



UNIVERSIDADE D COIMBRA

Projeto de Redes de Computadores

Etapa 3

António Dias - 2015232789

Pedro Ribeiro - 2011151425

Índice

1. Informação Geral
 - 1.1. Introdução
 - 1.2. Arquitetura
 - 1.3. Objetivo
 2. Coordenação
 - 2.1. Gestão de equipa
 3. Descrição do Projeto
 - 3.1. Autenticação de credenciais
 - 3.2. Criação de Contas
 - 3.3. Aplicação Central (AC)
 - 3.4. Aplicação para o Profissional de Saúde (APS)
 - 3.5. Aplicação para o Agente de Segurança (AAS)
 - 3.6. Aplicação para o Gestor de Sistemas (AGS)
 - 3.7. Botão de Alarme
 - 3.8. Design e *mockup*
 4. Testes de software
 - 4.1. Aplicação Central
 - 4.1.1. Credenciais de utilizadores
 - 4.1.2. Ocorrências
 - 4.2. Página inicial
 - 4.2.1. Opção de *login*
 - 4.3. Aplicação do Administrador do Sistema
 - 4.3.1. Autorização e gerenciamento de contas
-

NOME DA EMPRESA

- 4.4. Aplicação do Profissional de Saúde
 - 4.4.1. Registo de Ocorrências
 - 4.4.2. Alteração de conta
 - 4.4.3. Eliminação de conta
 - 4.5. Aplicação do Agente de Segurança
 - 4.5.1. Consulta do registo de ocorrências
 - 4.5.2. Alteração de conta
 - 4.5.3. Eliminação de conta
 - 4.6. Conclusão
5. Estado da arte
-

1. INFORMAÇÃO GERAL

1.1. Introdução

No âmbito da unidade curricular Redes de Computadores (RC) do Mestrado Integrado em Engenharia Eletrotécnica e de Computadores (MIEEC) da Universidade de Coimbra (UC), surge a necessidade de se desenvolver uma aplicação móvel que tem como objetivo criar mecanismos de prevenção, diagnóstico e intervenção em casos de violência nos serviços de saúde.

Para isto, foi proposto aos alunos que desenvolvessem um sistema de registo, de alerta, de prevenção e de combate à violência contra profissionais no sector da saúde. Para tal, deverão desenvolver um conjunto de aplicações de suporte que recorrem a *sockets* TCP e UDP, estudadas nas aulas da disciplina. A aplicação permite que profissionais de saúde reportem casos de violência a agentes de segurança, podendo inserir novos casos manualmente ou através de um botão de alarme que irá estabelecer um chat entre profissionais de saúde e agentes de segurança.

1.2. Arquitetura

O programa é desenvolvido em linguagem C, sendo a sua compilação e correção através de um terminal Linux.

Consistirá em 4 aplicações distintas:

- Aplicação para o Profissional de Saúde (APS): Permite aos profissionais de saúde autenticados efetuarem o registo de ocorrência(s) de violência;
- Aplicação de Gestor de Sistema (AGS): Permite a que gestor autenticado validar, consultar e apagar o registo no sistema de novos profissionais de saúde e agentes de segurança.
- Aplicação para Agente de Segurança (AAS): Permite aos agentes de segurança consultar ocorrências, podendo pesquisar por local, data ou nome.
- Aplicação Central (AC): Contem a base de dados de ocorrências e de credenciais de todos os utilizadores.

1.3. Objetivo

Nesta segunda fase do projeto foi proposto aos alunos que implementassem as funcionalidades F8 a F10, que constam em adicionar à primeira e segunda etapa de projeto as opções de “help”, anonimato e botão de alarme.

2. COORDENAÇÃO

2.1. Gestão de equipa

Para uma melhor organização do trabalho em equipa, foram definidas três funções e atribuídas aos membros do grupo.

- Gestor de Equipa e de Software- Coordena e planeia toda a gestão de equipa do projeto e consequentes métodos de implementação.
- Gestor de Cliente, Qualidade, Riscos e Testes - Define a interface de cliente, coordena o relatório, garante a qualidade de todos os módulos do projeto e efetua todos os testes necessários
- Equipa de Desenvolvimento - Desenvolve todo o software necessário.

Os cargos foram atribuídos em função das competências para os desempenhar de cada um dos membros.

António Dias - Gestor de Equipa e Software e Gestor de Cliente, Qualidade, Riscos e Testes

Pedro Ribeiro - Equipa de desenvolvimento

3. DESCRIÇÃO DO PROJETO

A aplicação é composta por 4 aplicações distintas, como dito anteriormente.

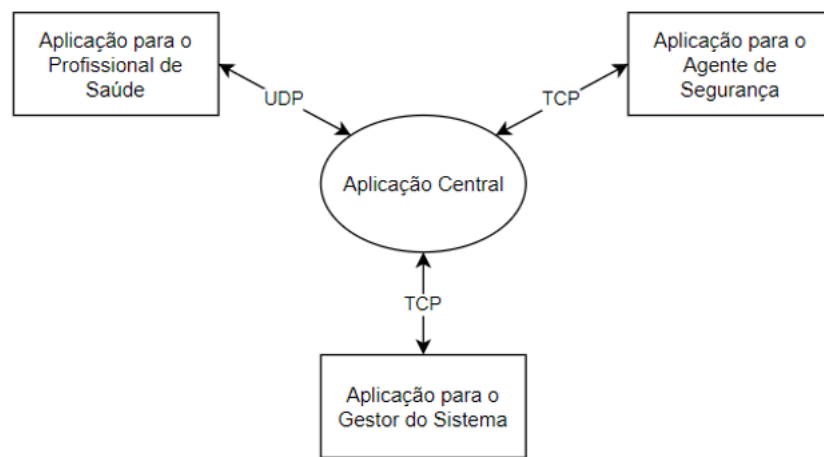


Fig. 2 - Estrutura geral do projeto

As 3 aplicações de cliente funcionam de maneiras semelhantes, primeiramente é sempre dada a escolha ao utilizador se quer fazer *login* ou *sign up*. Se o utilizador escolher *login* é-lhe pedido que introduza os seus dados de autenticação (username e password), posteriormente são enviados para a aplicação central para serem verificados nos ficheiros que contêm essas informações. Consoante o resultado dessa verificação é devolvido ao cliente a informação que as credências estão corretas, incorretas ou não existentes.

Se o utilizador quiser também pode criar uma conta. São-lhe pedidos os dados de autenticação e são enviados para a aplicação central para serem verificados. Se coincidirem com dados já existentes não serão criados e uma mensagem de erro será enviada ao cliente. Caso contrário o novo utilizador é gerado, porém não está autorizado a utilizar a aplicação de imediato e terá que aguardar que um gestor de sistema o autorize.

3.1. Autenticação de credenciais

A autenticação de credenciais é feita pela aplicação central. Quando recebe a string com informação acerca das credenciais do utilizador o sistema converte-a numa *sctruct* 'rg' que contém os parâmetros Username, Password, tipo e uma flag que indica o estado de autenticação. Posteriormente, o programa abre o ficheiro que contém as credenciais e, utilizando um algoritmo, copia os dados, caracter a caracter, para os parâmetros da struct. Depois, compara esses parâmetros com os dados recebidos, de forma a verificar se existem, ou não.

3.2. Criação de contas

Os clientes de Profissional de Saúde e Agente de Segurança permitem a criação de contas a novos utilizadores. Quando o menu inicial é apresentado, o utilizador pode escolher “criar conta” e é-lhe pedido o username desejado, esse username é enviado para a aplicação central que verifica se já existe ou não, se não existir é devolvida ao cliente uma mensagem de sucesso e é pedida a password desejada, após enviada para a AC é inserida uma string no documento utilizadores.txt que contem as informações necessárias sobre o novo utilizador, tem o seguinte aspeto “username;password;tipo;validação”. O parâmetro tipo é inserido consoante o cliente que enviou o username e password, “2” para Agente de Segurança e “3” para Profissional de Saúde. O parâmetro validação é predefinido a “1” e indica que o utilizador ainda não foi validado pelo gestor.

3.3. Aplicação Central (AC)

A AC estabelece comunicação por sockets com todas as outras aplicações.

De forma a poder utilizar as 3 aplicações simultaneamente, as sockets são estabelecidas em 3 processos diferentes. Com o auxílio da função fork() é possível criar um processo pai e dois processos filhos.

```
Int main(){
...
Int pid = fork();
If (pid == 0) {
    ... //socket UDP - Aplicação para Profissional de Saúde
}
else { //sockets TCP
    int pid2 = fork();
    if (pid2==0){
        ... //socket TCP - Aplicação para Agente de Segurança - Porto 9000
    }
    else {
        ... //socket TCP - Aplicação para Gestor de Sistema - Porto 9001
    }
}
}
```

Fig. 3 - Estrutura simplificada dos *forks*

A AC também gere todas as informações em ficheiros através das funções:

- fopen(“diretório”, “a”) para abrir ou criar o ficheiro;
 - fopen(“diretório”, “r”) para ler o ficheiro;
 - função fgets para aceder ao conteúdo existente no ficheiro;
-

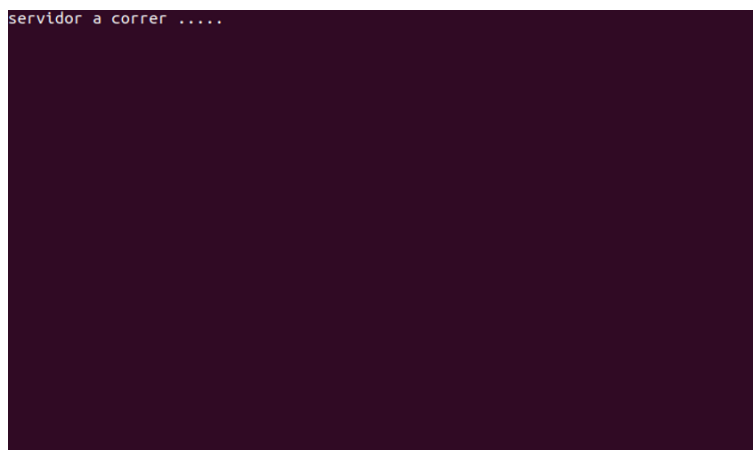
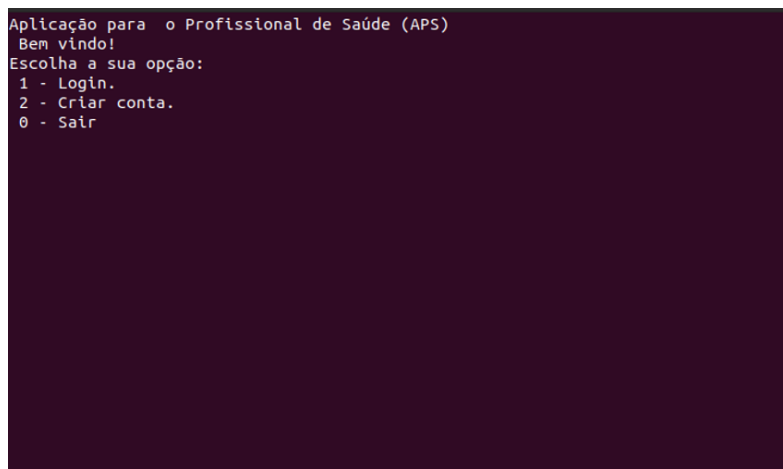


Fig. 4 - Servidor a correr

3.4. Aplicação para o Profissional de Saúde (APS)

A APS estabelece um socket UDP com a AC, uma vez que a sua função, nesta etapa, é apenas reportar casos de violência.

Ao ligar é perguntado ao utilizador se quer fazer *login*, criar uma conta ou sair. Se escolher fazer login serão pedidas as credenciais ao utilizador, e, se estiverem corretas e a conta se encontrar aprovada, vai ser apresentada uma mensagem de boas-vindas ao utilizador, e, de seguida, é-lhe pedido que insira os dados da ocorrência. Serão pedidos os dados pela ordem: local - tipo de agressão - nome. OS parâmetros “data” e “hora” são inseridos automaticamente através de funções da biblioteca <time.h>. Após a introdução, todos os inputs do utilizador são convertidos numa só string com o formato “data;hora;local;tipo;nome;” que é enviada para a AC para ser posteriormente adicionada ao ficheiro ‘ocorrencias.txt’. Se as credências que o utilizador colocar estiverem erradas ou não existirem na base de dados será pedido que repita o processo. Se o utilizador quiser criar uma conta ser-lhe-ão pedidos os dados, nome e password. Para evitar erros é pedida uma confirmação de palavra-passe, que deverá ser igual á primeiramente introduzida. Estas credenciais são guardadas no ficheiro de texto ‘utilizadores.txt’, juntamente com duas flags que indicam o seu tipo e estado de aprovação.

Fig. 5 Menu Inicial APS

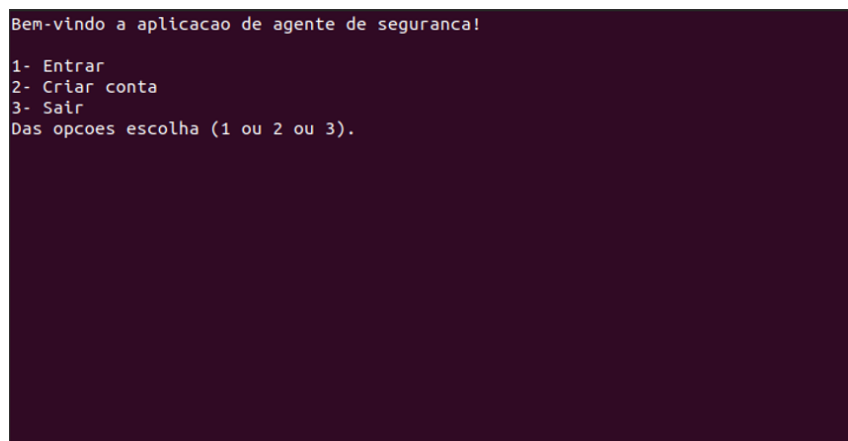
Nesta etapa do projeto foi preciso implementar a funcionalidade de o registo de ocorrências poder ser feito de uma forma anónima. Para isso, quando o utilizador insere uma nova ocorrência, o ultimo campo pergunta se deseja ser anónimo ou não, caso “sim” o ultimo parâmetro da string será “anónimo”, caso contrário o último parâmetro da string será o nome do utilizador que está com o login feito.

3.5. Aplicação para o Agente de Segurança (AAS)

A AAS estabelece um socket TCP com a AC, uma vez que a sua função, no futuro, passa por uma comunicação bilateral mais duradoura com o servidor.

Como na APS, ao ligar, é perguntado ao utilizador se quer fazer login, criar uma conta ou sair. O login e a criação de conta são idênticos aos da APS. Quando o login é efetuado com sucesso, o utilizador será remetido para o menu respetivo onde poderá consultar ocorrências e aplicar filtros. As credenciais das contas criadas são guardadas no ficheiro de texto ‘utilizadores.txt’, juntamente com duas flags que indicam o seu tipo e estado de aprovação.

É oferecida a possibilidade ao utilizador de aplicar filtros na sua pesquisa, estes podem ser “data”, “nome” ou “local”. Após a escolha, o utilizador indica o que quer pesquisar, essa informação é enviada á AC que percorre o ficheiro ocorrências, se encontrar uma ou mais ocorrências que coincidam com o que foi enviado, são enviadas as linhas completas de volta para o cliente e são apresentadas.



```
Bem-vindo a aplicacao de agente de seguranca!  
1- Entrar  
2- Criar conta  
3- Sair  
Das opcoes escolha (1 ou 2 ou 3).
```

Fig. 6 Menu Inicial AAS

```
Login efetuado com sucesso!  
Escolha a opção:  
1 - Todas as ocorrências.  
2 - Local.  
3 - Nome.
```

Fig. 7 Menu de pesquisa de ocorrências

3.6. Aplicação para o Gestor de Sistema (AGS)

A AGS estabelece, como a AAS, um socket TCP com a AC, por razões semelhantes.

Como na APS e AAS, ao ligar, é perguntado ao utilizador se quer fazer login, criar uma conta ou sair. O login e a criação de conta são idênticos aos da APS e AAS. Quando o login é efetuado com sucesso, o utilizador será remetido para o menu respetivo onde poderá gerir os registos. As credenciais das contas criadas são guardadas no ficheiro de texto 'utilizadores.txt', juntamente com duas flags que indicam o seu tipo e estado de aprovação.

```
Bem-vindo a aplicacao de Gestor de Sistema!  
1- Entrar  
2- Criar conta  
3- Sair  
Das opcoes escolha (1 ou 2 ou 3).
```

Fig. 8 Menu Inicial AGS

3.7. Botão de alarme

Foi proposto implementar um botão de alarme, que, ao ser selecionado pelo profissional de saúde, notifica em tempo real o agente de segurança.

De forma a fazer essa implementação foram criados novos processos nas aplicações cuja função será apenas tratar do transporte da informação.

Primeiramente criou-se um novo processo na aplicação para profissional de saúde, e um Pipeline entre os dois processos desta aplicação, assim, quando no processo pai é pressionado o “botão de alarme” o username é enviado para o processo filho através de um pipe. Posteriormente a informação é enviada através de um socket UDP para a aplicação central.

Na aplicação central também se criaram dois novos processos, um para receber a informação da aplicação para profissional de saúde, e outro para enviar a informação para a aplicação para agente de segurança. O primeiro recebe a informação por socket UDP, envia por pipe para o outro processo e este envia para a aplicação de agente de segurança. Lembrando que a informação passada é apenas o username.

Na aplicação de agente de segurança foi criado também um processo extra, cuja função é apenas esperar por informação vinda da aplicação central, este processo está ligado à AC por socket UDP, quando recebe o username imprime uma mensagem no ecrã a informar que o utilizador está em apuros.

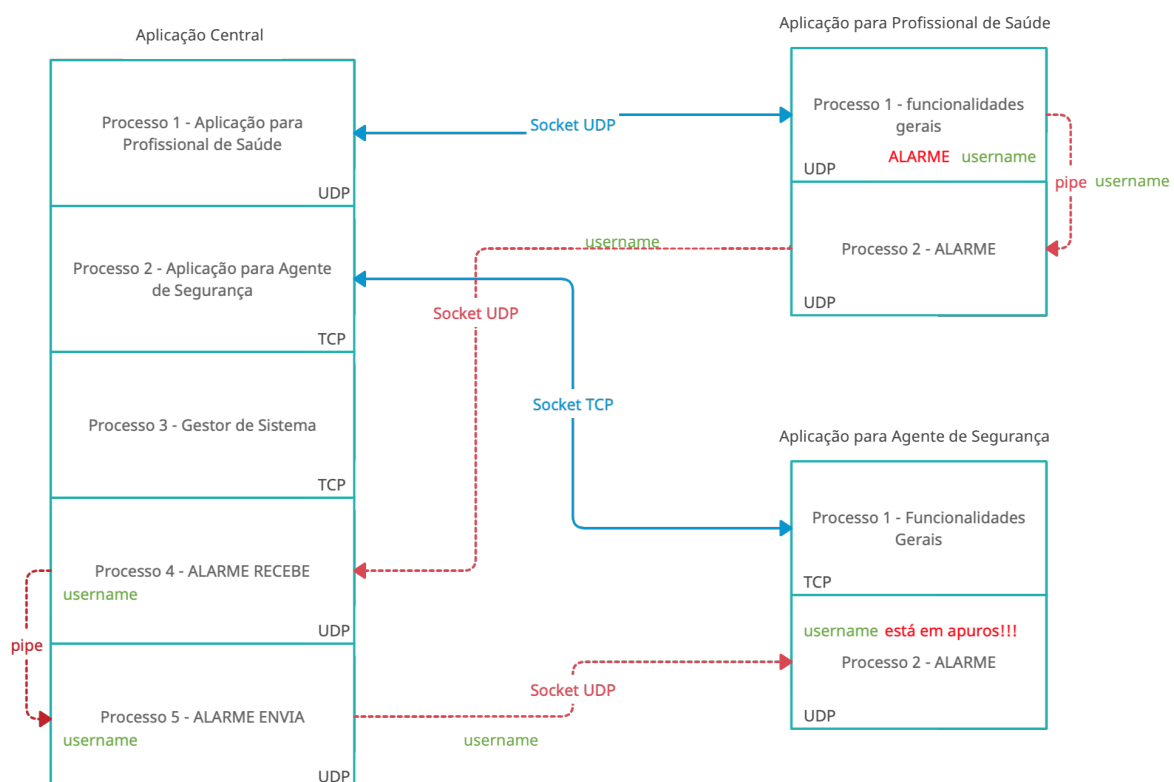


Fig. 9 - Esquema de funcionamento do botão de alarme

3.8. Design e Mockup

A aplicação final irá incorporar as 3 aplicações de cliente numa só, com um design simples e intuitivo.

Através do website www.mockitt.wondershare.com o gestor de cliente, na etapa passada, desenvolveu um *mockup* da *app* final.

O Menu inicial dará a opção de escolher qual o tipo de utilizador está a aceder. Após a seleção será apresentado ao utilizador um campo para introduzir as suas credenciais. Se estiverem corretas, dependendo do tipo de utilizador, irá ser apresentado o menu de funcionalidades associadas ao seu tipo.

Se for Profissional de Saúde, o menu irá apresentar as funcionalidades: Registar Ocorrências, Alterar Registo, Eliminar Registo, Chat, SOS e Help.

Se for Agente de Segurança, o menu irá apresentar as funcionalidades: Consultar Ocorrências, Alterar Registo, Eliminar Registo, Chat e Help.

Se for Administrador o menu apresenta as funcionalidades: Gerir Registos e Help.

Estas funcionalidades da aplicação estão ilustradas nos apêndices 1, 2 e 3.

4. TESTES DE SOFTWARE

O teste é destinado a mostrar que um programa faz o que é proposto fazer e para descobrir os defeitos do programa antes do uso. Quando se testa o *software*, o programa é executado usando dados fictícios. Os resultados do teste são verificados à procura de erros, anomalias ou informações sobre os atributos não funcionais do programa.

4.1. Aplicação Central

A aplicação central, como o nome indica, vai ser responsável por manter em duas bases de dados distintas, todos os registos de ocorrências e todas as credenciais dos utilizadores.

4.1.1. Credenciais dos utilizadores

Um dos aspetos mais importantes nas aplicações é a segurança dos dados pessoais e das credenciais da conta dos seus usuários. É então essencial o recurso a um conjunto de testes de forma a diminuir o risco de perda ou acesso indevido a estas informações:

- Numa fase inicial, é fundamental avaliar se as credenciais de uma conta são recebidas corretamente através da comunicação por *sockets*, tanto no acesso à aplicação como no registo.
- De seguida, é necessário averiguar se a aplicação central apresenta as opções corretas para as diferentes aplicações, consoante o tipo de usuário. Por exemplo, o *Menu Inicial* da aplicação do Agente de Segurança é diferente do *Menu Inicial* destinado ao Profissional de Saúde.
- Caso o utilizador tenha selecionado a opção de *Alteração de Conta*, averiguar se as alterações foram efetuadas e guardadas corretamente e não geraram conflito com o resto dos registos da base de dados.
- Ao selecionar a opção de *Eliminação de Conta*, é importante garantir que esta é devidamente apagada dos registos da aplicação.
- Na parte referente ao Gestor da Aplicação, ao optar pela consulta da lista de usuários, certificar que esta é enviada completa. Caso este decida fazer algumas alterações a uma ou mais contas, assegurar que são devidamente guardadas ou eliminadas.

4.1.2. Ocorrências

- Dentro do tópico das ocorrências, um dos testes mais importantes para o bom funcionamento da aplicação central, é assegurar que todas as informações fornecidas pelos utilizadores são entregues corretamente através da comunicação por *sockets*.
- O segundo teste é igualmente importante, é confirmar que após o recebimento das denúncias dos utilizadores, estas sejam devidamente guardadas na base de dados sem que se perca informação essencial.
- Na parte referente ao Gestor da Aplicação, é crucial testar as duas possibilidades de acesso à lista de crimes da base de dados. Isto é, ao optar pelo acesso total à lista de registos, garantir que esta é enviada completa. Na opção por filtragem, avaliar se apenas são enviados os registos com o filtro selecionado.

O sistema é constituído por quatro aplicações diferentes, das quais três delas é necessário realizar o acesso através do login ou registo de uma conta (profissional de saúde, agente de segurança e gestor da aplicação). Assim, é possível desenvolver uma lista de testes comuns a cada uma dessas aplicações no que toca ao assunto de autenticação ou criação de conta.

4.2. Página inicial

- Ao entrar em cada uma das aplicações, os primeiros testes a serem realizados dizem respeito às diferentes opções apresentadas pela *Página Inicial*. Assim, começamos por confirmar se após a seleção das diferentes opções, o utilizador é reencaminhado para as respetivas interfaces de cada uma, seja de Login ou Registo.

- Durante este primeiro ponto é também possível testar simultaneamente o botão de Voltar existente em cada uma destas interfaces, que torna possível ao utilizador regressar à página inicial, caso se tenha enganado na escolha da opção.

- Uma das opções também disponíveis nesta *Página Inicial* designa-se por *Help*, que contém orientações e informações sobre o funcionamento de cada uma das aplicações, sendo igualmente importante o seu teste.

4.2.1. Opção de login

- Nesta primeira opção, é necessário verificar se apenas é permitido o acesso a utilizadores com credenciais já registadas. Caso isso não aconteça, confirmar se os dados de acesso são solicitados novamente, após o envio de uma mensagem de erro.

- Conferir se é recebida uma mensagem de aviso e se é requerida nova inserção de dados caso o usuário introduza um nome de utilizador correto e a palavra-passe errada, ou o inverso.

4.2.2. Opção de registo:

- Na parte referente ao Registo, é necessário confirmar se os dados introduzidos da nova conta foram devidamente guardados na base de dados da aplicação, para posterior acesso.

- Testar o envio de uma mensagem de aviso caso já exista um nome de utilizador na base de dados igual ao introduzido para a nova conta.

Após a apresentação dos testes comuns a cada uma das aplicações, avançamos para as listas de testes específicos.

4.3. Aplicação do Administrador do Sistema:

A função do administrador, como já referido anteriormente, consiste apenas em autorizar e gerir as contas dos utilizadores. Assim, o trabalho do gestor de testes é garantir que não ocorrem erros no desempenho dessas funções.

4.3.1. Autorização e gerenciamento de contas:

- De forma a poder consultar e autorizar o acesso de novas contas à aplicação, é necessário assegurar que primeiramente o gestor irá receber uma lista completa com todas as contas criadas, tanto de profissional de saúde como de agente de segurança.
- Garantir que uma conta é eliminada da base de dados do sistema, se o Gestor assim o desejar.

4.4. Aplicação do Profissional de Saúde:

Após efetuar corretamente o seu login, o profissional de saúde tem acesso a um Menu Inicial com três opções diferentes: registar uma ocorrência e alterar ou eliminar a sua conta. De maneira a comprovar o seu bom funcionamento e a não haver qualquer tipo de falhas durante o uso da aplicação por parte do cliente, realizou-se a seguinte lista de testes:

4.4.1. Registo de ocorrências

- Um dos testes mais importantes a realizar nesta parte do programa é garantir que após o registo, a ocorrência foi devidamente enviada para o servidor principal, apresentando uma mensagem de confirmação ao cliente.
 - A anotação dos crimes tem um certo formato específico (Data; Hora; Local; Tipo de Agressão; Nome) e portanto é necessário assegurar que o registo é guardado dessa forma na base de dados.
 - Como também há a hipótese de anonimato na escrita das ocorrências, é fundamental garantir o bom funcionamento dessa opção para segurança dos profissionais de saúde. Este teste é feito através da inserção do termo *Anónimo* no campo referente ao *Nome*.
-

- Nas situações mais urgentes, o Profissional de Saúde tem a hipótese de reportar o crime em tempo real usando um botão de SOS. Assim, é de máxima importância garantir o sucesso desta funcionalidade. Este teste é feito através da simulação de envio de uma ocorrência, garantindo que esta é recebida em poucos segundos na aplicação do Agente de Segurança.

- Por último, e se necessário, é possível o Profissional de Saúde manter contacto constante com o Agente de Segurança através de um *Chat*. Deste modo, o último teste ao nível das ocorrências está relacionado com esta funcionalidade, e realiza-se através do envio de mensagens de teste de modo a garantir que estas são enviadas e recebidas por ambas as aplicações.

4.4.2. Alteração de conta

- Nesta interface, garantir que é apresentado ao utilizador a opção de alterar tanto o nome de utilizador como a palavra-passe. Após a inserção dos novos parâmetros, é necessário assegurar que as alterações são devidamente guardadas, apresentando uma mensagem de confirmação.

- Após as alterações serem efetuadas e confirmadas, assegurar que não é possível entrar na conta com as credenciais antigas, e sim com as novas.

4.4.3. Eliminação de Conta

- Chegando à última opção do Menu Inicial, é necessário garantir em primeiro lugar que são solicitados os dados de acesso da conta, de forma a evitar a sua eliminação por parte de terceiros. Após o preenchimento desses campos, verificar se é apresentado ao utilizador uma mensagem de confirmação. No fim e igualmente importante, assegurar que a conta foi apagada dos registos da aplicação.

4.5. Aplicação do Agente de Segurança:

Como referido anteriormente para o profissional de saúde, também na aplicação do agente de segurança o usuário irá ter acesso a um menu inicial com três opções diferentes: registar uma ocorrência e alterar ou eliminar a sua conta. De maneira a comprovar o seu bom funcionamento e a não haver qualquer tipo de falhas durante o uso da aplicação, realizou-se a seguinte lista de testes:

4.5.1. Consulta do registo de ocorrências:

- Numa primeira fase é importante garantir a apresentação ao agente de segurança das duas possíveis opções de pesquisa. A primeira, de ver uma lista com todos os crimes registados até a esse momento. A segunda, optar por filtrar e pesquisar uma ocorrência específica.
- Na primeira opção o gestor de testes é obrigado a assegurar que todos os crimes são devidamente recebidos pela aplicação do agente de segurança, e a lista não seja apresentada incompleta.
- Na segunda opção da aplicação de filtros à lista de crimes, confirmar se qualquer um dos campos de cada ocorrência é pesquisável. Este tipo de ensaios são mais trabalhosos, pois implicam o registo de um pequeno conjunto de crimes falsos e a sua pesquisa por parte do responsável dos testes.
- Garantir o bom desempenho da funcionalidade de SOS e simultaneamente de *Chat*.

4.5.2. Alteração de conta

- Nesta interface, garantir que é apresentado ao utilizador a opção de alterar tanto o nome de utilizador como a palavra-passe. Após a inserção dos novos parâmetros, é necessário assegurar que as alterações são devidamente guardadas, apresentando uma mensagem de confirmação.
- Após as alterações serem efetuadas e confirmadas, assegurar que não é possível entrar na conta com as credenciais antigas, e sim com as novas.

4.5.3. Eliminação de conta

- Chegando finalmente à última opção do Menu Inicial, é necessário garantir em primeiro lugar que são solicitados os dados de acesso da conta, de forma a evitar a sua eliminação por parte de terceiros. Após o preenchimento desses campos, verificar se é apresentado ao utilizador uma mensagem de confirmação. No fim é igualmente importante, assegurar que a conta foi apagada dos registos da aplicação.

4.6. Conclusão

Em suma, é importante realçar que o conjunto de testes apresentado têm em conta os requisitos propostos pelo cliente. Na última meta cada grupo é responsável por indicar e realizar os testes às funcionalidades extra implementadas na aplicação.

5. ESTADO DA ARTE

Nesta fase final do projeto ficaram implementadas todas as funcionalidades pretendidas. A aplicação central é capaz de receber e comunicar com todos os clientes em simultâneo. Ambas aplicações de cliente permitem a criação e alteração dos dados da conta. A aplicação para profissional de saúde permite ao utilizador efetuar login ou registar conta, uma vez autenticado pode editar os seus dados ou registar ocorrências, anonimato e botão de alarme. A aplicação para Agente de segurança permite ao utilizador efetuar login ou registar conta, uma vez autenticado pode editar os seus dados de autenticação e listar ocorrências através de filtros e receber sinais de alarme. A aplicação para gestor de sistema permite que este liste todos os utilizadores não autenticados e, por sua vez, proceder á sua autenticação.

Por fim, a equipa encontra-se satisfeita com o estado atual do desenvolvimento deste projeto, apenas ficou por fazer a parte de extras e chat.
