**FACULDADE CNEC CAMPO LARGO**

**BACHARELADO EM SISTEMAS DE INFORMAÇÃO**

**HELENA MAURA CARVALHO**

**LUCCAS MONTEIRO FONSECA**

**SISTEMA PARA CONTROLE DE DOCUMENTAÇÃO DE ALUNOS DA FACULDADE CNEC DE CAMPO LARGO**

**CAMPO LARGO**

**2016**

**HELENA MAURA CARVALHO**

**LUCCAS MONTEIRO FONSECA**

**SISTEMA PARA CONTROLE DE DOCUMENTAÇÃO DE ALUNOS DA FACULDADE CNEC DE CAMPO LARGO**

Planejamento de Pesquisa apresentado ao Curso de Sistemas de Informação da Faculdade CNEC de Campo Largo, como requisito parcial para a obtenção do grau de Bacharel em Sistemas de Informação. Orientador: Prof. Edjalma C. Ferreira

**CAMPO LARGO**

**2016**

**SIGLAS**

SQL - Structured Query Language

IDE - Integrated Development Environment

SGBD - Sistema Gerenciador de Banco de Dados

ORM - Object Relational Mapper

PO - Product Owner

UML - Unified Modeling Language

**SUMÁRIO**

[1. INTRODUÇÃO 6](#_Toc465277199)

[2. PROBLEMA 8](#_Toc465277200)

[3. OBJETIVOS 9](#_Toc465277201)

[3.1. OBJETIVO GERAL 9](#_Toc465277202)

[3.2. OBJETIVOS ESPECÍFICOS 9](#_Toc465277203)

[4. JUSTIFICATIVA DO PROJETO 10](#_Toc465277204)

[5. METODOLOGIA 12](#_Toc465277205)

[6. PESQUISA 13](#_Toc465277206)

[7. REVISÃO DE LITERATURA 14](#_Toc465277207)

[7.1. Requisitos 14](#_Toc465277208)

[7.2. Linguagem de desenvolvimento 18](#_Toc465277209)

[7.3. Banco de dados 18](#_Toc465277210)

[7.4. ORM 19](#_Toc465277211)

[7.5. Diagrama de caso de uso 19](#_Toc465277212)

[8. SEGURANÇA 21](#_Toc465277213)

[8.1. Autenticação 21](#_Toc465277214)

[8.2. Criptografia 21](#_Toc465277215)

[9. INTERFACE 23](#_Toc465277216)

[10. CRONOGRAMA 24](#_Toc465277217)

[REFERÊNCIAS 26](#_Toc465277218)

[APÊNDICE A – Diagrama de casos de uso 28](#_Toc465277219)

[APÊNDICE B – Tela de Login 29](#_Toc465277220)

[APÊNDICE C – Tela de Boas Vindas (Coordenação) 30](#_Toc465277221)

[APÊNDICE D – Tela de Documentos de alunos 31](#_Toc465277222)

[APÊNDICE E – Tela de Cadastro de Documentos 32](#_Toc465277223)

[APÊNDICE F – Tela de Solicitação de Documentos 33](#_Toc465277224)

[APÊNDICE G – Tela de Nova Solicitação 34](#_Toc465277225)

[APÊNDICE H – Tela de Acompanhamento da Solicitação de Documentos 35](#_Toc465277226)

[APÊNDICE I – Tela de Controle de Eventos 36](#_Toc465277227)

[APÊNDICE J – Tela de Cadastro de Novos Eventos 37](#_Toc465277228)

[APÊNDICE K – Tela de Meus Eventos (aluno) 38](#_Toc465277229)

# INTRODUÇÃO

Seja por influência de um pensamento ecologicamente correto, pela limitação de espaço físico ou pela necessidade de agilidade na obtenção de informações, é cada vez mais comum a opção pelo armazenamento digital de documentos. Segundo Arellano (2004), “o suporte físico da informação, o papel e a superfície metálica magnetizada se desintegram ou podem se tornar irrecuperáveis”, ou seja, além de despender de grandes instalações para o armazenamento físico de arquivos, estamos sujeitos à degradação dos mesmos, o que resultaria na perda de informações.

É preciso que saibamos que, apesar de benefícios como agilidade na obtenção de documentos, indexação de informações, redução de espaço físico dedicado à manutenção dos arquivos, entre outros, temos que nos atentar à preservação da integridade de tais informações. Por mais que a preocupação com autenticidade e integridade de documentos seja abordada como consequência da digitalização dos mesmos, “a preocupação com a autenticidade de documentos sempre existiu, apenas ganhou mais atenção devido à vulnerabilidade e à facilidade com que documentos digitais podem ser alterados sem que, em alguns casos, sejav possível identificar tal modificação” (CORRÊA, 2010). Conforme o artigo 27 da Lei 12.682 (BRASIL, 2012), “o processo de digitalização deverá ser realizado de forma a manter a integridade, a autenticidade e, se necessário, a confidencialidade do documento digital, com o emprego de certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira - ICP - Brasil” e “os meios de armazenamento dos documentos digitais deverão protegê-los de acesso, uso, alteração, reprodução e destruição não autorizados”.

Como uma forma de facilitar o armazenamento e controle das documentações dos alunos da instituições, propõe-se o desenvolvimento de um sistema destinado a armazenar os diversos documentos dos alunos, permitindo que estes sejam acessados rapidamente pelas partes interessadas, além de prover aos estudantes informações em tempo real sobre o cumprimento de cargas horárias de atividades complementares, atividades de estágios, bem como acompanhar o status e o andamento de requisições de documentação da instituição. Por se tratar de um software muito pontual e que atenda especificamente às necessidades da instituição selecionada (Faculdade CNEC de Campo Largo), não atentamos para a existência de produtos similares no mercado.

# PROBLEMA

Quanto tempo desperdiçamos no nosso dia-a-dia com processos repetitivos e desnecessários como procurar manualmente um arquivo numa pilha de documentos, simplesmente para descobrir que a informação desejada não se encontra lá? Quanto tempo poderíamos economizar com estas tarefas e dedicar a atividades mais importantes e que realmente requerem nosso esforço e atenção?

E se pudéssemos implementar um sistema informatizado cujo objetivo fosse facilitar a gestão dos documentos e, além disso, reduzir o gasto de papel e espaço necessário para armazenamento físico de documentos, diminuindo também o risco de degradação de tais arquivos?

# OBJETIVOS

## OBJETIVO GERAL

Desenvolvimento de um software para controle e armazenamento de documentação de alunos, facilitando a obtenção destes documentos e permitindo rápido acesso aos mesmos.

## OBJETIVOS ESPECÍFICOS

1. Organizar os documentos dos alunos por pastas, considerando curso e tipo de documento, facilitando o acesso aos arquivos;
2. Permitir a abertura de requisição de documentos para os alunos;
3. Permitir aos alunos realizar requisição de horas complementares online, anexando um documento comprobatório posteriormente validado pelo coordenador do curso;
4. Permitir a manutenção de eventos e a inscrição dos alunos nestes, sendo que caso tenham presença confirmada, seja gerado automaticamente certificado e horas complementares;

# JUSTIFICATIVA DO PROJETO

O projeto será desenvolvido para facilitar o controle de documentação dos alunos, além de oferecer uma alternativa ágil para controle de horas de atividades complementares e estágios, permitindo que o aluno acompanhe a qualquer momento a necessidade de carga horária em atividades extraclasse, evitando que se acumule para o final do curso.

Além da agilidade, o projeto proporcionará também a proteção dos documentos dos alunos contra danos e extravio, pois, segundo Arellano (2004), há vários fatores que colocam em risco a integridade de arquivos físicos, como “os efeitos da temperatura, umidade, nível de poluição do ar e das ameaças biológicas; os danos provocados pelo uso indevido e o uso regular, as catástrofes naturais e a obsolescência tecnológica”.

A instituição de ensino para a qual este projeto está sendo direcionado, sofreu em 2014 grandes prejuízos causados por um desastre natural que assolou parcialmente a cidade de Campo Largo, sendo decretado estado de emergência na região. Conforme relata o jornal Folha de Campo Largo, “A chuva de granizo, com pedras que chegaram a quase seis centímetros de diâmetro, destruiu e destelhou milhares de casas e estabelecimentos comerciais em Campo Largo”. Os danos materiais foram muitos e o risco de perda de documentos importantes em uma situação de alagamento como esta é inegável.

Se pensarmos pelo ponto de vista financeiro, vemos um outro bom motivo para a informatização de um ambiente, segundo Sarantis (2002), “papel é algo que, praticamente, toda empresa utiliza em grandes quantidades. Atualmente, cerca de 90% de todas as informações do negócio estão em formato impresso. Este uso é tão comum que, geralmente, não é questionado”, ela ainda afirma que “os gastos com papéis vão além de apenas comprar o papel. Existem também custos associados ao armazenamento, perda de documentos, postagem, obsolência e ineficiência no trabalho”. Outro tópico abordado pela autora supracitada é sobre a consciência ambiental, segundo ela “da mesma forma que o uso de papeis esconde efeitos negativos na eficiência do trabalho, o impacto ambiental causa por ele pode também não ser óbvio. Todos os passos envolvidos na fabricação do papel - extração da madeira, processamento, produção, transporte, uso e descarte - contribuem significantemente para mudanças ambientais”.

# METODOLOGIA

Para estabelecer o escopo e os requisitos do projeto, foram feitas entrevistas com o P.O. com o intuito de conhecer as necessidades da instituição em relação a armazenamento de arquivos e requisições de horas complementares.

Segundo Denis Rezende (2005, p. 162 a 164), a entrevista é a técnica mais recomendada para levantamento de dados, sendo que uma das vantagens citada por ele é que ela pode ser informal, deixando o entrevistado a vontade, “fornecendo, desse modo, importantes informações que dificilmente seriam obtidas mediante o emprego de outra técnica de levantamento”.

# PESQUISA

# REVISÃO DE LITERATURA

## Requisitos

Os requisitos, segundo Sommerville (2007, p. 79), podem ser definidos como “descrições dos serviços fornecidos pelo sistema e as suas restrições operacionais. ”, ele ainda completa dizendo que estes requisitos “refletem as necessidades dos clientes de um sistema que ajuda a resolver algum problema”.

Ainda de acordo com Sommerville (2007, p. 80), os requisitos do sistema são comumente divididos em requisitos funcionais, não funcionais e de domínio.

#### Requisitos Funcionais

Os requisitos funcionais, poder ser descritos, conforme Denis Rezende (2005, p. 123) como “as funções ou atividades que o software ou sistema faz (quando pronto) ou fará (quando em desenvolvimento) ”. Rezende ainda comenta que estes requisitos são muito importantes e que podem evitar manutenções no sistema.

Considerando estas colocações, foram observados os seguintes requisitos funcionais:

* RF01: Controlar acesso por perfis - O sistema deve prever três tipos de perfis de usuário, sendo eles Coordenador, Secretaria e Aluno, respeitando as seguintes permissões:
  + Coordenador: Manutenção de documentos de alunos, cadastro de tipos de documentos, manutenção de eventos, validação de presença em eventos, aprovação de requisição de horas complementares, manutenção de solicitação de documentos.
  + Secretaria: Manutenção de documentos de alunos, cadastro de tipos de documentos, manutenção de solicitação de documentos.
  + Aluno: Inscrição em eventos, visualização de requisições de horas complementares, atender solicitações de envio de documentos.
* RF02: Efetuar login - Permitir o login no sistema utilizando a senha de rede da instituição identificando o tipo de perfil neste momento.
* RF03: Manter cursos - O sistema deve permitir que a Secretaria e a Coordenação possam manter os cursos oferecidos na instituição, que servirão como meio de facilitar que os arquivos de determinado aluno sejam localizados.
* RF04: Manter tipo de documento - O sistema deve permitir que a Secretaria e a Coordenação possam manter os tipos de documentos dos alunos.
* RF05: Realizar upload de documento - O sistema deve permitir que a Secretaria e a Coordenação realizem o upload de documentos de alunos, organizando de acordo com o tipo de documento, curso e aluno.
* RF06: Filtrar documentos - O sistema deve permitir que a Secretaria e a Coordenação realizem o filtro dos documentos adicionados de cada aluno, considerando o curso, o tipo de documento e nome do aluno.
* RF07: Realizar download de documentos - O sistema deve permitir que a Secretaria e a Coordenação realizem o download de documentos de alunos.
* RF08: Solicitar documentos - O sistema deve permitir que a Secretaria e a Coordenação abram solicitações de documentos aos alunos, informando o tipo de documento, o prazo e uma descrição.
* RF09: Notificar sobre abertura de solicitação - Quando uma solicitação de documento for aberta, o sistema deve notificar o (s) aluno (s) via e-mail, enviando o link do sistema para que a solicitação seja atendida.
* RF10: Atender solicitação - O sistema deve permitir que um Aluno atenda uma solicitação de documentos, anexando o arquivo correspondente.
* RF11: Verificar atendimento de solicitação - O sistema deve permitir que a Secretaria aprove ou reprove um atendimento de solicitação, verificando o documento enviado pelo aluno.
* RF12: Aprovar atendimento de solicitação - Caso a solicitação seja aprovada, o documento é organizado de acordo com o curso, tipo de documento e aluno e fecha a solicitação.
* RF13: Reprovar atendimento de solicitação - Caso a solicitação seja reprovada, o sistema envia uma notificação ao aluno via e-mail informando da decisão com uma observação inserida pela Secretaria, mantendo a solicitação pendente.
* RF14: Manter eventos - O sistema deve permitir que a Coordenação possa manter eventos, informando a descrição, data e hora de início e fim, local, quantidade de horas e podendo relacionar com um ou mais cursos. A edição/cancelamento pode ser realizada apenas se o status do evento for “em aberto”.
* RF15: Notificar sobre criação de evento - Quando algum evento possua cursos relacionados o sistema deve disparar um e-mail para os alunos matriculados nestes cursos, informando da criação do evento e o link para inscrição.
* RF16: Realizar inscrição em evento - O sistema deve permitir que usuários do tipo Aluno realizem a inscrição em eventos que estejam com status em aberto.
* RF17: Cancelar inscrição - Caso o evento esteja com status em aberto, o sistema deve permitir que usuários do tipo Aluno que já tenham realizado sua inscrição possam cancelá-la.
* RF18: Alterar status de evento - O sistema deve atualizar o status do evento para “Em andamento”, quando o horário atual estiver entre o horário de início e fim do evento. Quando o horário atual for maior que o horário de fim, o evento deve ser atualizado para status “Finalizado”.
* RF19: Confirmar participação em evento - O sistema deve permitir que a Coordenação possa confirmar a presença dos alunos que realizaram a inscrição.
* RF20: Emitir certificado - Quando a participação de um aluno for confirmada, o sistema deve gerar um certificado para o aluno, armazená-lo automaticamente em sua pasta no sistema e enviá-lo para o e-mail do aluno informando que sua participação foi confirmada.
* RF21: Recusar participação - Caso a Coordenação recuse a participação de um aluno no evento, um e-mail para o aluno deve ser disparado informando da decisão.
* RF22: Emitir requisição de horas complementares - O sistema deve permitir que um usuário do tipo Aluno realize a requisição de horas complementares, preenchendo online um formulário de requerimento conforme o padrão da instituição e anexando documento comprobatório.
* RF23: Validar solicitação de horas complementares - O sistema deve permitir que o usuário do tipo Coordenação referente ao curso no qual o aluno está matriculado valide a requisição de horas complementares, podendo aprová-la ou reprová-la.
* RF24: Aprovar solicitação de horas complementares - Caso a solicitação seja aprovada pela Coordenação, o documento comprobatório deve ser armazenado na pasta do aluno e as horas complementares computadas pelo sistema.
* RF25: Reprovar solicitação de horas complementares - Caso a solicitação seja reprovada pela Coordenação, o sistema deve disparar um e-mail para o aluno informando da decisão.

#### Requisitos Não Funcionais

Em concordância com Sommerville (2007, p.80 a 81), os requisitos não funcionais são “restrições sobre os serviços ou as funções oferecidas pelo sistema”, ele afirma ainda que eles “aplicam-se, frequentemente, ao sistema como um todo. Em geral, eles não se aplicam às características ou serviços individuais de sistema”.

Tendo esta definição em mente, foram levantados os seguintes requisitos não funcionais:

* RNF01: Tamanho máximo de arquivos - O sistema deve realizar o upload de arquivos com até no máximo 2MB.
* RNF02: Extensões de arquivos aceitos - O sistema deve realizar o upload apenas de arquivos com a extensão .pdf.

#### Requisitos de Domínio

Os requisitos de Domínio, de acordo com Sommerville (2007, p. 84 a 85), “são derivados do domínio da aplicação do sistema, e, vez das necessidades específicas dos usuários do sistema”, ele ainda acrescenta que estes requisitos são fundamentais porque “se esses requisitos não forem satisfeitos, pode ser impossível fazer o sistema funcionar satisfatoriamente”.

Para o funcionamento do sistema fazem se necessários os seguintes requisitos:

* RD01: Armazenamento - Servidor de arquivos conectado à internet, com velocidade mínima de 56 Kbps;
* RD02: Compatibilidade de navegador - Os dispositivos que acessarão o sistema devem possuir navegador compatível com Javascript e CSS. Recomendados: Mozilla Firefox, Opera e Google Chrome.
* RD03: Domínio para envio de e-mail - Deve ser criado e disponibilizado um endereço de e-mail para ser utilizado pelo sistema como remetente em notificações.

## **Linguagem de desenvolvimento**

Para a implementação do projeto a IDE escolhida foi o Visual Studio, da Microsoft. Além de ser gratuita para fins acadêmicos, a IDE selecionada oferece suporte a diversas linguagens de programação e plataformas de desenvolvimento web, dentre as quais selecionamos o C# e o ASP.NET MVC. “C# é uma linguagem simples, poderosa, com tipagem segura e orientada a objetos. As várias inovações no C# permitem o desenvolvimento rápido de aplicações, mantendo a expressividade e a elegância do estilo de linguagens C" (VISUAL C#, 2015).

“O ASP.NET é uma plataforma Web que fornece todos os serviços necessários à criação de aplicativos Web baseados em servidor para ambientes corporativos. O ASP.NET foi criado em .NET Framework, de modo que todos os recursos do .NET Framework estão disponíveis nos aplicativos ASP.NET. Seus aplicativos podem ser escritos em qualquer linguagem compatível com CLR (Common Language Runtime), incluindo Visual Basic e C#” (ASP.NET and Visual Studio for Web, 2016).

“O padrão MVC (Model-View-Controller) é um princípio de design arquitetural que separa os componentes de um aplicativo Web. Essa separação dá a você mais controle sobre as partes individuais do aplicativo, que podem ser desenvolvidas, modificadas e testadas com maior facilidade” (Mapa de conteúdo do ASP.NET MVC 4, 2016).

Além de ser a linguagem abordada no decorrer do curso, o C# oferece todos os recursos necessários para o desenvolvimento do sistema proposto.

## **Banco de dados**

As informações geradas pelo sistema em questão, serão armazenadas em um banco de dados. Segundo Date (2000, p.2), “em essência, um sistema de bancos de dados é apenas um sistema computadorizado de armazenamento de registros. O banco de dados pode, ele próprio, ser visto como o equivalente eletrônico de um armário de arquivamento. Em outras palavras, é um repositório ou recipiente para uma coleção de arquivos de dados computadorizados. Os usuários do sistema poderão executar diversas operações sobre tais arquivos“.

Assim como a linguagem de desenvolvimento escolhida, o SGBD selecionado pertence à Microsoft: o SQL Server; isso permite que exista uma integração mais eficiente entre ambos. A escolha foi guiada pelo fato de que, atualmente, este é o SGBD utilizado pela instituição de ensino para a qual o sistema será desenvolvido, mas o intuito é que o sistema permita uma migração da base de dados para outras plataformas, como Oracle ou MySQL.

## **ORM**

As ORM’s são ferramentas utilizadas para persistência de dados que permitem que se faça um mapeamento de objetos do seu sistema em relação ao seu SGBD, tornando a troca de informações entre o sistema e sua base de dados mais simples.

Para o projeto atual, escolhemos o uso do Entity Framework, trata-se de um ORM gratuito, desenvolvido pela própria Microsoft e com integração total à plataforma .Net. “Entity Framework (EF) é um mapeador objeto-relacional que permite aos desenvolvedores .NET trabalhar com dados relacionais utilizando objetos específicos de domínio. Ele elimina a necessidade de os desenvolvedores precisarem escrever a maior parte dos códigos de acesso a dados” (Entity Framework, 2016).

O EF permite que criemos todas as classes do sistema com base num banco de dados já existente, permitindo que a base e o sistema estejam sempre bem alinhados no que se refere a entidades e objetos. O processo inverso, gerar as tabelas do banco de dados a partir de classes já existentes, também é permitido, eliminando a necessidade de codificação em SQL.

## **Diagrama de caso de uso**

O diagrama de casos de uso é um dos principais diagramas do UML. Guedes (2011, p.19) nos dá uma clara definição de UML, segundo ele, UML “é uma linguagem visual utilizada para modelar softwares baseados no paradigma de orientação a objetos. ”, ele completa ainda que o objetivo da UML é “auxiliar os engenheiros de software a definirem as características do sistema”.

Ainda em concordância com Guedes (2011, p. 30), o diagrama de casos de uso “é o diagrama mais geral e informal da UML”, e serve “para que os usuários possam ter uma ideia geral de como o sistema irá se comportar”. No diagrama, são identificados os atores e elencadas as principais funcionalidades do sistema de forma simples e de fácil entendimento.

# SEGURANÇA

## Autenticação

## Criptografia

Quando informações que trafegam no sistema só devem ser conhecidas pelo remetente e pelo destinatário, se faz necessário o uso de uma forma de codificação da informação, a esta, dá-se o nome “criptografia”.

A criptografia acompanha o homem desde os primórdios da escrita e era utilizada para transmissão de mensagens, armazenamento de informações secretas e etc.

As formas atuais de criptografia baseiam-se em chaves criptográficas, um conjunto de bits que, ao ser utilizado por um algoritmo, codificará ou decodificará a informação alvo, ou seja, só quem possui a chave certa é capaz de compreender a mensagem recebida.

#### Objetivos da **criptografia**

A criptografia possui quatro objetivos principais, mas é importante que se saiba que nem sempre o sistema criptográfico é utilizado para atingir todos os objetivos simultaneamente:

* Confidencialidade da informação;
* Integridade da informação;
* Autenticidade do remetente;
* Não-repúdio.

#### Confidencialidade da informação

É importante que a informação seja confidencial, de forma que somente o destinatário portador da chave criptográfica seja capaz de extrair a mensagem da cifra recebida.

#### Integridade da informação

É preciso garantir que a mensagem não seja adulterada no momento entre sua emissão e seu recebimento, ou seja, a mensagem que que foi enviada deve ser a mesma mensagem que será recebida.

#### Autenticidade do remetente

A menos que o remetente opte por manter-se anônimo, o destinatário deverá conseguir identificar de onde a mensagem foi enviada.

#### Não-repúdio

Deve-se garantir que o emissor não seja capaz de negar a autoria da mensagem.

#### Chaves criptográficas

Para que possamos criptografar e descriptografar as informações, precisamos recorrer a cifras, expressões matemáticas que, em conjunto com as chaves, gerarão um texto cifrado.

A segurança de uma chave baseia-se em seu tamanho, definido em bits. Quanto maior uma chave, mais difícil de ser quebrada, pois maiores são as combinações possíveis na tentativa de descoberta daquela chave. Exemplo:

* Chave de 4-bit: é expressa pelo cálculo 24, resultando em 16 possíveis combinações;
* Chave de 8-bit: é expressa pelo cálculo 28, resultando em 256 possíveis combinações;
* Chave de 16-bit: é expressa pelo cálculo 216, resultando em 65.513 possíveis combinações;
* Chave de 32-bit: é expressa pelo cálculo 232, resultando em 4.294.967.296 possíveis combinações;

Existem, basicamente, 2 tipos de chave: simétrica e assimétrica.

#### Chave simétrica

Na criptografia utilizando chave simétrica, tanto a chave para criptografar quando a de descriptografar são exatamente iguais. Alguns algoritmos que utilizam este tipo de chave:

* DES (*Data Encryption Standard*): este algoritmo utiliza chaves de 56-bit;
* RC (*Ron’s Code* ou *Rivest Cipher*): algoritmo utilizado comumente em *e-mails*, utiliza chaves com tamanho entre 8-bit e 1024-bit;
* AES (*Advanced Encryption Standard*): um dos mais populares algoritmos de criptografia, utiliza chaves de 128-bit, 192-bit ou 256-bit;
* IDEA (*International Data Encryption Algorithm*): algoritmo similar ao DES, mas que utiliza chaves de 128-bit.

Apesar de os algoritmos supracitados utilizarem chaves de criptografia relativamente grandes, o poder de processamento de computadores aumenta significantemente com o passar dos anos, ou seja, fica cada vez mais fácil a quebra destas chaves através de algoritmos de força bruta.

#### Chave assimétrica

Diferentemente da criptografia chaves simétricas, esta forma de criptografia utiliza chaves diferentes (assimétricas), mas matematicamente relacionadas. Ou seja, existe uma chave para criptografar (chave pública) e outra para descriptografar (chave privada).

Como o nome sugere, a chave pública pode ser compartilhada, pois serve apenas para criptografar a mensagem, enquanto que a privada deve ser mantida em sigilo, pois é através dela que poderá decifrar o código recebido.

Exemplos de algoritmo que usam chaves assimétricas:

* RSA (*Rivest, Shamir and Adleman*): um dos algoritmos de chave assimétrica mais utilizados, obtém suas chaves através de um cálculo complexo utilizando números primos, quanto maior os números utilizados, mais complexa a chave privada gerada;
* *ElGamal*: gera suas chaves através de “logaritmos discretos”. É comumente utilizada em assinaturas digitais.

#### Aplicações

Atualmente, a grande maioria das operações computadorizadas utilizam algum tipo de criptografia. Desde compras na internet, troca de e-mails, troca de mensagens instantâneas, acesso a *internet banking*, dentre outras atividades.

#### Rijndael

Para o sistema proposto, o algoritmo de criptografia selecionado foi o Rijndael (lê-se rain-dahl). Segundo Joan Daemen e Vincent Rijmen, criadores do algoritmo, “Rijndael é uma cifra iterativa, com blocos e chaves de comprimento variável”, neste algoritmo, pode-se utilizar chaves simétricas de 128-bit, 192-bit ou 256-bit, o que faz com que o algoritmo use um sistema de 9, 11 ou 13 rounds, respectivamente.

O algoritmo Rijndael foi selecionado pelo NIST (Instituto Nacional de Padrões e Tecnologia dos Estados Unidos) como sucessor do método AES.

No sistema proposto, durante o envio do documento, suas informações são criptografadas e o documento armazenado. O documento só será descriptografado novamente no momento em que for solicitado o download do mesmo através do próprio sistema, de forma que, se as bases de dados e os locais de armazenamento forem expostos, dificilmente algum tipo de dado será extraído dos arquivos obtidos.

# INTERFACE

# CRONOGRAMA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Atividades** | **Fevereiro** | **Março** | **Abril** | **Maio** | **Junho** | **Julho** |
| Pesquisa bibliográfica e leituras |  |  |  |  |  |  |
| Entrevista com o orientador |  |  |  |  |  |  |
| Redação parcial dos capítulos |  |  |  |  |  |  |
| Redação do texto final |  |  |  |  |  |  |
| Entrega do texto final |  |  |  |  |  |  |
| Defesa do trabalho |  |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Atividades** | **Agosto** | **Setembro** | **Outubro** | **Novembro** | **Dezembro** |
| Desenvolvimento do projeto |  |  |  |  |  |
| Distribuição de questionários |  |  |  |  |  |
| Complemento do trabalho escrito |  |  |  |  |  |
| Redação do texto final |  |  |  |  |  |
| Entrega do texto final |  |  |  |  |  |
| Defesa do trabalho |  |  |  |  |  |

# REFERÊNCIAS

ARELLANO, Miguel A. **Preservação de documentos digitais**. *Ci. Inf., Brasília*, v. 33, n. 2, p. 15-27, mai/ago. 2004. Disponível em: <<http://revista.ibict.br/ciinf/article/view/1043/1113>>. Acesso em: 11/05/2016.

CORRÊA, Amarílis Montagnolli Gomes. **Preservação digital: autenticidade e integridade de documentos em bibliotecas digitais de teses e dissertações***.* 2010. 98 f. Dissertação (Mestrado em Ciência da Informação) - Universidade de São Paulo, 2010.

BRASIL. **Lei 12682, de 9 de julho de 2012**. Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos. Disponível em <<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Lei/L12682.htm>>. Acesso em: 07/06/2016.

FOLHA DE CAMPO LARGO. **Decretado estado de situação de emergência**. Disponível em <<http://www.folhadecampolargo.com.br/vernoticia.php?id=32702>>. Acesso em: 07/06/2016.

SARANTIS, Heather.***Business Guide to Paper Reduction: A Step-by-Step Plan to Save Money by Saving Paper***. Disponível em <[http://sust63 ainability.tufts.edu/wp-content/uploads/BusinessGuidetoPaperReduction.pdf](http://sustainability.tufts.edu/wp-content/uploads/BusinessGuidetoPaperReduction.pdf)>. Acesso em: 14/06/2016.

**Mapa de conteúdo do ASP.NET MVC 4.** Disponível em <<https://msdn.microsoft.com/pt-br/library/gg416514(v=vs.108).aspx>>. Acesso em: 16/06/2016.

***ASP.NET and Visual Studio for Web***. Disponível em <<https://msdn.microsoft.com/pt-br/library/dd566231.aspx>>. Acesso em: 16/06/2016.

**Visual C#**. Disponível em <<https://msdn.microsoft.com/pt-br/library/kx37x362(v=vs.110).aspx>>. Acesso em: 16/06/2016.

***Entity Framework****.* Disponível em <<https://www.asp.net/entity-framework>>. Acesso em: 16/06/2016.

DATE, C.J. **Introdução a Sistemas de Banco de Dados.** Tradução da 7. ed. americana por Vandenberg D. de Souza. Rio de Janeiro, RJ. Editora Campus, 2005.

REZENDE, Denis Alcides. **Engenharia de Software e Sistemas de Informação.** 3. ed. rev. e ampl.Rio de Janeiro, RJ. Editora Brasport, 2005.

SOMMERVILLE, Ian. **Engenharia de Software.** Tradução por Selma Shin Shimizu Meknikoff, Reginaldo Arakaki, Edílson de Andrade Barbosa; revisão técnica por Kechi Kirama. 8ª edição. São Paulo, SP. Editora Pearson Addison-Wesley, 2007.

GUEDES, Gilleanes T. A.. **UML 2: Uma Abordagem Prática.** 2ª edição. São Paulo - SP. Editora Novatec, 2011.

ROUTO, Terada. **Segurança de dados - criptografia em redes de computador**. Ed. E. Blücher, 2000.

**Rijndael**. Disponível em <<http://searchsecurity.techtarget.com/definition/Rijndael>>. Acesso em: 24/10/2016.

KLEINSCHMIDT, João H. **Segurança da Informação: criptografia simétrica.**  Disponível em <<http://professor.ufabc.edu.br/~joao.kleinschmidt/aulas/seg2013/aula_02-1_seg.pdf>>. Acesso em: 26/10/2016.

DAEMEN, Joan; RIJMEN, Vincent. ***AES Proposal: Rijndael***. 1999. 42 f. Disponível em <<http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf>>. Acesso em: 26/10/2016.

# APÊNDICE A – Diagrama de casos de uso



# APÊNDICE B – Tela de Login



# APÊNDICE C – Tela de Boas Vindas (Coordenação)



# APÊNDICE D – Tela de Documentos de alunos



# APÊNDICE E – Tela de Cadastro de Documentos



# APÊNDICE F – Tela de Solicitação de Documentos



# APÊNDICE G – Tela de Nova Solicitação



# APÊNDICE H – Tela de Acompanhamento da Solicitação de Documentos



# APÊNDICE I – Tela de Controle de Eventos



# APÊNDICE J – Tela de Cadastro de Novos Eventos



# APÊNDICE K – Tela de Meus Eventos (aluno)

