UNIVERSIDADE REGIONAL DE BLUMENAU

CENTRO DE CIÊNCIAS EXATAS E NATURAIS

CURSO DE SISTEMAS DE INFORMAÇÃO – BACHARELADO

SISTEMA DE CONTROLE DE ACESSO, FREQÜÊNCIA E GESTÃO DE PERMISSÃO PARA AMBIENTE ACADÊMICO

LEONARDO DENARDI

BLUMENAU
2011

2011/2-18

LEONARDO DENARDI

SISTEMA DE CONTROLE DE ACESSO, FREQÜÊNCIA E GESTÃO DE PERMISSÃO PARA AMBIENTE ACADÊMICO

Trabalho de Conclusão de Curso submetido à Universidade Regional de Blumenau para a obtenção dos créditos na disciplina Trabalho de Conclusão de Curso II do curso de Sistemas de Informação— Bacharelado.

Prof. Jacques Robert Heckmann, Mestre – Orientador

BLUMENAU
2011

2011/2-18

SISTEMA DE CONTROLE DE ACESSO, FREQÜÊNCIA E GESTÃO DE PERMISSÃO PARA AMBIENTE ACADÊMICO

Por

LEONARDO DENARDI

Trabalho aprovado para obtenção dos créditos na disciplina de Trabalho de Conclusão de Curso II, pela banca examinadora formada por:

Presidente:	Prof. Jacques Robert Heckmann, Mestre – Orientador, FURB
Membro:	Prof. Wilson Pedro Carli, Mestre – FURB
Membro:	Prof. Francisco Adell Péricas, Mestre – FURB

Blumenau, 02 de dezembro de 2011.

Dedico este trabalho a todos os amigos, especialmente aqueles que me ajudaram diretamente na realização deste.

AGRADECIMENTOS

A Deus, pelo seu imenso amor e graça.

À minha namorada, Juliane Hardt, sempre esteve presente e apoiou em momentos difíceis, abdicou de minha presença em diversos momentos.

À minha família que sempre esteve presente.

Aos meus amigos, pelos empurrões e cobranças.

À Senior Sistemas que proporcionou em determinados momentos ausentar-me do trabalho.

Ao professor e orientador, Jacques Robert Heckmann, por toda ajuda e correções e por ter acreditado neste trabalho.

Não basta ensinar ao homem uma especialidade, por que se tornará assim uma máquina utilizável e não uma personalidade. É necessário que adquira um sentimento, senso prático daquilo que vale a pena ser empreendido, daquilo que é belo, do que é moralmente correto.

Albert Einstein

RESUMO

A necessidade de gerenciar ambientes e garantir a segurança de patrimônio e de pessoal em uma Universidade justificam a criação de uma ferramenta que automatize este processo. Utilizando o *framework* de desenvolvimento *web* GWT como *plugin* da ferramenta Eclipse e o banco de dados MySQL, foi desenvolvido um sistema capaz de controlar o acesso e a freqüência em um ambiente acadêmico, possibilitando aumentar a sua segurança e automatizar o controle de freqüência de alunos e professores.

Palavras-chave: Controle de Acesso. Gestão de Permissão. Controle de Freqüência.

ABSTRACT

The necessity to manipulate spaces and ensure the security of people and heritage at a university justifies the creation of a tool that automates this process. Using GWT web development framework as an Eclipse plugin tool and MySQL database, was developed a system that is capable of controlling access and frequency in an academic setting, enabling the increase of security and automating the frequency control of students and teachers.

Keywords: Access Control. Permission Management. Frequency Control

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

AJAX – *Asynchronous JavaScript and XML*

FURB – Universidade Regional de Blumenau

GWT – *Google Web Toolkit*

PDF – *Portable Document Format*

RIA - *Rich Internet Application*

RF – Requisito Funcional

RNF – Requisito não Funcional

SCAPE – Sistema de controle de acesso e ponto eletrônico

SDK – *Software Development Kit*

TCPIP- Transmission Control Protocol Internet Protocol

UC – *Use Case*

UML - *Unified Modeling Language*

SUMÁRIO

1 INTRODUÇÃO

Pode-se definir segurança como o conjunto de medidas que preserva o estado de um ambiente. Este conceito remete a uma preocupação presente tanto na vida pessoal como no ambiente em que se trabalha ou estuda. Como não há o controle dos meios externos que podem influenciar negativamente nestes ambientes, tem-se que criar artifícios para dificultar estas vulnerabilidades (SANTIAGO, 2008).

Nesta realidade e enfocando um ambiente acadêmico típico, como o da Universidade Regional de Blumenau (FURB), pode-se observar alguns pontos de fragilidade e ameaças aos alunos e ao patrimônio. Um destes pontos é que o acesso aos ambientes da FURB, como laboratórios e salas, não possui um controle formal e eficiente, deixando o patrimônio exposto e vulnerável. Outro ponto é que a FURB possui uma biblioteca pública, portanto não deve oferecer barreiras de acesso ao seu perímetro acadêmico.

Devido à distribuição dos ambientes de uma Universidade em vários campi e aos investimentos em equipamentos tecnológicos para melhorar a qualidade das aulas ministradas, as universidades contam com um alto valor patrimonial espalhado e agregado, possibilitando viabilizar projetos de controle e proteção deste patrimônio (UNIVERSIDADE REGIONAL DE BLUMENAU, 2011a).

Atualmente no Brasil o mercado de segurança patrimonial vem crescendo, assim como os investimentos na área de segurança empresarial, de condomínios e ambientes como os de universidades (ROBERTO, 2011). Esse crescimento se explica devido ao elevado número de incidentes na área de segurança vistos todos os dias nos jornais, somado à falta de investimentos pelo governo, além da desigualdade de distribuição de policiais efetuada pelo governo (SILVA, 2011).

Visando mitigar a fragilidade do ambiente da FURB e aproveitando o crescimento da área de segurança patrimonial, propõe-se o desenvolvimento de um sistema de controle de acesso e gestão de permissões, a fim de impedir que pessoas não autorizadas ou não acompanhadas tenham acesso livre ao patrimônio da mesma, criando uma cultura de proteção e vigilância por parte das pessoas que convivem neste mesmo ambiente.

1.1 OBJETIVOS DO TRABALHO

Este trabalho teve como objetivo principal desenvolver um sistema *web* que controla o acesso e a freqüência de alunos e professores, visando facilitar o controle dentro do ambiente acadêmico. Os objetivos específicos do trabalho são:

a) permitir aos usuários cadastrar permissões e efetuar reservas das salas de aula;
b) gerenciar o controle de entradas e saídas de salas de aula;
c) apresentar relatórios sobre o controle de freqüência acadêmica através dos dados obtidos com os acessos às salas de aula.

1.2 ESTRUTURAS DO TRABALHO

A estrutura deste trabalho está dividida em quatro capítulos.

O primeiro capitulo apresenta a contextualização, a origem para criação do trabalho.

O segundo apresenta as tecnologias utilizadas no desenvolvimento, com conceitos teóricos que justificam sua utilização.

O terceiro capítulo apresenta o desenvolvimento do aplicativo.

O último apresenta a conclusão e limitação de uso.

2 FUNDAMENTAÇÃO TEÓRICA

Nos tópicos de ambiente acadêmico, elementos operacionais e arquiteturais, sistemas de segurança, controle de acesso, controle de freqüência e Google Web Toolkit estão especificadas, as abordagens de cada área de pesquisa utilizadas como base para este trabalho.

2.1 AMBIENTE ACADÊMICO

A rotina em um ambiente acadêmico e a tranqüilidade que cerca um campus universitário mascara a vulnerabilidade do patrimônio de uma universidade, conforme cita Borges (2008).

> Tradicionalmente as instituições de ensino são vistas como locais onde se transmite conhecimentos (ciência, letras, artes ou ofícios), em um ambiente calmo e saudável, no qual as pessoas se sentem perfeitamente à vontade e seguras. Infelizmente esta não é a realidade. Todos os anos escolas e seus freqüentadores têm sido vítimas de ocorrências e de inseguranças diversas, muitas vezes envolvendo crianças e jovens. Certamente a maioria delas poderiam ser evitadas com o planejamento e implementação racional de medidas de prevenção e de dissuasão. (BORGES, 2008).

Além da vulnerabilidade patrimonial, causada por não haver um controle de acesso ao ambiente acadêmico, comprova-se também a necessidade de um sistema de controle de acesso Um fato ocorrido recentemente no qual “[...] de manhã, ex-aluno entrou em colégio, matou estudantes e se suicidou [...]” (GLOBO NOTÍCIAS, 2011), evidencia a necessidade de um sistema deste tipo.

Antes de implementar um sistema de segurança e controle de acesso, é muito importante que se faça uma avaliação da necessidade e da vulnerabilidade, garantindo que o controle realizado será efetivo.

> Para proteger a empresa e seus ativos, o primeiro passo é realizar uma análise de ameaças e vulnerabilidade.
> Com base nessa análise, a equipe de segurança deve implementar sistemas de proteção física (PPS) para fornecer garantias que atenuem as ameaças.
> No *The Desgin and Evaluation of Physical Protection Systems*, Mary Lynn Garcia afirma que "um sistema de proteção física (PPS) integra pessoas, processos e equipamentos para proteção de ativos ou recursos contra a sabotagem, roubo ou outros ataques humanos, mal intencionados.". (PETTERSON, 2005, p.1).

De acordo com Petterson (2005, p.2) pode-se dividir as medidas de segurança de espaços físicos em prevenção, correção e detecção. Desta forma o desenvolvimento de um controle de acesso para ambiente acadêmico atua diretamente dentro da área de prevenção. Utilizam-se alguns elementos importantes para este controle os quais são eles os elementos arquiteturais, como equipamentos de controle de acesso, os elementos operacionais, como

procedimentos e padrões organizacionais, e os sistemas de segurança, como sistemas automatizados de controle de acesso.

2.2 ELEMENTOS OPERACIONAIS E ELEMENTOS ARQUITETURAIS

Segundo Petterson (2005, p.2), para se efetuar um controle de acesso, visando o máximo de segurança do recinto, três pilares são necessários, um deles são os elementos fisicamente presentes no local a ser protegido, chamados de elementos arquiteturais. Estes são meios físicos para se controlar ou barrar acessos a determinados recintos. Estes elementos podem ser portas, catracas, bloqueios físicos, cancelas, terminais de acesso, ou seja, todo tipo de barreira que necessite uma identificação para ser liberado o acesso.

Outro pilar necessário para efetuar um controle de acesso são os elementos operacionais. Para Petterson (2005, p.2), elementos operacionais são regras, normas ou políticas que determinam quem e quando podem acessar determinados recintos.

> Uma política de segurança é a expressão formal das regras pelas quais é fornecido acesso aos recursos tecnológicos da empresa.
> O principal propósito de uma política de segurança é informar aos usuários, equipe e gerentes, as suas obrigações para a proteção da tecnologia e do acesso à informação. A política deve especificar os mecanismos através dos quais estes requisitos podem ser alcançados. (ROCKENBACH, 2011).

Estas políticas servem também para educar todos que convivem dentro deste recinto, como por exemplo, não deixar uma porta que necessita validação de acesso de crachá, aberta. Se uma pessoa que convive neste recinto não sabe de quais os problemas poderão ser causados ao deixar uma porta aberta, provavelmente não irá se preocupar com isso ao passar por este bloqueio físico.

2.3 SISTEMAS DE SEGURANÇA

O terceiro e último pilar são os sistemas de segurança, que segundo Petterson (2005), “são sistemas computacionais que processam informações e através de regras pré-definidas pelo usuário controlam o acesso de determinados recintos”.

O sistema de segurança tem um papel fundamental de unificar as políticas e regras de segurança com os equipamentos de bloqueio físico.

Sendo assim, os sistemas de segurança são o cérebro dos sistemas de controle de acesso, recebendo as informações dos bloqueios físicos, processam as informações utilizando as políticas e regras de segurança e devolvem para os bloqueios físicos permitirem ou

barrarem o acesso.

2.4 CONTROLE DE ACESSO

A necessidade de utilização de um controle de acesso nasce no momento em que a área a ser protegida corre riscos e fica vulnerável quando não há nenhum controle. Segundo Lopes Jr (2000, p. 22) risco é:

> [...] uma ou mais condições de variáveis com potencial suficiente para causar dano ao patrimônio.
> Riscos humanos são aqueles provenientes de ação direta, voluntaria ou não de pessoas, sendo internos ao ambiente, que freqüentam o local todos os dias ou externas, que podem ou não estar autorizadas a freqüentar o local. Existindo quatro possibilidades, surrupio furto, assalto e sabotagem.

Para evitar estes riscos, sistemas de controle de acesso, utilizando hardware e software integrados, são implementados em ambientes.

> Um sistema de controle de acesso é tanto uma medida preventiva e uma medida de detecção. Impede ataques, tornando mais difícil para as pessoas não autorizadas a entrar no ambiente.Também é um sistema que notifica,quando tentativas de entrada não autorizadas são feitas. (PETTERSON, 2005, p. 11).

Com um software e hardware gerenciando o controle de acesso é possível determinar quais pessoas terão direito de acesso, impedindo as demais pessoas não autorizadas. Segundo Jones (2011) software de controle de acesso é:

> [...] um sistema eletrônico de segurança que permite ou restringe o acesso a áreas específicas de uma loja.
> Ela não só protege a propriedade contra visitantes indesejados, mas garante a segurança da propriedade e das pessoas dentro.
> Em termos simples, fornece um controle de entrada (ou saída) através de portas nomeada através de um painel de controle e de alguma forma de mecanismo de travamento elétrico.

Aliando esse controle de acesso às informações geradas pelo hardware, é possível controlar também o período de permanência destas pessoas autorizadas, assim como quando e quem esteve presente no local. De acordo com Canedo (2003, p.16), “o controle de acesso visa restringir o acesso a lugares restritos somente a pessoas autorizadas, normalmente tem uma política de horários e pode ter incorporado um controle de ponto.”

2.5 CONTROLE DE FREQÜÊNCIA

Pode-se aproveitar o controle de acesso para gerar informações sobre a freqüência das pessoas em um ambiente. Como premissa em todo ambiente educacional, os alunos (principal alvo de estudo deste trabalho), necessitam, entre outras coisas, de uma freqüência mínima para serem aprovados pela instituição.

> Para aprovação, o acadêmico precisa de, no mínimo, 75% de freqüência e média final igual ou superior a seis (6,0). A avaliação do desempenho acadêmico envolve tanto a freqüência como o aproveitamento nos estudos, expressos em notas de 0 a 10. Se o acadêmico não se enquadrar nesses critérios de avaliação, estará reprovado na disciplina em questão. (UNIVERSIDADE REGIONAL DE BLUMENAU, 2011b).

Com um sistema de controle de acesso, todas as pessoas irão marcar sua freqüência ao entrar e sair do ambiente, podendo estes dados serem aproveitados pela instituição, evitando falhas e perdas na freqüência com controle por meio de anotações manuais.

2.6 GOOGLE WEB TOOLKIT

Com o objetivo de desenvolver um sistema para controle de acesso *web*, com um visual amigável e simples de utilizar, foi necessário escolher um *framework* de desenvolvimento que facilitasse a montagem de páginas *web*.

Este *framework, Google Web Toolkit (GWT)* foi escolhido por utilizar a linguagem Java no desenvolvimento, após o código pronto, quando o sistema é executado implicitamente código Java é compilado, gerando código Javascript, legível por todos os *browsers*.

> O Google Web Toolkit (GWT) é um conjunto de ferramentas para criação de aplicativos Web RIA (Rich Internet Application), gratuita. A proposta do GWT é tornar o desenvolvimento w*eb* mais produtivo, simples, com qualidade, diminuindo a incidência de erros.
>
> O GWT define um modelo de componentes visuais ricos, com ele o desenvolvedor não se preocupa em criar e manter código JavaScript para utilizar AJAX, e o melhor é que o GWT resolve incompatibilidades de navegadores. A "grande sacada" do GWT é: o desenvolvedor escreve código Java e o GWT transforma esse código em JavaScript. (MAGALHÃES, 2009).

Além disso, o GWT tem componentes prontos para utilização, sendo necessário somente programar os métodos de preenchimento dos dados que cada componente recebe, como por exemplos os dados de uma lista suspensa. Estes componentes possuem métodos de inclusão, exclusão e alteração destes dados, simplificando a utilização de formulários.

2.7 SISTEMA ATUAL

O sistema atual de controle de turmas por sala é realizado, na FURB, com as informações do sistema de registro de graduação (conhecido pela sigla RGRA), identificando todos os alunos em cada turma, bem como os professores de cada turma.

Para reservas adicionais de laboratórios de informática é utilizado outro sistema interno, desenvolvido pelo próprio departamento de computação, conhecido como Laboratórios de Ensino e Aprendizagem (LEA), cuja tela inicial pode ser vista na Figura 1.

Fonte: Universidade Regional de Blumenau (2011c).

Figura 1 – Tela inicial do sistema de Laboratórios de Ensino e Aprendizagem

Em se tratando de controle de acesso às salas, e conseqüentemente acesso ao patrimônio da Universidade, é realizado apenas um controle de chaves que são cedidas aos docentes, permitindo-se após a abertura das salas livre acesso de qualquer pessoa a qualquer ambiente.

O controle de freqüência, hoje pode ser realizado através de outro sistema interno, ou até mesmo por diário de classe.

2.8 TRABALHOS CORRELATOS

Foram encontrados três trabalhos correlatos, que mais se aproximam do que está sendo desenvolvido. O primeiro é um sistema, denominado Sistema de controle de acesso e ponto eletrônico (SCAPE). O segundo trabalho é sistema de terminal de controle de acesso e ponto utilizando biometria, também *web*. O terceiro trabalho é referente a um controle de freqüência de alunos, da própria FURB, porém com foco no desenvolvimento do hardware.

2.8.1 Sistema de controle de acesso e ponto eletrônico

É um sistema de controle de ponto e acesso a ambientes (D´AGOSTO, 2008). O trabalho foca no desenvolvimento do *middleware* de comunicação entre os dispositivos de controle e o gerenciamento dos dados e explana sobre os protocolos de comunicação, interfaces do software e quais hardwares foram utilizados.

O sistema possui relatórios de ponto dos trabalhadores, total de horas trabalhadas e ambientes freqüentados.

O sistema SCAPE se baseia em um controle de acesso e ponto de estruturas organizacionais como empresas e indústrias, com foco no controle do trabalho de seus funcionários e relatórios das atividades executadas por eles. A ferramenta utilizada para o desenvolvimento foi PHP para a comunicação e para apresentação do software ao usuário, sendo que no meu sistema foi utilizado o Java para a camada do servidor e o *GWT* para a camada de apresentação.

Este trabalho tem a mesma linha de pesquisa da utilizada por mim, em se tratando de controle de acesso a usuários e controle de freqüência, porém o foco do mesmo é voltado ao desenvolvimento do hardware de controle e da comunicação com o software desenvolvido.

2.8.2 Terminal de controle de acesso e ponto usando biometria

Este trabalho baseia-se em dados relevantes sobre o mercado de terminais de acesso e ponto, dando ênfase ao hardware de leitores biométricos para identificação de pessoas. (CANEDO, 2003).

O trabalho relata o desenvolvimento de um leitor biométrico de baixo custo que irá integrar-se com um de controle de acesso para validar os dados captados pelos leitor. O sistema possui telas simples para gerenciar os leitores e os dados enviados por estes efetuando as tratativas de controle de acesso necessárias, devolvendo as informações para o leitor efetuar a liberação ou não do acesso/ponto.

O motivo por este trabalho ser correlato é por tratar de uma das pontas do controle de acesso, recebendo os dados do usuário e enviado a uma base de dados.

Segundo Canedo (2003), o controle de acesso e freqüência pode ser realizado por vários tipos de equipamento, como leitor de barras, teclado, SmartCard e leitores biométricos.

A vantagem do leitor biométrico é que o objeto em questão, a digital, não pode ser repassado a nenhuma outra pessoa, como pode o cartão ser repassado a uma terceira pessoa para registro do ponto ou do acesso.

2.8.3 Hardware para controle de freqüência acadêmica

Este trabalho tem como objetivo desenvolver um hardware para controle de freqüência acadêmica (SILVA, 2002). Possui um grande foco nos protocolos de comunicação entre o *hardware* do microcontrolador e o software.

Utiliza-se de um microcontrolador que ao ler os dados dos cartões de alunos, irá enviar a freqüência de cada aluno via e-mail para o professor da respectiva disciplina.

Este trabalho é correlato ao sistema proposto, pois trata de um dos módulos apresentados neste documento: o controle da freqüência de ambientes acadêmicos. Porém todo desenvolvimento é baseado em receber os dados de um dispositivo e enviar através da rede os dados para um gerenciador que enviará um *e-mail* com os dados de freqüência dos alunos.

O trabalho correlato não trata de desenvolvimento de sistemas informatizados de controle de acesso ou sistemas com interfaces ricas para o gerenciamento dos dados de controle de acesso e freqüência.

Utiliza também um kit de hardware pronto (Figura 2), que segundo Silva, (2002) contém um módulo programável, interface Ethernet e portas seriais, além de entradas e saídas digitais, placa protótipo, ambiente de desenvolvimento C com bibliotecas para TCPIP, um cabo serial para programação e fonte de alimentação.

Fonte: Silva, (2002, p.24).

Figura 2 – Kit de hardware

3 DESENVOLVIMENTO

Neste capitulo estão descritos os requisitos funcionais, os requisitos não funcionais, as regras de negócio, o diagrama de casos de uso, o fluxo de atividades com o software desenvolvido, o modelo de entidade relacionamento, a implementação, os resultados e a sua discussão.

3.1 LEVANTAMENTO DE INFORMAÇÕES

Após observações do ambiente da FURB, foi possível identificar que um sistema que controle o acesso e a freqüência de professores e alunos vem a suprir uma necessidade de segurança e de gestão destas informações. Como o controle é manual, o processo é lento e frágil. Automatizando o processo se torna confiável e ágil.

Para o controle são necessárias informações de alunos, professores e do ambiente da FURB. Porém estas informações já existem em outro sistema, então o software desenvolvido,tem a função de determinar quais turmas (alunos e professores) tem acesso a determinados ambientes.

No sistema desenvolvido os ambientes são divididos em áreas, podem ser: laboratórios, salas, recintos, ou qualquer lugar que necessite de controle de acesso.

Estas são cadastradas a qualquer momento dentro do menu *"Cadastrar Área"*, informando a descrição de área e um número de identificação. Sempre que for necessário controlar o acesso de um local é necessário determinar esse local através do cadastramento de uma área.

Para que seja possível controlar o acesso e freqüência é preciso realizar os seguintes procedimentos, conforme fluxo de atividades da figura 3.

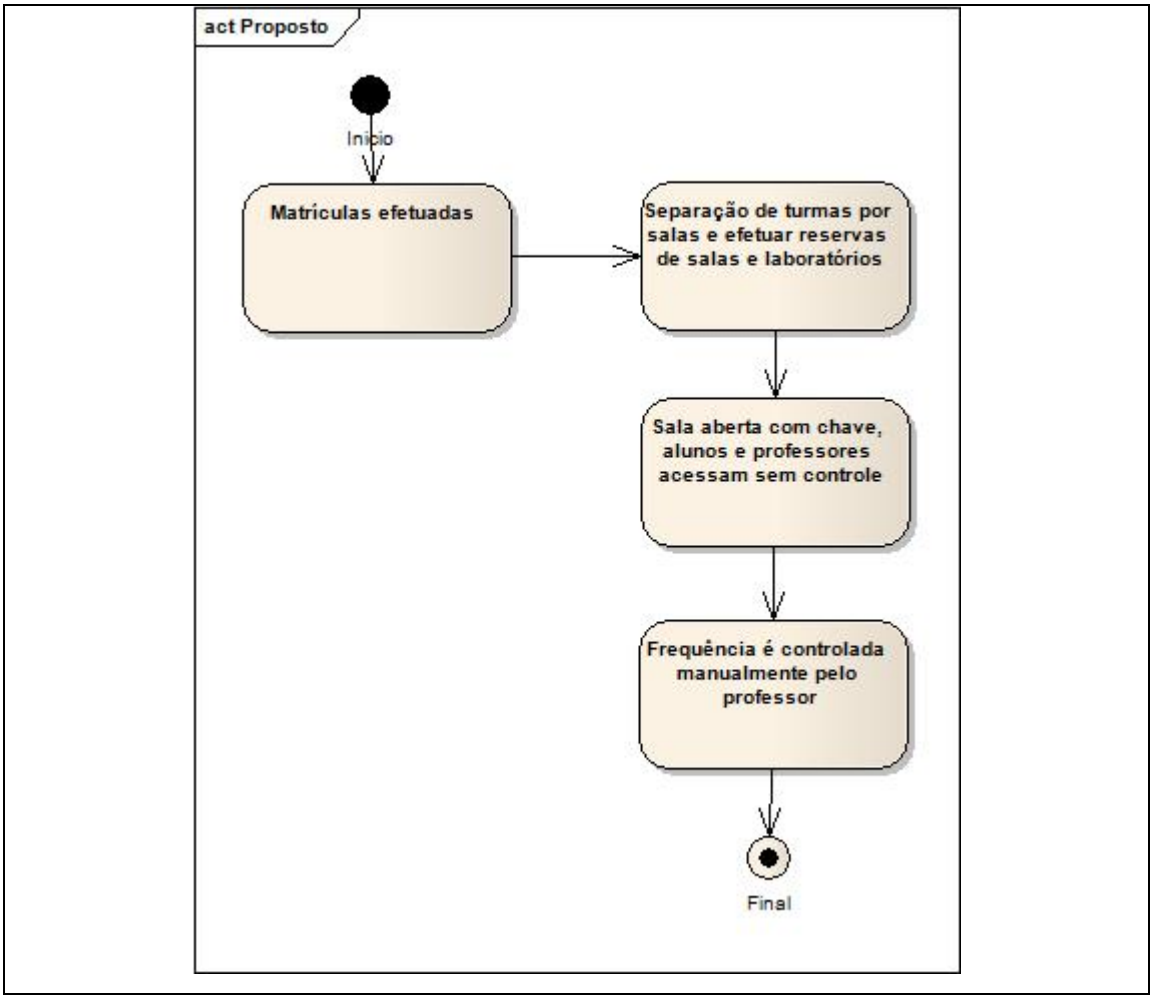


Figura 3 – Fluxo de atividades

A figura 03 exibe o funcionamento atual do controle de acesso às salas da FURB. Após as matrículas, são separadas as turmas por ambiente, onde qualquer pessoa tem o direito de acesso, sem nenhum controle. O professor é responsável por obter a freqüência dos alunos no diário de papel.

3.2 ESPECIFICAÇÃO

A seguir são apresentados os requisitos funcionais (RF), requisitos não funcionais (RNF), regras de negócio (RN), diagrama de casos de uso, fluxo de atividades e modelo entidade relacionamento (MER).

3.2.1 Requisitos Funcionais

O Quadro 1 apresenta os requisitos funcionais previstos para o sistema e sua rastreabilidade, ou seja, vinculação com o(s) caso(s) de uso associado(s).

Requisitos Funcionais	**Caso de Uso**
RF01: O sistema deve conter uma tela de *login* com os campos *login* e senha, exigindo autenticação do usuário.	UC01
RF02: O sistema deve permitir cadastrar pessoas. A tela deve conter um formulário com os campos nome, número do crachá, senha, tipo de pessoa e as disciplinas a que está vinculada.	UC02
RF03: O sistema deve permitir editar o cadastro de pessoas, deve exibir uma lista com todas as pessoas e ao selecionar alguém da lista os campos formulário de cadastro devem ser preenchidos com os dados.	UC02
RF04: O sistema deve permitir a exclusão de pessoas caso não tenha freqüência associada	UC02
RF05: O sistema deve permitir alterar a senha. A tela deve exibir um campo para digitar a nova senha.	UC03
RF06: O sistema deve permitir o cadastramento de novas turmas, a tela deve conter os campos de descrição (obrigatório) e duas listas para seleção de professores e alunos.	UC04
RF07: O sistema deve permitir editar o cadastro de turmas existentes. Deve ser exibida uma lista com todas as turmas e ao selecionar o formulário de cadastramento deve ser preenchido com os dados.	UC04
RF08: O sistema deve permitir excluir turmas caso não haja nenhuma disciplina associada.	UC04
RF09: O sistema deve permitir o cadastro de cursos, solicitando a descrição do curso.	UC05
RF10: O sistema deve permitir excluir um curso caso não tenha disciplinas associadas a ele.	UC05
RF11: O sistema deve permitir o cadastramento de novas disciplinas. A tela deve conter a lista de cursos e um campo para informar a descrição da disciplina. O sistema deve exigir o cadastramento de todos os campos.	UC06
RF12: O sistema deve permitir a exclusão de disciplinas	UC06

RF13: O sistema deve permitir o cadastramento de novas áreas. A tela deve conter um campo para descrição da área e outro para o número do dispositivo. Deve haver um campo para determinar se a área necessita de autorização para entrada de alunos ou não.	UC07
RF14: O sistema deve permitir excluir áreas cadastradas caso não tenha relação com nenhuma permissão.	UC07
RF15: O sistema deve permitir o cadastramento de novas permissões. A tela deve conter um formulário com a lista de turmas, a lista de áreas, um campo para data inicial outro para final, um campo para hora inicial e outro para hora final da permissão.	UC08
RF16: O sistema deve permitir excluir as permissões, a tela deve exibir uma lista com as permissões.	UC08
RF17: O sistema deve permitir editar as permissões. A tela deve exibir uma lista com as permissões.	UC08
RF18: O sistema deve permitir emitir um arquivo em *pdf* com todos os dados de freqüência dos alunos associados ao professor solicitante.	UC09
RF19: O sistema deve ao liberar o acesso de uma registrar a freqüência.	UC10
RF20: O sistema deve registrar as ocorrências de acesso negado.	UC11
RF21: O sistema deve permitir o usuário administrador consultar em tela as ocorrências	UC11
RF22: O sistema deve enviar um *e-mail* com as novas permissões a todas as pessoas da turma relacionada à permissão	UC08

Quadro 1 – Requisitos Funcionais

3.2.2 Requisitos Não Funcionais

O Quadro 2 lista os requisitos não funcionais previstos para o sistema.

Requisitos Não Funcionais	
RNF01: Utilizar Banco de Dados *Mysql*	Implementação
RNF02: O sistema deverá ser desenvolvido para plataforma *Web*	Portabilidade
RNF03: O sistema deverá ser desenvolvido utilizando Tecnologia Java	Portabilidade
RNF04: O sistema deverá validar o acesso em tempo real	Desempenho

RNF05: O sistema deverá permitir múltiplas tentativas de acesso	Desempenho
RNF06: O sistema deve exibir um *menu* com acesso a todas as telas. As telas disponíveis são: Cadastro de Pessoas, Cadastro de Curso,Cadastro de Disciplina, Cadastro de Turma, Cadastro de Área, Cadastro de Permissões, Alteração de Senha, Tela de ocorrências, botão de relatório e o botão *logout.*	Segurança

Quadro 2 – Requisitos Não Funcionais

3.2.3 Regras de negócio

No Quadro 3 são listadas algumas regras de negócio e os respectivos casos de uso que elas impactam.

Regras de Negócio	**Caso de Uso Impactado**
NEG01: O sistema não pode permitir que sejam cadastrados valores em branco no formulário de pessoas	UC02
NEG02: Para cadastrar pessoas é obrigatório o cadastramento de disciplinas	UC02
NEG03: O sistema não deve permitir o cadastramento de senha em branco.	UC02, UC03
NEG04: O sistema deve obrigar todas as turmas terem um aluno e um professor pelo menos.	UC04
NEG05: O sistema deve verificar se a pessoa é administradora ou professor, caso for professor, somente exibirá os botões de acesso as telas de cadastro de permissão, alteração de senha, geração de relatório e logout.	UC01
NEG06: Ao cadastrar uma nova permissão o sistema deve registrar esta permissão no banco de dados e verificar se não existe uma permissão igual. Caso existir não deve deixar inserir outra igual.	UC08
NEG07: O sistema deve verificar que o acesso atual é diferente do último acesso da pessoa, ou seja, somente poderá entrar se o último acesso for à direção de saída.	UC10
NEG08: Caso a área relativa ao acesso necessite de autorização, o	UC10

sistema deve consultar se já existe um autorizador presente na área.	
RF09: O sistema deve exibir somente os dados associados ao usuário. Quando *logado* como professor, somente as permissões associadas ao mesmo. Quando administrador mostrar todos os dados.	UC01

Quadro 3 – Regras de Negócio

3.2.4 Diagrama de casos de uso

Para o sistema de controle de acesso e freqüência foram definidos onze casos de uso. Os dois principais casos de uso são o cadastro de permissões (UC08), que associa turmas às áreas e determina a data e o horário que as pessoas da turma podem acessar as áreas. O outro é o controlar acesso (UC10) que ao receber o número do crachá via simulador de acesso, verifica de quem é este crachá e se ele tem permissão de acesso.

Os atores são o administrador, que tem acesso total ao sistema, e o professor, que pode consultar relatórios de freqüência, cadastrar permissões e alterar sua senha.

O detalhamento dos casos de uso está descrito no apêndice A. As figuras 04 e 05 exibem os diagramas de casos de uso do sistema.

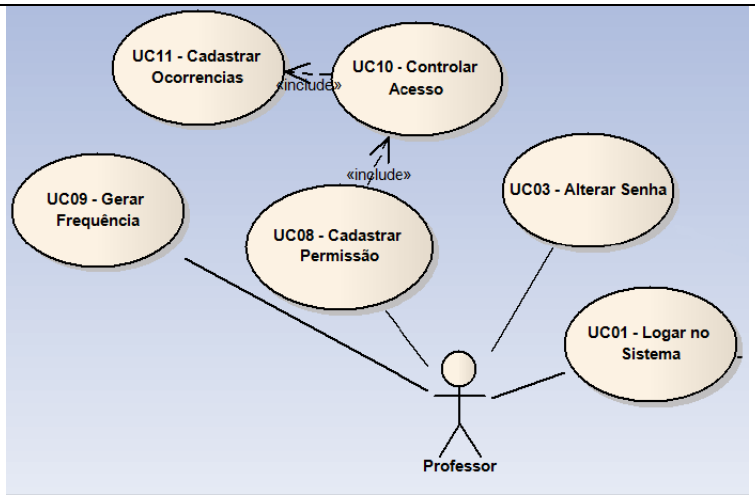


Figura 4 – Diagrama de caso de uso

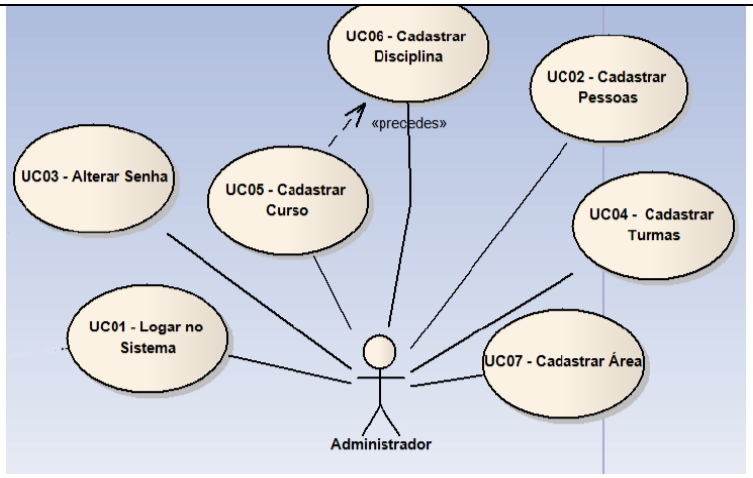


Figura 5 – Diagrama de caso de uso administrador

3.2.5 Fluxo de atividades

Neste tópico é apresentado o fluxo de atividades do aplicativo. As figuras 6 e 7 trazem de forma esquemática uma representação do processo com o sistema.

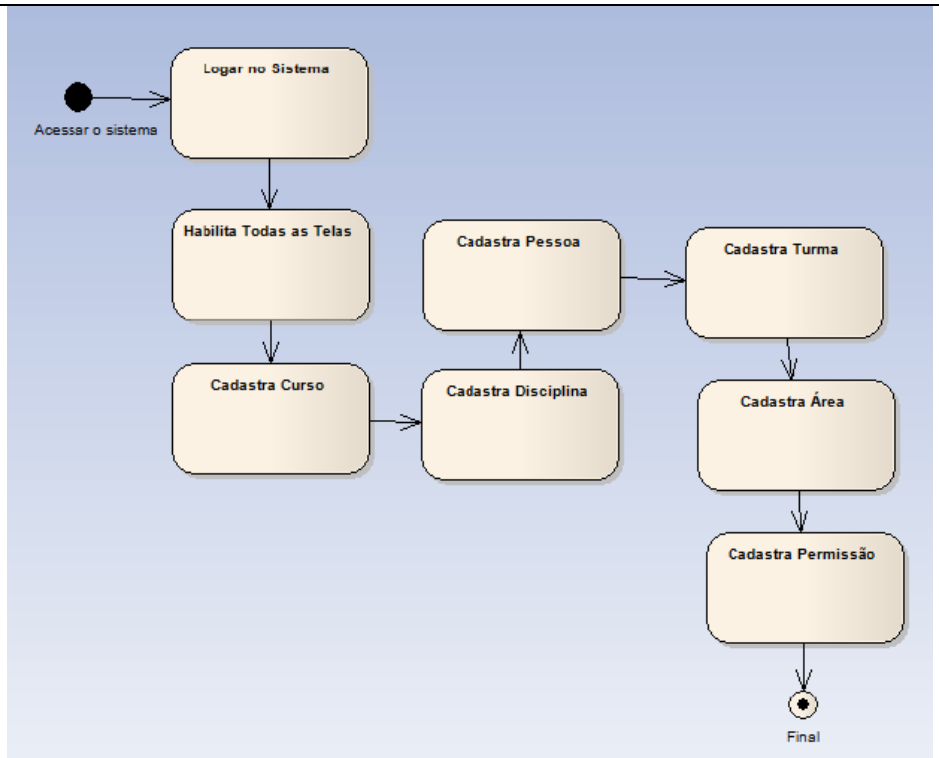


Figura 6 – Diagrama de atividades parte administrador

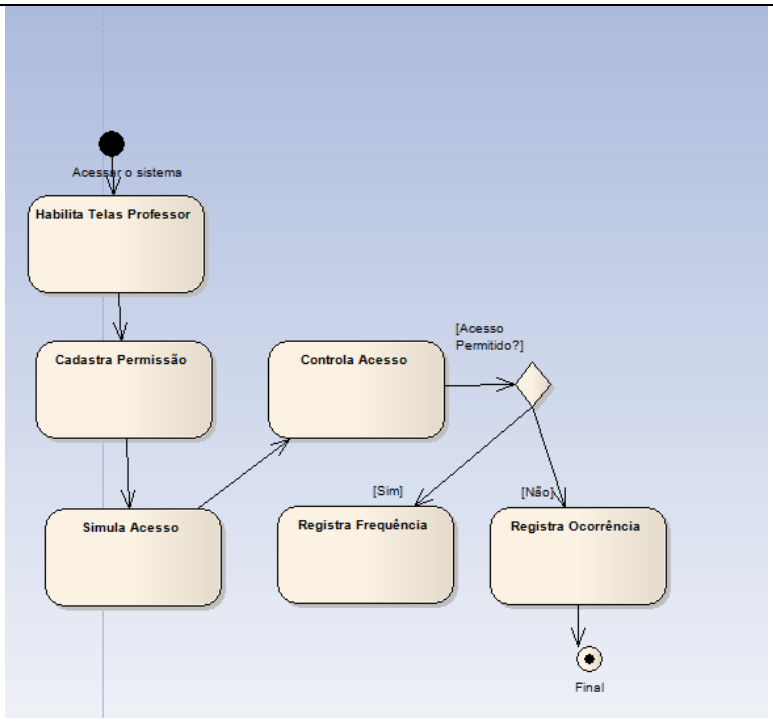


Figura 7 – Diagrama de atividades parte professor

Para o sistema de controle de acesso e freqüência há necessidade de informações estarem cadastradas, como o cadastro de disciplinas, cadastro de pessoas, cadastro de turmas, cadastro de áreas e permissão, pois sem essas informações não é possível o controle do acesso e a geração da freqüência. Os fluxos de atividades acima demonstram o funcionamento do sistema desenvolvido. Caso o usuário seja administrador, todas as telas serão exibidas, pode-se cadastrar pessoas, cursos, disciplinas, turmas, áreas, permissões e tirar relatórios de ocorrências. Caso seja Professor, poderá cadastrar permissões e tirar relatório de freqüência.

3.2.6 Modelo Entidade Relacionamento.

A figura 8 apresenta o modelo entidade-relacionamento no qual estão as tabelas que são persistidas no banco de dados utilizado pela aplicação.

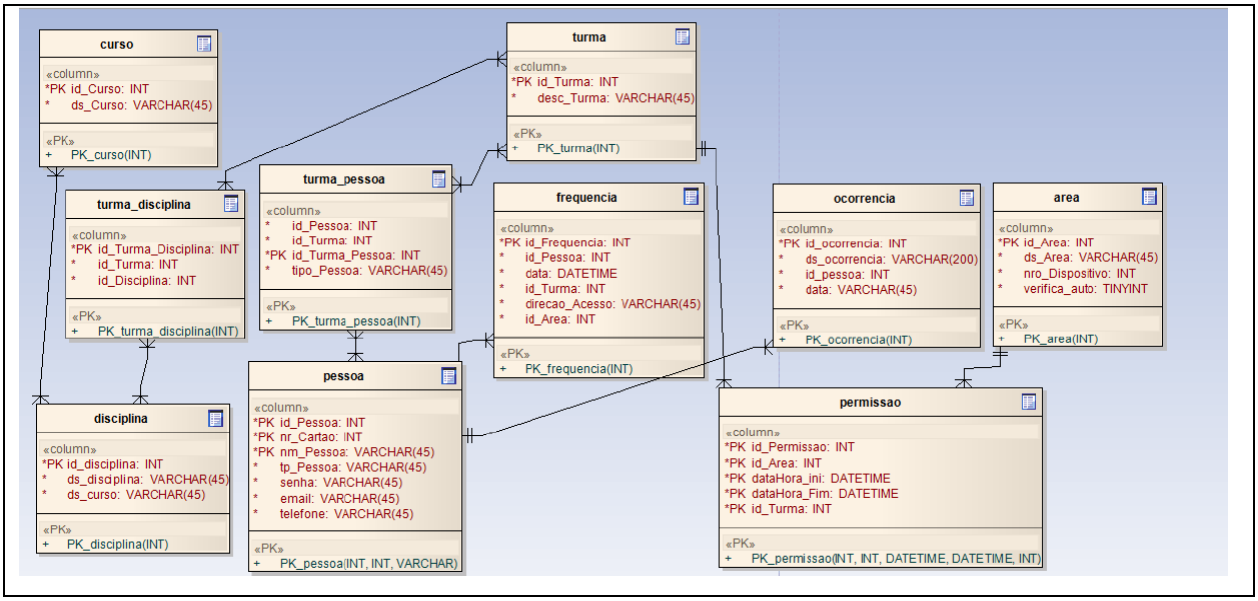


Figura 8 – Modelo Entidade Relacionamento

Foram definidas 10 tabelas no banco de dados para utilização no sistema de controle de acesso. No apêndice B consta o dicionário de dados.

3.3 IMPLEMENTAÇÃO

Nesta seção são mostradas as técnicas e ferramentas utilizadas, a operacionalidade da implementação, bem como codificação do sistema, operacionalidade da implementação, processos de parametrização da aplicação, processos de controle de acesso e processos de auditoria.

3.3.1 Técnicas e ferramentas utilizadas

Para o desenvolvimento do aplicativo de controle de licenças foi utiliza a linguagem Java, versão 1.6.0. Na compilação e depuração a ferramenta *Eclipse*, versão *Helios*. As telas foram geradas com o *framework GWT*. O banco de dados utilizado, conforme explicitado no RNF01, foi o MySQL, versão 1.2.17. O *contêiner* de aplicações *web Apache Tomcat* foi utilizado para a execução dos *servlets*.

A especificação deste aplicativo foi feita utilizando-se os diagramas da *Unified Model Language* (UML), usando o software de modelagem Enterprise Architect, produzindo os modelos de casos de uso, o diagrama de classes, modelo entidade relacional e o diagrama de atividades.

3.3.2 Codificação do sistema

Abaixo está a *Interface* utilizada pelo GWT para efetuar a troca de informações entre o cliente e o servidor (Figura 9) e método para chamar a interface (Figura 10).

```
@RemoteServiceRelativePath("greet")
public interface GreetingService extends RemoteService {

    public Evento simulaAcesso(String numeroCracha,String descArea, String direcao);
    void cadastraArea(String descricaoArea, int idDispositivo,Boolean verAut);
    boolean cadastraPermissao(Permissao permissao);
    List<Area> buscaArea();
    Pessoa verificaLogin(String login, String senha);
    void verificaSenha(String senha, String nomePessoa);
    void cadastraDisciplina(String descDisciplina, String curso);
    boolean cadastraPessoa(Pessoa pessoa);
    void cadastraTurma(String value, List<Pessoa> alunos,
            List<Pessoa> professores, String disciplina);
    List<Turma> buscaTurma(Pessoa p);
    List<Disciplina> buscaDis();
    List<Pessoa> buscaPessoa();
    String geraRelatorio(String desc, Date dataIni);
    Pessoa buscaPessoaAltera(String nomePessoa);
    void atualizaPessoa(Pessoa pessoa);
    void updateTurma(String dsTurma, List<Pessoa> listaAlunos, List<Pessoa> listaProfessores, String disciplina);
    List<Pessoa> alteraTurma(String dsTurma);
    List<Turma> buscaTurmas();
    List<Permissao> retornaPermissao(Pessoa logado2);
    void cadastraCurso(String value);
    List<Curso> buscaCurso();
    Boolean removePessoa(Pessoa p);
    Boolean removeTurma(Turma selectedItem);
    Boolean removeCurso(Curso selectedItem);
    Boolean removeDisciplina(Disciplina selectedItem);
    Boolean removeArea(Area selectedItem);
    Boolean removePermissao(String a, String b, String c, String d);
    List<Ocorrencia> buscaOcorrencia();
    List<Ocorrencia> buscaOcorrencias();
`
```

Figura 9 – Interface GWT

Esta interface contém todos os métodos chamados pelas telas do sistema e repassados para o servidor. No servidor classe GreetingSeviceImpl.java, todos estes métodos são implementados e retornam assincronamente um resultado.

```
greetingService.cadastraArea(panel.getFields().get(0).getValue().toString(),
        Integer.parseInt(panel.getFields().get(1)
                .getValue().toString()), ch.getValue(), callback);
```

Figura 10 – Exemplo de chamada de servidor via GWT

3.3.3 Operacionalidade da implementação

O sistema foi desenvolvido utilizando o *framework* GWT, que separa o sistema em duas partes: a parte do processamento de informações (o lado *server*) e a parte das telas do sistema (o lado *client*).

Todas as telas do sistema tem métodos que chamam suas respectivas implementações que estão no lado *server*, através de mensagens assíncronas, implementadas pelo próprio *framework.*

Isso faz com que estas duas partes do sistema fiquem bem isoladas e de fácil manutenção. Outro ponto importante a destacar é que apesar do sistema ser para a *web*, as telas são desenvolvidas em linguagem Java e o *framework*, por si, as converte para a linguagem *JavaScript*, executável nos *browsers.*

3.3.4 Processos de parametrização da aplicação

O início do uso do sistema dá-se através de uma tela de autenticação, chamada também de tela de *login* (Figura 11). Nesta tela são exigidos o *login* e a senha. Caso o usuário ou a senha sejam inválidos, o sistema apresentará a mensagem exibida na Figura 12.

Uma vez que o usuário esteja corretamente identificado e autenticado, o sistema verifica se o usuário em questão é da categoria professor ou da categoria administrador. Caso seja da categoria professor, ele só conseguirá cadastrar novas permissões, gerar relatórios ou trocar sua senha. O usuário da categoria administrador, por sua vez, pode ver todas as telas e efetuar todas as rotinas do sistema.

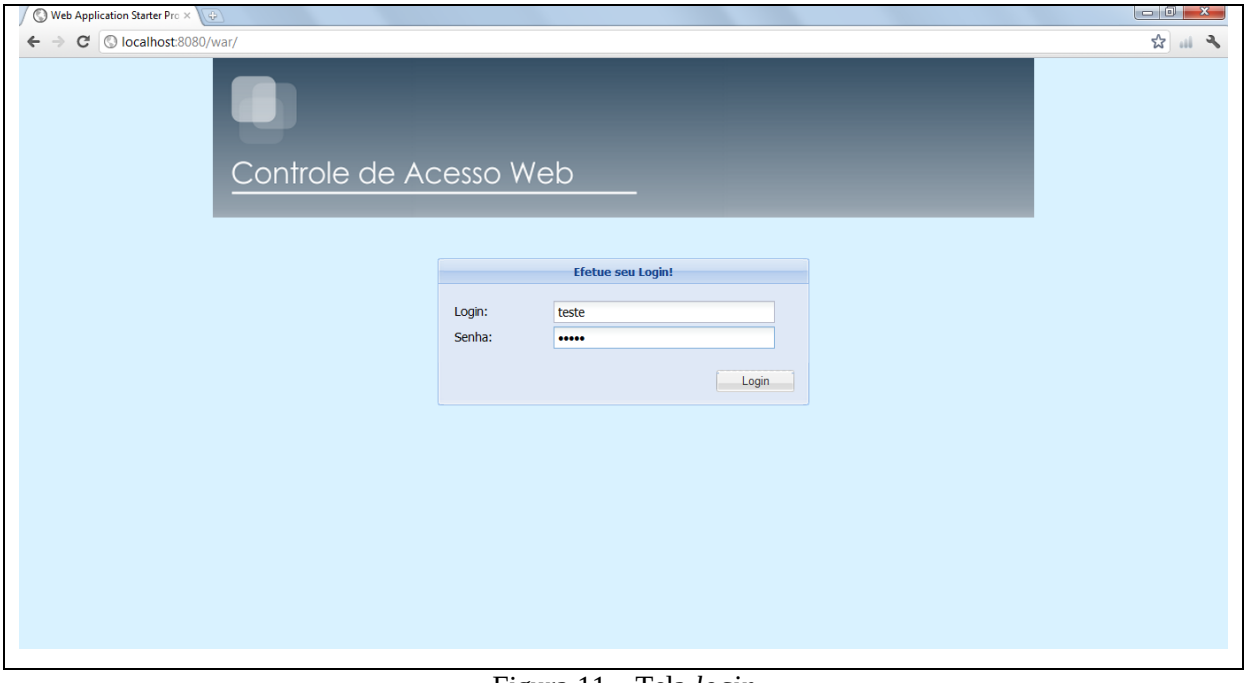


Figura 11 – Tela *login*

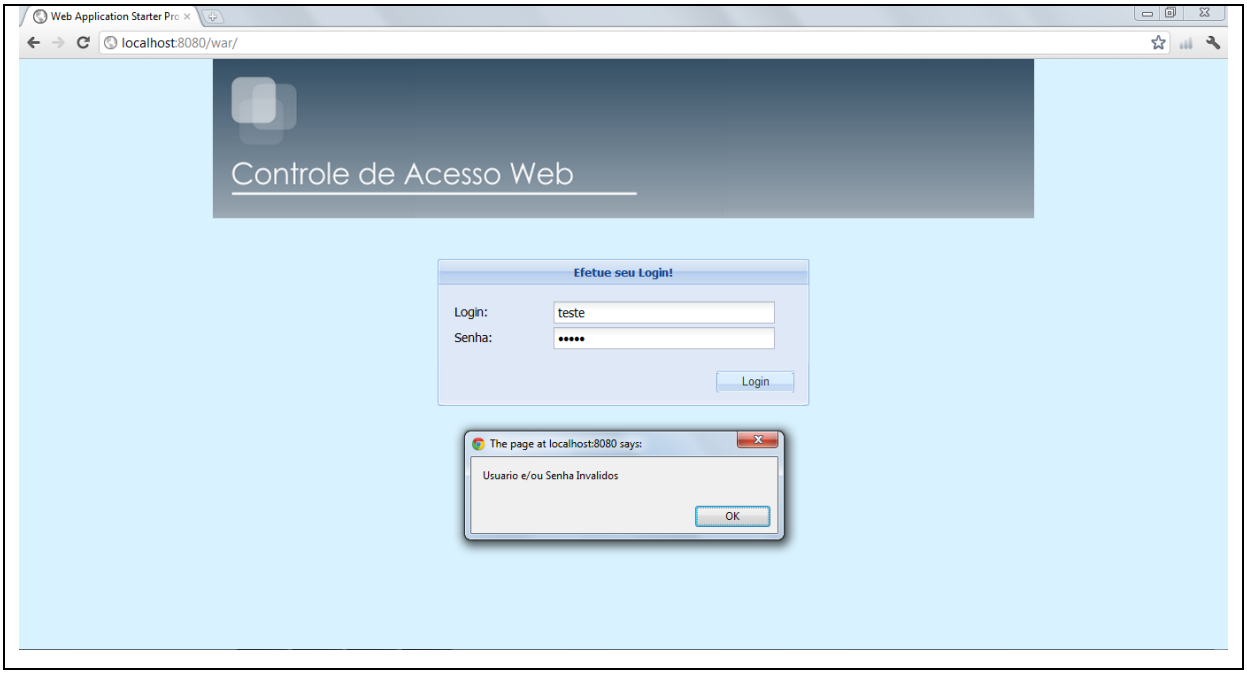


Figura 12 – Tela *login* com validação de usuário

Caso a categoria do usuário seja administrador do sistema, ele terá acesso a todas as telas do sistema (figura 13). Caso o usuário não seja usuário administrador, ele somente terá acesso as telas de cadastro de permissão, de relatório e alteração de senha (figura 14).

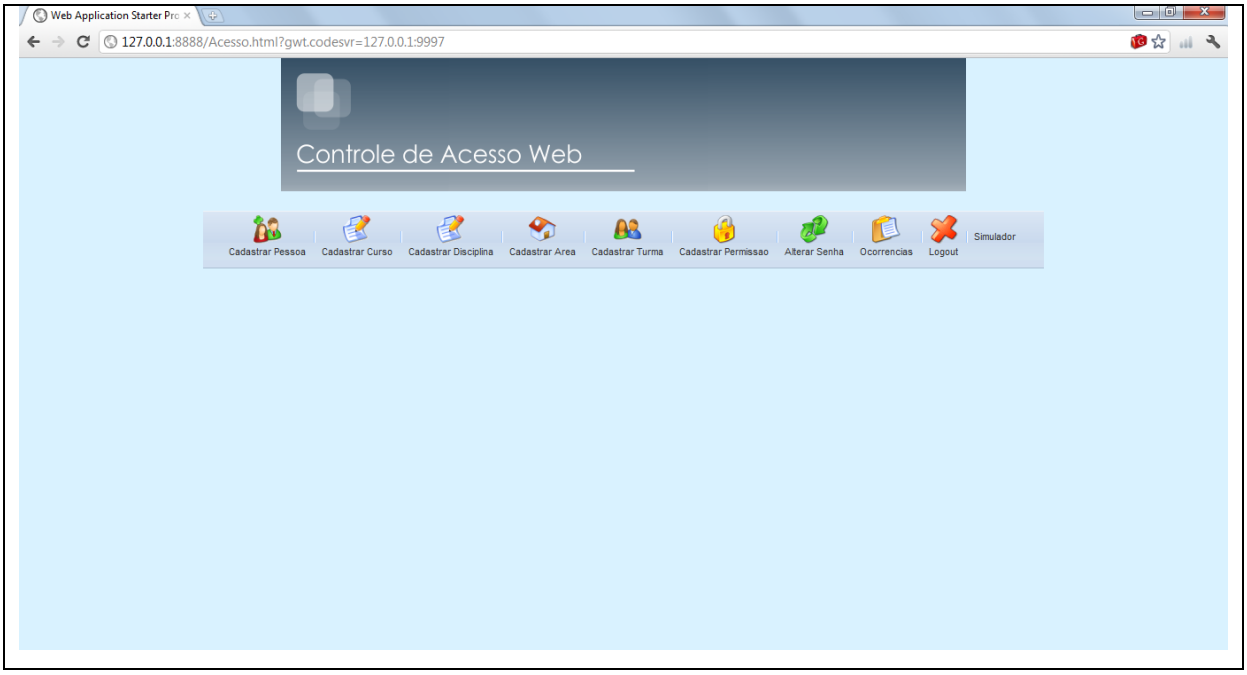


Figura 13 – Menu exibido ao administrador

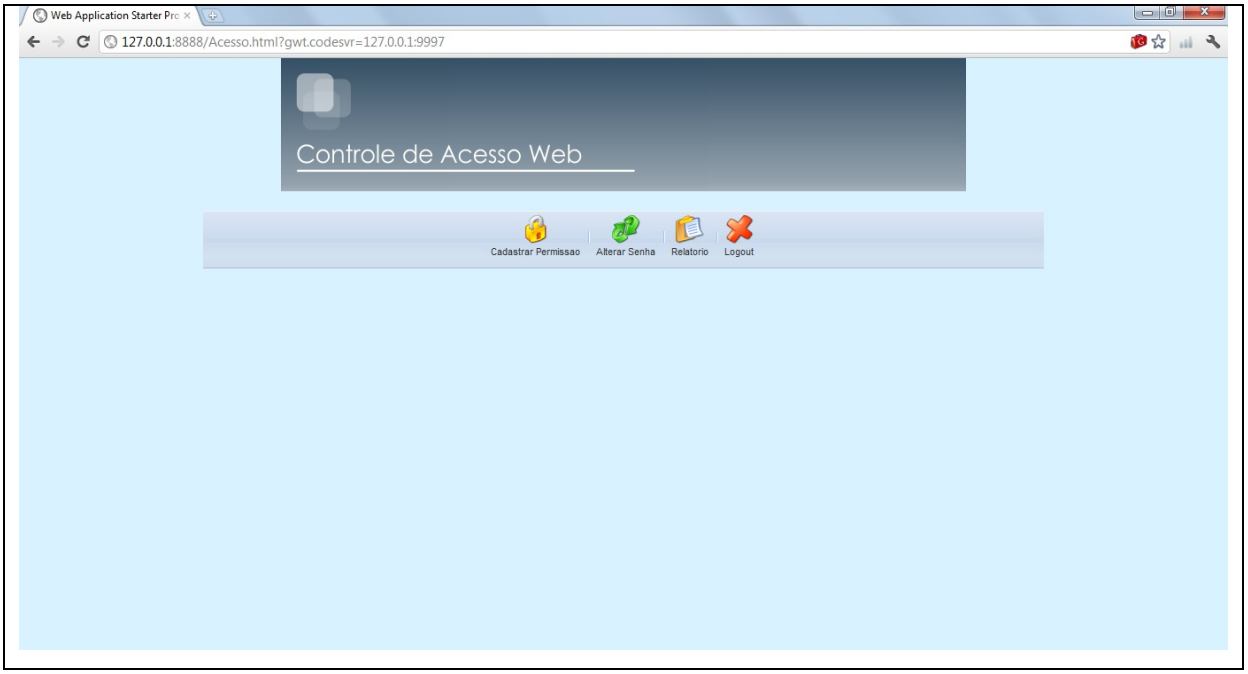


Figura 14 – Menu exibido ao professor

A figura 15 apresenta a tela de alteração de senha, caso o usuário necessite alterar sua senha de acesso ao sistema.

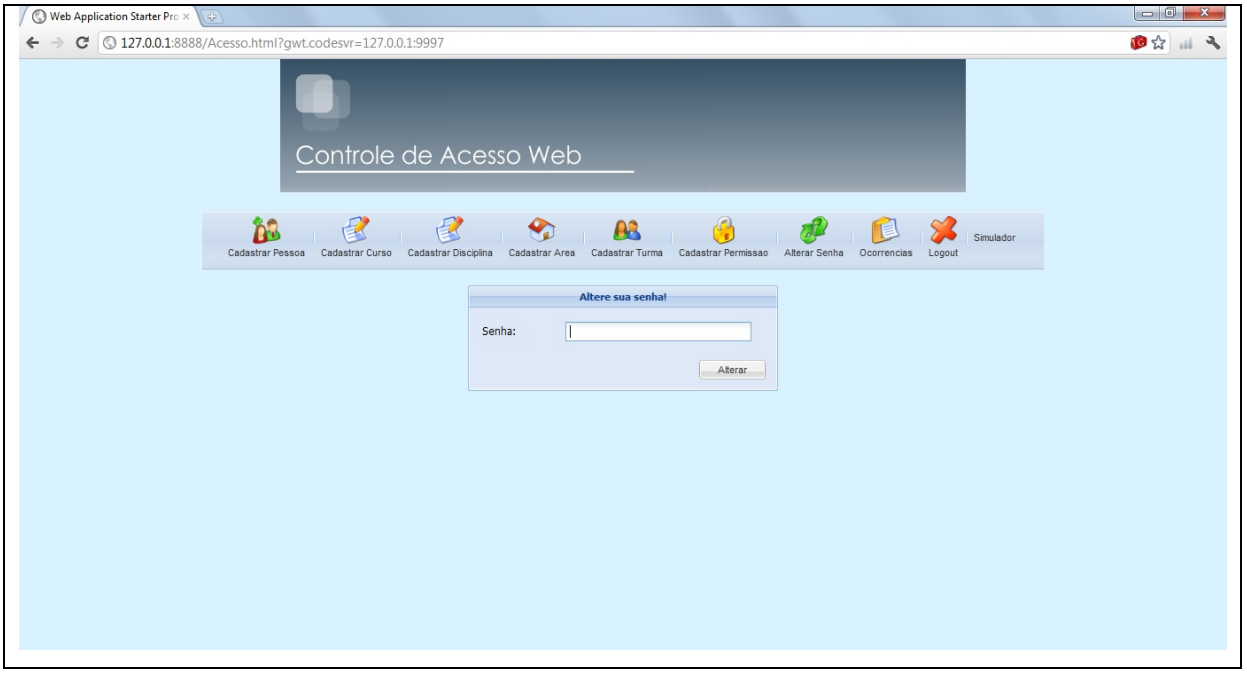


Figura 15 – Tela Alteração de Senha

Para controlar o acesso e a freqüência em um ambiente através do sistema desenvolvido, é necessário inicialmente o cadastro dos cursos disponíveis no ambiente acadêmico (Figura 16) e de suas respectivas disciplinas (Figura 17).

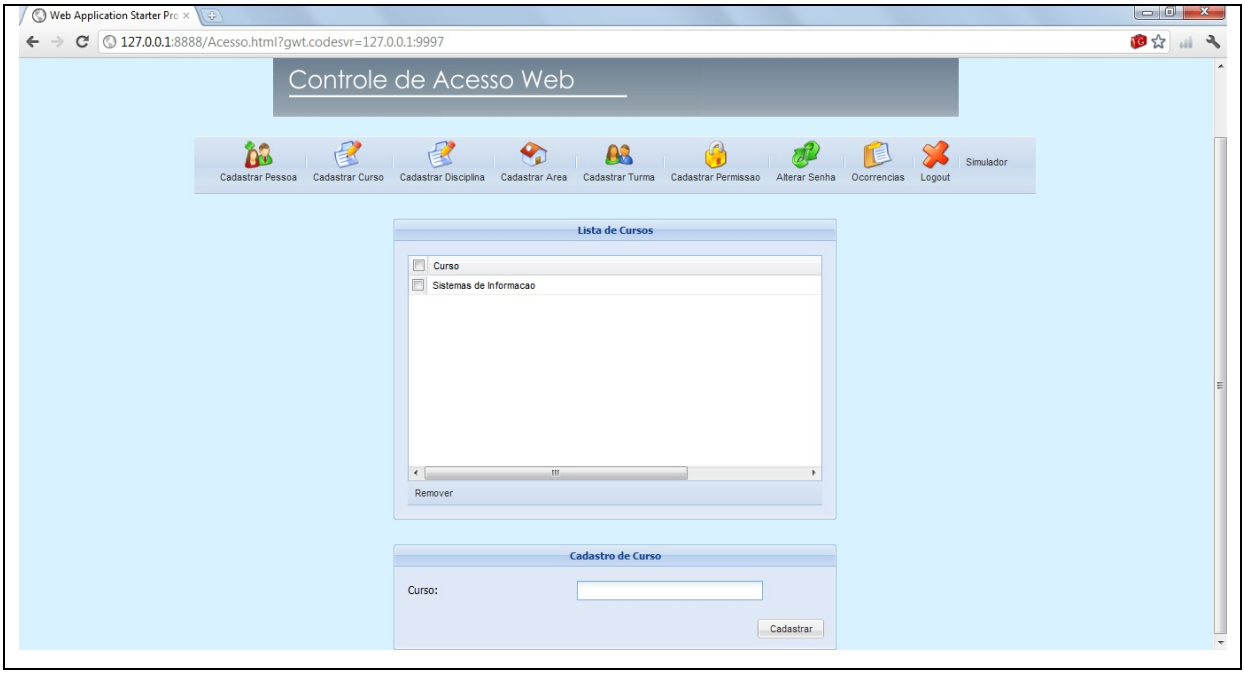


Figura 16 – Tela Cadastro de Curso

A figura 17 exibe a tela de cadastro de disciplinas, que são associadas a cursos já existentes na instituição de ensino.

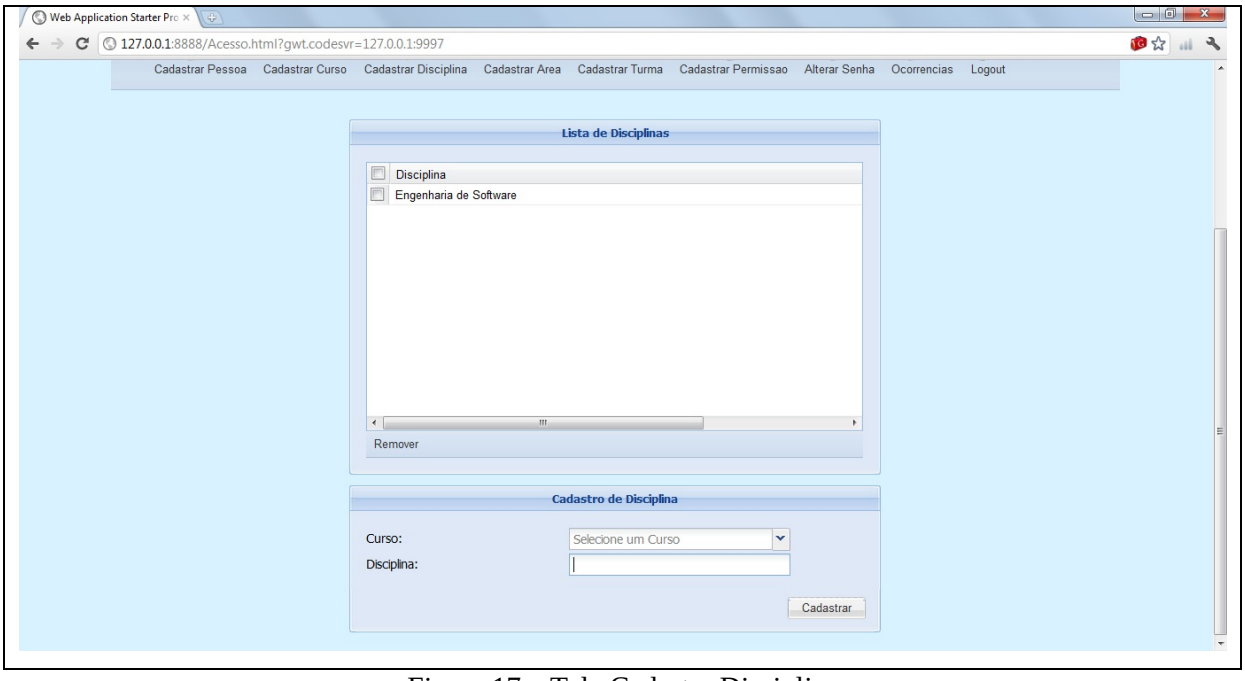


Figura 17 – Tela Cadastra Disciplina

Após, pode-se cadastrar os alunos e os professores que devem ter o acesso controlado pelo sistema. Conforme figura 18, para cadastrar uma pessoa, é necessário informar nome, *e-mail*, senha, número do seu cartão e o seu telefone. O *e-mail* será usado para que o sistema

comunique alterações de local e de data onde a pessoa irá ter aulas.

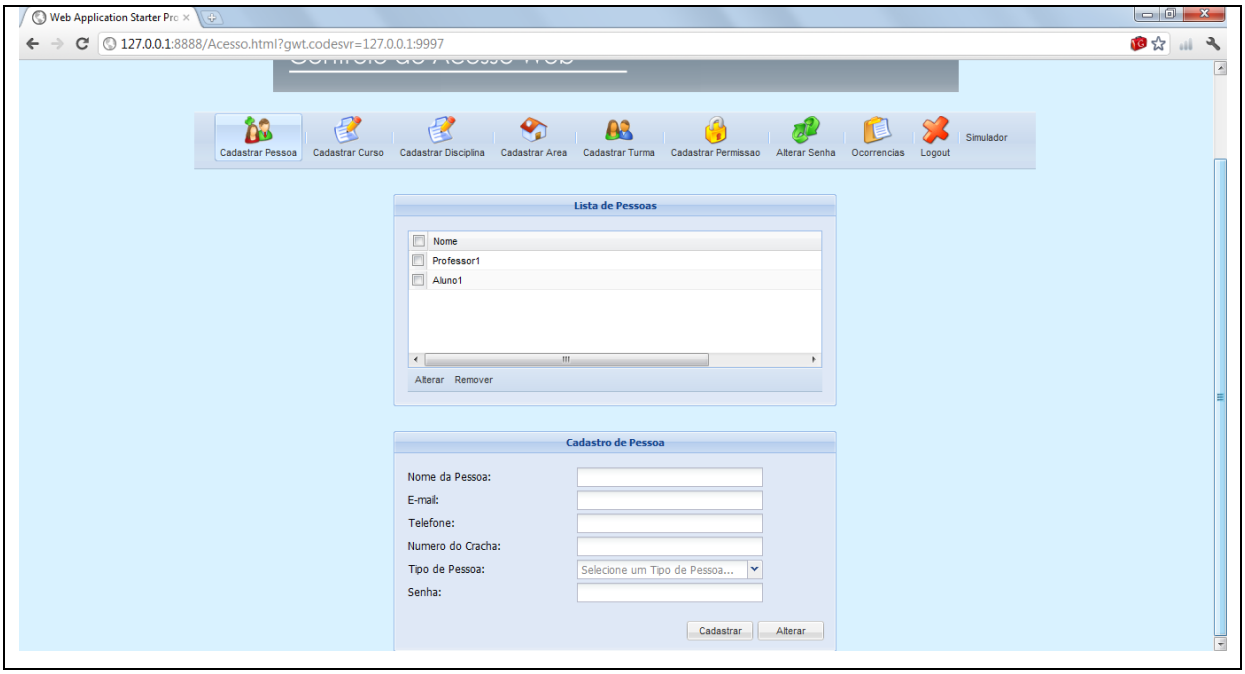


Figura 18 – Tela Cadastro de Pessoa

Efetuado o cadastro das pessoas, é necessário registrar as turmas em que estas pessoas (professores e alunos) participam (Figura 19). São as turmas que terão direitos de acessar ou não determinadas áreas. Para cadastrar-se uma turma, é necessário informar as disciplinas, os professores e os alunos, além de uma descrição que irá identificá-la dentro do sistema.

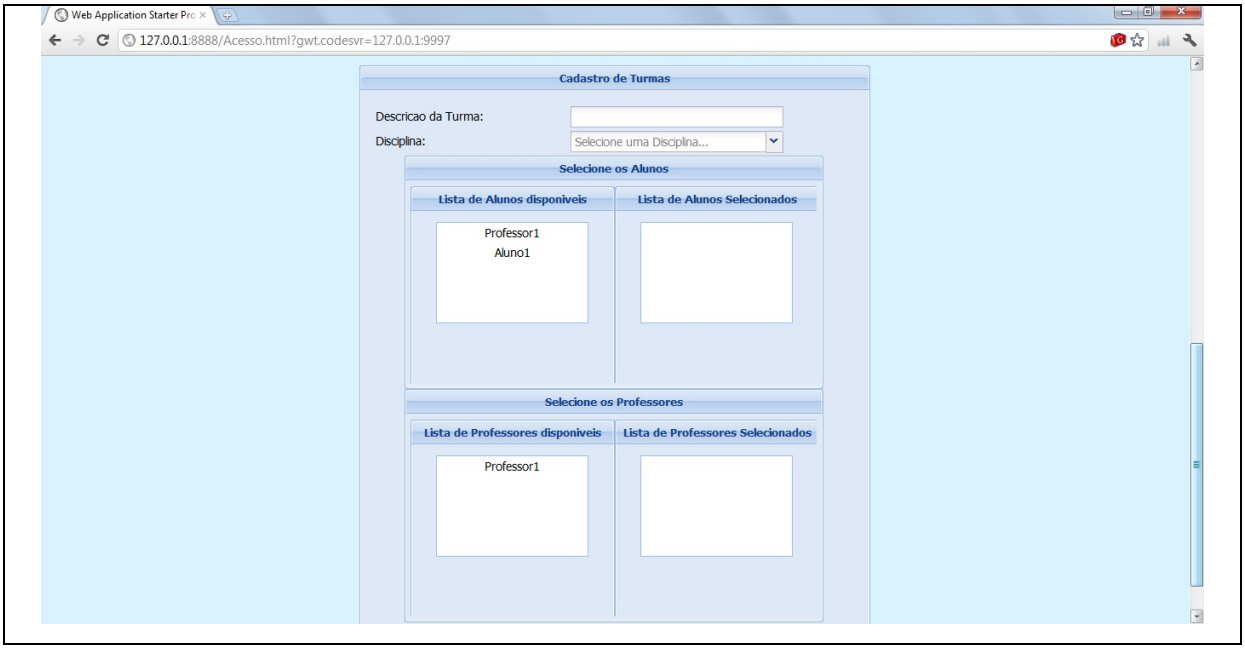


Figura 19 – Tela Cadastro de Turma

A figura 20 apresenta a tela de cadastro de áreas, estas áreas representam salas de aula e laboratórios. Cada área tem um número de dispositivo associado. Também pode ser selecionado se a área necessita que um professor acesse primeiro o ambiente, antes de qualquer aluno (acesso por autorizador).

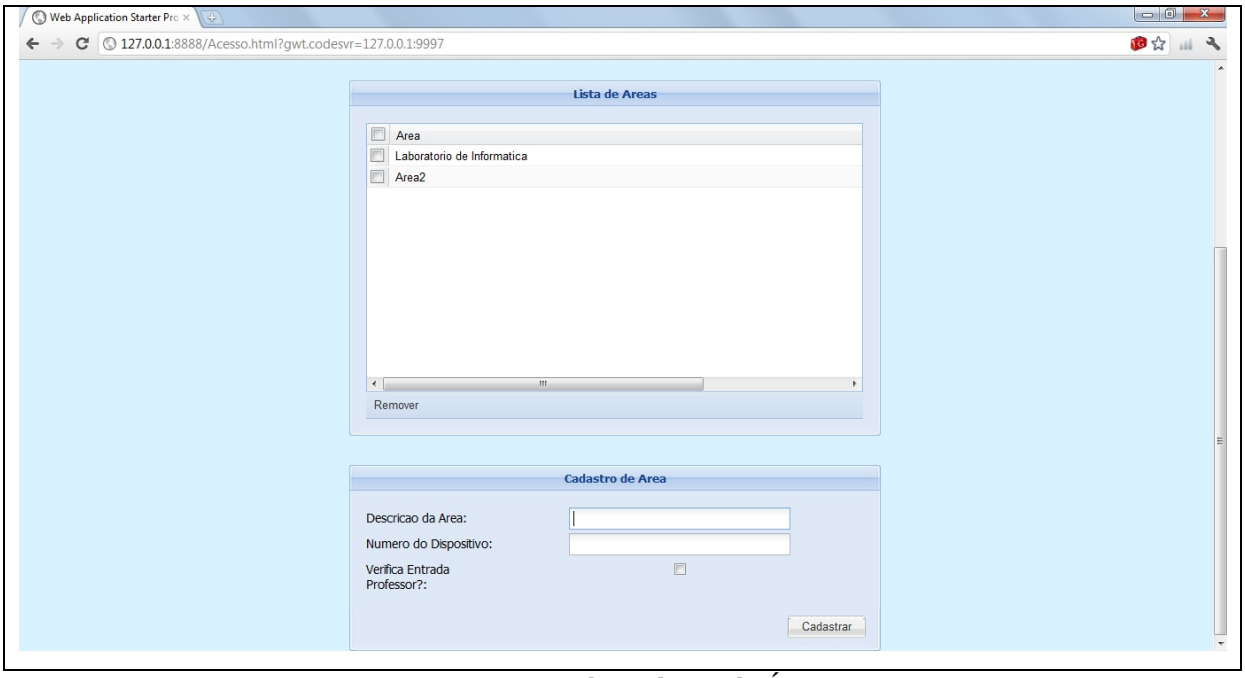


Figura 20 – Tela Cadastro de Áreas

Para efetuar a gestão das permissões e determinar quais turmas podem acessar determinadas áreas, em que dias e horários, devem ser cadastradas as permissões (Figura 21). Cada permissão contém a turma, a área, o horário de início e o horário de fim. É com estas informações que o sistema irá verificar a permissão de uma pessoa.

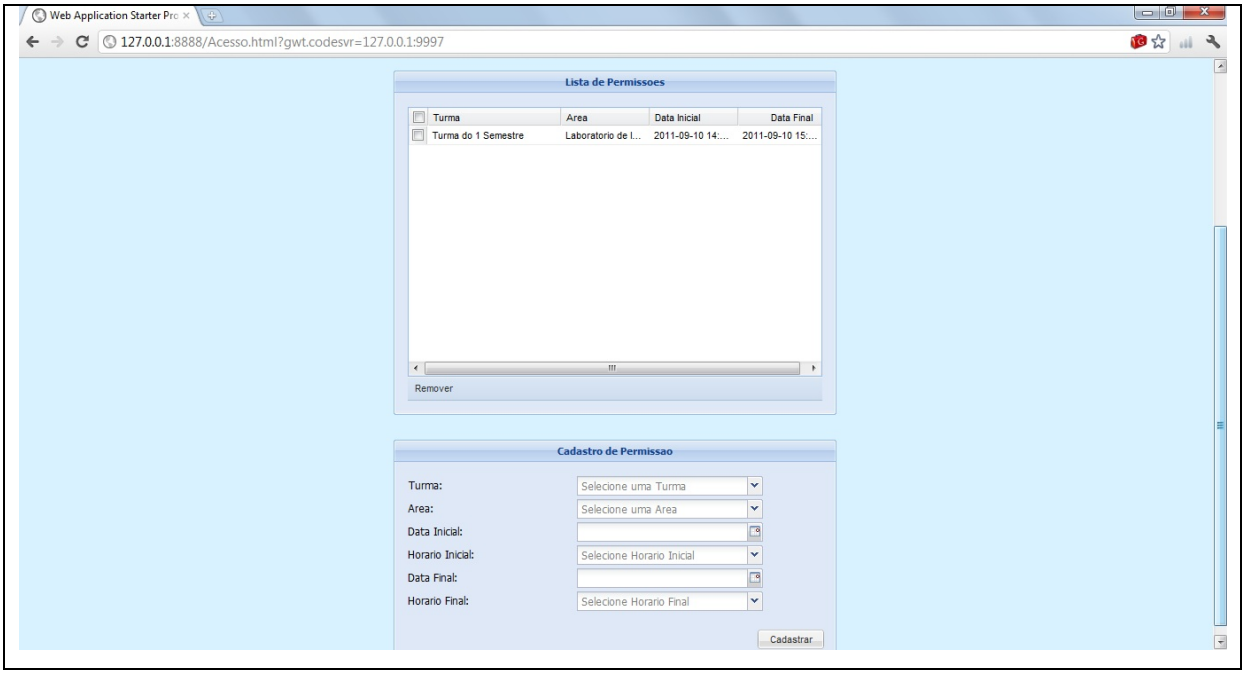


Figura 21 – Tela Cadastro de Permissão

Para efetuar o cadastro e alteração de permissões, um pré-requisito é que as áreas e turmas estejam cadastradas.

Após o cadastro da permissão um e-mail é e enviado a todas as pessoas que estão associadas à turma.

3.3.5 Processos de controle de acesso

Verifica-se a função de controle do sistema através de um simulador de acessos (que faz o papel do dispositivo que controla uma sala, por exemplo), no qual indica-se o número do crachá da pessoa e o número do dispositivo (relacionado à área). O sistema verifica então na tabela de permissões se o acesso não é um acesso repetido (no qual uma pessoa está tentando entrar duas vezes em uma mesma sala sem ter saído) (regra NEG25), verifica a necessidade de autorizador para acesso à área (regra NEG26), e por fim, libera (ou não) o acesso da pessoa. Nestes casos de acessos negados a freqüência não é registrada.

Após isto o sistema registra este acesso que poderá ser posteriormente visualizado em um relatório pelo professor responsável pela turma.

3.3.6 Processos de auditoria

Caso o acesso seja negado, por qualquer quebra de uma das regras, um outro tipo de relatório pode ser consultado, o relatório de ocorrências. A figura 22 apresenta um relatório de ocorrências do sistema. Este relatório é acessado pelo administrador do sistema e serve para controle de tentativas de acesso em áreas com controle, quando há tentativas de burlar o sistema de acesso.

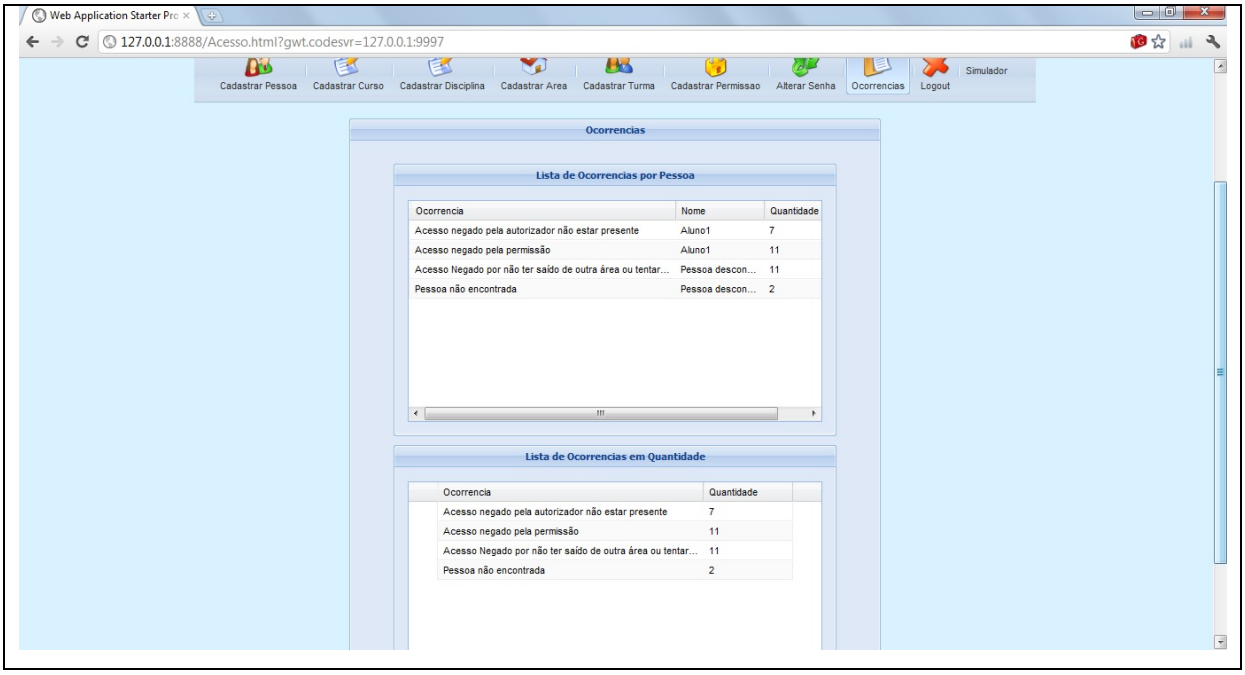


Figura 22 – Tela do relatório de ocorrências

A figura 23 apresenta a o relatório em *PDF* que registra a freqüência dos alunos de uma turma, organizados por data. Este relatório é gerado pelo professor da turma. Somente após acessos válidos apareceram registros neste documento.

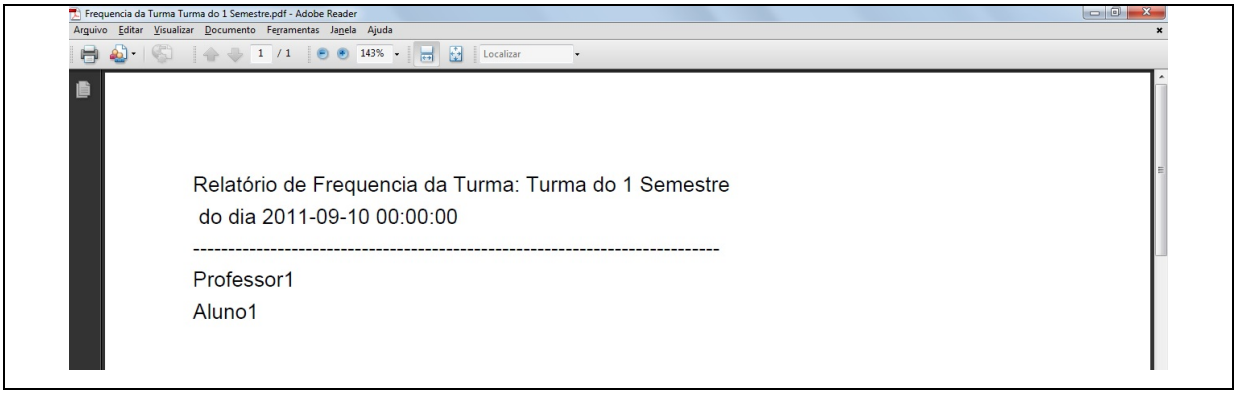


Figura 23 – Tela do relatório de freqüência

3.4 RESULTADOS E DISCUSSÃO

Através do livro de Petterson (2005), foi identificada uma necessidade de um controle de acesso no ambiente da FURB.

Foi utilizado o GWT para desenvolver um sistema simples e fácil de utilizar para *web*, para o controle de acesso na FURB.

Não foram utilizados equipamentos de controle de acesso, pois o foco do trabalho é um sistema robusto, para complementar os três trabalhos utilizados como correlatos, já que ambos tinham foco na pesquisa/desenvolvimento do hardware para controle de acesso.

Um sistema de gerenciamento de controle de acesso busca não somente fazer a integração com o equipamento e verificar a permissão ou não do usuário, mas sim gerenciar todas as áreas de acesso, todas as pessoas, todas as permissões e equipamentos que o controle de acesso necessita para funcionar.

Então com o desenvolvimento do sistema o foco foi criar um controle de acesso aos ambientes da FURB, deixando de lado, neste primeiro momento, os equipamentos necessários para isto, utilizando um simulador de acessos que imita um equipamento leitor de cartão por exemplo.

Como resultado final observa-se a evolução no controle de acesso as salas, a agilidade no controle da freqüência e a garantia de proteção do patrimônio da universidade. Através da utilização do sistema em uma situação controlada, efetuando o controle de acesso e freqüência da disciplina de Prática de Sistemas de Informação, do professor Jacques Robert Heckmann na sala C-303 na data 17 de novembro de 2011.

4 CONCLUSÕES

Os objetivos deste trabalho foram alcançados com sucesso, através da criação de um aplicativo de controle de acesso pôde-se aumentar o nível de segurança e confiabilidade no controle de acesso dos ambientes da FURB.

Para completar o sistema de segurança da Universidade são necessárias mais duas ações, bem como para completar os três pilares citados por Petterson (2005, p.2). A finalização da estrutura de segurança se conclui criando uma política de segurança e investindo em equipamentos de controle de acesso, que integram com o sistema desenvolvido.

Como o controle anterior era feito de forma manual, os resultados obtidos foram consideráveis, além do aumento da segurança do patrimônio, com o controle de freqüência integrado ao controle de acesso, houve uma mudança também no registro de presença dos acadêmicos, não tendo mais problemas com registros inválidos ou inexistentes/faltantes.

Além desta mudança, há uma alteração de conceito por parte dos alunos, sendo que é necessário ficar até o final das aulas para garantir que sua presença será computada.

Pode-se observar também uma redução no tempo desperdiçado por parte do professor em fazer o controle de freqüência, além de não precisar se preocupar com o diário de classe manual.

Com o controle de acesso implantado, não há mais problemas na utilização de salas por falta de quem as abra, também não se tem mais problemas com reservas de laboratórios.

Outra garantia é que todos os alunos recebem antecipadamente por *e-mail* o aviso onde será sua sala, caso haja uma alteração.

Portanto o investimento em um sistema controle de acesso justifica-se quando este é colocado em prática e notam-se os resultados observados acima.

4.1 EXTENSÕES

Como sugestões para trabalhos futuros, o sistema de controle de acesso poderá se integrar a diversos equipamentos de controle de acesso e ponto, pois na versão atual a ferramenta utiliza um *software* simulador.

Outra integração importante que pode ser feita é com sistemas já existentes dentro de universidades, como exemplo o sistema de matrículas da FURB.

Poderão também ser desenvolvidos relatórios sobre acesso, freqüência, distribuição geográfica e demográfica de professores e alunos para melhorar a utilização de salas.

REFERÊNCIAS BIBLIOGRÁFICAS

BORGES, Paulo Eduardo Derenne. Prevenção e execução planejadas são fundamentais | Segurança nas Instituições de Ensino, **Blog do Brasiliano**. São Paulo, [2008]. Disponível em: < http://www.brasiliano.com.br/blog/?p=1102 />. Acesso em: 18 fev. 2011.

CANEDO, José Alberto Fernandes. **Terminal de Controle de Ponto e Acesso usando biometria integrado a Web**. 2003. Monografia – Universidade Federal de Goiás, Goiânia.

D´AGOSTO, Rodrigo. **SCAPE: Sistema de Controle de Acesso e Ponto Eletrônico**. 2008. Monografia – Universidade Federal do Pará – Instituto de Tecnologia – Faculdade de Engenharia da Computação, Belém.

GLOBO NOTÍCIAS. Computador de autor do massacre em escola no Rio é achado queimado, **G1 Globo Notícias**, Rio de Janeiro, 2011. Disponível em: < http://g1.globo.com/Tragedia-em-Realengo/noticia/2011/04/computador-de-autor-do-massacre-em-escola-no-rio-e-achado-queimado.html>. Acesso em: 23 out. 2011.

JONES, Chris. **Access Control Systems**. Londres, [2011]. Disponível em: < http://www.ciaalarms.co.uk/access_control.htm/>. Acesso em: 18 mar. 2011.

LOPES JR., Rubens**. Segurança Eletrônica Proteção Ativa**. São Paulo:Sicurezza, 2000.

MAGALHÃES, Eder. GWT, **Global Code,** São Paulo, 2011. Disponível em: < http://www.globalcode.com.br/noticias/EntrevistaGWT>. Acesso em: 23 out. 2011.

PETTERSON, David G. **Implementing Physical Protection System - A pratical guide**. São Paulo:ASIS, 2005.

ROBERTO, Paulo. Ascensão do mercado de segurança privada – Crescimento e Tecnologia, **Portal da Blindagem**. São Paulo, 2011. Disponível em: <http://portaldablindagem.com.br/ascensao-do-mercado-de-seguranca-privada-%E2%80%93-crescimento-e-tecnologia.html>. Acesso em: 23 out. 2011.

ROCKENBACH, Alexis. Site Security Book, **UFRGS**. Porto Alegre, 23 out. 2011. Disponível em: < http://penta.ufrgs.br/gereseg/rfc2196/>. Acesso em: 23 out. 2011.

SANTIAGO, Simone. MATERIA. **Blog Simone Santiago**. São Paulo, 2011 Disponível em: < http://simonesantiago.blogspot.com/2008/10/segurana-patrimonial-definio.html>. Acesso em: 30 set. 2011.

SILVA, Anderson. Litoral recebe número abaixo do esperado: Dos 202 policiais civis formados pelo Estado ontem, Blumenau terá direito a um delegado, **Jornal de Santa Catarina**, Blumenau, 2011. Disponível em: <http://www.clicrbs.com.br/jsc/sc/impressa/4,784,3279804,16933>. Acesso em: 16 out. 2011.

SILVA, Luis Fernando Melati da. **Protótipo de Hardware para controle de freqüência acadêmica.** 2002. 49f. Trabalho de Conclusão de Curso (Bacharelado em Ciências da Computação) - Centro de Ciências Exatas e Naturais, Universidade Regional de Blumenau, Blumenau.

UNIVERSIDADE REGIONAL DE BLUMENAU. Infraestrutura, **Universidade Regional de Blumenau.** Blumenau, 2011a. Disponível em: <http://www.furb.br/novo/index.php?option=conteudo&Itemid=14&sis_id_lang=1>. Acesso em: 23 out. 2011.

UNIVERSIDADE REGIONAL DE BLUMENAU. **Sistema de Avaliação** Blumenau, 2011b. Disponível em: <http://www.furb.br/novo/index.php?option=conteudo&Itemid=231/>. Acesso em: 23 out. 2011.

UNIVERSIDADE REGIONAL DE BLUMENAU. **Lea** Blumenau, 2011c. Disponível em: <http://www.furb.br/lea>. Acesso em: 23 out. 2011.

APÊNDICE A – Detalhamento dos casos de uso

Segue documentação que contem o detalhamento dos casos de uso previstos no(s) diagrama(s) apresentado(s) na seção 3.2.3. No Quadro 4 apresenta-se o caso de uso "Logar no Sistema".

UC01 - Caso de uso – Logar no Sistema
Ator: Administrador/Professor
Objetivo: Entrar no sistema através de um login e de uma senha
Pré-condições: Administrador/Professor cadastrado no sistema
Pós-condições: Pessoa logada no sistema com o menu específico sendo exibido

Cenário Principal:
1. Administrador informa usuário
2. Administrador informa senha
3. Administrador clica em Logar
4. Sistema abre a tela principal, exibindo todos os menus do sistema

Cenário Alternativo:
No passo 2, administrador informa senha inválida
3.1 Sistema apresenta mensagem de erro para o informando que a senha está inválida

Cenário Alternativo:
No passo 1, Professor informar login
4.1 Professor informa senha
4.2 Professor clica em Logar
4.3 Sistema abre a tela principal, exibindo somente os menus visíveis ao professor

Quadro 4 – Descrição do caso de uso *Logar* no Sistema

No Quadro 5 apresenta-se o caso de uso "Cadastro de Pessoas".

UC02 - Caso de uso – Cadastro de pessoas
Ator: Administrador
Objetivo: Cadastrar uma pessoa nova no sistema
Pré-condições: Administrador Logado
Pós-condições: Pessoa cadastrada, alterada e exlcuida do sistema

Cenário Principal:
1. Após login, administrador acessa a tela de cadastro de pessoas
2. Administrador informa nome, telefone, senha, tipo de pessoa, email e número de cadastro
3. Administrador clica em Cadastrar
4. Sistema cadastra nova pessoa no banco

Cenário Alternativo:
No passo 2, administrador não informa os dados
3.1 Administrador clica em cadastrar

3.2 Sistema exibe uma mensagem de erro informando que é necessário preencher os campos

Cenário Alternativo:
4.1 Administrador seleciona uma pessoa na lista e clica em alterar
4.2 Sistema busca os dados da pessoa e insere nos campos de edição
4.3 Administrador alterar o nome da pessoa e clica em alterar
4.4 Sistema grava na base de dados a alteração

Cenário Alternativo:
5.1 Administrador seleciona uma pessoa na lista e clica em excluir
5.2 Sistema exclui a pessoa da base de dados

Quadro 5 – Descrição do caso de uso Cadastro de Pessoa

No Quadro 6 apresenta-se o caso de uso "`Alterar Senha`".

UC03 - Caso de uso – Alterar Senha
Ator: Administrador/Professor
Objetivo: Alterar a senha de uma pessoa
Pré-condições: Administrador/Professor logado no sistema
Pós-condições: Pessoa alterou sua senha

Cenário Principal:
1. Administrador acessa a tela de alteração de senha
2. Administrador informa nova senha
3. Sistema altera a senha na base

Cenário Alternativo:
No passo 2, administrador informa senha em branco
3.1 Sistema apresenta mensagem de erro para o informando que a senha está inválida

Quadro 6 – Descrição do caso de uso Alterar Senha

No Quadro 7 apresenta-se o caso de uso "`Cadastrar Turmas`".

UC04 - Caso de uso – Cadastrar Turma
Ator: Administrador
Objetivo: Cadastrar e excluir uma turma
Pré-condições: Administrador logado no sistema
Pós-condições: Administrador cadastrou e excluiu uma turma

Cenário Principal:
1. Administrador acessa a tela de cadastro de turma
2. Administrador informa disciplina, professores e alunos da turma
3. Administrador clica em cadastrar
4. Sistema cadastra uma nova turma

Cenário Alternativo:
No passo 2, administrador informa os dados em branco

3.1 Sistema apresenta mensagem de erro para o informando que todos os campos são obrigatórios **Cenário Alternativo:** 4.1 Administrador seleciona uma turma para excluir 4.2 Administrador clica em exluir 4.3 Sistema exclui a turma da base de dados

Quadro 7 – Descrição do caso de uso Cadastrar Turmas

No Quadro 8 apresenta-se o caso de uso "`Cadastrar Curso`".

UC05 - Caso de uso – Cadastrar Curso **Ator:** Administrador **Objetivo:** Cadastrar e excluir um curso **Pré-condições:** Administrador logado no sistema **Pós-condições:** Administrador cadastrou e excluiu um curso **Cenário Principal:** **1.** Administrador acessa a tela de cadastro de curso **2.** Administrador informa descrição do curso **3.** Administrador clica em cadastrar 4. Sistema cadastra um novo curso **Cenário Alternativo:** No passo 2, administrador informa os dados em branco 3.1 Sistema apresenta mensagem de erro para o informando que todos os campos são obrigatórios **Cenário Alternativo:** 4.1 Administrador seleciona um curso para excluir 4.2 Administrador clica em exluir 4.3 Sistema exclui o curso da base de dados

Quadro 8 – Descrição do caso de uso Cadastrar Curso

No Quadro 9 apresenta-se o caso de uso "`Cadastrar Disciplina`".

UC06 - Caso de uso – Cadastrar Disciplina **Ator:** Administrador **Objetivo:** Cadastrar e excluir uma disciplina **Pré-condições:** Administrador logado no sistema **Pós-condições:** Administrador cadastrou e excluiu uma disciplina **Cenário Principal:** **1.** Administrador acessa a tela de cadastro de disciplina **2.** Administrador informa qual o curso e a descrição da disciplina **3.** Administrador clica em cadastrar

4. Sistema cadastra uma nova disciplina

Cenário Alternativo:
No passo 2, administrador informa os dados em branco
3.1 Sistema apresenta mensagem de erro para o informando que todos os campos são obrigatórios

Cenário Alternativo:
4.1 Administrador seleciona uma disciplina para excluir
4.2 Administrador clica em exluir
4.3 Sistema exclui a disciplina da base de dados

Quadro 9 – Descrição do caso de uso Cadastrar Disciplina

No Quadro 10 apresenta-se o caso de uso "`Cadastrar Àrea`".

UC07 - Caso de uso – Cadastrar Área
Ator: Administrador
Objetivo: Cadastrar e excluir uma área
Pré-condições: Administrador logado no sistema
Pós-condições: Administrador cadastrou e excluiu uma área

Cenário Principal:
1. Administrador acessa a tela de cadastro de área
2. Administrador informa descrição da área e o número do dispositivo
3. Administrador clica em cadastrar
4. Sistema cadastra uma nova área

Cenário Alternativo:
No passo 2, administrador informa os dados em branco
3.1 Sistema apresenta mensagem de erro para o informando que todos os campos são obrigatórios

Cenário Alternativo:
4.1 Administrador seleciona uma área para excluir
4.2 Administrador clica em exluir
4.3 Sistema exclui a área da base de dados

Quadro 10 – Descrição do caso de uso Cadastrar Área

No Quadro 11 apresenta-se o caso de uso "`Cadastrar Permissão`".

UC08 - Caso de uso – Cadastrar Permissão
Ator: Administrador
Objetivo: Cadastrar e excluir uma permissaõ
Pré-condições: Administrador logado no sistema
Pós-condições: Administrador cadastrou e excluiu uma permissão

Cenário Principal:
1. Administrador acessa a tela de cadastro de permissão
2. Administrador informa área, turma, data/hora inicial e final
3. Administrador clica em cadastrar
4. Sistema cadastra uma nova permissão

Cenário Alternativo:
No passo 2, administrador informa os dados em branco
3.1 Sistema apresenta mensagem de erro para o informando que todos os campos são obrigatórios

Cenário Alternativo:
4.1 Administrador seleciona uma permissão para excluir
4.2 Administrador clica em exluir
4.3 Sistema exclui a permissão da base de dados

Quadro 11 – Descrição do caso de uso Cadastrar Permissão

No Quadro 12 apresenta-se o caso de uso "`Gerar Relatório`".

UC09 - Caso de uso – Gerar Relatório
Ator: Professor
Objetivo: Gerar relatório de frequencia
Pré-condições: Professor logado no sistema
Pós-condições: Professor com o relatório gerado

Cenário Principal:
1. Professor acessa a tela de realtório
2. Professor informa turma e data
3. Administrador clica em Gerar

4. Sistema gerar o relatório no C:\

Cenário Alternativo:
No passo 2, professor não informa data
3.1 Sistema gera relatório com todas as datas da turma

Quadro 12 – Descrição do caso de uso Gerar Relatório

No Quadro 13 apresenta-se o caso de uso "`Controle de Acesso`".

UC10 - Caso de uso – Controle de Acesso
Ator: Usuário
Objetivo: Controlar o acesso de qualquer usuário
Pré-condições: Simular em funcionamento
Pós-condições: Controle de acesso efetuado

Cenário Principal:
1. Usuário simula um acesso com um crachá válido que tenha permissão na área
2. O sistema controla o acesso e libera como acesso permitido

Cenário Alternativo:
2.1 Usuário simula um acesso com um crachá que não existe no sistema
2.2 O sistema controla o acesso e nega pela permissão

Cenário Alternativo:
3.1 Usuário simula um acesso com um crachá em uma área que valida permissão do professor
3.2 O sistema controla o acesso e nega acesso por autorizador não está presente

Cenário Alternativo:
4.1 Usuário simula um acesso com um crachá válido na mesma área do mesmo passo 1
4.2 O sistema controla o acesso e nega acesso por anti-dupla

Quadro 13 – Descrição do caso de uso Controle de Acesso

No Quadro 14 apresenta-se o caso de uso "`Controle de Ocorrências`".

UC11 - Caso de uso – Controle de Ocorrência
Ator: Usuário
Objetivo: Controlar as ocorrências no sistema
Pré-condições: Simular em funcionamento
Pós-condições: Controle de acesso efetuado

Cenário Principal:
1. Usuário simula um acesso com um crachá que não existe no sistema
2. O sistema controla o acesso e nega pela permissão gravando uma ocorrência na base

Cenário Alternativo:

Cenário Alternativo:
2.1 Usuário simula um acesso com um crachá em uma área que valida permissão do professor
2.2 O sistema controla o acesso e nega acesso por autorizador não está presente gravando uma ocorrência na base

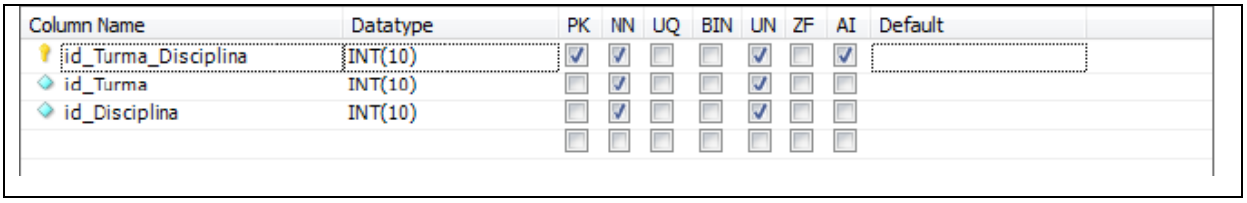
Cenário Alternativo:
3.1 Usuário simula um acesso com um crachá válido na mesma área do mesmo passo 1
3.2 O sistema controla o acesso e nega acesso por anti-dupla gravando uma ocorrência na base

Quadro 14 – Descrição do caso de uso Controle de Ocorrências

APÊNDICE B – Detalhamento do dicionário de dados

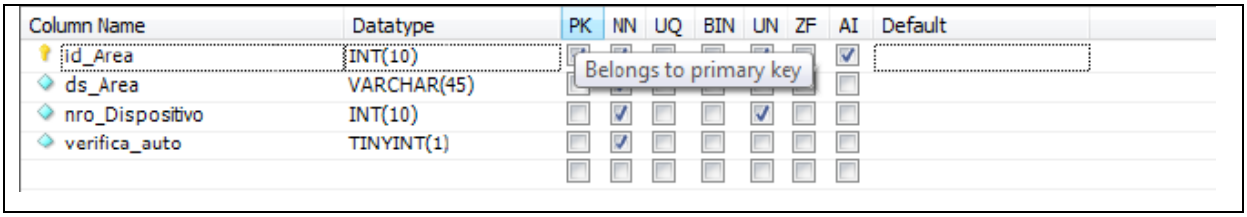
Segue documentação que contem o detalhamento do dicionário de dados, descrevendo o MER que está na seção 3.2.6.

Na figura 24 a 33 estão presentes os dados de todas as tabelas utilizadas pelo sistema, onde PK representa as chaves primárias da tabela, NN representa se o campo não pode ser vazio, UM representa qual campo é chave única e AI representa que o campo é auto incremental.



Column Name	Datatype	PK	NN	UQ	BIN	UN	ZF	AI	Default
id_Turma_Disciplina	INT(10)	☑	☑	☐	☐	☑	☐	☑	
id_Turma	INT(10)	☐	☑	☐	☐	☑	☐	☐	
id_Disciplina	INT(10)	☐	☑	☐	☐	☑	☐	☐	

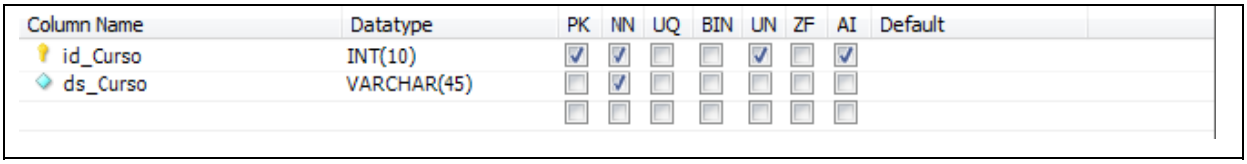
Figura 24 – Dicionário da tabela turma_disciplina



Column Name	Datatype	PK	NN	UQ	BIN	UN	ZF	AI	Default
id_Area	INT(10)	☑						☑	
ds_Area	VARCHAR(45)							☐	
nro_Dispositivo	INT(10)	☐	☑	☐	☐	☑	☐	☐	
verifica_auto	TINYINT(1)	☐	☑	☐	☐	☐	☐	☐	

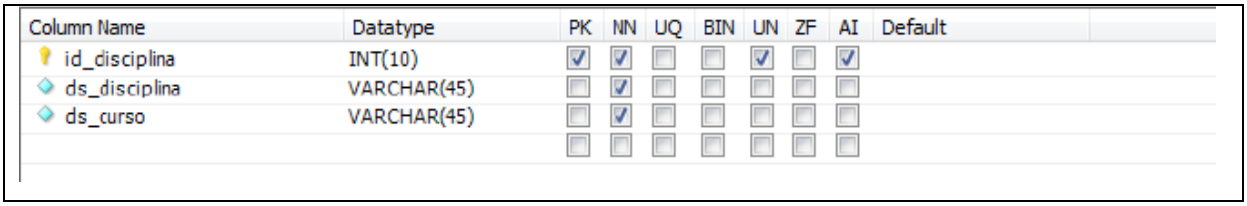
Belongs to primary key

Figura 25 – Dicionário da tabela area



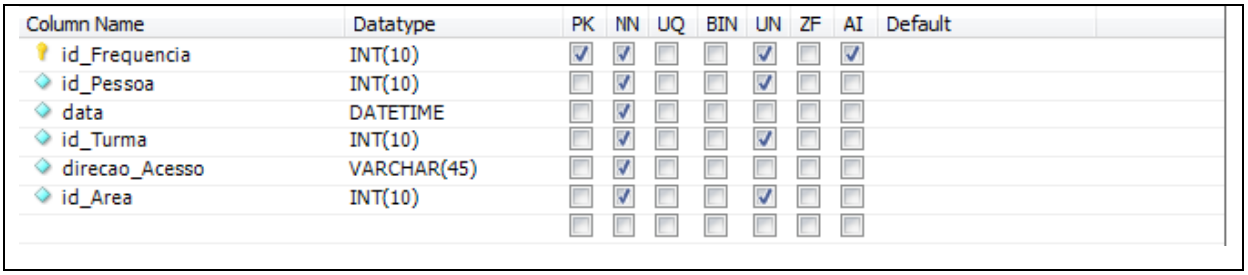
Column Name	Datatype	PK	NN	UQ	BIN	UN	ZF	AI	Default
id_Curso	INT(10)	☑	☑	☐	☐	☑	☐	☑	
ds_Curso	VARCHAR(45)	☐	☑	☐	☐	☐	☐	☐	

Figura 26 – Dicionário da tabela curso



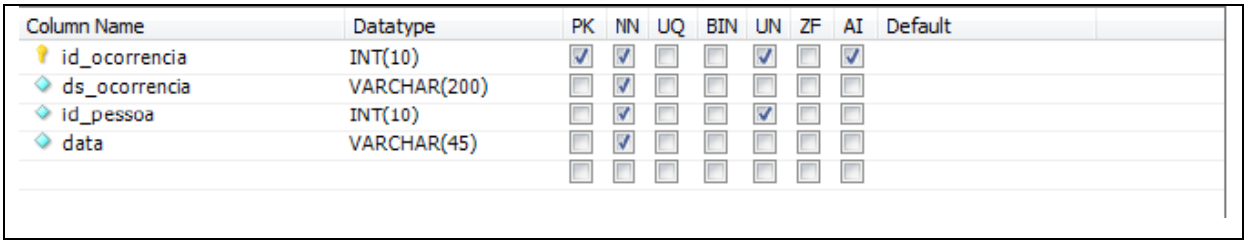
Column Name	Datatype	PK	NN	UQ	BIN	UN	ZF	AI	Default
id_disciplina	INT(10)	☑	☑	☐	☐	☑	☐	☑	
ds_disciplina	VARCHAR(45)	☐	☑	☐	☐	☐	☐	☐	
ds_curso	VARCHAR(45)	☐	☑	☐	☐	☐	☐	☐	

Figura 27 – Dicionário da tabela disciplina



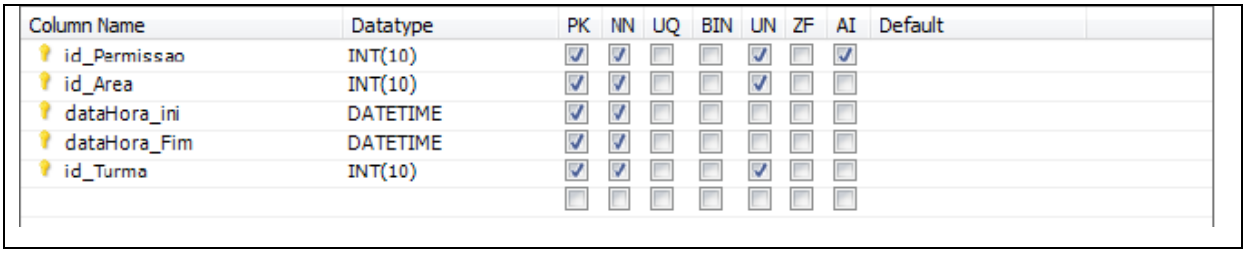
Column Name	Datatype	PK	NN	UQ	BIN	UN	ZF	AI	Default
id_Frequencia	INT(10)	☑	☑	☐	☐	☑	☐	☑	
id_Pessoa	INT(10)	☐	☑	☐	☐	☑	☐	☐	
data	DATETIME	☐	☑	☐	☐	☐	☐	☐	
id_Turma	INT(10)	☐	☑	☐	☐	☑	☐	☐	
direcao_Acesso	VARCHAR(45)	☐	☑	☐	☐	☐	☐	☐	
id_Area	INT(10)	☐	☑	☐	☐	☑	☐	☐	

Figura 28 – Dicionário da tabela freqüência



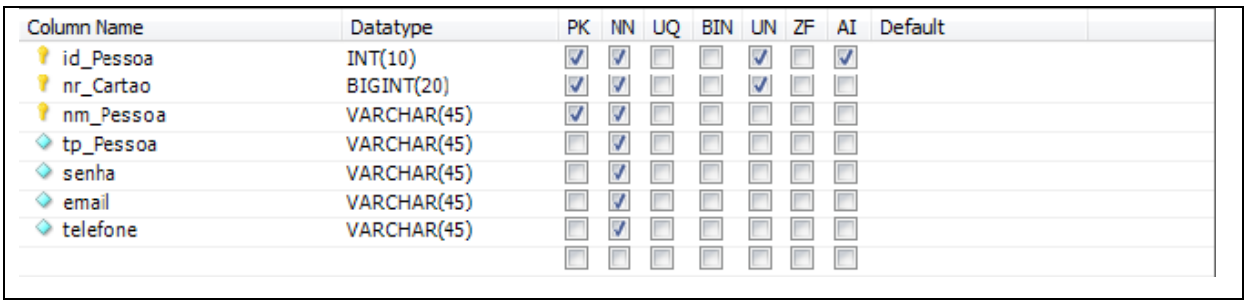
Column Name	Datatype	PK	NN	UQ	BIN	UN	ZF	AI	Default
id_ocorrencia	INT(10)	☑	☑	☐	☐	☑	☐	☑	
ds_ocorrencia	VARCHAR(200)	☐	☑	☐	☐	☐	☐	☐	
id_pessoa	INT(10)	☐	☑	☐	☐	☑	☐	☐	
data	VARCHAR(45)	☐	☑	☐	☐	☐	☐	☐	

Figura 29 – Dicionário da tabela ocorrência



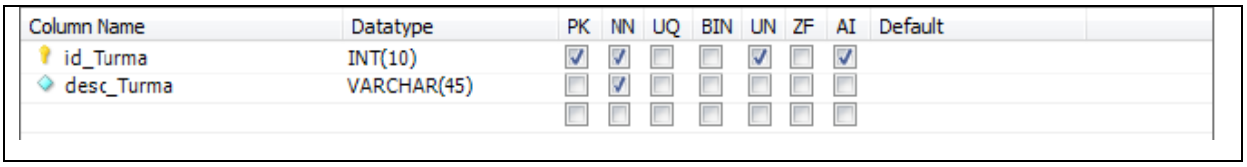
Column Name	Datatype	PK	NN	UQ	BIN	UN	ZF	AI	Default
id_Permissao	INT(10)	☑	☑	☐	☐	☑	☐	☑	
id_Area	INT(10)	☑	☑	☐	☐	☑	☐	☐	
dataHora_ini	DATETIME	☑	☑	☐	☐	☐	☐	☐	
dataHora_Fim	DATETIME	☑	☑	☐	☐	☐	☐	☐	
id_Turma	INT(10)	☑	☑	☐	☐	☑	☐	☐	

Figura 30 – Dicionário da tabela permissão



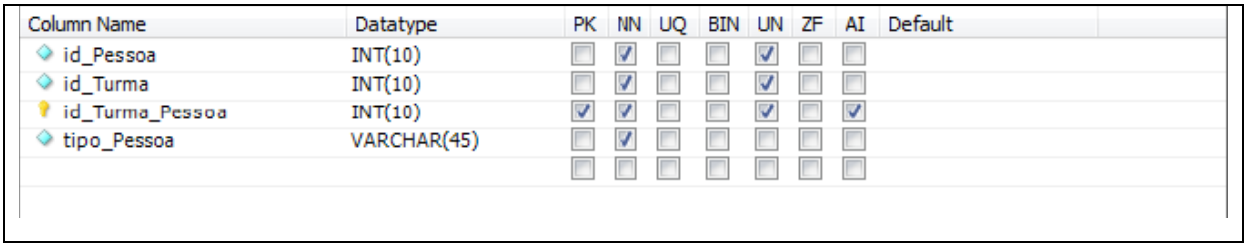
Column Name	Datatype	PK	NN	UQ	BIN	UN	ZF	AI	Default
id_Pessoa	INT(10)	☑	☑	☐	☐	☑	☐	☑	
nr_Cartao	BIGINT(20)	☑	☑	☐	☐	☑	☐	☐	
nm_Pessoa	VARCHAR(45)	☑	☑	☐	☐	☐	☐	☐	
tp_Pessoa	VARCHAR(45)	☐	☑	☐	☐	☐	☐	☐	
senha	VARCHAR(45)	☐	☑	☐	☐	☐	☐	☐	
email	VARCHAR(45)	☐	☑	☐	☐	☐	☐	☐	
telefone	VARCHAR(45)	☐	☑	☐	☐	☐	☐	☐	

Figura 31 – Dicionário da tabela pessoa



Column Name	Datatype	PK	NN	UQ	BIN	UN	ZF	AI	Default
id_Turma	INT(10)	☑	☑	☐	☐	☑	☐	☑	
desc_Turma	VARCHAR(45)	☐	☑	☐	☐	☐	☐	☐	

Figura 32 – Dicionário da tabela turma



Column Name	Datatype	PK	NN	UQ	BIN	UN	ZF	AI	Default
id_Pessoa	INT(10)	☐	☑	☐	☐	☑	☐	☐	
id_Turma	INT(10)	☐	☑	☐	☐	☑	☐	☐	
id_Turma_Pessoa	INT(10)	☑	☑	☐	☐	☑	☐	☑	
tipo_Pessoa	VARCHAR(45)	☐	☑	☐	☐	☐	☐	☐	
		☐	☐	☐	☐	☐	☐	☐	

Figura 33 – Dicionário da tabela turma_pessoa