UNIVERSIDADE REGIONAL DE BLUMENAU

CENTRO DE CIÊNCIAS EXATAS E NATURAIS

CURSO DE CIÊNCIA DA COMPUTAÇÃO – BACHARELADO

PROTÓTIPO DE AMBIENTE VIRTUAL DE AVALIAÇÕES UTILIZANDO CERTIFICADOS DIGITAIS

FERNANDO GEVARD

BLUMENAU
2011

2011/1-19

FERNANDO GEVARD

PROTÓTIPO DE AMBIENTE VIRTUAL DE AVALIAÇÕES UTILIZANDO CERTIFICADOS DIGITAIS

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 Ciência da Computação — Bacharelado.

Prof. Paulo Fernando da Silva , Ms. - Orientador

BLUMENAU
2011

2011/1-19

PROTÓTIPO DE AMBIENTE VIRTUAL DE AVALIAÇÕES UTILIZANDO CERTIFICADOS DIGITAIS

Por

FERNANDO GEVARD

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

Presidente:	Prof. Paulo Fernando da Silva, Ms. – Orientador, FURB
Membro:	Prof. Francisco Adell Péricas, Ms. – FURB
Membro:	Prof. Sérgio Stringari, Ms. – FURB

Blumenau, 27 de junho de 2011.

Dedico este trabalho aos meus pais, Valmir e Carla, a minha noiva Bianca, a minha irmã Jéssica e a todos os amigos que colaboraram para a sua realização.

AGRADECIMENTOS

A Deus, por ter me abençoado em todas as áreas, por ter me dado muita força e por ter atendido todas as minha orações.

Aos meus pais Valmir Gevard e Carla Lúcia Colley Gevard, pelo amor, pela força, pelo total incentivo e apoio, e principalmente por sempre priorizarem a conclusão da minha graduação.

A minha noiva Bianca Custódio, por toda a paciência, carinho, amor e confiança em mim depositados.

Ao meu grande amigo Andrey Carmisini, pela sincera amizade, pela constante companhia desde o início do curso, e por ter me ajudado e me apoiado durante a realização deste trabalho e de todo o curso.

Ao meu orientador, Paulo Fernando da Silva, por ter acreditado na minha capacidade, me orientando para a conclusão deste trabalho.

A todos que contribuíram, indiretamente, para a realização deste trabalho.

RESUMO

Este trabalho apresenta o desenvolvimento de um ambiente virtual que permite a criação e a execução de avaliações entre professores e alunos. O ambiente também implementa os requisitos de segurança autenticação do usuário e trilhas de auditoria. O diferencial deste trabalho está na utilização de um certificado digital (E-CPF) do tipo A1 da Infraestrutura de Chaves Públicas Brasileira (ICP-BRASIL). O certificado digital é utilizado para autenticar o administrador do ambiente virtual e para permitir que este usuário possa assinar digitalmente o diploma virtual de um aluno. Para o desenvolvimento do ambiente utilizou-se a linguagem de programação PHP e o ambiente de programação DreamWeaver CS5 juntamente com o banco de dados MySQL.

Palavras-chave: E-CPF. ICP-BRASIL. Certificados digitais. Assinatura digital. Avaliações. Segurança da informação.

ABSTRACT

This papper presents the development of a virtual environment that enables the creation and implementation of tests between teachers and students. The environment also implements the security requirements user authentication and audit trails. The differential of this papper is to use a digital certificate (E-CPF) type A1 of the Brazilian Public Key Infrastructure (ICP-BRAZIL). The digital certificate is used to authenticate the administrator of the virtual environment and to allow this user to digitally sign the virtual diploma of a student. For the development of the environment used the PHP programming language and programming environment DreamWeaver CS5 with the MySQL Database.

Key-words: E-CPF. ICP-BRAZIL. Digital certificates. Digital signature. Tests. Ratings. Information security.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

AC – Autoridade Certificadora

AVA – Ambiente Virtual de Aprendizagem

AVACD – Protótipo de Ambiente Virtual de Avaliações Utilizando Certificados Digitais

CI – Carteira de Identidade

CNPJ – Cadastro Nacional de Pessoa Jurídica

CPF – Cadastro de Pessoa Física

DER – Diagrama de Entidade-Relacionamento

EaD – Ensino à Distância

e-CPF – Cadastro de Pessoa Física Eletrônico

FURB - Universidade Regional de Blumenau

HTML - *HyperText Markup Language*

HTTPS - *HyperText Transfer Protocol Secure*

ICP-BRASIL - Infraestrutura de Chaves Públicas Brasileira

MD5 - *Message-Digest algorithm* 5

PHP - *Hypertext Preprocessor*

RSA - Rivest Shamir Adleman

SSL - *Secure Sockets Layer*

TIC - Tecnologias de Informação e Comunicação

UML - *Unified Modeling Language*

SUMÁRIO

1 INTRODUÇÃO

As primeiras propostas de Educação a Distância (EaD) surgiram em forma de livros, cartilhas e até mesmo de guias especialmente redigidos para este nicho do ensino. Nos anos 70, a televisão e o rádio começaram a fazer parte do conjunto de propostas a serem utilizadas na EaD. Já com a chegada dos anos 80, as mídias de áudio e vídeo como fitas cassete, entraram para este seleto conjunto de materiais viabilizadores deste método de ensino. Mas segundo Litto (2006, p. 64), foi com a chegada da internet nos anos 90, e sua disseminação ao longo desta década, que as possibilidades e as oportunidades fizeram com que o ensino a distância alcançasse o seu ápice, desenvolvendo-se e ampliando-se de forma surpreendente.

Na EaD, as novas tecnologias ampliam o espectro das formas do ensino e da aprendizagem numa dimensão quase inimaginável, possibilitam aos estudantes formas de ativação jamais conhecidas antes, o que pode tornar a aprendizagem mais atraente e eficiente, e consequentemente amplia-se o espaço para decisões didáticas (PETERS, 2001, p. 230).

Com o passar dos anos, as novas tecnologias atingem mais indivíduos. Isso faz com que esses acabem sempre procurando alguma forma para facilitar o seu trabalho. Maia (2003, p. 104) aponta a EaD como uma alternativa viável para atender a uma grande demanda que existe na educação do país. Além disso, o tema Ambiente Virtual de Aprendizagem (AVA) ainda é um campo de pesquisa muito recente e por este motivo, é difícil encontrar ambientes virtuais via web para avaliação online que proporcione ao professor auxílio eficiente na avaliação de seus alunos e que protejam os dados adequadamente.

Segundo Paula (2005, p. 10), a proteção das informações é muito importante para uma empresa ou instituição, pois em muitos casos a informação representa o sucesso dos negócios, e nesse caso, a perda ou roubo de informação pode representar um grande prejuízo.

Dias (2000, p. 40) comenta sobre a importância da segurança da informação, afirmando que muitas vezes as informações são consideradas um dos maiores patrimônios de uma instituição, e por este motivo estão sujeitas a um grande risco.

Segundo Pereira (2007, p. 9), um AVA pode possuir inúmeras funcionalidades, ou seja, o desenvolvimento de um AVA pode ser bastante complexo, exigindo muito mais do que o tempo disponível para execução deste trabalho.

Diante do exposto, é desenvolvido somente a funcionalidade de avaliações, que permita ao professor cadastrar questões em um banco de dados e gerar uma prova a partir das questões cadastradas, e que permita ao aluno executar as avaliações geradas pelo professor.

Para executar estes processos serão utilizados alguns importantes requisitos de segurança, tais como: certificados digitais, assinatura digital, função de *hash*[1], autenticação do usuário e trilhas de auditoria.

1.1 OBJETIVOS DO TRABALHO

O objetivo deste trabalho é o desenvolvimento de um Protótipo de Ambiente Virtual de Avaliações, que permita ao professor criar avaliações para serem executadas pelos alunos e que utilize certificados digitais, assinatura digital, trilhas de auditoria, autenticação e função de *hash*.

Os objetivos específicos do trabalho são:

a) disponibilizar um sistema via *web* para um professor cadastrar questões e gerar avaliações para serem executadas por seus alunos;
b) garantir o controle de acesso de usuários com certificado digital;
c) garantir o controle de acesso às informações e a autenticação do usuário;
d) garantir a proteção das senhas de acesso dos usuários utilizando funções de *hash;*
e) garantir a trilha de auditoria para visualizar as ações dos usuários;
f) apresentar um relatório final com o resultado da avaliação executada pelo aluno;
g) garantir a geração de um diploma[2] virtual do aluno, contendo informações sobre o aluno e a assinatura digital do diretor do sistema, utilizando um e-CPF;
h) garantir que qualquer usuário do sistema possa fazer a verificação da assinatura digital do diploma virtual do aluno.

1.2 ESTRUTURA DO TRABALHO

Este trabalho está estruturado em quatro capítulos. O segundo capítulo contém a

[11] *Hash* - é uma sequência de caracteres (letras ou números) gerada por um algoritmo de dispersão que transforma uma grande quantidade de dados em uma pequena quantidade. Geralmente, é uma variável que serve para identificar grandes cadeias de dados (PEREIRA, 2009).

fundamentação teórica necessária para o entendimento do trabalho. Nele são discutidos tópicos relacionados a avaliações à distância, aos aspectos de segurança da informação, a certificado digital, a Infraestrutura de Chaves Públicas Brasileira (ICP-BRASIL) e apresentam-se dois trabalhos correlatos.

O terceiro capítulo trata sobre o desenvolvimento do ambiente, onde são explanados os principais requisitos do problema trabalhado, a especificação contendo diagramas de caso de uso, classe e seqüência. Também são feitos sobre os resultados e discussão.

O quarto capítulo refere-se às conclusões do presente trabalho e sugestões para trabalhos futuros.

[2] Diploma é o documento legal que confere um grau acadêmico ao discente que completou, com sucesso, um determinado programa de estudos: curso de graduação, curso superior de formação específica (sequencial) ou programa de pós-graduação (mestrado ou doutorado) (UNIVERSIDADE REGIONAL DE BLUMENAU, 2009).

2 FUNDAMENTAÇÃO TEÓRICA

Na seção 2.1 é abordado avaliações à distância. Na seção 2.2 são apresentados os aspectos de segurança da informação, abordando certificado digital, criptografia, auditoria, autenticação, dentre outros, e por fim, na seção 2.3 são apresentados trabalhos correlatos ao tema em questão.

2.1 AVALIAÇÕES À DISTÂNCIA

Segundo Fáveri e Kruscinsck (2004, p. 78), as avaliações servem para "controlar os alunos, medir e quantificar saberes, condicionar e intensificar comportamentos". Além disso, Fáveri e Kruscinsck (2004, p. 80) afirmam que "a avaliação não poderia ser deixada de lado, pois ela faz parte do conjunto das ações pedagógicas, como por exemplo, a seleção de conteúdos a serem trabalhados e os encaminhamentos didático-metodológicos".

Para Staa (2007), as avaliações *online* oferecem vantagens suficientes para substituir as avaliações em papel, além de aumentar a freqüência de aplicação de avaliações, a facilidade para fazer a correção, e também por reduzir o gasto de papel.

Para realizar a construção e a execução de uma avaliação através da *web* é conveniente que se utilize um ambiente virtual. Segundo Pereira (2007, p. 5), "O Ambiente Virtual de Aprendizagem (AVA) consiste em uma opção de mídia que está sendo utilizada para mediar o processo ensino-aprendizagem à distância."

> A EaD, conhecida também como Ensino a Distância, teve seu início sem data muito precisa, porém pode-se assegurar que no século XVIII houve o oferecimento de cursos por correspondência. Impulsionado pelos avanços científicos e tecnológicos e pela demanda e necessidade social, a oferta de cursos a distância aumentou e, novas mídias, à medida que aparecem, foram utilizadas como suporte. A popularização da Internet nos anos 90, permitiu a construção de ambientes virtuais de aprendizagem através dos quais a comunicação entre os participantes pôde acontecer em qualquer lugar, a qualquer hora na modalidade de um para um, um para muitos, muitos para um e muitos para muitos. (MORAES, 2004, p. 38).

De acordo com Bastos (2003, p. 78), o termo EaD relaciona o fato de pessoas estarem em diferentes espaços geográficos, de possuir vínculo com uma instituição de ensino, e de ser desenvolvida através de Tecnologias de Informação e Comunicação (TIC).

Apesar da educação no Brasil via internet ainda ser recente, a mesma já faz parte da

legislação brasileira. Segundo Pereira (2007, p. 7), o poder público deve incentivar o desenvolvimento e a veiculação de programas EaD.

De acordo com Brasil (2005), a mesma pode ser ofertada nos seguintes níveis e modalidades de ensino:

a) educação básica;

b) educação de jovens e adultos;

c) educação especial;

d) educação profissional;

e) educação superior (graduação, especialização, mestrado e doutorado).

Além disso, este mesmo conceitua e afirma que o ensino à distância relaciona a utilização de meios de tecnologia de informação e comunicação com estudantes e professores desenvolvendo atividades educativas em lugares ou tempos diversos.

No desenvolvimento de um AVA, existem muitas funcionalidades diferentes que podem ser aplicadas, mas segundo Moran (2002), professores e alunos devem interagir de acordo com suas necessidades.

> O número de recursos e ferramentas já desenvolvidos e, em desenvolvimento, para a educação baseada na web está incentivando a utilização desses ambientes virtuais como apoio ao ensino presencial e como modalidade única de ensino-aprendizagem. Diante deste cenário, torna-se cada vez mais complicado escolher, entre outras opções, as que melhor ajustam-se às necessidades e aos objetivos dos programas educacionais. Certamente não existe uma escolha correta, mas sim ambientes que se moldam melhor a determinados propósitos. (PEREIRA, 2007, p. 9).

Para que se possa moldar um ambiente virtual de avaliação da melhor forma possível é preciso observar e especificar bem as necessidades do curso e do público alvo que fará uso desta ferramenta.

A tecnologia aplicada ao processo de ensino-aprendizagem pode concentrar-se no contexto de um AVA. Com esta abordagem, surge a tecnologia educacional.

> Tecnologia educacional é um processo integrado complexo, que envolve pessoas, procedimentos, idéias, recurso e organização para analisar problemas e planejar, implementar, avaliar e gerir soluções para esses problemas, envolvidos em todos os aspectos da aprendizagem humana [...] a tecnologia educacional abrange três aspectos básicos: recursos destinados à aprendizagem, funções de gestão educacional e funções de desenvolvimento educacional. (NETTO, 1998, p. 30).

Para dar uma ampla visão sobre o que é possível desenvolver dentro de um AVA, Pereira (2007, p. 9) comenta os principais recursos tecnológicos, que podem ser agrupados em quatro eixos:

a) informação e documentação;

b) comunicação;

c) gerenciamento pedagógico e administrativo;

d) produção.

No eixo da informação e documentação destacam-se as hipermídias de conteúdo em *HyperText Markup Language* (HTML), Flash, aplicações Java, servidor de arquivos para inserção, ferramentas de ajuda e glossário.

Destaca-se no eixo da comunicação o fórum, o *chat* e o *e-mail*.

No eixo do gerenciamento pedagógico e administrativo destacam-se as notas de trabalhos, exercícios, histórico de conteúdos visitados, número de participação em fóruns e *chats* e grupos de trabalhos.

Por fim, no eixo da produção destacam-se o sistema para avaliação, publicação de notas e o histórico de disciplinas cursadas, sistema de controle para cadastro de pagamento, agenda e controle de atividades e a criação e controle de cursos.

Portanto, a funcionalidade de execução de avaliações do conhecimento pode ser desenvolvida através de um AVA, mesmo que este já exista e que possua inúmeras funcionalidades, ou ainda, pode se criar um ambiente virtual que contemple apenas a funcionalidade de avaliações.

2.2 ASPECTOS DE SEGURANÇA DA INFORMAÇÃO

Segundo Wanderley (2005, p. 7), desde o surgimento da informática e da internet já existia a preocupação com a segurança dos sistemas, pois muitas organizações lançavam suas informações no mundo virtual, sendo que muitas delas só existem neste ambiente. Desta forma, proteger suas informações e seu ambiente computacional é vital para a realização dos negócios.

A informação é, na atualidade, uma das mais valiosas ferramentas de uma corporação. Logo, se não houver mecanismos de proteção, cedo ou tarde, haverá prejuízo, moral ou material para a corporação (TADEU, 2006, p. 5).

Para entender melhor sobre os aspectos de segurança, segundo Albuquerque e Ribeiro (2002, p. 1) apresentam-se algumas definições, que são:

a) autenticação: capacidade de garantir que um usuário, sistema ou informação é mesmo quem alega ser;
b) não repúdio: capacidade do sistema de provar que um usuário executou determinada ação no sistema;

c) auditoria: capacidade do sistema de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque.

2.2.1.1 Criptografia

De acordo com Albuquerque e Ribeiro (2002, p. 155), um ponto importante para segurança é a criptografia, que é um processo onde a informação é embaralhada utilizando-se um algoritmo de criptografia e uma chave de acesso, de tal forma que só seja possível obter a informação original através da utilização do mesmo algoritmo de criptografia e de uma chave de acesso correspondente.

Segundo Terada (2000, p. 16), a criptografia é uma ciência que estuda a transformação de dados de maneira a torná-los incompreensíveis e secretos, de forma que somente com a chave secreta os dados poderão ser decifrados.

Galvão (2007) explica que existem dois tipos de criptografia, a simétrica e a assimétrica. Na criptografia simétrica, usa-se apenas uma chave para cifrar e decifrar os dados, já na criptografia assimétrica, usa-se duas chaves, geralmente chamadas de chave pública e chave privada, neste caso, utiliza-se uma chave para cifrar e outra para decifrar. Na criptografia assimétrica, a chave privada é secreta e pessoal, e a chave pública deve ser divulgada para que qualquer pessoa possa cifrar informações que só o destinatário decifrará com a sua chave privada correspondente.

2.2.1.2 Auditoria

Auditoria em software baseia-se na gravação, armazenamento e análise das informações. O sistema mantém o registro de tudo que foi feito nele de forma que, em caso de problema de segurança, seja possível identificar o que ou quem o causou. As rotinas de auditoria devem determinar uma série de fatores como registrar as ações importantes, tratar a privacidade, analisar as trilhas e armazená-las com segurança (ALBUQUERQUE; RIBEIRO, 2002, p. 109).

Segundo Silva (2005, p. 42), para cada evento auditado deve-se registrar ao menos a data e a hora do evento, o tipo de evento, a identidade do sujeito (usuário ou sistema) e o resultado final (sucesso ou falha);

2.2.2 CERTIFICADO DIGITAL

Para Bayão Júnior (2009, p. 43), a certificação digital é a mais nova tecnologia que identifica com segurança pessoas físicas ou jurídicas, garantindo confiabilidade, privacidade, integridade e inviolabilidade em mensagens e em diversos tipos de transações realizadas via internet. Isso tudo é possível porque os certificados digitais têm como base a criptografia.

Segundo Aguiar (2005, p. 23), certificado digital associa a identidade de alguém a um par de chaves eletrônicas (privada e pública) que, usadas em conjunto, fornecem a comprovação da identidade desta pessoa. É uma versão eletrônica (digital) de uma Carteira de Identidade (CI) e para que o certificado digital seja válido, ele pode ser auto-assinado, ou seja, sem precisar de uma Autoridade Certificadora (AC) oficial.

> Se você recebesse a assinatura digital pessoalmente de um amigo seu, teria certeza de que é confiável. Se seu amigo também confirmou a validade de chaves recebidas pessoalmente, então você pode confiar nelas. Caso alguém perca sua chave pública, você precisa de alguma forma ser notificado, para que possa trocá-la por uma nova confiável. Uma rede de confiança dessas fica enormemente complexa numa abrangência como a Internet. Para resolver esse problema foram criadas as Autoridades Certificadoras (AC) que certificam que uma determinada pessoa possui a chave pública que diz possuir. (ZANINI, 2007, p. 22).

De acordo com Aguiar (2005, p. 24), um certificado digital contém três elementos:

a) informação de atributo: informação sobre o objeto que é certificado. No caso de uma pessoa, isso pode incluir seu nome, organização, departamento, dentre outros;
b) chave de informação pública: esta é a chave publicada na AC. O certificado atua para associar a chave pública à informação de atributo. A chave pública pode ser qualquer chave assimétrica;
c) assinatura da autoridade certificadora: assina os dois primeiros elementos, validando os. Quem recebe o certificado verificará a assinatura e acreditará na informação de atributo e chave pública associadas.

2.2.2.1 Assinatura digital

Assinatura digital é um mecanismo eletrônico que faz uso de criptografia, mais precisamente, de chaves criptográficas. Estas são um conjunto de *bits* baseado em um determinado algoritmo capaz de cifrar e decifrar informações. Para isso, podem-se usar chaves simétricas ou chaves assimétricas (ALECRIM, 2009).

As chaves simétricas são mais simples, pois com elas o emissor e o receptor utilizam a mesma chave para, respectivamente, cifrar e decifrar uma informação. Já as chaves assimétricas, por sua vez, trabalham com duas chaves: a chave privada e a chave pública. Assim, uma pessoa ou uma organização deve utilizar uma chave de codificação e disponibilizá-la a quem for mandar informações a ela, esta é a chave pública. A outra chave deve ser usada para o processo de decodificação: esta é a chave privada, que é sigilosa e individual. Ambas as chaves são geradas de forma conjunta, portanto, uma está associada à outra (ALECRIM, 2009).

Segundo Santos (2009) a assinatura digital é o *hash* de toda a informação a ser enviada cifrada com a chave privada do remetente. A assinatura digital deve ser enviada juntamente com o conteúdo original utilizado para fazer o *hash*. Para que o destinatário possa verificar a integridade e a autenticidade da assinatura digital, é necessário possuir o conteúdo que o remetente utilizou para gerar o *hash* e a sua chave pública, desta forma, o destinatário poderá utilizar a chave pública do remetente para decifrar a assinatura digital e comparar o resultado obtido com um novo *hash* do conteúdo original recebido, caso os dois *hahs* sejam iguais, a autenticidade e a integridade estarão garantidas.

2.2.3 ICP-BRASIL

A Autoridade Certificadora Raiz da ICP-Brasil é a primeira autoridade da cadeia de certificação. É executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Portanto, compete à AC Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subseqüente ao seu (INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, 2011).

2.2.3.1 e-CPF

O Cadastro de Pessoa Física Eletrônico (e-CPF) é um documento voltado para pessoa física e utilizado na comunicação virtual com as instituições governamentais ou não. O intuito deste documento é manter um nível de segurança bastante elevado na troca de arquivos com o fisco e outras instituições (TALUA, 2010).

De acordo com a Talua (2010), as principais atividades relacionadas com o e-CPF são:

a) importações e exportações;
b) assinatura de documentos eletronicamente;
c) enviar as declarações de pessoas jurídicas se o responsável do certificado for o mesmo responsável na receita federal pelo Cadastro Nacional de Pessoa Jurídica (CNPJ) da empresa.

Desta forma o e-CPF funciona como um Cadastro de Pessoa Física (CPF) virtual que comprova na internet a autoria de determinada pessoa física.

De acordo com a Certisign (2010) existem dois tipos de e-CPF:

a) tipo A3: o e-CPF Tipo A3 oferece maior segurança porque seus dados são gerados, armazenados e processados em um cartão inteligente ou *token*, permanencendo invioláveis e únicos. A validade deste certificado é de até 3 anos, e somente o detentor da senha de acesso do cartão ou do *token* pode utilizá-lo;
b) tipo A1: o e-CPF tipo A1 é gerado e armazenado em um computador pessoal, dispensando o uso de cartões inteligentes ou *tokens*. Para maior segurança, no momento da emissão do certificado, deve-se optar por protegê-lo com uma senha de acesso. Recomenda-se que um único computador armazene o e-CPF e que seja criada apenas uma cópia de segurança. Este certificado digital possui validade de 1 ano.

2.3 TRABALHOS CORRELATOS

Existem muitos trabalhos sobre Ambiente Virtual de Aprendizagem, porém, poucos trabalhos semelhantes ao proposto, ou seja, que implementam requisitos de segurança ou certificados digitais. Devido a esta dificuldade, dentre eles, foram escolhidos três trabalhos que se aproximam às características desse. Foram selecionados os trabalhos “Software de Apoio a Geração de Avaliações de Aprendizagem” (DANEY, 2007), “Ambiente Virtual de Aprendizagem da Universidade Regional de Blumenau (FURB)” (UNIVERSIDADE REGIONAL DE BLUMENAU, 2009) e “Protótipo de Software para Emissão de Certificados Digitais” (MATHIAS, 2007), respectivamente.

2.3.1 Software de Apoio a Geração de Avaliações de Aprendizagem

Segundo Daney (2007, p. 15), o software apresentado propõe a geração de avaliações, onde cada avaliação pode conter questões de diferentes tipos, como, objetiva, subjetiva, preenchimento de lacuna, somatória, verdadeiro ou falso e relacionamento de colunas. Esta ferramenta utiliza o conceito de raciocínio baseado em casos, que é uma abordagem para solução de problemas e aprendizado por meio de casos anteriormente elaborados. Desta forma, a ferramenta pode gerar novas avaliações a partir de avaliações já existentes.

Além disso, a ferramenta também é capaz de gerar avaliações e também exercícios, e por fim, o usuário pode optar por imprimir a avaliação, ou exportá-la para alguns formatos de documentos conhecidos.

2.3.2 Ambiente Virtual de Aprendizagem da FURB

Segundo Universidade Regional De Blumenau (2009), o AVA é um sistema *web* que visa facilitar a comunicação e interação entre alunos e professores. Através deste instrumento, a universidade é capaz de disponibilizar uma via mais prática de comunicação entre a comunidade acadêmica.

Esta ferramenta possui um módulo para professor e um módulo para o aluno. No módulo do professor pode-se criar um questionário para o aluno. Este questionário pode ser personalizado de acordo com a necessidade do professor, que pode optar por permitir ao aluno que visualize a resposta de cada questão ao responder, controlar quantas questões cada aluno irá responder, definir um período ou data em que o questionário estará disponível para responder e optar por randomizar as questões que serão selecionadas para cada aluno.

Além das funcionalidades comentadas acima, os professores também podem disponibilizar arquivos, exercícios, fóruns de debate, galeria de imagens, dentre outros.

2.3.3 Protótipo de Software para Emissão de Certificados Digitais

De acordo com Mathias (2007, p. 13), este trabalho apresenta o desenvolvimento de um protótipo de software capaz de emitir certificados digitais auto-assinados, emitir e revogar certificados digitais para os objetos distribuídos e, juntamente com a revogação, mantém uma lista dos certificados revogados. No desenvolvimento do protótipo foram utilizadas técnicas de criptografia como o algoritmo Rivest Shamir Adleman (RSA) responsável pela emissão do par de chaves e o algoritmo *Message-Digest algorithm* 5 (MD5) utilizado para gerar *hash code*, podendo assim assinar o certificado digitalmente.

3 DESENVOLVIMENTO

Este capítulo detalha as etapas do desenvolvimento do protótipo de ambiente virtual de avaliações. São apresentados os requisitos, a especificação e a implementação do mesmo, mencionando as técnicas e ferramentas utilizadas. Também são comentadas questões referentes à operacionalidade e os resultados obtidos.

3.1 REQUISITOS PRINCIPAIS DO PROBLEMA A SER TRABALHADO

O levantamento de requisitos é indispensável para que usuários e desenvolvedores tenham a mesma visão do problema a ser modelado.

Os requisitos funcionais do sistema são:

a) o sistema deve permitir apenas a entrada de usuários com certificado digital válido;
b) o sistema deve permitir a autenticação do usuário;
c) o sistema deve apresentar uma auditoria de segurança para usuários administradores;
d) o sistema deve permitir ao professor o cadastro de questões;
e) o sistema deve permitir ao professor configurar uma avaliação com as questões cadastradas;
f) o sistema deve permitir ao aluno executar uma avaliação gerada pelo professor;
g) o sistema deve permitir ao professor gerar um relatório das avaliações executadas para fins de correção;
h) o sistema deve permitir ao diretor gerar um diploma virtual em formato de texto e assinado digitalmente com a sua chave privada;
i) o sistema deve permitir ao diretor excluir qualquer diploma virtual gerado por ele anteriormente;
j) o sistema deve permitir a qualquer usuário do sistema fazer a verificação e validação da assinatura digital do diretor contido no diploma virtual gerado.

Os requisitos não-funcionais do sistema são:

a) o sistema deve ser implementado na linguagem de programação Hypertext Preprocessor (PHP);

b) o sistema deve ser implementado utilizando o ambiente de desenvolvimento Adobe DreamWeaver CS5;
c) o sistema deve utilizar o banco de dados MySQL para armazenar os dados de entrada do usuário;
d) o sistema deve utilizar certificados digitais gerados pela ferramenta OpenSSL, que também será utilizada para efetuar conversões entre diferentes formatos de certificado.

3.2 ESPECIFICAÇÃO

Na seqüência é apresentada a especificação do sistema, que foi modelado na ferramenta Entreprise Architect (SPARXSYSTEMS, 2000). Foram utilizados conceitos da orientação a objetos e a *Unified Modeling Language* (UML) (OMG, 2005) para a criação dos diagramas de casos de uso, classe e de sequência.

3.2.1 Diagrama de casos de uso

Na especificação do sistema existem quatro cenários. O primeiro (Figura 1) tem como ator o professor, o segundo (Figura 2) tem como ator o aluno, o terceiro (Figura 3) tem como ator o diretor, e o quarto (Figura 4) tem como ator o visitante.

O ator professor possui o maior número de funcionalidades a serem executadas, estas funcionalidades tratam-se na maior parte das funcionalidades gerais do sistema, como criar prova, excluir prova, criar questão, excluir questão, selecionar alunos para prova, excluir seleção de aluno para prova, gerar relatório referente às provas executadas, autenticar-se, e por fim, a funcionalidade de verificar a assinatura digital de um diploma, que também está disponível para os outros atores, sendo desnecessário estar autenticado no sistema para efetuar esta verificação.

O ator diretor possui as funcionalidades mais relevantes do sistema, como gerar diploma, excluir diploma, cadastrar usuários, excluir usuários, e outras como, autenticar-se e verificar assinatura digital de um diploma.

O ator aluno possui o menor número de funcionalidades dentre aqueles atores que

podem se autenticar no sistema, tais como autenticar-se, executar prova, verificar assinatura digital de um diploma, e efetuar o download de um diploma gerado caso exista algum disponível, ou seja, caso o diretor tenha gerado um diploma para aquele aluno anteriormente.

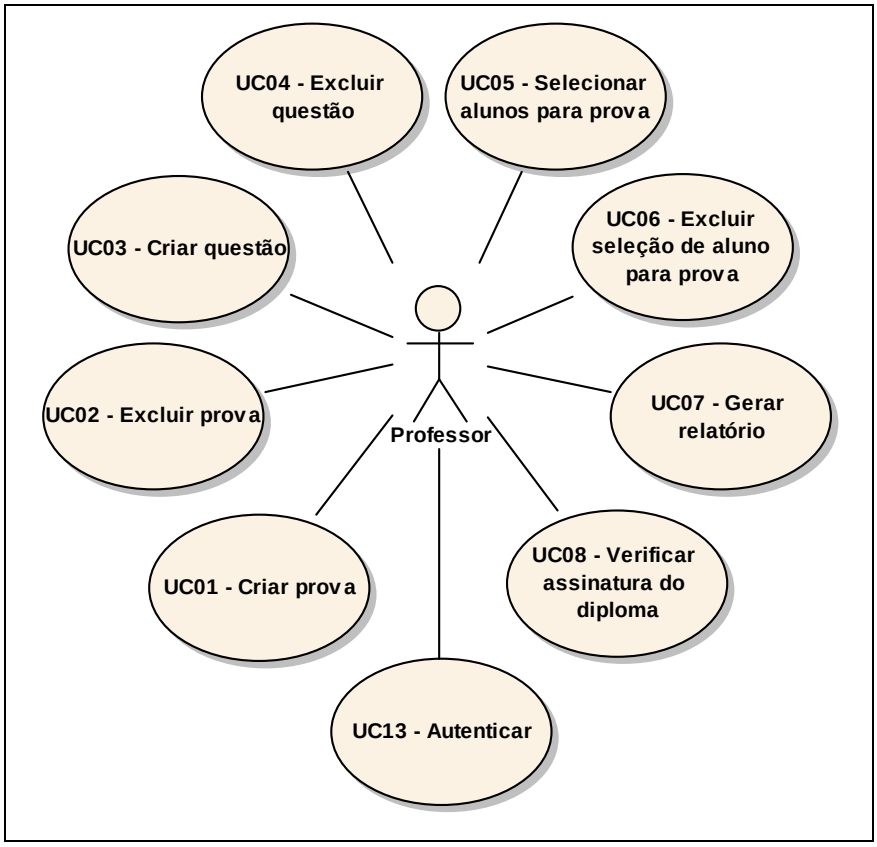

Figura 1 – Diagrama de casos de uso executados pelo professor

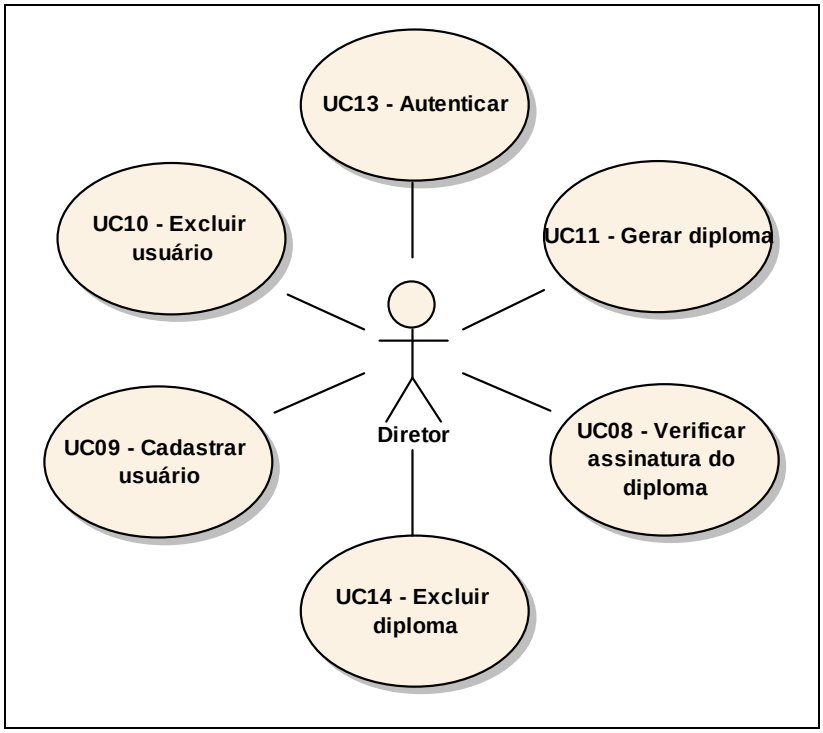

Figura 2 – Diagrama de casos de uso executados pelo diretor

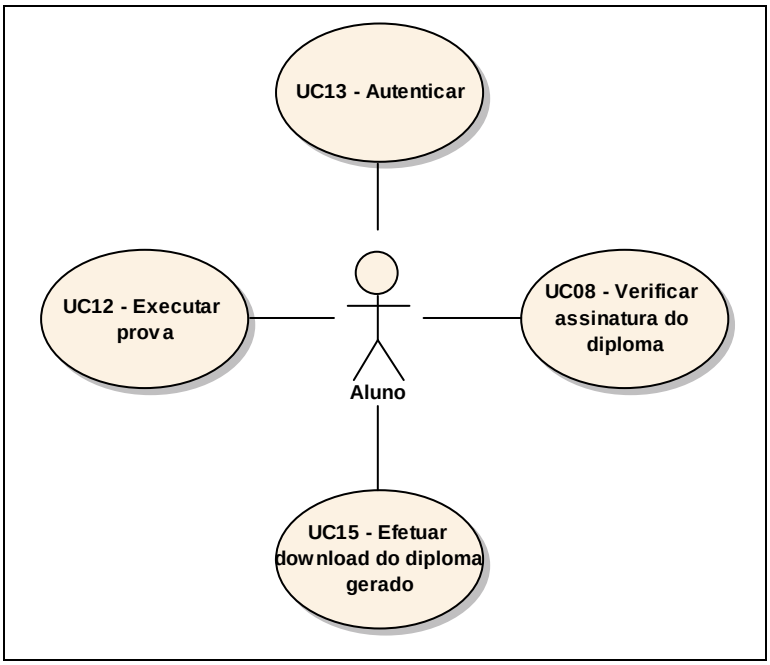

Figura 3 – Diagrama de casos de uso executados pelo aluno

O ator visitante é um ator que não se autentica no sistema, ou seja, que não possui cadastrado. Através deste ator é possível formalizar que, todo e qualquer usuário que não esteja autenticado no sistema, poderá `verificar assinatura do diploma` gerado pelo ator diretor.

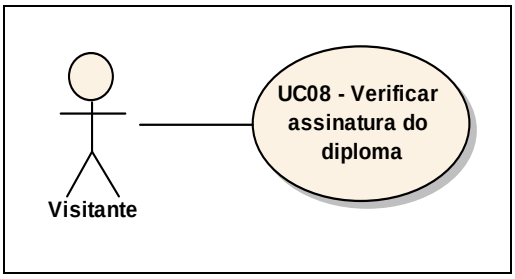

Figura 4 – Diagrama de casos de uso executados pelo visitante

Os quadros 1 a 13 apresentam a descrição dos casos de uso da ferramenta, mostrando o nome do caso de uso e a sua descrição, atores associados, pré-condições, cenário principal, cenários de exceção (se houverem), cenários alternativos (se houverem) e por fim as pós-condições.

UC01 – Criar prova: Cria uma nova prova.	
Ator	Professor.
Pré-condições	O Professor deve estar autenticado no sistema.
Cenário principal	1. O Professor acessa o menu Criar Prova 2. O Sistema retorna o formulário com os campos a serem preenchidos. 3. O Professor informa o assunto da prova e uma observação. 4. O Professor clica no botão Cadastrar Prova. 5. O Sistema valida os dados. 6. O sistema apresenta a mensagem “A prova foi cadastrada com sucesso!”
Exceção 1	No passo 5, caso o assunto da prova não tenha sido informado, o sistema apresenta a mensagem “Digite o assunto da prova!”.
Pós-condições	Prova cadastrada com sucesso.

Quadro 1 – Detalhamento do caso de uso `UC01 – Criar prova`

O caso de uso `UC01 – Criar prova` (Quadro 1) é responsável por permitir ao professor inserir uma nova prova no banco de dados a partir do assunto informado pelo professor.

UC02 – Excluir prova: Exclui uma prova existente	
Ator	Professor.
Pré-condições	O Professor deve estar autenticado no sistema. Deve haver no mínimo uma Prova cadastrada no sistema.
Cenário principal	1. O Professor acessa o menu Excluir Prova. 2. O Sistema apresenta uma lista com as Provas cadastradas. 3. O Professor clica no botão “X” de acordo com a prova que deseja excluir. 4. O sistema apresenta a mensagem “A prova foi excluída com sucesso!”
Pós-condições	Prova excluída com sucesso.

Quadro 2 – Detalhamento do caso de uso `UC02 – Excluir prova`

No caso de uso `UC02 – Excluir prova` (Quadro 2), o professor tem a possibilidade de excluir uma prova cadastrada no banco de dados, para isso, o sistema apresenta uma lista com todas as provas cadastradas.

UC03 – Criar questão: Cria uma nova questão para uma prova existente.	
Ator	Professor.
Pré-condições	O Professor deve estar autenticado no sistema. Deve haver no mínimo uma Prova cadastrada no sistema.
Cenário principal	1. O Professor acessa o menu Criar Questões para Prova. 2. O Sistema retorna o formulário com os campos a serem preenchidos. 3. O Professor seleciona uma prova para criar uma nova questão. 4. O Professor digita a pergunta. 5. O Professor clica no botão Cadastrar Questão. 6. O sistema apresenta a mensagem “A questão foi cadastrada com sucesso!”
Pós-condições	Questão cadastrada com sucesso.

Quadro 3 – Detalhamento do caso de uso `UC03 – Criar questão`

O caso de uso `UC03 – Criar questão` (Quadro 3) é responsável por permitir ao professor inserir uma questão de uma prova no banco de dados, para este procedimento é necessário informar um enunciado para questão e selecionar uma prova já existente, desta forma a questão está associada a uma prova.

No caso de uso `UC04 – Excluir questão` (Quadro 4) para que o professor possa efetuar a exclusão de uma questão, o sistema apresenta ao professor uma lista com todas as questões cadastradas no banco de dados.

UC04 – Excluir questão: Exclui uma questão existente.	
Ator	Professor.
Pré-condições	O Professor deve estar autenticado no sistema. Deve haver no mínimo uma Questão cadastrada no sistema.
Cenário principal	1. O Professor acessa o menu Excluir Questões. 2. O Sistema apresenta uma lista com as questões cadastradas. 3. O Professor clica no botão “X” de acordo com a questão que deseja excluir. 4. O sistema apresenta a mensagem “A questão foi excluída com sucesso!”
Pós-condições	Questão excluída com sucesso.

Quadro 4 – Detalhamento do caso de uso `UC04 – Excluir questão`

O caso de uso `UC05 – Selecionar alunos para prova` (Quadro 5) é responsável por permitir ao professor associar ou desassociar um aluno a uma prova, permitindo ao aluno executar a prova associada posteriormente. No caso da associação (cenário principal), o professor deve selecionar uma prova e um aluno já cadastrados no banco de dados, já no caso da desassociação (cenário alternativo), o sistema apresenta uma lista com todos os alunos já associados a uma respectiva prova, bastando ao professor excluir o aluno desejado.

UC05 – Selecionar alunos para prova: Seleciona alunos para executar a prova posteriormente.	
Ator	Professor.
Pré-condições	O Professor deve estar autenticado no sistema. Deve haver no mínimo uma Prova cadastrada no sistema. Deve haver no mínimo um Aluno cadastrado no sistema.
Cenário principal	1. O Professor acessa o menu Selecionar Alunos para Prova. 2. O Sistema apresenta uma lista com todos os Alunos selecionados para cada prova. 3. O Professor seleciona a Prova desejada. 4. O Professor seleciona o Aluno desejado. 5. O Professor clica no botão “Selecionar Aluno”. 6. O Sistema apresenta a mensagem “O Aluno foi selecionado com sucesso!”
Alternativo 1	No passo 2, o professor pode optar por excluir a “seleção” de um aluno já “selecionado” para executar a prova. 2.1 O Professor clica no botão “X” de acordo com o aluno que deseja remover. 2.2. O sistema apresenta a mensagem “Aluno removido com sucesso!”.
Exceção 1	No passo 5, caso o Aluno selecionado já esteja cadastrado para executar a prova, o sistema apresenta a mensagem “O Aluno selecionado já está cadastrado”.
Pós-condições	Aluno relacionado para executar uma Prova.

Quadro 5 – Detalhamento do caso de uso `UC05 – Selecionar alunos para prova`

O caso de uso `UC06 – Excluir seleção de aluno para prova` (Quadro 6) é equivalente ao cenário alternativo do caso de uso `UC05 – Selecionar Alunos para Prova` (Quadro 5), onde o sistema apresenta uma lista com os alunos já associados a uma respectiva prova e permite que o professor desassocie o aluno desejado.

UC06 – Excluir seleção de aluno para prova: Remove a seleção de alunos para executar a prova posteriormente.	
Ator	Professor.
Pré-condições	O Professor deve estar autenticado no sistema. Deve haver no mínimo uma Prova cadastrada no sistema. Deve haver no mínimo um Aluno cadastrado no sistema. O Aluno deve estar selecionado para executar a prova.
Cenário principal	1. O Professor acessa o menu Selecionar Alunos para Prova. 2. O Sistema apresenta uma lista com todos os Alunos selecionados para cada prova. 3. O Professor clica no botão “X” de acordo com o aluno que deseja remover. 4. O sistema apresenta a mensagem “Aluno removido com sucesso!”
Pós-condições	Aluno excluído da execução de uma Prova.

Quadro 6 – Detalhamento do caso de uso `UC06 – Excluir seleção de aluno para prova`

O caso de uso `UC07 – Gerar relatório` (Quadro 7) é responsável permitir ao professor gerar um relatório com as perguntas e respostas de um aluno que executou uma prova, para isso, ao acessar o menu, o professor deve informar a prova e o aluno desejados.

UC07 – Gerar relatório: O Sistema apresenta um relatório completo de acordo com a prova e o aluno selecionado.	
Ator	Professor.
Pré-condições	O Professor deve estar autenticado no sistema. Deve haver no mínimo uma Prova cadastrada no sistema. Deve haver no mínimo uma Questão cadastrada no sistema. Deve haver no mínimo um Aluno cadastrado no sistema. Deve haver no mínimo um Aluno selecionado para executar a Prova.
Cenário principal	1. O Professor acessa o menu Gerar Relatório. 2. O Sistema carrega uma lista com as provas disponíveis. 3. O Professor seleciona a Prova desejada. 4. O Professor clica no botão Selecionar Prova. 5. O Sistema carrega uma lista com os alunos disponíveis. 6. O Professor seleciona o aluno desejado. 7. O Professor clica no botão Gerar Relatório. 8. O sistema apresenta o relatório gerado.
Pós-condições	Relatório gerado com sucesso.

Quadro 7 – Detalhamento do caso de uso `UC07 – Gerar relatório`

O caso de uso `UC08 – Verificar assinatura do diploma` (Quadro 8) representa uma das funcionalidades mais relevantes do sistema, pois é responsável por permitir a qualquer usuário que faça uma verificação de autenticidade e integridade de um diploma submetido ao sistema. Para fazer a verificação, não é necessário que o usuário esteja autenticado no sistema, e ao acessar o menu e submeter o diploma assinado, o sistema efetua a verificação e informa se o diploma é válido ou inválido.

UC08 – Verificar assinatura do diploma: O Sistema verifica a integridade e a autenticidade de diploma gerado e assinado pelo Diretor.	
Ator	Visitante, Aluno, Diretor, Professor.
Cenário principal	1. O Usuário do sistema acessa o menu Verificar Diploma. 2. O Usuário do sistema submete o diploma clicando no botão Escolher arquivo. 3. O Sistema carrega o diploma para ser verificado. 4. O Usuário clica no botão Verificar Diploma 5. O Sistema verifica a integridade e autenticidade do diploma utilizando a chave pública do diretor. 6. Caso o diploma seja autêntico e esteja íntegro, o Sistema apresenta a mensagem “O diploma é válido! (Integridade e Autenticidade confirmadas com sucesso!)”
Exceção 1	No passo 4, caso o diploma não tenha sido selecionado, o sistema apresenta a mensagem “Nenhum diploma foi selecionado!”.
Exceção 2	No passo 6, caso o diploma não esteja íntegro e/ou não seja autêntico, o sistema apresenta a mensagem “O diploma não é válido! (O diploma pode ter sido violado/adulterado)”.
Pós-condições	Diploma verificado com sucesso!

Quadro 8 – Detalhamento do caso de uso `UC08 – Verificar assinatura do diploma`

O caso de uso `UC09 – Cadastrar usuário` (Quadro 9) é responsável por permitir ao diretor cadastrar um novo usuário no sistema, sendo este um aluno ou professor. De acordo com o tipo de usuário selecionado na hora do cadastro, o sistema faz uma classificação por nível, para que depois seja possível ter o controle de permissão de acordo com este nível cadastrado.

UC09 – Cadastrar usuário: Cadastra um novo usuário no Sistema.	
Ator	Diretor.
Pré-condições	O Diretor deve estar autenticado no sistema.
Cenário principal	1. O Diretor acessa o menu Cadastrar Usuário. 2. O Sistema apresenta o formulário de cadastro. 3. O Diretor digita os dados do usuário a ser cadastrado. 4. O Diretor seleciona qual o nível/tipo de usuário (Aluno, Professor) 5. O Diretor clica no botão Cadastrar Usuário. 6. O Sistema valida os dados e utiliza uma função de *hash* para gravar a senha do usuário. 7. O Sistema apresenta as mensagens “Dados gravados com sucesso!”, “Seu cadastro foi efetuado com sucesso!”.
Exceção 1	No passo 11, caso o nome de usuário já exista. 11.1 O sistema apresenta a mensagem “Usuário já existente”. 11.2 Retorna ao passo 11.
Exceção 2	No passo 11, caso o campo Senha e o campo Confirmar Senha sejam diferentes. 11.1 O sistema apresenta a mensagem “As senhas digitadas são diferentes”. 11.2 Retorna ao passo 11.
Exceção 3	No passo 11, caso o e-mail já exista. 11.1 O sistema apresenta a mensagem “E-mail já existente”. 11.2 Retorna ao passo 11.
Exceção 4	No passo 11, caso o campo Nome esteja em branco. 11.1 O sistema apresenta a mensagem “Digite seu nome!”. 11.2 Retorna ao passo 11.
Exceção 5	No passo 11, caso o campo Senha esteja em branco. 11.1 O sistema apresenta a mensagem “Digite sua senha!”. 11.2 Retorna ao passo 11.
Exceção 6	No passo 11, caso o campo Usuário esteja em branco. 11.1 O sistema apresenta a mensagem “Digite seu Usuário!”. 11.2 Retorna ao passo 11.
Exceção 7	No passo 11, caso o campo Lembrete de Senha esteja em branco. 11.1 O sistema apresenta a mensagem “Digite seu Lembrete de Senha!”. 11.2 Retorna ao passo 11.
Exceção 8	No passo 11, caso o campo E-mail esteja em branco. 11.1 O sistema apresenta a mensagem “Digite seu e-mail!”. 11.2 Retorna ao passo 11.
Exceção 9	No passo 11, caso o campo Data de Nascimento esteja em branco. 11.1 O sistema apresenta a mensagem “Digite sua data de nascimento!”. 11.2 Retorna ao passo 11.
Exceção 10	No passo 11, caso o campo E-mail seja inválido. 11.1 O sistema apresenta a mensagem “E-mail inválido!”. 11.2 Retorna ao passo 11.
Pós-condições	Usuário cadastrado com sucesso.

Quadro 9 – Detalhamento do caso de uso `UC09 – Cadastrar usuário`

No (Quadro 10) caso de uso `UC10 – Excluir usuários`, o diretor tem a possibilidade de excluir um usuário cadastrado no banco de dados, para isso, o sistema apresenta uma lista com todos os usuários já cadastrados. Quando um usuário é excluído do sistema, o sistema apenas cancela o seu direito de autenticação, mantendo no banco de dados algumas informações vinculadas àquele usuário, como por exemplo, as respostas de uma prova executada por um aluno, neste caso, mesmo que o usuário aluno tenho sido excluído do sistema, o professor ainda poderá gerar um relatório segundo as provas que aquele aluno excluído executou.

UC10 – Excluir usuários: Exclui um usuário do Sistema.	
Ator	Diretor.
Pré-condições	O Direitor deve estar autenticado no sistema. Deve haver no mínimo um Usuário cadastrado no sistema.
Cenário principal	1. O Diretor acessa o menu Excluir Usuários. 2. O Sistema apresenta uma lista com todos os usuários cadastrados. 3. O Diretor clica no botão “X” de acordo com o usuário que deseja excluir. 4. O Sistema apresenta a mensagem “Usuário excluído com sucesso!”
Pós-condições	Usuário excluído com sucesso!

Quadro 10 – Detalhamento do caso de uso `UC10 – Excluir usuários`

O caso de uso `UC11 – Gerar diploma` (Quadro 11) é um dos casos de uso mais importantes e relevantes do sistema, pois permite ao diretor gerar um diploma virtual assinado digitalmente com a chave privada do seu certificado digital. Para executar este processo é necessário que exista no mínimo um aluno cadastrado, sendo assim, o professor pode selecionar o aluno desejado, selecionar a sua chave privada, que pode estar em seu computador ou em um disco removível e por fim, gerar e assinar o diploma virtual.

É importante destacar que após o diretor gerar o diploma assinado, este passa a ficar disponível para que o aluno correspondente possa efetuar o download.

UC11 – Gerar diploma: Gera um diploma para um aluno assinado digitalmente pelo Diretor usando a chave privada do seu e-CPF.	
Ator	Diretor.
Pré-condições	O Diretor deve estar autenticado no sistema. O Diretor precisa possuir uma chave privada em sua máquina local ou em sua unidade de armazenamento externa. Deve haver no mínimo um Aluno cadastrado no sistema.
Cenário principal	1. O Diretor acessa o menu Gerar Diploma. 2. O Diretor seleciona o aluno desejado. 3. O Diretor clica no botão Escolher arquivo para submeter a sua chave privada. 4. O Sistema carrega a Chave Privada do Diretor. 5. O Diretor clica no botão Gerar e Assinar Diploma. 6. O Sistema carrega as informações do Aluno, gera e assina o Diploma. 7. O Sistema apresenta a mensagem “Diploma gerado com sucesso!”
Exceção 1	No passo 4, caso a chave privada seja inválida, o sistema apresenta a mensagem “Chave Privada Inválida! Clique em voltar e tente novamente!”.
Exceção 2	No passo 5, caso a chave privada não tenha sido selecionada, o sistema apresenta a mensagem “Nenhuma chave privada selecionada!”.
Pós-condições	Diploma gerado com sucesso.

Quadro 11 – Detalhamento do caso de uso `UC11 – Gerar diploma`

O caso de uso `UC12 – Executar prova` (Quadro 12) é responsável permitir ao aluno executar uma prova. Para que ele possa fazer esta execução é necessário que o professor tenha associado o aluno a respectiva prova.

UC12 – Executar prova: Aluno executa a prova criada pela Professor.	
Ator	Aluno.
Pré-condições	O Aluno deve estar autenticado no sistema. Deve haver no mínimo um Professor cadastrado no sistema. Deve haver no mínimo uma Prova cadastrada no sistema. Deve haver no mínimo uma Questão cadastrada no sistema. O Aluno deve estar selecionado para executar uma Prova.
Cenário principal	1. O Aluno acessa o menu Executar Prova. 2. O Sistema retorna uma lista com as Provas disponíveis para aquele Aluno. 3. O Aluno seleciona uma Prova. 4. O Aluno clica no botão Executar. 5. O Sistema retorna um formulário para responder as questões da Prova. 6. O Aluno digita suas respostas. 7. O Aluno clica no botão Enviar Prova. 8. O Sistema apresenta a mensagem “Sua Prova foi respondida e enviada com sucesso!”
Pós-condições	Prova executada com sucesso.

Quadro 12 – Detalhamento do caso de uso `UC12 – Executar prova`

O caso de uso `UC13 – Autenticar` (Quadro 13) é responsável por autenticar o diretor, o professor e o aluno no sistema. Este caso de uso torna-se muito importante pelo diferencial que apresenta, sendo este a autenticação de um usuário do tipo diretor, a partir de um certificado digital válido.

UC13 – Autenticar: Usuário do sistema faz a autenticação para poder visualizar o menu conforme o seu nível de usuário.	
Ator	Diretor, Professor, Aluno.
Pré-condições	O Usuário deve estar cadastrado no sistema.
Cenário principal	1. O Usuário acessa a página inicial do sistema. 2. O Sistema carrega a página e o menu de Autenticação. 3. O Usuário informa o seu usuário e senha. 4. O Sistema valida os dados. 5. O Sistema faz a autenticação abrindo as opções no menu conforme o seu nível de usuário.
Alternativo 1	No passo 3, caso o usuário seja do tipo diretor, e caso ele possua um certificado digital válido, o usuário pode clicar no botão “Autenticar (Certificado)” para efetuar a sua autenticação. Este processo não exige que o diretor forneça o seu nome de usuário e senha.
Exceção 1	No passo 4, caso seja informado algum dado incorreto, o sistema apresenta a mensagem “Usuário ou senha inválida!”.
Pós-condições	Usuário autenticado com sucesso.

Quadro 13 – Detalhamento do caso de uso `UC13 – Autenticar`

No caso de uso `UC14 – Excluir diploma` (Quadro 14) o sistema permite ao diretor excluir um diploma gerado anteriormente, indisponibilizando o download deste ao aluno.

UC14 – Excluir Diploma: Exclui um diploma do Sistema.	
Ator	Diretor.
Pré-condições	O Diretor deve estar autenticado no sistema. Deve haver no mínimo um diploma gerado no sistema.
Cenário principal	1. O Diretor acessa o menu Excluir Diplomas. 2. O Sistema apresenta uma lista com todos os diplomas gerados. 3. O Diretor clica no botão “X” de acordo com o diploma que deseja excluir. 4. O Sistema apresenta a mensagem “Diploma excluído com sucesso!”
Pós-condições	Diploma excluído com sucesso!

Quadro 14 – Detalhamento do caso de uso `UC14 – Excluir diploma`

No caso de uso `UC15 – Efetuar download do diploma gerado` (Quadro 15) quando o aluno se autentica, o sistema verifica se existe algum diploma disponível, e caso exista, o sistema permite que o aluno efetue o download do seu diploma, gerado e assinado digitalmente pelo diretor.

UC15 – Efetuar download do diploma gerado: Verifica se existe um diploma gerado para o respectivo aluno e disponibiliza-o na página inicial.	
Ator	Aluno.
Pré-condições	O Aluno deve estar autenticado no sistema. Deve haver um diploma gerado no sistema para o respectivo aluno.
Cenário principal	1. O Aluno se autentica no sistema. 2. O Sistema verifica se existe um diploma disponível para o aluno. 3. O Sistema disponibiliza o diploma disponível para download.
Exceção 1	No passo 2, caso não existe um diploma disponível para o respectivo Aluno, o sistema apresenta apenas a tela de boas vindas.
Pós-condições	Diploma disponibilizado com sucesso!

Quadro 15 – Detalhamento do caso de uso `UC15 – Efetuar download do diploma gerado`

3.2.2 Diagrama de classes

O diagrama de classes do sistema está representado na Figura 5.

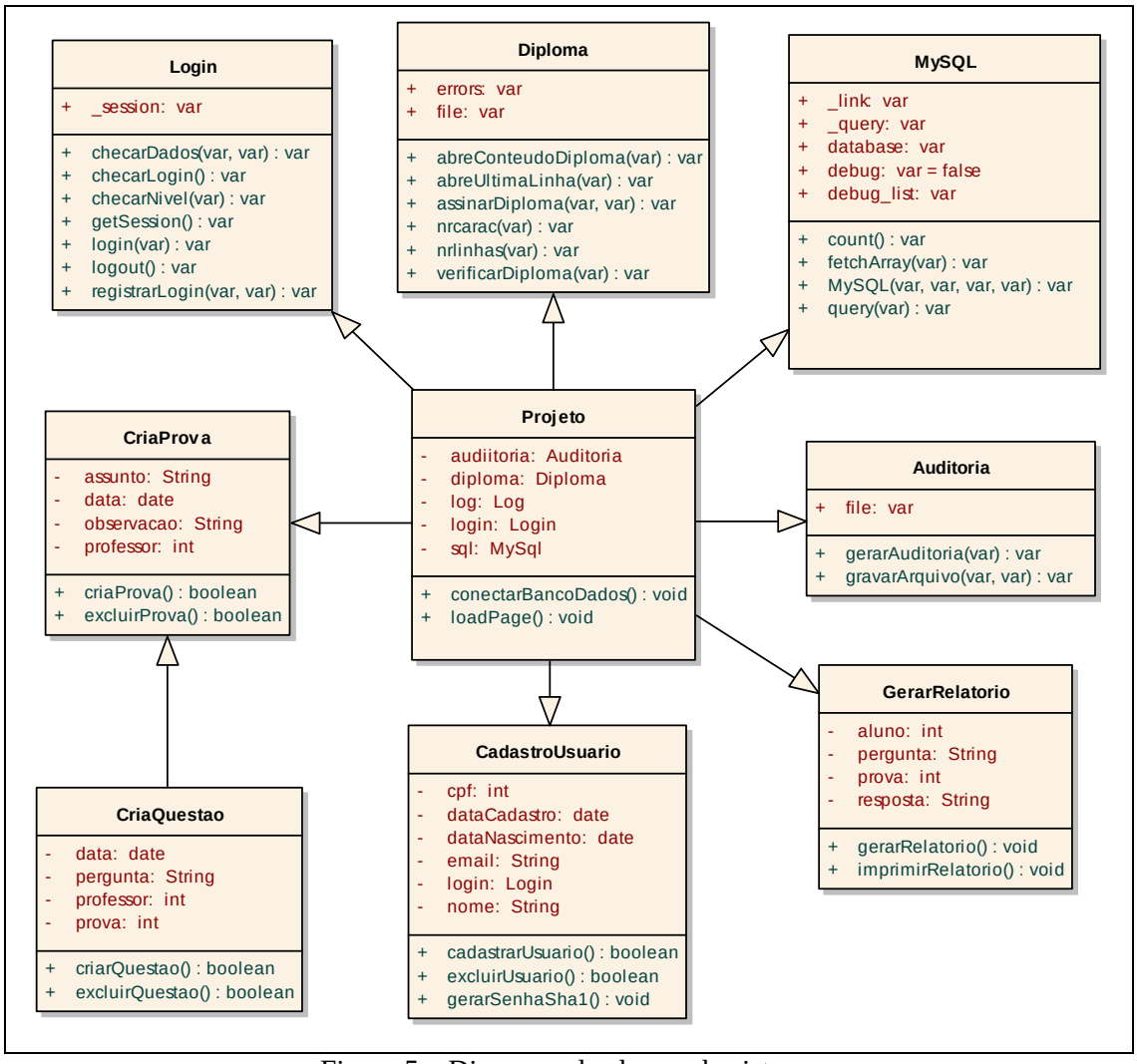

Figura 5 – Diagrama de classes do sistema

Segue o detalhamento das classes relacionadas da Figura 5, descrevendo o papel de cada uma delas:

a) `Login`: classe responsável pela autenticação do usuário;

b) `Auditoria`: classe responsável por atualizar as trilhas de auditoria;

c) `MySQL`: classe responsável pela conexão com o banco de dados e pela execução dos comandos SQL;

d) `CriaProva`: classe responsável por criar e excluir as prova;

e) `CriarQuestao`: classe responsável por criar e excluir as questões de uma prova;

f) `CadastroUsuario`: classe responsável por efetuar o cadastro de usuários;

g) `GerarRelatorio`: classe responsável por gerar o relatório das questões respondidas;

h) `Diploma`: classe responsável por gerar o diploma assinado digitalmente e por verificar e validar a assinatura de um diploma existente;

i) `Projeto`: Classe principal do sistema, onde todos os scripts são executados.

3.2.3 Diagrama de atividades

Na Figura 6, é apresentado o diagrama de seqüência referente aos casos de uso, `UC09 – Cadastrar usuário`, `UC10 – Excluir usuário` e `UC11 – Gerar diploma`.

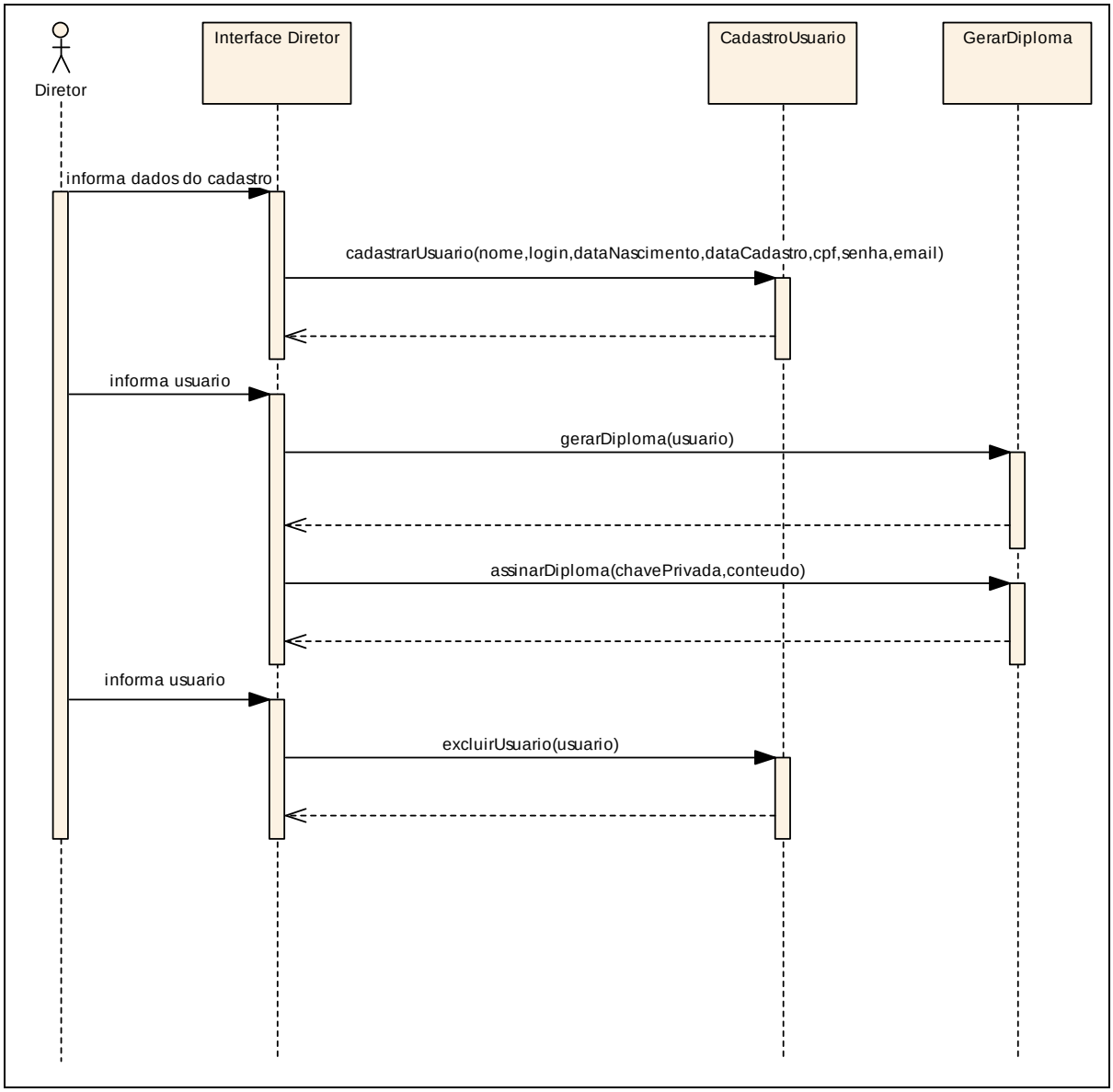

Figura 6 – Diagrama de seqüência dos casos de uso, `UC09 – Cadastrar usuário`, `UC10 – Excluir usuário` e `UC11 – Gerar diploma`

O ator diretor é o que mais se destaca, pois é este o único tipo de usuário que poderá gerar um diploma assinado digitalmente com a chave privada extraída do seu e-CPF, sendo esta a funcionalidade mais importante do sistema.

3.2.4 Diagrama de entidade-relacionamento

Segundo Carvalho (2005, p.2), o Diagrama Entidade Relacionamento (DER), é um modelo diagramático que descreve o modelo de dados de um sistema com alto nível de abstração, ou seja, com a utilização deste diagrama, é possível modelar o banco de dados de um sistema assim como o relacionamento entre as suas respectivas tabelas.

A Figura 7 ilustra o DER físico do ambiente desenvolvido.

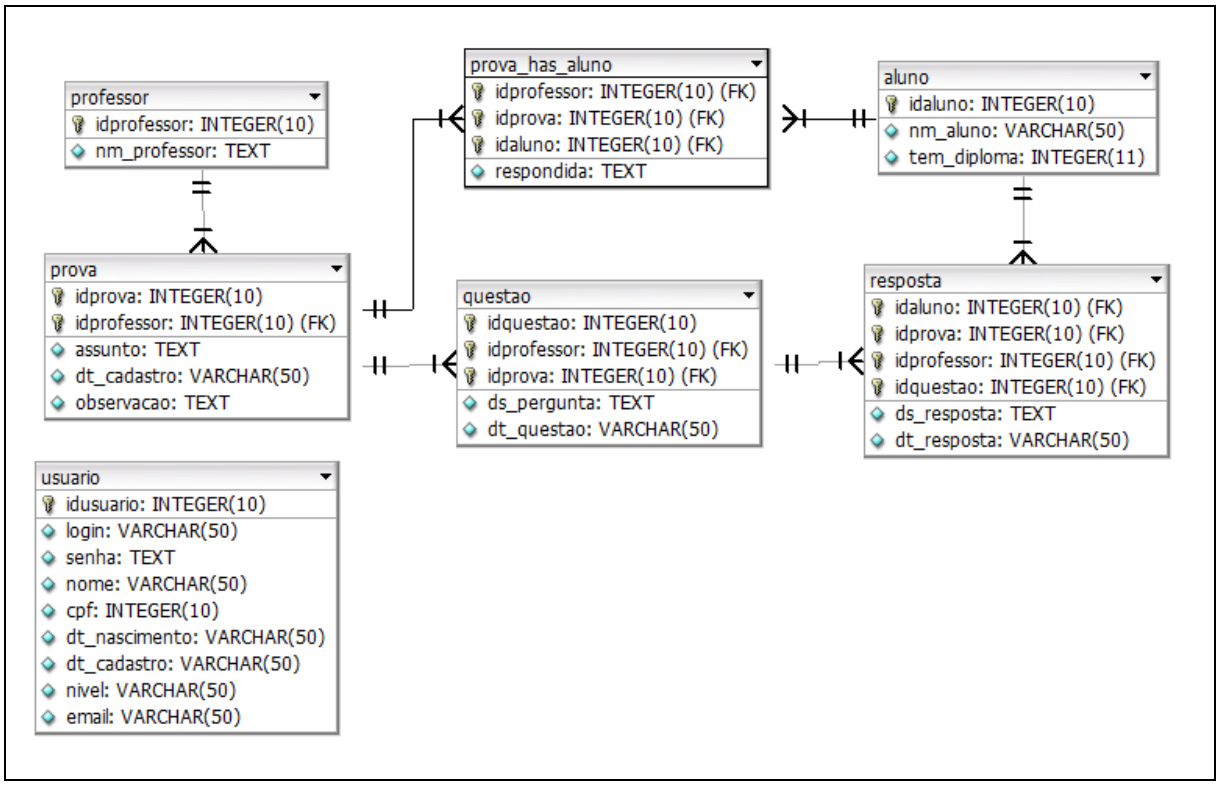

Figura 7 - Diagrama de Entidade-Relacionamento do ambiente

3.3 IMPLEMENTAÇÃO

Nesta seção são apresentadas informações sobre as técnicas e ferramentas utilizadas para a implementação do ambiente, bem como o processo de implementação.

3.3.1 Técnicas e ferramentas utilizadas

O ambiente foi implementado na linguagem de programação PHP 5 (PHP, 2011), utilizando-se o ambiente de desenvolvimento DreamWeaver CS5 (DREAMWEAVER, 2011), juntamente com o banco de dados MySQL 5 (MYSQL, 2011) e o servidor Apache 2 (APACHE, 2011).

3.3.2 Técnicas e código fonte implementados

Nas seções seguintes são apresentadas as técnicas utilizadas e trechos de código fonte referentes às implementações das principais classes do sistema.

3.3.2.1 Implementação da classe diploma

A classe `diploma` tem como função assinar digitalmente um diploma virtual e verificar a assinatura deste.

A Figura 8 ilustra e simplifica o entendimento do processo de funcionamento da assinatura digital, que pode ser decomposta em dois processos diferentes, onde o primeiro processo é o *hash* do diploma original e o segundo é a criptografia deste *hash* utilizando a chave privada do emissor. Ao final da execução destes dois processos, obtem-se a chave privada, que por sua vez é inserida no diploma original.

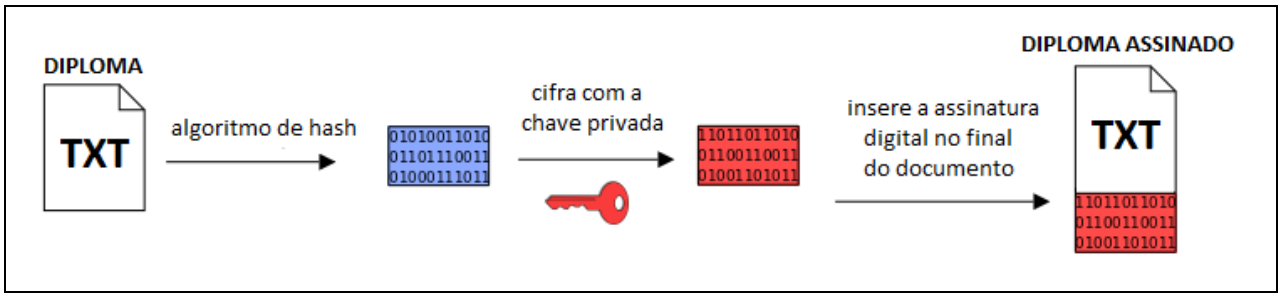

Figura 8 - Processo de funcionamento da assinatura digital do diploma

O processo ilustrado a partir da Figura 8 apresenta-se no método `assinarDiploma` demonstrado no Quadro 16, que por sua vez recebe como parâmetro o *hash* do conteúdo do diploma virtual a ser assinado e a chave privada fornecida pelo usuário diretor, que pode estar em seu computador ou em um disco removível. O retorno deste método é a assinatura digital,

que é gravada na última linha do diploma.

```
//Assina o diploma gerado
function assinarDiploma($conteudo,$nm_chav_priv){
    $chave_privada=""; //armazena a chave privada
    $file = file_get_contents($nm_chav_priv); //armazena todo o arquivo
    //percorre o arquivo
    for($i=0;$i<$this->nrcarac($nm_chav_priv);$i++){
        //testa se é o início da chave
        if($file[$i]=="-" and $file[$i+1]=="-"){
            //carrega a chave privada do arquivo para a variável
            while ($i<$this->nrcarac($nm_chav_priv)){
                $chave_privada .= $file[$i];
                $i++;
            }
        }
    }

    //se a chave privada for inválida retorna false
    if(!openssl_get_privatekey ($chave_privada)){
        return false;
    }
    //cifra o conteudo(diploma) passado como parametro
    //com a chave privada carregada
    openssl_private_encrypt($conteudo,$finaltext,$chave_privada);
    //retorna assinatura digital
    return $finaltext;
}
```

Quadro 16 – Método responsável por assinar digitalmente o diploma

A Figura 9 ilustra e simplifica o entendimento do processo de funcionamento da validação da assinatura digital, que pode ser decomposta em três processos diferentes, sendo o primeiro o *hash* do conteúdo do diploma submetido à validação, o segundo a descriptografia da assinatura digital embutida no diploma submetido, e por fim, o terceiro processo é comparação entre o resultado dos dois processos anteriores, sendo que, caso sejam iguais, o diploma é válido e caso sejam diferentes, o diploma é inválido.

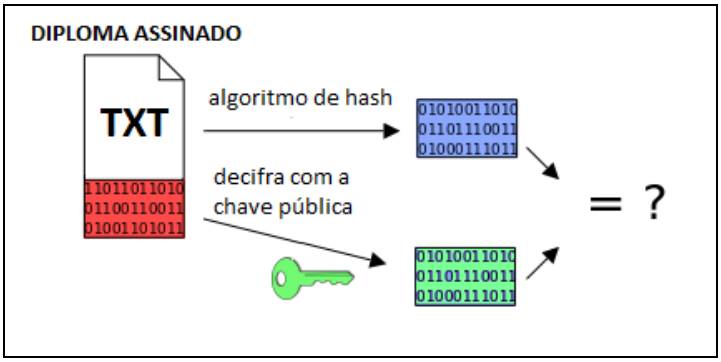

Figura 9 - Processo de funcionamento da validação da assinatura digital

Para executar o processo de *hash* do conteúdo do diploma submetido pelo usuário que deseja efetuar a verificação, é necessário a utilização do método `abreConteudoDiploma`

conforme o Quadro 17, que elimina a assinatura digital do diploma submetido, retornando apenas o conteúdo do diploma.

```
//Abre o arquivo sem a última linha(sem a assinatura)
function abreConteudoDiploma($arq){
    $cont="";
    $nr_linha_desejada = $this->nrlinhas($arq);
    $f_contents = file($arq);

    for ($i=0; $i<$nr_linha_desejada-1; $i++){
        $cont .= $f_contents [$i];
    }
    return $cont; //retorna conteudo
}
```

Quadro 17 – Método responsável por carregar somente o conteúdo do diploma (sem a assinatura digital)

Já para decifrar a assinatura digital e obter *hash* original do arquivo submetido, é necessário utilizar o método `abreUltimaLinha`, que retorna a somente a assinatura digital, conforme demonstrado no Quadro 18.

```
//abre arquivo pegando somente a assinatura (ultima linha)
function abreUltimaLinha($arq){
    $nr_linha_desejada = $this->nrlinhas($arq);
    $f_contents = file($arq);

    $ultima = $f_contents [$nr_linha_desejada-1];
    return $ultima; //retorna ultima linha
}
```

Quadro 18 – Método responsável por carregar somente a assinatura digital de um diploma

Após obter a assinatura digital do diploma submetido à validação, devemos utilizar o método `verificarDiploma` exposto no Quadro 19, que receberá como parâmetro o retorno do método `abreUltimaLinha`, ou seja, a assinatura digital, e por sua vez decifrará a mesma utilizando a chave pública do emissor. Como resultado, este método retorna o *hash* do conteúdo original, que é feito durante o processo de assinatura.

```
//Decifra a assinatura digital recebida como parâmetro
function verificarDiploma($conteudo){
    //carrega o arquivo que contém a chave pública que está na pasta chaves
    $nm_chav_pub = "chaves/publica_fg_ecpf.pem";
    $chave_publica = "";
    $file = file_get_contents($nm_chav_pub);
    //percorre chave pública
    for($i=0;$i<$this->nrcarac($nm_chav_pub);$i++){
        //testa se é o início da chave pública
        if($file[$i]=="-" and $file[$i+1]=="-"){
            //carrega a chave pública do arquivo para uma variável
            while ($i<$this->nrcarac($nm_chav_pub)){
                $chave_publica .= $file[$i];
                $i++;
            }
        }
    }
    //carrega chave pública com a função openssl
    openssl_get_publickey ($chave_publica);
    //decifra o conteúdo passado como parâmetro (assinatura digital)
    openssl_public_decrypt ($conteudo,$resultado,$chave_publica);
    //retorna a assinatura digital decifrada (que é um hash)
    return $resultado;
}
```

Quadro 19 – Método responsável pela verificação da assinatura digital de um diploma

Após este processo, conforme ilustra a Quadro 20, o sistema compara o retorno do método `verificarDiploma` (variável `$hash2`) com o *hash* do retorno do método `abreConteudoDiploma` (variável `$hash`), após esta comparação, caso os *hashs* sejam iguais, o sistema informa que o diploma é válido, caso contrário o sistema informa que o diploma é inválido.

```
//gera o hash do conteudo do diploma - retorno do método abreConteudoDiploma
$hash = sha1($diploma->abreConteudoDiploma($uploaddir.$_FILES['fileName']['name']));

//abreUltimaLinha - carrega a ultima linha do diploma (assinatura)
//verificarDiploma - decifra com a chave pública e retonra o hash original
$hash2 = $diploma->
verificarDiploma($diploma->abreUltimaLinha($uploaddir.$_FILES['fileName']['name']));

if ($hash == $hash2){
    echo "<center>O diploma é válido! <br>(Integridade e Autenticidade
    confirmadas com sucesso!)</center>";
    $auditoria->gerarAuditoria("verificou um diploma (válido) com sucesso!");
}else{
    echo "<center>O diploma não é válido! <br>(O diploma pode ter sido
    violado/adulterado)</center>";
    $auditoria->gerarAuditoria("verificou um diploma (inválido) com sucesso!");
}
```

Quadro 20 - Comparação entre os *hashs* para validação do diploma

```php
//Conta o número de linhas do arquivo passando como parâmetro
function nrlinhas($arq){
    $arquivo = fopen ($arq, "r");
    $num_linhas = 0;
    $caracteres = 0;
    //percorre o arquivo linha a linha ate o final do arquivo
    while (!feof ($arquivo)) {
        //se ainda existe linha no arquivo
        if ($linha = fgets($arquivo)){
            //acumula número de linhas
            $num_linhas++;
            //acumula número de caracteres desta linha
            $caracteres += strlen($linha);
        }
    }
    fclose ($arquivo);
    return $num_linhas; //retorna número de linhas
}
```

Quadro 21 – Método auxiliar responsável por retornar o número de linhas de um arquivo

Os métodos `nrlinhas` (Quadro 21) e `nrcarac` (Quadro 22) têm como função auxiliar os outros métodos da classe, retornando o número de linhas e o número de caracteres do arquivo passado como parâmetro respectivamente.

```php
//Conta o número de caracteres do arquivo passando como parametro
function nrcarac($arq){
    $arquivo = fopen ($arq, "r");
    $num_linhas = 0;
    $caracteres = 0;
    //percorre o arquivo linha a linha ate o final do arquivo
    while (!feof ($arquivo)) {
        //se ainda existe linha no arquivo
        if ($linha = fgets($arquivo)){
            //acumula número de linhas
            $num_linhas++;
            //acumulo o número de caracteres desta linha
            $caracteres += strlen($linha);
        }
    }
    fclose ($arquivo);
    return $caracteres; //retorna o número de caracteres
}
```

Quadro 22 – Método auxiliar responsável por retornar o número de caracteres de um arquivo

3.3.2.2 Implementação da classe auditoria

A classe `auditoria` tem como função gerar e formatar as trilhas de auditoria, assim

como, gravá-las em um arquivo.

O método `gerarAuditoria` (Quadro 23) recebe uma mensagem como parâmetro a formata, já o método `gravarArquivo` (Quadro 24) é utilizado para efetuar a gravação do arquivo no servidor.

```
//Formata a mensagem passada como parâmetro e prepara para gravação
function gerarAuditoria($mensagem){
    $arquivo = "auditoria/log.txt";
    $fp = fopen ($arquivo, "a");
    //formata mensagem
    $cont = "[".date('d/m/Y H:i:s')."] - Usuario: "
    .$_SESSION['login']." - ".$mensagem."\n";

    if (!fwrite($fp, $cont)){
        echo "Erro - Não foi possível escrever no arquivo.";
    }
    fclose($fp);
}
```

Quadro 23 – Método responsável por formatar a trilha de auditoria

```
//Grava a mensagem formatada no arquivo passado como parâmetro
function gravarArquivo($arquivo,$conteudo){
    $fp = fopen($arquivo, "w");
    fwrite($fp, $conteudo);
    fclose($fp);
}
```

Quadro 24 – Método responsável por gravar a trilha de auditoria no arquivo

3.3.3 Operacionalidade da implementação

Esta seção tem como objetivo mostrar a operacionalidade do ambiente, abordando os casos de uso atendidos pelo mesmo. Na seção 3.3.3.1 é apresentado a operacionalidade da autenticação utilizando certificado digital. Na seção 3.3.3.2 são apresentadas as funcionalidades gerais do sistema, já na seção 3.3.3.3 é apresentado a operacionalidade da assinatura digital e a verificação, e por fim, na seção 3.3.3.4 é apresentado a operacionalidade da auditoria.

3.3.3.1 Autenticação utilizando certificado digital

Para o usuário poder acessar o ambiente via HTTPS e visualizar a validade do certificado no navegador, seria necessário que o servidor possuísse um certificado digital

assinado por uma AC reconhecida como a Verisign, cujo certificado digital já está instalado na maioria dos computadores, mas devido ao alto custo de se obter um certificado desta natureza, optou-se por gerar um certificado de servidor auto-assinado utilizando o comando makecert do servidor Apache, conforme ilustra a Figura 10.

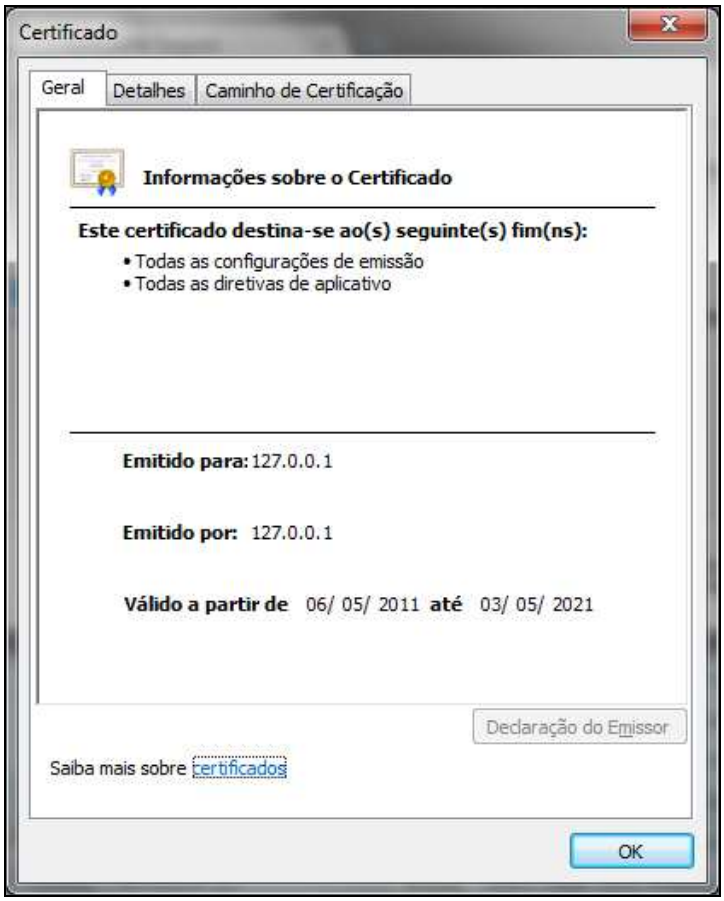

Figura 10 - Certificado digital do servidor

Após obter o certificado auto-assinado para o servidor, foi necessário instalar este certificado no repositório de autoridades certificadoras confiáveis através do navegador, desta forma o navegador consegue reconhecer o certificado enviado pelo servidor conforme ilustrado na Figura 11. Este processo de instalação do certificado não seria necessário caso o mesmo fosse assinado por uma AC reconhecida que já estivesse instalada no computador.

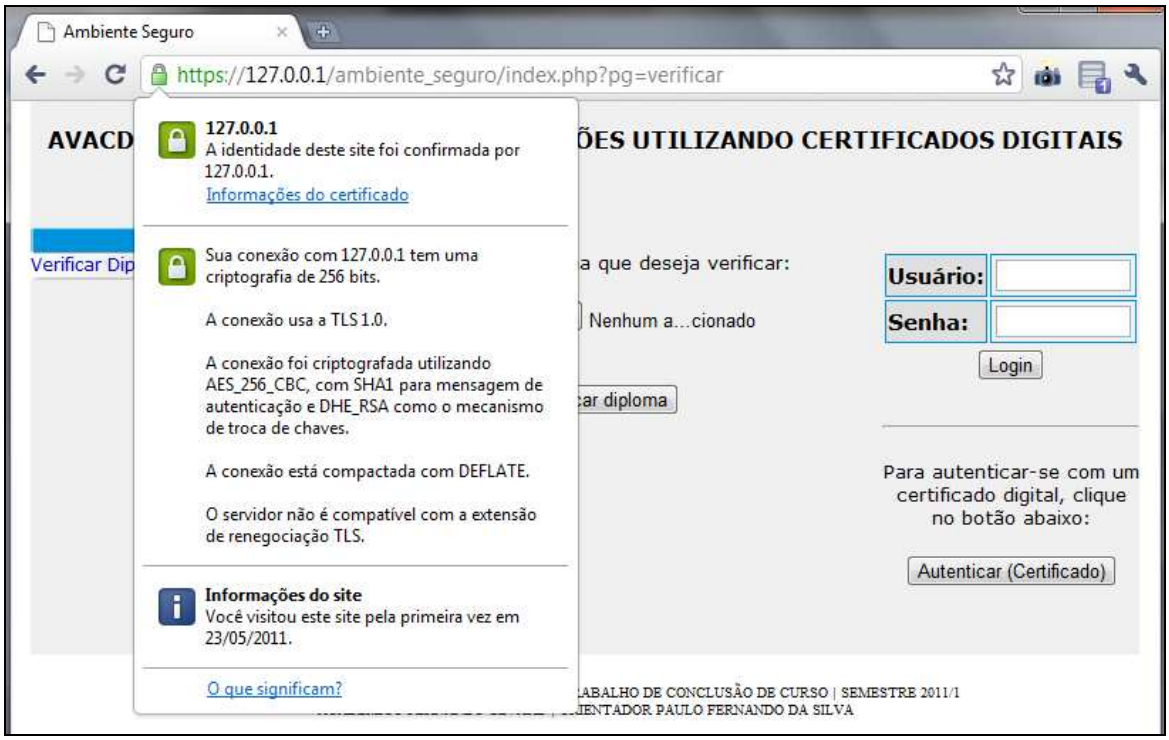

Figura 11 - Detalhes do certificado digital do servidor

Para gerar o certificado digital do cliente[3], criou-se uma AC[4] chamada TCC e utilizou-se este certificado para assinar[5] o certificado do cliente diretor, que por sua vez foi instalado no repositório pessoal de certificados conforme ilustra a Figura 13, já a AC TCC foi instalada no repositório de autoridades de certificação raiz confiáveis conforme ilustra a Figura 12. Destaca-se que a instalação dos certificados inclui as suas respectivas chaves privadas, e não é possível efetuar a autenticação se estes não estiverem devidamente instalados.

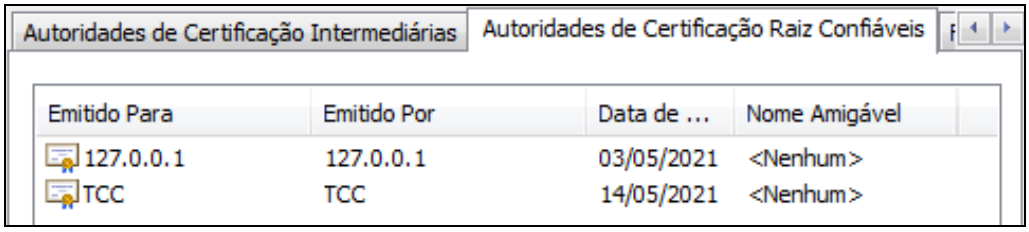

Figura 12 - Repositório de autoridades de certificação raiz confiáveis

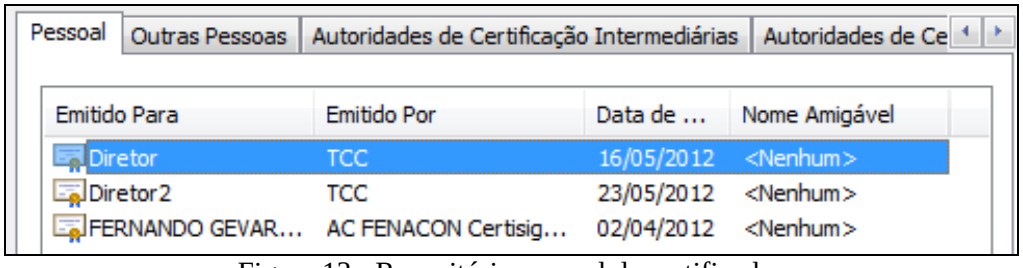

Figura 13 - Repositório pessoal de certificados

Conforme ilustrado na Figura 14, para instalar o certificado do diretor no repositório, é

[3] Veja no anexo A, como gerar o certificado digital do cliente.
[4] Veja no anexo A, os passos para gerar o certificado digital da AC TCC (auto-assinado).

necessário digitar a senha referente à chave privada, desta forma, caso o certificado seja furtado, ele não poderá ser instalado sem esta senha, além disso, a instalação ainda permite selecionar uma opção que avisa o usuário quando a sua chave privada está sendo utilizada por algum aplicativo, oferecendo a oportunidade ao usuário de cancelar um suposto uso indevido de sua chave. Outra questão importante na hipótese de um possível furto é a opção que o usuário tem de não marcar a sua chave como exportável, fazendo com que ninguém possa obter a sua chave através do navegador. Conforme demonstra o nível de segurança alto na Figura 15, o usuário também poderá definir uma senha de proteção para ser exigida no momento em que alguma aplicação for utilizar a sua chave privada.

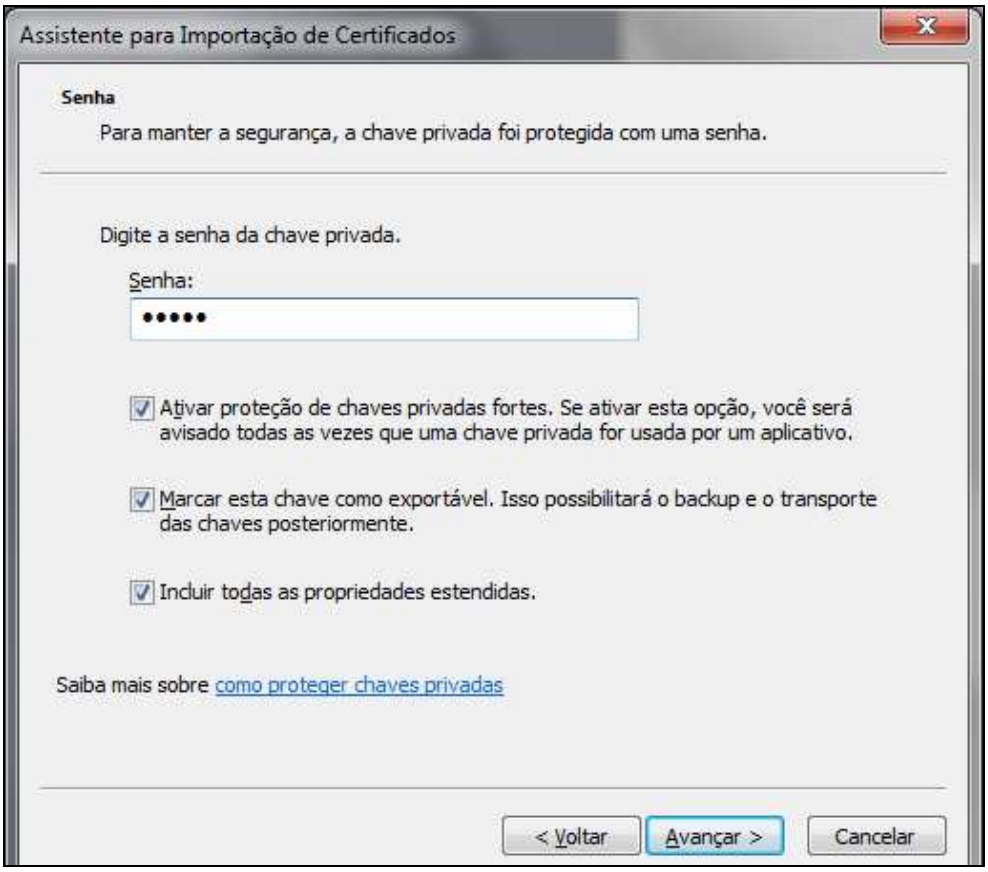

Figura 14 - Opções de instalação do certificado do diretor

Para que o servidor Apache reconhecesse os certificados do tipo cliente da AC TCC foi necessário configurar[6] algumas diretivas dentro do seu arquivo de configurações do SSL.

Destaca-se que para gerar e assinar os certificados digitais, assim como converter os certificados para um formato conforme especificado pelo servidor, novamente utilizou-se a ferramenta OpenSSL.

[5] Veja no anexo A, os passos para assinar um certificado digital de cliente utilizando o certificado de uma AC.
[6] Veja no anexo B, como configurar o apache para fazer a autenticação utilizando certificados digitais.

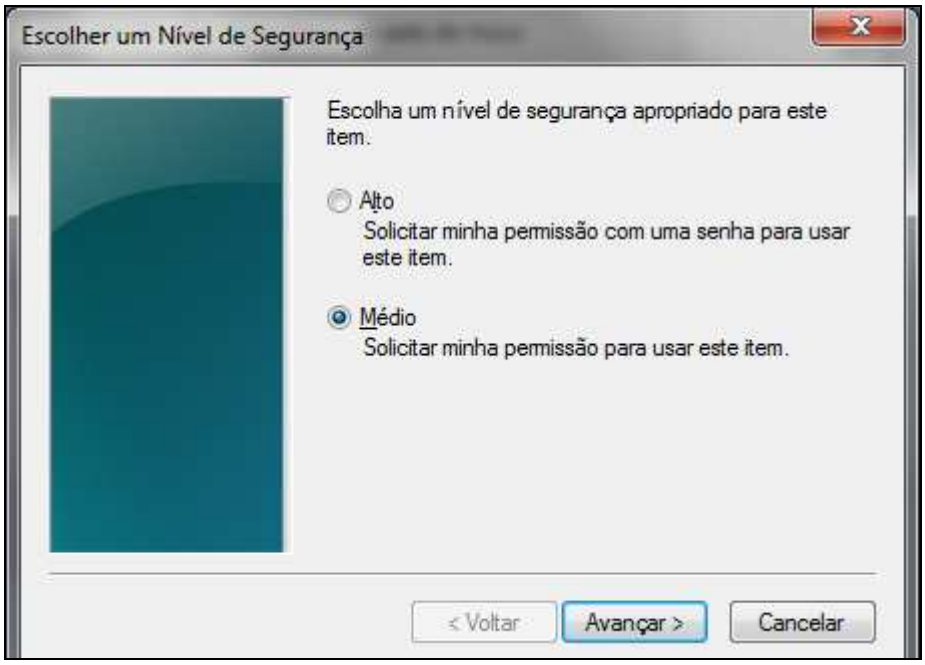

Figura 15 - Nível de segurança da chave privada do diretor

Conforme ilustra a Figura 16, ao acessar o ambiente, caso o usuário possua algum certificado digital assinado pela AC TCC, o navegador abre uma janela para que o usuário possa escolher com qual certificado ele deseja se autenticar no servidor, após esta escolha, caso o usuário clique no botão `Autenticar (Certificado)`, conforme ilustrado na Figura 11, o sistema verifica se o certificado do cliente foi reconhecido com sucesso e se o campo "nome" do certificado é igual a "diretor", de forma que se estas condições forem satisfeitas, o usuário do tipo diretor é autenticado no sistema. Destaca-se também que não é necessário possuir um certificado assinado pela AC TCC instalado para acessar o ambiente, e que o usuário do tipo diretor também possui a opção de se autenticar através de um nome de usuário e senha.

É importante comentar que o ambiente está preparado para trabalhar somente com um usuário do tipo diretor, desta forma, caso o usuário escolha um certificado digital válido, como o certificado do "Diretor2" ilustrado na Figura 16, apesar de servidor autenticar o cliente, o ambiente não efetuará a autenticação, pois o campo "nome" do certificado não é igual a "Diretor".

Para que o ambiente pudesse trabalhar com mais de um usuário do tipo diretor, um gerenciamento de chaves públicas de cada diretor poderia ser implementado, fazendo com que ao verificar a validade de um diploma virtual assinado, o sistema selecionasse a chave pública de acordo com o diretor que assinou o diploma submetido.

Para os usuários dos tipos professor e aluno, optou-se pela autenticação somente via nome de usuário e senha.

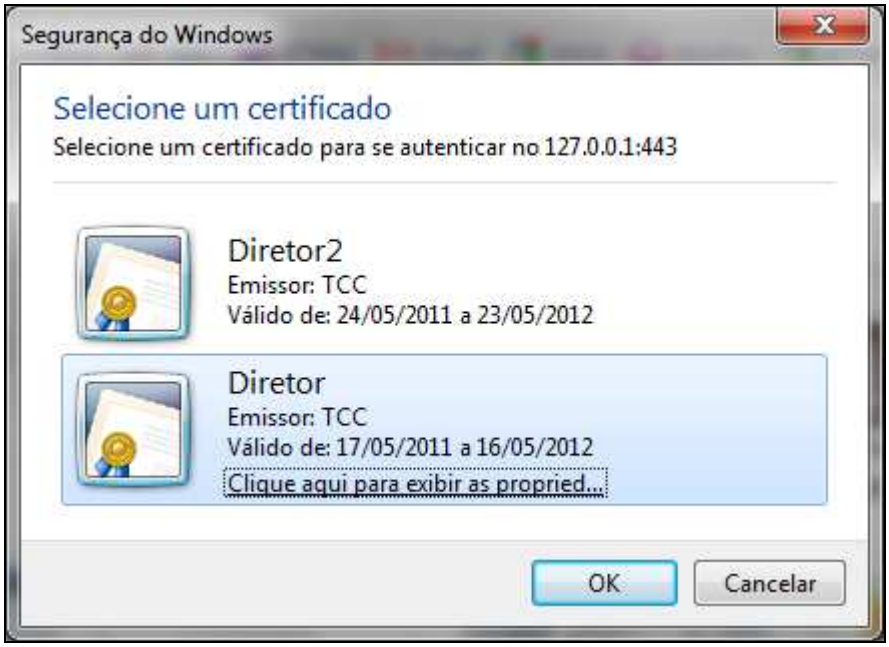

Figura 16 – Selecionando um certificado válido para autenticar o cliente

3.3.3.2 Funcionalidades gerais

Esta subseção apresenta apenas as particularidades mais relevantes das funcionalidades gerais do ambiente.

Algumas características gerais do ambiente destacam-se na Figura 29, onde é possível observar o menu geral, que permite, a verificação de um diploma sem estar autenticado, a autenticação através da utilização de um nome de usuário e senha, e a autenticação utilizando um certificado digital válido, ou seja, assinado pela AC configurada no servidor.

Uma das funcionalidades mais relevantes desta subseção é a utilização da função de *hash* no cadastro de usuários ilustrado na Figura 18. Este processo ocorre antes de armazenar a senha do usuário no banco de dados, desta forma, após o usuário informar a senha na hora da autenticação, o sistema faz o *hash* da senha informada e compara com o *hash* que está no banco conforme ilustra a Figura 17.

idusuario	login	senha	nome	cpf	dt_nascimento	dt_cadastro	nivel
4	proff	78be2913e9faa3c49fdf2ffc1f92d9eae3522497	PROF	4294967295	1222-12-12	2011-04-02	2
5	diretor	a381c49be4281e966501440a58ef30914abc4b37	DIRETOR	0	1988-1-1	2011-04-19	3
19	aluno1	f72eafc539768d2970925fd963a8f3b015a917c6	ALUNO1	198798	1999-1-1	2011-05-11	1
20	aluno2	b7ef9da90a2bd79099ebd48db885344a872bb155	ALUNO2	9879879	1999-1-1	2011-05-11	1

Figura 17 - Utilização da função de *hash* para armazenar a senha do usuário

No item tipo/nível do cadastro de usuários ilustrado na Figura 18, define-se a

permissão de cada usuário cadastrado no sistema, de tal forma que cada um destes possa ter acesso apenas as suas respectivas funcionalidades. Após efetuar o cadastro de um professor, já é possível que este se autentique e utilize todas as funcionalidades destinadas a ele.

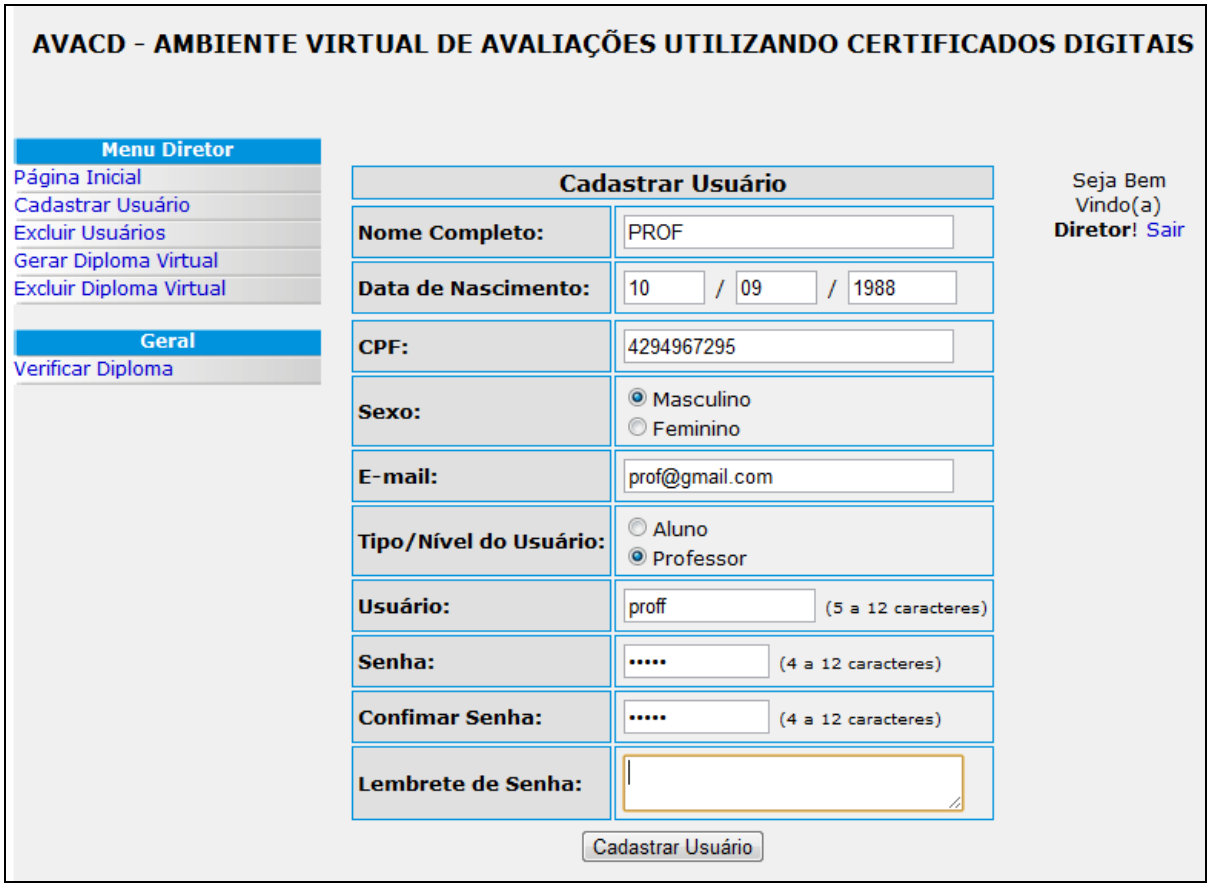

Figura 18 - Tela do caso de uso `UC09 – Cadastrar usuário`

É importante comentar que ao excluir um usuário do tipo aluno, conforme ilustra a Figura 19, o diretor apenas retira o seu direito de autenticação no sistema, desta forma, o professor ainda poderá gerar relatórios das provas executadas pelo aluno que foi excluído.

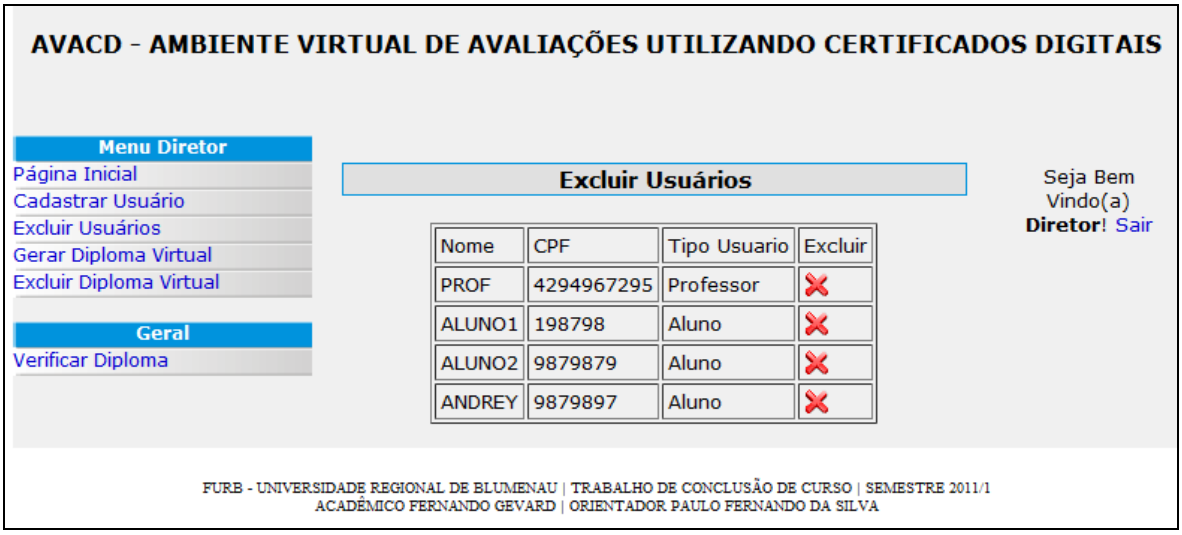

Figura 19 - Tela do caso de uso `UC10 – Excluir usuário`

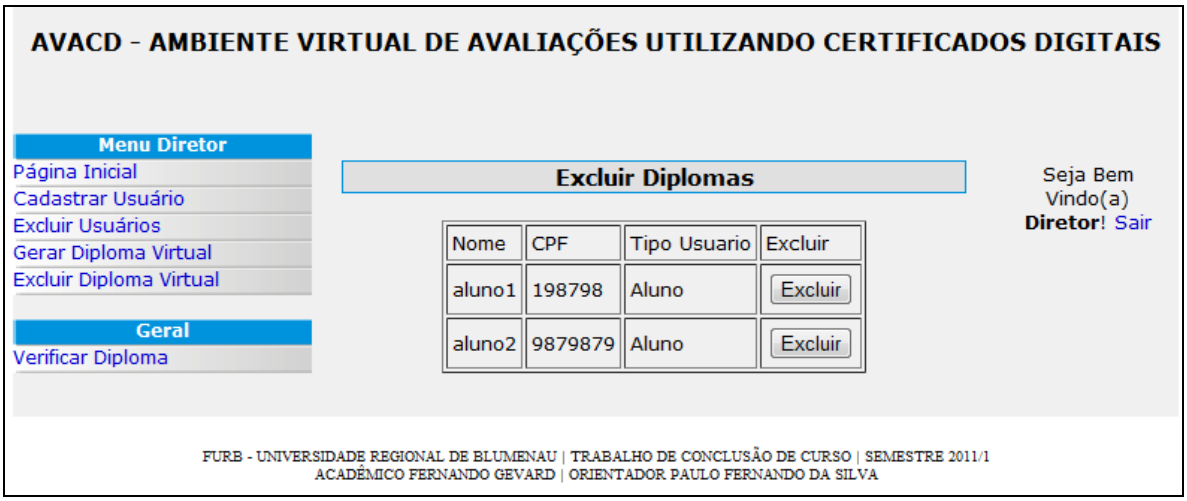

Figura 20 - Tela do caso de uso `UC14 – Excluir diploma`

Na Figura 20, ao clicar no botão `excluir`, o sistema apaga o diploma virtual gerado, desta forma, o diploma passa a ficar indisponível para o aluno efetuar o download.

A Figura 21 ilustra a funcionalidade criar provas, que pode ser executada pelo professor, bastando apenas digitar o assunto da prova e clicar no botão `cadastrar prova`.

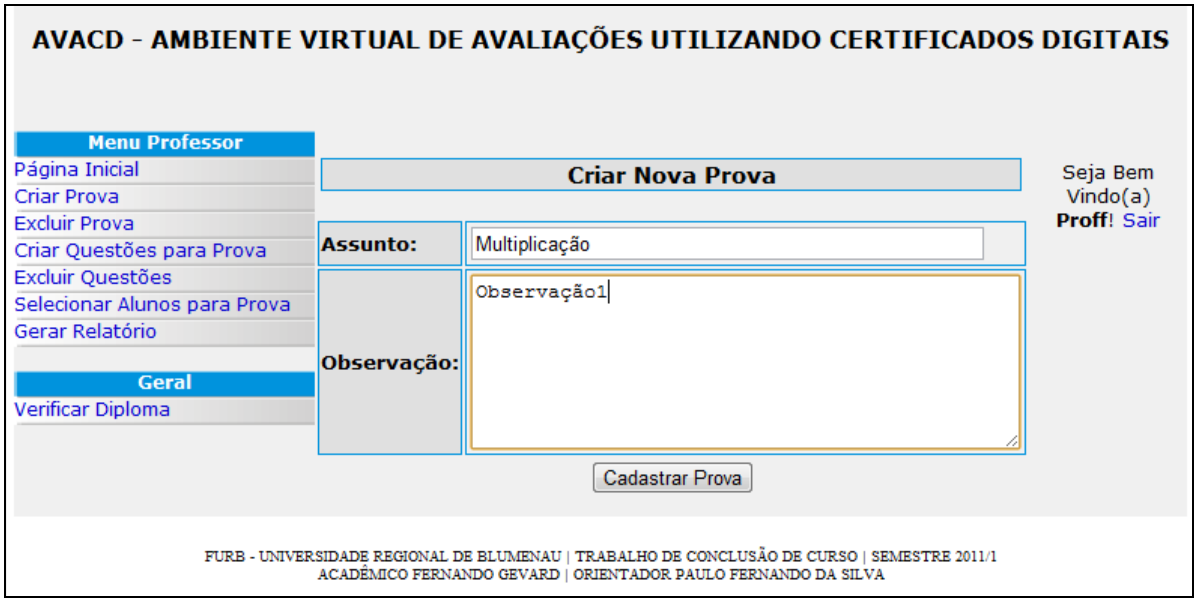

Figura 21 - Tela do caso de uso `UC01 – Criar prova`

A Figura 22 apresenta a funcionalidade de exclusão de provas. Ao excluir uma prova, todas as questões vinculadas a ela também são excluídas, impossibilitando até mesmo a geração relatórios das execuções da mesma.

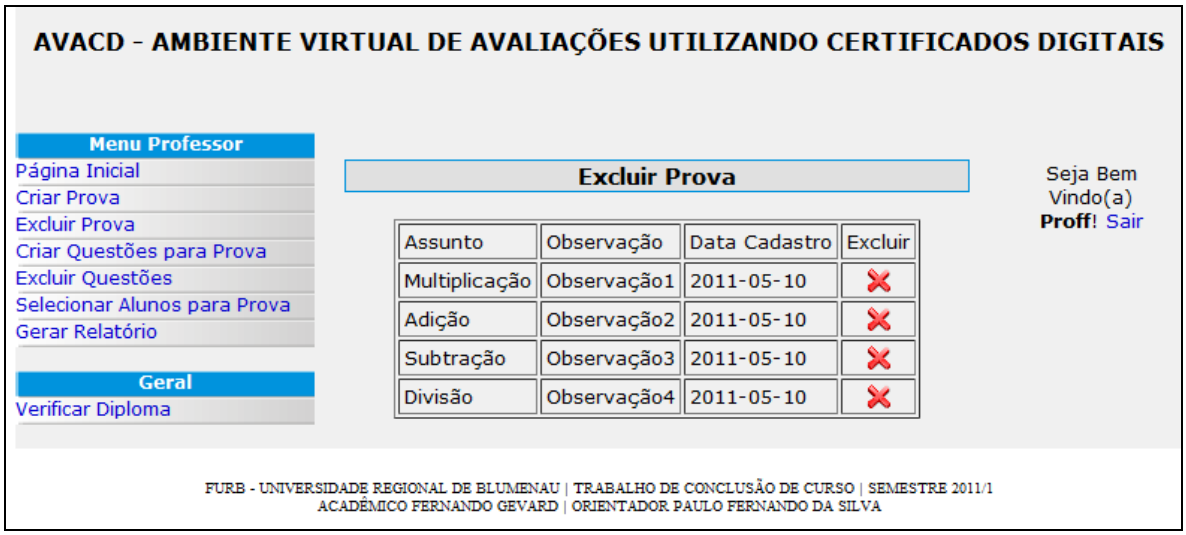

Figura 22 - Tela do caso de uso `UC02 – Excluir prova`

A Figura 23 destaca a funcionalidade criar uma questão, enquanto a Figura 24 destaca a opção de excluir uma questão, que caso seja executada faz também com que o sistema apague todas as respostas vinculadas a ela.

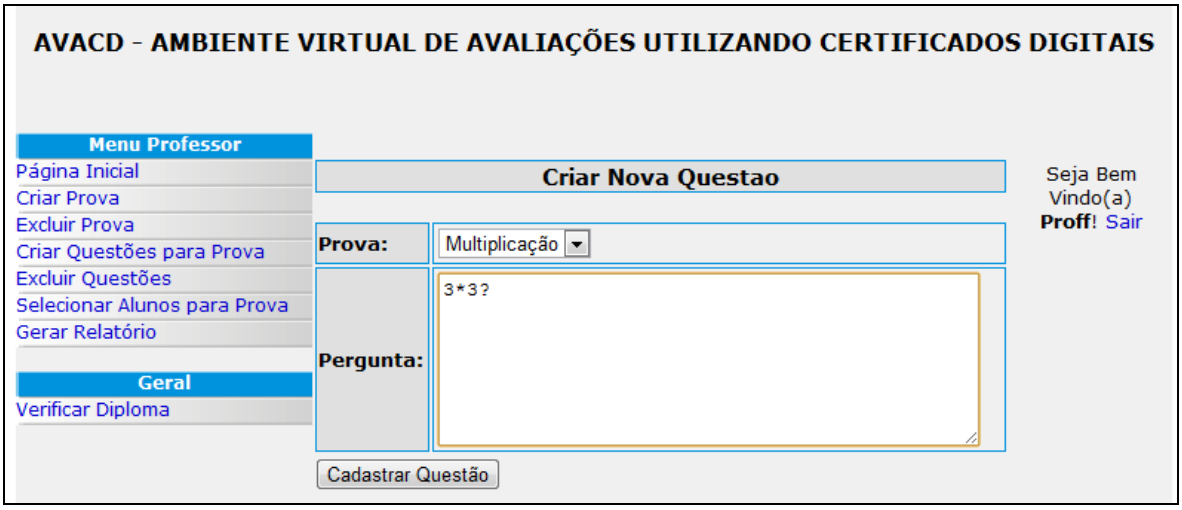

Figura 23 - Tela do caso de uso `UC03 – Criar questão`

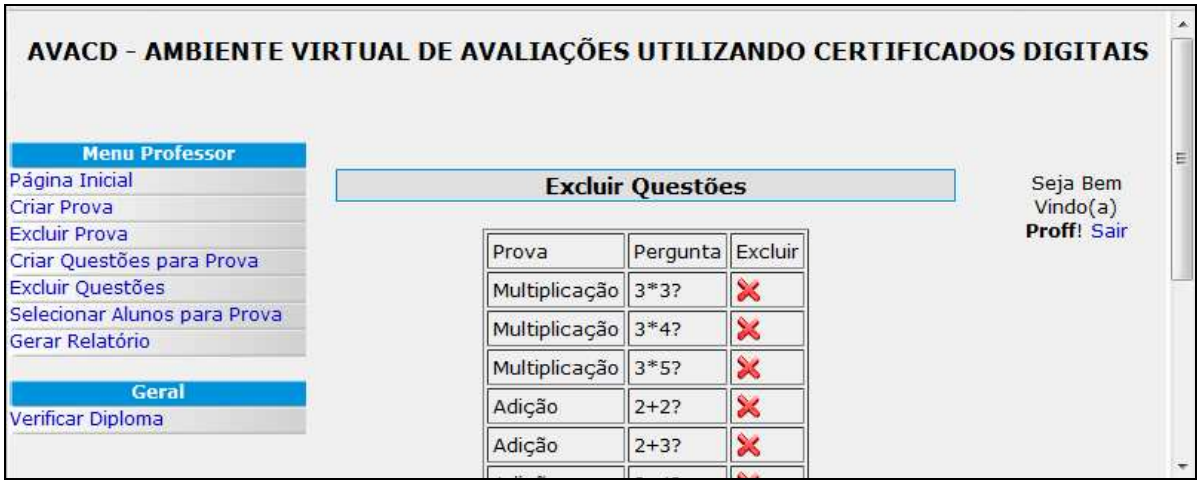

Figura 24 - Tela do caso de uso `UC04 – Excluir questão`

A Figura 25 demonstra a funcionalidade de associar ou desassociar um aluno para executar uma prova. Para que não haja problema com a perda de alguma prova respondida, o sistema passa a permitir somente a desassociação das provas que ainda não foram respondidas.

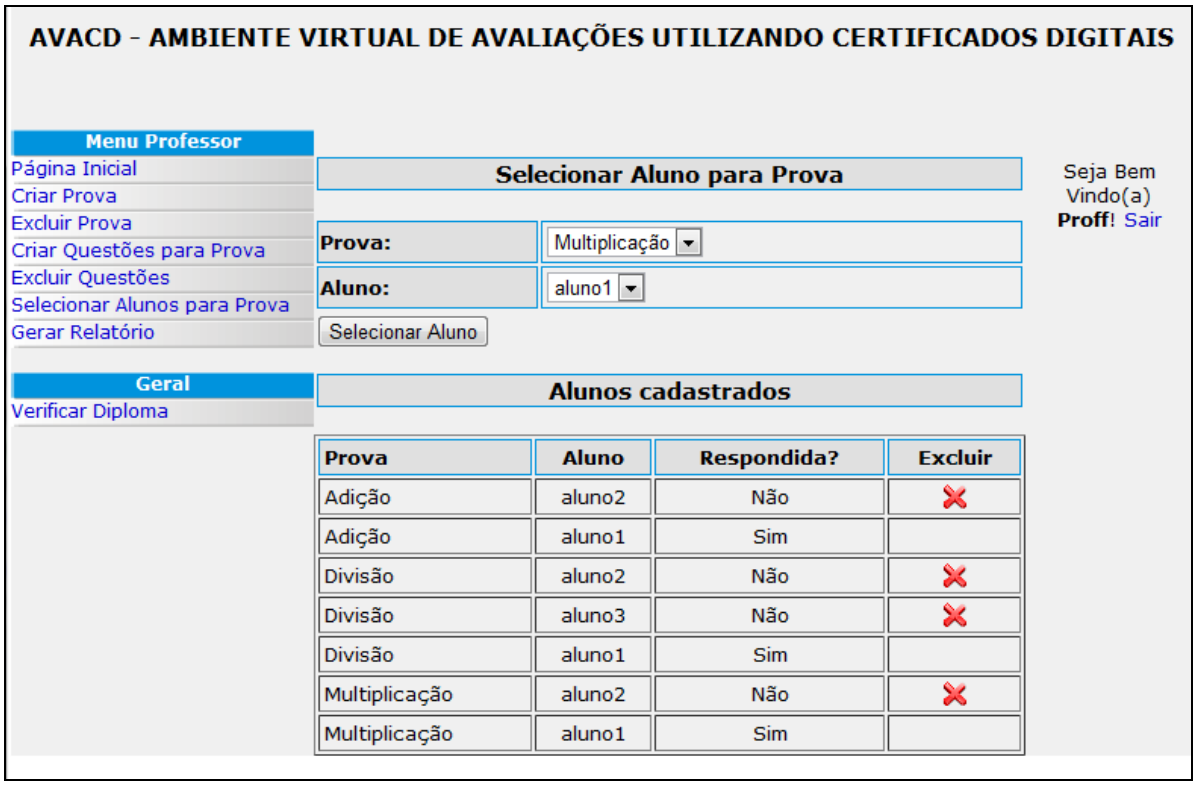

Figura 25 - Tela do caso de uso `UC05 – Selecionar alunos para prova`

Conforme ilustrado na Figura 28, para o usuário do tipo aluno as funcionalidades disponíveis são apenas a execução de provas, a verificação do diploma e o download de um diploma virtual caso exista algum disponível.

3.3.3.3 Assinatura digital e verificação

Para assinar digitalmente o diploma virtual do aluno, optou-se por utilizar um certificado digital e-CPF da ICP-BRASIL, onde foi utilizado a ferramenta OpenSSL (YOUNG; HUDSON, 1999) para extrair[7] a chave privada e a chave pública.

Para acessar o menu gerar diploma virtual ilustrado na Figura 26, usuário diretor deve estar autenticado no sistema, após este procedimento, o diretor seleciona a sua chave privada, que pode estar em seu computador ou em um disco removível, clicando no botão `escolher`

arquivo. Após ter a sua chave privada carregada, o diretor seleciona o aluno a receber o diploma, e por fim, clica no botão gerar e assinar diploma, fazendo com que o sistema crie um diploma virtual assinado digitalmente e o disponibilize na página principal do aluno.

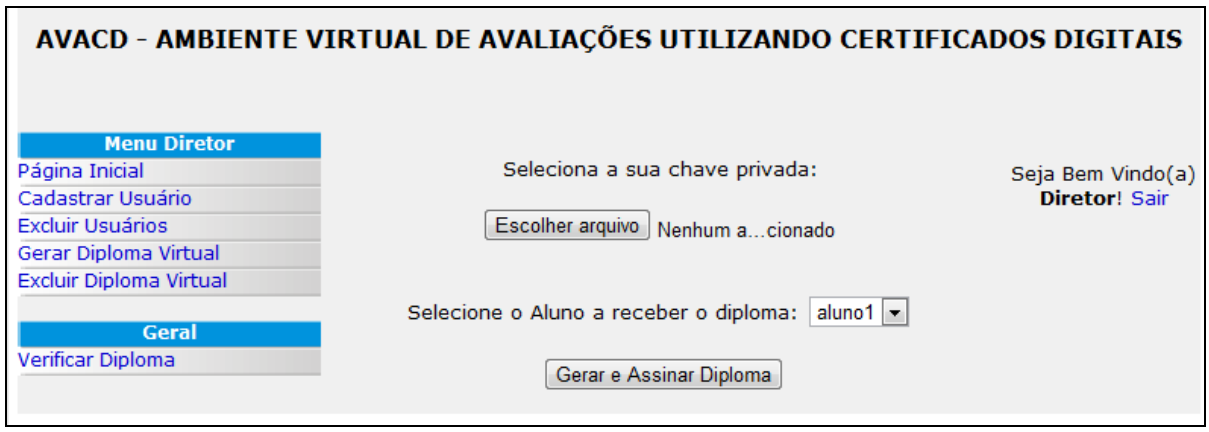

Figura 26 - Tela do caso de uso UC11 – Gerar diploma

Após o processo de geração e assinatura do diploma virtual, obtemos o arquivo usuario_diploma_assinado.txt ilustrado na Figura 27, que contém as informações pessoais do aluno, como nome do aluno, data de nascimento e CPF. No diploma também consta o nome do diretor que assinou o diploma e por fim, a assinatura digital.

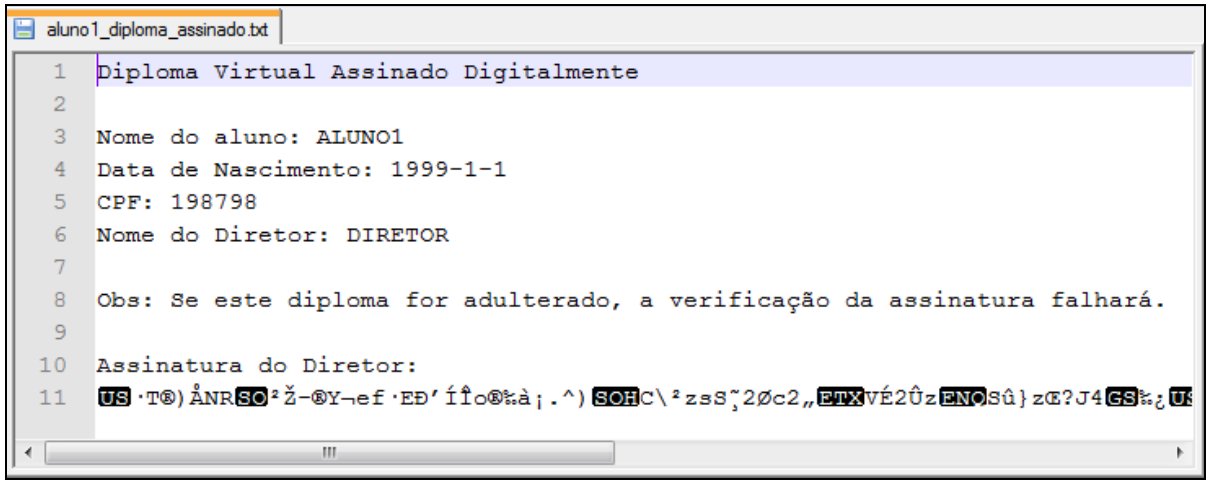

Figura 27 - Conteúdo de um diploma virtual gerado e assinado pelo diretor

O diploma virtual assinado ilustrado na Figura 27 é disponibilizado ao aluno para download conforme ilustrado na Figura 28.

[7] Veja no anexo A, os comandos de extração das chaves privada e pública (após exportá-las do navegador) utilizando o OpenSSL.

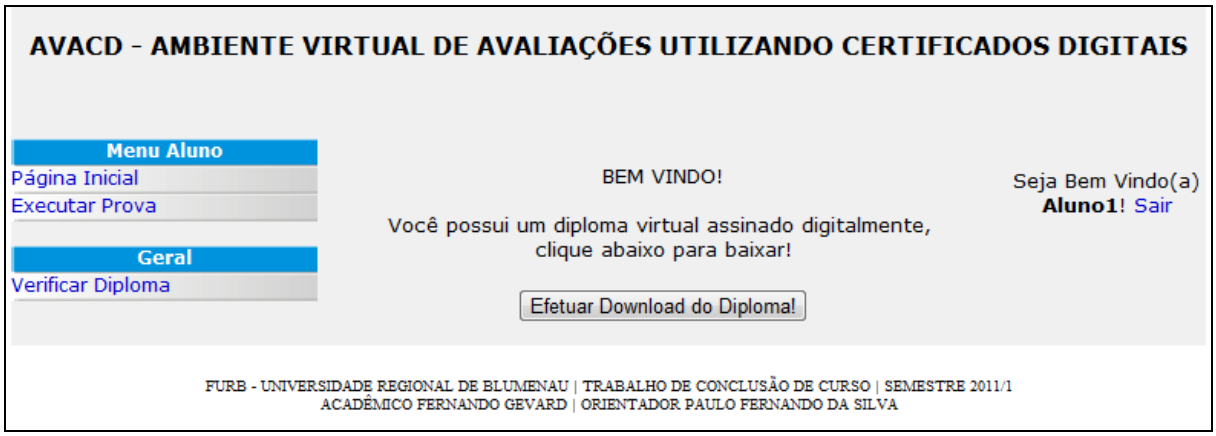

Figura 28 - Tela do caso de uso `UC15 – Efetuar download do diploma gerado`

Para fazer a validação do diploma virtual assinado, ou seja, verificar se este é ou não um diploma válido, não é necessário estar autenticado no sistema, desta forma, qualquer usuário poderá entrar no ambiente para fazer a verificação.

Ao acessar o menu verificar diploma ilustrado na Figura 29, e ao clicar no botão `escolher arquivo`, o sistema abre uma janela para que o usuário selecione o diploma em seu computador ou em um disco removível, e após clicar em verificar diploma, o sistema informa se o diploma é válido ou inválido.

O processo de verificação do diploma virtual pode ser observado na Figura 9.

Figura 29 - Tela do caso de uso UC08 – Verificar assinatura do diploma

3.3.3.4 Auditoria

O processo de auditoria do sistema é feito a cada ação relevante do usuário, tais como fazer autenticação, cadastrar usuários, excluir usuários, gerar e assinar diploma, excluir diploma, verificar diploma, criar prova, excluir prova, criar questões para prova, excluir

questões, selecionar aluno para prova, excluir seleção de aluno para prova, gerar relatório, executar prova, efetuar o download do diploma e sair do sistema.

A Figura 30 demonstra o arquivo `log.txt` responsável por armazenar todas as trilhas de auditoria.

log.txt

```
[26/05/2011 11:07:49] - Usuario: diretor -  logado com sucesso!
[26/05/2011 11:09:03] - Usuario: diretor - cadastrou o usuário fernando com sucesso.
[26/05/2011 11:09:13] - Usuario: diretor - excluiu o usuario FERNANDO com sucesso!
[26/05/2011 11:10:26] - Usuario: diretor - gerou o diploma do aluno (aluno2) com sucesso!
[26/05/2011 11:10:29] - Usuario: diretor - excluiu o diploma do aluno aluno1 com sucesso!
[26/05/2011 11:11:02] - Usuario: diretor -  efetuou logout com sucesso!
[26/05/2011 11:11:20] - Usuario: diretor - verificou um diploma (válido) com sucesso!
[26/05/2011 11:12:06] - Usuario: proff -  logado com sucesso!
[26/05/2011 11:12:22] - Usuario: proff - criou a prova (assunto: Matemática) com sucesso!
[26/05/2011 11:12:36] - Usuario: proff - excluiu a prova (assunto: Divisão) com sucesso!
[26/05/2011 11:12:44] - Usuario: proff - criou a questão (1+1?) com sucesso!
[26/05/2011 11:12:55] - Usuario: proff - criou a questão (1+2?) com sucesso!
[26/05/2011 11:13:03] - Usuario: proff - excluiu a questao (1+2?) com sucesso!
[26/05/2011 11:13:11] - Usuario: proff - selecionou o aluno (aluno1) para realizar a prova (assunto: Matemática)
[26/05/2011 11:13:13] - Usuario: proff - selecionou o aluno (aluno2) para realizar a prova (assunto: Matemática)
[26/05/2011 11:13:17] - Usuario: proff - excluiu o aluno (aluno2) de executar a prova (assunto: Matemática)
[26/05/2011 11:13:27] - Usuario: proff -  efetuou logout com sucesso!
[26/05/2011 11:13:34] - Usuario: aluno1 -  logado com sucesso!
[26/05/2011 11:13:44] - Usuario: aluno1 - executou a prova (assunto: Matemática) com sucesso!
[26/05/2011 11:13:48] - Usuario: aluno1 -  efetuou logout com sucesso!
[26/05/2011 11:14:35] - Usuario: aluno2 -  logado com sucesso!
[26/05/2011 11:14:38] - Usuario: aluno2 - efetuou download do seu diploma virtual assinado!
[26/05/2011 11:14:40] - Usuario: aluno2 -  efetuou logout com sucesso!
[26/05/2011 11:14:49] - Usuario: proff -  logado com sucesso!
[26/05/2011 11:14:56] - Usuario: proff - gerou relatório da prova (assunto: Matemática) com sucesso!
[26/05/2011 11:15:00] - Usuario: proff -  efetuou logout com sucesso!
[26/05/2011 11:15:05] - Usuario:  - verificou um diploma (válido) com sucesso!
[26/05/2011 11:15:25] - Usuario:  - verificou um diploma (inválido) com sucesso!
```

Figura 30 - Arquivo responsável por armazenar as trilhas de auditoria

3.4 RESULTADOS E DISCUSSÃO

Os resultados obtidos com o término do trabalho são satisfatórios, pois com a utilização do ambiente foi possível constatar que todos os requisitos e objetivos foram de fato atingidos.

O sistema foi implementado utilizando a linguagem PHP, o banco de dados MySQL e o servidor Apache.

A ferramenta OpenSSL mostrou-se indispensável para executar tarefas como, a exportação das chaves privada e pública do certificado digital e-CPF, a geração do certificado da AC TCC, a geração do certificado do cliente diretor, e por fim, a conversão[8] dos certificados para alguns formatos necessários, tais como, o formato PEM para o servidor

[8] Veja no anexo A, como converter um certificado digital para outros formatos.

Apache e o formato P12 para importar o certificado do cliente para o repositório de certificados pessoais do navegador.

Para a assinatura digital dos diplomas, optou-se pela utilização de um certificado digital e-CPF da ICP-BRASIL, desta forma, pode-se constatar que o resultado de se trabalhar com um certificado gerado por uma AC como a ICP-BRASIL, é igual a se trabalhar com um certificado gerado pela ferramenta OpenSSL.

A Figura 10 mostra que o certificado é de fato auto-assinado, pois o campo “emitido para” é igual ao campo “emitido por”, e para que ele seja reconhecido, é necessário que ele seja instalado no repositório de chaves confiáveis.

As maiores vantagens apresentadas pelo ambiente são também os diferenciais que ela apresenta, tais como, a autenticação segura com o certificado digital do tipo cliente, que permite ao usuário se autenticar sem necessitar de um usuário e senha, o acesso ao ambiente de forma segura utilizando HTTPS, que permite ao usuário ter certeza de que ele está navegando no site correto, o uso da função de *hash* para armazenar a senha dos usuários cadastrados no banco de dados, que faz com que nenhum administrador do banco possa descobrir a senha de algum usuário, e por fim, a utilização da assinatura digital para garantir a integridade e a autenticidade do diploma gerado pelo diretor.

Em relação aos trabalhos correlatos o trabalho de Daney (2007), apresentou-se como uma ferramenta que possui apenas a funcionalidade de gerar avaliações, pois não possui nenhum requisito de segurança da informação implementado além da autenticação de usuários, já o trabalho de Mathias (2007) explora apenas as funcionalidades de segurança da informação, tais como geração de par de chaves e emissão de certificados auto-assinados.

O trabalho correlato AVA da FURB destacou-se como uma ferramenta que possui a funcionalidade de avaliação, mas não possui muitos requisitos de segurança de informação implementados conforme demonstrado no Quadro 25.

O Quadro 25 apresenta as principais características em comum entre os trabalhos correlatos e o ambiente implementado neste trabalho, as quais são:

a) cadastro de usuários: cadastrar um novo usuário no banco de dados;
b) níveis de permissão de acesso para cada usuários: liberar as funcionalidades pertinentes ao usuário autenticado de acordo com o seu nível de permissão definidos na hora do cadastro de usuários;
c) cadastrar prova: cadastrar uma nova prova no banco de dados;
d) cadastrar questão: cadastrar uma questão no banco de dados;
e) gerar relatório: gerar relatório de uma prova executada pelo aluno;

f) executar provas: permitir que o aluno execute uma prova existente e associada a ele;
g) autenticação: permitir que apenas o usuário do sistema acesse uma área restrita;
h) auditoria: gerar um arquivo com trilhas de auditoria para armazenar todas as ações executadas pelos usuários do sistema;
i) proteção de dados do usuário: utilizar a função de *hash* antes de armazenar a senha do usuário no banco de dados;
j) criptografia: utilizar no mínimo um algoritmo de criptografia para cifrar ou decifrar alguma informação importante;
k) certificado digital: utilizar no mínimo um certificado digital;
l) assinatura digital: utilizar a técnica de assinar digitalmente alguma informação ou arquivo;
m) canais seguros: utilizar algum canal seguro, como por exemplo o HTTPS.

Características	**Possui a respectiva característica implementada?**			
	Este Ambiente	**Trabalho Daney**	**Trabalho Mathias**	**AVA - FURB**
Cadastro de Usuários	Sim	Sim	Não	Sim
Níveis de permissão de acesso para cada usuário	Sim	Sim	Não	Sim
Cadastrar Provas	Sim	Sim	Não	Sim
Cadastrar Questões	Sim	Sim	Não	Sim
Gerar Relatório (Provas)	Sim	Sim	Não	Sim
Executar Provas	Sim	Não	Não	Sim
Autenticação	Sim	Sim	Não	Sim
Auditoria	Sim	Não	Não	Não
Proteção de dados do usuário (*hash*)	Sim	Não	Sim	Sim
Criptografia	Sim	Não	Sim	Não
Certificado Digital	Sim	Não	Sim	Não
Assinatura Digital	Sim	Não	Não	Não
Canais seguros (HTTPS)	Sim	Não	Não	Não

Quadro 25 – Comparativo com os trabalhos correlatos

4 CONCLUSÕES

O Protótipo de Ambiente Virtual de Avaliações Utilizando Certificados Digitais (AVACD) teve por objetivo ser capaz de gerar diplomas virtuais assinados digitalmente, criar e executar avaliações de forma segura, utilizando HTTPS, protegendo as senhas dos usuários com função de *hash*, controlando o acesso, a permissão e as ações dos usuários cadastrados.

O público alvo deste ambiente não é somente da área de computação e, sabendo-se que os usuários leigos geralmente cometem erros de operação foi implementado as trilhas de auditoria, que permitem desvendar todas as ações feitas pelos usuários, desta forma, contemplando também o não-repúdio destas ações.

Durante este trabalho, desenvolveu-se um estudo na área de segurança da informação, mais detalhadamente sobre certificados digitais. Este estudo trouxe subsídios para a aplicação dos requisitos referentes à segurança da informação no AVACD.

Com a compra do certificado digital e-CPF e com as técnicas de criptografia assimétrica, foram implementados os métodos responsáveis por assinar digitalmente o conteúdo de um diploma virtual gerado pelo professor, assim como, outro método para verificar a assinatura digital do diploma posteriormente. Para assinar e fazer a verificação da assinatura, utilizaram-se as chaves (privada e pública) extraídas do e-CPF com a ajuda da ferramenta OpenSSL.

O diploma virtual assinado foi gerado no formato de texto para que impossibilite a colisão de *hash*, ou seja, para que seja impossível que outra pessoa altere o diploma virtual assinado de tal forma que a função de *hash* deste diploma adulterado retorne o mesmo resultado da função de *hash* de um diploma válido.

Para fazer a autenticação dos usuários do tipo aluno e professor, optou-se pela utilização de um usuário e senha, já para a autenticação do usuário do tipo diretor, por ser o que executa a função mais relevante no sistema, optou-se pela utilização do certificado digital e-CPF, que é um mecanismo mais seguro.

Na auditoria implementou-se a classes responsável por gravar a trilha de auditoria em um arquivo no servidor em formato de texto.

Com relação às técnicas e tecnologias utilizadas para o desenvolvimento do ambiente, a linguagem de programação PHP em conjunto com o banco de dados MySQL e com as ferramentas DreamWeaver e OpenSSL, atenderam as expectativas permitindo que todos os requisitos elicitados fossem atendidos.

Após o término do trabalho, destaca-se a conclusão de todos os principais objetivos planejados, tais como a utilização de certificados digitais, assinatura digital, trilhas de auditoria, autenticação e função de *hash*.

Com este trabalho pode-se concluir que o desenvolvimento de um ambiente que atenda os itens de segurança da informação é viável, porém torna-se muito trabalhoso quando o estudo de uma tecnologia como certificados digitais faz-se necessário.

4.1 EXTENSÕES

Como extensão para o presente trabalho propõe-se:

a) gerenciar várias chaves públicas de vários usuários do tipo diretor, para que mais diretores possam gerar e assinar um diploma virtual;
b) permitir ao professor gerar de provas com questões já cadastradas e selecionadas de maneira aleatória pelo sistema;
c) permitir ao professor informar o nível de dificuldade de cada questão cadastrada, para que seja possível gerar uma prova de acordo com o nível de dificuldade desejado;
d) implementar mais tipos de questões além da questão do tipo dissertativa já existente;
e) implementar um sistema de auto-correção de provas;
f) implementar um quadro de notas para todos os alunos e gerar automaticamente diplomas virtuais assinados a partir da média final do aluno;
g) permitir ao aluno a visualização de suas notas e médias.

REFERÊNCIAS BIBLIOGRÁFICAS

AGUIAR, Paulo A. F. **Seguranças em redes wi-fi**. 2005. 79 f. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Centro de Ciências Exatas e Tecnológicas, Universidade Estadual de Montes Claros, Montes Claros.

ALBUQUERQUE, Ricardo; RIBEIRO, Bruno. **Segurança no desenvolvimento de software**: como desenvolver sistemas seguros e avaliar a segurança de aplicações desenvolvidas com base na ISO 15.408. Rio de Janeiro: Campus, 2002.

ALECRIM, Emerson. **Entendendo a certificação digital**. São Paulo, 2009. Disponível em: <http://www.infowester.com/assincertdigital.php>. Acesso em: 26 out. 2009.

APACHE. [S.l.], 2011. Disponível em: <http://www.apache.org/>. Acesso em: 10 mar. 2011.

BASTOS, Luiz E. M. **Avaliação do e-learning corporativo no Brasil**. 2003. 264 f. Dissertação (Mestrado Profissional em Administração) – Curso de Pós-Graduação Profissional em Administração, Escola de Administração da Universidade Federal da Bahia, Bahia. Disponível em: <http://www.adm.ufba.br/luis_eduardo2.pdf>. Acesso em: 02 abr. 2010.

BAYÃO JÚNIOR, Cloves. **As novas tecnologias sendo utilizadas pelos cartórios mineiros como ferramentas de aperfeiçoamento e modernização na prestação de serviços**. 2009. 49 f. Monografia (Curso de Especialização em Tecnologia em Recursos Humanos) – Curso de Pós-graduação a distância via-internet, Escola Superior Aberto do Brasil, Vila Velha.

BRASIL. **Decreto-lei n 5.622, de 19 de dezembro de 2005**. Estabelece as diretrizes e bases da educação nacional. Brasília, 2005. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5622.htm>. Acesso em: 01 abr. 2010.

CARVALHO, Juliano Varella de. **Banco de dados.** Novo Hamburgo, 2005. Disponível em: <http://www2.wzero.com.br:81/paulo/feevale/bd/ >. Acesso em: 20 maio. 2011.

CERTISIGN. **A sua identidade na rede**. [S.l.], 2010. Disponível em: <http://www.certisign.com.br/produtos-e-servicos/certificados-digitais/e-cpf>. Acesso em: 20 fev. 2011.

DANEY, Derlis. C. R. **Software de apoio a geração de avaliações de aprendizagem**. 2007. 102 f. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Centro de Ciências Exatas e Naturais, Universidade Regional de Blumenau, Blumenau.

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel, 2000.

DREAMWEAVER. [S.l.], 2011. Disponível em: <http://www.adobe.com/products/dreamweaver.html>. Acesso em: 10 mar. 2011.

FÁVERI, Helena J. de; KRUSCINSCK, Sueli T. de O. A avaliação a serviço da aprendizagem. **Caminhos**, Rio do Sul, n. 3, p. 77-92, 2004.

GALVÃO, Júnior. **Diferenças entre chaves simétrica e assimétrica para criptografia**. São Paulo, 2007. Disponível em: <http://pedrogalvaojunior.wordpress.com/2007/11/16/diferencas-entre-chaves-simetrica-e-assimetrica-para-criptografia>. Acesso em: 30 abr. 2011.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Estrutura da ICP-Brasil**. [S.l.], [2011?]. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/EstruturaIcp>. Acesso em: 20 fev. 2011.

LITTO, Frederic M. **A nova ecologia do conhecimento**: conteúdo aberto, aprendizagem e desenvolvimento. Brasília, 2006. Disponível em: <http://www2.abed.org.br/visualizaDocumento.asp?Documento_ID=193>. Acesso em: 04 abr. 2010.

MAIA, Marta C. **O uso da tecnologia de informação para a educação a distância no ensino superior**. 2003. 294 f. Tese (Doutorado em Administração de Empresas) – Escola de Administração de Empresas de São Paulo, Fundação Getúlio Vargas, São Paulo.

MATHIAS, Derlei. A. **Protótipo de software para emissão de certificados digitais para objetos distribuídos**. 2007. 56 f. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Centro de Ciências Exatas e Naturais, Universidade Regional de Blumenau, Blumenau.

MORAES, Mari P. **A monitoria como serviços de apoio ao aluno na educação à distância**. 2004. 237 f. Tese (Doutorado em Engenharia de Produção) – Centro Tecnológico, Universidade Federal de Santa Catarina, Florianópolis.

MORAN, José M. **O que é educação a distância**. Rio de Janeiro, 2002. Disponível em: <http://www.eca.usp.br/prof/moran/dist.htm>. Acesso em: 28 maio 2010.

MYSQL. [S.l.], 2011. Disponível em: <http://dev.mysql.com/doc/>. Acesso em: 10 mar. 2011.

NETTO, Samuel P. **Telas que ensinam mídia e aprendizagem**: do cinema ao computador. 2. ed. Campinas: Alínea, 1998. 225 p.

OMG. **UML - Unified Modeling Language specification**. Version 2.0. [S.l.], 2005. Disponível em: <http://www.uml.org/>. Acesso em: 12 abr. 2010.

PAULA, Cirilo V. F. F. **Uma abordagem para avaliação da segurança em sistemas de TI**. 2005. 45 f. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Faculdade de Ciências Aplicadas de Minas, União Educacional Minas Gerais, Uberlândia.

PEREIRA, Ana P. S. S. **O que é hash e pra que serve**. [S.l], 2009. Disponível em: <http://www.baixaki.com.br/info/1663-o-que-e-hash-.htm>. Acesso em: 15 maio 2010.

PEREIRA, Alice T. **Cybis ambientes virtuais de aprendizagem em diferentes contextos**. Rio de Janeiro: Ciência Moderna, 2007. 210 p.

PETERS, Otto. **Didática do ensino a distância:** experiências e estágios da discussão numa visão. Tradução Ilson Kayser. São Leopoldo: UNISINOS, 2001. 402 p.

PHP. [S.l.], 2011. Disponível em: <http://php.net/>. Acesso em: 10 mar. 2011.

SANTOS, Luiston. **O que é assinatura digital**. [S.l.], 2009. Disponível em: <http://www.luistonsantos.adv.br/ver-todas-as-noticias/18-noticias-diversas/83-o-que-e-assinatura-digital-.html>. Acesso em: 30 abr. 2011.

SPARXSYSTEMS. Creswick, 2000. Disponível em: <http:// www.sparxsystems.com/>. Acesso em: 15 mar. 2010.

STAA, Betina V. **Avaliação on-line**: qual é a vantagem afinal. [S.l.], 2007. Disponível em: <http://www.icshvalparaiso.edu.br/index.php?option=com_content&task=view&id=38&Itemid=1>. Acesso em: 25 abr. 2008.

TADEU, Luciano S. **Políticas de segurança da informação:** recomendações para redução de riscos e vulnerabilidades humanas. 2006. 73 f. Trabalho de Conclusão de Curso (Bacharelado em Licenciatura em Computação) – Instituto de Ciências Exatas, Universidade de Brasília, Brasília.

TALUA. **O que é e-cpf**. [S.l.], 2010. Disponível em: <http://www.certificado-digital.org/certificado-digital/o-que-e-e-cpf>. Acesso em: 20 fev. 2011.

TERADA, Routo. **Segurança de dados**: criptografia em redes de computador. São Paulo: Edgar Blucher, 2000.

UNIVERSIDADE REGIONAL DE BLUMENAU. **Ambiente virtual de aprendizagem**. Blumenau, 2009. Disponível em: <http://www.furb.br/ava>. Acesso em: 06 abr. 2010.

UNIVERSIDADE REGIONAL DE BLUMENAU. **Diploma**. Blumenau, 2009. Disponível em: < http://www.furb.br/novo/index.php?option=conteudo&Itemid=213 >. Acesso em: 28 junho. 2010.

WANDERLEY, Danillo L. **Políticas de segurança**. 2005. 48 f. Monografia (Especialização em Administração em Rede Linux) – Curso de Pós-graduação em Rede Linux, Universidade Federal de Lavras, Lavras.

YOUNG Eric A.; HUDSON Tim J. **The openssl project**. [S.l.], 1999. Disponível em: <http://www.openssl.org/>. Acesso em: 06 maio 2010.

ZANINI, Michel. **Formulários eletrônicos**. 2007. 78 f. Trabalho de Conclusão de Curso (Bacharelado em Ciências da Computação) – Centro Tecnológico, Universidade Federal de Santa Catarina, Florianópolis.

ANEXO A – Principais comandos utilizados na ferramenta OpenSSL

No Quadro 27, são apresentados os principais comandos utilizados com a ferramenta OpenSSL para, criar a AC TCC, criar o certificado digital do cliente (diretor), assinar o certificado do cliente (diretor) utilizando o certificado da AC TCC, extrair as chaves privada e pública de um certificado exportado do navegador e para converter o certificado digital para outros formatos.

A conversão para diferentes formatos deve ser feita porque o servidor Apache aceita apenas o formato PEM, e para importar um certificado digital (do tipo cliente) para o navegador, ele deve estar no formato P12.

1) Criar a Autoridade Certificadora TCC (certificado auto assinado)

1.1) Criar a chave privada

```
genrsa -des3 –out actcc.key 1024
```

1.2) Criar o arquivo de requisição de assinatura para a AC poder auto-assinar

```
req –new –key actcc.key –out actcc.csr
```

1.3) Auto assinar o certificado utilizando a requisição

```
x509 –req -days 3650 –in actcc.csr –out actcc.crt –signkey actcc.key
```

2) Criar a chave privada e a requisição para o certificado digital do cliente (Diretor)

2.1) Criar a chave privada

```
genrsa –des3 –out diretor.key 1024
```

2.2) Criar o arquivo de requisição de assinatura para a AC poder assinar

```
req –new –key diretor.key –out diretor.csr
```

3) Criar e assinar o certificado do cliente (Diretor) utilizando o certificado da AC (TCC)

```
x509 –req -days 3650 –in actcc.csr –out actcc.crt –signkey actcc.key
```

4) Extrair as chaves pública e privada de um certificado exportado do navegador (PFX)

4.1) Extrair chave pública do formato (PFX) exportado do navegador

```
pkcs12 -in certificado.pfx -out chave_publica.pem -clcerts -nokeys
```

4.2) Extrair chave privada do formato (PFX) exportado do navegador

```
pkcs12 -in certifciado.pfx -out chave_privada.pem -nocerts
```

4.2) Extrair chave privada do formato (PFX) exportado do navegador (sem password)

pkcs12 -in certificado.pfx –out chave_privada.pem -nocerts –nodes

5) Converter o certificado digital para outros formatos

5.1) Do formato CRT ou CER para o formato PEM

5.1.1) Primeiro converte-se para o formato DER

x509 -in diretor.crt -out diretor.der -outform DER

5.1.2) Converter para o formato PEM

x509 -in actcc.der -inform DER -out actcc.pem -outform PEM

5.2) Do formato CRT para o formato P12

pkcs12 –export –clcerts –in diretor.crt –inkey diretor.key –out diretor.p12

Quadro 26 - Principais comandos utilizados na ferramenta OpenSSL

ANEXO B – Configurações do servidor Apache para autenticar via certificado digital

No Quadro 27, são apresentados os principais configurações para que o servidor Apache possa utilizar um certificado digital para autenticação.

Observação: Nos arquivos de configuração do servidor Apache, o carácter # significa início de comentário.

1) No Arquivo <u>httpd.conf</u>

1.1) Descomentar as linhas (eliminando sustenido)

```
#LoadModule ssl_module modules/mod_ssl.so
#Include "conf/extra/httpd-ssl.conf"
```

2) No Arquivo <u>httpd-ssl.conf</u>

```
#Inserir em uma cláusula <IfModule ssl_module>
Listen 443
```

2.2) Denifir dentro do VirtualHost

```
<VirtualHost _default_:443>
   DocumentRoot "D:/xampp/htdocs" #diretório raiz
    #ServerName deve ser o IP e deve possuir o mesmo nome do campo,
   #Common Name (CN) cadastrado no certificado do servidor.
   ServerName 127.0.0.1
SSLEngine on
#Certificado do Servidor (criar com o comando makecert do Apache)
SSLCertificateFile "conf/ssl.crt/server.crt"
#Chave Privada do Servidor
# (gerado ao criar o certificado com o comando makecert)
SSLCertificateKeyFile "conf/ssl.key/server.key"
#Certificado da AC da qual se deseja reconhecer os certificados de Cliente
#(Chave pública que deve estar no formato PEM)
SSLCACertificateFile "conf/ssl.crt/actcc.pem"
```

Quadro 27 – Configuração do servidor Apache para autenticar via certificado digital