**CENTRO UNIVERSITÁRIO DE GOIÁS UNI-ANHANGUERA**

**SISCVC –** **SISTEMA DE Controle DA VALIDADE DO CERTIFICADO DIGITAL**

**MURILO PIGHINI DE SOUSA**

**WINICIUS NOEL OLIVEIRA LEAL**

GOIÂNIA

Dezembro/2020

**MURILO PIGHINI DE SOUSA  
WINICIUS NOEL OLIVEIRA LEAL**

**SISCVC – SISTEMA DE Controle DA VALIDADE DO CERTIFICADO DIGITAL**

Trabalho de Conclusão de Curso apresentado ao Centro Universitário de Goiás Uni-ANHANGUERA, sob orientação do Professor Especialista Francismar de Oliveira, como requisito parcial para obtenção do título de bacharelado em engenharia da computação.

GOIÂNIA

Dezembro/2020

**FOLHA DE APROVAÇÃO**

MURILO PIGHINI DE SOUSA  
WINICIUS NOEL OLIVEIRA LEAL

SISCVC – SISTEMA DE Controle DA VALIDADE DO CERTIFICADO DIGITAL

Trabalho de conclusão de curso apresentado à banca examinadora como requisito parcial para obtenção do Título de Bacharel em Engenharia da Computação do Centro Universitário de Goiás – Uni-Anhanguera, deferido e aprovado em \_\_\_ de \_\_\_ de \_\_\_\_ pela banca examinadora constituída por:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Professor Prof(a). Dr(a). ou Ms. Nome do(a) Orientador(a) Orientador(a)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Professor Prof(a). Dr(a). ou Ms. Nome do(a) Orientador(a) Membro

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Professor Prof(a). Dr(a). ou Ms. Nome do(a) Orientador(a) Membro

**RESUMO**

O uso do termo certificado digital foi criado, quando o governo o adotou no meio como mecanismo de identificação eletrônico, o verdadeiro significado do certificado digital. Agências federais e estaduais, para agilizar processos, digitalizam muitos serviços, com o passar dos dias. Com uma série de processos, é obrigatório o uso do certificado digital. O certificado digital do ICP-Brasil, além de personificar os cidadãos na rede mundial de computadores, garante, por via disso, auxiliar a prática daqueles com seu uso. É uma ferramenta usada para assinar documentos, de maneira criptografada, não como uma mídia virtual. A criptografia é uma maneira de codificar informações para que apenas o remetente e o destinatário possam ser identificados como uma mensagem, sem que outros obtenham acesso às informações. Essa é uma técnica de manipulação de dados em códigos indecifráveis. Com uma grande demanda no uso do certificado digital, surgiu a necessidade de manter a validade do certificado. O problema do controle é a validade, devido à obrigatoriedade mensal e análogos do governo. Portanto, através de um software que realiza o monitoramento e a notificação ao usuário, o controle da certificação ficará por conta do cliente.

**PALAVRAS-CHAVE:** Certificação Digital. Criptografia. Assinatura digital. Software.

**SUMÁRIO**

[1. INTRODUÇÃO 7](#_Toc56617396)

[1.1. Objetivos 9](#_Toc56617397)

[1.1.1. Geral 9](#_Toc56617398)

[1.1.2. Específicos 9](#_Toc56617399)

[1.2. Justificativa 9](#_Toc56617400)

[2. REFERENCIAL TEÓRICO 10](#_Toc56617401)

[2.1. Certificado Digital 10](#_Toc56617402)

[2.2. Banco de Dados 12](#_Toc56617403)

[2.2.1. Modelos de banco de dados 14](#_Toc56617404)

[2.2.1.1. Modelo conceitual 14](#_Toc56617405)

[2.2.1.2. Modelo lógico 14](#_Toc56617406)

[2.2.1.3. Modelo conceitual como modelo de organização 14](#_Toc56617407)

[2.2.2. Níveis de abstração de informações e dados 15](#_Toc56617408)

[2.2.3. Privacidade dos dados 17](#_Toc56617409)

[2.3. MySQL 18](#_Toc56617410)

[2.4. Redes de comunicação e computadores 18](#_Toc56617411)

[2.4.1. Evolução das redes de comunicação e computadores 19](#_Toc56617412)

[2.4.2. Conceito básico de comunicação de dados 20](#_Toc56617413)

[2.4.2.1. Princípios da comunicação 20](#_Toc56617414)

[2.5. Linguagem de programação - JAVA 21](#_Toc56617415)

[2.6. Linguagem de Modelagem Unificada - UML 22](#_Toc56617416)

[2.6.1. Diagrama de classe 22](#_Toc56617417)

[2.6.2. Diagramas de casos de uso 22](#_Toc56617418)

[2.6.3. Diagrama de sequência 23](#_Toc56617419)

[2.7. Criptografia 24](#_Toc56617420)

[2.7.1. Criptografia Simétrica e Assimétrica 25](#_Toc56617421)

[2.7.2. Algoritmos de Criptografia 26](#_Toc56617422)

[2.7.2.1. Algoritmos para criptografia simétrica 26](#_Toc56617423)

[2.7.2.2. Algoritmo para criptografia assimétrica 29](#_Toc56617424)

[2.7.3. Técnicas básicas de cifragem 29](#_Toc56617425)

[2.7.4. Gerenciamento de chaves e certificados digitais 31](#_Toc56617426)

[2.7.5. Aplicações da criptografia em comunicação digital 33](#_Toc56617427)

[2.7.6. Assinatura digital 34](#_Toc56617428)

[2.7.7. Autenticidade de usuários 35](#_Toc56617429)

[2.7.8. Segurança de mensagens eletrônicas 35](#_Toc56617430)

[3. PROJETO 36](#_Toc56617431)

[3.1. Conceitos iniciais 36](#_Toc56617432)

[3.2. Algoritmo de criptografia utilizado 37](#_Toc56617433)

[3.2.1. Criptografando a senha 38](#_Toc56617434)

[3.2.2. Descriptografando a senha 42](#_Toc56617435)

[3.3. Diagramas utilizados 44](#_Toc56617436)

[3.3.1. Diagrama de casos de uso 44](#_Toc56617437)

[3.3.1.1. Descrições textuais dos casos de uso 45](#_Toc56617438)

[3.3.2. Diagrama de classe 61](#_Toc56617439)

[3.3.3. Diagrama de sequência 63](#_Toc56617440)

[3.3.3.1. Diagrama de sequência – Login com usuário e senha 63](#_Toc56617441)

[3.3.3.2. Diagrama de sequência – Login com certificado 64](#_Toc56617442)

[3.3.3.3. Diagrama de sequência – Cadastro de usuário 66](#_Toc56617443)

[3.3.3.4. Diagrama de sequência – Consultar, alterar e excluir usuário 68](#_Toc56617444)

[3.3.3.5. Diagrama de sequência – Cadastro do certificado do usuário 70](#_Toc56617445)

[3.3.3.6. Diagrama de sequência – Cadastro de cliente 72](#_Toc56617446)

[3.3.3.7. Diagrama de sequência – Consultar, alterar e excluir cliente 74](#_Toc56617447)

[3.3.3.8. Diagrama de sequência – Cadastro de certificado para o cliente 76](#_Toc56617448)

[3.3.3.9. Diagrama de sequência – Monitoramento do prazo de validade 78](#_Toc56617449)

[4. CONCLUSÃO 80](#_Toc56617450)

[REFERÊNCIAS BIBLIOGRÁFICAS 82](#_Toc56617451)

1. INTRODUÇÃO

Neste trabalho abordaremos a utilização do certificado digital junto a sua criptografia, verificando sua importância cotidiana, segurança e desempenho. Posteriormente, através da implementação de um software na linguagem Java, vincularemos esse software com o certificado digital, fazendo com que, o usuário tenha total controle dos dados de forma prática e eficiente.

Visando a segurança dos dados, aplicamos os conceitos de criptografia simétrica, para criptografar alguns dados dos usuários ao inserir no banco de dados, com isso dificultando que indivíduos não autorizados tenha acesso as informações confidenciais tais como senha.

O certificado digital é a identidade de uma pessoa ou instituição, que pode ser armazenado em um computador como um arquivo de modelo A1, ou em mídias como Token ou Smartcard, de modelo A3. Exemplos semelhantes a um certificado digital são: RG, CPF e Carteira de Habilitação (CNH). Cada um desses documentos contém um conjunto de informações como nome, número de identificação, estado, etc. Nos certificados são encontrados ainda o nome da Autoridade Certificadora (AC) regulamentada pela ICP Brasil, o número de série, período de validade e assinatura digital da AC (garantindo para outra entidade a veracidade da informação contida) (LIMA, 2006, p.38).

Da mesma maneira que trouxe segurança, o certificado transformou a maneira tradicional de fazer negócios, trouxe a possibilidade de mudar os processos burocráticos, facilitando a vida do usuário e eliminando o uso de grande volume de documentos impressos. O certificado digital está sendo esse grande instrumento dessa mudança (HUANG; SIAU; WEI, 2005, p.89).

A certificação digital facilitou a vida das empresas, que hoje utilizam a internet para realizar diversas tarefas de maneira rápida e segura, do preenchimento de guias para pagamentos de tributos ao acesso a diversos serviços do governo, como o acompanhamento fiscal de pessoas físicas e jurídicas na Receita federal.

Com a mesma proporção, houve a necessidade das contabilidades controlarem a validade dos certificados digitais de seus clientes. Com isso, pensamos em um sistema que monitorará a validade dos certificados cadastrados. A principal função do sistema é notificar os usuários e clientes por e-mail, pois após o vencimento, os certificados não possuem nenhuma outra utilidade, impossibilitando realizar acessos, assinaturas de documentos, como também realizar transações em órgãos estaduais e/ou federais, podendo gerar consequências jurídicas, tais como multas para os seus clientes.

O certificado digital é bastante utilizado para realizar assinaturas de documentos evitando a impressão dos mesmos, acesso a portais e sites que exigem uma segurança maior na identificação do usuário, deixando de utilizar o acesso por login e senha.

Demonstraremos também alguns conceitos de banco de dados, linguagem Java, mostrando sua importância e explorando sua utilização. Enfim, explicando ao público-alvo, o objetivo e necessidade do software.

* 1. Objetivos

Os objetivos do presente trabalho são apresentados a seguir:

* + 1. Geral

Relatar a necessidade de um software de monitoramento da validade dos certificados digitais, evitando com que as contabilidades não enfrentem futuros problemas com seus clientes, devido à obrigatoriedade do uso do certificado digital em determinados portais, que são supervisionados pelos governos frente ao paradigma de que é um mecanismo para facilitar o cotidiano do usuário.

Relatar a necessidade da segurança dos dados inseridos no banco de dados, evitando que indivíduos sem autorização, tenham acessos a essa lista de clientes e informações dos certificados digitais cadastrados.

* + 1. Específicos

Observar e avaliar a utilização do software, que realizará o monitoramento da validade dos certificados digitais, apresentando também os benefícios na utilização e assegurar que esses dados inseridos estarão seguros.

* 1. Justificativa

Nos dias atuais, as contabilidades enfrentam dificuldades para controlar o prazo de validade dos certificados digitais de seus clientes. Logo, a necessidade de criar uma solução para realizar esse controle. Com isso, desenvolvemos um software que realiza esse monitoramento de acordo com os certificados cadastrados pelos usuários. Assim, as contabilidades previnem que seus clientes tenham futuros problemas, tais como notificações e multas, devido a obrigatoriedades estabelecidas por esses órgãos. Com a inserção de vários dados de clientes, precisamos garantir que essas informações estejam seguras.

1. REFERENCIAL TEÓRICO
   1. Certificado Digital

Segundo o Instituto Nacional de Tecnologia da informação (ITI), o certificado digital da ICP – Brasil, além de personificar o cidadão na rede mundial de computadores, garante, por força da legislação atual, validade jurídica aos atos praticados com seu uso.

A identificação digital de uma pessoa física ou jurídica é estabelecida por meio do certificado digital, foi criado por meio da medida provisória 2.200-2 em agosto de 2001 visando garantir a equidade de documentos e transações feitas pela web, ou mensagem, além de permitir que seja feitas assinaturas digitalmente de documentos, mensagens realizadas on-line com confidencia, integridade e validade jurídica.

O certificado é requisitado por uma pessoa física, empresas e instituições são utilizadas para minimização de tempo e custo, uma transação, por exemplo, de assinatura de documentos que poderiam ser feitas em dias, com a utilização da ferramenta é feita por meio eletrônico em segundos, visando promover a segurança das transações e envio de mensagens no ambiente da Internet.

Documentos eletrônicos que antes eram vistos com falta de prestígio pela população, hoje ganha confiabilidade pelo uso da assinatura digital. Surgiu para o meio jurídico a necessidade de regulamentar esse novo modelo documental. Adaptar-se à nova realidade eletrônica aos conceitos legais clássicos de documento e assinatura culminou no desenvolvimento legal de normas com a finalidade de situar o tema no arcabouço jurídico brasileiro (GUELFI, 2007, p.52).

Para que a tecnologia seja válida é necessário que o usuário adquira um documento eletrônico e a chave pública do destinatário. Utilizando programas computacionais o documento é criptografado de acordo com a chave pública e somente pode ser utilizado pelo receptor que, para isso, deverá uma chave privada exclusivamente dele. Se qualquer bit for modificado, o documento perde sua validade jurídica.

Um fator importante a se ter em mente, é que um documento, seja eletrônico ou não, tem que apresentar as condições para ter validade jurídica.

“Seu funcionamento pode ser comparado a de um serviço notarial efetuado pelo tabelião. Fundamenta-se na existência de uma autoridade certificadora [responsável pela emissão do certificado digital] que possui registrado, em sua base de informações, a chave pública [usada para decifrar a mensagem – criptoanálise do emissor do documento]. Através de mecanismos próprios, a autoridade certificadora pode identificar como original o documento do emissor e, a partir desta comprovação, certificar, com uma assinatura digital própria, a autenticidade do documento eletrônico.” (VOLPI; MARLON, p.36).

O certificado digital seria o similar a um RG eletrônico, enquanto a assinatura digital, o equivalente ao carimbo acompanhado de selo que os cartórios brasileiros colocam para reconhecer firma em documentos. Juntos, esses dois elementos, aliados à criptografia, garantem a autenticidade, a integridade, o não repúdio à transação e a confidencialidade da informação.

De acordo com o ICP – Brasil, o modelo A1 é um arquivo armazenado diretamente na máquina, podendo-se realizar cópias, mandar por e-mail, possível ser utilizado simultaneamente em duas máquinas. Entretanto o modelo A3 o certificado é armazenado em dispositivos criptográficos. Em vista de segurança, o A3 é mais seguro, pois só pode ser utilizado com dispositivo conectada a máquina, e não tem como fazer cópias do mesmo, o certificado é único e intransferível. O modelo A3 é bastante utilizado por advogados, pois portais de uso dos mesmos somente é reconhecido o modelo A3.

Os documentos convencionais como RG e CPF são solicitados apenas uma única vez, sem ter a necessidade de renovar por um período de validade, exceto em casos documentos danificados, perda ou roubo. Em contrapartida o certificado digital possui prazos de validades, que pode variar de acordo com o modelo adquirido e solicitado pelo titular. Contudo o usuário poderá adquirir um novo certificado, com uma nova validade de acordo com a sua necessidade.

E importante que os titulares tenham um grande cuidado com a utilização do certificado digital, tendo em vista a segurança dos seus registros pessoais, evitando com que indivíduos não autorizados o utilizem. Segundo o Instituto Nacional de Tecnologia da Informação (ITI) é necessário seguir algumas recomendações para o uso de um certificado digital, que são:

I. A senha de acesso da chave privada e a própria chave privada não devem ser compartilhadas com ninguém;

II. Caso o computador onde foi gerado o par de chaves criptográficas seja compartilhado com diversos usuários, não é recomendável o armazenamento da chave privada no disco rígido, pois todos os usuários terão acesso a ela, sendo melhor o armazenamento em disco removível;

III. Caso a chave privada esteja armazenada no disco rígido de algum computador, deve-se protegê-lo de acesso não autorizado, mantendo-o fisicamente seguro. Nunca deixe a sala aberta quando sair e for a necessário deixar o computador ligado. Utilize também um protetor de tela com senha. Cuidado com os vírus de computador, eles podem danificar sua chave privada;

IV. Caso o software de geração do par de chaves permite optar entre ter ou não uma senha para proteger a chave privada, recomenda-se a escolha pelo acesso por meio de senha. Não usar uma senha significativa que qualquer pessoa que tiver acesso ao computador poderá se passar pelo titular da chave privada, assinando contratos e movimentando contas bancárias. Em geral e bem mais fácil usar uma senha do que proteger um computador fisicamente;

V. Utilize uma senha longa, intercalando letras e números, uma vez que existem programas com a função de desvendar senhas. Deve-se evitar o uso de dados pessoais como nome de cônjuge ou de filhos data de aniversários, endereço, telefone, ou outros elementos relacionados com a própria pessoa. A senha nunca deve ser anotada, sendo recomendável sua memorização.

* 1. Banco de Dados

Heuser (2009) declara que com o passar do tempo muitas empresas estão procurando automatizar todas as suas áreas, inicialmente isso ocorre somente nas principais, mas com o avanço da informática vão sendo estudadas as possibilidades de que a automatização se espalhe para todas as áreas.

Abreu e Machado (2009) afirmam que para que ocorra a informatização em qualquer área, precisamos conhecer a fundo como funcionam todos os seus processos. Como por exemplo, uma empresa que tem vários departamentos como: vendas, produção e compras. Em vendas temos atividades como: cotação de preços, informação para clientes e informações de disponibilidade de produtos. Já em produção temos: atividades da empresa, planejamento da produção e controle do que foi produzido. Em compras temos atividades como: aquisição de insumos, cotação de preços junto a fornecedores, compras e acompanhamento do fornecimento.

No exemplo acima citados por Abreu e Machado (2009) podemos ver que para cada área precisamos conhecer cada função, pois uma função pode depender da outra para que seja executada de maneira correta e em alguns casos elas precisam se comunicar. Informatizar cada função de forma separada não é uma boa escolha e poderiam ocorrer problemas futuramente como a redundância de dados.

Existem dois tipos de redundância de dados, a redundância controlada e a não controlada. A redundância controlada acontece quando o software tem conhecimento da múltipla representação da informação e pode sincronizar diversas representações. A redundância não controlada ocorre geralmente quando a sincronia de dados fica na responsabilidade dos usuários e não com o software. Um dos problemas que podemos detectar conforme Abreu e Machado (2009) é a entrada repetida de dados, que exige trabalho desnecessário e transposição de dados

A melhor maneira para evitar a redundância é fazer com que os dados sejam compartilhados e que as informações possam ser acessadas por todo o sistema, assim só será necessário inserir as informações uma única vez.

Para facilitar a organização dos sistemas e dos dados usamos o SGBD, pois a cada passo o sistema vai se tornando mais complexo e com isso precisamos de ferramentas para organizá-los

A programação e o modo como é feito, sofre várias mudanças ao longo tempo, tais mudanças que facilitam muito a vida do usuário e do programador. No início os programadores agrupavam em um programa toda funcionalidade almejada. O programa continha as operações da interface do usuário, as transformações de dados, cálculos, as operações de armazenamento de dados, bem como tarefas de comunicações com outros sistemas e programas (AUTOR DESCONHECIDO).

Com o tempo Heuser (2009) notou-se que havia várias funcionalidades em comum e poderia ser feita uma modularização de programas, que funciona do seguinte modo:

Sistema de gerenciamento de banco de dados (SGBD) é o mesmo que um Software que incorpora as funções de definição, recuperação e alteração de dados em banco.

Essa modularização trouxe várias vantagens, pois os programas tornaram-se mais simples e os programas ficaram menores, pois usam funções já construídas.

* + 1. Modelos de banco de dados

Na construção de um modelo de banco de dados usa uma linguagem de banco de dados, que podem ser definidas de acordo com o que foi apresentado em linguagens textuais ou linguagens gráficas. Todas as linguagens recebem uma designação esquema de banco de dados de acordo com o seu nível de abstração (HEUSER, 2009, p.24).

* + - 1. Modelo conceitual

De acordo com Heuser (2009) o modelo conceitual é o modelo de dados abstrato, que descreve a estrutura de um banco de dados de forma independente de um SGBD, mas não demostra como estes dados estão armazenados.

A técnica de modelagem conceitual mais difundida é a abordagem entidade relacional (ER). E é representada através de um diagrama, chamado de diagrama entidade relacional (DER).

* + - 1. Modelo lógico

O modelo lógico descreve a estrutura do banco de dados, vista pelo usuário do SGBD.

Heuser (2009) afirma que esse detalhe não influencia a programação no SGBD, mas pode afetar o desempenho das aplicações que não fazem parte do modelo lógico.

* + - 1. Modelo conceitual como modelo de organização

De acordo com Abreu e Machado (2009) o modelo usual pode ser interpretado de duas formas, como modelo abstrato da organização, que decide as entidades da organização que têm guardadas no banco de dados. Como modelo abstrato de banco de dados, que decide que arquivos farão parte do banco de dados.

Os autores ressaltam que na prática convêm que modelos conceituais sejam modelos que descrevem as organizações, por isso são mais simples de compreender por usuários leigos em informática do que modelos que envolvem detalhes de implementação.

* + 1. Níveis de abstração de informações e dados

Conforme Setzer (1989) os dados vem sendo abstraídos do universo de forma cada vez mais clara e objetiva, assim podendo ser expressos matematicamente. Esses dados que inserimos no computador são tratados por espécie de fórmulas, representados pelos programas que são executados diretamente ou indiretamente pelo computador.

O mesmo ainda afirma que a base de dados é formada pela abstração de dados. Sendo assim, tendo vários níveis de abstração. O mais alto é do mundo real, considerando que os objetos são os seres, os fatos, organismos sociais e as coisas.

Já o segundo nível é caracterizado por relatórios escritos em uma linguagem natural, que é caracterizada por informações informais, podendo ser considerado de nível descritivo. A abstração para esse nível constitui um modelo da realidade, exigindo que a descrição de um universo seja de fácil entendimento e melhor organizado para o usuário que interagirá com as informações abstraídas do universo tornando fácil e prático.

O terceiro nível está relacionado as informações formais consideradas como modelos conceituais, onde o objetivo é chegar no nível posterior a um modelo computacional, ou seja, sendo possível ser processado e fornecido por um computador. Nesse modelo temos dois aspectos distintos, o primeiro é estruturas de informações, exemplo em uma empresa os dados pessoais de um funcionário, consideramos a estrutura de informações. O segundo aspecto é a parte de atualização, eliminação, leitura e processamento desses dados caso seja necessário. Esse aspecto é chamado de manipulação de informações, nesse terceiro nível podemos utilizar uma linguagem de definição das estruturas de informações (LDEI), essa linguagem é utilizada para definir as manipulações na base de dados.

O quarto nível pode ser considerado como modelos operacionais sendo os símbolos a serem inseridos de forma clara pois o computador precisa tratar esses símbolos, através de um algoritmo com fórmula matemática complexa de cálculo pois não pode ser informada diretamente da linguagem de programação para o computador.

O quinto nível é direcionado ao computador e não ao usuário final, ou seja, qual linguagem utilizada como os dados são estruturados e manipulados esse nível e chamado de modelos internos.

Para Setzer (1989) os níveis de abstração são importantes para saber o tipo de informação que está sendo inserido na base dados e também sobre a estruturação do computador para suportar esses dados e manipular com consistência ficando de forma clara e inteligível tanto para o usuário final quanto para o operando.

De acordo com Elmasri e Navathe (2011) os sistemas de computação estão sendo produzidos em um nível cada vez mais alto no ponto de vista do usuário final, ou seja, fazendo que o usuário não precise conhecer muito os detalhes de computação para especificar seus problemas e seus dados, podendo usar a comunicação com a máquina exclusivamente aos termos que emprega profissionalmente na área administrativa a exigir do usuário apenas o aprendizado, existem tentativas de se fornecer aos usuários sistemas em que ele emprega a linguagem do nível descritivo, que é a linguagem natural com grandes limitações no reconhecimento das especificações dadas pelo usuário, o problema de ser usar diretamente o nível conceitual ou descritivo é que o nível operacional pode dar enumeras especificações de eficiência necessitando para isso conhecimento de linguagem de programação.

Segundo Setzer (1989) os modelos de nível operacional é tradicionalmente divido em modelo relacional, modelo de redes e modelo hierárquico, o modelo relacional está divido em dois tipos o normalizado e o não normalizado, sendo assim a maioria dos bancos de dados comerciais sendo normalizado já o segundo está presente em pesquisa.

Segundo o autor será abordado dois tipos de métodos para derivar os níveis de abstração sendo eles o descendente e o ascendente, o último será descrito como um método de síntese de relações normalizadas do modelo operacional relacional. O método descendente é aquele que aborda os níveis de abstração “de cima para baixo”, é feito um modelo descritivo a partir e informações e vivências do mundo real, a partir dessas informações adquiridas do modelo descritivo é deriva-se o modelo conceitual, e deste um modelo operacional que é inserido no banco de dados através da máquina.

Conforme Abreu e Machado (2009) o modelo conceitual pode ser derivado a partir de uma análise gramatical de sentenças essa derivação é mais informal do que formal, já a derivação de um modelo conceitual pode ser feito praticamente todo de maneira formal. Não pode haver um mapeamento total de um modelo no outro, pois, existem elementos que pertencem a cada um dos níveis e que não ocorrem no outro, por exemplo, se especificar um modelo operacional um item de busca, ou seja, nas consultas na base de dados, no caso de um funcionário de uma empresa de grande porte que precisa realizar consultas com frequência na base, os dados como, por exemplo, salário e data de contratação, devem ser estruturados de maneira especial para que a busca seja realizado com eficiência a partir deles, mas essas especificações não podem existir no modelo conceitual, pois o fato das especificações refletirem o melhor possível no mundo real não importando o aspecto computacional, o deixando exclusivamente para o nível operacional.

* + 1. Privacidade dos dados

A privacidade e a preservação dos dados têm sido alvos de estudos há algum tempo pelos responsáveis pelo SGBDs. Com isso, especialistas em segurança tem como objetivo reduzir os riscos de quebra de privacidade constantemente (GALVÃO, 2015, p.70).

Atualmente, algumas estratégias são utilizadas para que a privacidade de indivíduos cadastrados não seja violada de forma alguma. Como por exemplo, armazenar os dados já criptografados.

De acordo com Galvão (2015), criptografando algum desses dados conseguimos diminuir o risco de acesso a sujeitos não autorizados e que esse indivíduo mal-intencionado não consiga descobrir por meio de dedução, a identidade de uma pessoa.

* 1. MySQL

O Structured Query Language (SQL) é uma linguagem estruturada para manipulação de dados. É padronizada para os bancos de dados relacionais, mas cada gerenciador pode possuir uma extensão própria dessa linguagem (SQL Server, 2000). O *Mysql* é atualmente um dos bancos de dados mais populares, com mais de 10 milhões de instalações pelo mundo, devido a sua confiabilidade e compatibilidade com os sistemas operacionais existentes. É importante ressaltar que o *MySql* tem um alto poder de execução e armazenamento.

De acordo com Maxfield (2002) o SQL é um padrão de comunicação com o banco de dados de qualquer tipo, não importando os métodos de escrever e ler dados. O mesmo ressalta que *MySql* é um software de banco de dados que suporta linguagem de consulta de banco de dados chamado de SQL.

* 1. Redes de comunicação e computadores

De acordo com Dantas (2002) as redes de comunicação são um conjunto de dispositivos, enlaces de comunicação e pacotes de software que permitem que pessoas e equipamentos possam trocar informações. Quando nos referimos as redes de comunicação, a primeira coisa a se pensar é em uma rede telefônica.

As redes de telefonia foram nos seus primórdios projetadas exclusivamente para serem responsáveis pela transmissão da voz. Porém, isso não é mais uma realidade.

De uma forma mais abrangente do que as antigas redes de telefonia, Dantas (2002) afirma que as redes de comunicação são a resposta para a troca de qualquer tipo de informação nos dias atuais. Por tanto, as redes de comunicação são as espinhas dorsais que suportam a cada dia, as transformações tecnológicas as quais que permite que não somente a voz seja a única informação a ser transportada na rede. Modernas redes de comunicação são desenvolvidas para o transporte de uma variedade de formas de informação, entre dois pontos quaisquer no ambiente da rede. Exemplos de vários tipos de informações são os e-mails, arquivos de textos, vídeos, imagens, sons, gráficos, figuras e voz.

Devido a equipamentos ligados às redes e o tipo diferente de informação transmitida, somos levados a crer que as redes de comunicação e as redes de computadores têm características díspares. Entretanto, este raciocínio é um engano. Pois os princípios que orientam a transmissão da informação de forma geral, são similares nos dois ambientes de rede (DANTAS, 2002, p.3).

* + 1. Evolução das redes de comunicação e computadores

Para Dantas (2002) a evolução das redes de comunicação foi iniciada com certeza, há mais de 170 anos com o desenvolvimento do telégrafo por Morse, em 1830. Seguindo-se ao advento do desenvolvimento do telégrafo, temos em 1876 Graham Bell efetuando a primeira ligação de usuários, através de um sistema de linhas telefônicas ponto a ponto.

No século XX, na década de 70, verificamos nos ambientes de redes de comunicação a utilização de estações de comutação computadorizadas.

Porém nas redes de computadores, os primeiros equipamentos que conhecemos começaram a ser desenvolvidos entre 1930 e 1940. Nos Estados Unidos, Eckert e Mauchly nos anos 40 durante a II Grande Guerra, desenvolveram o ENIAC. Este, sob a responsabilidade da empresa Remington, torna-se o primeiro computador vendido comercialmente, o Univac.

Na Europa, vários projetos de desenvolvimentos de computadores são relatados. Na Alemanha, nos anos 30, Konrad Zuse desenvolve uma máquina muito parecida com um computador. Na Inglaterra, observamos o desenvolvimento do Projeto Colossus e do EDSAC pelo professor Wilkes, de Cambridge (DANTAS, 2002, p.4).

Conforme Dantas (2002) a técnica de interligar os comutadores e recursos localizados geograficamente dispersos era denominada de teleprocessamento. Isso se tornou um fator comum para todos os fabricantes de computadores, que entenderam muito rapidamente que as redes de computadores eram o caminho a ser trilhado para a obtenção de um valor computacional maior.

* + 1. Conceito básico de comunicação de dados
       1. Princípios da comunicação

O modelo genérico de comunicação é composto por uma fonte geradora de informação, um transmissor de sinal, uma rede de comunicação, um receptor de sinal e um destinatário, para o qual se deseja enviar a informação.

Para Dantas (2002) uma fonte é caracterizada pela geração da informação gerada e na fonte pode ser a voz de uma pessoa ou sinal binário e um computador, entre outros. A Informação gerada na fonte deve ser tratada antes de se utilizar a rede de comunicação. A mesma deve se adequar ao meio de comunicação para que possa ser transmitida.

Segundo Dantas (2002) é bastante comum ouvirmos a afirmação de que a voz de uma determinada pessoa é diferente ao telefone. A explicação mais simples para este fenômeno é que a voz foi tratada e então colocada no sistema.

Os sistemas de comunicação são projetados considerando-se determinados parâmetros de custo e desempenho, estes não poderão abrigar todas as frequências das vozes de todas as pessoas. Um limite de sinal é estabelecido e desta forma a voz da pessoa será representada de modo apropriado para ser transportada.

Nas palavras de Dantas (2002) o transmissor é o modelo responsável por converter a informação gerada na fonte para uma forma de sinal. O sinal é a entidade que é transmitida num sistema de comunicação. Exemplos de transmissores clássicos são os aparelhos telefônicos, modens, codecs e transmissores digitais. É nos transmissores que ocorre a modulação ou codificação da informação para que a mesma seja transformada em sinal apropriado para trafegar na rede de comunicação.

Conforme o autor, as técnicas mencionadas serão responsáveis pelo trabalho de conversão da informação orientada pelo tipo de sinal que a rede de comunicação deverá transportar, ou seja, o sinal analógico ou digital.

A rede de comunicação é a porção na qual o sinal vai trafegar para chegar ao receptor remoto e só então ao destino solicitado. A rede de comunicação pode ser uma rede pública ou privada de telefonia, uma rede pública ou privada de pacotes/quadros/células, uma rede metropolitana, uma rede geograficamente distribuída ou simplesmente, uma rede local (DANTAS, 2002, p.9).

O elemento receptor é o dispositivo que recebe o sinal da rede de comunicação e faz o tratamento necessário para que o mesmo seja recebido pelo destinatário como informação. O processo de conversão do sinal em informação ou tratamento do sinal como denominamos, é dependente do tipo de sinal que é utilizado na rede de comunicação.

De acordo com Dantas (2002) o processo de tratamento do sinal poderá ser um processo de demodulação ou um processo de decodificação do sinal. O último dos componentes do nosso modelo genérico de comunicação é o destinatário que é o elemento para o qual a informação da fonte foi endereçada.

Assim, após a informação ter sido originada na fonte, transformada em um sinal pelo transmissor, ter trafego pela rede de comunicação como um sinal, ter sido transformada pelo receptor, é então recebida pelo destinatário.

* 1. Linguagem de programação - JAVA

A linguagem Java é uma das mais utilizadas nos dias atuais para desenvolver softwares de sistemas, no mundo todo (FELIX, 2016, p.69).

Devido a utilização da linguagem orientada a objetos, o Java tem ser tornado mais produtivo aos desenvolvedores, já que os objetos são mais fácil de ser entendidos, corrigidos e alterados.

Uma das suas características a se observar é a capacidade de integração com outas linguagens de programação e com a grande maioria dos sistemas de gerenciamento de banco de dados.

A *Application Programming Inferface* (API) é composta por amplo conjunto de classes já implementadas e testadas que fornecem variados recursos aos desenvolvedores (ASCENCIO; CAMPOS, 2012, p.11).

* 1. Linguagem de Modelagem Unificada - UML

A *UML* (Unified Modeling Language) é uma linguagem visual utilizada para modelar softwares baseados no paradigma de orientação a objetos.

Guedes (2009) afirma que UML não é uma linguagem de programação, e sim uma linguagem de modelagem, uma notação, cujo objetivo é auxiliar os engenheiros de software a definirem as características do sistema, tais como seus requisitos, seu comportamento, sua estrutura lógica, a dinâmica de seus processos e até mesmo suas necessidades físicas em relação ao equipamento sobre o qual o sistema deverá ser implantado.

Pender (2004) ressalta que o principal objetivo da *UML* é representar qualquer tipo de sistema ou software, em termos de diagramas orientados a objeto. Vale ainda ressaltar que a *UML* facilita a comunicação de todas as pessoas envolvidas no processo de desenvolvimento de um sistema - gerentes, coordenadores, analistas, desenvolvedores - por apresentar um vocabulário de fácil entendimento.

* + 1. Diagrama de classe

Segundo Pender (2004) o diagrama de classe é núcleo do processo de modelagem de objetos. Serve para modelar as definições de recursos essenciais à operação correta do sistema. Ele é a origem para geração e também de conversão do código para o modelo. O diagrama de classes provavelmente é o diagrama mais utilizado da UML.

Booch, Rumbaugh e Jacobson (2005) afirmam que o seu principal objetivo é definir a base para que os outros diagramas apresentem outras visões do sistema. Ele descreve a visão estática do sistema em termos de classes e relacionamentos entre as classes.

Com certeza este diagrama é o mais importante em uma documentação de software, onde podemos encontrar as informações sobre métodos, atributos, nome das funções e como serão integradas

* + 1. Diagramas de casos de uso

O diagrama de casos de uso é um diagrama mais geral e informal da UML, utilizado na maioria das vezes nas fases de levantamento e análise de requisitos do sistema. Este diagrama é consultado durante todo o processo de modelagem e também utilizado como base para outros diagramas.

Com isso, os usuários conseguem ter uma fácil compreensão e ideia geral de como o sistema irá se comportar (GUEDES, 2009, p.31).

Quando um diagrama de casos de uso é especificado, seu projetista deve ter em mente as seguintes recomendações (BOOCH; RUMBAUGH; JACOBSON, 2005, p.199):

- O diagrama deve estar focado em um aspecto do sistema, sendo que esse aspecto pode ser o próprio escopo do sistema (diagrama de mais alto nível);

- O diagrama deve apresentar apenas os agentes e os casos de uso que são essenciais ao entendimento desse aspecto;

- O diagrama ser consistente com seu nível de abstração;

- O diagrama não deve apresentar especificação excessiva e muito menos deixar de especificar procedimentos importantes para seu nível de abstração;

- O diagrama deve ter um nome para que possa ser referenciado;

- O diagrama deve dispor seus elementos de tal forma que aqueles que forem semanticamente relacionados estejam próximos entre si;

- O projetista deve pesar o número de elementos no diagrama e verificar se não é conveniente construir um novo diagrama para aumentar a compreensão do modelo;

- O projetista deve procurar minimizar o cruzamento de linhas.

* + 1. Diagrama de sequência

O diagrama de sequência tem como foco a identificação de interações entre os objetos com o tempo. Em geral, baseia-se em um diagrama de caso de uso e apoia-se no diagrama de classes para determinar os objetos evolvidos no processo (GUEDES, 2009, p.35).

Pender (2004) afirma que no diagrama de sequência a troca de mensagem exige um transmissor e um receptor, um receptor precisa ter uma interface para poder receber uma mensagem. Logo, se uma mensagem precisar ser enviada de um objeto para outro, o receptor terá de definir uma interface em conformidade com a mensagem.

Segundo Brooch, Rumbaugh, Jacobson (2005) “o objetivo do diagrama de sequência é apresentar as interações entre objetos na ordem temporal em que elas acontecem”. O diagrama de sequência é um diagrama de interação que dá ênfase à ordenação temporal das mensagens. Um diagrama de sequência mostra um conjunto de papéis.

* 1. **Criptografia**

A criptografia vem do grego e significa escrita (graphos) secreta (crypto), sendo importante em segurança de redes, pois é responsável por promover confidencialidade, autenticidade e integridade das informações, baseado em conhecimentos de matemática, registra uma informação utilizando uma série de regras de tal forma que, sem o conhecimento dessas, é impossível de compreender a informação, correspondendo às etapas de encriptar e decriptar (CARISSIMI, ROCHOL e GRANVILLE, 2009, p.346).

O processo de encriptar e decriptar funciona conceituando a criptografia simétrica e assimétrica, confrontando suas ideias, com intuito de mostrar como uma comunicação entre remetente e destinatário pode ser mais segura e confiável utilizando esse recurso.

Para ser realizado a encriptação, é necessário transformar a mensagem original, aplicando-se um conjunto de regras em um texto codificado ou cifrado, correspondendo a etapa de encriptação. Com isso, a mensagem cifrada é enviada para o destino desejado por meio não confiável, o destinatário realiza o processo de decriptação do texto cifrado para obter a mensagem original. Caso a mensagem cifrada chegue em destinatários não autorizados, as informações não serão acessadas ou alteradas, se eles não possuírem as regras utilizadas na transformação.

Para Carissimi, Rochol e Granville (2009) a confidencialidade na criptografia pode ser composta por três elementos básicos, são eles: método de encriptar, decriptar e chave. Os métodos de encriptar e decriptar são denominados de algoritmo de cifragem e decifração. O primeiro recebe uma chave como entrada e a informação clara a ser cifrada e fornece o texto cifrado como saída, o segundo recebe a chave de decifração e a informação cifrada e obtém a informação original. Se tratando de métodos de criptografia podemos classificar em duas categorias a função da chave de cifragem, chave simétrica e assimétrica.

* + 1. Criptografia Simétrica e Assimétrica

Carissimi, Rochol e Granville (2009) afirmam que a criptografia simétrica utiliza uma única chave para realizar o procedimento de cifragem e decifração, onde elas são idênticas. Sendo assim o remetente e o destinatário devem possuir a mesma chave. Devido a essa característica esse método é conhecido como criptografia de chave secreta. A chave simétrica possui uma vantagem que é sua complexidade computacional. Isso faz com que as operações de cifragem e decifração sejam reduzidas.

Os autores complementam que existem duas desvantagens, uma delas é que o remetente e o destinatário devem ter conhecimento sobre a chave secreta, pois a mesma que cifra é utilizada para decifrar. Assim, temos um problema, como divulgar o valor da chave sem comprometer o sigilo. A segunda desvantagem ocorre quando a chave é compartilhada para vários pares de usuários, podendo assim não garantir o segredo.

A criptografia assimétrica utiliza para cifragem e decifração duas chaves distintas, sendo uma chave pública e a outra chave privada. Uma chave é utilizada para cifrar e a outra para decifrar. Utilizando a criptografia de chave assimétrica, o mesmo par de chaves ao trocar informações cifradas pela chave pública só conseguirá decifrar utilizando a chave privada. Da mesma forma é realizado o procedimento inverso (CARISSIMI, ROCHOL e GRANVILLE, 2009, p.348).

Na criptografia assimétrica, cada parte envolvida na troca de informação deve possuir seu próprio par de chaves (Kpub, Kpriv), onde a chave pública é distribuída e divulgada. Porém, a chave privada é de conhecimento apenas do proprietário; no entanto, a criptografia assimétrica apresenta duas vantagens e desvantagem em relação a criptografia de chaves simétrica.

A primeira vantagem da chave assimétrica em relação a chave simétrica é na distribuição da chave, que é reduzida para n partes se comunicarem. Outra vantagem é em relação a divulgação e conhecimento da chave pública entre as partes envolvidas. Uma desvantagem da criptografia de chaves públicas é porque as duas chaves são relacionadas matematicamente de forma que a informação cifrada por uma é apenas decifrada pela outra. Outro ponto é o custo computacional que leva a uma complexidade no algoritmo para realizar a cifração e decifração. Desta forma é inviável evitar a criptografia assimétrica.

Outra desvantagem da criptografia assimétrica é de garantir que o destinatário e remetente, estão se comunicando através da chave pública correta. Caso outro destinatário mal-intencionado tente intervir na comunicação, esse problema é resolvido através do método para distribuição de chaves públicas denominado de infraestrutura de chave pública (IPC) ou public key infrastructure (PKI) (CARISSIMI, ROCHOL e GRANVILLE, 2009, p.349).

* + 1. Algoritmos de Criptografia

São códigos de computador que misturam lógica matemática, lógica de programação e protocolos que faz com que as mensagens fiquem com texto inelegíveis, possibilitando a transferência de informações com uma certa segurança, tanto por canais internos ou externos. Abaixo citaremos alguns algoritmos para criptografia tanto assimétrica como para simétrica.

* + - 1. Algoritmos para criptografia simétrica

“Os algoritmos de chave simétrica têm como característica a rapidez na execução, porém eles não permitem a assinatura e a certificação digitais.” (NAKAMURA E GEUS, 2007, p. 303).

A seguir dois algoritmos mais conhecidos na criptografia simétrica:

Embora tenham sido desenvolvidas várias cifras simétricas, o Data Encryption Standard (DES) é uma das mais utilizadas (STALLINGS, 2015, p.46).

Os dados são encriptados em blocos de 64bits usando uma chave de 56bits. O Algoritmo transforma a entrada de 64 bits em uma série de etapas para uma saída de 64 bits. As mesmas etapas, com a mesma chave, são empregadas para reverter a encriptação.

Com o passar dos anos, DES tornou-se algoritmo de encriptação simétrica dominante, especialmente em aplicações financeiras.

Assim como em qualquer esquema de encriptação, existem duas entradas na função, o texto claro a ser encriptado e a chave. Nesse caso, o texto claro precisa ter 64 bits de extensão, e a chave tem 56 bits de extensão.

Mesmo permitindo até 72 quatrilhões de combinações, este algoritmo foi desvendado utilizando-se as chamadas técnicas de "força bruta" (tentativa e erro) em um desafio promovido na internet.

De acordo com Stallings (2015) como qualquer cifra de Feistel, a decriptação usa o mesmo algoritmo da encriptação, exceto que a aplicação das sub-chaves é invertida. Além disso, as permutações inicial e final são invertidas.

Uma propriedade desejável de qualquer algoritmo de encriptação é que uma pequena mudança no texto claro ou na chave produza uma alteração significativa no texto cifrado. Em particular, uma mudança em um bit do texto claro ou um bit da chave deverá produzir uma modificação em muitos bits do texto cifrado. Se a mudança fosse pequena, esta poderia oferecer um modo de reduzir o tamanho do espaço de texto claro ou de chave a ser pesquisado.

A possibilidade de que a criptoanálise seja possível explorando-se as características do algoritmo DES se torna uma preocupação. O foco disso tem sido as outo tabelas de substituição, ou S-boxes que são usadas em cada iteração. Como os critérios de projeto para essas caixas, e, na realidade, para o algoritmo inteiro, não se tornaram públicos, existe uma suspeita de que elas foram construídas de modo que a criptoanálise seja possível para um oponente que conheça as fraquezas nelas. Essa afirmação é torturante, e com o passar dos anos, diversas regularidades e comportamentos inesperados das S-boxes foram descobertos.

Apesar disso, ninguém até aqui teve sucesso desvendando a suposta fraqueza fatal nas S-boxes.

De acordo com Carissimi, Rochol e Granville (2009) outro algoritmo bastante utilizado, o IDEA (International Data EncryptionAlgorithm). Sendo bastante similar ao DES, o mesmo utiliza a cifragem em blocos de 64 bits com várias etapas de soma e multiplicação e transposição. Sua principal vantagem em relação ao DES é o fato de empregar uma chave maior de 128 bits, e de ter um processamento mais elaborado em cada uma de suas etapas.

“Os algoritmos DES e IDEA, foram definidos para permitir suas implementações tanto em hardware e software. A criptografia utilizada nesses algoritmos é a simétrica, pois a mesma chave utilizada para cifrar os dados é utilizada para decifrar.” (CARISSIMI, ROCHOL e GRANVILLE, 2009, p.358).

O AES é uma cifra simétrica de bloco que pretende substituir o DES como o padrão para uma grande variedade de aplicações.

Comparada às cifras de chave pública como o RSA, a estrutura do AES e a maioria das cifras simétricas são bastante complexas e não são explicadas tão facilmente, quanto outras cifras criptográficas.

No AES, todas as operações são realizadas em 8 bits. Em particular, as operações aritméticas de soma, multiplicação e divisão são feitas sobre o corpo finito (STALLINGS, 2015, p.102).

Conforme o autor, um corpo é um conjunto no qual nós podemos somar, subtrair, multiplicar e dividir sem sair dele. Um exemplo de um corpo finito (aquele que possui um número finito de elementos) é o conjunto Zp, que contém todos os inteiros, onde p é um número primo e cujo cálculo é feito módulo de p.

Os desenvolvedores do Rijndael indicam, como sua motivação para selecionar esse dentro os 30 polinômios irredutíveis possíveis de grau 8, que ele é o primeiro na lista dada em [LIDL94].

O Rijndael é um algoritmo de criptografia de blocos, trabalhando com blocos de 128 ***bits*** e chaves de 128, 192 ou 256 ***bits***. O Rijndael original foi desenvolvido para suportar tamanhos diferentes de blocos de dados e de chaves, porém, estes não são adotados na versão AES (TREVISAN ET AL., 2013, p. 15).

O AES é dividido em dois módulos, sendo um para cifragem e um para decifragem. O módulo para cifragem conta com quatro transformações: um de permutação e três de substituição.

- SubBytes: utiliza uma S-box para realizar uma substituição byte a byte do bloco

- ShiftRow - uma permutação simples

- MixColumns: uma substituição que utiliza aritmética sobre GF(2\_8)

- AddRoundKey: um XOR bit a bit simples do bloco atual com uma parte da chave expandida

* + - 1. Algoritmo para criptografia assimétrica

“Os algoritmos de chave pública ou assimétrica, como RSA e outros, podem possibilitar, além do sigilo, integridade, não-repúdio e autenticidade. É possível ainda que a assinatura e a certificação digitais possam ser utilizadas.” (NAKAMURA E GEUS, 2007, p. 303).

A seguir o algoritmo mais conhecido e utilizado na criptografia assimétrica.

Carissimi, Rochol e Granville (2009) afirmam que se tratando do algoritmo de chave pública RSA, ambas as chaves são definidas por dois pares de números (N, e) e (N, d) respectivamente. O valor de N é comum a ambas as chaves, o emissor cifra a mensagem através da função C=T^3 mod N, onde C é o texto cifrado, T o texto em claro, o par (N, e) é chave pública do destinatário. Com isso, a tentativa de decifrar uma mensagem por tentativa é inviável devido à complexidade matemática, ao se escolher os pares (N, e) e (N, d), derivados de números primos grandes. As chaves públicas e privadas são relacionadas por uma função matemática baseada na fatoração desses números.

Atualmente é o algoritmo de chave pública mais utilizado e utiliza-se números primos. A premissa por trás do RSA consiste na facilidade de multiplicar dois números primos par obter um terceiro número, mas muito difícil de recuperar os dois primos a partir daquele terceiro número. Isso é conhecido como fatoração. Por exemplo, os fatores primos de 3.337 são 47 e 71. Gerar uma chave pública envolve fatorar um grande número. Se o número for grande o suficiente e bem escolhido, netão ninguém pode fazer isso em uma quantidade de tempo razoável. Uma chave RSA de 512 bits foi quebrada em 1999 pelo Instituto Nacional de Pesquisa da Holanda, com o apoio de cientistas de mais 6 países. No Brasil, o RSA é utilizado pela ICP-Brasil, no seu sistema de emissão de certificados digitais. Atualmente essas chaves são emitidas com o comprimento de 4.096 bits (OLIVEIRA, 2012, p.13).

* + 1. Técnicas básicas de cifragem

Carissimi, Rochol e Granville (2009) afirmam que na cifragem por substituição, cada letra da palavra é substituída por outra letra. No caso da cifra de César, cada letra é substituída pela terceira letra à sua direita do alfabeto, exemplo, se a palavra a ser cifrada tiver a letra “a” irá ser substituída por “d”, que é a terceira letra depois de “a” no alfabeto. Na cifragem por transposição, as letras da palavra são trocadas de posição entre si, seguindo uma determinada regra, exemplo, pode dividir a palavra em blocos de quatro caracteres, incluindo os espaços em branco e enviar primeiro todas as letras iniciais de cada bloco e assim sucessivamente. Nesse caso, a mensagem chegará trocada para o destinatário. Com isso, através da regra de transposição aplicada, ele saberá a palavra original.

Carissimi, Rochol e Granville (2009, p.354) complementam: “Uma forma de dificultar a dedução da regra de cifragem é usar uma combinação de substituição e transposição, dando origem ao que se denomina de cifragem produto”

A cifragem de um produto quando aplicada em dados binários, permite que as substituições ou as transposições ocorram em bits, que são agrupados em uma quantidade menor que a unidade de informação. Sendo assim, substituição e transposição podem ser feitas tomando os bits em dois a dois. Os cifrados produtos são constituídos sobre dois blocos básicos, P-box e S-box.

Conforme Carissimi, Rochol e Granville (2009) o bloco P-box é responsável pela execução da transposição e permite três modos básicos, direto, expansão e compressão. No modo direto, uma entrada é dividida em n bits e é reordenada de acordo com uma regra de em baralhamento, fornecendo uma saída também em bits. No modo por expansão, os n bits da entrada são reordenados e repetidos, fornecendo uma saída com um número de bits superior ao de entrada. A sequência de reordenação e dos bits que serão repetidos é fornecida por uma regra de formação. No modo por compressão, a saída é composta apenas por alguns bits da entrada que são selecionadas com base em uma regra. Conceitualmente, a regra mencionada nos três métodos é denominada de chave.

Sendo assim, Carissimi, Rochol e Granville (2009) informam que a principal desvantagem do P-box é a definição da chave, ou seja, a regra utilizada para determinar qual entrada está associada a qual saída. Com uma única chave, cifrar vários textos é possível estaticamente deduzir a regra, quebrando o código. O ideal seria fazer com que cada unidade de informação tivesse sua própria chave. Uma forma de reduzir a largura da chave é colocar a P-box entre um multiplexador e um demultiplexador, que atuam como uma espécie de codificador, trocando uma sequência de entrada por outra de saída, ou seja, fazendo uma substituição, sendo o modelo S-box.

Carissimi, Rochol e Granville (2009) afirmam que no processo de cifragem quanto mais complexo, aumenta a dificuldade de ser quebrado, combinando múltiplos P-boxes e S-boxes em diferentes etapas. Outro ponto importante é que esses blocos básicos, podem ser facilmente implementados por circuitos lógicos, fazendo com que os procedimentos de cifragem e decifração sejam realizados em hardware de forma rápida e eficiente.

De acordo com Carissimi, Rochol e Granville (2009) um algoritmo de cifragem bastante utilizado para aplicar esta técnica é o DES (Data Encryption Standard), pois executa uma cifragem em blocos, onde a informação e subdividida em blocos de tamanho fixo de 64 bits. Cada um desses blocos sofre um conjunto de operações de substituição e de transposição. Assim, de posse de uma chave secreta, o remetente cifra a mensagem, envia para o destinatário que utiliza a mesma chave para decifrar a mensagem.

* + 1. Gerenciamento de chaves e certificados digitais

De acordo com Carissimi, Rochol e Granville (2009) o gerenciamento de chaves tem como finalidade mostrar como as chaves públicas e privadas são geradas, mantidas e também como são entregue as informações aos destinatários. Isso pode gerar um problema ao gerenciamento de distribuição de chaves, que atua de diferentes formas de acordo a criptográfica, se é simétrica ou assimétrica.

A utilização da chave simétrica apresenta três problemas. No primeiro caso, cada par de indivíduos deve possuir uma chave para comunicarem de forma segura. Esse processo pode se complicar em um grupo de n pessoas, cada uma delas possua n-1 chaves, o que implica no sistema n\*(n-1) /2 chaves diferentes. Assim nesse sistema, há uma grande quantidade de chaves, dificultando o gerenciamento, obtenção e manutenção das chaves. O segundo problema está diretamente relacionado com o primeiro, pois cada usuário deve possuir armazenar e lembrar n-1 chaves. O terceiro é garantir que essas chaves sejam distribuídas de forma segura impedindo que caíssem em destinatários indevidos e mal-intencionada. Caso a chave pública distribuída caia nas mãos de terceiros indevidamente, deve ser substituída e retribuída para os autorizados dessa chave, trazendo então dificuldades no gerenciamento.

Os estudos de Carissimi, Rochol e Granville (2009) afirmam que esses três problemas da chave simétrica podem ser resolvidos simultaneamente criando uma autoridade central de distribuição de chaves (CDC), ou key distribtion center (KDC). Quando necessário, as duas partes se comunicarem, ambas entraram em contato com a CDC que distribui uma chave simétrica, gerada e valida. Somente para essa comunicação, essa chave é denominada de chave de sessão. Assim, os pares não precisam saber armazenar a chave do correspondente, transferindo toda responsabilidade de segurança para CDC.

Conforme Carissimi, Rochol e Granville (2009, p.351) “A infraestrutura da chave pública (public key infrastructure-PKI) é fundamentada em dois componentes importantes que garante a autenticidade e integridade das chaves, sendo o certificado digital e a autoridade certificadora”.

A autoridade certificadora (certificateauthority-CA) é responsável por emitir um documento digital denominado como certificado digital, que é utilizado para identificar uma pessoa física ou jurídica. O certificado digital entre outras informações possui o nome de seu proprietário, sua chave pública, um número único de série, data de validade e a assinatura digital da empresa certificadora, assim podendo iniciar uma transação segura com uma parte, através do certificado digital que obtêm a chave pública (CARISSIMI, ROCHOL e GRANVILLE, 2009, p.352).

As empresas certificadoras são responsáveis por garantir a autenticidade de uma pessoa física ou jurídica. Essas informações fornecidas por elas devem ser verificadas cuidadosamente de forma que, garanta que a chave pública pertencerá a quem diz ser proprietário antes de emitir o certificado digital, devido a isso, essas empresas são auditadas e regidas sob fortes legislações jurídicas. Os certificados emitidos são armazenados e disponibilizados publicamente em um repositório, um usuário que deseja manter uma comunicação segura com um terceiro, deverá acessar esse repositório para recuperar o certificado digital de seu correspondente. Esse certificado pode ser instalado na máquina local, para evitar que o repositório precise ser novamente acessado. O certificado instalado permanecerá válido até que se expire, seja removido, ou seja, revogado por algum motivo (CARISSIMI, ROCHOL e GRANVILLE, 2009, p.352).

Conforme os autores, o proprietário do certificado digital deverá confiar na autoridade certificadora. Pois, os certificados digitais são assinados com a chave privada dessa autoridade, essa assinatura é a cifragem de alguns campos do certificado, como a chave pública do proprietário.

As autoridades são organizadas em uma estrutura hierarquia em árvore no qual, cada nodo depende de um novo pai para garantir sua identificação. Assim, o certificado digital de uma entidade certificadora é assinado por outra entidade de nível hierárquico mais alto e assim sucessivamente até a IPRA (Internet Policy Registration Authority - IPRA), que deve ser vista como entidade responsável, única e extremamente confiável desse sistema. Dessa forma, usando uma chave raiz a IPRA assina exclusivamente certificados para autoridades de criação de vez, também são responsáveis por estabelecer políticas, para a obtenção de certificados digitais junto às autoridades certificadoras e por assiná-los.

Carissimi, Rochol e Granville (2009) explicam que é dever das autoridades certificadoras manterem uma lista de revogação de certificados (Certification Revogation List - CRL). Nesta lista, são mantidos os certificados cuja data de validade expiraram e não foram revalidados por seus proprietários quando, por exemplo, sua chave privada foi comprometida antes da data de expiração do certificado.

O uso do certificado digital soluciona o problema da distribuição da chave pública. Porém, o proprietário deverá tomar cuidado ao permitir que o certificado seja instalado e usado por diferentes sistemas operacionais e aplicações, evitando que possa comprometer a segurança da chave pública. A autoridade de registro (AR) é responsável por identificar uma pessoa física ou jurídica que deseja adquirir um certificado digital, essa identificação é presencial e necessita coletar os documentos comprobatórios para garantir que a pessoa é realmente quem diz ser (CARISSIMI, ROCHOL e GRANVILLE, 2009, p.353).

* + 1. Aplicações da criptografia em comunicação digital

Os requisitos de privacidade, integridade e autenticidade conforme Carissimi, Rochol e Granville (2009) são bastante importantes na utilização de troca de informações na internet, como as aplicações que realizam transações bancárias, trocam de informações de documentos sigilosos, comércio eletrônico, entre outros. Também surge um quarto requisito, o não repudio, sendo a capacidade de identificar de forma segura a origem de um determinado documento, com objetivo de ter um mecanismo que evite que um remetente negue que foi ele quem gerou, ou enviou um determinado documento ou mensagem.

O uso de criptográfica simétrica e assimétrica na utilização de meios de comunicação digital é combinado de forma que garanti os requisitos básicos de privacidade, integridade, autenticidade e não repudio, nas aplicações. Neste capítulo serão mostrados três exemplos de aplicações baseadas em técnicas de criptografia, sendo elas, assinatura digital, segurança em mensagens eletrônicas e autenticação de usuários (Carissimi, Rochol e Granville, 2009, p.358).

* + 1. Assinatura digital

O objetivo da assinatura digital é garantir a autenticidade e a integridade de um documento eletrônico. De forma que se tenha a mesma validade judicial que os documentos com assinatura por escrito possuem, facilitando as transações comerciais e jurídicas de forma eletrônica. Tendo em vista a integridade e garantida de forma com qual se obtém a assinatura de um documento eletrônico.

Segundo Carissimi, Rochol e Granville (2009) os documentos eletrônicos são cifrados usando criptografia assimétrica, neste caso o emissor do documento cifra o conteúdo empregando sua chave privada e a informação pode ser decifrada por terceiros que possuírem a chave pública do emissor, como a chave privada é apenas de conhecimento único do emissor, somente ele teria condições de modificar o documento garantindo assim a sua integridade, não há como alterar ou forjar um documento sem o conhecimento da chave privada do emissor, pois se ele fosse alterado por um terceiro, este não teria como cifrar novamente, o que garante sua integridade, além disso, a unicidade da relação do par de chaves pública e privada atesta ainda que o documento fosse assinado pelo indivíduo de quem se detém a chave pública, ou seja, atesta-se a autenticidade do documento.

O uso de assinatura digital não implica em privacidade, ou confidencialidade das informações, ou seja, os documentos assinados digitalmente podem ser transmitidos em claro na rede, o que importa é a sua integridade, autenticidade e o não repudiam. “Caso a privacidade seja necessária, pode-se obter a propriedade cifrando o documento antes de enviá-lo.” (CARISSIMI, ROCHOL E GRANVILLE,2009, p.360).

* + 1. Autenticidade de usuários

O acesso a recursos de um sistema operacional é obtido por meio de dos mecanismos básicos, autenticação e autorização. Por autenticação entende-se o procedimento de verificar a identidade de uma entidade, usuário ou processo, perante outra entidade.

Uma vez autenticado, é identificado, é necessário consultar se a entidade tem direito para executar uma determinada operação ou acessar um determinado recurso, isso é autorização.

Nas palavras de Carissimi, Rochol e Granville (2009, p.362) o usuário é identificado no sistema, o mesmo passa a ter acesso a todos os recursos que sua autorização permite, portanto o problema é garantir que o usuário que efetuou o login no sistema seja realmente que ele afirma ser. O sistema de autenticação é bastante suscetível a falhas por ser baseado apenas no conhecimento de um nome de usuário e de uma senha. Uma primeira abordagem é forçar que os usuários cifrem seus nomes de usuários e senha no momento de autenticação no sistema, no entanto tal procedimento não resolve o problema, pois na realidade não importa conhecer o nome de usuário e a senha, mas sim tê-los, esse tipo de ataque é conhecido de replay ou playback.

* + 1. Segurança de mensagens eletrônicas

Carissimi, Rochol e Granville (2009) afirmam que com o avanço da tecnologia nos dias atuais, a troca de informações por correio eletrônico vem sendo uma opção bastante utilizada, de forma que as mensagens eletrônicas ultrapassem a barreira da simples comunicação pessoal e passam a ser um mecanismo de troca de informações importante surge à preocupação com a segurança das informações.

As seguranças de mensagens eletrônicas mantêm os quatro requisitos básicos, privacidade, autenticidade, integridade e não repudio. A privacidade diz respeito ao fato de que o conteúdo de uma mensagem deve ser conhecido única e exclusivamente pelas partes envolvidas, ou seja, entre o remetente e o destinatário, essa confidencialidade na troca de informação é obtida cifrando o texto da mensagem com o uso de técnicas de criptografia simétrica e assimétrica, assim se a mensagem for obtida por um destinatário não autorizado, as informações manterão a integridade (CARISSIMI, ROCHOL e GRANVILLE, 2009, p.360).

1. PROJETO

Este capítulo tem como objetivo principal apresentar a proposta em desenvolver um software que realiza o monitoramento da validade do certificado digital, junto com a aplicação da Criptografia Simétrica, denominado de SisCVC (Sistema de Controle de Validade do Certificado Digital)

* 1. Conceitos iniciais

O SisCVC é um sistema projetado para monitorar a validade dos certificados digitais, que serão cadastrados pelos usuários das contabilidades. Sendo assim, o sistema monitorará todos os dias, em um horário definido, quais certificados cadastrados no banco de dados que expirarão, de acordo com as opções selecionadas pelo usuário ao cadastrar o certificado digital, sendo elas de 1, 15 ou 30 dias antes do certificado expirar. Assim, o sistema notificará o cliente referente a validade do certificado via e-mail e aos usuários cadastrados no sistema.

O sistema também aplicará os conceitos matemáticos da criptografia simétrica, ou seja, a chave que é utilizada para criptografar as informações, que no caso serão as senhas dos usuários, será a mesma chave para descriptografar.

Desenvolvemos um algoritmo de criptografia, visando o aperfeiçoamento da cifra de césar, que é um tipo de cifra por substituição.

Para elaboração do software foi utilizada a tecnologia Java que é formada pela linguagem de programação e a plataforma, que é projetada em orientação a objetos. Sendo formada pelos componentes, Java Virtual Machine (JVM), que representa a máquina virtual Java, responsável por executar os softwares feitos na linguagem Java. Outro componente é o Java Application Programming (API), que representa por uma coleção dos componentes do software sendo agrupada em bibliotecas, classes e interfaces.

A interface utilizada foi baseada na ferramenta Swing, pois fornece componentes flexíveis, tais como botões, caixas de seleção, rótulos e balanço. Fornece também vários componentes avançados, como painel com abas, painéis de rolagem, árvores, tabelas e listas. Já para o armazenamento dos dados dos usuários e clientes, utilizamos o banco de dados MySQL por sua facilidade de programação, possui funções simples e assim facilitando a manipulação de dados.

* 1. Algoritmo de criptografia utilizado

Visando o aperfeiçoamento da cifra de césar que é um tipo de cifra por substituição, desenvolvemos um algoritmo de criptografia simétrica. O algoritmo terá uma chave definida, que será utilizada para criptografar e descriptografar.

Através dessa chave será aplicado os conceitos matemáticos nas senhas criadas pelos usuários. Sendo assim, adicionando as no banco de dados, garantindo mais segurança, integridade e dificultando que indivíduos não autorizados tenha acesso as senhas.

* + 1. Criptografando a senha

Com a chave definida, a mesma será salva em uma variável do tipo string, posteriormente o sistema realizará a conversão para um array do tipo char e o seu tamanho será definido de acordo com a chave. Com isso, é realizado a conversão dos caracteres da chave para array do tipo int, de acordo com a tabela ASCII (Figura1).

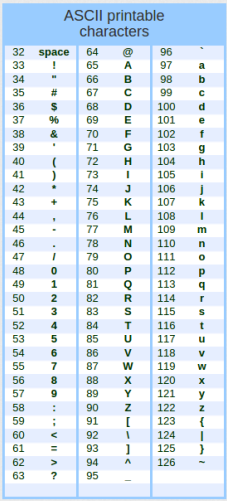


Figura 1 – Tabela ASCII Printable Characters

Assim que for cadastrada uma senha para o usuário, a mesma será salva em uma variável do tipo string. Logo em seguida é realizada a conversão da senha para o array do tipo char, o seu tamanho será de acordo com o tamanho da senha digitada. Com isso, é realizado a conversão dos caracteres da senha para array do tipo int, de acordo com a tabela ASCII.

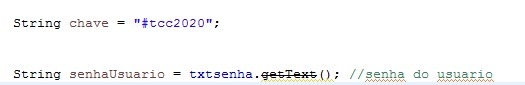
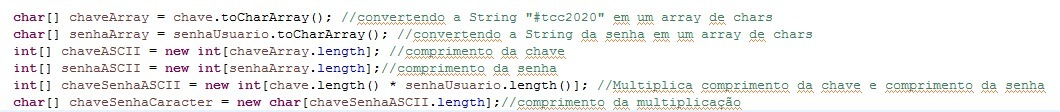


Figura 2 – Chave e Senha do usuário

Na figura 3, mostraremos as arrays da chave e senha do usuário, juntamente com a senha e chave do tipo char e int.

Figura 3 – Arrays e tipo de variável

Na figura 4, mostraremos a conversão da chave de acordo com a figura 1.

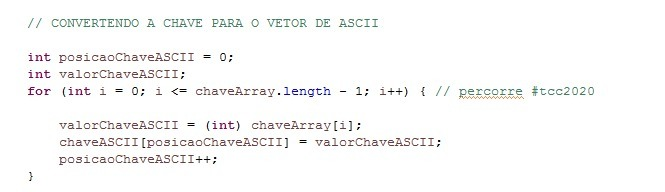


Figura 4 – Conversão da chave

Na figura 5, mostraremos a conversão da senha do usuário de acordo com a Figura 1.

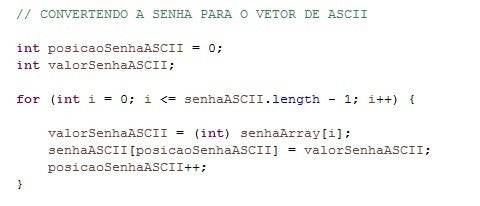


Figura 5 – Conversão da senha

Após a conversão da chave e da senha são realizados os seguintes cálculos matemáticos, foi criado um laço de repetição que pega o primeiro inteiro da chave e realiza a soma com todos os inteiros da senha. Logo após, o segundo inteiro da chave também é somado com todos inteiros da senha, assim sucessivamente até finalizar o tamanho da chave. Com isso, a senha criptografada é gerada com a multiplicação da chave com a senha digitada, que será salva em um vetor do tipo int e depois será realizada a conversão do array do tipo int para array do tipo char, que será o tamanho da senha criptografada.

A chave e a senha devem estar entre os numerais 32 e 126, baseando na figura 1. Se a soma dos numerais for maior que 158 é realizada a subtração por 126. Com isso o valor fica menor que 126. Caso a soma dos numerais for menor que 158 é realizada a subtração da por 32, garantindo que os valores fiquem entre 32 a 126 de acordo com a tabela ASCII.

Na figura 6, mostraremos os cálculos informados acima.

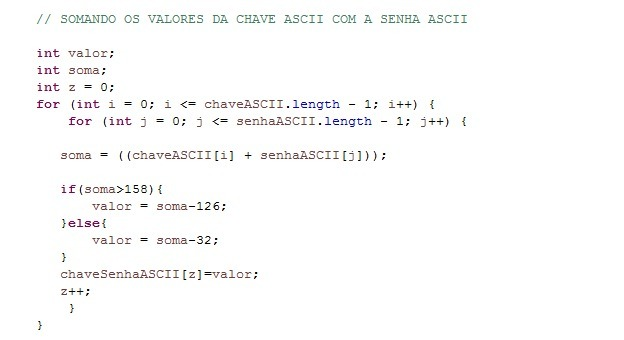


Figura 6 – Cálculos criptografia

Na figura 7 mostraremos a conversão da senha criptografada de ASCII para caracteres.

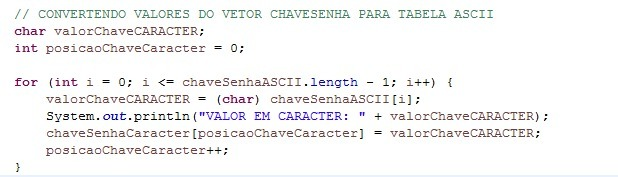


Figura 7 – Conversão da senha criptografada

Na figura 8 mostraremos o resultado da senha armazenada no banco de dados.



Figura 8 – Armazenamento banco de dados

* + 1. Descriptografando a senha

Como é necessário a mesma chave utilizada para descriptografar, no software essa etapa ocorre no processo de login, onde é realizada a busca da senha no banco de dados, selecionando o usuário que está realizando o login.

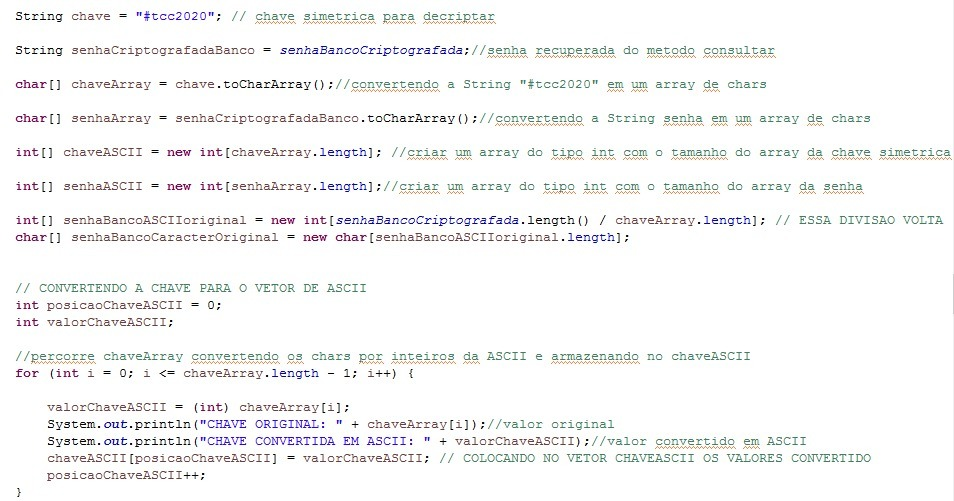


Figura 9 – Conversão senha criptografada

Ao realizar a busca da senha criptografada é realizada a conversão para array do tipo char, posteriormente é realizado a conversão para array do tipo int. Lembrando que é de acordo com os valores da tabela ASCII (Figura 1).

Após a conversão da senha criptografada para array do tipo int são realizadas as seguintes operações: é coletado o primeiro inteiro da chave criptografada convertida para ASCII, o mesmo é somando com 126 e subtraído com o primeiro inteiro da chave e assim sucessivamente. Caso o resultado dessa operação seja maior que 126 é realizada outra operação, onde o valor da senha criptografada convertida para ASCII é somado com 32 e posteriormente subtraído com o valor da chave.

Na figura 10 mostraremos os cálculos para descriptografar, usando a chave e a senha em valores ASCII numeral.

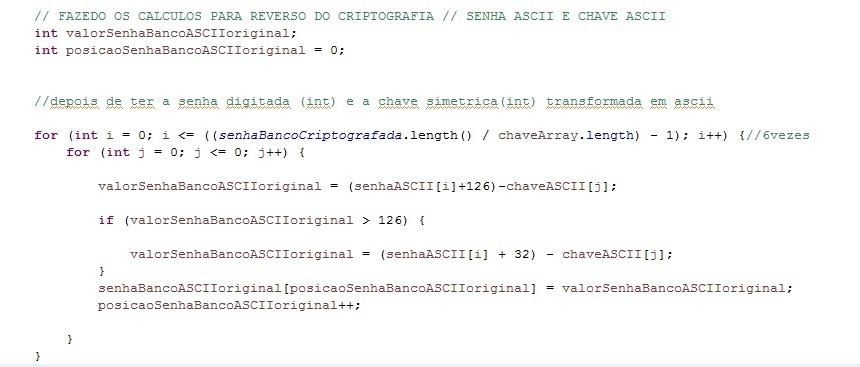


Figura 10 – Cálculos descriptografar

Na figura 11 mostraremos a conversão da senha descriptografada em ASCII para caracteres.

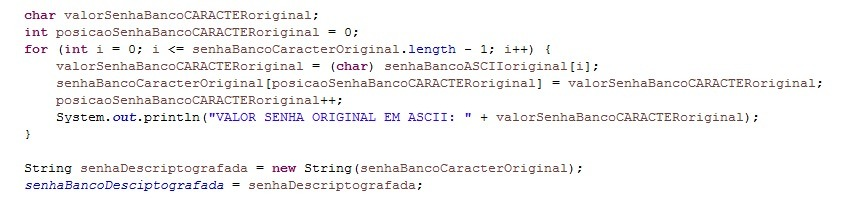


Figura 11 – Conversão senha descriptografada

Após esses processos, conseguimos descriptografar a senha do banco de dados, posteriormente é salvo o valor em uma variável do tipo string e comparada com o valor da senha que o usuário digitou.

* 1. Diagramas utilizados
     1. Diagrama de casos de uso

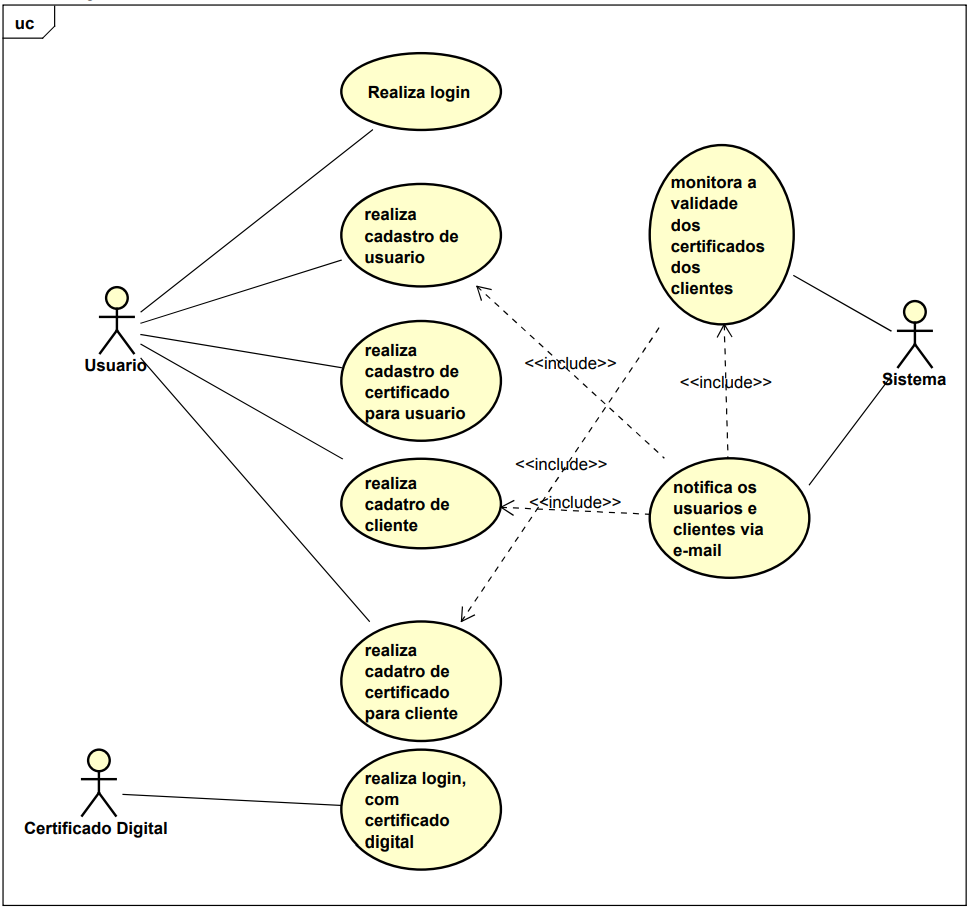
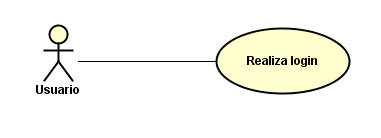


Figura 12 – Diagrama de Caso Uso – SISCVC

* + - 1. Descrições textuais dos casos de uso

UC – 01: Realizar login



* + - **Descrição do UC**

Esse caso de uso descreve como o usuário faz o login no software com usuário e senha.

* + - **Atores envolvidos**

Usuário

* + - **Pré-condições**

O usuário deve estar cadastrado no software, para realizar login.

* + - **Fluxo Básico**

1 – O software exibe a tela de login.

2 – O software solicita, o login e senha;

3 – Com todos os dados preenchidos corretamente, o software então permite o acesso ao usuário.

4 – Com os dados do certificados cadastrados corretamente, o software então permite o acesso ao usuário.

* + - **Fluxo Alternativo**

1 – Login ou senha do usuário digitado incorretamente, exibe a mensagem, usuário ou senha inválidos.

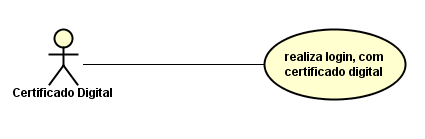
2 – Campos vazios, de login ou senha, exibe a mensagem, preencha todos os campos.

* + - **Regras de Negócio**

1 – O login e a senha devem estar cadastrado na base de dados, e deve estar ligados um ao outro

2 – Os campos login e senha não podem estar vazios.

**UC – 02: Realizar login com certificado**



* + - **Descrição do UC**

Esse caso de uso descreve como o usuário realiza o login no software com o certificado digital.

* + - **Atores envolvidos**

Usuário

* + - **Pré-condições**

O usuário e o certificado do usuário, devem estar cadastrados no software, para realizar o login.

* + - **Fluxo Básico**

1 – O software exibe a tela de login.

2 – O usuário solicita o login com certificado digital.

3 – O usuário seleciona o certificado digital que deseja utilizar.

4 – Com os dados do certificados cadastrados corretamente, o software então permite o acesso ao usuário.

* + - **Fluxo Alternativo**

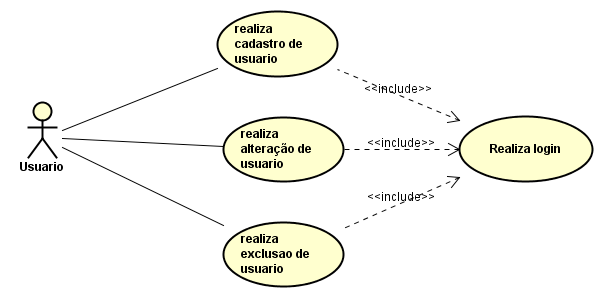
1 – Certificado do usuário selecionado incorretamente ou certificado não cadastrado, exibe a mensagem, certificado não cadastrado ou inválido.

* + - **Regras de Negócio**

1 – O certificado digital, deve estar cadastrado na base de dados e vinculado ao usuário.

2 – O certificado digital tem que ser do tipo PF A3.

UC – 03: Realizar cadastro de usuário.



* + - **Descrição do UC**

Esse caso de uso descreve como o usuário realiza cadastro de usuários no software.

* + - **Atores envolvidos**

Usuário

* + - **Pré-condições**

1 – O usuário deve estar logado no software.

2 – O usuário deve clicar na opção usuários.

* + - **Fluxo Básico**

1 – O software exibe a tela de cadastro de usuário.

2 – O usuário preenche todos os campos solicitados.

3 – O usuário clica na opção incluir.

4 – Com os dados corretos, o usuário é cadastrado e habilita a opção cadastrar certificado, caso o usuário desejar vincular certificado para o usuário.

5 – O software exibe a mensagem, usuário cadastrado com sucesso.

* + - **Fluxo Alternativo**

1 – Usuário não logado no software.

2 – Caso tenha alguma campos vazios, é exibida a mensagem, preencha todos os campos.

* + - **Regras de Negócio**

1 – O usuário deve estar logado no web site.

2 – Todos os campos são obrigatórios.

3 – O usuário não pode já está cadastrado.

UC – 03-1: Realizar alteração de usuário.

* + - **Descrição do UC**

Esse caso de uso descreve como o usuário realiza alteração de usuários no software.

* + - **Atores envolvidos**

Usuário

* + - **Pré-condições**

1 – O usuário deve estar logado no software.

2 – O usuário deve clicar na opção usuários.

* + - **Fluxo Básico**

1 – O software exibe a tela de consultar de usuário.

2 – O usuário consulta o usuário que deseja realizar alteração.

3 – O usuário, seleciona o usuário desejado clica na opção alterar.

4 – O usuário altera os dados desejados e clica na opção atualizar.

5 – O software exibe a mensagem, usuário alterado com sucesso.

* + - **Fluxo Alternativo**

1 – Usuário não logado no software.

2 – Caso tenha alguns campos vazios, é exibida a mensagem, preencha todos os campos.

* + - **Regras de Negócio**

1 – O usuário deve estar logado no software.

2 – Todos os campos são obrigatórios.

UC – 03-2: Realizar exclusão de usuário.

* + - **Descrição do UC**

Esse caso de uso descreve como o usuário realiza exclusão de usuários no software.

* + - **Atores envolvidos**

Usuário

* + - **Pré-condições**

1 – O usuário deve estar logado no software.

2 – O usuário deve clicar na opção usuários.

* + - **Fluxo Básico**

1 – O software exibe a tela de consultar de usuário.

2 – O usuário consulta o usuário que deseja realizar exclusão.

3 – O usuário, seleciona o usuário desejado, clica na opção excluir.

4– O software exibe a mensagem, usuário excluído com sucesso.

* + - **Fluxo Alternativo**

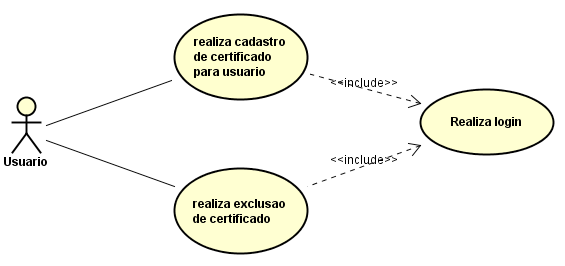
1 – Usuário não logado no software.

2 – Caso tenha alguns campos vazios, é exibida a mensagem, preencha todos os campos.

* + - **Regras de Negócio**

1 – O usuário deve estar logado no software.

UC – 04: Realizar cadastro do certificado ao usuário



* + - **Descrição do UC**

Esse caso de uso descreve como o usuário realiza cadastro de certificado digital para o usuários.

* + - **Atores envolvidos**

Usuário

* + - **Pré-condições**

1 – O usuário deverá estar logado no software.

* + - **Fluxo Básico**

1 – O usuário, consulta o usuário que deseja realizar o cadastro do certificado digital.

2 – O usuário clica na opção cadastrar certificado digital.

3 – O software direciona para a tela de cadastro de certificado digital.

4 – O usuário clica na opção buscar certificados digital.

5 – O software busca todos os certificados cadastrados no computador.

6 – O usuário seleciona o certificado desejado, e clica na opção cadastrar certificado.

7 – O software exibe a mensagem, certificado cadastrado com sucesso.

* + - **Fluxo Alternativo**

1 – O usuário não selecionou o certificado para cadastrar.

2 – Usuário não preencheu todos os campos.

3 – O software exibe a mensagem, todos os campos devem ser preenchidos.

* + - **Regras de Negócio**

1 – O usuário deve estar logado no software.

2 – Usuário não pode já ter algum certificado cadastrado.

3 – O certificado digital não poderá estar cadastrado.

4 – O certificado digital não pode estar vencido.

5 – O certificado digital tem que ser do tipo PF A3

6 – Todos os campos tem que estar preenchidos.

UC – 04-1: Realizar exclusão do certificado do usuário

* + - **Descrição do UC**

Esse caso de uso descreve como o usuário realiza a exclusão do certificado digital para os usuários.

* + - **Atores envolvidos**

Usuário

* + - **Pré-condições**

1 – O usuário deverá estar logado no software.

* + - **Fluxo Básico**

1 – O usuário, consulta o usuário que deseja realizar a exclusão do certificado digital.

2 – O usuário clica na opção excluir certificado digital.

6 – O usuário seleciona o certificado desejado, e clica na opção excluir certificado.

7 – O software exibe a mensagem, certificado excluído com sucesso.

* + - **Fluxo Alternativo**

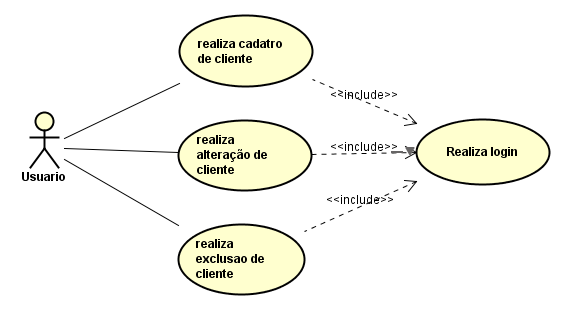
1 – O usuário não selecionou o certificado para excluir.

2 – Usuário não cadastrado.

* + - **Regras de Negócio**

1 – O usuário deve estar logado no software.

UC – 05: Realizar cadastro de cliente



* + - **Descrição do UC**

Esse caso de uso descreve como o usuário realiza cadastro de clientes no software.

* + - **Atores envolvidos**

Usuário

* + - **Pré-condições**

1 – O usuário deve estar logado no software.

2 – O usuário deve clicar na opção clientes.

* + - **Fluxo Básico**

1 – O software exibe a tela de cadastro de clientes.

2 – O usuário preenche todos os campos solicitados.

3 – O usuário clica na opção incluir.

4 – Com os dados corretos, o cliente é cadastrado.

5 – O software exibe a mensagem, cliente cadastrado com sucesso.

* + - **Fluxo Alternativo**

1 – Usuário não logado no software.

2 – Caso tenha algum campo vazio é exibida a mensagem, preencha todos os campos.

* + - **Regras de Negócio**

1 – O usuário deve estar logado no web site.

2 – Todos os campos são obrigatórios.

3 – O cliente não poderá estar cadastrado.

UC – 05-1: Realizar alteração de cliente

* + - **Descrição do UC**

Esse caso de uso descreve como o usuário realiza alteração de clientes no software.

* + - **Atores envolvidos**

Usuário

* + - **Pré-condições**

1 – O usuário deve estar logado no software.

2 – O usuário deve clicar na opção cliente.

* + - **Fluxo Básico**

1 – O software exibe a tela de consulta de clientes.

2 – O usuário consulta o cliente que deseja alterar.

3 – O usuário clica na opção alterar.

4 – O usuário altera os dados desejados, e clica na opção atualizar.

5 – O software exibe a mensagem, cliente cadastrado com sucesso.

* + - **Fluxo Alternativo**

1 – Usuário não logado no software.

2 – Caso tenha algum campo vazio é exibida a mensagem, preencha todos os campos.

* + - **Regras de Negócio**

1 – O usuário deve estar logado no web site.

UC – 05-2: Realizar exclusão de cliente

* + - **Descrição do UC**

Esse caso de uso descreve como o usuário realiza exclusão de clientes no software.

* + - **Atores envolvidos**

Usuário

* + - **Pré-condições**

1 – O usuário deve estar logado no software.

2 – O usuário deve clicar na opção cliente.

* + - **Fluxo Básico**

1 – O software exibe a tela de consulta de clientes.

2 – O usuário consulta o cliente que deseja excluir.

3 – O usuário clica na opção excluir.

4 – O usuário altera os dados desejados, e clica na opção atualizar.

5 – O software exibe a mensagem, cliente excluido com sucesso.

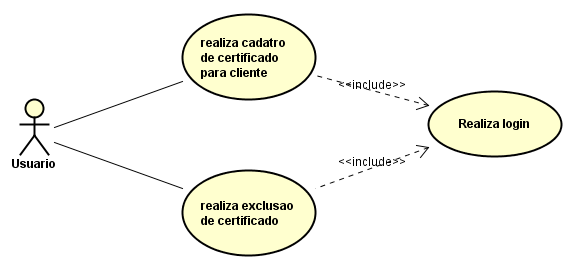
* + - **Fluxo Alternativo**

1 – Usuário não logado no software.

* + - **Regras de Negócio**

1 – O usuário deve estar logado no software.

UC – 06: Realizar cadastro de certificado para o cliente



* + - **Descrição do UC**

Esse caso de uso descreve como o usuário realiza cadastro de certificado digital para os clientes.

* + - **Atores envolvidos**

Usuário

* + - **Pré-condições**

1 – O usuário deverá estar logado no software.

* + - **Fluxo Básico**

1 – O usuário consulta o cliente que deseja realizar o cadastro do certificado digital.

2 – O usuário clica na opção cadastrar certificado digital.

3 – O software direciona para a tela de cadastro de certificado digital.

4 – O usuário clica na opção buscar certificados digital.

5 – O software busca todos os certificados cadastrados no computador.

6 – O usuário seleciona o certificado desejado, e clica na opção cadastrar certificado.

7 – O software exibe a mensagem, certificado cadastrado com sucesso.

* + - **Fluxo Alternativo**

1 – O usuário não selecionou o certificado para cadastrar.

2 – Usuário não preencheu todos os campos.

3 – O software exibe a mensagem, todos os campos devem ser preenchidos.

* + - **Regras de Negócio**

1 – O usuário deve estar logado no software.

2 – O certificado digital não poderá estar cadastrado.

3 – O certificado digital não poderá estar vencido.

4 – Todos os campos tem que estar preenchidos.

UC – 06-1: Realizar exclusão do certificado do cliente

* + - **Descrição do UC**

Esse caso de uso descreve como o usuário realiza a exclusão do certificado digital para dos clientes.

* + - **Atores envolvidos**

Usuário

* + - **Pré-condições**

1 – O usuário deverá estar logado no software.

* + - **Fluxo Básico**

1 – O usuário, consulta o cliente que deseja realizar a exclusão do certificado digital.

2 – O usuário clica na opção excluir certificado digital.

6 – O usuário seleciona o certificado desejado, e clica na opção excluir certificado.

7 – O software exibe a mensagem, certificado excluído com sucesso.

* + - **Fluxo Alternativo**

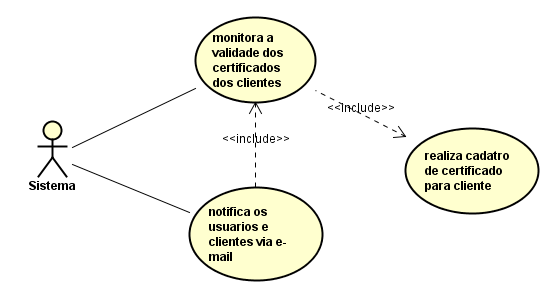
1 – O usuário não selecionou o certificado para excluir.

2 – Usuário não cadastrado.

* + - **Regras de Negócio**

1 – O usuário deve estar logado no software.

UC – 07: Realizar o monitoramento do prazo de validade dos certificados digitais cadastrados



* + - **Descrição do UC**

Esse caso de uso descreve como o sistema realiza o monitoramento dos certificados digitais dos clientes cadastrados.

* + - **Atores envolvidos**

Software.

* + - **Pré-condições**

1 – Os certificados digitais deverão estar cadastrados.

* + - **Fluxo Básico**

1 – O software consulta todos os certificados dos clientes cadastrados.

2 – O software verifica a diferença entre as datas de prazo de validade que consta no certificado digital com a data atual do servidor.

3 – O software notifica via e-mail os usuários e clientes, caso a diferença entre datas seja 1,15 ou 30 dias.

* + - **Fluxo Alternativo**

1 – O software não encontrou nenhum certificado digital cadastro

* + - **Regras de Negócio**

1 – Deverá possuir certificados digitais cadastrados.

2 – O certificado digital não poderá estar vencido.

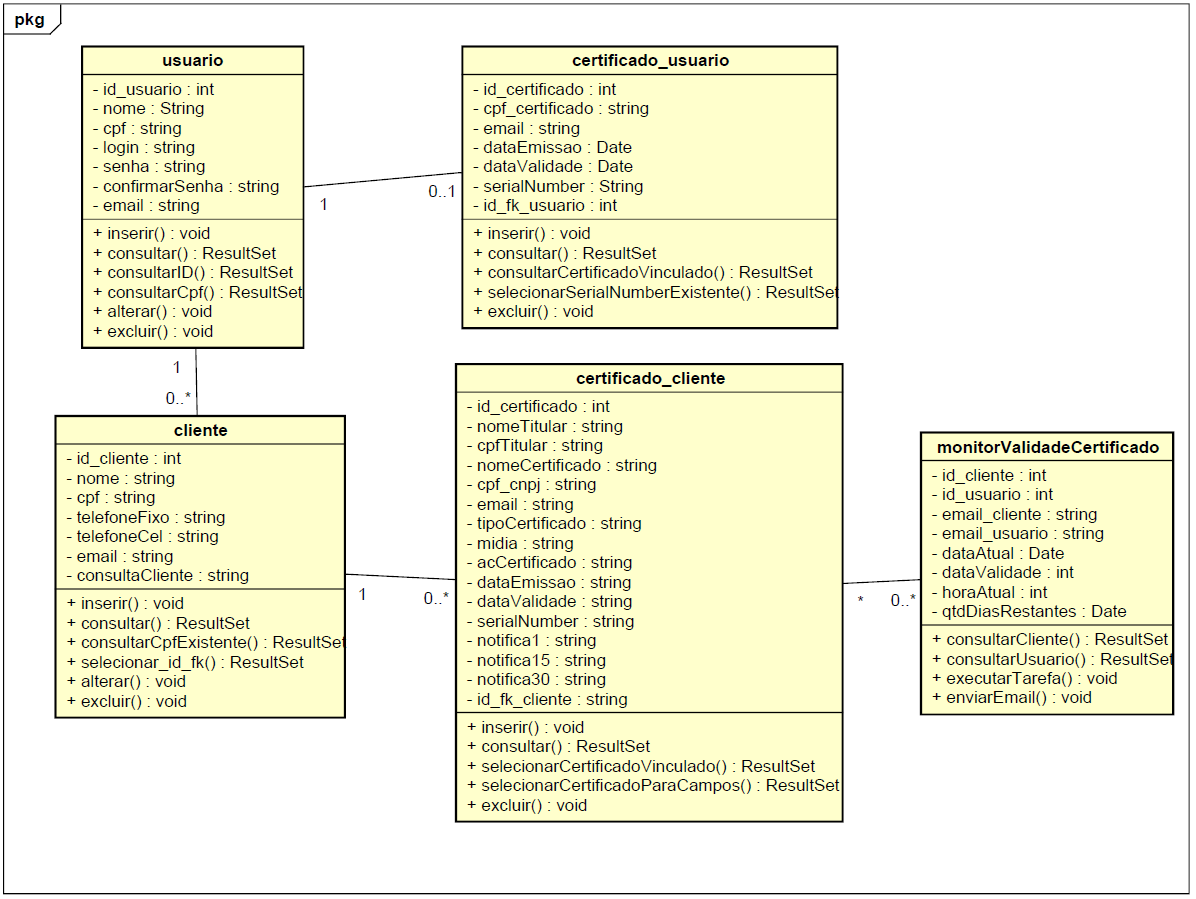
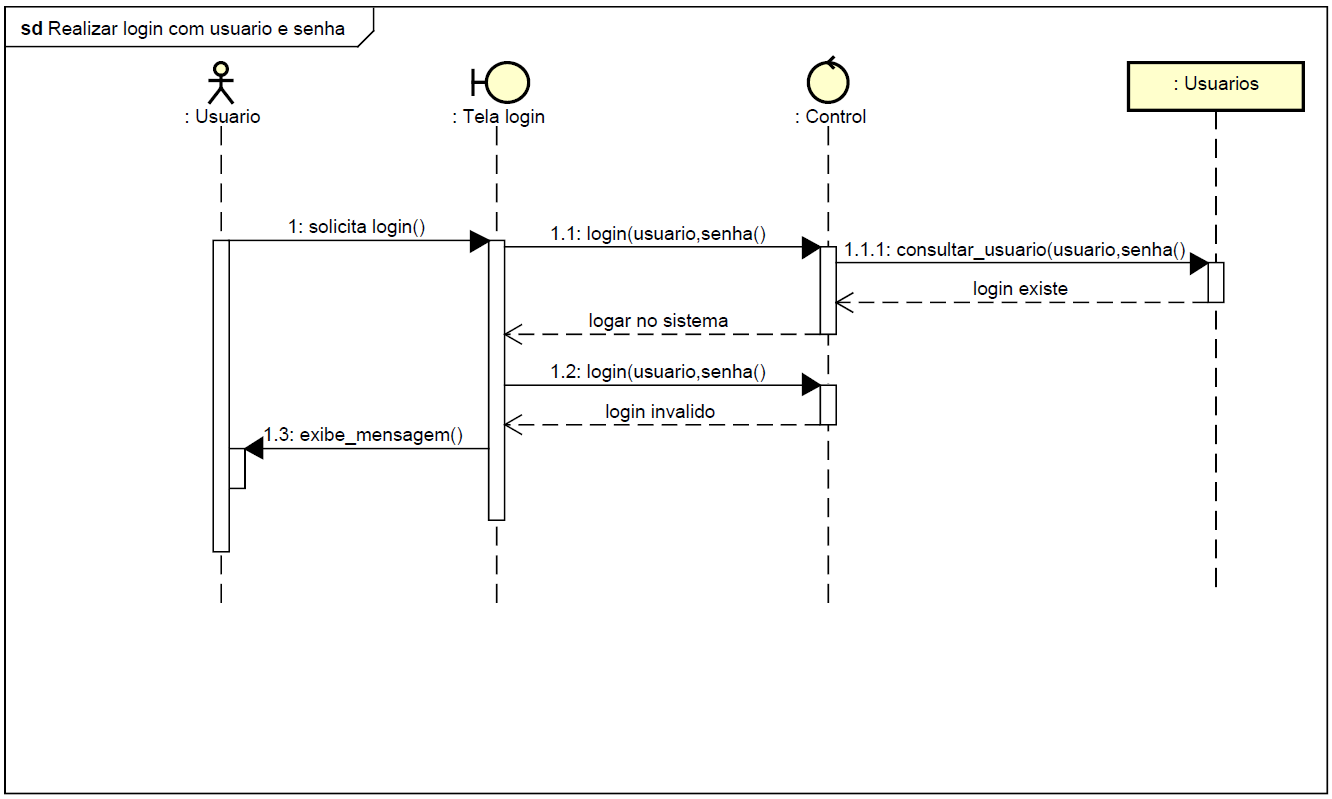
* + 1. Diagrama de classe

Figura 13 – Diagrama de Classe – SISCVC

* + 1. Diagrama de sequência
       1. Diagrama de sequência – Login com usuário e senha

No diagrama abaixo é possível acompanhar o fluxo da operação realizar login com usuário e senha no software.

Figura 14 - Diagrama de sequência – Login com usuário e senha

* + - 1. Diagrama de sequência – Login com certificado

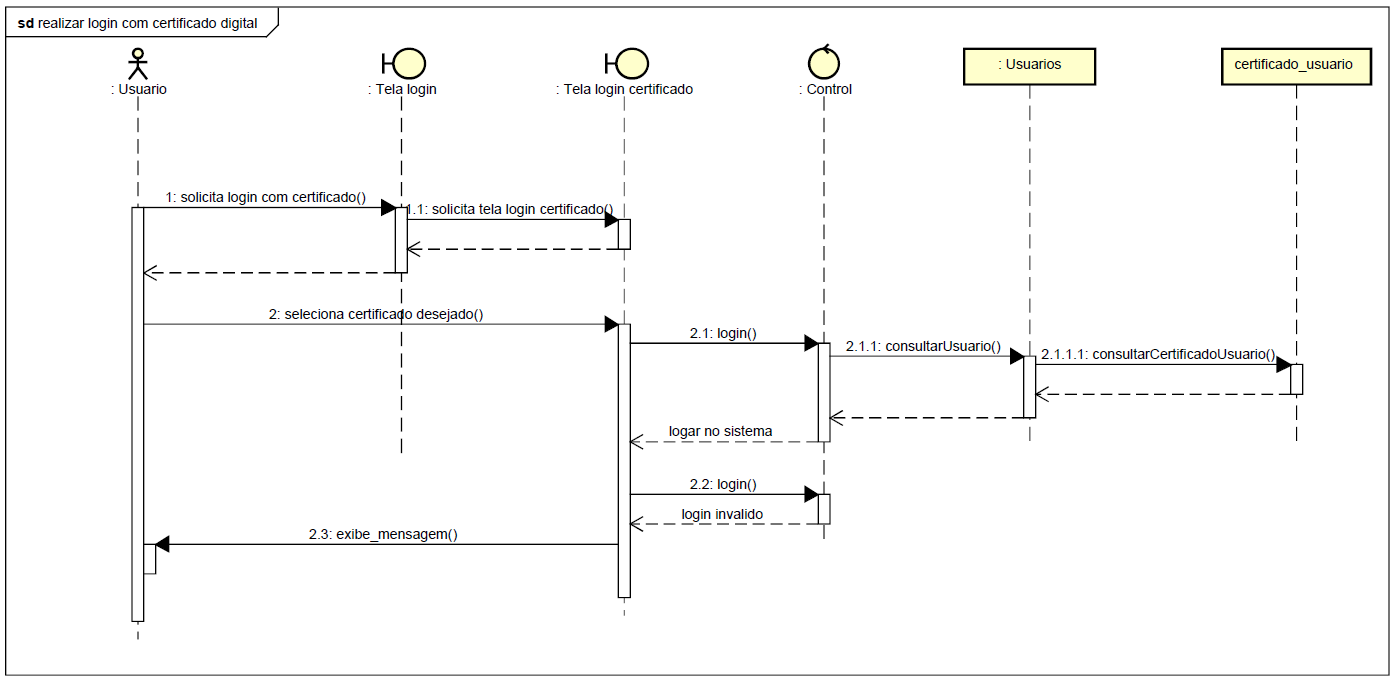
No diagrama abaixo é possível acompanhar o fluxo da operação realizar login com certificado digital no software.

Figura 15 - Diagrama de sequência – Login com certificado

* + - 1. Diagrama de sequência – Cadastro de usuário

No diagrama abaixo é possível acompanhar o fluxo da operação para realizar cadastro de usuário no software.

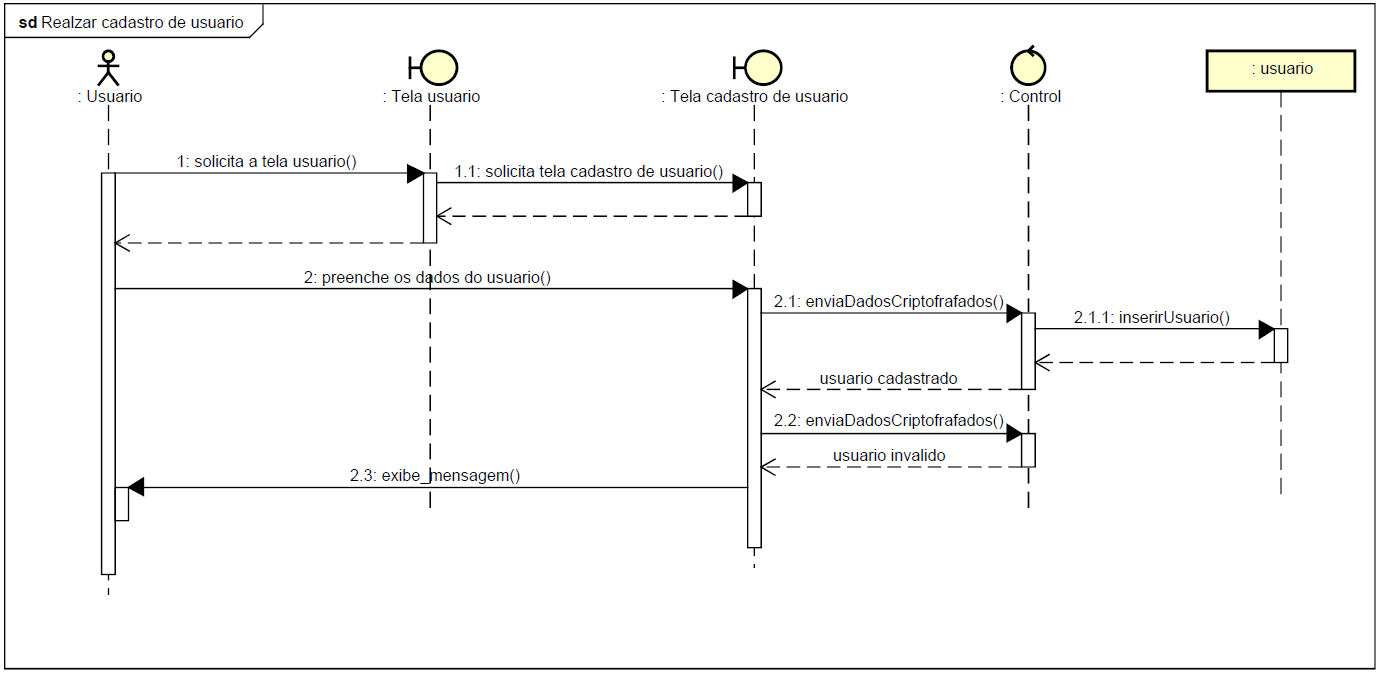


Figura 16 - Diagrama de sequência – Cadastro de usuário

* + - 1. Diagrama de sequência – Consultar, alterar e excluir usuário

No diagrama abaixo é possível acompanhar o fluxo da operação de realizar consulta, alteração e exclusão de usuários no software.

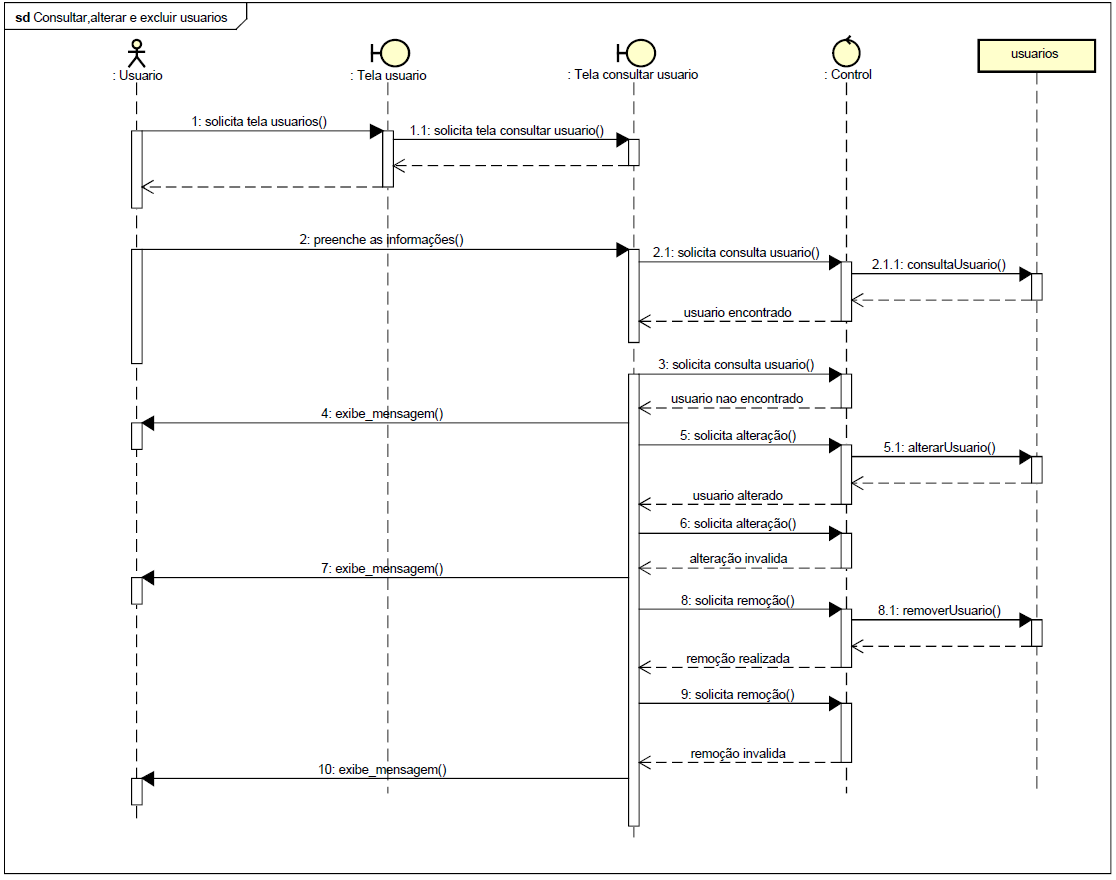


Figura 17 – Diagrama de sequência – Consultar, alterar e excluir usuário

* + - 1. Diagrama de sequência – Cadastro do certificado do usuário

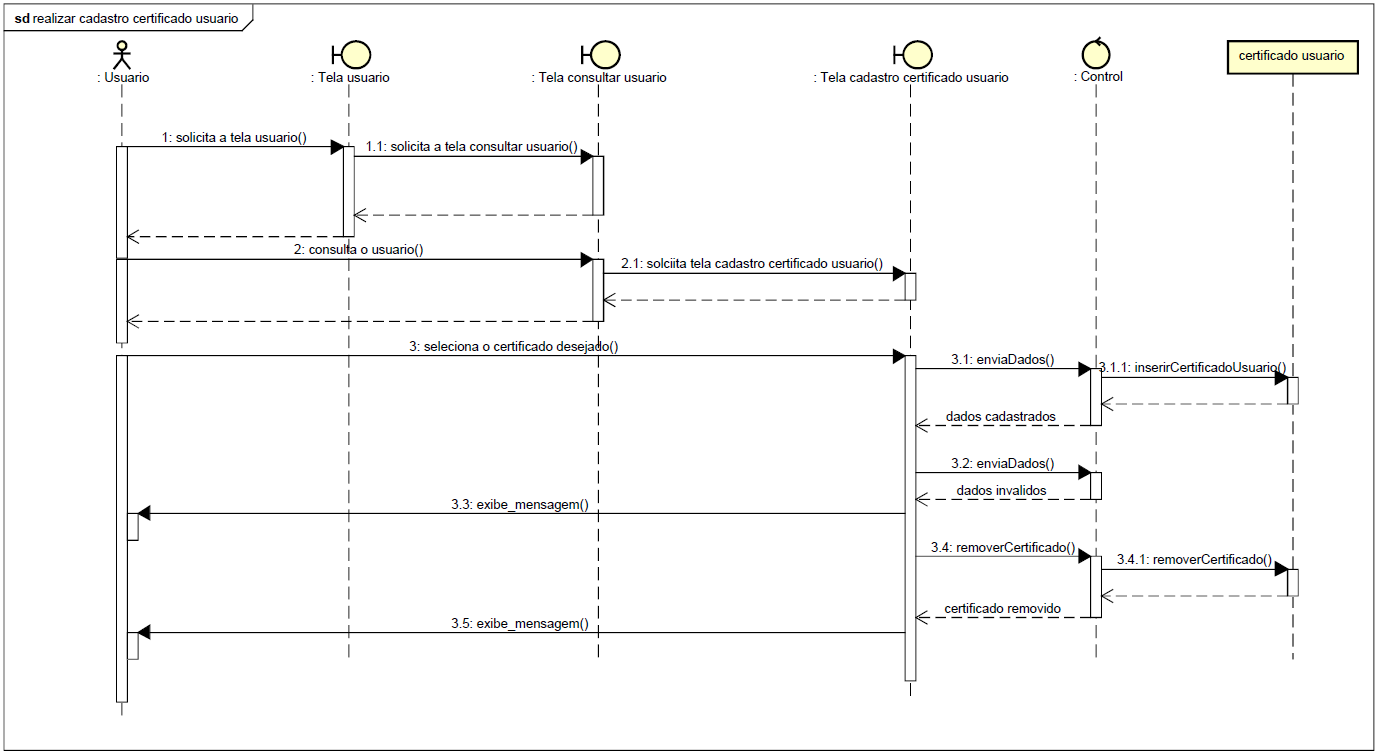
No diagrama abaixo é possível acompanhar o fluxo da operação de realizar cadastro de certificado digital do usuário.

Figura 18 – Diagrama de sequência – Cadastro do certificado ao usuário

* + - 1. Diagrama de sequência – Cadastro de cliente

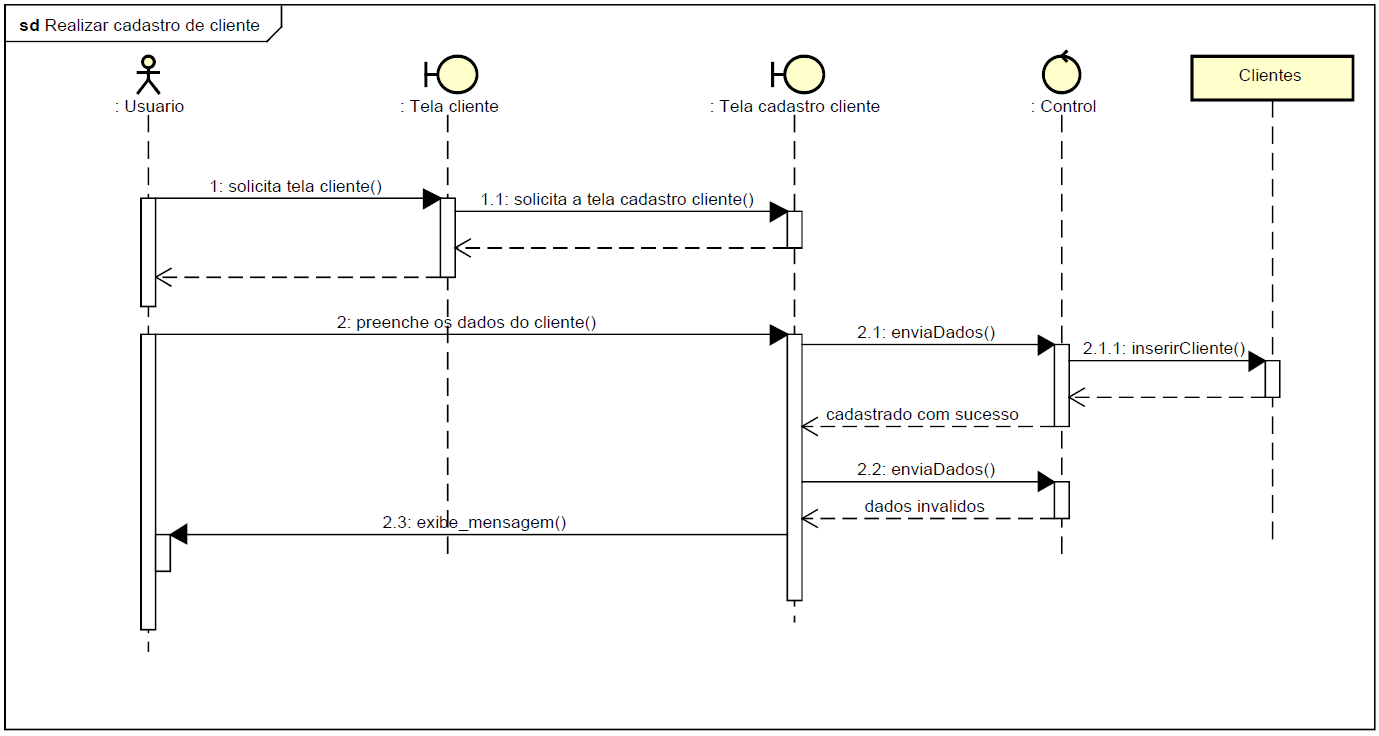
No diagrama abaixo é possível acompanhar o fluxo da operação de realizar cadastro de cliente.

Figura 19 - Diagrama de sequência – Cadastro de cliente

* + - 1. Diagrama de sequência – Consultar, alterar e excluir cliente

No diagrama abaixo é possível acompanhar o fluxo da operação de realizar consulta, alteração e exclusão de clientes no software.

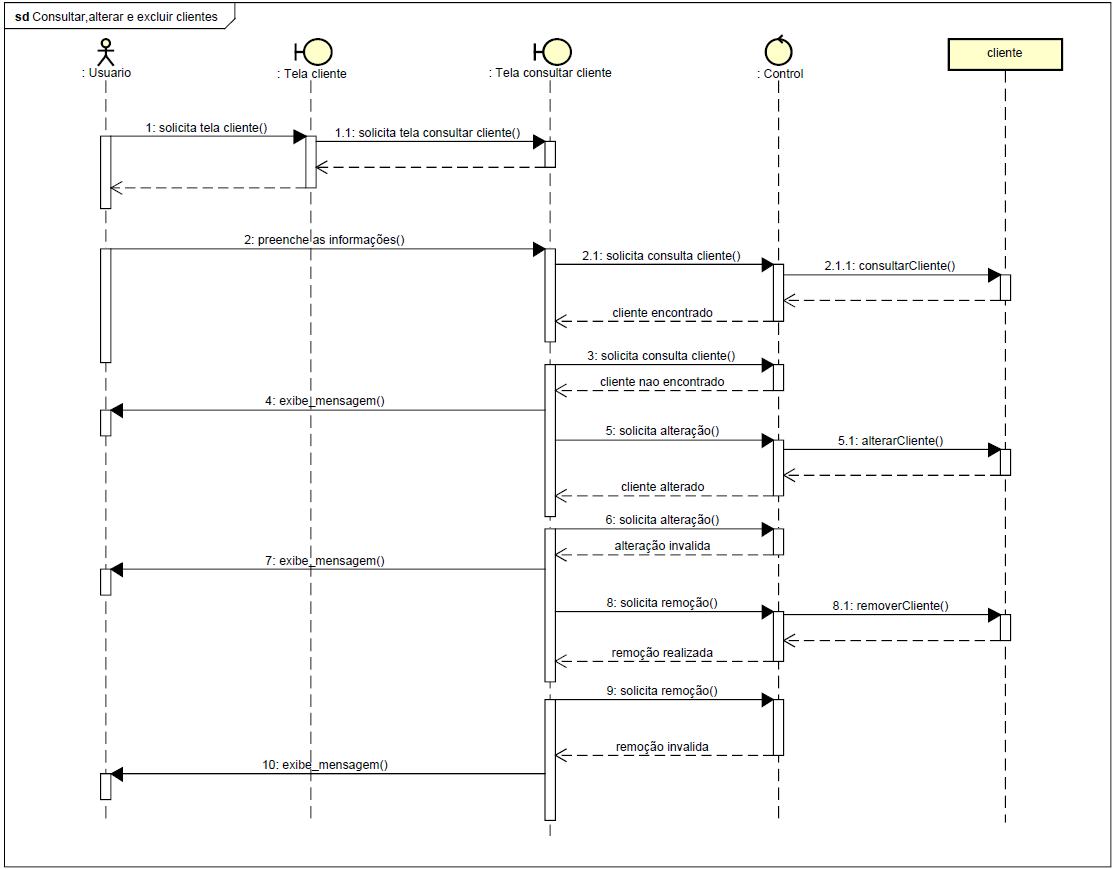


Figura 20 – Diagrama de sequência – Consultar, alterar e excluir cliente

* + - 1. Diagrama de sequência – Cadastro de certificado para o cliente

No diagrama abaixo é possível acompanhar o fluxo da operação de realizar cadastro de certificado digital para o cliente.

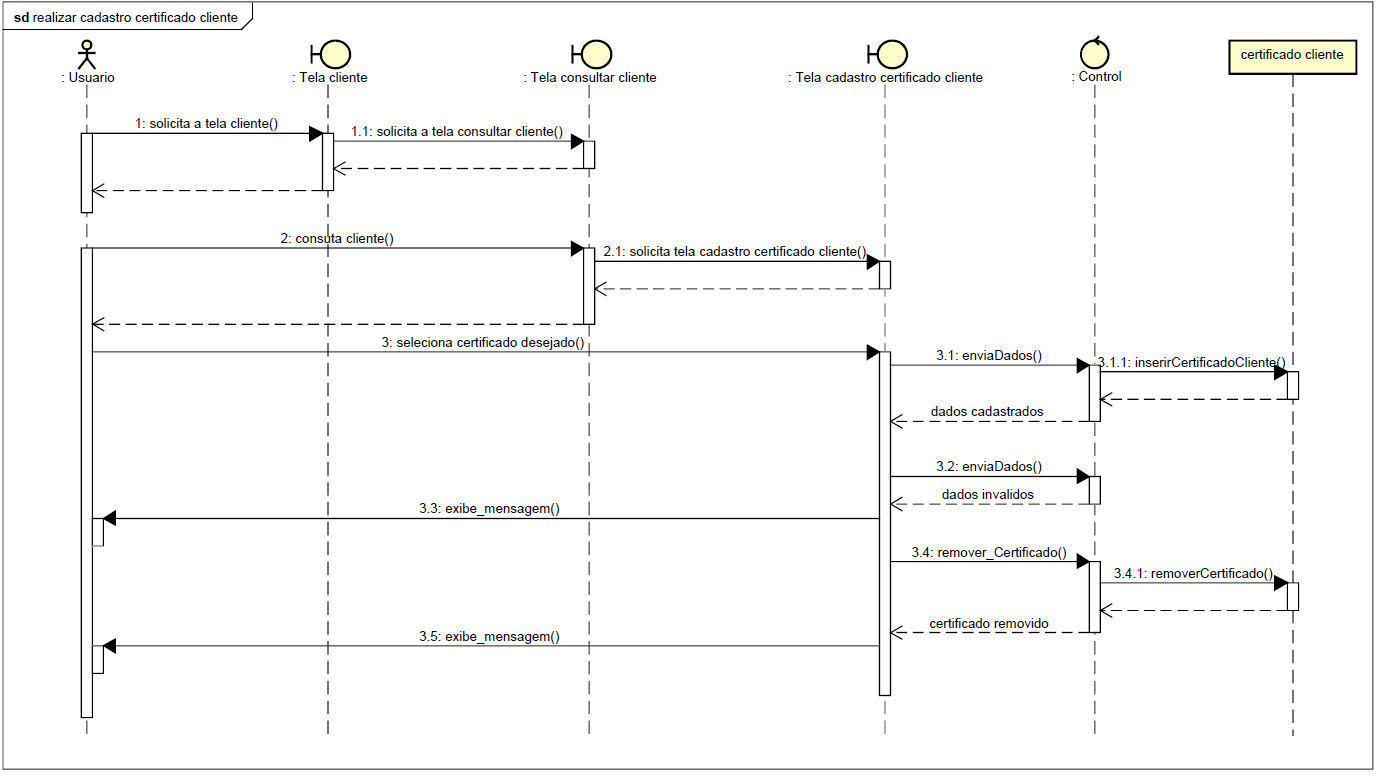


Figura 21 – Diagrama de sequência – Cadastro de certificado para o cliente

* + - 1. Diagrama de sequência – Monitoramento do prazo de validade

No diagrama abaixo é possível acompanhar o fluxo da operação de como o software realiza o monitoramento dos certificados dos clientes cadastrados no banco de dados, e notifica via e-mail os usuários e clientes.

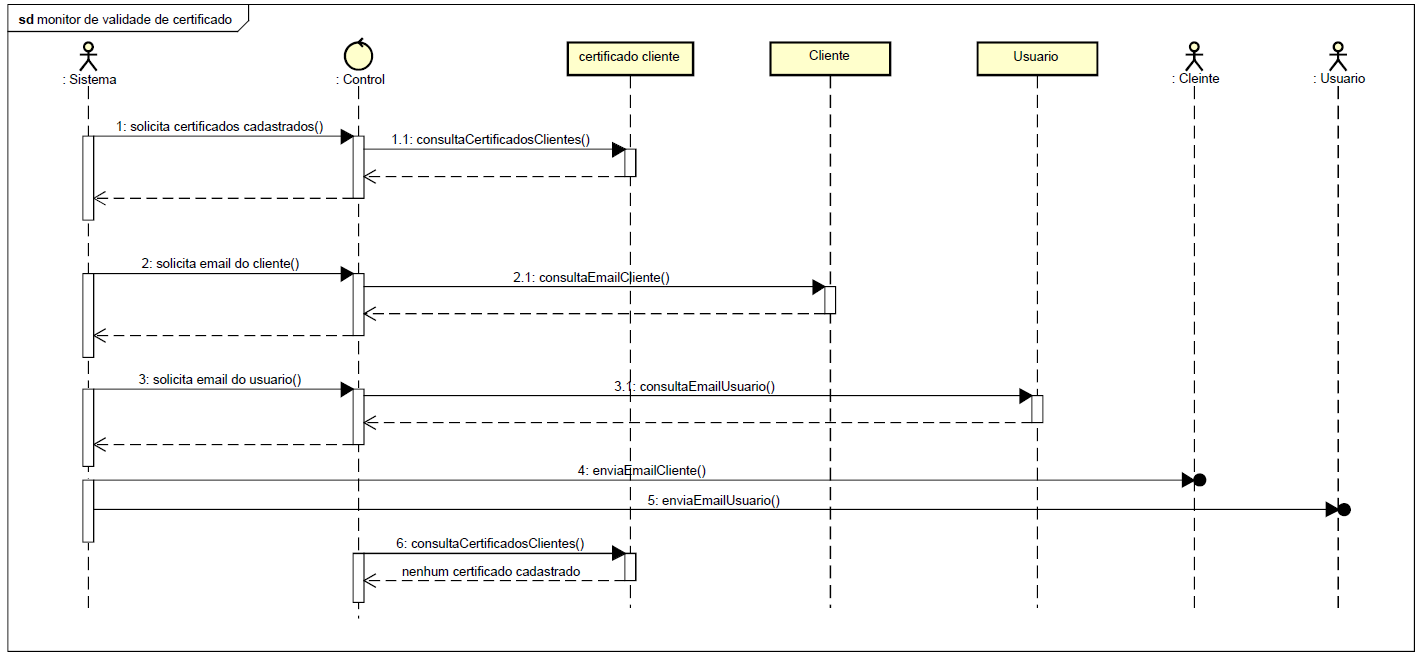


Figura 22 – Diagrama de sequência – Monitoramento do prazo de validade

1. CONCLUSÃO

Após uma vasta experiência adquirida na área da certificação digital e por presenciar diversas vezes os problemas apresentados pelos cidadãos e empresas, identificamos a necessidade de um software, onde o usuário conseguirá controlar a validade dos certificados digitais e não ser prejudicado devido as obrigatoriedades impostas pelo governo.

O software desenvolvido denominado de SisCVC, realiza o monitoramento dos certificados dos clientes que estão cadastrados no banco de dados, todos os dias em um horário definido, de acordo com opção marcada pelo usuário, sendo elas 1,15 e 30 dias antes do certificado expirar. Após o monitoramento, o mesmo notifica via e-mail os clientes referentes aos certificados que estão próximo de expirar e os usuários.

Como requisito do software, foram aplicados conceitos matemáticos da criptografia simétrica, baseando no algoritmo que criamos.

Este algoritmo foi desenvolvido com objetivo de melhorar a segurança nos tipos acessos, pois ao cadastrar um usuário no software, a senha é imediatamente criptografada, antes de ser inserida no banco de dados e descriptografada somente ao realizar a autenticação no software, validando se a senha está correta.

Para desenvolver o software, utilizamos a linguagem de programação Java que é projetada em orientação a objeto. A mesma é representada por uma coleção de componentes como, bibliotecas, classes e interface. Na interface utilizamos a ferramenta Swing.

O banco de dados utilizado foi o MySQL, devido à grande facilidade na programação, funções simples e na manipulação de dados.

Na implementação do algoritmo houve a dificuldade de encontrar a forma de criptografar a senha, pois ao definir a chave tivemos que realizar algumas operações matemáticas, para que a mesma fosse criptografada e descriptografada de forma correta utilizando a chave definida.

Mediante tudo que foi estudado, pode-se afirmar que o certificado na sua essência veio para facilitar e modificar o cotidiano das pessoas e se tornou uma tecnologia essencial para toda população nos dias atuais. Com o seu crescimento e com uma visão futura, pode-se afirmar que cada cidadão e empresas, realizarão diversas transações na internet com segurança. Assim, será indispensável o uso e controle da sua identidade digital.

Com os conhecimentos adquiridos nas disciplinas de redes, linguagem de programação e banco de dados, conseguimos aplicar os conceitos matemáticos da criptografia simétrica para criptografar e descriptografar dados. Consequentemente conseguimos aumentar a confidencialidade, autenticidade e integridade das informações que são inseridas no banco de dados, dificultando acesso as informações na base de dados.

O software desenvolvido foi projetado com uma alta usabilidade, de forma que os usuários não terão dificuldades em utilizar nenhuma das funcionalidades.

REFERÊNCIAS BIBLIOGRÁFICAS

ASCENCIO, A. F. G; CAMPOS, E. A. V. Fundamentos da programação de computadores: algoritmos, PASCAL, C/C++ (padrão ANSI) e JAVA, 3. ed. São Paulo: Pearson, 2012.

BOOCH, G; RUMBAUGH, J; JACOBSON, I. **UML Guia do Usuário**, 2ª

Edição, tradução de Fabio Freitas da Silva e Cristina de Amorim Machado -

Rio de Janeiro, Editora: Campus, 2005.

CARISSIMI, A. S; ROCHOL, J; GRANVILLE, L. Z. **Redes de Computadores**.

Porto Alegre: Bookman, 2009.

DANTAS, M. **Tecnologia de Redes de Comunicação e Computadores**. Rio

de Janeiro: Axcel Books, 2002.

ELMASRI R.; NAVATHE S.B. **Sistemas de Banco de Dados**. Tradução

Daniel Vieira. 6. ed. São Paulo: Pearson Addison Wesley, 2011.

GALVÃO, M. C. **Fundamentos em segurança da informação**. São Paulo,

Ed. Pearson, 2015.

GUEDES, G. T. A. **UML 2: uma abordagem prática**. São Paulo, Ed. Novatec, 2009. HEUSER, C. A. **Projeto de Banco de Dados**. 6. Porto Alegre: Bookman, 2009.

HUANG, W.; SIAU, K.; WEI, K. K. **Electronic government strategies and**

**Implementation.** Hershey: Idea GroupPublishing, 2005.

LIMA, P. M. F. **Crimes de computador e segurança computacional**.

Campinas SP, 2006.

MACHADO, F. N. R; ABREU, M. P. **Projeto de Banco de Dados:** uma visão

prática. 16. São Paulo: Érica, 2009.

MAXFIELD, Wade. **Aprendendo MySQL e PHP**. 1.ed. Ed. Makron. 2002.

NAKAMURA, T. E; GEUS, L. P. **Segurança De Redes Em Ambientes**

**Cooperativos**.1. ed. São Paulo: Novatec, 2007.

OLIVEIRA, R. R. Criptografia simétrica e assimétrica: os principais algoritmos

de cifragem. **Revista Segurança Digital**, [on-line], v. 05, p. 13, mar. 2012;

Disponível em <https://www.researchgate.net/publication/303367222\_

Criptografia\_simetrica\_e\_assimetrica\_os\_principais\_algoritmos\_de\_cifragem>

Acesso em: 14 out, 2018

PENDER, Tom. **UML, a Bíblia**, Tradução Daniel Vieira - Rio de Janeiro:

Ed. Campus, 2004.

SETZER, V. W. **Banco de Dados:** conceitos, modelos, gerenciadores, projeto

logico, projeto físico. 3. São Paulo: Blucher, 1989.

SQL SERVER. **O que é SQL Server**. Disponível em: Acesso: 27 set. 2000.

TREVISAN, F. D; SACHI, P. S. R; SANABRIA, L. Estudo do padrão avançado

De criptografia aes – advanced encryption standard. **Revista de Informática**

**Teórica e Aplicada (RITA)**, [on-line], v. 20, n. 1, p. 13-24, 2013. Disponível

em: <http://seer.ufrgs.br/index.php/rita/index>. Acesso em: 18 set. 2015.

VOLPI, Marlon Marcelo. **Assinatura Digital – Aspectos Técnicos, Práticos**

**e Legais**. Rio de Janeiro, Ed. Axcel Books, 2001.