

FAET – FACULDADE DE CIÊNCIAS EXATAS E TECNOLOGIA
CURSO DE ENGENHARIA DA COMPUTAÇÃO

RICARDO HENRIQUE CARVALHO DE OLIVEIRA

LAVRAGEM DE AUTO DE INFRAÇÃO VIA PALM

BRASÍLIA,
DEZEMBRO 2007



RICARDO HENRIQUE CARVALHO DE OLIVEIRA

LAVRAGEM DE AUTO DE INFRAÇÃO VIA PALM

Trabalho de Conclusão de Curso apresentado à Faculdade de Ciências Exatas e Tecnologia, como requisito à aprovação final no Curso de Engenharia da Computação.

Orientador: Prof. MSc **MARCO ANTÔNIO ARAÚJO**

BRASÍLIA,
DEZEMBRO 2007

À minha avó Aldenice de Miranda Cousseiro.

AGRADECIMENTOS

Agradeço a Deus primeiramente por estar presente em minha vida todos os dias e principalmente quando necessário.

Aos meus Pais, José Valdo de Oliveira e Aldenice Cousseiro de Carvalho Filha, por terem-me tornado reflexo da educação deles.

Ao meu tio Acácio Ferreira de Carvalho Filho, por servir como exemplo de Engenheiro e de amigo.

Aos meus irmãos Carlos Vinicius Ramos de Oliveira e Angélica Carvalho de Oliveira por estarem presentes na minha vida.

Ao Sr. Nelson Gonçalves Rezende, chefe do Centro Nacional de Telemática do IBAMA – SEDE, pela confiança e oportunidade concedidas, as quais contribuíram na minha formação profissional.

Ao meu amigo Raul Heringer de Souza Cruz, por ser uma pessoal criteriosa, exigente, mas acima de tudo amiga.

Ao meu amigo Kleber Ferreira Gomes, pelo apoio técnico na implementação do projeto.

Á minha noiva, Ana Raquel Gomes Faria, pelo carinho, amor, respeito e principalmente pela sinceridade.

Aos professores Abiezer Marilia Fernandes, Francisco Javier Obaldia e ao meu professor orientador Marco Antonio Araújo, pelas orientações necessárias para a finalização deste projeto.

Valeu à pena?
Tudo vale a pena,
Se a alma não é pequena.
Fernando Pessoa

RESUMO

Este projeto visa desenvolver um sistema para aquisição e transferência remota de dados com uso de Palm. A principal motivação é apresentar uma solução que pode ser utilizada por várias empresas que têm necessidade de levantar, registrar, enviar e armazenar informações que precisam ser verificadas em campo e transmitidas com segurança para o ambiente corporativo. Atualmente, observamos vários casos de registros e envio de dados de forma imprecisa, muitas vezes sendo necessário o preenchimento manual de formulários, os quais precisarão ser digitados ou digitalizados muitas vezes por pessoas diferentes daquelas que fizeram a leitura e registro das informações. Com isto, existe uma grande possibilidade dos dados não chegarem a tempo, serem registrados de forma imprecisa, sem falar na possibilidade de fraude. Também é verdade que temos observado várias formas de se resolver problemas como este, dependendo do que se quer registrar e transferir remotamente. Em alguns casos, são utilizados nos levantamentos, registros e transferência de dados remotamente, laptops, celulares, controladores, palms, enfim, dispositivos capazes de realizar uma leitura e/ou aquisição de dados, com interfaces de comunicação, para transmitir de forma remota. A idéia deste projeto consiste na utilização do Palm com interface de comunicação acima mencionada, para registrar e transferir dados.

Palavras-Chave: Palm - Transferência de dados.

LISTA DE ILUSTRAÇÕES

Figura 2.1 - Formação de uma Piconet 16
Figura 2.2 - Formação de uma rede de dispersão Scatternet . . .17
Figura 3 - Tela de varredura do aplicativo Bloover 25
Figura 4 - Topologia do Ambiente Proposto 27
Figura 5 - Diagrama de Casos de Uso 32
Figura 6 - Caso de Uso – Login no Sistema 33
Figura 7 - Tela inicial (Página Login) 34
Figura 8 - Tela Principal 35
Figura 9 - Caso de Uso – Alterar CPF do Infrator 35
Figura 10 - Selecionando Módulo Alterar Cpf 36
Figura 11 - Tela Alterar – Cpf do Infrator 37
Figura 12 - Tela Consulta Dinâmica 37
Figura 13 - Tela Alterando Cpf 38
Figura 14 - Caso de Uso – Cadastrando Pessoas sem Cpf 38
Figura 15 - Selecionando Cadastro Pessoas sem CPF 39
Figura 16 - Tela Cadastro Pessoas sem Cpf 40
Figura 17 - Caso de Uso – Incluir CPF (Infrator sem CPF) . . .40
Figura 18 - Selecionando Incluir CPF 41
Figura 19 - Tela Incluir CPF/CNPJ para Infrator 42
Figura 20 - Tela Consulta Dinâmica 42
Figura 21 - Caso de Uso – Alterar Dados do Infrator 43
Figura 22 - Selecionando nome e endereço 44
Figura 23 - Tela Alterar Dados da Pessoa 44
Figura 24 - Tela Consulta Dinâmica 45
Figura 25 - Caso de Uso – Consultar Auto de Infração 45
Figura 26 - Tela Selecionando Consulta Auto 46
Figura 27 - Tela Consulta Auto de Infração 47
Figura 28 - Caso de Uso – Processar Arquivos Palm 47
Figura 29 - Tela Selecionando opção Processar arquivos Palm . .49

Figura 30 - Tela Processar arquivos PALM 49
Figura 31 - Caso de Uso – Alterar dados de um Auto de Infração . .50
Figura 32 - Tela Selecionando opção Cadastro de Auto de Infração . .51
Figura 33 - Tela Cadastro de Auto de Infração 51
Figura 34 - Caso de Uso – Relatórios de Auto de Infração por estado . .52
Figura 35 - Tela Selecionando Opção Relatórios por Estado. . . .53
Figura 36 - Tela Relatórios Auto de Infração por Estado 53
Figura 37 - Caso de Uso – Relatórios de Auto de Infração por Código . .54
Figura 38 - Tela Selecionando Opção Relatórios por Código . . .55
Figura 39 - Tela Relatórios Auto de Infração por Código de Infração . .55
Figura 40 - Diagrama de Casos de Uso da Aplicação em Casl . . .56
Figura 41 - Caso de Uso – Cadastrar Auto de Infração 56
Figura 42 - Tela Auto de Infração. 57
Figura 43 - Tela Cadastrar Auto de Infração 58
Figura 44 - Caso de Uso – Editar Auto de Infração 58
Figura 45 - Tela Editar de Autos de Infração 59
Figura 46 - Tela de Editar Autos de Infração 60
Figura 47 - Caso de Uso – Excluir Auto de Infração 60
Figura 48 - Tela de Exclusão de Autos de Infração 61
Figura 49 - Programa FileZ – Envio de Arquivo via Bluetooth . . .62
Figura 50 - Programa FileZ – Selecionando Arquivo para envio . . .63
Figura 51 - Programa FileZ – Enviando Arquivo via Bluetooth . . .63
Figura 52 - Programa FileZ – Detectando Dispositivos Bluetooth . . .64
Figura 53 - Programa FileZ – Enviando Arquivo 64
Figura 54 - Confirmação de Recebimento de Arquivo 65
Figura 55 - Configurações do Windows 65
Figura 56 - Configurações do Windows - Geral. 66
Figura 57 - Configurações do Windows - Padrão 67
Figura 58 - Programa Conversor de arquivo na extensão txt . . .67

LISTA DE TABELAS

Tabela 1 - Primeiro teste de preenchimento de dados em Casl . . .68
Tabela 2 - Segundo teste de preenchimento de dados em Casl . . .69
Tabela 3 - Terceiro teste de preenchimento de dados em Casl . . .69
Tabela 4 - Primeiro teste de preenchimento de dados em Php . . .70
Tabela 5 - Segundo teste de preenchimento de dados em Php . . .70
Tabela 6 - Terceiro teste de preenchimento de dados em Php . . .71
Tabela 7 - Quarto teste de preenchimento de dados em Php . . .71
Tabela 8 - Quinto teste de preenchimento de dados em Php . . .72
Tabela 9 - Primeiro teste de edição de dados em Casl 73
Tabela 10 - Primeiro teste de deleção de auto de infração em Casl. . .74
Tabela 11 - Primeiro teste de deleção do arquivo AutoInfraDB.txt . . .74
Tabela 12 - Primeiro teste de criptografia em Casl 75
Tabela 13 - Primeiro teste de descriptografia em Php 75
Tabela 14 - Primeiro teste de transmissão de dados via fileZ . . .76

SUMÁRIO

1 INTRODUÇÃO 11
1.1 Motivação 11
1.2 Objetivos do Trabalho 12
2 TECNOLOGIA BLUETOOTH 13
2.1 Definição 13
2.2 Histórico 14
2.3 Forma de Comunicação 15
2.4 Freqüência e Comunicação 17
2.5 Conexões no Bluetooth 18
2.6 Estrutura de uma Piconet 19
2.7 Vantagens e Desvantagens 19
3 SEGURANÇA, RISCOS E APLICAÇÕES BLUETOOTH 21
3.1 Riscos 23
3.1.1 Tipos de Ataques 23
3.2 Ferramentas 25
3.3 Criptografia 25
4 IMPLEMENTAÇÃO, CENÁRIOS, TESTES E RESULTADOS . . .27
4.1 Introdução 27
4.2 Formulário Dinâmico 30
4.3 Pacotes ORACLE 31
4.4 Descrição dos Casos de Uso da Aplicação Php 31
4.4.1 Efetuar “Login” no Sistema 32
4.4.2 Alterar CPF do Infrator 35
4.4.3 Cadastro de Pessoas sem CPF 38
4.4.4 Incluir CPF (Infrator sem CPF) 40
4.4.5 Alterar dados do Infrator 43
4.4.6 Consultar Auto de Infração 45
4.4.7 Processar Arquivos Palm 47
4.4.8 Alterar Dados de um Auto de Infração 49

4.4.9 Relatórios de Auto de Infração por Estado 51
4.4.10 Relatórios de Auto de Infração por Código de Infração . . .53
4.5 Descrição dos Casos de Uso da Aplicação Casl 56
4.5.1 Cadastrar Auto de Infração 56
4.5.2 Editar Auto de Infração 58
4.5.3 Excluir Auto de Infração 60
4.6 Softwares Gratuitos Utilizados 61
4.7 Testes e Resultados 68
4.7.1 Preenchimento de Dados em Casl 68
4.7.2 Preenchimento de Dados em Php 69
4.7.3 Edição de Dados em Casl. 72
4.7.4 Deletação de Dados em Casl 73
4.7.5 Deletação do Arquivo AutoInfraDB.txt em Php 74
4.7.6 Criptografia de Dados em Casl 74
4.7.7 Descriptografia de Dados em Php 75
4.7.8 Transmissão de Dados via Software fileZ 75
4.8 Dificuldades Encontradas 76
5 CONCLUSÕES E PROPOSTA PARA PROJETOS FUTUROS . .78
REFERÊNCIAS 80
APÊNDICE A - Exemplo da Classe Formulário Dinâmico . . .82
APÊNDICE B - Exemplo de um Pacote Oracle 84
APÊNDICE C - Função de Criptografia em Casl 87

1 INTRODUÇÃO

Atualmente o uso de palmtops trás inúmeras vantagens para órgãos do governo e para empresas. Algumas dessas vantagens são: Custo baixo do produto, longa durabilidade das baterias, fácil mobilidade, alta capacidade de armazenamento, grande disponibilidade de programas, possibilidade de sincronização de dados com outros portáteis e computadores convencionais e portabilidade como novas tecnologias tais como Wireless e Bluetooth.

A experiência profissional adquirida no Ibama no decorrer de seis anos possibilitou a participação em soluções de diversos problemas relacionados ao meio ambiente na parte de tecnologia da informação. Como também a verificação da carência de sistemas em levantar, registrar, enviar e armazenar informações que precisam ser verificadas em campo e transmitidas para o ambiente corporativo.

Será desenvolvido um software, que possibilitará o envio de dados para um notebook ou desktop, desde que os equipamentos mencionados possuam placa wireless Bluetooth. Os dados antes de serem enviados para um desktop e/ou notebook serão criptografados, minimizando assim possibilidades de furto das informações contidas no palm. Após a transmissão, os mesmos podem ser encaminhados para serem processados e armazenados no ambiente de rede corporativa, através de acesso autenticado via cpf e senha ao sistema existente por um broswer de navegação para internet conforme padrão de acesso aos sistemas do Ibama. Dessa forma o aplicativo em palm, visa minimizar erros de digitação na entrada de dados e aperfeiçoar o envio e entrada dos mesmos no ambiente corporativo.

O trabalho está dividido em cinco capítulos. Após o primeiro capítulo, destinado à introdução, temos o seguinte: no capitulo 2 são descritas as características da Tecnologia Bluetooh; no capitulo 3 são ilustrados riscos, aplicações, ferramentas e a parte de criptografia que será utilizada no desenvolvimento da aplicação em palm; no capitulo 4 é detalhada a implementação de todo o projeto; e, no capitulo 5, é descrita a conclusão deste trabalho.

1.1 Motivação

A principal motivação é apresentar uma solução que pode ser utilizada por empresas com necessidade de levantar, registrar, enviar e armazenar informações que precisam ser verificadas em campo e transmitidas com segurança para o ambiente corporativo.

1.2 Objetivos do Trabalho

O projeto tem por objetivo principal o desenvolvimento de uma interface que permita a entrada e envio de dados de forma remota através de um palm. Para isso faremos uma demonstração utilizando a simulação de um processo de lavragem de autos de infração, conforme especificações verificadas nos procedimentos utilizados pelo Ibama.

Outro objetivo do projeto é evitar que operadores do sistema em php digitem informações do auto de infração lavrado em campo. Quando as mesmas forem atualizadas no sistema em php, estarão disponíveis on-line através de relatórios no formato em pdf para consultas.

2 TECNOLOGIA BLUETOOTH

Neste capítulo, será apresentada a definição de tecnologia Bluetooth, seu histórico, forma de comunicação, freqüência, comunicação e conexões. Além disso, será informada a estrutura de uma piconet, vantagens e desvantagens da rede Bluetooth.

2.1 Definição

A tecnologia Bluetooth é um tipo de comunicação sem fio de custo e consumo de energia baixa e de curto alcance. O alcance dependendo da especificação pode ter uma variação de até aproximadamente 100 metros. As especificações abaixo vêm sendo constantemente desenvolvidas:

- Bluetooth 1.0;
- Bluetooth 1.0B;
- Bluetooth 1.1;
- Bluetooth 1.2;
- Bluetooth 2.0.

A Bluetooth 2.0 é a mais atual e é a que possibilita uma melhor velocidade de transmissão e alcance de dados com uma maior economia de energia(SCHWEITZER et al., 2005). Com essa tecnologia, é possível conectar diversos tipos de dispositivos de comunicação, tais como *notebooks, palmtops, handhelds*, impressoras, scanners, telefones celulares e outros.

A conexão ocorre de uma maneira simples e fácil, praticamente automática, não sendo necessário uso de cabos. Para que a mesma seja estabelecida, basta que os sinais de rádio dos dispositivos sejam detectados um pelo outro através de um chip também chamado de Bluetooth (MILLER, 2001).

Essa tecnologia tem por finalidade possibilitar a comunicação de dados e de voz em tempo real. Funciona através de ondas de rádio na freqüência de 2.4 GHz, com a velocidade de 721Kbps e três canais de voz. Os dispositivos que fazem uso desse

tipo comunicação são classificados de acordo com a potencia e alcance em três níveis (MILLER, 2001):

- Classe 1: Potência 100 mW, Alcance de até 100m;
- Classe 2: Potência 2,5 mW, Alcance de até 10m;
- Classe 3: Potência 1mW Alcance de até 1m;

A maioria dos equipamentos é de classe 2, ideal para as chamadas *Personal Area Networks*, redes sem fio que integram apenas os aparelhos próximos ao usuário. É o caso da comunicação entre teclado ou mouse sem fio e de dois Pdas que precisam trocar informações (PREUSS, Julio, 2006).

Os dispositivos eletrônicos se comunicam espontaneamente oferecendo três grandes vantagens (MILLER, 2001):

- **Ponto de acesso de voz e dados:** Simplifica o acesso através do fácil reconhecimento de dispositivos em diferentes tipos de redes através de uma conexão Bluetooth.
- **Substituição de cabos**: Elimina a necessidade de conexões a cabo
- **Redes *ad-hoc* personalizadas:** Caracterizadas pela ausência da necessidade de uma infra-estrutura de retransmissão de dados de um ponto a outro, ou seja, a comunicação entre dois dispositivos ocorre de forma direta sem uso de intermediários.

2.2 Histórico

A principio, a tecnologia Bluetooth foi idealizada para eliminar a necessidade de cabos na conexão de aparelhos. No entanto, aprimorou – se o projeto com o intuito de transforma – lá em um tipo de comunicação com uma boa relação de custo e benefício.

Em 1994, a Ericsson começou a desenvolver um projeto de uma interface de rádio com consumo e custo baixos. Uma tecnologia que pudesse ligar telefones móveis e os seus acessórios sem o uso de fios. Em 1998, após a Ericsson verificar que o potencial da comunicação entre dispositivos de rádio de curto alcance era praticamente ilimitado, os grandes IBM, Nokia, Toshiba e Intel se uniram e formaram o

chamado Bluetooth Special Interest Group com o objetivo de conduzir e desenvolver a tecnologia sem fios. O consórcio Bluetooth cresceu incrivelmente em poucos anos e conta com a participação de mais de 2000 empresas, tais como HP, 3Com, Philips, Motorola, Samsung, Siemens, Dell, Sony e outras. Possibilitando desta forma uma ampla divulgação da tecnologia em todo o mundo (MILLER, 2001).

O nome Bluetooth foi escolhido em homenagem ao rei da Dinamarca e Noruega Harald Blatand, conhecido como Harald Bluetooth. Esse apelido lhe foi dado pelo fato de possuir uma coloração azulada em seus dentes. Blatand é conhecido por unificar as tribos norueguesas, suecas e dinamarquesas por isso o significado de Bluetooth é unificação. Dessa forma, o protocolo visa unir diferentes tecnologias tais como telefones móveis e computadores. O logotipo Bluetooth é a união de duas runas nórdicas para as letras H e B, suas iniciais (MILLER, 2001).

2.3 Forma de Comunicação

A tecnologia Bluetooth utiliza um chip com rádio-transmissor pequeno e de baixa voltagem em um dispositivo eletrônico normal. Os rádios Bluetooth utilizam uma banda de rádio chamada ISM (Banda Industrial, Médica e Cientifica), na faixa de 2.4 e 2.48 GHz.

Segundo Stallings (2002), quando dois dispositivos Bluetooth estabelecem uma conexão criam uma rede denominada piconet ou picorede. Nesta rede, apenas oito dispositivos no máximo podem estar conectados entre si. Dentre eles, um é necessariamente o master, o principal, e os demais são os escravos, slaves. É possível sobrepor vários piconets aumentando – se dessa forma os pontos de comunicação. Essa técnica denominada ad-hoc scatternet, possibilita a coexistência de até 10 piconets em um mesmo lugar de cobertura de rádio (STALLINGS, W, 2002).

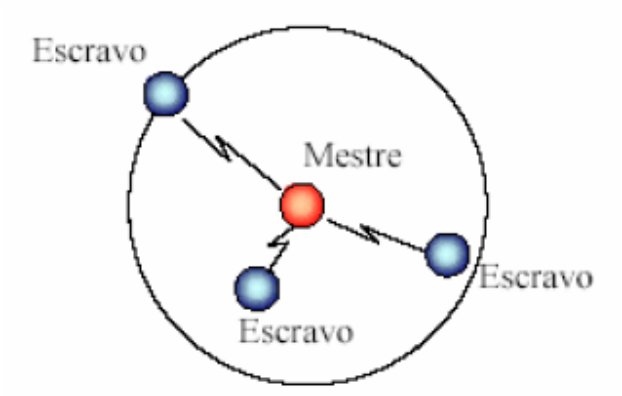


Figura 2.1 - Formação de uma piconet, retirado de Santana (2004).

A figura 2.1 ilustra a formação de uma piconet entre dispositivos Bluetooth. Nela é possível verificar que uma piconet é formada por um dispositivo mestre e dispositivos escravos. Sendo que o mestre é ilustrado na cor vermelha e os escravos na cor azul.

A segurança está preservada graças à decodificação e proteção contra interferências que ocorrem em cada piconet.

Para a operação do Bluetooth na faixa ISM de 2.45 GHz, foram definidas 79 portadoras espaçadas de 1 MHz. São 79 freqüências nas quais instantaneamente um dispositivo pode estar transmitindo. Uma seqüência deve ser escolhida e estabelecida pelo dispositivo mestre da piconet, os dispositivos escravos devem tomar conhecimento da mesma para de uma forma sincronizada se comunicar.

Para minimizar interferências, o dispositivo mestre pode modificar a freqüência 1600 vezes por segundo. Possui um máximo de largura de banda de 1 Mbit/s. Em relação à sua velocidade pode chegar a 721 Kbps e possui três canais de voz (EMERSON, 2003).

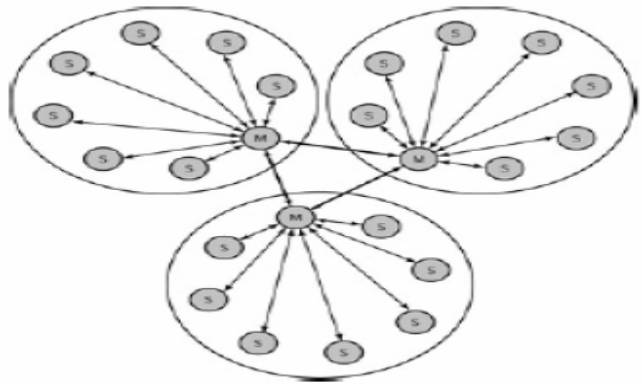


Figura 2.2 – Formação de uma rede de dispersão Scatternet, retirado de Miller (2001).

A figura 2.2 ilustra a formação de uma rede de dispersão Scatternet, que é constituída pela união de diversas piconets, ou seja, para conectar mais de oito dispositivos, há a necessidade de formar outras piconets e conectar os dispositivos mestres de cada piconet.

Segundo Stallings (2002), toda comunicação entre piconets em uma rede de difusão, são filtradas pelos seus dispositivos mestres. Em uma rede de difusão é possível ter até dez piconets, contendo um total de oitenta dispositivos Bluetooth diferentes. Acima desse número a rede pode ficar saturada, visto que a tecnologia Bluetooth só utiliza setenta e nove freqüências no total. Como cada piconet opera em um canal de salto de freqüência diferente, é possível que diversas piconets compartilhem o mesmo espaço físico sem estarem conectadas.

2.4 Freqüência e Comunicação

Os dispositivos Bluetooth trabalham na freqüência de faixa ISM em 2,45 GHz. Pelo fato da mesma possuir características diferentes entre paises distintos, são necessárias pequenas adaptações visando pleno funcionamento. No entanto, existem iniciativas padronizar o uso de uma única faixa para comunicação via Bluetooth.

Essa comunicação é feita através de um canal FH-CDMA (Frequency Hopping – Code-Division Multiple Access). Nesse método, o transmissor envia um sinal sobre uma série randômica de freqüências de rádio, o receptor captura o sinal de uma

forma sincronizada com o transmissor. A mensagem somente é recebida se o receptor conhecer a série de freqüências na qual o transmissor trabalha para envio do sinal (DIAS, 2006).

A tecnologia Bluetooth permite a ocorrência de um elevado número de comunicações descoordenadas em uma mesma área. Com isso, é possível usar vários canais dentro de um mesmo ambiente. Para essa tecnologia, existe um grande número de canais independentes e não sincronizados, cada um servindo a um número limitado de participantes. Esses canais estão associados a um piconet um por um, a diferenciação entre eles ocorre através da seqüência de freqüências usadas por cada um (MILLER, 2001).

Para evitar a colisão entre as múltiplas transmissões de dispositivos escravos, o dispositivo mestre faz uso da técnica denominada polling, a qual possibilita transmissão somente por parte do dispositivo indicado no slot mestre-para-escravo para o slot escravo-para-mestre seguinte (MILLER, 2001).

2.5 Conexões no Bluetooth

Para serem estabelecidas conexões no Bluetooth, são necessários três elementos:

- **Scan:** Usado para economia de energia. Quando dispositivos estiverem ociosos, entram em modo stand-by e passam a verificar a cada 10 ms a existência de outros dispositivos tentando estabelecer uma conexão (LEANDRO; MELLO, 2000).
- **Page:** É utilizado pelo dispositivo que deseja estabelecer conexão. A cada 1,25 ms são transmitidos dois pedidos de conexão seguidos em diferentes portadoras. O dispositivo também verifica duas vezes se há respostas (LEANDRO; MELLO, 2000).
- **Inquiry:** São mensagens enviadas por um dispositivo para determinar quais outros dispositivos estão em sua área e quais são suas características. Ao receber esta mensagem, um dispositivo deve retornar um pacote chamado FHS (Frequency Hopping-Synchronization) contendo além de sua identidade, informações para o sincronismo entre os dispositivos(LEANDRO; MELLO, 2000).

2.6 Estrutura de uma piconet

Uma piconet pode ser formada com pelo menos dois dispositivos denominados mestre e escravo. O dispositivo mestre é encarregado de sincronizar a comunicação de diferentes dispositivos escravos. Cada piconet independente é denominada de Scatternet. Varias piconets podem ser estabelecidas e ligadas juntas em ad-hoc scatternets, possibilitando a comunicação entre as mesmas através de configurações continuas e flexíveis (ARTSEN; NAGHSHINEH; INOUYE, 1999).

Todos os dispositivos de uma mesma piconet possuem prioridade de sincronização, outros dispositivos podem se integrar a qualquer momento. Uma piconet tem como topologia, uma estrutura flexível e múltipla.

Quando dois ou mais aparelhos habilitados com a tecnologia Bluetooth se aproximam, uma conexão é estabelecida automaticamente sem a necessidade cabos ou programas específicos. Nesse momento, é formada uma pequena rede piconet (MILLER, 2001).

Cada rede piconet interliga até oito dispositivos. Podendo ser desde uma conexão a poucos centímetros, como um teclado sem fio conectado ao computador, como também aparelhos em salas diferentes.

Numa mesma sala, podem ser estabelecidas várias redes piconet sem que ocorra interferência entre as mesmas. Esse fato ocorre, pois, cada rede piconet se diferencia uma das outras através de profiles, configuração especifica que possibilita comunicações entre dispositivos Bluetooth. Aparelhos Bluetooth com o mesmo profile se conectam com outros aparelhos de profile idêntico operando em um canal de salto de freqüência diferente (MILLER, 2001).

2.7 Vantagens e Desvantagens

A seguir, serão especificadas as vantagens e desvantagens da rede Bluetooth.

a) Vantagens:

- Uso desnecessário de cabos para estabelecimento de conexões. Os dispositivos em uma rede Bluetooth se comunicam por uma espécie de antena, conforme ilustrado em figura abaixo;
- Uma solução viável e de baixo custo para redes de curto alcance;
- Maior quantidade de dispositivos com chips Bluetooth;
- Suporte a comunicação tanto de voz quanto de dados;
- Tecnologia facilmente integrada aos protocolos de comunicação, como o TCP/IP, por exemplo;
- Existência de um Grupo Especial de interesse denominado SIG, o qual reúne empresas que lideram o desenvolvimento da tecnologia Bluetooth com o propósito de desenvolver software e hardware seguindo as especificações criteriosas.

b) Desvantagens:

- O numero limitado de dispositivos que podem se conectar ao mesmo tempo;
- O Alcance é bastante curto, por isso de uma rede ser apenas local;
- Necessidade de adequação da tecnologia para interconexão de dispositivos;
- Necessidade de criação de softwares que possibilitem uma correta comunicação entre aplicações de diferentes dispositivos;

3 SEGURANÇA

Sinais de rádio podem ser interceptados com facilidade, por isso é importante que dispositivos Bluetooth sejam configurados com níveis de segurança. Dessa forma previne-se o recebimento de mensagens não autorizadas, o acesso a informações confidenciais e transferência de dados não autorizada (PEREIRA, 2006).

Esses níveis são mencionados abaixo:

- **Service level security (modo de segurança 2)**: Nível de segurança de acesso versátil, especialmente para acionar aplicações com diferentes níveis de segurança em paralelo. Dois níveis de confiança para os dispositivos estão presentes:

1º) Dispositivo confiável, de relação fixa com acesso irrestrito a todos os serviços;

2º) Dispositivo não confiável, sem relação fixa com acesso aos serviços restrito

- **Link level security (modo de segurança 3)**: O Nível de segurança é o mesmo para todas as aplicações de conexões iniciadas. Embora seja menos flexível esse modo mantém o nível comum de segurança e é mais fácil de implementar que o modo 2. Todas as funções são baseadas no conceito de código de ligação, número aleatório de 128 bits armazenado individualmente para cada par de dispositivos. A cada comunicação de dois dispositivos via transmissores Bluetooth, o código de ligação é usado para autenticação e criptografia, não influenciando na topologia da piconet. O tipo de código de ligação mais seguro é uma combinação de código, derivado dos códigos inseridos em ambos os dispositivos.

Um procedimento visando proteção seria o nível de segurança dos dispositivos para os serviços ou grupo de serviços. Para dispositivos com baixa capacidade de armazenamento, há opção de escolher um código unitário, o qual pode ser usado por muitos dispositivos remotos. Para transmissão, um código temporário é necessário, não utilizado para autenticação, mas previne acesso não-autorizado de fora da piconet.

Para serviços que exigem autorização (permissão ou negação de acesso a serviços), autenticação (identificação de quem está do outro lado da linha) e criptografia, existem três níveis de segurança que visam controle do acesso dos mesmos (BRINGEL FILHO, 2004):

1º) Para serviços que requerem autorização e autenticação, o acesso automático é garantido em dispositivos confiáveis, apenas; para os demais, a autorização manual se faz necessária;
2º) Serviços que exigem apenas autenticação. Serviços disponíveis a todos os dispositivos. O nível de segurança padrão é definido no intuito de servir às necessidades das aplicações herdadas. A diretriz padrão será usada a menos que outras aplicações sejam consideradas como base de dados de segurança.

Outro procedimento que não necessita de inserção de códigos seria o de autenticação. Isto envolve uma interpelação dispositivo-dispositivo e o esquema de resposta exige um código de ligação comum de 128 bits, uma interpelação de 128 bits e uma resposta de 32 bits. Quando dois dispositivos se comunicam pela primeira vez, um procedimento de inicialização é necessário para que o código de ligação comum de um modo seguro seja criado, procedimento denominado emparelhamento (pairing). O modo básico de se fazer isto assume que o usuário tem acesso a ambos dispositivos simultaneamente. Na primeira conexão, um código Bluetooth de 16 bytes ou de 128 bits é exigido entre o par de dispositivos.

Quando, por algum motivo, um código de ligação é deletado e o emparelhamento inicial tem que ser repetido, qualquer código de segurança Bluetooth pode ser novamente inserido pelo usuário. No caso de exigências de pouca segurança, é possível ter um código fixo nos dispositivos que não possuam a interface homem-máquina para permitir o emparelhamento (SCHWEITZER et al., 2005).

O procedimento de emparelhamento envolve:

- geração de um código numérico de inicialização aleatório comum, a partir do código de segurança Bluetooth fornecido pelo usuário para os dispositivos emparelhados;
- autenticação faz a verificação da existência de códigos de segurança Bluetooth igual em dispositivos emparelhados;
- geração de um código de ligação aleatório comum de 128 bits armazenado temporariamente ou semi-permanentemente nos dispositivos emparelhados.

Quanto maior for o código de ligação armazenado em ambos os dispositivos, a repetição do emparelhamento não se faz necessária. Apenas o procedimento normal de autenticação é utilizado.

A criptografia para banda passante de ligação não exige entrada de dados por parte do usuário. Após uma autenticação ocorrer com sucesso e o código de ligação atual ser verificado, um código criptografado é gerado a partir do código de ligação para cada sessão de comunicação. Um algoritmo cifrado adequado é usado para implementação em hardware. O tamanho do código criptografado varia de 8 a 128 bits, dependendo do nível de segurança e do hardware utilizados.

A segurança Bluetooth não pretende substituir as redes de segurança existentes. Para os casos de exigência extremamente alta ou especial (como comercio eletrônico) mecanismos de segurança adicionais podem ser implementados.

O tipo de código de ligação mais seguro é uma combinação derivada dos códigos inseridos em ambos os dispositivos. Para dispositivos com baixa capacidade de armazenamento, há opção de escolher um código unitário, o qual pode ser usado por muitos dispositivos remotos.

3.1 Riscos

Redes Bluetooth estão expostas a riscos similares presentes em redes sem fio, tais como a identificação de equipamentos de uma rede, negação de serviço, captura e escuta de tráfego de rede entre outros.

Uma das principais vulnerabilidades dos dispositivos Bluetooth consiste na habilidade que esses dispositivos possuem de descobrir uns aos outros e criarem conexões entre si sem a intervenção do usuário. Se um dispositivo Bluetooth está no “modo correto” (visível ou passível de ser descoberto), outros dispositivos podem estabelecer comunicação sem intervenção do usuário. Neste caso, em áreas públicas, um PDA ou laptop com Bluetooth pode ser comprometido e, conseqüentemente, os dados armazenados no dispositivo podem ser ameaçados (SCHWEITZER et al., 2005).

3.1.1 Tipos de Ataques

Os ataques mais comuns sobre a tecnologia Bluetooth são: Bluetracking, Bluesnarfing, Bluejacking, Bluebugging e Warnibbling (SCHWEITZER et al., 2005).

Bluetracking: O dispositivo Bluetooth tem um identificador único, similar a um endereço físico de rede. O ataque acontece quando um hacker obtém este identificador e através de dispositivos especiais pode rastrear os movimentos deste dispositivo Bluetooth.

Bluesnarfing: É viável, porque em alguns dispositivos antigos é possível acesso ao dispositivo sem conhecimento do dono e conseqüentemente obter os dados. É um ataque a dispositivos Bluetooth habilitados em telefones móveis, sendo possível copiar informações de contatos, calendários, ou outras informações armazenadas na memória do telefone. Isso ocorre quando um dispositivo Bluetooth está configurado no modo visível ou passível de ser descoberto, possibilitando outros dispositivos estabelecer comunicação sem intervenção do usuário.

Bluejacking: Tira vantagem do processo de pairing de dispositivos Bluetooth. Quando estabelecida conexão inicial, uma comunicação peer-to-peer é feita (formando uma rede ad hoc), o nome do dispositivo é enviado e apresentado para outro dispositivo. Como é permitido um campo do nome do dispositivo maior que 248 caracteres, é possível usar o protocolo para enviar mensagens anônimas. Como também buscar por outros dispositivos Bluetooth. Uma vez que o pairing é estabelecido, os dispositivos estão vulneráveis a um ataque do tipo snarf.

Bluebugging: É o processo de enviar comandos executáveis a dispositivos Bluetooth. Especificamente, BlueBug é o nome de uma fragilidade de segurança em dispositivos Bluetooth habilitado em telefones móveis. Esse ataque permite acesso a comandos de configuração, o que significa, habilita ao atacante fazer chamadas telefônicas, uso de SMS, ou conexões à Internet. O atacante além de usar o dispositivo para fins fraudulentos, pode se passar pelo usuário proprietário do dispositivo.

Warnibbling: É a técnica de coletar dados de na área de alcance de comunicação de dispositivos Bluetooth. Redfang ou outros softwares similares são usados, e permitem aos hackers revelar informações confidenciais, pessoais e/ou corporativas. Redfang permite aos hackers encontrar dispositivos Bluetooth em uma

determinada área e uma vez encontrados, o software coleta qualquer dado armazenado no dispositivo, inclusive em dispositivos configurados em modo não visível.

3.2 Ferramentas

Atualmente, ferramentas possibilitam interferir em um trafego existente ou se fazem passar por outro equipamento. Grande parte dessas ferramentas está disponível gratuitamente na Internet. Pode-se citar como exemplo a ferramenta Bloover, que é uma aplicação para identificação e teste de vulnerabilidade escrita em Java. Funciona tanto em computadores convencionais quanto em celulares. Pode identificar redes nas proximidades, conforme figura 3 abaixo:



Figura 3 – Tela de Varredura do Aplicativo Bloover, retirado de Oliveira (2006).

A figura 3 ilustra o funcionamento do aplicativo Bloover. Esse permite visualizar vários tipos de testes, em busca de vulnerabilidades conhecidas em equipamentos ou implementações Bluetooth, como, por exemplo: fazer chamada usando o telefone atacado, redirecionar chamadas, copiar agenda, enviar e copiar arquivos no padrão SMS etc.

3.3 Criptografia

Proteção de uma mensagem mediante um dos métodos (código ou cifrado) que transformam um texto linguagem natural em texto cifrado ou vice – versa. O primeiro método primário consiste em substituição de cada elemento individual do texto cifrado em código, pode ser elemento correspondente em linguagem natural. A lista dessas

substituições recebe o nome de código de chaves e deve manter – se secreto com objetivo de proteger a informação. O processo de cifragem consiste em mudar um texto em linguagem natural para texto em linguagem cifrada (criptografada) mediante transformação criptográfica, geralmente de tal modo que cada bit, caractere ou palavra do texto normal seja substituído por bit, caractere ou palavra do texto cifrado (criptografado) (CAMARÃO, 1989).

No projeto será utilizada uma função de criptografia da linguagem Casl. Quando o usuário preencher todas as informações do formulário do aplicativo em palm e for armazenar as mesmas no sistema, deverá pressionar o botão de criptografia, dessa forma dificultará a leitura das informações contidas no formulário, visando manter a integridade e segurança das informações presentes no mesmo quando forem enviadas via bluetooth para um notebook ou desktop.

4 IMPLEMENTAÇÃO, CENÁRIOS, TESTES E RESULTADOS

Neste capítulo abordaremos as formas de implementação, os cenários, testes e resultados com a proposta desta monografia.

4.1 Introdução

A idéia do trabalho é simular um ambiente corporativo para ilustrar o funcionamento de um sistema de lavragem de auto de infração. Desde o uso do Palm até o cadastro das informações em servidores Web e de Banco de Dados, conforme topologia descrita abaixo:

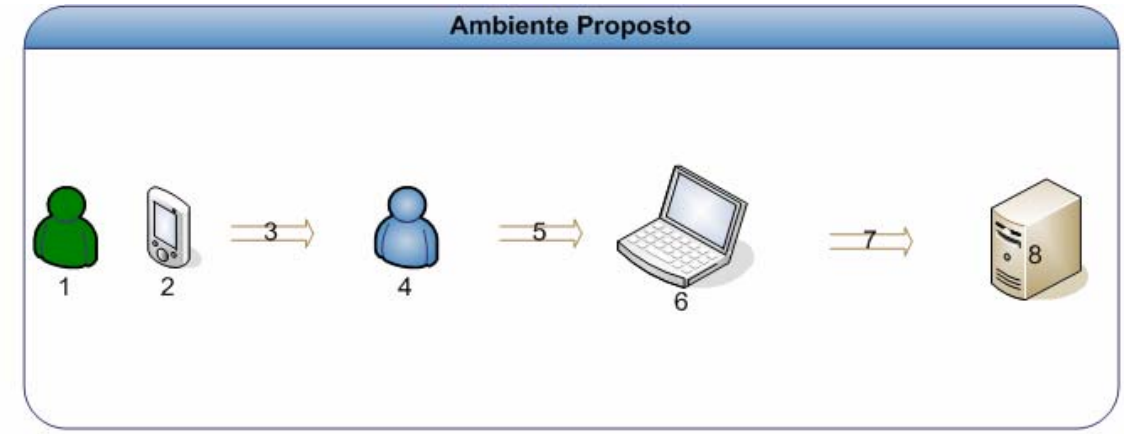


Figura 4 – Topologia do Ambiente Proposto.

Legenda:

1 – Fiscal do órgão;
2 – Palmtop com placa wireless Bluetooth usado para lavragem do auto de infração;
3 – Fiscal entrega o palm para o operador do sistema em php;
4 – Operador com acesso ao sistema em php;
5 – Meio de transmissão dos dados do auto de infração, Bluetooh;
6 – Notebook com placa wireless Bluetooth usado para receber os dados do auto de infração;
7 – Dados do auto de infração sendo enviados pela interface de upload de arquivos desenvolvida em php;
8 – Servidor Web e de Banco de Dados;

Para tanto foi necessário o uso de algumas tecnologias, tais como:

- **Hardware:**

  a) Palmtop Zire 72 com sistema operacional Palm OS Garnet 5.2.8, uma tela colorida com resolução de 320x320 um processador da Intel de 312MHz um memória interna de 32MB, (24MB disponíveis), um cartão de memória flash de 32 MB, uma câmera digital de 1.2MP, compatível com Bluetooth, um conector mini USB para sincronismo de dados, um cabo de energia e uma bateria recarregável;

  b) Laptop Dell Latitude D520 com Processador Celeron 430 (1.73GHZ), Memória 1.0GB, DDR2-533 (1 pente), disco rígido de 60GB SATA 7200RPM, com sistema operacional Windows XP Professional, SP2 em português, placa wireless Intel 3945 WLAN (802.11 a/g) mini PCI, placa wireless 350 Bluetooth com uma unidade óptica interna de DVD 8X e DVD /-RW 8X.

  Software:

  a) Wmware 1.0.1 – Software Console, para permitir que múltiplas máquinas virtuais, com sistemas operacionais heterogêneos rodem isoladamente, paralelamente na mesma maquina física. Foi instalada, configurada e customizada no notebook;

  b) Sistema Operacional Linux Fedora Core 4, um sistema operacional livre que oferece uma melhor combinação de estabilidade com softwares customizados que existe no mundo livre;

  c) CASL 4.3, para desenvolvimento de aplicativos palm;

  d) Apache versão 2.2.4, servidor web gratuito que apresenta um bom funcionamento com linguagens de scripts como PHP e Perl. Compatível com Linux, Unix e também com Windows;

  e) PHP versão 5.2.1, uma linguagem para programar scripts do lado do servidor, que se incrustam dentro do código HTML. Esta linguagem é gratuita e de multiplataforma;

f) Classes em php para criação e gerenciamento da interface web e comunicação com banco de dados;

g) Banco de Dados Oracle Express Edition 10G R2, oferece liberdade para desenvolver e programar aplicativos de muitas plataformas e traz suporte para uma grande variedade de ambientes de desenvolvimento. Tais como Java, NET, PHP e da Web;

h) Browsers Mozilla Firefox 2.0.1 e Internet Explorer versão 7;

i) Aplicativo para o Palm será desenvolvido através do uso do software livre de desenvolvimento CASL 4.3. Esse terá interface que permitirá a entrada de dados via formulários de auto de infração com as opções obrigatórias predefinidas.

Criou-se uma máquina virtual linux com o sistema operacional Fedora Core 4. Foram instalados e configurados servidor Web Apache versão 2.2.4, PHP 5 customizado com classes em PHP para criação e gerenciamento da interface Web e o banco de dados Oracle Express Edition 10G.

O Laptop tem a figura de cliente para o recebimento dos arquivos no formato de banco de dados do palm contendo dados do auto de infração. É feito o sincronismo entre o palmtop e o Laptop, esse com sistema operacional Windows, através da interface de transmissão de dados do aplicativo fileZ via Bluetooth.

O mesmo Laptop tem a figura de Servidor. Foi instalado o software Wmware 1.0.1 e configurada uma maquina virtual linux que usa 15 GB para armazenamento de dados e 412 MB de memória RAM.

Nessa maquina virtual, foi instalado e configurado o sistema operacional Fedora Core 4, o servidor web Apache versão 2.2.4, linguagem de programação PHP versão 5.2.1 customizada com classes em php para criação, gerenciamento da interface web e comunicação com banco dados Oracle Express Edition 10G R2, que também foi instalado e configurado.

Após o envio dos arquivos criptografados pela interface de transmissão de dados do aplicativo fileZ via Bluetooth pelo notebook e da conversão do arquivo pdb, banco de dados de palm para txt, usa - se o aplicativo abc Amber palm converter e

após usa–se a interface Web, desenvolvida em php, para fazer o upload do arquivo no servidor de banco dados.

O arquivo recebe o tratamento do sistema e o auto de infração fica disponível no módulo de fiscalização do Sistema Sicafi interface Web.

Para o desenvolvimento da interface Web foi utilizado o modelo do ciclo de desenvolvimento em cascata, pois para o problema apresentado os requisitos do sistema são estáveis. Inicialmente na etapa de Análise, foram descritos os requisitos do software para poder levantar as necessidades do sistema. Além da descrição dos requisitos nesta primeira fase, também foram utilizados como ferramenta para a modelagem do diagrama de processos do sistema Lavragem Auto de Infração via PALM.

Em seguida, na etapa de Projeto, foi utilizada a técnica de orientação a objetos para se construir um modelo de formulário dinâmico para gerar as páginas de formulários do sistema em formato HTML. A base de dados foi modelada em um diagrama de Entidade-Relacionamento, obtido a partir dos requisitos do sistema. Foram utilizados pacotes de programação PL/SQL ORACLE para separar a camada de apresentação (Formulários HTML) da camada de negócio do sistema (Pacotes ORACLE).

Foram instalados os softwares ABC Amber Palm Converter no laptop e o fileZ no palmtop. O Laptop foi configurado para receber arquivos via bluetooth.

4.2 Formulário Dinâmico

O formulário dinâmico, formdin3.class.php, é uma classe desenvolvida no PHP 5 e orientada a objeto. Essa classe possui um conjunto de operações pré-definidas que torna possível a criação do formulário dinâmico separando a arquitetura do desenvolvimento do sistema em várias camadas.

Através da utilização da classe, é possível separar o conteúdo HTML da criação do formulário dinâmico tornando mais fácil sua manutenção e desenvolvimento. A utilização dessa classe para a geração de páginas de formulários em formato HTML torna-se útil, pois é possível reaproveitar funções comuns ao sistema.

Através da classe de geração de formulário dinâmicos é possível criar botões, campos texto, campos data, campos numéricos através da função que cria o formulário dinâmico.

4.3 Pacotes ORACLE

Para separar a camada de apresentação da camada de negócios, optou-se por utilizar pacotes de programação em PL/SQL ORACLE. Pacote é um objeto do banco de dados capaz de armazenar procedimentos e funções integradas, que podem ser executadas separadamente como se fossem parte de uma biblioteca ou a partir de uma execução provocar várias execuções encadeadas. Os pacotes dividem o trabalho em duas partes: a especificação que é apresentada na camada de apresentação do sistema e a operação. Como a parte de operação não é apresentada na camada de apresentação do sistema, tem – se segurança com relação à visualização do código de programação. Como os pacotes são executados diretamente no servidor de banco de dados além de segurança, possibilitam ganhos de desempenho na utilização do sistema.

4.4 Descrição de Casos de Uso da Aplicação em PHP

Abaixo, apresenta-se o diagrama referente aos casos de uso de aplicação em PHP.

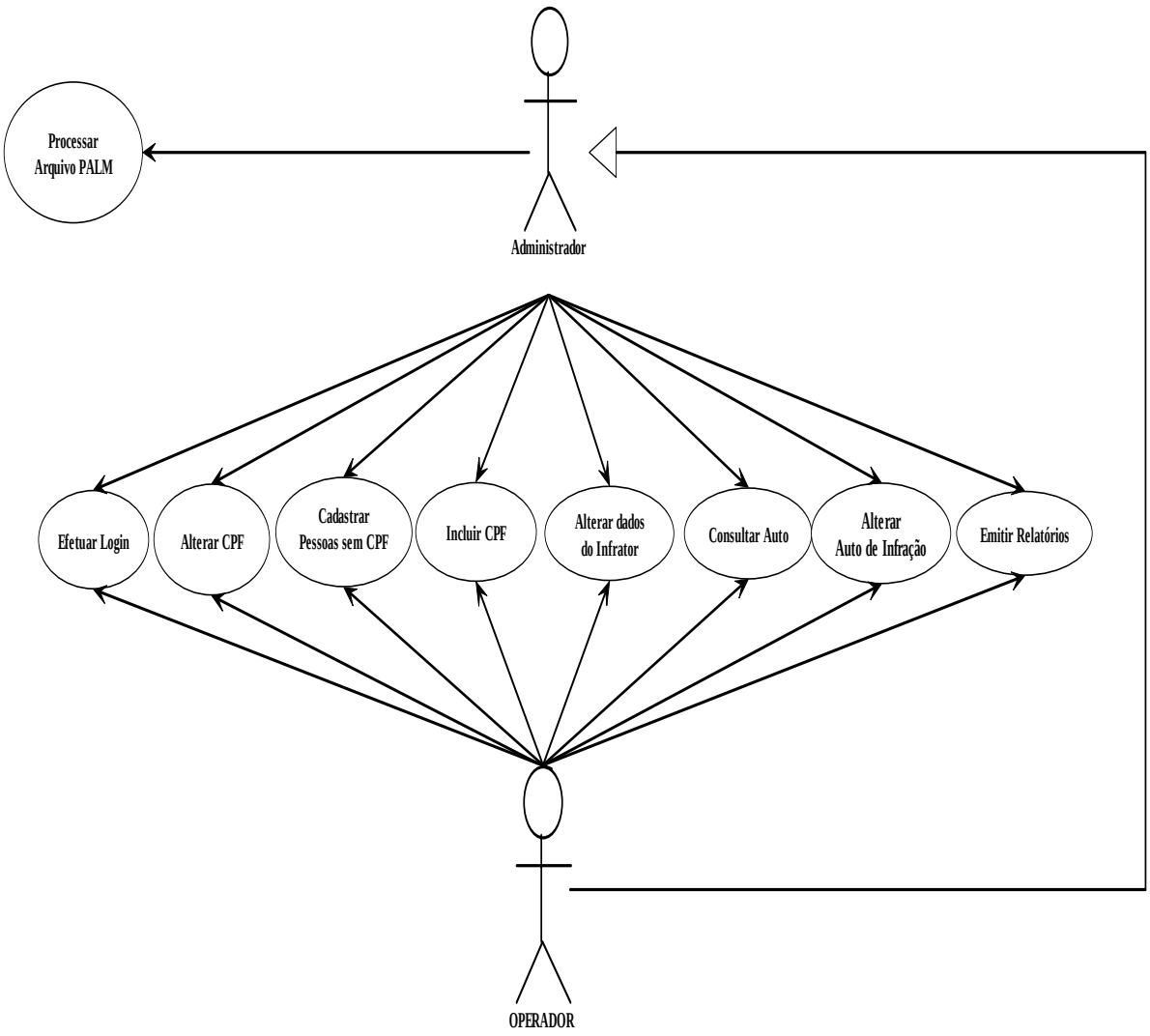


Figura 5 – Diagrama de casos de uso da aplicação em PHP.

4.4.1- Efetuar “Login” no Sistema

A figura abaixo refere-se à atividade do operador em efetuar "login" no sistema, a fim de iniciar o ambiente no SICAFI.



Figura 6 – Caso de Uso – Login no Sistema.

Objetivo: Efetuar “Login” no Sistema para iniciar o ambiente do SICAFI.

Atores participantes: Todos os Usuários do Sistema.

Pré-condição: Usuário deve estar cadastrado no sistema.

Fluxo Principal: (Efetuar “Login” no Sistema)

F1 - Usuário digita endereço URL correspondente do SICAFI no Browser. (http://endereco_ip/html/sicafi/index.php)

F2 - Sistema apresenta a ***“Tela Login”***.

F3 - Usuário preenche o campo ***Login*** com seu “*CPF*”, e no campo de ***senha***, a senha de acesso ao sistema.

F4 - Usuário seleciona o botão ***“Confirmar”.***

F5 - Sistema verifica se o usuário existe, se a senha está correta e armazena na variável de sessão do usuário a credencial (objeto usuário e um array de páginas, opções no menu do sistema, que o usuário pode acessar). **(E1)**

F6 - Sistema direciona para a ***“Tela Principal”***.

Exceções:

E1 - Usuário não existe, ou senha incorreta.

E1.1 - Sistema emite um alerta em forma de mensagem na tela, explicando o erro ao usuário.

Alternativas: Não existem alternativas para este caso de uso.

Pós-condição: Após a confirmação dos campos usuário e senha, o usuário estará habilitado a utilizar o sistema.



Figura 7 – Tela Inicial (Pagina Login).

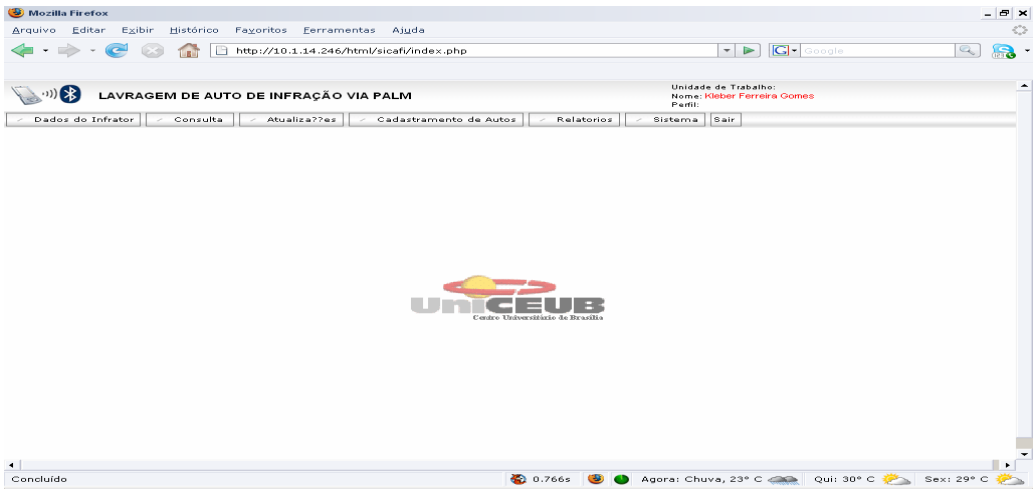


Figura 8 – Tela Principal.

4.4.2- Alterar CPF do Infrator

A seguir, representa-se a forma de alterar o CPF do infrator.



Figura 9 – Caso de Uso – Alterar CPF do Infrator.

Objetivo: Alterar o CPF inválido, cadastrado incorretamente, de um determinado Infrator.

Atores participantes: Usuários com perfil Cadastro e Administrador do Sistema.

Pré-condição: Usuário deve estar “Logado” no sistema.

Fluxo Principal: (Alterar CPF cadastrado incorretamente).

F1 - Usuário na tela principal seleciona a opção no menu: **Dados do Infrator ➔ Alterar CPF do Infrator**. (**Tela Selecionando módulo Alterar CPF)**

F2 - Sistema apresenta a ***"Tela ALTERAR - CPF DO INFRATOR"***.

F3 - Usuário seleciona a Lupa para realizar a pesquisa.

F4 - Sistema apresenta a ***"Tela Consulta Dinâmica"***.

F5 - Usuário preenche o nº do CPF inválido e seleciona o botão ***"Pesquisar"***.

F6 - Sistema apresenta os dados do infrator pesquisado. Usuário preenche no campo **CPF** o nº de CPF correto e seleciona botão **"GRAVAR"**. **"TELA ALTERANDO CPF" (E1).**

F7 – Sistema emite mensagem confirmando que o CPF foi alterado com sucesso.

Exceções:

E1 – Infrator não encontrado

E1.1 - Sistema emite um alerta em forma de mensagem na tela, explicando o erro ao usuário.

Alternativas: Não existem alternativas para este caso de uso.

Pós-condição: Não existe pós-condição para este caso de uso.

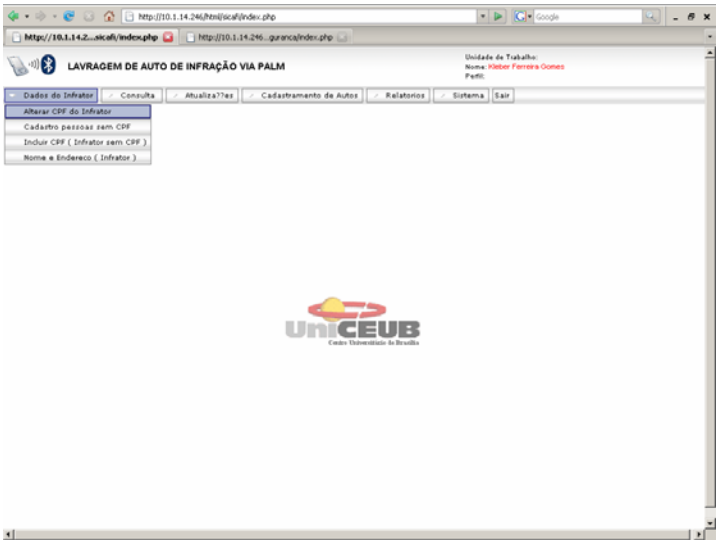


Figura 10 – Selecionando Módulo Alterar Cpf.

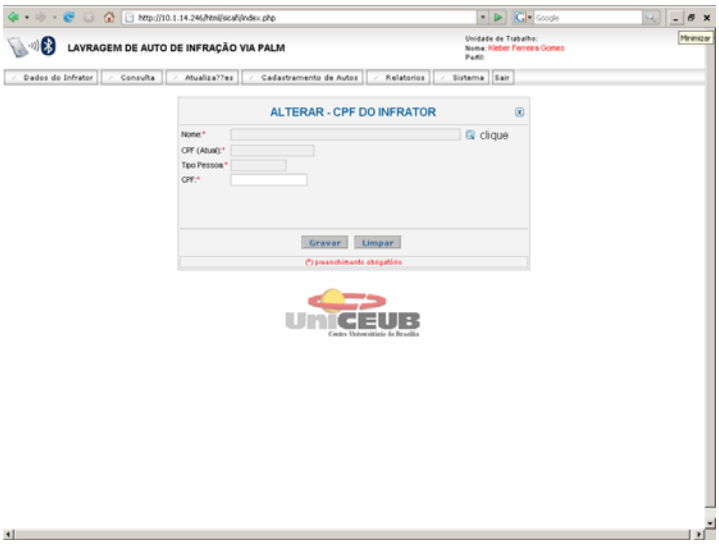


Figura 11 –Tela Alterar – Cpf do Infrator.

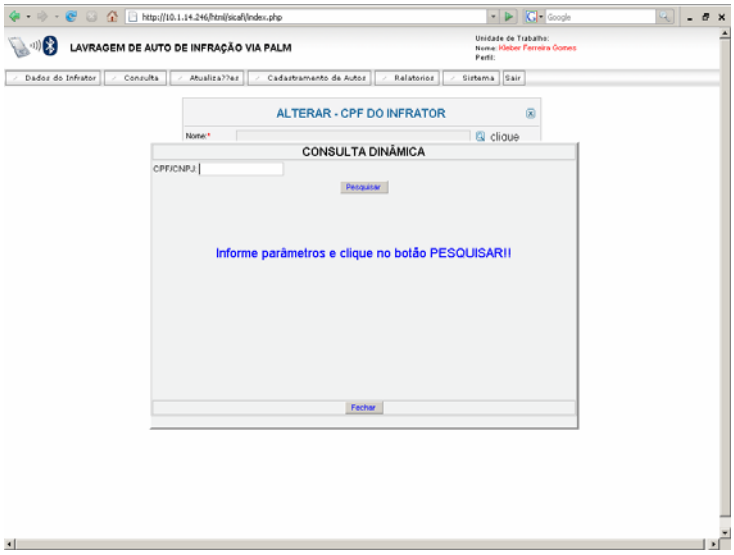


Figura 12 – Tela Consulta Dinâmica.

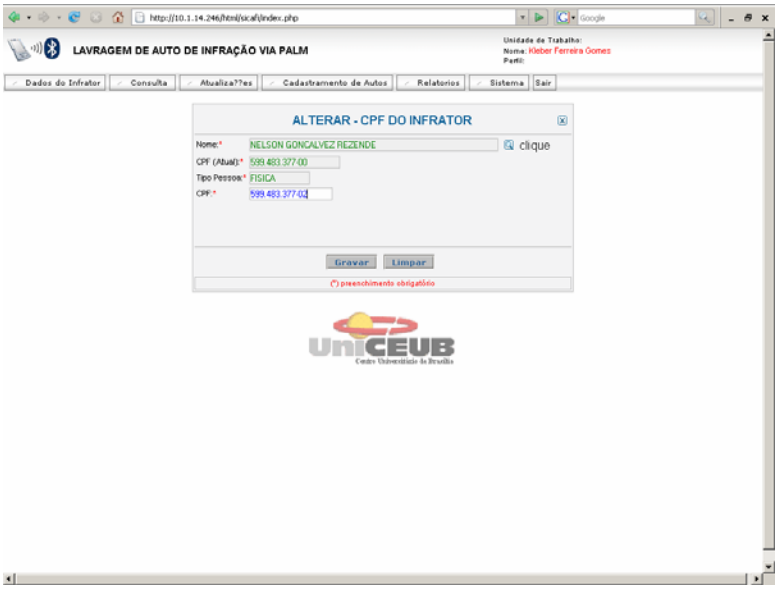


Figura 13 – Tela Alterando CPF.

4.4.3 Cadastro de Pessoas sem CPF

A representação abaixo mostra o procedimento, pelo operador, de cadastramento de pessoas sem CPF.



Figura 14 – Caso de Uso – Cadastro de Pessoas sem CPF.

Objetivo: Cadastrar um infrator que não possua CPF.

Atores participantes: Usuários com perfil Cadastro e Administrador do Sistema.

Pré-condição: Usuário deve estar “Logado” no sistema.

Fluxo Principal: (Cadastrar infrator sem CPF).

F1 - Usuário na tela principal seleciona a opção no menu: **Dados do Infrator ➔ Cadastro de Pessoas sem CPF**. (**Tela Selecionando Cadastro Pessoas sem CPF).**

F2 - Sistema apresenta a ***"Tela Cadastro Pessoas sem CPF"***.

F3 - Usuário preenche dados do infrator e seleciona o botão: "***Cadastrar Pessoa***".

F4 – Sistema emite mensagem confirmando que o Infrator foi cadastro com sucesso.

Exceções: Não existem exceções para este caso de uso.

Alternativas: Não existem alternativas para este caso de uso.

Pós-condição: Após o cadastro do infrator, o mesmo, já pode ser associado a um Auto de Infração.

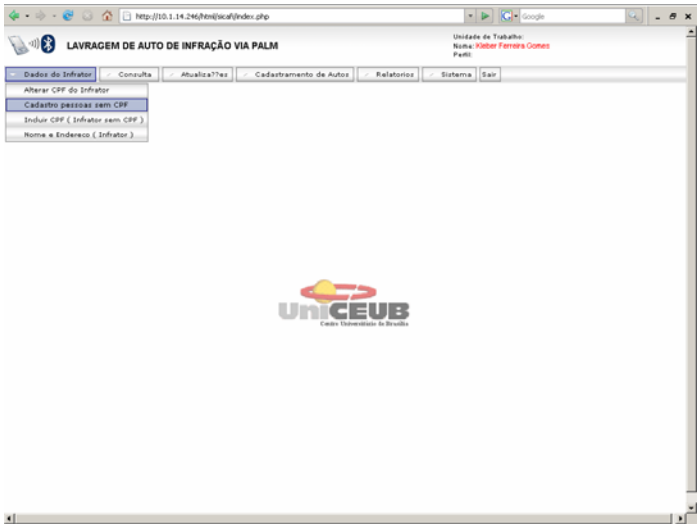


Figura 15 – Selecionando Cadastro Pessoas sem CPF.

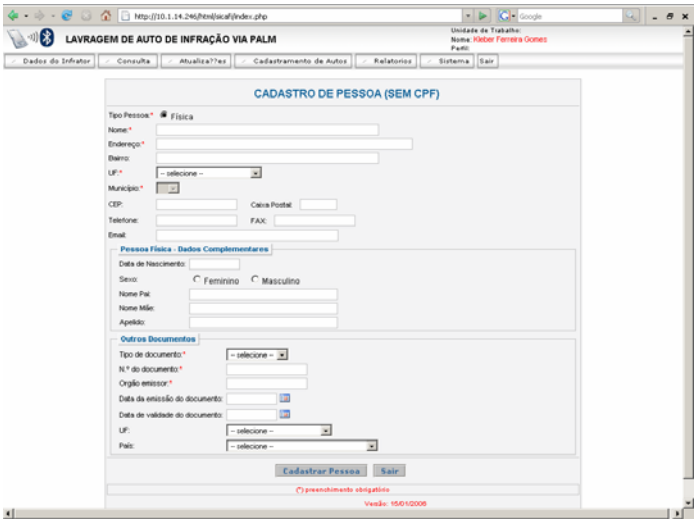


Figura 16 – Tela Cadastro Pessoas sem CPF.

4.4.4 Incluir CPF (Infrator sem CPF)

Representa-se, a seguir, a inclusão do CPF do infrator sem seu registro.



Figura 17 **– Caso de Uso – Incluir CPF (Infrator sem CPF).**

Objetivo: Incluir o CPF no cadastro de um infrator.

Atores participantes: Usuários com perfil Cadastro e Administrador do Sistema.

Pré-condição: Usuário deve estar “Logado” no sistema.

Fluxo Principal: (Incluir CPF).

F1 - Usuário na tela principal seleciona a opção no menu: **Dados do Infrator ➔ Incluir CPF**. (**Tela Selecionando Incluir CPF).**

F2 - Sistema apresenta a **“Tela Incluir CPF/CNPJ para Infrator”**.

F3 - Usuário seleciona a Lupa para realizar a pesquisa.

F4 - Sistema apresenta a ***“Tela Consulta Dinâmica”***.

F5 - Usuário preenche o nome do Infrator e seleciona o botão ***“Pesquisar”***.

F6 - Sistema apresenta os dados do infrator pesquisado. Usuário preenche no campo **CPF/CNPJ** o nº do CPF e seleciona botão **“GRAVAR”**. **“Tela Incluir CPF/CNPJ para Infrator” (E1).**

F7 – Sistema emite mensagem confirmando que o CPF foi incluído com sucesso.

Exceções:

E1 – Infrator não encontrado.

E1.1 - Sistema emite um alerta em forma de mensagem na tela, explicando o erro ao usuário.

Alternativas: Não existem alternativas para este caso de uso.

Pós-condição: Não existe pós-condição para este caso de uso.

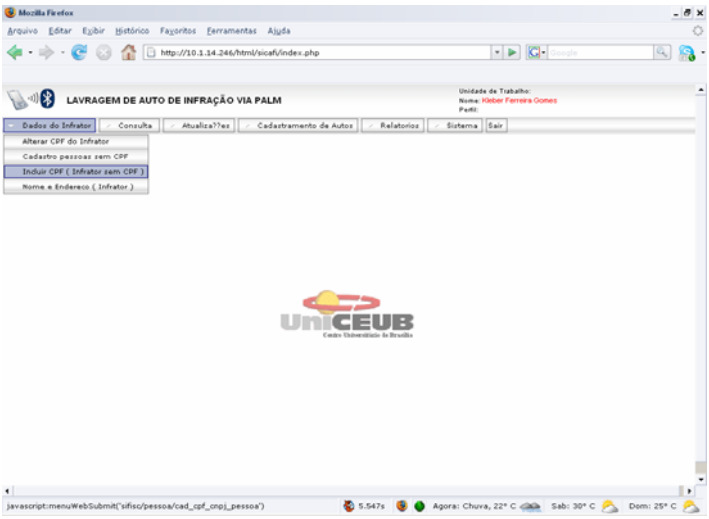


Figura 18 – Selecionando Incluir CPF.

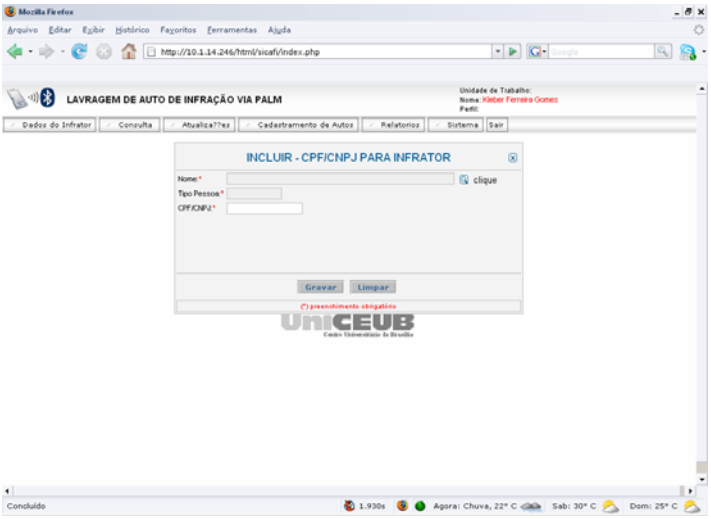


Figura 19 – Tela Incluir CPF/CNPJ para Infrator.



Figura 20 – Tela Consulta Dinâmica.

4.4.5 Alterar dados do Infrator

O objetivo da próxima etapa é demonstrar como se alteram os dados do infrator.



Figura 21 – Caso de Uso – Alterar Dados do Infrator.

Objetivo: Alterar os dados de um infrator.

Atores participantes: Usuários com perfil Cadastro e Administrador do Sistema.

Pré-condição: Usuário deve estar “Logado” no sistema.

Fluxo Principal: (Alterar nome e endereço).

F1 - Usuário na tela principal seleciona a opção no menu: **Dados do Infrator ➔ Nome e Endereço**. (**Tela Selecionando Nome e Endereço).**

F2 - Sistema apresenta a ***“Tela Alterar dados da Pessoa”***.

F3 - Usuário seleciona a Lupa para realizar a pesquisa.

F4 - Sistema apresenta a ***“Tela Consulta Dinâmica”***.

F5 - Usuário preenche o CPF do Infrator e seleciona o botão ***“Pesquisar”***.

F6 - Sistema apresenta os dados do infrator pesquisado. Usuário preenche os dados que deseja alterar e seleciona botão **“GRAVAR”**. **“Tela Alterar dados da Pessoa” (E1).**

F7 – Sistema emite mensagem confirmando que os dados foram alterados com sucesso.

Exceções:

E1 – Infrator não encontrado.

E1.1 - Sistema emite um alerta em forma de mensagem na tela, explicando o erro ao usuário.

Alternativas: Não existem alternativas para este caso de uso.

Pós-condição: Não existe pós-condição para este caso de uso.

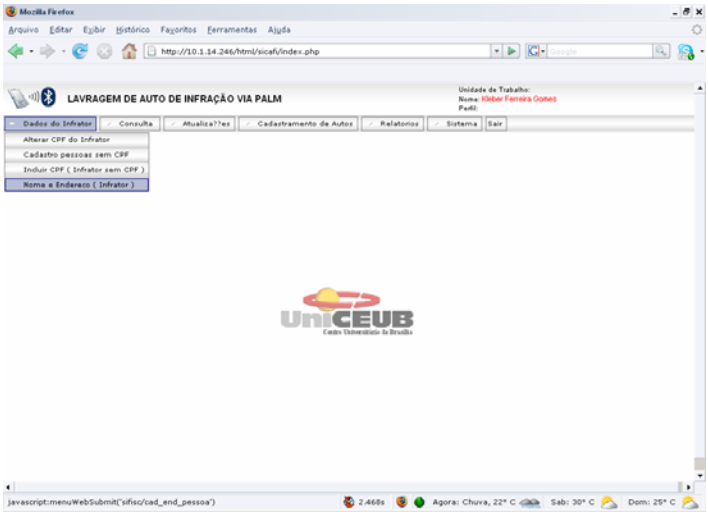


Figura 22 – Selecionando nome e endereço.

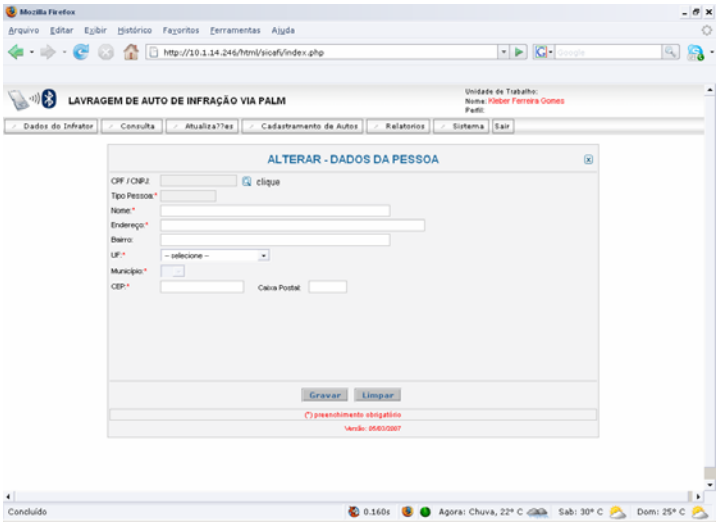


Figura 23 – Tela Alterar Dados da Pessoa.

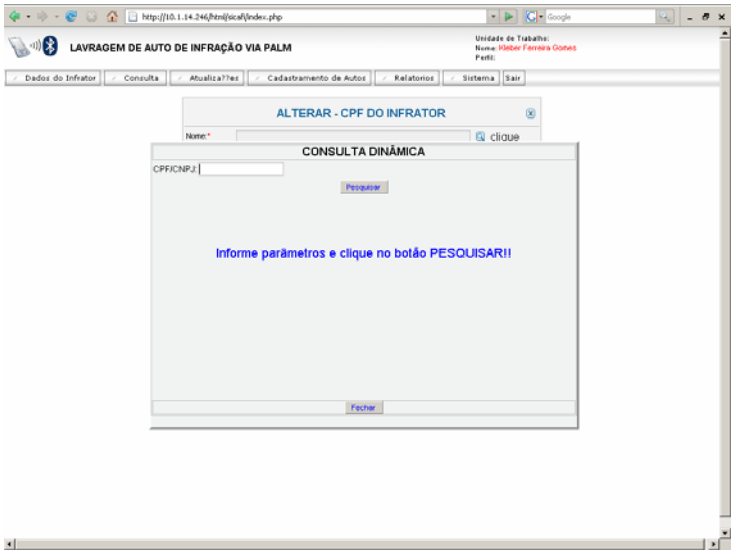


Figura 24 – Tela Consulta Dinâmica.

4.4.6 Consultar Auto de Infração

A seguir, ilustra-se o modo de consulta de um auto de infração.



Figura 25 – Caso de Uso – Consultar auto de infração.

Objetivo: consultar os dados de um auto de infração.

Atores participantes: usuários com perfil, cadastro e administrador do sistema.

Pré-condição: usuário deve estar “Logado” no sistema.

Fluxo Principal: (consultar auto de infração).

F1 - Usuário na tela principal seleciona a opção no menu: **Consulta ➔ Auto de Infração**. (**Tela Selecionando Consulta Auto).**

F2 - Sistema apresenta a ***"Tela Consulta Auto de Infração"***.

F3 – Usuário seleciona a forma de pesquisa e seleciona o botão "*Pesquisar*".

F4 - Sistema apresenta os dados do Auto de Infração pesquisado. (E1)

Exceções:

E1 – Auto de Infração não encontrado.

E1.1 - Sistema emite um alerta em forma de mensagem na tela, explicando o erro ao usuário.

Alternativas: Não existem alternativas para este caso de uso.

Pós-condição: Não existe pós-condição para este caso de uso.



Figura 26 – Tela Selecionando Consulta Auto.

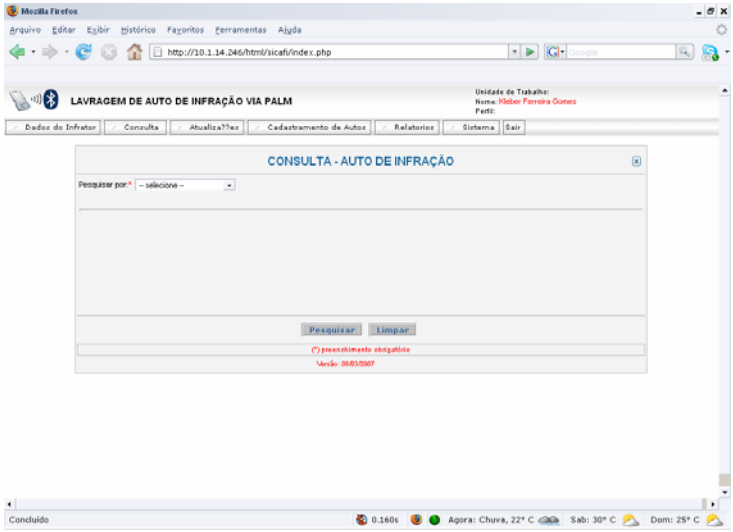


Figura 27 – Tela Consulta Auto de Infração.

4.4.7 Processar Arquivos PALM

Vê-se, a seguir, a ilustração do processamento de arquivos PALM pelo administrador.



Figura 28 – Caso de Uso – Processar Arquivos Palm.

Objetivo: Processar arquivos enviados pelo PALM.

Atores participantes: Administrador do Sistema.

Pré-condição: Usuário deve estar “Logado” no sistema.

Fluxo Principal: (Processar arquivo PALM).

F1 - Usuário na tela principal seleciona a opção no menu: **Atualizações ➔ Processar arquivos PALM**. (**Tela Selecionando opção Processar arquivos PALM).**

F2 - Sistema apresenta a ***"*Tela PROCESSAR ARQUIVOS PALM*"***.

F3 – Usuário seleciona o botão "***Arquivo***", seleciona a pasta de origem do arquivo e o arquivo que deseja processar. (A1) (A2)

F4 - Usuário seleciona o botão "***Gravar***".(E1)

F5 – Sistema emite mensagem confirmando que o arquivo foi processado com sucesso.

Exceções:

E1 – Arquivo corrompido ou formato inválido.

E1.1 - Sistema emite um alerta em forma de mensagem na tela, explicando o erro ao usuário.

Alternativas:

A1 – Usuário seleciona o ícone "***Lixeira***" no gride de arquivos processados.

A1.1 – Sistema emite mensagem confirmando que o arquivo foi excluído com sucesso.

A2 – Usuário seleciona o ícone "***Editar***" no gride de arquivos processados.

A2.1 – Sistema abre o arquivo para edição e visualização.

A2.2 – Usuário realiza as alterações e seleciona botão "***Gravar***".

A2.3 – Sistema emite mensagem confirmando atualização.

Pós-condição: Não existe pós-condição para este caso de uso.

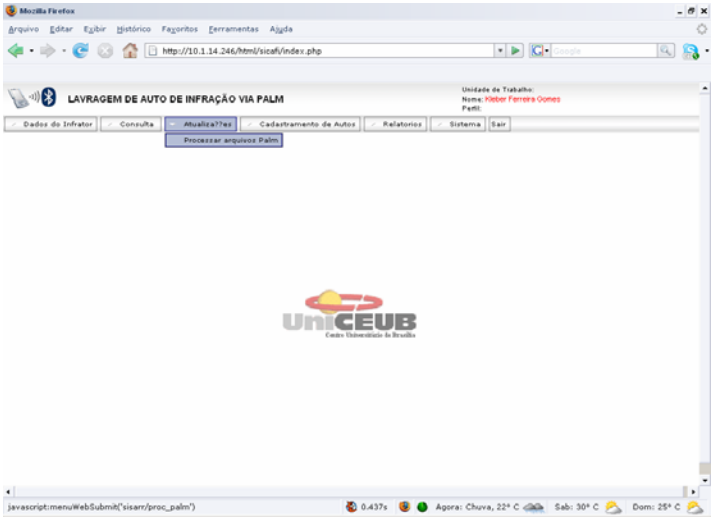


Figura 29 – Tela Selecionando opção Processar arquivos PALM.

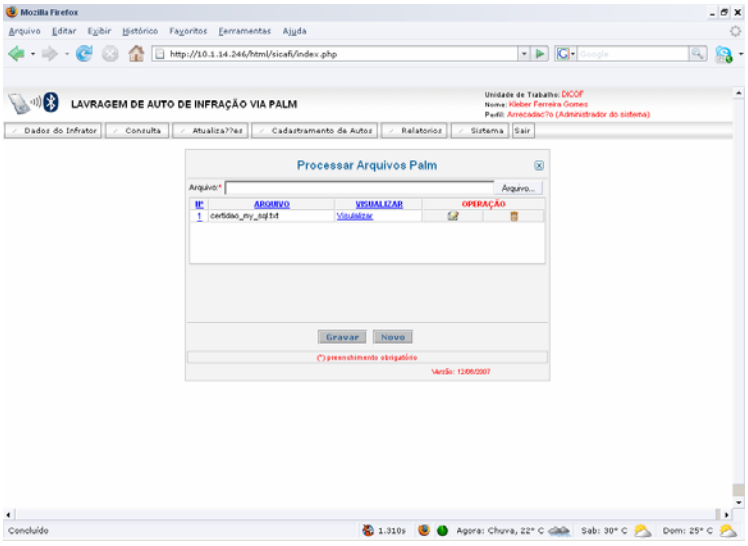


Figura 30 – Tela Processar arquivos PALM.

4.4.8 Alterar dados de um Auto de Infração

Mostra-se a seguir como se alteram os dados de um auto de infração.



Figura 31 – Caso de Uso – Alterar dados de um Auto de Infração.

Objetivo: Alterar dados de um auto de infração.

Atores participantes: Usuários com perfil Cadastro e Administrador do Sistema.

Pré-condição: Usuário deve estar "Logado" no sistema.

Fluxo Principal: (Alterar dados de um Auto de Infração).

F1 - Usuário na tela principal seleciona a opção no menu: **Cadastramento de Autos ➔ Auto de Infração**. (**Tela Selecionando opção Cadastro de Autos).**

F2 - Sistema apresenta a ***"Tela CADASTRO AUTO INFRAÇÃO"***.

F3 – Usuário seleciona a lupa para pesquisar o Auto de Infração.

F4 – Sistema apresenta tela de pesquisa dinâmica.

F5 – Usuário entra com o nº de Auto e Série.

F6 – Sistema apresenta os dados do Auto de Infração. (E1)

F7 – Usuário realiza as alterações e seleciona o botão "***Gravar Auto***".

F8 – Sistema emite mensagem confirmando atualização.

Exceções:

E1 – Auto de Infração não encontrado.

E1.1 - Sistema emite um alerta em forma de mensagem na tela, explicando o erro ao usuário.

Alternativas: não existem alternativas para este caso de uso.

Pós-condição: não existe pós-condição para este caso de uso.

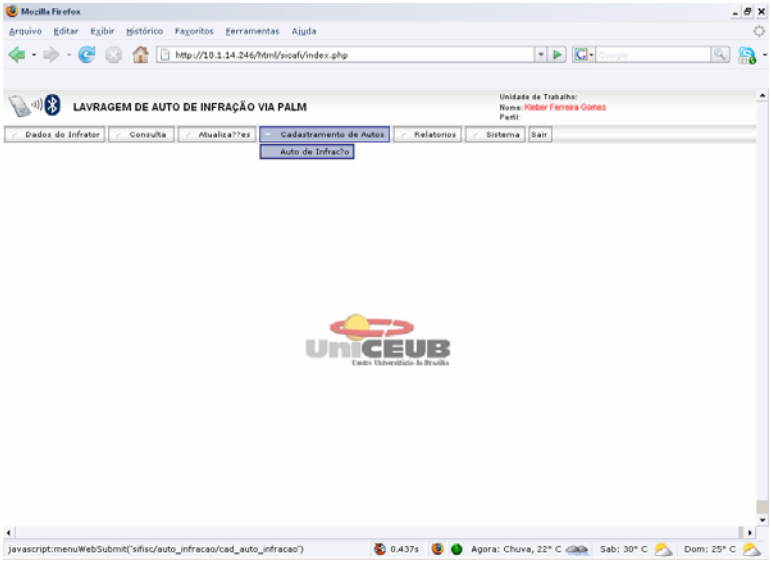


Figura 32 – Tela Selecionando opção Cadastro de Auto de Infração.

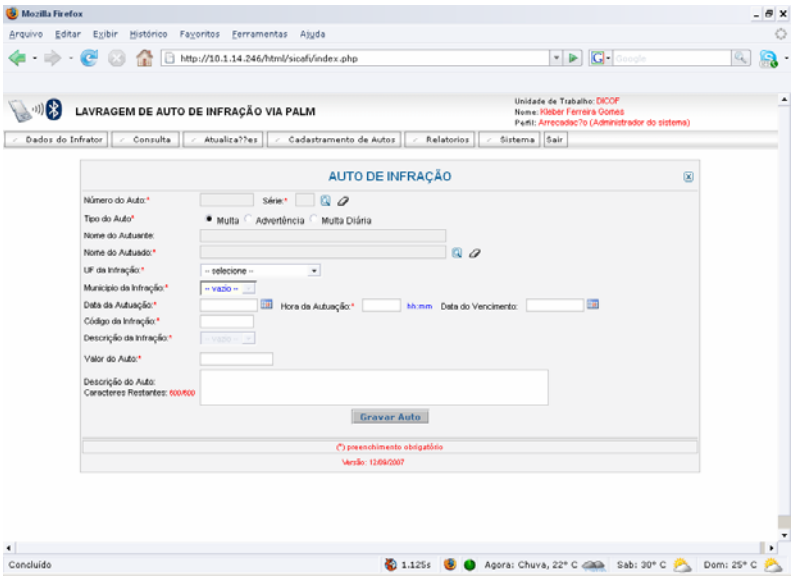


Figura 33 – Tela Cadastro de Auto de Infração.

4.4.9 Relatórios de Auto de Infração por Estado

Abaixo, representa-se o modo de emissão de relatório de auto de infração por estado.



Figura 34 – Caso de Uso – Relatórios de auto de infração por estado.

Objetivo: emitir relatórios auto infração por estado.

Atores participantes: Usuários com perfil Cadastro e Administrador do Sistema.

Pré-condição: Usuário deve estar "Logado" no sistema.

Fluxo Principal: (Emitir relatórios Auto Infração por Estado).

F1 - Usuário na tela principal seleciona a opção no menu: **Relatórios ➔ Auto de Infração ➔ Por Estado**. (**Tela Selecionando Relatórios por Estado).**

F2 - Sistema apresenta a **"Tela RELATÓRIO AUTO DE INFRAÇÃO POR ESTADO"**.

F3 – Usuário preenche os argumentos de pesquisa e seleciona o botão "***Visualizar Relatório***". (E1)

F4 – Sistema apresenta relatório em PDF.

Exceções:

E1 – Nenhum Auto de Infração foi encontrado com os argumentos de pesquisa.

E1.1 - Sistema emite um alerta em forma de mensagem na tela, explicando o erro ao usuário.

Alternativas: Não existem alternativas para este caso de uso.

Pós-condição: Não existe pós-condição para este caso de uso.

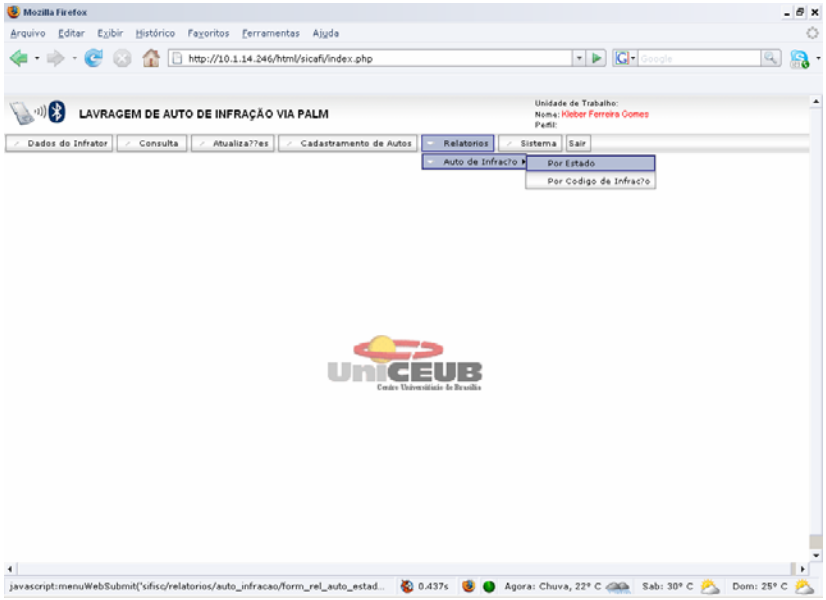


Figura 35 – Tela Selecionando Opção Relatórios por Estado.

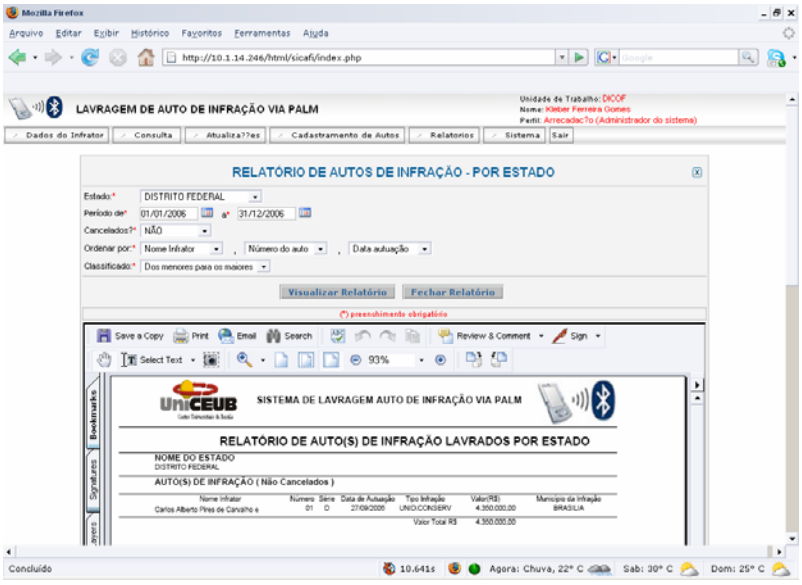


Figura 36 – Tela Relatórios Auto de Infração por Estado.

4.4.10 Relatórios de Auto de Infração por Código de Infração

Os relatórios de auto de infração de acordo com o código são elaborados nessa etapa dos procedimentos.



Figura 37 – Caso de Uso – Relatórios de Auto de Infração por Código de Infração.

Objetivo: Emitir relatórios Auto Infração por Código Infração.

Atores participantes: Usuários com perfil Cadastro e Administrador do Sistema.

Pré-condição: Usuário deve estar "Logado" no sistema.

Fluxo Principal: (Emitir relatórios Auto Infração por Código de Infração).

F1 - Usuário na tela principal seleciona a opção no menu: **Relatórios ➔ Auto de Infração ➔ Por Código Infração**. (**Tela Selecionando Relatórios por Código).**

F2 - Sistema apresenta a **"Tela RELATÓRIO AUTO DE INFRAÇÃO POR CÓDIGO"**.

F3 – Usuário preenche os argumentos de pesquisa e seleciona o botão "***Visualizar Relatório***". (E1)

F4 – Sistema apresenta relatório em PDF.

Exceções:

E1 – Nenhum Auto de Infração foi encontrado com os argumentos de pesquisa.

E1.1 - Sistema emite um alerta em forma de mensagem na tela, explicando o erro ao usuário.

Alternativas: Não existem alternativas para este caso de uso.

Pós-condição: Não existe pós-condição para este caso de uso.

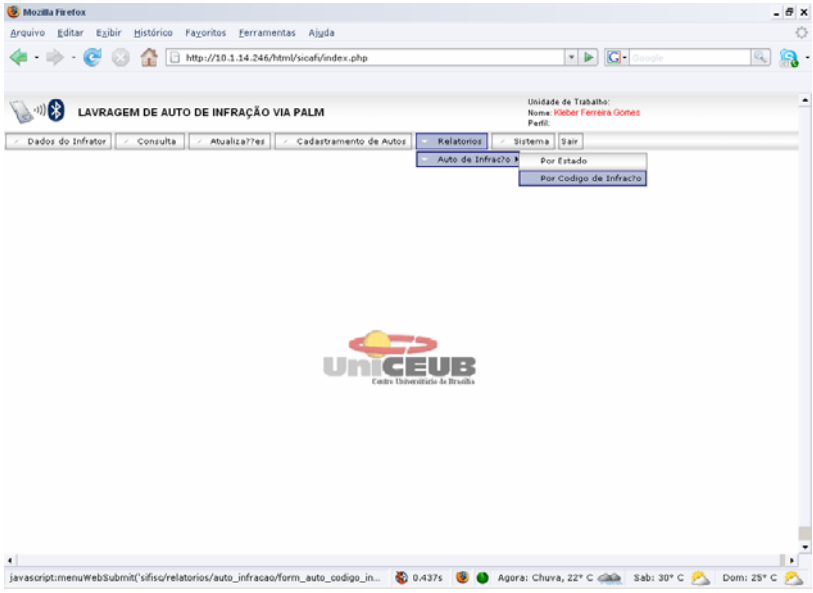


Figura 38 – Tela Selecionando Opção Relatórios por Código de Infração.

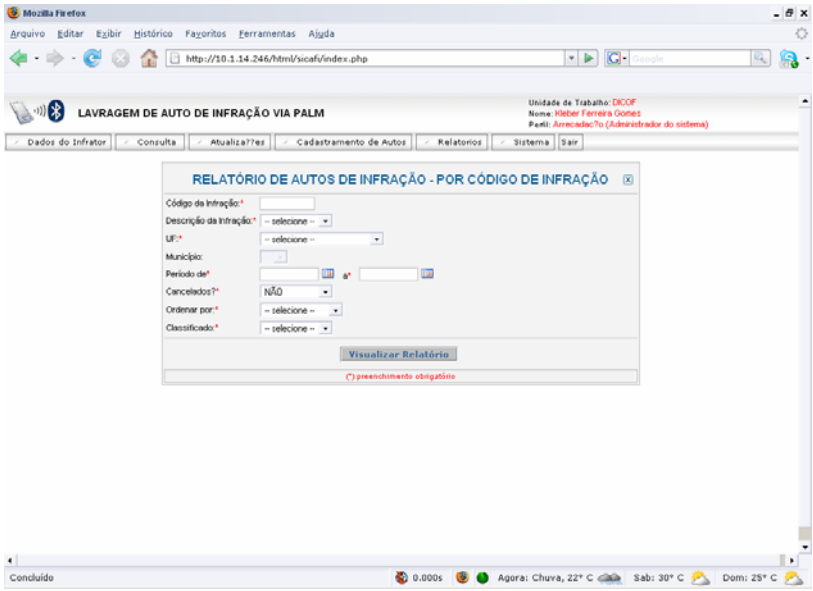


Figura 39 – Tela Relatórios Auto de Infração por Código de Infração.

4.5 Descrição dos casos de uso da aplicação em CASL

A figura abaixo especifica as principais funcionalidades da aplicação em PALM.

Principais Funcionalidades da Aplicação em PALM

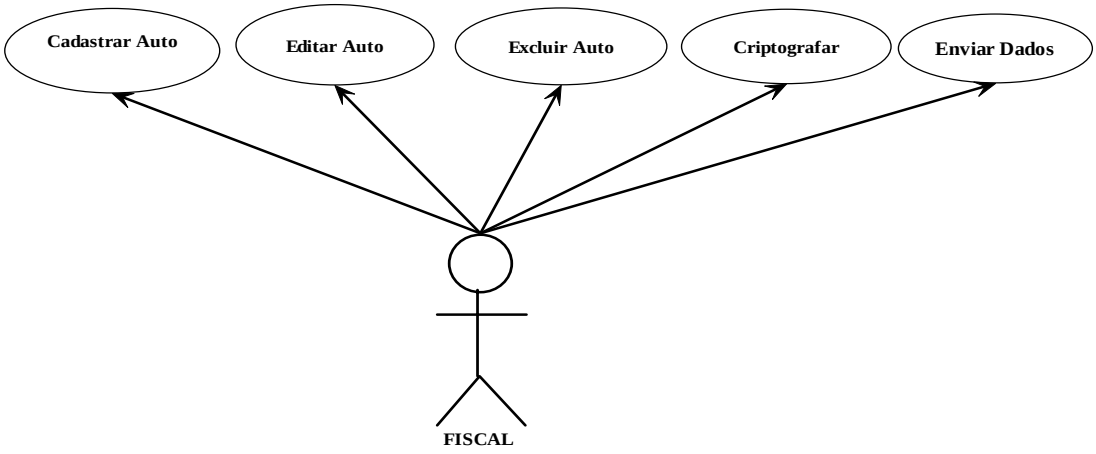


Figura 56 - Diagrama de Casos de Uso da Aplicação em Casl.

4.5.1 Cadastrar Auto de Infração

A seguir, apresentamos a figura esquemática de como se proceder ao cadastramento de um auto de infração.



Figura 41 – Caso de Uso – Cadastrar Auto de Infração.

Objetivo: cadastrar autos de Infração.

Atores participantes: usuários utilizadores do Palm

Pré-condição: Usuário deve estar “Logado” no sistema.

Fluxo Principal: (Cadastrar Auto de Infração).

F1 - Usuário na tela principal seleciona a opção no menu: **Auto de Infração ➔ Cadastrar**. (**Tela Selecionando Cadastrar Auto de Infração).**

F2 - Sistema apresenta a ***“Tela Cadastrar”***.

F3 - Usuário preenche dados do auto de infração, gera criptografia e seleciona o botão: “***Gravar***”.

F4 – Sistema emite mensagem confirmando que o auto de infração foi cadastrado com sucesso.

Exceções: Não existem exceções para este caso de uso.

Alternativas: Não existem alternativas para este caso de uso.

Pós-condição: Após o cadastro do auto de infração, o mesmo encontra – se disponibilizado para manipulação.

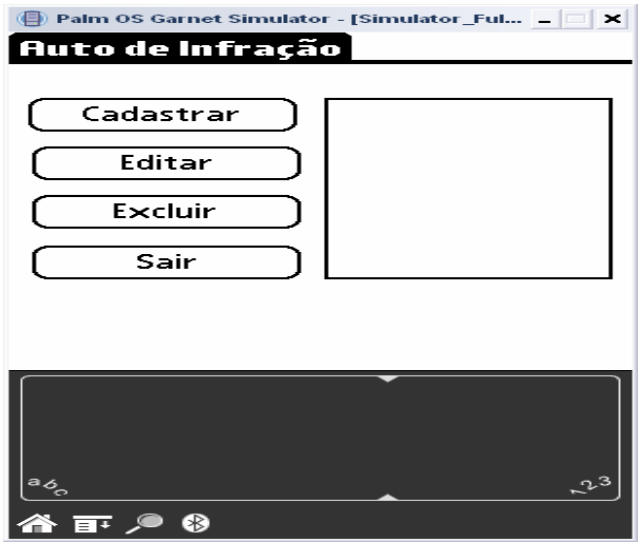


Figura 42 – Tela Auto de Infração.

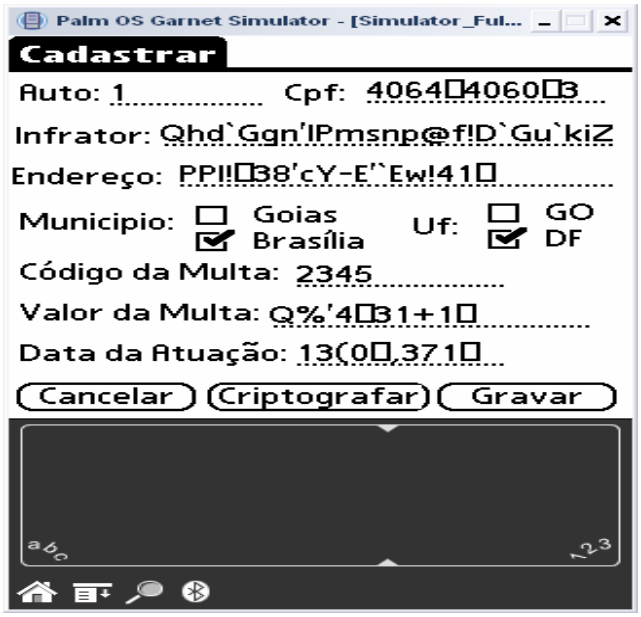


Figura 43 – Tela Cadastrar Auto de Infração.

4.5.2 Editar Auto de Infração

Abaixo, representa-se a edição de um auto de infração pelo fiscal.



Figura 44 – Caso de Uso – Editar Auto de Infração.

Objetivo: editar autos de Infração.

Atores participantes: usuários utilizadores do Palm

Pré-condição: auto de Infração deve estar cadastrado no sistema.

Fluxo Principal: (editar auto de infração).

F1 - Usuário na tela principal seleciona a opção no menu: **Auto de Infração ➔ Editar**. (**Tela Selecionando Editar Auto de Infração).**

F2 - Sistema apresenta a ***"Tela Editar"***.

F3 - Usuário altera dados do auto de infração, gera criptografia e seleciona o botão: "***Gravar***".

F4 – Sistema emite mensagem confirmando que o auto de infração foi alterado com sucesso.

Exceções: Não existem exceções para este caso de uso.

Alternativas: Não existem alternativas para este caso de uso.

Pós-condição: Após o cadastro do auto de infração, o mesmo encontra – se disponibilizado para manipulação.



Figura 45 – Tela Editar de Autos de Infração.



Figura 46 – Tela de Editar Auto de Infração.

4.5.3 Excluir Auto de Infração

Abaixo, representa-se a ação de exclusão de um auto de infração.



Figura 47 – Caso de Uso – Excluir Auto de Infração.

Objetivo: Excluir Autos de Infração.

Atores participantes: Usuários utilizadores do Palm

Pré-condição: Auto de Infração deve estar cadastrado no sistema.

Fluxo Principal: (Excluir Auto de Infração).

F1 - Usuário na tela principal seleciona a opção no menu: **Auto de Infração ➔ Excluir**. (**Botão Excluir Auto de Infração).**

F2 - Sistema apresenta a mensagem ***"Deletar Auto"***.

F3 - Usuário exclui auto de infração seleciona o botão: "***Sim***".

F4 – Sistema emite mensagem confirmando que o auto de infração foi excluído com sucesso.

Exceções: Não existem exceções para este caso de uso.

Alternativas: Não existem alternativas para este caso de uso.

Pós-condição: Após a exclusão do auto de infração, será necessário cadastro do mesmo para posterior manipulação.



Figura 48 – Tela de Exclusão de Auto de Infração.

4.6 Softwares Gratuitos Utilizados

Abaixo, apresenta-se a tela de softwares gratuitos utilizados para envio de arquivos via Bluetooh e sua conversão para formato txt.

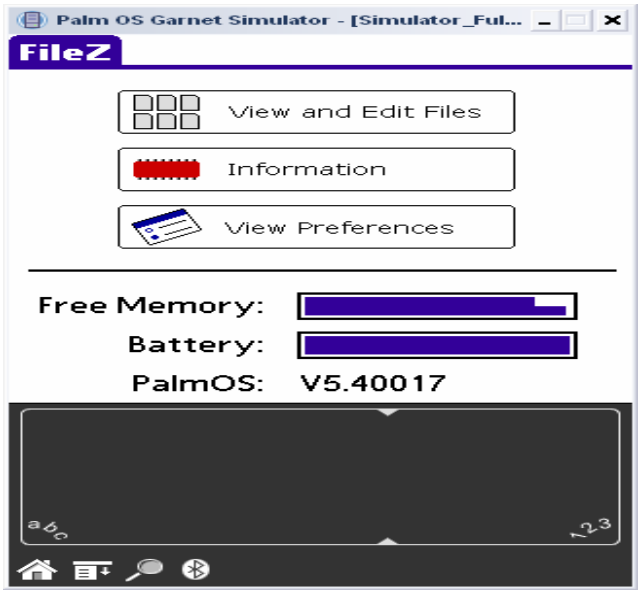


Figura 49 – Programa Filez – Envio de Arquivo via Bluetooh.

Na figura 49, acima, é demonstrado o uso do software Filez, esse é um software gratuito que envia qualquer arquivo contido no Palm. Esse software foi utilizado, pois a versão da programação Casl 4.3, apesar de possuir biblioteca bluetooh, não envia arquivos binários para dispositivos bluetooh, apenas abre e fecha a porta serial virtual de dispositivos bluetooth. Para a próxima versão está prevista a funcionalidade de envio de arquivos binários. A figura 50 demonstra o arquivo de banco de dados em palm sendo selecionado para envio. Na figura 51, verifica – se que o sistema fileZ possibilita opções de envio do arquivo, no caso do projeto será utilizado o de Bluetooth. Na figura 52, pode–se observar que o sistema usa a porta serial virtual para localizar dispositivos bluetooth próximos do palmtop.

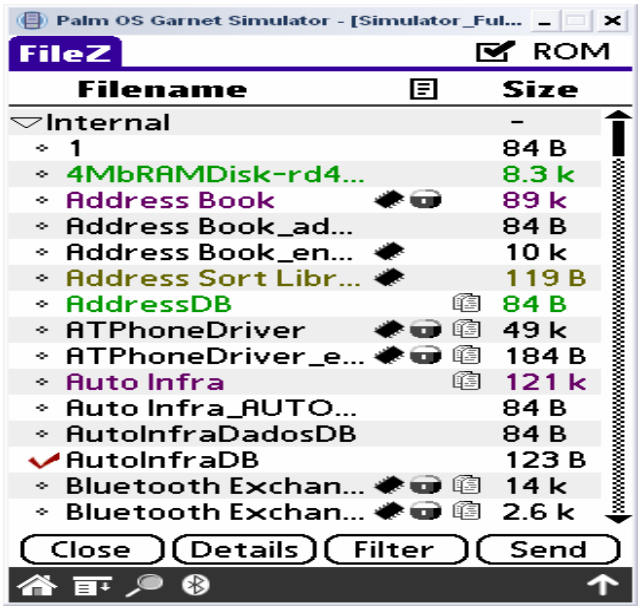


Figura 50 – Programa Filez – Selecionando Arquivo para envio.

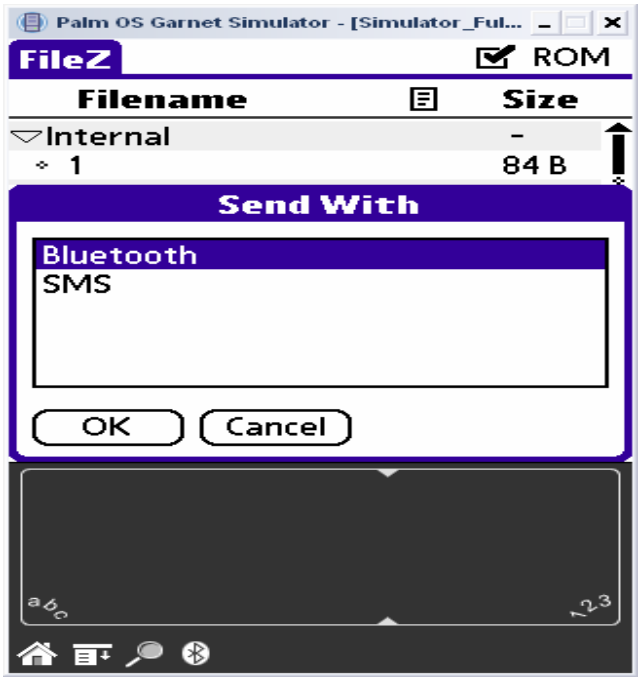


Figura 51 – Programa Filez – Enviando Arquivo via Bluetooth.



Figura 52 – Programa Filez – Detectando Dispositivos Bluetooh.

Após a seleção do dispositivo Bluetooh conforme demonstrado na figura 52, o arquivo é enviado conforme ilustrado na figura 53.



Figura 53 – Programa Filez – Enviando Arquivo.

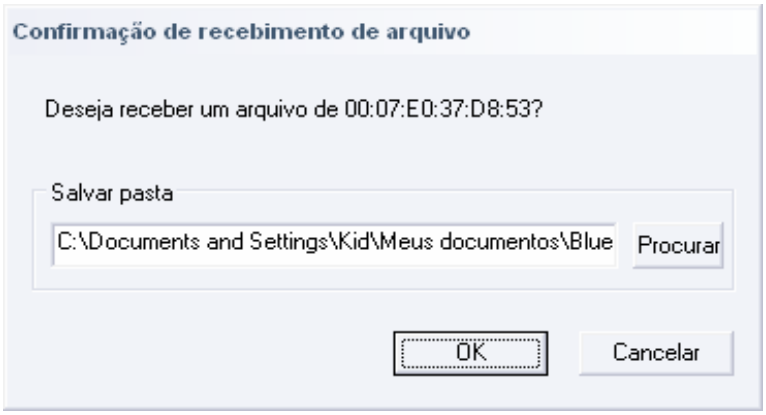


Figura 54 – Confirmação de Recebimento de Arquivo.

No notebook ou desktop aparecerá uma mensagem solicitando recebimento do arquivo enviado por parte do palm conforme demonstrado na figura 54.

Para possibilitar o envio do arquivo, o notebook ou desktop deve ser configurado. Para tanto as seguintes configurações no sistema operacional Windows devem ser feitas:



Figura 55 – Configurações do Windows.

Depois de pressionado o botão opções da tela demonstrada na figura 55, serão apresentadas várias opções de configuração tais como: Geral, Segurança e Intercambio de informações Bluetooth, Outras e Diagnóstico. Para o projeto só serão utilizadas as opções Geral e Segurança. Para a opção geral devem ser mantidas as configurações conforme ilustrado na figura 56.

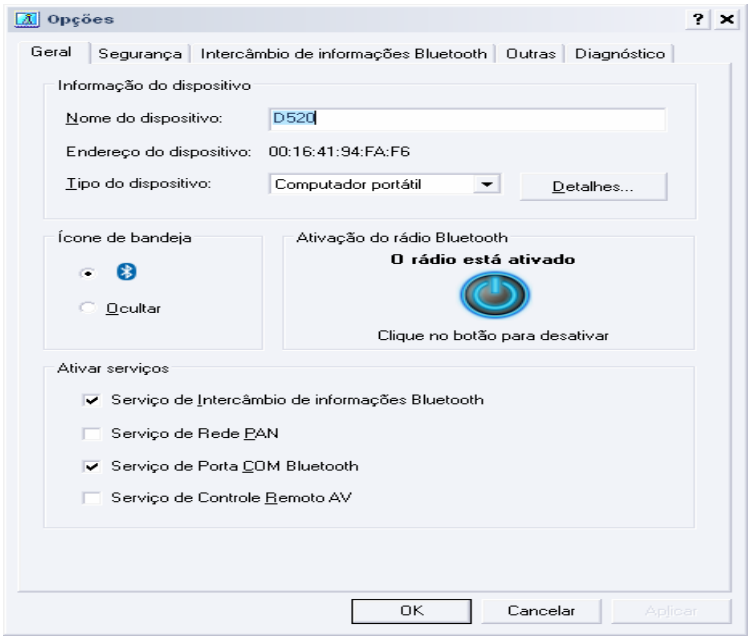


Figura 56– Configurações do Windows - Geral.

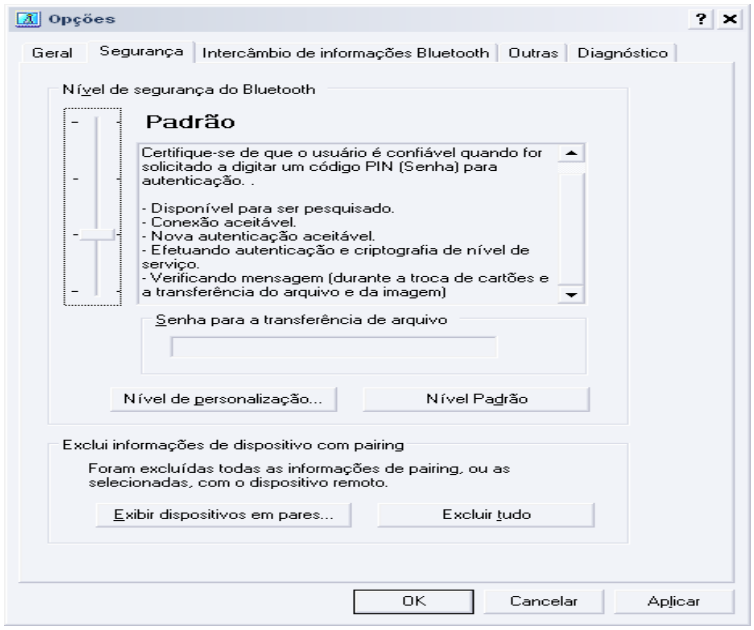


Figura 57 – Configurações do Windows - Padrão.

Conforme demonstrado na figura 57, o nível de segurança deve ser o padrão, pois além de requerer senha de acesso, disponibiliza o notebook ou desktop para a rede ad-hoc bluetooth.

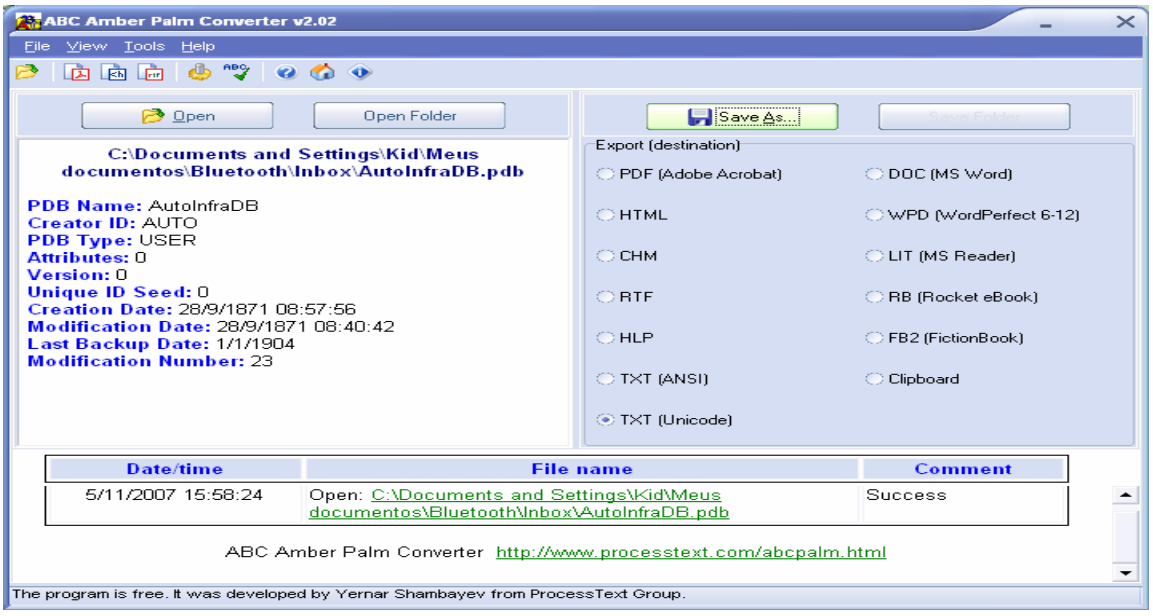


Figura 58 – Programa conversor de arquivo na extensão txt.

Na figura 58 pode–se verificar a conversão do arquivo de banco de dados de palm para qualquer formato desejável. No caso do projeto, será utilizado o formato txt. Importante salientar aqui, que embora seja possível fazer a conversão do arquivo para qualquer formato das opções acima ilustradas, o conteúdo do arquivo continua criptografado, esse, só será discriptografado quando for feito o carregamento do mesmo no aplicativo em php.

4.7 Testes e Resultados

Os testes foram feitos nas aplicações em Php e Casl visando identificar possíveis falhas de preenchimento, edição, deleção, validação, criptografia e transmissão de dados.

4.7.1 Preenchimento de Dados em Casl

Para esta etapa de testes foi tomado como base o módulo de Cadastrar. No primeiro teste foi feito o preenchimento de todos os campos do formulário de um auto de infração no sistema em Casl visando verificar o cadastro das informações.

As informações utilizadas para o cadastro foram:

- **N° do Auto:** 1;
- **Cpf:** 0161361784;
- **Infrator:** Carlos Alberto Pires;
- **Endereço**: ROD GAL EURYALE J ZERBINI;
- **Município:** Brasília;
- **Uf:** DF;
- **Código da multa**: 812001;
- **Valor da multa:** 4350000;
- **Data da Atuação:** 22/09/2006.

O teste e resultados podem ser verificados na tabela 1 ilustrada abaixo:

Teste	Resultado Esperado	Resultado Obtido
Preenchimento de dados	Sucesso no cadastro das informações	Sucesso no cadastro das informações

Tabela 1 – Primeiro teste de preenchimento de dados em Casl.

Um segundo teste visando verificação de cadastro foi feito dessa vez não foi digitado nenhum campo no formulário do auto de infração.

O teste e resultados podem ser verificados na tabela 2 ilustrada abaixo:

Teste	Resultado Esperado	Resultado Obtido
Não preenchimento de dados	Erro ao tentar cadastrar as informações	Erro ao tentar cadastrar as informações

Tabela 2 – Segundo teste preenchimento de dados em Casl.

Um terceiro teste foi feito visando verificar cadastro do auto de infração dessa vez foi preenchido apenas o campo auto do formulário de cadastro de auto de infração.

A informação utilizada para o cadastro foi:

- **N° do Auto:** 1.

O teste e resultados podem ser verificados na tabela 3 ilustrada abaixo:

Teste	Resultado Esperado	Resultado Obtido
Preenchimento do campo auto no formulário	Erro ao tentar cadastrar as informações	Sucesso no cadastro da informação

Tabela 3 – Terceiro teste preenchimento de dados em Casl.

4.7.2 Preenchimento de Dados em Php

Para esta etapa de testes foram tomados como base os módulos Dados do Infrator e Cadastramento de Autos, os testes foram feitos nos submódulos: Alterar CPF do Infrator, Cadastro Pessoas sem CPF, Incluir CPF (Infrator sem Cpf), Alterar Nome e endereço (Infrator), referentes ao módulo Dados do Infrator e o submódulo Auto de Infração referente ao módulo Cadastramento de Autos.

O primeiro teste foi feito no submódulo Alterar CPF do infrator. Nesse, foram verificadas as críticas do sistema para o não preenchimento dos campos obrigatórios. Foram feitas duas tentativas de alteração do Cpf do infrator, uma sem dados e a outra com os dados do mesmo.

As informações utilizadas para o cadastro foram:

- **Nome:** Kleber Ferreira Gomes;
- **CPF atual**: 60260238104;
- **Tipo pessoa**: Física;
- **CPF:** 1234567809.

Os testes e resultados podem ser verificados na tabela 4.ilustrada abaixo:

Teste	Resultado Esperado	Resultado Obtido
Não preenchimento de dados	Erro ao tentar cadastrar as informações	Erro ao tentar cadastrar as informações
Preenchimento de dados	Sucesso no cadastro das informações	Sucesso no cadastro das informações

Tabela 4 – Primeiro teste preenchimento de dados em Php – Módulo Dados do Infrator-Submódulo Alterar CPF do Infrator.

O segundo teste foi feito no submódulo Cadastro de Pessoa (SEM CPF). Nesse teste, foram verificadas as críticas do sistema para o não preenchimento dos campos obrigatórios. Foram feitas duas tentativas de cadastro de pessoa uma sem dados e outra com os dados obrigatórios.

As informações utilizadas para o cadastro foram:

- **Nome:** Ricardo Henrique Carvalho de Oliveira;
- **Endereço**: SQN 209 bl D apt 301;
- **UF**: Distrito Federal;
- **Tipo de Documento:** RG;
- **N° do Documento:** 2096094;
- **Órgão Emissor:** SSP-DF.

Os testes e resultados podem ser verificados na tabela 5 ilustrada abaixo:

Teste	Resultado Esperado	Resultado Obtido
Não preenchimento de dados	Erro ao tentar cadastrar as informações	Erro ao tentar cadastrar as informações
Preenchimento de dados	Sucesso no cadastro das informações	Sucesso no cadastro das informações

Tabela 5 – Segundo teste preenchimento de dados em Php – Módulo Dados do Infrator-Submódulo Cadastro de Pessoa (SEM CPF)

O terceiro teste foi feito no submódulo Incluir – CPF/CNPJ para infrator. Nesse teste, foram verificadas as críticas do sistema para o não preenchimento dos campos obrigatórios. Foram feitas duas tentativas de inclusão de cpf para o infrator uma sem dados e outra com dados obrigatórios.

As informações utilizadas para o cadastro foram:

- **Nome:** Nelson Gonçalves Rezende;
- **Tipo Pessoa**: Física;
- **CPF/CNPJ**: 59948337700.

Os testes e resultados podem ser verificados na tabela 6 ilustrada abaixo:

Teste	Resultado Esperado	Resultado Obtido
Não preenchimento de dados	Erro ao tentar cadastrar as informações	Erro ao tentar cadastrar as informações
Preenchimento de dados	Sucesso no cadastro das informações	Sucesso no cadastro das informações

Tabela 6 – Terceiro teste preenchimento de dados em Php – Módulo Dados do Infrator-Submódulo Incluir – CPF/CNPJ

O quarto teste foi feito no submódulo Alterar Nome e endereço (Infrator). Nesse teste, foram verificadas as críticas do sistema para o não preenchimento dos campos obrigatórios. Foram feitas duas tentativas de alteração de dados da pessoa uma sem dados e outra com dados obrigatórios.

As informações utilizadas para o cadastro foram:

- **CPF/CNPJ:** 60260238104;
- **Tipo Pessoa**: Física;
- **Nome**: Kleber Ferreira Gomes;
- **Endereço:** SQN 215 BLOCO J apt 601;
- **Bairro:** ASA NORTE
- **Município:** BRASÍLIA
- **CEP:** 12300000

Os testes e resultados podem ser verificados na tabela 7 ilustrada abaixo:

Teste	Resultado Esperado	Resultado Obtido
Não preenchimento de dados	Erro ao tentar cadastrar as informações	Erro ao tentar cadastrar as informações
Preenchimento de dados	Sucesso no cadastro das informações	Sucesso no cadastro das informações

Tabela 7 – Quarto teste preenchimento de dados em Php – Módulo Dados do Infrator-Submódulo Alterar Nome e Endereço (Infrator)

O Quinto teste foi feito no submódulo Auto de Infração. Nesse teste, foram verificadas as críticas do sistema para o não preenchimento dos campos obrigatórios.

Foram feitas duas tentativas de alteração de dados de auto de infração uma sem dados e outra com dados obrigatórios.

As informações utilizadas para alteração de dados foram:

- **Número do Auto:** 1;
- **Série:** D;
- **Tipo do Auto**: Multa;
- **Nome do Autuante**: Ricardo Henrique Carvalho de Oliveira;
- **Nome do Autuado:** Kleber Ferreira Gomes;
- **UF da Infração:** GOIAS;
- **Município da Infração:** GOIAS;
- **Data da Autuação:** 01/02/2007;
- **Código da Infração:** 405001;
- **Descrição da Infração:** Vender (Exportar) madeira serrada;
- **Valor do Auto:** 1.500,00;
- **Descrição do Auto:** Este é um teste, estou fazendo alterações;

Os testes e resultados podem ser verificados na tabela 8 ilustrada abaixo:

Teste	Resultado Esperado	Resultado Obtido
Não preenchimento de dados	Erro ao tentar cadastrar as informações	Erro ao tentar cadastrar as informações
Preenchimento de dados	Sucesso no cadastro das informações	Sucesso no cadastro das informações

Tabela 8 – Quinto teste preenchimento de dados em Php – Módulo Cadastramento de Autos-Submódulo Auto Infração.

4.7.3 Edição de Dados em Casl

Para esta etapa de testes foi tomado como base o módulo de Editar. No primeiro teste foi feita a edição com o preenchimento de todos os campos do formulário de um auto de infração, com exceção do campo auto que não pode ser alterado, no sistema em Casl visando verificar a edição das informações.

As informações utilizadas para o cadastro foram:

- **N° do Auto:** 1;
- **CPF:** 0161361784;

- **Infrator:** Carlos Alberto Pires;
- **Endereço**: ROD GAL EURYALE J ZERBINI;
- **Município:** Brasília;
- **Uf:** DF;
- **Código da multa**: 812001;
- **Valor da multa:** 4350000;
- **Data da Atuação:** 22/09/2006.

- **N° do Auto:** 2;
- **CPF:** 60260238104;
- **Infrator:** Kleber Ferreira Gomes;
- **Endereço**: SQN 215 BLOCO J apt 601;
- **Município:** Brasília;
- **Uf:** DF;
- **Código da multa**: 812001;
- **Valor da multa:** 10000000;
- **Data da Atuação:** 03/05/2007.

O teste e resultados podem ser verificados na tabela 9 ilustrada abaixo:

Teste	Resultado Esperado	Resultado Obtido
Edição de dados	Sucesso na edição das informações	Sucesso na edição das informações do último auto de infração lavrado

Tabela 9 – Primeiro teste de Edição de dados em Casl.

4.7.4 Deletação de Dados em Casl

Para esta etapa de testes foi tomado como base o módulo de Excluir. No primeiro teste foi feita a exclusão de dois autos de infração no sistema em Casl visando verificar a exclusão das informações.

As informações utilizadas para a exclusão foram:

- **N° do Auto:** 1;
- **N° do Auto:** 2;

O teste e resultados podem ser verificados na tabela 10 ilustrada abaixo:

Teste	Resultado Esperado	Resultado Obtido
Deleção de autos de infração	Sucesso na exclusão dos autos de infração	Sucesso na exclusão dos autos de infração

Tabela 10 – Primeiro teste de Deleção de auto de infração em Casl.

4.7.5 Deletação do Arquivo AutoInfraDB.txt em Php

Para esta etapa de testes foi tomado como base o módulo de Atualizações e submódulo Processar Arquivos Palm. No primeiro teste foi feita a exclusão do arquivo AutoInfraDB.txt.

As informações utilizadas para a exclusão foram:

- **N°:** 1;
- **ARQUIVO:** AutoInfraDB.txt;
- **OPERAÇÃO:** Excluir Registro;

O teste e resultados podem ser verificados na tabela 11 ilustrada abaixo:

Teste	Resultado Esperado	Resultado Obtido
Deleção do arquivo AutoInfraDB.txt	Sucesso na exclusão do arquivo AutoInfraDB.txt	Sucesso na exclusão do arquivo AutoInfraDB.txt

Tabela 11 – Primeiro teste de Deleção do arquivo AutoInfraDB.txt em Php.

4.7.6 Criptografia de Dados em Casl

Para esta etapa de testes foram tomados como base os módulos Cadastra e Editar. No primeiro teste foi feita a criptografia dos dados de infração no sistema em Casl visando verificar a criptografia das informações.

As informações utilizadas para a exclusão foram:

- **N° do Auto:** 1;
- **Cpf:** 0161361784;
- **Infrator:** Carlos Alberto Pires;
- **Endereço**: ROD GAL EURYALE J ZERBINI;
- **Município:** Brasília;
- **Uf:** DF;

- **Código da multa**: 812001;
- **Valor da multa:** 4350000;
- **Data da Atuação:** 22/09/2006.

O teste e resultados podem ser verificados na tabela 12 ilustrada abaixo:

Teste	Resultado Esperado	Resultado Obtido
Criptografia de dados	Sucesso na criptografia dos dados	Sucesso na criptografia dos dados

Tabela 12 – Primeiro teste de Criptografia de dados em Casl.

4.7.7 Descriptografia de Dados em Php

Para esta etapa de testes foram tomados como base o módulo de Atualizações e submódulo Processar Arquivos Palm. No primeiro teste foram feitos os carregamentos de dados completos criptografados de um auto de infração e de dados incompletos criptografados no sistema em Php visando verificar a descriptografia das informações.

As informações utilizadas para a exclusão foram:

- **N°:** 1;
- **ARQUIVO:** AutoInfraDB.txt;
- **OPERAÇÃO:** Gravar;

- **N°:** 2;
- **ARQUIVO:** AutoInfraDB_1.txt;
- **OPERAÇÃO:** Gravar;

O teste e resultados podem ser verificados na tabela 13 ilustrada abaixo:

Teste	Resultado Esperado	Resultado Obtido
Descriptografia de dados	Sucesso na descriptografia dos dados	Sucesso na descriptografia dos dados
Descriptografia de dados	Erro na leitura dos campos criptografados	Erro na leitura dos campos criptografados

Tabela 13 – Primeiro teste de Descriptografia de dados em Php.

4.7.8 Transmissão de Dados pelo software fileZ

Para esta etapa de testes foi utilizado o software livre fileZ. No primeiro teste foi feito o envio do arquivo AutoInfraDB.txt para o notebook via Bluetooth visando verificar a transmissão das informações.

As informações utilizadas para a transmissão foram:

- **Filename:** AutoInfraDB.txt;
- **Enviar com:** Bluetooth;
- **Mostrar Dispositivos Próximos:** D520;

O teste e resultados podem ser verificados na tabela 14 ilustrada abaixo:

Teste	Resultado Esperado	Resultado Obtido
Transmissão do arquivo AutoInfraDB.txt	Sucesso na transmissão do arquivo AutoInfraDB.txt	Sucesso na transmissão do arquivo AutoInfraDB.txt

Tabela 14 – Primeiro teste de transmissão de dados via fileZ.

4.8 Dificuldades Encontradas

Algumas dificuldades ocorreram na implementação do projeto, tais como:

- Inexperiência na linguagem de programação Casl versão tabela 3;
- Ausência de funcionalidades de envio de arquivos binários na linguagem Casl através de Bluetooth;
- Ausência de funcionalidades de conversão de arquivos de banco de dados em palm para a extensão txt;
- Necessidade de delimitar os campos criptografados do arquivo de banco de dados do palm.

A inexperiência na linguagem de programação Casl versão tabela 3 foi o fator que contribui para a não conclusão do projeto no período de seis meses previsto na proposta de projeto. Para suprir essa dificuldade, foi necessário adquirir um curso de programação em Casl. Após o estudo da apostila do curso, foi desenvolvido um software em Casl chamado Health Trak, esse software foi utilizado como padrão para o desenvolvimento do sistema para palm.

No desenvolvimento do sistema supramencionado, foram descobertos fatores complicadores na linguagem de programação Casl que inviabilizariam cumprir todos os itens descriminados na proposta. Foram adotados os softwares livres fileZ e Abc Amber Palm Converter. Esses softwares respectivamente servem para o envio de arquivo

binários via Bluetooth e conversão do arquivo de banco de dados em palm para a extensão txt. É necessário delimitar os campos do arquivo txt para inserção das informações no banco de dados Oracle e o software Abc Amber Palm Converter não tem esse recurso. Com o uso desses softwares, foi possível atender e desenvolver toda a solução fazendo a aquisição e transferência remota de dados com uso de Palm para um ambiente corporativo de uma forma segura.

5 Conclusão e proposta para projetos futuros

Atualmente o uso de palmtops trás inúmeras vantagens para órgãos do governo e para empresas. Algumas dessas vantagens são: Custo baixo do produto, longa durabilidade das baterias, fácil mobilidade, alta capacidade de armazenamento, grande disponibilidade de programas, possibilidade de sincronização de dados com outros portáteis e computadores convencionais e portabilidade como novas tecnologias tais como Wireless e Bluetooth.

O estudo sobre as características, funcionalidades, vantagens e desvantagens, segurança, riscos, tipos de ataques e ferramentas da tecnologia Bluetooth viabilizou um dos objetivos do trabalho que é a transmissão dos dados de um auto de infração remotamente via palmtop.

A concepção deste projeto constou de quatro etapas. Na primeira, foram levantados os softwares necessários para implementação, bem como sua instalação, configuração e customização. Na segunda, foram desenvolvidas as aplicações nas linguagens de programação Php, PL/SQL e Casl. Na terceira, foi feito o envio do arquivo AutoInfraDB.pdb gerado pela aplicação em Casl via Bluetooh pelo software livre fileZ remotamente pelo palmtop. Na quarta, o arquivo AutoInfraDB.pdb foi convertido para a extensão txt pelo software livre Abc Amber Palm Converter e delimitado para posteriormente ser carregado pela interface em Php. As informações foram disponibilizadas on-line através de relatórios no formato em pdf.

As linguagens de programação empregadas neste trabalho foram Php, PL/SQL e Casl. Essas foram escolhidas respectivamente pelo fato de a primeira e a segunda serem utilizadas como padrão no Ibama e a terceira por ser a linguagem de programação em palm que apesar de ser proprietária, possui uma versão gratuita para desenvolvedores iniciantes.

No desenvolvimento do trabalho foram encontradas algumas limitações relativas à linguagem de programação Casl. Soluções foram adotadas substituindo-se algumas funcionalidades necessárias para o pleno funcionamento do projeto. Os softwares livres fileZ e Abc Amber Palm Converter foram utilizados. O primeiro foi utilizado para fazer o envio do arquivo AutoInfraDB.pdb para o notebook via Bluetooth e

o segundo para conversão do arquivo AutoInfraDB.pdb para extensão txt, extensão necessária para leitura de dados da interface em Php. Para leitura dos campos do arquivo AutoInfraDB.txt foi necessário fazer a delimitação dos mesmos usando delimitadores ponto e vírgula e final de linha.

Como contribuição principal desse trabalho, demonstra-se que o uso da tecnologia Bluetooth aliada com o sistema Sicafi em Casl e em Php podem melhorar e otimizar o trabalho da fiscalização do Ibama, diminuindo consideravelmente a quantidade de papel utilizada no processo de lavragem de auto de infração e o tempo para um infrator ser penalizado pela infração.

Pode-se concluir com os resultados obtidos no projeto, que o sistema em Casl aliado com o módulo de Fiscalização em Php, traz agilidade, mobilidade e rapidez no processo de lavragem de um auto de infração.

Sugere-se como continuação desse trabalho, a implementação na própria aplicação Casl de funcionalidades de conversão do arquivo de banco de dados do palm para a extensão txt bem como a delimitação dos campos e envio do mesmo via Bluetooth para dispositivos próximos. A integração com redes Wireless, bem como o desenvolvimento de uma versão para Smartphones, telefones celulares com a tecnologia de um palmtop, criação de uma funcionalidade para verificação de cpf e autenticação de acesso na tela inicial do sistema para palm.

REFERÊNCIAS

ALECRIM, Emerson. Tecnologia Bluetooth. InfoWester, São Paulo, 30 Ago. 2003. Disponível em: <http://www.infowester.com/bluetooth.php> Acesso em: 21 abr. 2007.

BRINGEL FILHO, José de Ribamar Martins. *FRAMESEC:* um Framework para a provisão de segurança fim-a-fim para aplicações no ambiente de computação móvel. 2004. 149f. Dissertação (Mestrado em Ciência da Computação). Fortaleza: Universidade Federal do Ceará.

CAMARÃO, Paulo César Bhering. *Glossário de Informática*. Rio de Janeiro: LTC – Livros Técnicos e Científicos 1989.

COELHO, Leandro Rodrigues et al. Sistemas de Rádio Celulares e de Rádio Acesso. Centro de Estudos em telecomunicações. Rio de Janeiro: PUC, ago. 2000.

DIAS, Gustavo Neves. Mini-Curso Tecnologias de Rede sem Fio: 6° SEMANA DA INFORMÁTICA DA UESC (SINFORM), 2006, Bahia. **Anais de Mini Curso**, Bahia: Universidade de Santa Cruz – UESC, 2006.

MILLER, Michael. "**Bluetooth"**, *Descobrindo o Bluetooth*: Rio de Janeiro: Campos 2001.

NASCIMENTO, Juarez. *Telecomunicações.* São Paulo: Makron Books, 1992.

PEREIRA, Daniel Arraes. *Jogos ubíquos com Bluetooth*. 2006. 44f. Monografia (conclusão do curso) – Recife: Universidade Federal de Pernambuco, Ciência da Computação, 2006.

PREUSS, Julio. Bluetooth? O que é isso, afinal? . W News, São Paulo, 20 Jun. 2006. Disponível em: <http://wnews.uol.com.br/site/noticias/materia_especial.php?id_secao =17&id_conteudo=256> Acesso em: 21 abr. 2007.

SANTANA, André A. et al. Novos Paradigmas de Projeto e Soluções Desempenho em Redes Sem fio. **Anais de Mini Curso do SBRC**. 2004. São Paulo

SCHWEITZER, Christiane M. et al. Tecnologias de Redes sem fio: Wpans, Wlans E Wmans Desafios de Segurança, Vulnerabilidades e Soluções: 7° SIMPÓSIO SEGURANÇA EM INFORMÁTICA, 2005, São Paulo. **Anais de Mini Curso**, São Paulo: Instituto Tecnológico de Aeronáutica – ITA, 2005.

STALLINGS, W.; *Wireless Communications and Networking*. Prentice Hall; 1st edition; 2002.

OLIVEIRA, Jorge Leite. *Texto acadêmico*: técnicas de redação e de pesquisa científica. 3. ed. Petrópolis: Vozes, 2007.

OLIVEIRA, Marcio Aurélio B. *Aspectos técnicos e práticos da tecnologia Bluetooth*. 2006. 62f. Monografia (conclusão do curso) – São Paulo: Universidade São Francisco, Ciência da Computação, 2006.

APÊNDICE A – Exemplo da Classe Formulário Dinâmico

Função em php que gera relatórios em pdf

```
<?php
//Recuperando as variáveis de ação da seleção (botões).
$formAcao = $_POST['formDinBotao'].$_POST['formDinAcao'];
//carregando os arrays dos campos select.
$ArrOrdenacao = array('NUMERO_AUTO'=>'Nmero do auto','SERIE_AUTO'=>'Srie do Auto');
$ArrAscDesc = array('ASC'=>'Dos menores para os maiores','DESC'=>'Dos maiores para os menores');

//Instanciando os campos do formulário
$campos['dat_inicio']  = new campoData('dat_inicio','Perodo de',true,null,null,null,null,null,false);
$campos['dat_fim']  = new campoData('dat_fim','a',true,null,null,null,null,null,true);
$campos["ordenacao_1"] = new CampoSelect("ordenacao_1","Ordenar por:",true,null,$ArrOrdenacao,null,false);
$campos["asc_desc"] = new CampoSelect("asc_desc","Classificado:",true,null,$ArrAscDesc,null,true);
$campos['gride_uf'] = new campoHtml  ('gride_uf',null,'');

//gerando o formulário dinâmico
$frm = new FormDin3($campos,'Relatório de Autos de Infração - por Estado',$_POST);

//Setando a variável de localização da pagina.
$frm->setVariavel('modulo','sifisc/relatorios/auto_infracao/form_rel_auto_estado');

//Setando a largura e altura do formulario
$frm->setLargura(600);
$frm->setAltura(50);
//Definindo as opções de botão
$frm->botaoAcao[''] = array('Visualizar Relatório');
//Analisando uma ação
if( $formAcao == 'Visualizar Relatrio'){
//Validando os campos obrigatórios no formulário
$erro = $frm->validar();


  if( !$erro ){
    $bvars = array('DAT_INICIO'=>$_POST['dat_inicio']
                  ,'DAT_FIM'=>$_POST['dat_fim']
                  ,'ORDENACAO_1'     =>$_POST['ordenacao_1']
                  ,'ASC_DESC'      =>$_POST['asc_desc']);
```

```
// Carregando o PACOTE ORACLE para retornar o resultado da consulta
    if( $erro = recuperarPacote('SIFISC.PK_RELATORIOS.SEL_AUTO_UF',$bvars,$res_auto_uf,100) ) {
      $frm->msgerros[] = $erro[0];
    } else {
          if(is_array($res_auto_uf)){
                $_SESSION['RELATORIO']['res_auto_uf'] = $res_auto_uf;

                   //Carregando o PDF para exibição do resultado.
                $frm->detalhe='<IFRAME id="relpdf" src="modulos/sifisc/auto_infracao/rel_auto_estado.php"></iframe>'."\n";

                //Redefinindo as opções de botão quando cair nessa opção.
                $frm->botaoAcao['"] = array('Visualizar Relatrio','Fechar Relatrio');

          }else
            $frm->msgerros[] = 'Nenhum auto foi encontrado nesta pesquisa!!! Realize a consulta com outros dados!';


   }else
      $frm->msgerros[] = $erro;
}
if( $formAcao == 'Fechar Relatrio')
  unset($_SESSION['RELATORIO']);
// Apresentar o formulario na tela
echo($frm->criarForm($formAcao));
?>
```

APÊNDICE B – Exemplo de um Pacote Oracle

Exemplo de um pacote oracle que inclui um novo perfil de usuário para o sistema

Especificação:

```
create or replace package pk_base is
  function inc_perfil_pessoa(p_num_pessoa        in menu_perfil_pessoa.num_pessoa%type
                            ,p_seq_perfil        in menu_perfil_pessoa.seq_perfil%type
                            ,p_cod_unidade_ibama in menu_perfil_pessoa.cod_unidade_ibama%type)
    return varchar2;

  function exc_usuario_sistema(p_seq_sistema in menu_perfil.seq_sistema%type
                              ,p_num_pessoa  in menu_perfil_pessoa.num_pessoa%type)
    return varchar2;

end pk_base;
/
```

Operação

```
create or replace package body pk_base is
  v_user varchar2(30) := user;
  function inc_perfil_pessoa(p_num_pessoa        in menu_perfil_pessoa.num_pessoa%type
                            ,p_seq_perfil        in menu_perfil_pessoa.seq_perfil%type
                            ,p_cod_unidade_ibama in menu_perfil_pessoa.cod_unidade_ibama%type)
    return varchar2 is
    v_role        varchar2(30);
    v_num_cpf     varchar2(11);
    v_existe      integer;
    v_seq_sistema number;
    v_menserro    varchar2(100);
  begin
    begin
      select 1
        into v_existe
        from all_users a, pessoa_fisica pf
       where a.username = pf.num_cpf
         and pf.num_pessoa = p_num_pessoa;
    exception
      when no_data_found then
        return 'Usuário sem conta oracle';
    end;

    select s.des_role_sistema, s.seq_sistema
      into v_role, v_seq_sistema
      from menu_perfil p, menu_sistema s
     where s.seq_sistema = p.seq_sistema
       and p.seq_perfil = p_seq_perfil;
```

```
  v_menserro := exc_usuario_sistema(v_seq_sistema, p_num_pessoa);
  insert into menu_perfil_pessoa
    (num_pessoa
    ,seq_perfil
    ,num_pessoa_inclusao
    ,sit_cancelado
    ,dat_inclusao
    ,cod_unidade_ibama)
  values
    (p_num_pessoa
    ,p_seq_perfil
    ,(select num_pessoa from pessoa_fisica where num_cpf = v_user)
    ,'N'
    ,sysdate
    ,p_cod_unidade_ibama);

  -- Temos que cadastrar os roles dos sistema na tabela sistema
  -- e dar direito ao sistema de menus de incluir os funcionarios nos roles.
  if v_role is not null then
    select pf.num_cpf
      into v_num_cpf
      from pessoa_fisica pf
     where pf.num_pessoa = p_num_pessoa;
    execute immediate 'grant ' || v_role || ' to "' || v_num_cpf || '"';
  end if;

  return v_menserro;
 exception
  when no_data_found then
    return 'Perfil inexistente';
  when others then
    return 'Erro de inclusão do perfil/usuário';
 end;

 function exc_usuario_sistema(p_seq_sistema in menu_perfil.seq_sistema%type
                             ,p_num_pessoa  in menu_perfil_pessoa.num_pessoa%type)
  return varchar2 is
  v_role    varchar2(30);
  v_cnt     integer;
  v_num_cpf varchar2(11);
begin
  update menu_perfil_pessoa
     set sit_cancelado           = 'S'
        ,num_pessoa_cancelamento = (select num_pessoa
                                      from pessoa_fisica
                                     where num_cpf = v_user)
        ,dat_cancelamento        = sysdate
```

```
    where seq_perfil in (select seq_perfil
                           from menu_perfil
                          where seq_sistema = p_seq_sistema)
      and num_pessoa = p_num_pessoa;

   if v_role is not null then
     select count(*)
       into v_cnt
       from menu_perfil_pessoa pp, menu_perfil p
      where pp.seq_perfil = p.seq_perfil
        and p.seq_sistema = p_seq_sistema
        and pp.num_pessoa = p_num_pessoa
        and pp.sit_cancelado = 'N';

     if v_cnt = 0 then
       select num_cpf
         into v_num_cpf
         from pessoa_fisica
        where num_pessoa = p_num_pessoa;
       execute immediate 'revoke ' || v_role || ' from "' || v_num_cpf || '"';
     end if;
   end if;

   return null;
  exception
   when others then
     return 'Erro excluindo usuário';
  end;

end pk_base;
```

APÊNDICE C – Função de Criptografia em CASL

Função em casl criptografa as informações contidas no formulário do Auto

```
# Criptografia.cpk

function EncryptData(string PlainText,string Secret) as string;

# Esta função irá criptografar/discriptografar os dados passados para função
# baseada no valor da string Secret

variables;
        string a;
        string b;
        numeric c;
        numeric i;
   string pTb;
        numeric cTb;
        string cT;
        numeric pseudoi;
end;

        # Criptogra a String PlainText, usando a string de Valor Secret

        for i=0,i<length(PlainText);
                pseudoi=i % length(secret);
                if pseudoi=-1;
                        pseudoi=0;
                end_if;

                a = mid(Secret, pseudoi,1);
                b = mid(Secret, pseudoi+1,1);
                c = asc(a) xor asc(b);

                pTb = mid(plaintext, i, 1);
                cTb = c xor asc(pTb);
                ct=ct+char(cTb);
        next i+1;

        # Retorna dado Criptografado
        EncryptData=ct;
end;
```