**Universidade Nove de Julho**

**PROJETO PRÁTICO DE PROGRAMAÇÃO**



São Paulo

2014

**Universidade Nove de Julho**

**PROJETO PRÁTICO DE PROGRAMAÇÃO**



<Nome> <RA>

<Nome> <RA>

<Nome> <RA>

<Nome> <RA>

<Nome> <RA>

São Paulo

2014

**Universidade Nove de Julho**

Trabalho de conclusão de semestre apresentado no curso de Tecnologia em Análise e Desenvolvimento de Sistemas, na Universidade Nove de Julho, Campus Memorial.

Orientador: Prof. Ms. Renato Penha

Dedico este trabalho a todos os nossos amigos, familiares e professores que nos ajudaram nessa importante etapa de nossas vidas.

**AGRADECIMENTOS**

Agradeço primeiramente a nossa família que é à base de toda a força e incentivo que nos faz ter vontade de crescer cada vez mais na vida. O nosso Orientador Prof. Ms. Renato Penha pelos pertinentes conselhos e revisões desse trabalho. Aos nossos amigos e colegas, pois a elaboração deste trabalho não teria sido possível sem a colaboração, estímulo e empenho de todos. Por isso gostaria de expressar toda a minha gratidão e apreço a todos aqueles que, direta ou indiretamente, contribuíram para que este trabalho se tornasse uma realidade. A todos quero manifestar os meus sinceros agradecimentos.

Muito obrigado.

“Ser feliz sem motivo é a mais autêntica forma de felicidade”

**Carlos Drummond de Andrade**

**RESUMO**

O conceito deste projeto e mostrar todo o processo que será feito na criação e desenvolvimento de um software voltado para o segmento de transporte publico que será desenvolvido pela empresa CRTLSoftware. O objetivo principal deste software e informatizar a forma de fiscalização feita nos transportes públicos. Desse modo as informações coletas pelos usuários serão transmitidas diretamente para as suas respectivas empresas de transporte de forma mais rápida e segura.

**ABSTRACT**

The concept of this project and show the whole process will be done in producing software aimed at the segment of public transport will be developed by CRTLSoftware. The main purpose of this software and computerize the form of inspection by public transport. Thus the information collected by users will be sent directly to their respective shipping companies more quickly and safely.

**LISTA DE FIGURAS**

[**Figura 1 Organograma da Equipe** 23](#_Toc389435557)

[**Figura 2 WBS** 31](#_Toc389435558)

[**Figura 3 Matriz GUT** 32](#_Toc389435559)

[**Figura 4 Imagem do Diagrama de Gantt parte 1** 43](#_Toc389435560)

[**Figura 5 Imagem do Diagrama de Gantt parte 2** 44](#_Toc389435561)

**LISTA DE TABELAS**

**Tabela 1 Orçamento** 19

**Tabela 2 Dicionário EAP** 30

**Tabela 3 Riscos gerais de um projeto de software** 33

**Tabela 4 Tabela de Riscos Específicos** 36

**LISTA DE SIGLAS**

DFD Diagrama de Fluxo de Dados

DER Diagrama Entidade Relacionamento

MER Modelo Entidade Relacionamento

EAP Entrega Analítica do Projeto

SQL Struct Query Language

**Sumario**

[1 Introdução 14](#_Toc389437040)

[**1.1** **Definição do Problema** 14](#_Toc389437041)

[**1.2** **Objetivos** 14](#_Toc389437042)

[**1.3** **Empresa** 15](#_Toc389437043)

[**1.3.1** **Descrição da Empresa** 15](#_Toc389437044)

[**1.4** **Plano de Negócio** 16](#_Toc389437045)

[**1.4.1** **Analise de Mercado** 16](#_Toc389437046)

[**1.4.2** **Oportunidades e Ameaças** 16](#_Toc389437047)

[**1.4.3** **Concorrência** 17](#_Toc389437048)

[**1.4.4** **Parceiras** 17](#_Toc389437049)

[**1.4.5** **Fornecedores** 17](#_Toc389437050)

[**1.4.6** **Vantagens Competitivas** 17](#_Toc389437051)

[**1.4.7** **Preço** 18](#_Toc389437052)

[**1.4.8** **Contrato Social** 18](#_Toc389437053)

[**1.4.9** **Organograma** 23](#_Toc389437054)

[**1.4.10** **Descrição da Equipe de suas Funções e Áreas de Atuação** 23](#_Toc389437055)

[2 Apresentação 24](#_Toc389437056)

[**2.1** **Termo de abertura** 24](#_Toc389437057)

[**2.2** **Declaração do escopo** 27](#_Toc389437058)

[**3.1** **Dicionário da EAP** 30](#_Toc389437059)

[**3.2** **WBS** 31](#_Toc389437060)

[4 Análise e Gestão de riscos 31](#_Toc389437061)

[**4.1** **Matriz Gut** 32](#_Toc389437062)

[**4.2** **Riscos do projeto** 33](#_Toc389437063)

[**4.3** **Tabela de riscos** 35](#_Toc389437064)

[**4.4** **Redução e Gestão do Risco** 37](#_Toc389437065)

[5 Planejamento Temporal 42](#_Toc389437066)

[**5.1** **Conjunto de Tarefas do Projeto** 42](#_Toc389437067)

[**5.2** **Diagrama de Gannt** 43](#_Toc389437068)

[**5.3** **Organização do Pessoal** 44](#_Toc389437069)

[**5.4** **Estrutura da equipe** 44](#_Toc389437070)

[Conclusão 46](#_Toc389437071)

[Bibliografia 46](#_Toc389437072)

[Anexo 1 47](#_Toc389437073)

[Anexo 2 51](#_Toc389437074)

# **Introdução**

Neste trabalho será apresentado um sistema de informatização de fiscalização de ônibus que será desenvolvido pela empresa CRTLSoftware, que e uma empresa desenvolvimento de softwares voltada para o setor de transporte publico. Um dos papéis extremamente importantes desempenhados pela empresa durante o processo de desenvolvimento e à qualidade e a segurança dos dados utilizados pelo software. Sendo assim e executado uma análise e verificação, assegurando que o software cumpra com o que foi especificado durante o período de análise e atenda a necessidade do cliente.

## **Definição do Problema**

Hoje grande parte das empresas de transporte tem suas fiscalizações feitas na base manual, ou seja, através de pranchetas que contem formulários onde são feitas as anotações de numeração dos carros, horários de chegada e saída, nome do cobrador e motorista. Mas em um caso de emergência para entrega dos dados iria demorar e a segurança dessas informações será muito frágil.

## **Objetivos**

O objetivo deste projeto e a criação e desenvolvimento de software que informatize da fiscalização feita em transportes públicos atendendo a todos requisitos solicitados pelo cliente, garantindo a integridade, disponibilidade e a segurança das informações utilizadas.

## **Empresa**



Razão Social: CRTLSoftware Ltda.

Nome Fantasia: CRTLSoftware

Endereço: Estrada Velha de Itapevi – n°4296 – Parque das nações – Barueri – SP

CEP: 19280-970

Telefone Comercial: (11)3569-4589

Site: www.crtlsoftware.com.br

E-mail: [atendimento@crtlsoftware.com.br](mailto:atendimento@crtlsoftware.com.br)

### **Descrição da Empresa**

A CRTLSoftware e uma empresa criada a um ano e meio que tem sua sede situada em Barueri - São Paulo. Tem como objetivo prestar serviços de desenvolvimento e criação de softwares para o setor de transportes públicos.

## **Plano de Negócio**

A nossa meta é atingir 10%, de empresas que trabalhem neste ramo de transportes, quase neste início iremos oferecer o produto e usar como teste para ver como será a movimentação do fiscal e, se ele vai se acostumar ao produto ou não. Aí que veremos qual será o ponto positivo e o ponto negativo do produto e, ou melhoramos ou modificamos algumas coisas para que ele tenha uma possibilidade de 80% em uma empresa de médio porte.

A empresa CtrlSoftware tem como foco, a segurança da informação e a prevenção de perdas de arquivos para que não haja conflitos entre gerente e funcionário.

* + 1. **Analise de Mercado**

O setor no qual a CRTLSoftware pretende ingressar é bastante competitivo. O preço, a qualidade e criação dos produtos são os fatores críticos de sucesso. A CRTLSoftware vê nessas restrições o seu nicho de mercado, já que pretende associar boa imagem ao seu produto. Adequada à suprir a grande demanda e qualidade dos softwares, para que possa atender da melhor forma possível a necessidade dos clientes.

* + 1. **Oportunidades e Ameaças**

Entre as oportunidades identificadas neste ramo de negócios, destacam-se: alta necessidade de um sistema confiável e de qualidade, crescimento do mercado consumidor; criação do imposto Simples para as micros e pequenas empresas; novos equipamentos disponíveis a baixo custo.

Entre as principais ameaças estão grande dispersão do público-alvo, concorrência dos fornecedores de softwares, altas taxas de juros, utilização pelas grandes empresas de equipamentos modernos, que possibilitam significativos ganhos de escala.

Nos estudos de mercado feitos para subsidiar este Plano de Negócios, foi utilizada fontes secundárias, principalmente através da Internet, mas também foram feitas pesquisas junto ao consumidor final e junto aos criadores dos sistemas. Os objetivos da pesquisa foram identificar as necessidades existentes, analisando assim o perfil do usuário, suas opiniões, sugestões.

Os resultados da pesquisa mostraram um ambiente altamente favorável à entrada da (nome da empresa) no mercado, tendo sido possível identificar inovações e melhorias no produto, que permitirão a sua diferenciação da concorrência.

* + 1. **Concorrência**

A pesquisa de mercado indicou que existem somente três concorrentes da CRTLSoftware todos eles pesquisados diretamente durante a elaboração deste Plano de Negócios. Após a entrevista com cada um dos concorrentes, percebeu-se que as principais dificuldades encontradas dizem respeito à implantação e treinamento do sistema, sendo levado em consideração a distancia entre produto e cliente.

* + 1. **Parceiras**

CtrlSoftware vai atuar juntamente com empresas terceirizadas, governos municipais e estaduais e outras prestadoras de serviços, para atender este mercado.

* + 1. **Fornecedores**

A análise dos fornecedores indicou que os esforços de conquista para novos funcionários deverão se concentrar na procura de pessoal qualificado, para que a empresa possa atender a toda demanda. Assim, foi feita uma relação de todos os fornecedores e aplicada à mesma pesquisa já realizada com os concorrentes, para se tiver uma análise do mercado na visão das empresas fornecedoras de matérias-primas. Qualidade do produto, prazo de entrega, tempo de atuação no mercado, preço, entre outros itens.

* + 1. **Vantagens Competitivas**

Os softwares da CRTLSoftware apresenta algumas vantagens em relação à dos concorrentes, tais como:

• Qualidade do produto, rapidez, fácil manuseio;

• Rápida e acessível manutenção do sistema;

* + 1. **Preço**

Para a determinação do preço de venda foi considerados:

• os preços de mercado comparados com os da concorrência;

• o preço que os clientes estariam dispostos a pagar;

• os custos da criação dos softwares.

* + 1. **Contrato Social**

**Ctrlsoftware**

Pelo presente instrumento particular **Leandro Soares da Silva,** brasileiro, solteiro, maior, portador da cédula de identidade, RG nº 42.795.368-9, portador do CPF/MF nº 325.658.987-45, domiciliado em São Paulo, onde reside à Prof. João da Matta e Luz, 84 - CEP: 06401-120; **Alexandre Abreu,** brasileiro, solteiro, maior, portador da cédula de identidade, RG nº 11.586.956-8, portador do CPF/MF nº 364.986.458-23, domiciliado em São Paulo, onde reside à R. Diana, 53 – CEP : 05019-000, **Alexandre da Silva Andrade,** brasileiro, solteiro, maior, portador da cédula de identidade, RG nº 41.587.569-9 , portador do CPF/MF nº 364.890.581-83 ,domiciliado em São Paulo, onde reside à R. Coração Brasileiro 80 - CEP: 08257060, **Jaqueline de Sousa Silva,** brasileira, solteira, maior, portadora da cédula de identidade, RG nº 53.85.458-7, portador do CPF/MF nº 258.458.963-86 ,domiciliado em São Paulo, onde reside à R. Renata Agondi, 77- CEP : 08131-320, **Edenilson Bila,** brasileiro, solteiro, maior, portador da cédula de identidade, RG nº 54.856.785-4, portador do CPF/MF nº 456.785.963-12 ,domiciliado em São Paulo, onde reside à R. Pedro Vicente, 625 - CEP: 01109-010, **Wiliam Alves Soares,** brasileiro, solteiro, maior, portador da cédula de identidade, RG nº 23.589.412-8, portador do CPF/MF nº 569.856.954-78,domiciliado em São Paulo, onde reside à R. Conselheiro Furtado, 868 – CEP : 01511-001**,** brasileiros, tecnólogos em informática, resolvem constituir, como constituído têm, a referida sociedade (simples, empresária, s/ ou Ltda.) que se regerá pelas cláusulas e condições seguintes:

**1 –** A sociedade gera sob a razão social de Ctrlsoftware,e tem sua sede social à Estrada Velha de Itapevi – n°4296 – Parque das nações – Barueri – São Paulo.

**Parágrafo Único –** A critério dos sócios a sociedade poderá abrir manter e extinguir escritórios em todo território nacional.

**2 –** O prazo de duração da sociedade é indeterminado.

**3 –** O capital totalmente subscrito e integralizado é de R$ 46.200,00(reais), dividido em (6) quotas do valor, cada uma, de R$7.700,00(reais)

**Tabela 1 Orçamento**

|  |  |  |
| --- | --- | --- |
| **Sócio** | **Quotas** | **Valor** |
| **1 – Leandro Soares da Silva** | **1** | **R$7.700,00** |
| **2 – Alexandre Abreu** | **1** | **R$7.700,00** |
| **3 – Alexandre da Silva Andrade** | **1** | **R$7.700,00** |
| **4 – Jaqueline de Sousa Silva** | **1** | **R$7.700,00** |
| **5 – Edenilson Bila** | **1** | **R$7.700,00** |
| **6 – Wiliam Alves Soares** | **1** | **R$7.700,00** |
| **TOTAL** |  | **R$46.200,00** |

**Parágrafo Único –** Quando no exercício de serviços relacionados à informática com uso da razão social todos os sócios respondem pessoal, solidária e ilimitadamente pelos danos que causarem aos clientes, por ação ou omissão, sem prejuízo de responsabilidade disciplinar em que porventura incorrer o responsável direto pelo ato.

**4 –** A sociedade tem por objetivo disciplinar o expediente e os resultados patrimoniais auferidos na prestação de serviços advocatícios, tais serviços, porém serão exercidos individualmente, em se tratando de atos privativos ainda mesmo que revertam ao patrimônio social os respectivos honorários.

**5 –** A gerência da sociedade será exercida por todos os sócios, podendo cada qual usar isoladamente a razão social, e representar a sociedade ativa e passivamente, em juízo ou fora dele.

**Parágrafo Único –** A gerência da sociedade poderá ainda ser exercida por um estranho ao objetivo social, bem como para a prestação de avais, fianças e abonos de mero favor.

**6 –** Fica expressamente vedado o uso da razão social para negócios estranhos ao objetivo social, bem como para a prestação de avais, fianças e abonos de mero favor.

**7 –** Os sócios fixarão, de comum acordo, as retiradas “pro labore”, as quais serão levadas à conta de Despesas Gerais.

**8 –** Nenhum dos sócios poderá ceder ou transferir, total ou parcialmente, suas cotas a terceiros sem ofertá-las, em igualdade de condições, ao outro sócio, que terá direito de preferência para sua aquisição.

**9 –** O direito de preferência para a aquisição de cotas sociais deverá ser manifestado dentro de 30 (trinta) dias da data em que o sócio vendedor efetuar a comunicação de sua intenção de vender.

**10 –** A interdição ou falecimento de qualquer dos sócios não extingue a sociedade, que permanecerá com os sócios remanescentes, regulando-se a apuração dos haveres do sócio falecido ou interditado e o seu pagamento pelo disposto na cláusula seguinte.

**11 –** O sócio que se retirar da sociedade, bem como os herdeiros do sócio que falecer ou representante legal do sócio interditado receberão os haveres, apurados de acordo com um balanço especialmente levantado, na data da retirada ou do óbito. O que for apurado será pago em 12 (doze) prestações mensais e consecutivas, vencendo-se a primeira a 30 (trinta) dias do balanço, correndo juros sobre os restantes, desde já estipulados em 12% ao ano.

**Parágrafo Único –** A critério dos sócios, a sociedade poderá criar contas de reserva, bem como levantar balanços intermediários ou intercalares.

**12 –** Em 31 de dezembro de cada ano será levantado um balanço geral, e, após as deduções previstas em lei, os lucros líquidos ou prejuízos serão distribuídos ou suportados entre os sócios na proporção das cotas que possuírem.

**13 –** Os casos omissos serão resolvidos de acordo com a legislação em vigor.

E, por estarem assim justos e contratados, assinam o presente instrumento em quatro vias de igual teor e para a mesma finalidade, na presença das testemunhas.

São Paulo, ­\_\_\_\_\_de \_\_\_\_\_\_\_\_\_\_\_\_, de 2013.

**Leandro Soares da Silva**

**Alexandre Abreu**

**Alexandre da Silva Andrade**

**Jaqueline de Sousa Silva**

**Edenilson Bila**

**Wiliam Alves Soares**

**Testemunhas**:

1 - -------------------------------------------------

1. - ------------------------------------------------
   * 1. **Organograma**

O organograma da equipe do projeto se apresenta conforme o gráfico a seguir:

**Figura 1 Organograma da Equipe**

* + 1. **Descrição da Equipe de suas Funções e Áreas de Atuação**

Alexandre Abreu – Segurança de Sistemas

Alexandre Andrade – Gerenciamento de Projetos de Softwares

Edenilson Bila – Desenvolvimento de banco de dados SQL

Jaqueline de Sousa – Desenvolvimento de banco de dados SQL

Leandro Soares – Analise e projeto de Sistemas

William Soares – Manutenção de Sistema

1. **Apresentação**
   1. **Termo de abertura**

|  |  |
| --- | --- |
|  | **Termo de Abertura** |
| **CRTLSoftware** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Controle de Versões** | | | |
| **Versão** | **Data** | **Autor** | **Notas da Revisão** |
| 1.1 | 20.05.2014 | Alexandre Andrade | Elaboração inicial |
| 1.2 | 30.05.2014 | Alexandre Abreu  Alexandre Andrade  Edenilson  Jaqueline de Sousa Silva  Leandro Soares da Silva  Wiliam Alves Soares | Revisão do Documento |

**Objetivos deste documento**

Autorizar o início do projeto, atribuir principais responsáveis e documentar requisitos iniciais, principais entregas, premissas e restrições.

**Justificativa**

Criar e desenvolver um software que informatize a forma de fiscalização feita em empresas de transporte publico.

**Descrição do Projeto e principais requisitos**

O Objetivo do projeto e desenvolver um software que auxilie os funcionários de empresas de transporte a fazer a fiscalização de suas frotas de ônibus de forma mais rápida, pratica e segura. Este software terá como principais funções, cadastro de funcionários, ônibus, empresas, linhas, pesquisa e exclusão de cadastro de funcionários, ônibus, empresas, linhas, tela de cadastro de fiscalização onde serão informados dados referentes a linha de ônibus, os funcionários operantes, a empresa contratante ,ônibus utilizado, o tempo de percurso, o itinerário, os horários .

Consulta de fiscalização onde serão buscados todos os dados referentes a fiscalização já feita e armazenadas no banco de dados do sistema.

**Equipe do projeto**

|  |  |
| --- | --- |
| **Equipe do Projeto** | |
| Alexandre Andrade | Analista de sistemas |
| Alexandre Abreu | Projetista do Software |
| Edenilson Bila | Desenvolvedor |
| Jaqueline de Sousa | Desenvolvedor |
| Leandro Soares | Gerente do Projeto |
| William Soares | Testador |

**Premissas**

* Os membros da equipe de projetos terão dedicação integral e exclusiva ao projeto.
* O treinamento de utilização do software será feita aos funcionários por pessoas especializadas.

**Restrições**

* Não deverá haver atrasos no prazo de entrega do projeto.
* O orçamento não poderá ultrapassar o estipulado.
* Não impactar nos prazos dos processos em andamento.
* O prazo limite deve ser respeitado sem que possa ser realizadas atividades fora do horário comercial.

**Marcos**

|  |  |
| --- | --- |
| Marcos | Previsão |
| Iniciação do Projeto | 25/02/2014 |
| Planejamento do Projeto | 14/03/2014 |
| Execução | 16/04/2014 |
| Encerramento | 02/06/2014 |

**Orçamento**

|  |
| --- |
| Orçamento Previsto |
| R$ 46.000,00(quarenta e seis mil reais) |

**Riscos**

* O tempo necessário para o desenvolvimento do software foi subestimado.
* A organização foi reestruturada e gerentes diferentes ficaram responsáveis pelo projeto.
* Problemas financeiros na organização forçaram reduções no orçamento do projeto.
* Indisponibilidade da infraestrutura de desenvolvimento (espaço físico, ferramentas de software e hardware) não disponível nos momentos delimitados no plano do projeto.

|  |  |  |
| --- | --- | --- |
| **Aprovações** | | |
| **Participante** | **Assinatura** | **Data** |
| Patrocinadores do Projeto | Empresas de Transporte | 01/02/2014 |
| Gerentes do Projeto | Leandro Soares | 01/02/2014 |

* 1. **Declaração do escopo**

|  |  |
| --- | --- |
|  | **Declaração do escopo do projeto** |
| **CRTLSoftware** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Controle de Versões** | | | |
| **Versão** | **Data** | **Autor** | **Notas da Revisão** |
| 1.1 | 20.05.2014 | Alexandre Andrade | Elaboração inicial |
| 1.2 | 24.05.2014 | Alexandre Abreu  Alexandre Andrade  Edenilson  Jaqueline de Sousa Silva  Leandro Soares da Silva  Wiliam Alves Soares | Revisão do Documento |

**Objetivos do projeto**

O Objetivo do projeto e desenvolver um software que auxilie os funcionários de empresas de transporte a fazer a fiscalização de suas frotas de ônibus de forma mais rápida, pratica e segura.

**Escopo do Produto**

Nesse projeto será entregue um software de fiscalização de ônibus que terá como funcionalidades o cadastro de funcionários, cadastro de ônibus, cadastro de empresas, cadastro de linhas.

Pesquisa e exclusão de cadastro de funcionários, ônibus, empresas, Linhas.

Tela de cadastro de fiscalização onde serão informados dados referentes à linha de ônibus, os funcionários operantes, a empresa contratante, ônibus utilizado, o tempo de percurso, o itinerário, os horários.

Consulta de fiscalização onde serão buscados todos os dados referentes a fiscalização já feita e armazenadas no banco de dados do sistema. Para o desenvolvimento desse software o projeto será divido em quatro fases (iniciação. planejamento, execução, encerramento).

(**Visualize o documento de requisitos funcionais e Não funcionais no** [**anexo1**](#_Anexo_1))

**Fora do Escopo**

* Serão consideradas atividades fora do escopo, qualquer outra atividade que não estejam reportadas no tópico acima.
* Infraestrutura de rede.

**Restrições**

* Não deverá haver atrasos no prazo de entrega do projeto.
* O orçamento não poderá ultrapassar o estipulado.
* Não impactar nos prazos dos processos em andamento.
* O prazo limite deve ser respeitado sem que possa ser realizadas atividades fora do horário comercial.

**Premissas**

* Os membros da equipe de projetos terão dedicação integral e exclusiva ao projeto.
* O treinamento aos funcionários será feito por pessoas especializadas.

|  |  |  |
| --- | --- | --- |
| **Aprovações** | | |
| **Participante** | **Assinatura** | **Data** |
| Patrocinador do Projeto | Empresas de Transportes | 14/03/2013 |
| Gerente do Projeto | Leandro Soares da Silva | 14/03/2013 |

1. **Estrutura Analítica do Projeto (EAP)**

**CRTLSoftware**

1**. Iniciação do Projeto**

1.1. Definição do projeto

1.2. Reuniões com o cliente

1.3. Documentação

1.4. Termo de abertura do Projeto

2. **Planejamento do Projeto**

2.1 Levantamentos de Requisitos

2.2. Declaração do escopo

2.3. WBS

2.4. Cronograma

2.5. Orçamento

3. **Execução**

3.1. Reuniões e Relatórios

3.2. Desenvolvimento

3.2.1. Criação das interfaces

3.2.2. Criação do banco de Dados

3.2.3. Codificação

3.3. Infraestrutura

3.4. Implantação

3.5. Testes

3.6. Treinamento

3.7 Operação

4. **Encerramento**

4.1. Documentação final

4.2. Encerramento de Contratos

4.3. Encerramento do Projeto

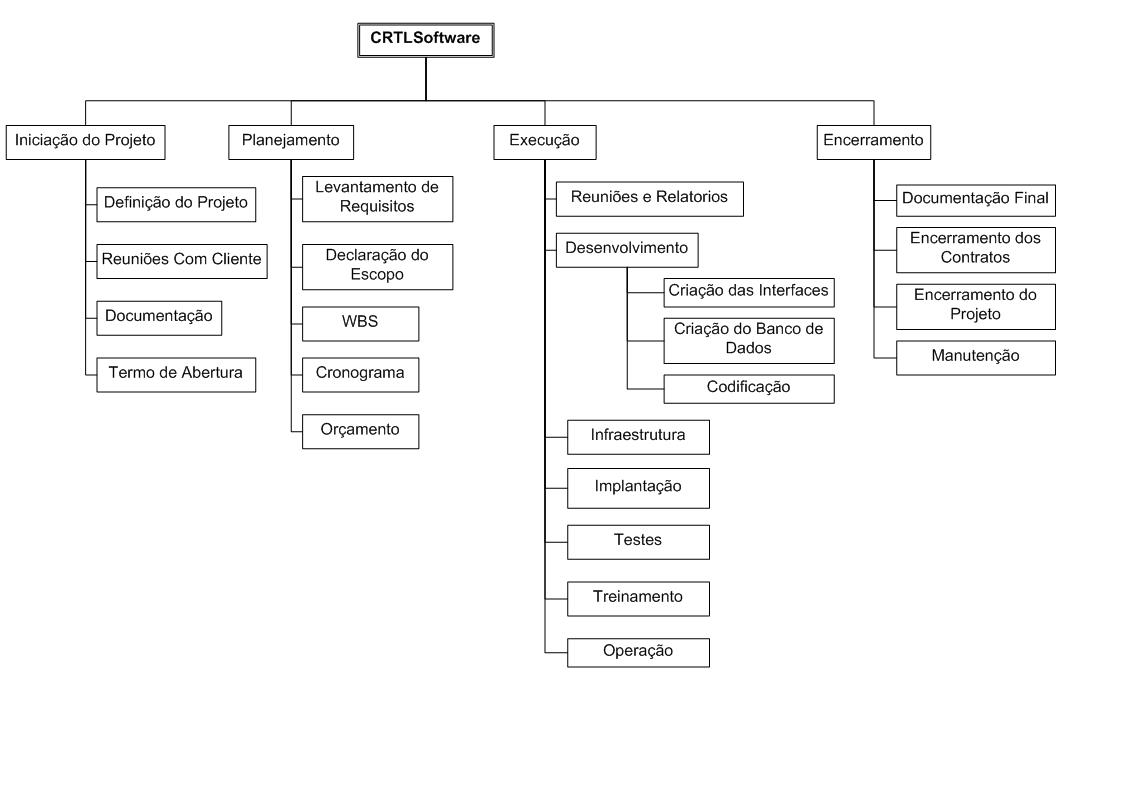
4.4. Manutenção

* 1. **Dicionário da EAP**

**Tabela 2 Dicionário EAP**

|  |  |  |
| --- | --- | --- |
| **Cód. EAP** | **Entrega/Pacote de Trabalho** | **Descrição** |
| **1.** | Iniciação do Projeto |  |
| 1.1 | Definição do Projeto | Definir qual o objetivo do software. |
| 1.2 | Reuniões com o cliente | Processo para definir quais serão as características do software. |
| 1.3 | Documentação | Documentação de todo o plano de ação do projeto para o desenvolvimento do software solicitado. |
| 1.4 | Termo de Abertura do projeto | E o documento de liberação de inicio do projeto. |
| **2.** | Planejamento Do Projeto | E a definição de todas as etapas do projeto. |
| 2.1 | Levantamento de Requisitos | Definir quais as necessidades do sistema. |
| 2.2 | Declaração do Escopo | Detalhes do Projeto |
| 2.3 | WBS | Processo de subdivisão das entregas e do trabalho do projeto em componentes menores e mais facilmente gerenciáveis. |
| 2.4 | Cronograma | Definir o cronograma de atividades do projeto. |
| 2.5 | Orçamento | Definir o custo de todo o projeto. |
| **3.** | Execução | Etapa de inicio de desenvolvimento do software. |
| 3.1 | Reuniões e Relatórios | Reuniões periódicas e relatórios de todo o processo de desenvolvimento. |
| 3.2 | Desenvolvimento | Inicio da criação do software. |
| 3.2.1 | Criação das Interfaces | Desenvolver todas as interfaces do software. |
| 3.2.2 | Criação do Banco de Dados | Criar o banco de dados de armazenamento das informações do software. |
| 3.2.3 | Codificação | Desenvolvimento do software através de uma linguagem de programação |
| 3.3 | Infraestrutura | Estrutura de Hardware que o projeto ira utilizar para o desenvolvimento e implantação do software. |
| 3.4 | Testes | Testes feitos pelo próprio programador durante a programação para verificar se todas as funcionalidades estão de acordo com os requisitos. |
| 3.5 | Implantação | Etapa de Instalação do software finalizado. |
| 3.6 | Treinamento | Capacitar os usuários que utilizarão o software. |
| 4. | Encerramento | Finalização do projeto. |
| 4.1 | Documentação Final | Entrega de toda a documentação referente ao projeto de desenvolvimento do software. |
| 4.2 | Encerramento de Contratos | Finalizar os contratos de todos os envolvidos no projeto. |
| 4.3 | Encerramento do projeto | Finalizar o projeto |
| 4.3 | Manutenção | Processo de melhoria e otimização do software já desenvolvido. |
|  |  |  |

* 1. **WBS**



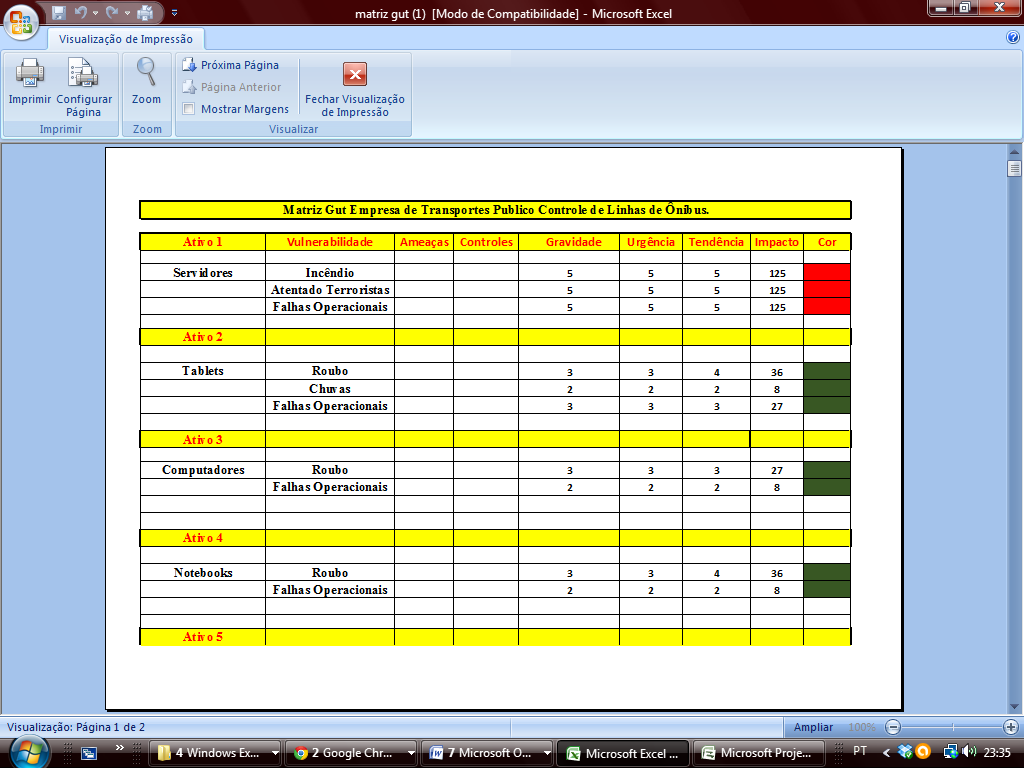
**Figura 2 WBS**

1. **Análise e Gestão de riscos**

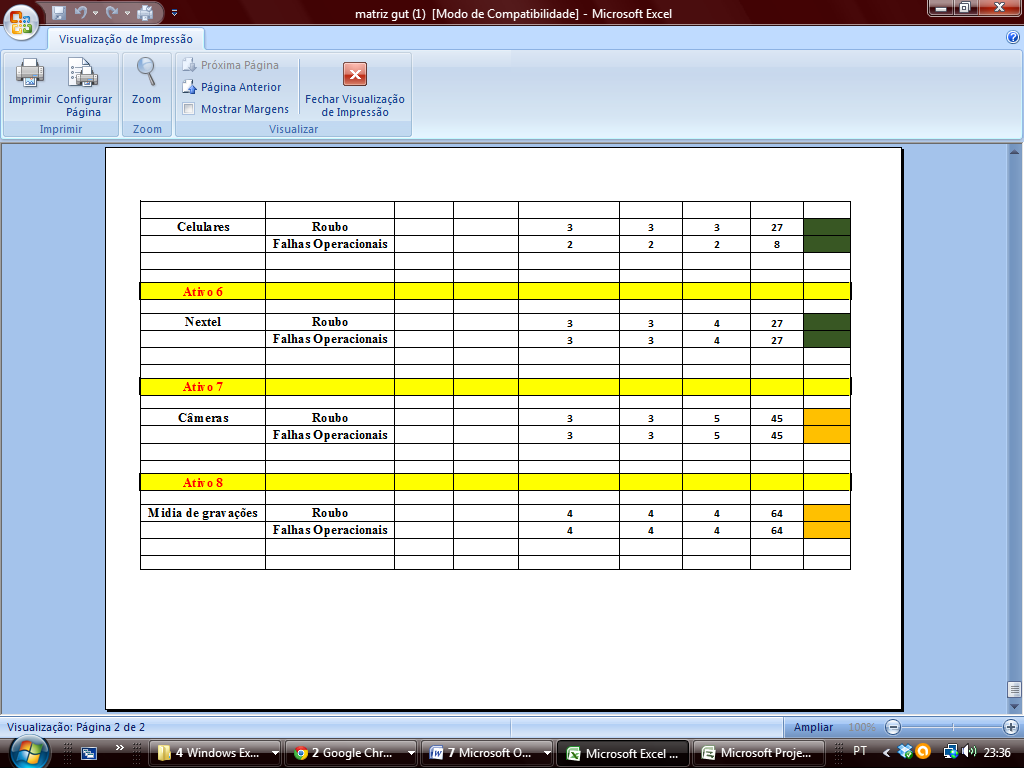
Um risco é um problema em potencial, ou seja, um problema com certa probabilidade de acontecer que pode afetar de diversas formas o andamento do projeto.

Todo projeto está sujeito a determinados riscos. Cada risco tem um percentual de chance de acontecer (sendo uns com maior e outros com menor possibilidade de ocorrência), e um determinado impacto sobre o projeto. É preciso conhecê-los e determinar as formas de minimizar a probabilidade de sua ocorrência, bem como o seu impacto, caso ele venha a acontecer.

* 1. **Matriz Gut**



**Figura 3 Matriz GUT**



* 1. **Riscos do projeto**

Os riscos de um projeto podem ser distinguidos em gerais (comuns a todo projeto) e específicos (únicos de cada projeto). Os riscos gerais, comuns a qualquer projeto são listados abaixo:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risco | Projeto | Técnico | Negócio | Comum | Especial |
| Equipamento não disponível |  | X |  |  |  |
| Requisitos incompletos | X |  |  | X |  |
| Uso de metodologias especiais |  | X |  |  | X |
| Problemas na busca da confiabilidade requerida |  | X |  |  | X |
| Retenção de pessoas chaves | X |  |  | X |  |
| Subestimativas do esforço | X |  |  | X |  |

**Tabela 3 Riscos gerais de um projeto de software**

Avaliação global dos riscos:

**1. O Gestor de Software dá suporte ao projeto?**

Sim. O gestor de software tem um papel importante para o bom andamento do projeto, e seu apoio tem sido fundamental durante a consecução do trabalho.

**2. Os Clientes estão entusiasmados com o projeto e o produto?**

O cliente está muito interessado no produto pois a ferramenta automatizará o atual processo de controle dos leitos, o que evitará os frequentes erros incorridos pelo processo manual de trabalho.

**3. Os Engenheiros de Software compreenderam bem os requisitos?**

Sim, os engenheiros compreendem bem os requisitos do projeto, pois estão participando desde o início do trabalho.

**4. Os Clientes estiveram envolvidos na definição dos requisitos?**

Sim. Devido ao grande interesse no sistema, eles estiveram evolvidos durante a definição dos requisitos.

**5. O âmbito do projeto é estável?**

Sim.

**6. Os engenheiros de Software têm as competências requeridas?**

Apesar de pouco experientes, os Engenheiros de Software tem como principal objetivo a busca por novas experiências e, consequentemente, o aumento de suas competências.

**7. Os requisitos do projeto são estáveis?**

Os requisitos foram bem definidos no início do trabalho, porém algumas alterações foram solicitadas para melhor desenvolvimento do produto. A metodologia utilizada para o desenvolvimento do software visa lidar com essas mudanças de maneira que não impacte tanto no desenvolvimento do trabalho.

**8. A Equipe de Desenvolvimento tem experiência na tecnologia a implementar?**

Não, poucos membros da equipe tem um boa experiência técnica profissional, já a maioria tem apenas experiência em desenvolvimento de trabalhos acadêmicos.

**9. É adequado o número de pessoas da equipe de trabalho?**

Não. Apesar de o sistema não ser tão grande, é necessária a presença de mais uma pessoa na equipe, desde que esta seja experiente, devido à falta de experiência da equipe atual.

Nesta tarefa demonstraremos as fragilidades e as prevenções de um aplicativo do nosso sistema.

* 1. **Tabela de riscos**

Para o desenvolvimento do software, alguns riscos foram identificados e classificados quanto a sua probabilidade e seu impacto no projeto. A tabela abaixo demostra os riscos com seus valores associados.

|  |  |  |
| --- | --- | --- |
| **Nome do risco** | **Probabilidade** | **Impacto** |
| Desistência do cliente | 10% | Catastrófico |
| Poucos programadores no desenvolvimento | 80% | Crítico |
| Requisitos mal compreendidos | 60% | Crítico |
| Ausência de inspeções no processo de software. | 50% | Crítico |
| Custos associados a um Produto defeituoso | 30% | Crítico |
| Ausência de ferramentas CASE adequada para testes de software | 80% | Moderado |
| Dedicação integral dos desenvolvedores ao projeto | 50% | Moderado |
| Atraso na entrega | 50% | Moderado |
| Disponibilidade do cliente para o desenvolvimento | 30% | Moderado |
| Falta de treinamento da equipe nas ferramentas de desenvolvimento | 20% | Moderado |
| Grande número de classes | 20% | Moderado |
| Restrições governamentais | 30% | Marginal |
| Grande volume de dados | 25% | Marginal |
| Manutenção associada às tecnologias e ferramentas livres | 20% | Marginal |
| Grande número de usuários | 15% | Marginal |
| Ausência de integração das ferramentas de desenvolvimento | 50% | Desprezível |

**Tabela 4 Tabela de Riscos Específicos**

* 1. **Redução e Gestão do Risco**

Visando garantir a redução da probabilidade dos riscos identificados na seção anterior, bem como seu impacto em caso de ocorrência, abaixo serão descritas as formas de redução bem como o plano de contingência necessário em caso de ocorrência.

|  |
| --- |
| **1.** Desistência do Cliente |
| **Probabilidade:** 10% **Impacto:** Catastrófico |
| **Descrição:** Insatisfação do cliente com o andamento do projeto, ou desinteresse pode levá-lo a desistir do projeto. |
| **Estratégia de redução:** Envolvê-lo em todas as fases do projeto, para que ele se sinta parte importante no processo de desenvolvimento, mostrando sempre a evolução do software. |
| **Plano de contingência:** Durante o desenvolvimento do projeto, demonstrar a possíveis novos clientes as funcionalidades do sistema e como ele poderia ser importante em suas empresas. |
| **Responsável:** Alexandre Abreu |
| **Status:** Iniciado |

|  |
| --- |
| **2.** Poucos programadores no desenvolvimento |
| **Probabilidade:** 80% **Impacto:** Crítico |
| **Descrição:** O número de programadores no desenvolvimento do projeto deste software é pequeno. |
| **Estratégia de redução:** Melhorar a produtividade dos programadores através de incentivos financeiros e pessoais ou contratar mais alguns programadores. |
| **Plano de contingência:** Fazer com que os programadores alocados para o projeto tenham bastante produtividade, dadas às limitações existentes. |
| **Responsável:** Leandro Soares |
| **Status:** Iniciado |

|  |
| --- |
| **3.** Requisitos mal compreendidos |
| **Probabilidade:** 60% **Impacto:** Crítico |
| **Descrição:** Diferentes *stakeholders* têm em mente diferentes requisitos e podem expressá-los de maneiras distintas. |
| **Estratégia de redução:** Combinar o uso das mais diversas técnicas de elicitação no processo de descoberta dos requisitos do *stakeholders*. |
| **Plano de contingência:** Analisar os artefatos oriundos da elicitação dos requisitos com os *stakeholders* e encontrar os pontos comuns e os pontos conflitantes. |
| **Responsável:** Alexandre Andrade |
| **Status:** Em andamento |

|  |
| --- |
| **4.** Ausência de inspeções no processo de software |
| **Probabilidade:** 50% **Impacto:** Crítico |
| **Descrição:** A inspeção de software pode não ser executada, geralmente, devido a atrasos no cronograma. |
| **Estratégia de redução:** Não pular etapas do processo de software estabelecido na Organização. O processo de software deve ser seguido. |
| **Plano de contingência:** Intensificar os testes de sistema. |
| **Responsável:** Alexandre Abreu |
| **Status:** Em andamento |

|  |
| --- |
| **5.** Custos associados a um produto defeituoso |
| **Probabilidade:** 30% **Impacto:** Crítico |
| **Descrição:** Qualquer software possui erros. Com isso, as correções deles são custosas a depender de quando são encontrados. Além disso eles podem gerar grandes prejuízos a instituição usuária do software. |
| **Estratégia de redução:** Enfatizar a fase de teste no processo de desenvolvimento de software. A equipe de teste deve testar exaustivamente o software sempre procurando pelos erros. |
| **Plano de contingência:** Focar a equipe desenvolvedora do software na resolução do erro. |
| **Responsável:** Jaqueline de Sousa |
| **Status:** Em andamento |

|  |
| --- |
| **6.** Ausência de ferramentas CASE adequada para testes de software |
| **Probabilidade:** 80% **Impacto:** Moderado |
| **Descrição:** O processo de gerar testes automatizados auxilia na produção de um software com mais qualidade. Neste contexto, a ausência de ferramentas CASE que dão suporte à essa atividade obriga a execução de testes manuais exaustivos. |
| **Estratégia de redução:** Ter um enfoque na fase de testes, elaborando casos de teste que abranjam as possíveis entradas e combinações de entradas do software. |
| **Plano de contingência:** Terceirizar o processo de testes do software. |
| **Responsável:** Leandro Soares |
| **Status:** Em andamento |

|  |
| --- |
| **7.** Dedicação integral dos desenvolvedores ao projeto |
| **Probabilidade:** 50% **Impacto:** Moderado |
| **Descrição:** A maioria dos integrantes não tem como se dedicar exclusivamente para o projeto, principalmente por questões de compatibilidade de horário com outros afazeres. |
| **Estratégia de redução:** Tentar adequar o trabalho de cada um com o seu tempo disponível, sem que isto afete seu tempo de lazer. As atribuições de cada membro serão dividas de forma a não onerar o seu tempo de disponibilidade nem atrasar o andamento do projeto. |
| **Plano de contingência:** Incentivar os integrantes da equipe para que eles usem um pouco do seu tempo de lazer disponível, em momentos de grande necessidade, para consecução do trabalho. |
| **Responsável:** Leandro Soares |
| **Status:** Em andamento |

|  |
| --- |
| **8.** Atraso na entrega |
| **Probabilidade:** 50% **Impacto:** Moderado |
| **Descrição:** É comum o atraso na entrega do software. Entretanto é algo que não deve acontecer. Esse é um risco que pode levar a descredibilidade da empresa desenvolvedora além de caracterizar uma quebra de contrato. |
| **Estratégia de redução:** Planejar o desenvolvimento do software levando em conta todas as possíveis eventualidades, além de estimar o tempo do desenvolvimento com um acréscimo. Com esse planejamento a equipe deve seguir o cronograma e assim cumprir as atividades no tempo correto. |
| **Plano de contingência:** Focar equipe no projeto sem dispersar com outras atividades. |
| **Responsável:** Alexandre Abreu |
| **Status:** Iniciado |

* 1. **Politica de segurança**

Nossa política de segurança foi feita baseada no [anexo 2](#_Anexo_2)

1. **Planejamento Temporal**

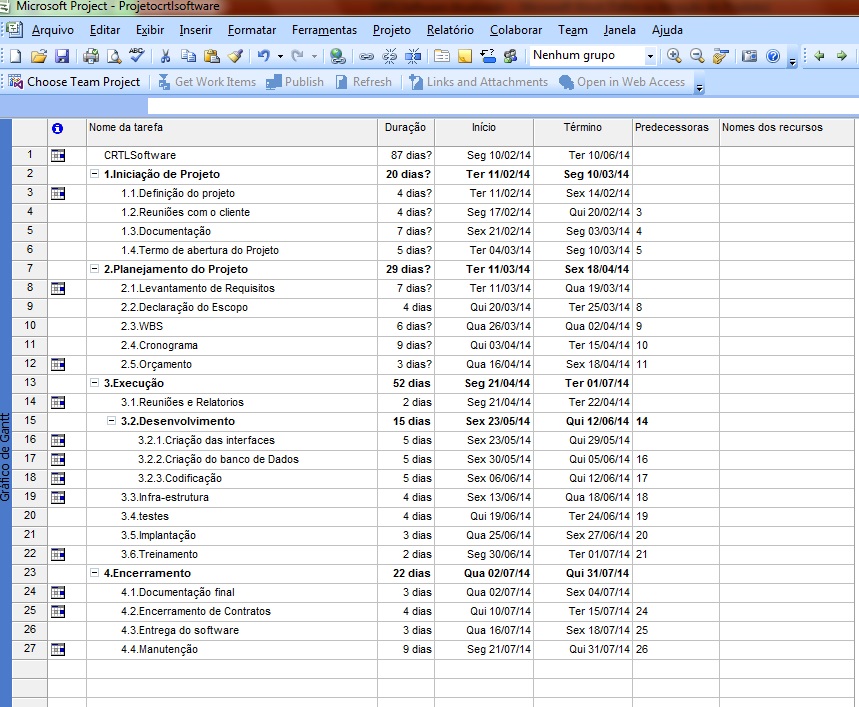
Nesta seção, são definidas as datas de execução das tarefas, bem como seus responsáveis. Para descrever esse aspecto temporal, foi elaborado o Diagrama de Gantt.

* 1. **Conjunto de Tarefas do Projeto**

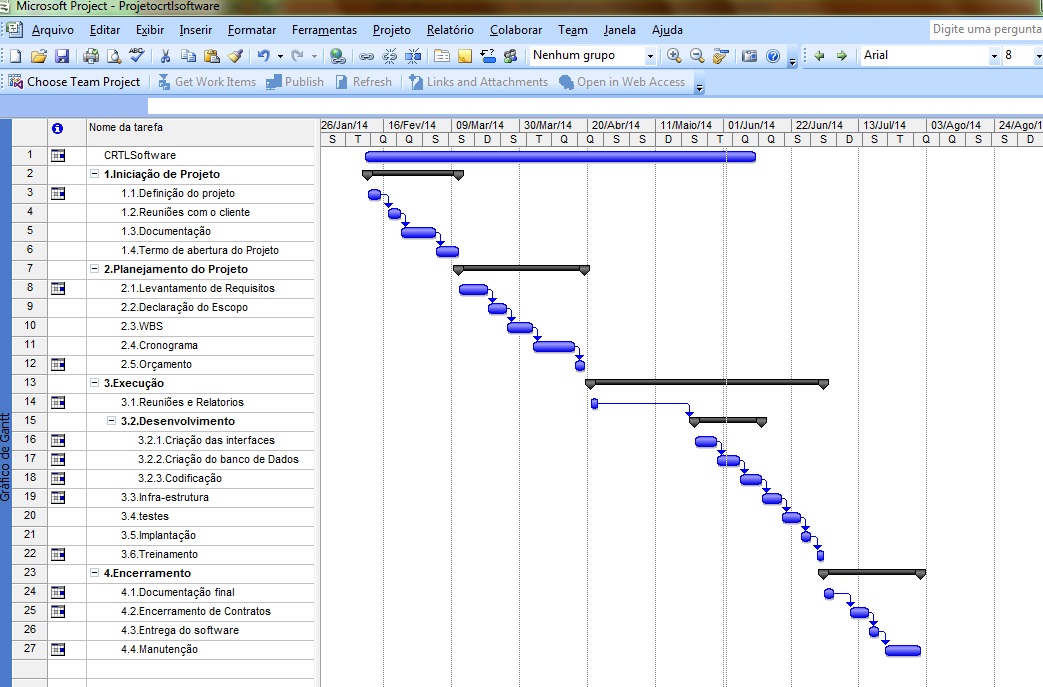
|  |  |  |
| --- | --- | --- |
| **Tarefas** | **Porcentagem** | **Dias de Trabalho** |
| Iniciação do Projeto | 15% | 20 |
| Planejamento do projeto | 24% | 29 |
| Execução | 45% | 52 |
| Encerramento | 16% | 22 |

* 1. **Diagrama de Gannt**

O diagrama de Gantt é ilustrado a seguir, trata-se de um gráfico que mostra todas as tarefas planejadas com suas datas de inicio e fim e os recursos utilizados.



**Figura 4 Imagem do Diagrama de Gantt parte 1**



**Figura 5 Imagem do Diagrama de Gantt parte 2**

Uma visão mais detalhada do diagrama de gantt pode ser vista no arquivo <Projetocrtlsoftware.mpp>.

* 1. **Organização do Pessoal**

Cada membro da equipe possui as suas atribuições e deveres bem definidos, assim, cada um sabe qual tarefa deve ser realizada e até onde ele pode fazer. As decisões serão tomadas em conjunto com todos os stakeholders do projeto.

* 1. **Estrutura da equipe**

**Gerente do Projeto:** tem a responsabilidade de coordenar todo o desenvolvimento do projeto, combinando reuniões, distribuindo tarefas, resolver conflitos e manter a motivação e bom ambiente no seio do grupo, além de ser responsável pelo planejamento temporal do projeto compondo o diagrama de Gantt.

Responsável: Leandro Soares

**Analista de sistema:** tem a função de analisar o software e desenhar os vários diagramas do sistema e criar as classes e interfaces a implementar.

Responsável: Alexandre Andrade

**Projetista de software:** estuda e seleciona tanto as ferramentas utilizadas como o hardware e plataformas onde o software será utilizado.

Responsável: Alexandre Abreu

**Desenvolvedores:** recebem o trabalho do analista e programam o código do novo sistema.

Responsável: Edenilson Bila e Jaqueline de Sousa

**Testador:** no fim testa exaustivamente todo o sistema de forma a detectar erros na implementação.

Responsável: William Soares

**Conclusão**

Acredita-se ter alcançado todos os objetivos e requisitos propostos no início deste trabalho resultando no desenvolvimento do software de informatização da fiscalização de transportes públicos.

A metodologia aplicada no presente trabalho utiliza conceitos clássicos de engenharia de software adquiridos e aplicados durante o curso. As linguagens de programação utilizadas foram: VB. NET.

Sendo assim, o software desenvolvido tem aplicação e relevância no mercado atual, viabilidade comercial e contribui para o crescimento da tecnologia móvel entre seus usuários.

**Bibliografia**

<http://projetoseti.com.br/planejamento-do-projeto-definir-o-escopo/>

<http://pt.slideshare.net/paulohrcunha/estrutura-analtica-do-projeto-eap>

<http://escritoriodeprojetos.com.br/termo-de-abertura-do-projeto.aspx>

[www.pmi.org](http://www.pmi.org)

PMBOK Guide – 3ª. Edição

KERZNER, Harold. Gestão de Projetos: As melhores práticas. 2ª Ed. Porto Alegre: Bookman, 2006. PMI. Guia PMBOK. 4. ed. Atlanta: PMI, 2009

Gestão de Projetos em TI - Aula 9 - © 2014-1 - Sérgio Almeida Dias

# **Anexo 1**

**Documento de Requisitos Funcionais e Não funcionais**

**Requisitos Funcionais**

**Nome: Cadastrar Funcionário**

**Objetivo**: Cadastrar todos os dados pessoais do funcionário requeridos pelo sistema no banco de dados. Como código do funcionário, nome, endereço, cargo, telefone data de admissão, data de demissão, CPF, RG, foto.

**Nome: Alterar Funcionário**

**Objetivo**: O Sistema possibilitará ao usuário modificações/alterações nas informações do cadastro pessoal do funcionário armazenadas na base de dados. Exceto seu código identificador.

**Nome: Excluir Funcionário**

**Objetivo**: O sistema deverá possibilitar a exclusão de todos os dados referentes ao funcionário armazenadas no banco de dados atualizando-o automaticamente.

**Nome: Pesquisar Funcionário**

**Objetivo**: O sistema possibilitará a pesquisa de um funcionário já armazenado no banco de dados e disponibilizar a informação para o usuário. Mostrando ao usuário do sistema os dados pessoais do cadastro do funcionário. A busca deverá ser realizada pelo nome do funcionário ou código identificador.

**Nome: Cadastro de ônibus**

**Objetivo:** Cadastro dos dados referente aos ônibus a serem utilizadas no sistema como código do ônibus, tipo de ônibus, empresa fabricante, placa, ano. Facilitando assim o controle da frota de ônibus.

**Nome: Alterar Ônibus**

**Objetivo:** O Sistema possibilitará ao usuário modificações/alterações nas informações do cadastro do ônibus armazenadas na base de dados. Exceto seu código identificador.

**Nome: Excluir Ônibus**

**Objetivo:** O sistema deverá possibilitar a exclusão de todos os dados referentes aos ônibus armazenados no banco de dados atualizando-o automaticamente.

**Nome: Pesquisar Ônibus**

**Objetivo:** O sistema possibilitará a pesquisa de um ônibus já armazenado no banco de dados do sistema e disponibilizar a informação para o usuário. Mostrando ao usuário do sistema os dados de cadastramento do ônibus. A busca deverá ser realizada pelo código identificador.

**Nome: Cadastro de Empresa**

**Objetivo:** Cadastrar os dados referentes às empresas de ônibus que serão utilizadas pelo sistema em seu banco de dados. Como código da empresa, nome da empresa, endereço, CNPJ, telefone, e-mail. Facilitando controle das empresas de ônibus.

**Nome: Alterar Empresa**

**Objetivo:** O Sistema possibilitará ao usuário modificações/alterações nas informações do cadastro referente a empresa armazenada na base de dados. Exceto seu código identificador.

**Nome: Excluir Empresa**

**Objetivo:** O sistema deverá possibilitar a exclusão de todos os dados referentes à empresa armazenada no banco de dados atualizando-o automaticamente.

**Nome: Pesquisar Empresa**

**Objetivo:** O sistema possibilitará a pesquisa de uma empresa já armazenado no banco de dados do sistema e disponibilizar a informação para o usuário. Mostrando ao usuário do sistema os dados de cadastramento da empresa. A busca deverá ser realizada pelo nome ou código identificador.

**Nome: Cadastro das regiões de São Paulo**

**Objetivo:** cadastrar os dados referentes às regiões existentes em São Paulo que serão utilizadas no sistema no seu banco de dados. Como numeração da região, cor da região, nome da região, nome da empresa atuante na região. Desse modo sistema terá um controle maior das linhas operantes de ônibus, controle da frota de ônibus, controle das empresas atuantes em cada região.

**Nome: Tela de fiscalização**

**Objetivo:** cadastrar todas as informações referentes à fiscalização que será feita no transporte público no banco de dados do sistema. Tendo como atributos Código de fiscalização, Nome do Fiscal, Nome do cobrador, Nome do motorista, data, horário de saída, horário de chegada, nome da linha, área, nome da região, nome da empresa.

**Nome: Consulta de Fiscalização**

**Objetivo:** O sistema possibilitará a consulta de uma fiscalização já armazenado no banco de dados do sistema e disponibilizar a informação para o usuário. Mostrando ao usuário do sistema os dados de cadastramento da fiscalização. A busca deverá ser realizada código identificador.

**Requisitos Não – Funcionais**

**Nome: Desempenho do sistema**

Objetivo: Toda mensagem de erro produzida deve ser clara e significativa, de modo a permitir que o usuário possa se recuperar do erro ou cancelar a operação.

**Nome: Desempenho do sistema**

Objetivo: Qualquer interação entre o usuário e o sistema não deve exceder 10 segundos.

**Nome: Segurança do sistema**

Objetivo: Somente usuários autorizados podem ter acesso à base de dados do sistema através de um login e senha.

**Nome: Segurança dos dados**

Objetivo: O sistema deverá possuir padronização para troca de informações entre o aplicativo móvel, o software, o banco de dados.

**Nome: Interfaces do software**

Objetivo: A interface do software e do aplicativo móvel deve ser intuitiva, possibilitando o fácil entendimento e uso da ferramenta.

# **Anexo 2**

**Empresa – CRTLSoftware*.***

***PSI – Política de Segurança da Informação.***

***Documento de Diretrizes e Normas Administrativas***

**PSI - Política de Segurança da Informação**

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da empresa para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país. Com a intenção de aumentar a segurança da infraestrutura tecnológica direcionada ao uso acadêmico, foi desenvolvida paralelamente uma Norma de Segurança da Informação

Educacional, visando a orientação de nossos clientes para a utilização dos ativos de tecnologia da informação disponibilizados.

Tais documentos encontram-se disponíveis na intranet da empresa, na seção SisNormas.

**OBJETIVOS**

Estabelecer diretrizes que permitam aos colaboradores da empresa seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo. Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações da empresa quanto à:

**Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

**Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

**Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

**APLICAÇÕES DA PSI**

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

**PSI - Política de Segurança da Informação**

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras. É também obrigação de cada colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência de

Sistemas sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

**PRINCÍPIOS DA PSI**

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela empresa pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços. A empresa, por meio da Gerência de Sistemas, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

**REQUISITOS DA PSI**

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores da empresa a fim de que a política seja cumprida dentro e fora da empresa. Deverá haver um comitê multidisciplinar responsável pela gestão da segurança da informação, doravante designado como Comitê de Segurança da Informação.

Tanto a PSI quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança.

Deverá constar em todos os contratos da empresa o anexo de Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os

**PSI - Política de Segurança da Informação**

Procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um termo de responsabilidade. Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à

Gerência de Sistemas e ela, se julgar necessário, deverá encaminhar posteriormente ao Comitê de Segurança da Informação para análise.

Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação. Todos os requisitos de segurança da informação, incluindo a necessidade de planos de

Contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pela empresa ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

A empresa exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis. Esta PSI será implementada na empresa por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

**PSI - Política de Segurança da Informação**

**DAS RESPONSABILIDADES ESPECÍFICAS**

**1 - Dos Colaboradores em Geral**

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a empresa e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

**2 - Dos Colaboradores em Regime de Exceção (Temporários)**

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança da Informação. A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de

motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

**3 - Dos Gestores de Pessoas e/ou Processos**

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão. Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da

PSI da empresa. Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da empresa. Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais. Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI, bem como aos termos da Norma Educacional.

**PSI - Política de Segurança da Informação**

**4.1 - Da Área de Tecnologia da Informação**

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais. Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes. Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI, e em sua versão educacional, pelas Normas de Segurança da Informação complementares. Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto,

Isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente. Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Garantir segurança especial para sistemas com acesso público, incluindo o ambiente educacional, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação. Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a empresa. Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela. O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custo diante.

Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

**PSI - Política de Segurança da Informação**

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.

os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção

da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.

Realizar auditorias periódicas de configurações técnicas e análise de riscos. Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

Monitorar o ambiente de TI, gerando indicadores e históricos de:

* Uso da capacidade instalada da rede e dos equipamentos.
* Tempo de resposta no acesso à internet e aos sistemas críticos da empresa.
* Períodos de indisponibilidade no acesso à internet e aos sistemas críticos da empresa.
* Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante).

**PSI - Política de Segurança da Informação**

* Atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

**4.2 - Da Área de Segurança da Informação**

Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação. Propor e apoiar iniciativas que visem à segurança dos ativos de informação da empresa.

Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pelo Comitê de Segurança da Informação.

Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da empresa, mediante campanhas, palestras, treinamentos e outros meios de marketing.

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação. Apresentar as atas e os resumos das reuniões do Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria. Manter comunicação efetiva com o Comitê de Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para a empresa.

Buscar alinhamento com as diretrizes corporativas da instituição.

**4.3 - Do Comitê de Segurança da Informação**

Deve ser formalmente constituído por colaboradores com nível hierárquico mínimo gerencial**,** nomeados para participar do grupo pelo período de um ano. A composição mínima deve incluir um colaborador de cada uma das áreas: GO, GD, CAS, AJ,

GEP, GCR, GMS e GES.

Deverá o CSI reunir-se formalmente pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a empresa. O CSI poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

**PSI - Política de Segurança da Informação**

Cabe ao CSI:

* Propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;
* Propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares; avaliar os incidentes de segurança e propor ações corretivas;
* Definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas de Segurança da Informação complementares.

**5 - DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE**

Para garantir as regras mencionadas neste PSI, bem como de sua versão educacional, a empresa poderá:

* Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede ‒ a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
* Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do

Comitê de Segurança da Informação.

* Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade.
* Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

**CORREIO ELETRÔNICO**

O objetivo desta norma é informar aos colaboradores da empresa quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo. O uso do correio eletrônico da empresa é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a empresa e também não cause impacto no tráfego da rede.

**PSI - Política de Segurança da Informação**

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da empresa para:

* Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição.
* Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar.
* Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a empresa ou suas unidades vulneráveis a ações civis ou criminais.
* Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação.
* Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas.
* Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades da empresa estiver sujeita a algum tipo de investigação.
* Produzir, transmitir ou divulgar mensagem que:
* Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da empresa.
* Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador.
* Contenha arquivos com código executável (.exe,. com, .bat, .pif, .js, .vbs, .hta, .src,.cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança.
* Vise obter acesso não autorizado a outro computador, servidor ou rede;
* Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
* Vise burlar qualquer sistema de segurança.
* Vise vigiar secretamente ou assediar outro usuário.
* Vise acessar informações confidenciais sem explícita autorização do proprietário.
* Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa.
* Inclua imagens criptografadas ou de qualquer forma mascaradas;
* Contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet).
* tenha conteúdo considerado impróprio, obsceno ou ilegal.

**PSI - Política de Segurança da Informação**

* Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros.
* Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas.
* Tenha fins políticos locais ou do país (propaganda política).
* Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.
* As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

|  |
| --- |
| * Nome do colaborador |
| * Gerência ou departamento |
| * Nome da empresa |
| * Telefone (s) |
| * Correio eletrônico |

**INTERNET**

Todas as regras atuais da empresa visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a empresa, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A empresa, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o

devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades

decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

**PSI - Política de Segurança da Informação**

A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades. Como é da empresa que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio. Somente os colaboradores que estão devidamente autorizados a falar em nome da empresa para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros. Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais

dispositivos legais. É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades na empresa e deverão providenciar o que for

necessário para regularizar a licença e o registro desses programas, desde que autorizados pela GES.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela Gerência de Sistemas.

Os colaboradores não poderão em hipótese alguma utilizar os recursos da empresa para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional. O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer

formato) poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias. Para tal, grupos de segurança, cujos integrantes deverão ser definidos pelos respectivos gestores, precisam ser criados a fim de viabilizar esse acesso especial. Mediante solicitação e aprovação da área técnica responsável, o uso de jogos será passível de concessão, em regime de exceção, quando eles tiverem natureza intrínseca às atividades de cursos relacionados ao desenvolvimento de jogos.

**PSI - Política de Segurança da Informação**

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Caso seja necessário, grupos de segurança deverão ser criados para viabilizar esse perfil de usuário especial e seus integrantes definidos pelos respectivos gestores.

Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado a empresa ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores não poderão utilizar os recursos da empresa deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores. O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea (MSN, ICQ e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisite formalmente à Gerencia de Sistemas.

Não é permitido acesso a sites de proxy.

**IDENTIFICAÇÃO**

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a empresa e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade). Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores. Todos os dispositivos de identificação utilizados na empresa, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

**PSI - Política de Segurança da Informação**

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a empresa e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas. O Departamento de Recursos Humanos da empresa é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

A Gerência de Sistemas responde pela criação da identidade lógica dos colaboradores na instituição, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários. Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a

sua senha conforme as orientações apresentadas. Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $%) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $

%) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel,

etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser

constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras. Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a Gerência de Sistemas da empresa. Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade). Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 45 (quarenta e cinco) dias, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os

**PSI - Política de Segurança da Informação**

logins com privilégios administrativos devem exigir a troca de senhas a cada 30 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de

Recursos Humanos deverá imediatamente comunicar tal fato ao Departamento de Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

**COMPUTADORES E RECURSOS TECNOLÓGICOS**

Os equipamentos disponíveis aos colaboradores são de propriedade da empresa, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico

da Gerência de Sistemas da empresa, ou de quem este determinar.

As gerências que necessitarem fazer testes deverão solicitá-los previamente à Gerência de Sistemas e/ou à Gerência de Materiais e Serviços, ficando responsáveis jurídica e tecnicamente pelas ações

realizadas. Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois

de sua disponibilização pelo fabricante ou fornecedor. Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no service desk.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

**PSI - Política de Segurança da Informação**

Arquivos pessoais e/ou não pertinentes ao negócio da empresa (fotos, músicas, vídeos, etc.) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os colaboradores da empresa e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Gerência de

Sistemas.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.Todos os computadores de uso individual deverão ter senha de Bios para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pela Gerência de Sistemas da empresa, que terá acesso a elas para manutenção dos equipamentos.

Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.

É vedada a abertura ou o manuseio de computadores ou outros equipamentos de

informática para qualquer tipo de reparo que não seja realizado por um técnico da Gerência de Sistemas da empresa ou por terceiros devidamente contratados para o serviço.

Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de

contingência mediante a autorização dos gestores das áreas e da área de informática.

É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.

O colaborador deverá manter a configuração do equipamento disponibilizado pela empresa, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade

como custo diante de informações.

**PSI - Política de Segurança da Informação**

Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.

Todos os recursos tecnológicos adquiridos pela empresa devem ter imediatamente suas senhas padrões (default) alteradas.

Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da empresa.

Tentar ou obter acesso não autorizado a outro computador, servidor ou rede. Burlar quaisquer sistemas de segurança.

Acessar informações confidenciais sem explícita autorização do proprietário.

Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).

Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

**DISPOSITIVOS MÓVEIS**

A empresa deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis. Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua Gerência de Sistemas, como: notebooks, smartphones e pendrives.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

**PSI - Política de Segurança da Informação**

A empresa, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na empresa, mesmo depois de terminado o vínculo contratual mantido com a instituição.

Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não carregá-los juntos.

O suporte técnico aos dispositivos móveis de propriedade da empresa e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs,

sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico da Gerência de Sistemas.

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da Gerência de Sistemas da empresa. A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do

fabricante.

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela empresa, notificar imediatamente seu gestor direto e a Gerência de Sistemas.

Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar a empresa e/ou a terceiros.

**PSI - Política de Segurança da Informação**

O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da empresa deverá submeter previamente tais equipamentos

ao processo de autorização da Gerência de Sistemas.

Equipamentos portáteis, como smart phones, palmtops, pen drives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, não serão validados para uso e conexão em sua rede corporativa.

**DATACENTER**

O acesso ao Datacenter somente deverá ser feito por sistema forte de autenticação. Por exemplo: biometria, cartão magnético entre outros.

Todo acesso ao Datacenter, pelo sistema de autenticação forte, deverá ser registrado (usuário, data e hora) mediante software próprio. Deverá ser executada semanalmente uma auditoria nos acessos ao Datacenter por meio do relatório do sistema de registro.

O usuário "administrador" do sistema de autenticação forte ficará de posse e administração do coordenador de infraestrutura, de acordo com o Procedimento de Controle de Contas Administrativas.

A lista de funções com direito de acesso ao Datacenter deverá ser constantemente atualizada, de acordo com os termos do procedimento de Controle de Acesso ao Datacenter, e salva no

diretório de rede. Nas localidades em que não existam colaboradores da área de tecnologia da informação, pessoas de outros departamentos deverão ser cadastradas no sistema de acesso para que possam exercer as atividades operacionais dentro do Datacenter, como: troca de fitas de backup, suporte em eventuais problemas, e assim por diante.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado, que deverá preencher a solicitação de acesso prevista no Procedimento

de Controle de Acesso ao Datacenter, bem como assinar o Termo de Responsabilidade. O acesso ao Datacenter, por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do Datacenter for comprometida, como por incêndio,

inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando. Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer colaborador responsável pela administração.

**PSI - Política de Segurança da Informação**

Liberação de acesso, conforme lista salva em Procedimento de Controle de Acesso ao Datacenter.

Deverão existir duas cópias de chaves da porta do Datacenter.

Uma das cópias ficará de posse do coordenador responsável pelo Datacenter, a outra, de posse do coordenador de infraestrutura.

O Datacenter deverá ser mantido limpo e organizado.

Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de

Serviços Gerais. Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pelo responsável do Datacenter, de acordo com os termos do Procedimento de Controle e Transferência de Equipamentos.

No caso de desligamento de empregados ou colaboradores que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da

lista de colaboradores autorizados, de acordo com o processo definido no Procedimento de Controle de Acesso ao Datacenter.

**BACKUP**

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de

backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida

(quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter.

**PSI - Política de Segurança da Informação**

As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial. Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de backup nos termos do Procedimento de Controle de Mídias de Backup. As mídias de backups históricos ou especiais deverão ser armazenadas em instalações seguras,

preferencialmente com estrutura de sala-cofre, distante no mínimo 10 quilômetros do Datacenter. Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios da empresa, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade nos termos do Procedimento de Controle de Backup e Restore. Quaisquer atrasos na execução de backup ou restore deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Mídias de Backup.

Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo coma criticidade do backup.Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

**PSI - Política de Segurança da Informação**

Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo coordenador de infraestrutura, nos termos do Procedimento de Controle de Backup e Restore. Os colaboradores responsáveis descritos nos devidos procedimentos e na planilha de responsabilidade poderão delegar a um custo diante a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custo diante não poderá se eximir da

responsabilidade do processo.

**DAS DISPOSIÇÕES FINAIS**

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da empresa ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.