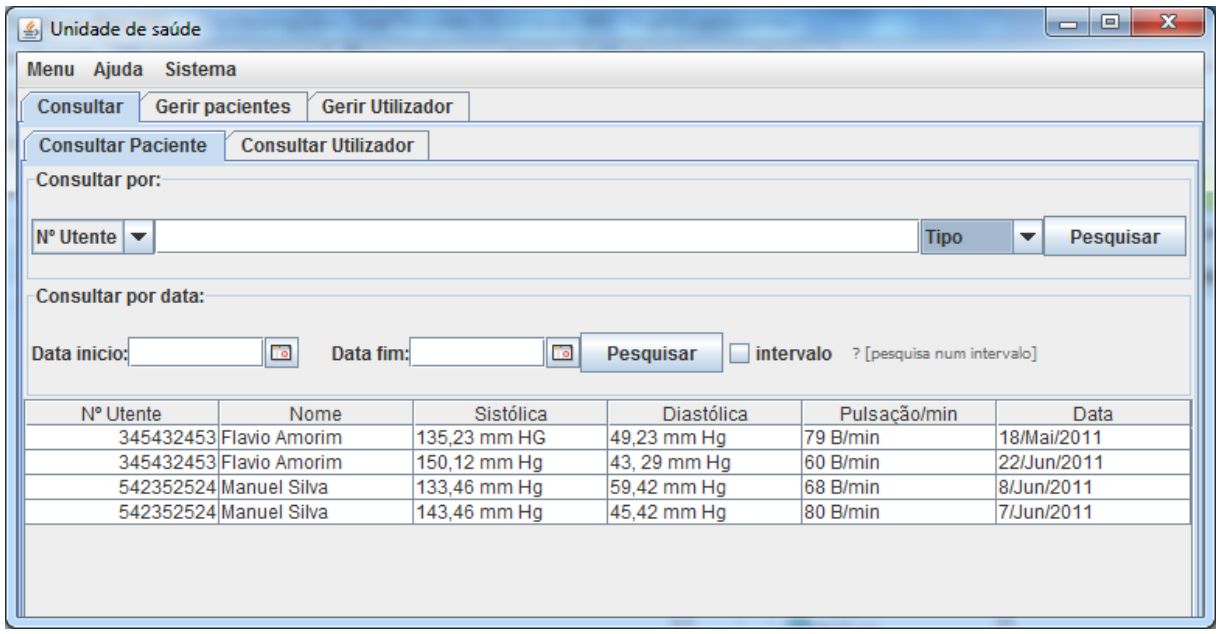

Figura 5.28: Consultar Paciente

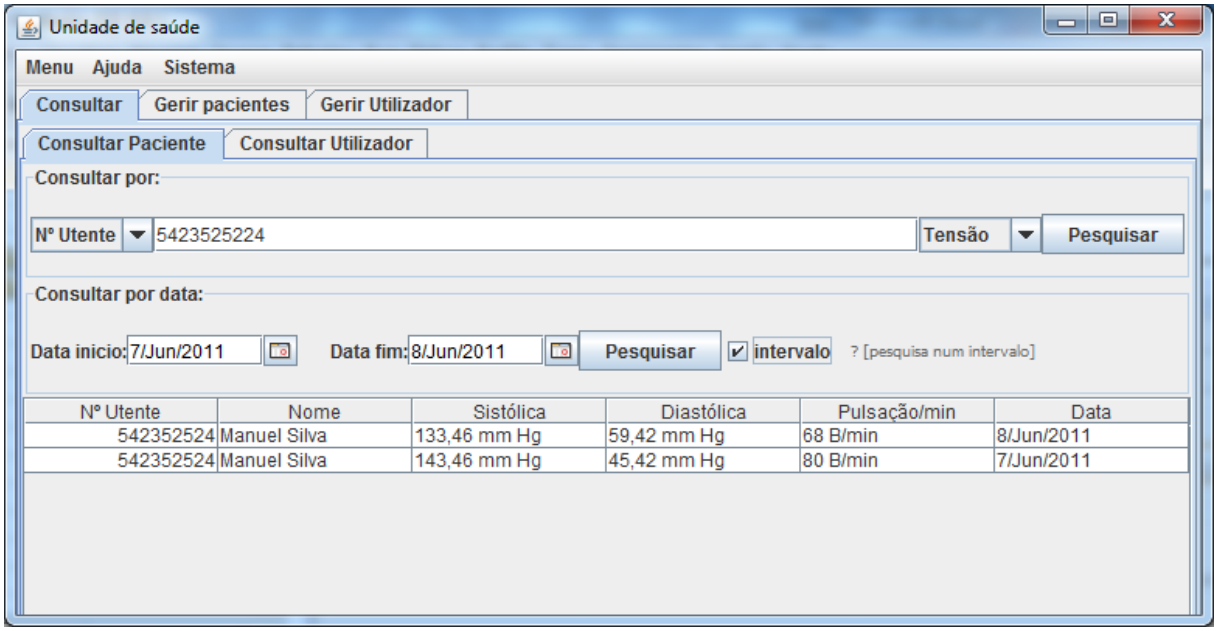

Figura 5.29: Consultar Paciente com filtros

Capítulo 6

Trabalho Futuro

Ao longo do desenvolvimento deste sistema foram surgindo sempre novas ideias e muitas não foram aplicadas porque seria preciso mudar grande parte da filosofia de funcionamento do sistema.

Algumas destas ideias seriam:

- O serviço prestado pela aplicação "Anunciador"deixa de ser necessário, porque os dados referentes aos serviços disponíveis passaram a ser disponibilizados pelo serviço de telemedicina.

- Alterar o processo de registo dos pacientes nas entidades de saúde para um sistema mais amigável para o utilizador. A ideia é aproveitar a funcionalidade Plug And Play de modo a que ao introduzir uma pen usb possa ser executado automaticamente um software de configuração. Este último terá as instruções necessárias para instalar a aplicação "HomeStation"e configurar todo o processo de ligação ao serviço de telemedicina. Desde definir automaticamente o IP do serviço, o certificado necessário para autenticação, que tipo de serviços pretende usufruir (ex. serviço de tensão arterial) e predefinições para o equipamento que pretende usar. Esta modificação remove qualquer necessidade de configuração por parte do paciente, apenas precisará de saber minimamente manusear a aplicação para realizar exames. Desta forma o paciente apenas precisará dirigir-se a uma entidade prestadora de serviços de saúde, criar um registo em que lhe é devolvido uma pen usb com todos os programas necessários para o serviço contratado. Após o processo explicitado anteriormente o utente precisará introduzir essa pen usb no computador e automaticamente fica apto para usufruir

do serviço sem precisar de fazer alguma configuração.

- Criar um canal bidirecional de voz sobre IP (Voip), para o profissional de saúde comunicar sem custo adicionais com o utente e dar pequenas instruções, conselhos ou prestar assistência.

- Ser possível entrar em videoconferência caso o paciente deseje ter um contato visual com o profissional de saúde, para que haja um contato visual entre os dois e um aumento da qualidade e empatia com o utente.

- Construir novos módulos de software para a aplicação HomeStation, de forma a que seja possível integrar a domótica na aplicação. A ideia é que possa ser possível receber mensagens ou chamadas voz sobre ip do serviço de telemedicina e apresentar automaticamente na televisão por exemplo ou encaminhar para um smarphone.

No entanto todo o sistema precisa de alguns ajustes no interface e correção de pequenas falhas. Numa etapa final seria necessário realizar testes de stress ao sistema, para definir padrões para a quantidade de utilizadores que pode estar ao mesmo tempo a usufruir do serviço de saúde, bem como tratar outras possíveis falhas de segurança tanto a nível protocolar como a nível aplicacional.

Capítulo 7

Conclusão

O sistema ficou a funcionar corretamente no seu todo, embora necessite de alguns ajustes no controlo e recuperação de erros.

A grande maioria das exceções foram devidamente tratadas, no entanto algumas delas podem não recuperar corretamente, isto porque aplicações como o SaudeGest têm uma grande complexidade. As funções mais complexas trabalham com inúmeras subfunções o que torna a tarefa de recuperação de erros um grande desafio.

Os mecanismos de segurança estão a funcionar corretamente. A utilização do protocolo "Station-to-Station"acrescenta características únicas ao sistema, como a confidencialidade, autenticidade, integridade e não repudio.

A importância dada à segurança eleva a confiança na utilização do sistema, tanto para o utilizador como para os fornecedores de serviços médicos.

Os mecanismos implementados para garantir a estabilidade e disponibilidade do sistema distribuído têm um papel importante no incremento da fiabilidade. No entanto não foram realizados testes de stress ao sistema, embora fossem validar e garantir que os mecanismos implementados são eficazes e acrescentam valor á solução implementada.

O interface desenvolvido na aplicação HomeStation está bastante amigável do utilizador, como o comprovam as opiniões de docentes especialistas e alunos da Universidade Da Beira Interior. Contudo, não foi possível dispor de um Tablet Pc para testar se a aplicação estava completamente funcional para ecrãs tácteis.

Bibliografia

[1] Merrell RC Doarn CR, Nicogossian AE. Applications of telemedicine in the united states space program. *TeleMed J*, 1998.

[2] Bakalar RS. Telemedicine in the u.s. navy - healthcare at the deckplates. *TeleMed J*, 1998.

[3] Tomkins G Gilbert GR Cramer TJ Lea RK Ehnes SG Zajtchuk R Calcagni DE, Clyburn CA. Operation joint endeavor in bosnia: telemedicine systems and case reports. *TeleMed J*, 1996.

[4] Merrell RC Doarn CR, Nicogossian AE. Applications of telemedicine in the united states space program. *TeleMed J*, 1998.

[5] UNIFESP 2003 120p Tese (Doutorado em Medicina). [4] Camelo F.D.1 Vieira R.A.C.2 Mauad E.C. 3 Carvalho A.L.4 Tsunoda A.T.5 Guerreiro J.H.F.T.6 Oliveira D.M.7 consultoria, São Paulo. UtilizaÇÃo da telemedicina em hospital oncolÓgico - sus. 2009.

[6] Gersak B. Gorjup V, Jazbec A. Transtelephonic transmission of electrocardiograms in slovenia. *TeleMed J*, 2000.

[7] NewCardio. Cardiobip. `http://www.newcardio.com/products-cardio-bip.php`.

[8] Gary Cornel Cay S. Horstmann. *Core Java 2 Volume II - Advanced Features*. Prentice Hall PTR, seventh editioneven edition, 2004.

[9] Yang-Seo Choi Jin-Tae Oh Jong-Soo Jang Jae-Cheol Ryou. Integrated ddos attack defense infrastructure for effective attack prevention. *IEEE*, 2010.

[10] DailyMail. How michael jackson's death shut down twitter, brought chaos to google... and 'killed off' jeff goldblum. http://www.dailymail.co.uk/sciencetech/article-1195651/, ,2009.

[11] Zhe Chen Shize Guo Rong Duan Sheng Wang. Security analysis on mutual authentication against man-in-the-middle att. *IEEE*, 2009.

[12] P.C. van Oorschot W. Diffie and M.J. Wiener. Authentication and authenticated key exchanges. 1992.

[13] P. Jones D. Eastlake. Us secure hash algorithm 1 (sha1). RFC 3174, Internet Engineering Task Force, September 2001.

[14] S. Chokhani W. Ford. Internet x.509 public key infrastructure, certificate policy and certification practices framework. RFC 2527, Internet Engineering Task Force, 1999.

[15] Isidro Vila Verde. *Criptografia Clássica*. Faculdade de Engenharia do Porto.

[16] Departamento de Informática da Universidade DA beira Interior. *Apontamentos de Engenharia de Software*.

[17] Uml® resource page. http://www.uml.org/.

[18] astah* professional - software design tool. http://astah.change-vision.com/en/product/astah-professional.html.

[19] Netbeans ide 6.9.1. http://netbeans.org/.

[20] Mysql 5.5. http://dev.mysql.com/downloads/mysql/.

[21] Bouncy castle crypto api. http://www.bouncycastle.org/java.html.

[22] Djamal Zeghlache Wassef Louati. Wide-area publish/subscribe service discovery - application to personal networks. 2007.

[23] Fábio Campos. Algomed: Algoritmos médicos. Master's thesis, Universidade da Beira Interior, Junho 2011.