

**Tiago Teixeira**

***Controle de Fluxo de Pessoas Usando RFId***

São José – SC

agosto / 2011

**Tiago Teixeira**

## ***Controle de Fluxo de Pessoas Usando RFId***

Monografia apresentada à Coordenação do  
Curso Superior de Tecnologia em Sistemas  
de Telecomunicações do Instituto Federal de  
Santa Catarina para a obtenção do diploma de  
Tecnólogo em Sistemas de Telecomunicações.

Orientador:

Prof. Márcio Henrique Doniak, M. Eng.

CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES  
INSTITUTO FEDERAL DE SANTA CATARINA

São José – SC

agosto / 2011

Monografia sob o título “*Controle de Fluxo de Pessoas Usando RFId*”, defendida por Tiago Teixeira e aprovada em 17 de agosto de 2011, em São José, Santa Catarina, pela banca examinadora assim constituída:

---

Prof. Márcio Henrique Doniak, M. Eng  
Orientador

---

Prof. Ederson Torresini, Mr.  
IFSC

---

Prof. Deise Monquelate Arndt, Tecg.  
IFSC

*A ideia de pessoa de mau caráter é, no fundo,  
uma maneira de expressão de preconceitos sobre pessoas diferentes de nós.*

*Autor Desconhecido*

# *Agradecimentos*

À Deus em primeiro lugar, pelo dom da vida e por tudo o que nela conquistei e ainda conquistarei.

À minha família, pelo exemplo de vida, por me incentivar aos estudos e estar sempre presente.

Ao meu orientador, pelo auxílio, compreensão, paciência e flexibilidade ao longo do trabalho.

Aos meus colegas, por todos os bons momentos e experiências de vida que tivemos e todos os maus momentos que superamos juntos.

Aos professores, tanto aos que me ajudaram nesta longa jornada de estudos, quanto aos que tornaram o caminho ainda mais cheio de obstáculos.

Ao Instituto Federal de Santa Catarina, que por tantos anos me forneceu estrutura de qualidade, educação de alto nível e formação profissional e pessoal, tornando-se praticamente meu segundo lar.

E a todos aqueles que me ajudaram ou incentivaram, tanto na conclusão do trabalho, quanto no decorrer do curso: muito obrigado!

# *Resumo*

A tecnologia de RFId ou identificação por radiofrequência, pode ser considerada uma evolução da comunicação sem fio que foi desenvolvida devido à miniaturização dos componentes eletrônicos. Um sistema de RFId é formado basicamente por: tag (etiqueta), antena, leitor e módulo de *middleware* (*software* final). Esta tecnologia permite realizar a coleta de dados remotamente e, na maioria das vezes, de forma mais rápida que os métodos convencionais. As tags têm vida útil praticamente infinita, não têm necessidade de manutenção e ainda podem ser reutilizadas (por outros usuários, ou para diferentes aplicações). Um aplicativo de controle de fluxo que utilize a tecnologia de RFId pode ser muito útil em empresas, pois, com ele é possível controlar o acesso às áreas restritas da instituição, registrar o horário de entrada e saída de cada colaborador e até o deslocamento deles pela empresa. Este trabalho apresenta a tecnologia de identificação por radiofrequência (RFId), destacando o desenvolvimento de um aplicativo de controle de fluxo de pessoas que demonstra a viabilidade de um sistema de RFId e exemplifica como esta tecnologia pode ser inserida de forma simples nas instituições. Para comprovar e exemplificar o potencial de uso desta tecnologia, foi realizado um experimento gerenciando o registro de entrada e saída de alunos em um ambiente escolar.

# *Abstract*

The *Radio Frequency Identification* (RFID) technology can be considered an evolution of wireless communication which was developed due to the miniaturization of electronic components. An RFID system is basically formed by: tag (label), antenna, reader and middleware module (final software). This technology allows you to perform remote data collection and, in most cases, faster than conventional methods, your tags have virtually infinite shelf life, needs no maintenance and can still be reused (to other users, or for different applications.). The access control that uses RFID technology can be very useful in business, because with it you can control access to restricted areas of the institution, register the time of entry and exit of each employee and their dislocation through the company remotely, other words, imperceptible to people. This paper presents the RFID technology, highlighting the development of an application control flow of people that demonstrates the feasibility of an RFID system and exemplifies how this technology can be simply inserted in the institutions. To demonstrate and illustrate the potential use of this technology, an experiment was conducted managing the registration of incoming and outgoing students in a school environment.

# *Sumário*

## **Lista de Figuras**

## **Lista de Tabelas**

<b>1</b>	<b>Introdução</b>	p. 14
1.1	Motivação . . . . .	p. 15
1.2	Organização do texto . . . . .	p. 15
<b>2</b>	<b>Fundamentação Teórica de RFID</b>	p. 16
2.1	Definição . . . . .	p. 16
2.2	Contextualização Histórica . . . . .	p. 17
2.3	Componentes do Sistema de RFID . . . . .	p. 20
2.3.1	Tag . . . . .	p. 21
2.3.1.1	Utilização da Bateria . . . . .	p. 22
2.3.1.1.1	Tag Passiva . . . . .	p. 22
2.3.1.1.2	Tag Semi-passiva . . . . .	p. 22
2.3.1.1.3	Tag Ativa . . . . .	p. 23
2.3.1.2	Forma de Encapsulamento . . . . .	p. 23
2.3.1.2.1	Botões, Discos e Moedas . . . . .	p. 23
2.3.1.2.2	Cartões . . . . .	p. 24
2.3.1.2.3	Rótulos de Papel . . . . .	p. 24
2.3.1.2.4	Cápsulas de Vidro . . . . .	p. 24
2.3.1.3	Frequência . . . . .	p. 25



2.3.1.3.1	<i>Low Frequency (LF)</i> . . . . .	p. 25
2.3.1.3.2	<i>High Frequency (HF)</i> . . . . .	p. 26
2.3.1.3.3	<i>Ultra High Frequency (UHF)</i> . . . . .	p. 26
2.3.1.3.4	<i>Microwave Frequency (MF)</i> . . . . .	p. 26
2.3.1.4	Acoplamento . . . . .	p. 27
2.3.1.4.1	Difuso de Retorno . . . . .	p. 27
2.3.1.4.2	Indutivo . . . . .	p. 27
2.3.1.4.3	Magnético . . . . .	p. 28
2.3.1.5	Capacidade de Armazenamento . . . . .	p. 28
2.3.1.5.1	<i>Eletronic Article Surveillance</i> . . . . .	p. 29
2.3.1.5.2	<i>Surface Acoustic Wave</i> . . . . .	p. 29
2.3.1.5.3	<i>N-bit Transponder</i> . . . . .	p. 30
2.3.2	Antena . . . . .	p. 30
2.3.2.1	Leiaute das Antenas . . . . .	p. 31
2.3.2.1.1	Portal . . . . .	p. 31
2.3.2.1.2	Túnel . . . . .	p. 32
2.3.2.1.3	Portátil . . . . .	p. 32
2.3.2.1.4	Empilhadeira . . . . .	p. 33
2.3.2.1.5	Prateleira . . . . .	p. 33
2.3.3	Leitor . . . . .	p. 34
2.3.3.1	Estrutura dos Leitores . . . . .	p. 35
2.3.3.1.1	Parte Física . . . . .	p. 35
2.3.3.1.2	Parte Lógica . . . . .	p. 36
2.3.4	Módulo de <i>Middleware</i> . . . . .	p. 37
2.4	Padrões . . . . .	p. 37
2.4.1	EPC Global . . . . .	p. 38

2.4.2	ISO . . . . .	p. 39
2.4.3	Brasil-ID . . . . .	p. 40
2.5	Aplicações RFId . . . . .	p. 40
2.5.1	Identificação de Animais . . . . .	p. 40
2.5.2	Sistema Antirroubo de Carros . . . . .	p. 41
2.5.3	<i>Smart Cards</i> . . . . .	p. 41
2.5.4	Implantes em Humanos . . . . .	p. 42
2.5.5	Bibliotecas . . . . .	p. 42
2.5.6	Supermercados . . . . .	p. 43
2.6	Vantagens e Desvantagens da Tecnologia de RFId . . . . .	p. 43
2.7	Segurança e Privacidade . . . . .	p. 44
2.7.1	Segurança . . . . .	p. 44
2.7.2	Privacidade . . . . .	p. 46
2.8	RFId Versus Código de Barras . . . . .	p. 47
2.9	Futuro do RFId . . . . .	p. 48
<b>3</b>	<b>Aplicativo de Controle de Fluxo de Pessoas</b>	p. 50
3.1	Ambiente . . . . .	p. 50
3.2	Especificação . . . . .	p. 51
3.2.1	<i>Hardware</i> . . . . .	p. 51
3.2.2	<i>Software</i> . . . . .	p. 53
3.3	Aplicativo . . . . .	p. 53
3.3.1	<i>Software</i> de Monitoramento . . . . .	p. 53
3.3.1.1	Funções do <i>Software</i> de Monitoramento . . . . .	p. 55
3.3.2	<i>Software</i> de Gerenciamento . . . . .	p. 56
3.3.2.1	Banco de Dados . . . . .	p. 56
3.3.2.1.1	Tabelas do Banco de Dados . . . . .	p. 56

3.3.2.2	Funções do <i>Software</i> de Gerenciamento . . . . .	p. 58
3.4	Etapa de Testes . . . . .	p. 61
3.5	Resultados dos Testes . . . . .	p. 63
3.5.1	Consistência do <i>Software</i> . . . . .	p. 63
3.5.2	Desempenho do Sistema de RFId . . . . .	p. 64
3.6	Considerações Finais . . . . .	p. 65
3.7	Futuro do Aplicativo . . . . .	p. 65
<b>4</b>	<b>Conclusões</b>	p. 67
	<b>Lista de Abreviaturas</b>	p. 69
	<b>Referências Bibliográficas</b>	p. 71

## *Lista de Figuras*

2.1	Esquema básico do funcionamento de um sistema de RFId. . . . .	p. 17
2.2	A utilização da radiação refletida. . . . .	p. 18
2.3	Evolução tecnológica do RFId (1960 - 1990). . . . .	p. 19
2.4	Evolução tecnológica do RFId a partir de 1990. . . . .	p. 20
2.5	Exemplo de uma tag. . . . .	p. 21
2.6	Modelos de tags. . . . .	p. 21
2.7	Tag em formato de botão. . . . .	p. 23
2.8	Exemplo de um <i>smart card</i> . . . . .	p. 24
2.9	Exemplo de uma tag em formato de rótulo de papel. . . . .	p. 24
2.10	Tag de vidro implantada em uma pessoa. . . . .	p. 25
2.11	Acoplamento indutivo entre antena e tag. . . . .	p. 28
2.12	Exemplo de tag SAW. . . . .	p. 30
2.13	Modelos de antenas RFId. . . . .	p. 31
2.14	Exemplo de antena em formato de portal. . . . .	p. 32
2.15	Exemplo de antena em túnel. . . . .	p. 32
2.16	Exemplo de um leitor (RFId e código de barras) portátil com antena integrada. . . . .	p. 33
2.17	Exemplo de antena em uma empilhadeira. . . . .	p. 33
2.18	Ilustração de uma prateleira inteligente. . . . .	p. 34
2.19	Exemplo de leitor RFId. . . . .	p. 35
2.20	Componentes físicos de um leitor. . . . .	p. 36
2.21	Estrutura de um número EPC. . . . .	p. 38
2.22	Armazenamento de dados em uma tag. . . . .	p. 39

3.1	<i>Hardware</i> utilizado . . . . .	p. 52
3.2	Fluxograma do <i>software</i> de monitoramento . . . . .	p. 55
3.3	Ilustração da comunicação do <i>software</i> de gerenciamento com as tabelas do banco de dados . . . . .	p. 57
3.4	Tela de Login . . . . .	p. 58
3.5	Tela de Cadastro . . . . .	p. 59
3.6	Tela de Cadastro listando os usuários e IDs cadastrados . . . . .	p. 59
3.7	Tela de Menu . . . . .	p. 60
3.8	Tela de Geração de Relatórios . . . . .	p. 60
3.9	Sistema de RFId para testes . . . . .	p. 62
3.10	Exemplo de relatório gerado pelo <i>software</i> . . . . .	p. 63

## *Lista de Tabelas*

- 2.1 Classe de tags reconhecidas pela EPC Global . . . . . p. 39
- 2.2 Comparativo entre uma etiqueta de código de barras em uma tag RFId passiva p. 48

# 1 *Introdução*

A tecnologia de RFID é um método de identificação através de sinais de rádio, que recupera e armazena dados remotamente através dos componentes de seu sistema. O sistema de RFID é composto por quatro componentes, conhecidos, entre outras denominações, como: tag, *transceiver*, antena e *middleware*. Quando a antena é encontrada junto ao *transceiver*, ela é chamada de leitor.

Basicamente, o funcionamento da tecnologia de RFID ocorre da seguinte forma: o leitor, através de ondas eletromagnéticas energiza a tag, que responde transmitindo seu código de identificação. Então, o leitor recebe este código e o disponibiliza para o *middleware* que definirá a finalidade dos dados recebidos.

Como exemplos de aplicações comuns envolvendo esta tecnologia, podem ser citados as etiquetas de vigilância eletrônica, utilizadas em bibliotecas como método antifurto de acervo; os brincos de identificação usados no gado, que na verdade são tags RFID; e os *smart cards* utilizados no controle de acesso em *shoppings* e condomínios.

Foi realizado um estudo sobre a tecnologia de RFID, do qual serão abordados: a história da tecnologia, os principais componentes do sistema e suas classificações, a padronização, aplicações, vantagens e desvantagens de seu uso, a questão da segurança e da privacidade, entre outras características importantes. E foi desenvolvido um aplicativo de controle de fluxo de pessoas usando esta tecnologia.

Este trabalho descreve o estudo que foi realizado sobre a tecnologia e o desenvolvimento do aplicativo de controle de fluxo de pessoas, que é o objetivo principal deste trabalho. Para este aplicativo, foi realizada uma etapa de teste de campo para avaliar seu desempenho e correção de eventuais problemas, chegando a uma solução completa e de maior credibilidade. A referência para o desenvolvimento do aplicativo de controle de fluxo foi o registro de ponto de colaboradores em uma empresa.

## 1.1 Motivação

As aplicações atuais da tecnologia de RFId utilizadas no controle de fluxo de pessoas ainda não utilizam todo o potencial que um sistema de RFId disponibiliza. Esta tecnologia pode ser empregada não apenas para registrar o horário de entrada e saída de pessoas em uma instituição, mas também para restringir o acesso a determinadas áreas, definir o perfil de acesso dos ambientes, rastrear as pessoas dentro da instituição, etc. Portanto, a implementação de aplicativos que utilizem RFId no controle de fluxo de pessoas pode ser muito útil e vantajosa em empresas, escolas, condomínios e outros tipo de instituições em que este controle seja uma prática desejável. Além disso, participar de um projeto de pesquisa sério e trabalhar com uma tecnologia que está crescendo dentro do mercado corporativo também é razão de motivação.

Este trabalho foi desenvolvido com o financiamento de uma bolsa de Iniciação Tecnológica do programa PIBIT/CNPq, cujo título é: ‘Controle de Fluxo de Pessoas e Veículos Usando RFId’.

## 1.2 Organização do texto

Este trabalho está organizado com a seguinte estrutura: No primeiro capítulo foi apresentada uma breve introdução sobre as principais características da tecnologia de RFId e os objetivos, contribuições e motivações do trabalho. Já no segundo capítulo, será descrito o estudo que foi realizado sobre a tecnologia. No terceiro capítulo serão abordados o funcionamento e as etapas do desenvolvimento do aplicativo de controle de fluxo de pessoas. Finalizando, o quarto capítulo apresentará as conclusões do trabalho e prospecções para a expansão do projeto.



## 2 *Fundamentação Teórica de RFId*

Este capítulo apresenta: a definição da tecnologia de RFId, contextualização histórica, componentes do sistema e suas classificações, padronização, principais aplicações, vantagens e desvantagens do uso, segurança das informações, privacidade dos usuários do sistema, comparação entre as tecnologias de código de barras e RFId e futuro da tecnologia.

### 2.1 Definição

“A identificação por radiofrequência (RFId) é uma tecnologia capaz de captar, gerenciar, analisar e responder aos dados provenientes de sensores eletrônicos. (...) RFId é uma tecnologia de identificação que utiliza a radiofrequência para capturar os dados, permitindo que uma etiqueta RFId seja lida sem a necessidade de contato ou campo visual, através de barreiras e objetos tais como madeira, plástico, papel, entre outros. É um método de armazenamento e recuperação de dados de forma remota. Ele funciona como um sistema poderoso de aquisição de dados em tempo real, com a vantagem de eliminar as intervenções humanas manuais e visuais, dinamizando assim o tempo de transições e assegurando eficiência e eficácia no processo.” (GREFF, 2009, p. 20).

O sistema de RFId possui quatro componentes básicos: tag, *transceiver* (leitor), antena e módulo de *middleware*. O funcionamento da tecnologia de RFId, como descrito em (NISHIDA, 2008), envolve uma tag que transmite seu código de identificação para o leitor (*reader*), este recebe o código e o disponibiliza para o aplicativo que definirá qual será a funcionalidade do sistema de RFId. Este funcionamento pode ser visualizado na Figura 2.1.

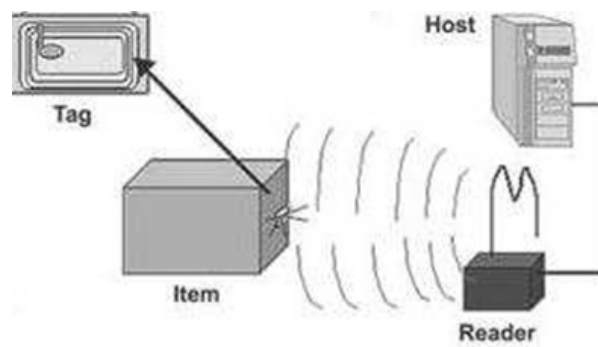


Figura 2.1: Esquema básico do funcionamento de um sistema de RFID.

FONTE: (GLOVER; BHATT, 2007)

## 2.2 Contextualização Histórica

É consenso entre os pesquisadores que a tecnologia de identificação por radiofrequência está fundamentada nas descobertas da indução mútua ou eletromagnética de Faraday e que seu princípio de funcionamento tem raízes nas transmissões por rádio e por radar, utilizados na Segunda Guerra Mundial (DOBKIN, 2008). Os alemães, americanos, ingleses e japoneses utilizavam o radar para ter conhecimento da presença de aviões com antecedência, enquanto eles ainda estavam muito distantes.

“Contudo, a simples descoberta da presença da aeronave não garantia estarem livres de ataques, pois muitas vezes havia falha na transmissão dos dados de identificação. Não se sabia de que lado estava a aeronave, se ela era inimiga.”, explica (GREFF, 2009, p. 14). Então, os alemães descobriram que se seus pilotos girassem os aviões quando estivessem retornando à base (radiação refletida), como na Figura 2.2, iriam modificar o sinal de rádio, que seria refletido de volta ao radar localizado na base terrestre. Este artifício alertava os técnicos responsáveis pelo radar que se tratava de um avião alemão (este é considerado o primeiro sistema passivo de RFID).

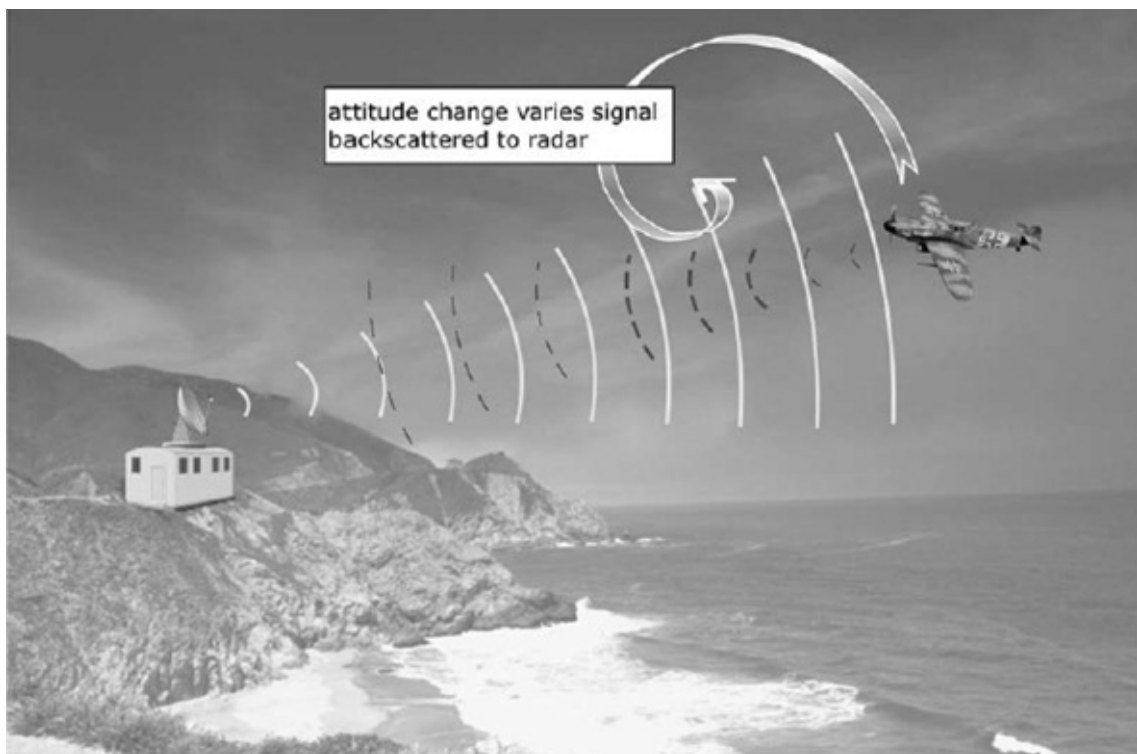


Figura 2.2: A utilização da radiação refletida.  
FONTE: (DOBKIN, 2008)

Os primeiros sistemas de RFID eram muito complexos e possuíam poucos recursos e aplicações, mas ao decorrer dos anos, eles tiveram uma vasta evolução tecnológica. Na década de 60 começaram a ser comercializados sistemas anti-roubo que utilizavam ondas de rádio para identificar se determinado item havia sido pago. Estas tags RFID, denominadas de ‘etiquetas de vigilância eletrônica’, são utilizadas até hoje.

Em 1970, empresas como a RCA, Fairchild e Raytheon começaram a fazer pesquisas sobre RFID. Por volta deste mesmo ano, o governo dos Estados Unidos também realizava pesquisas sobre a tecnologia, e o laboratório nacional de Los Alamos teve um pedido do departamento de energia para desenvolver um sistema rastreador de materiais nucleares. Um grupo de cientistas idealizou um projeto onde eram colocadas tags nos caminhões transportadores e leitores posicionados estrategicamente nos locais de acesso permitidos para receber esses materiais. Este sistema foi comercializado posteriormente, na década de 80, para automatizar praças de pedágio, sistema muito utilizado até hoje.

“Em 23 de janeiro de 1973 Mario W. Cardullo reivindicou a primeira patente americana por uma etiqueta de RFID ativa com possibilidade de gravar informações nas memórias das tags. No mesmo ano, um empreendedor americano chamado Charles Walton recebeu a patente por um transponder passivo usado para destravar uma porta sem precisar usar chaves. (...) Outro setor dos Estados Unidos que se interessou pelo processo de automação proporcionado pelo RFID foi o da agropecuária. Os cientistas do Laboratório Nacional de Los Alamos, que também haviam criado o sistema para controle de veículos nos pedágios, desenvolveram um tag passivo para o rastreamento de vacas utilizando frequências mais altas. Algum tempo depois foi desenvolvido um RFID que operava em frequência baixa (low-frequency) a 125KHz, possibilitando desenvolvimento de tags menores, sendo assim mais práticos para a implantação sob a pele dos animais através de uma cápsula de vidro. Este sistema é utilizado ainda hoje em animais e também em controles de acesso restrito em prédios.” (HECKEL, 2007, p. 40).

A Figura 2.3 ilustra a evolução tecnológica do RFID entre as décadas de 60 e 90.

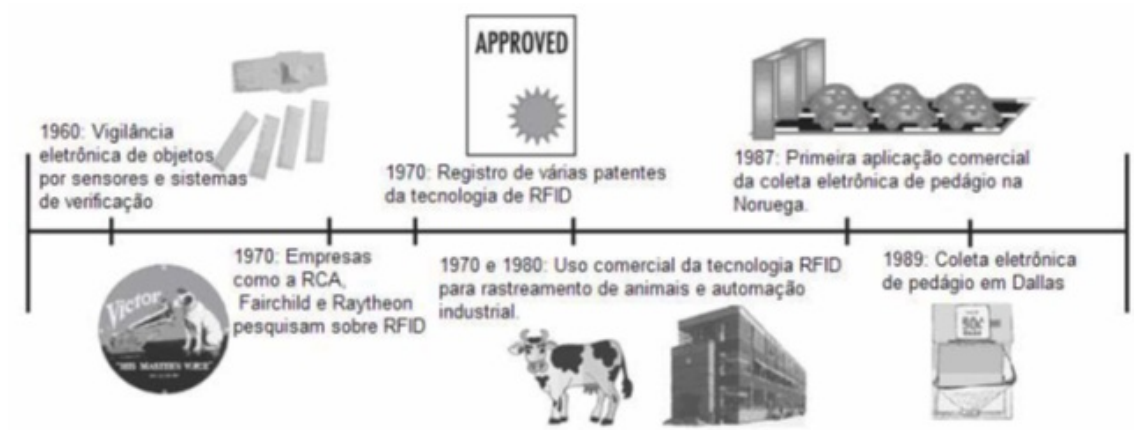


Figura 2.3: Evolução tecnológica do RFID (1960 - 1990).

FONTE: (SHAHRAM; MANISH, 2005)

No ano de 1990, como explicam (SHAHRAM; MANISH, 2005): a E-Z PASS iniciou um trabalho de padronização da tecnologia de RFID; houve o surgimento de novas aplicações em vários segmentos do mercado, como no setor logístico, automobilístico e de vestuário; e trens de ferro nos Estados Unidos foram equipados com esta tecnologia. Em 1991, a Texas Instruments criou a TIRIS, divisão da empresa responsável pela produção e desenvolvimento da tecnologia de RFID, com o objetivo de realizar pesquisas avançadas sobre a mesma. Também no começo desta década, engenheiros da IBM desenvolveram e patentearam um sistema de RFID baseado na tecnologia *Ultra High Frequency* (UHF).

Em 1999, o *Uniform Code Council* (UCC), a *European Article Number* (EAN) Internacional, a *Procter e Gamble* e a *Gillette* se uniram e financiaram a criação do *Auto-ID Center* no *Massachusetts Institute of Technology* (MIT). Este era um centro de pesquisas sobre RFID que abordava principalmente os benefícios da frequência UHF. O UCC juntamente à EAN

Internacional criaram a EPC Global, responsável pela regulamentação do *Electronic Product Code* (EPC) que é um código padronizado para compor as identificações das tags, como descreve (HECKEL, 2007).

No ano 2000, a rede de supermercados Wal-Mart exigiu de seus fornecedores o uso da tecnologia de RFId para identificar produtos. Em 2003, a EPC Global criou um laboratório de *Auto-ID Center* no *Massachusetts Institute of Technology* (MIT), e iniciou pesquisas em cinco das maiores universidades de pesquisas do mundo (Harvard – EUA, Cambridge – Inglaterra, Oxford – Inglaterra, MIT – EUA, Stanford – EUA), envolvendo mais de cem empresas do mundo, representando uma ampla rede de indústrias com diferentes necessidades e interesses.

Cada vez mais, o *Auto-ID Center* ganhou o apoio de inúmeras empresas e até do próprio Departamento de Defesa dos Estados Unidos, tanto que em 2003, este departamento utilizou a tecnologia de RFId na operação de libertação do Iraque. A Figura 2.4 ilustra a evolução tecnológica do RFId a partir da década de 90.

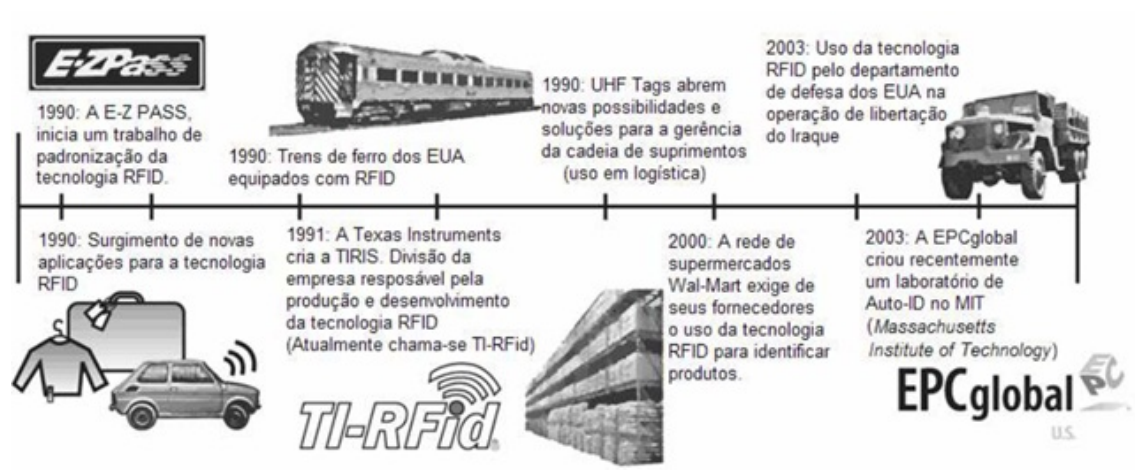


Figura 2.4: Evolução tecnológica do RFId a partir de 1990.

FONTE: (SHAHAM; MANISH, 2005)

Conforme pôde ser observado, a tecnologia de RFId vem evoluindo a ponto de se tornar uma poderosa ferramenta no processo de automação e controle de processo nas empresas. Algumas tecnologias de RFId já possuem alguns anos e são utilizadas praticamente sem alterações nos dias atuais.

## 2.3 Componentes do Sistema de RFId

A arquitetura geral de um sistema de RFId pode variar de acordo com a bibliografia. Alguns autores como (AHSON; ILYAS, 2008) a consideram possuindo apenas dois componentes: tag

e leitor. Contudo, por motivos didáticos e para facilitar a compreensão da arquitetura de RFId, neste trabalho ela será dividida em quatro componentes básicos: tag, antena, leitor e módulo de *middleware*. A tecnologia de RFId utiliza frequências dentro da faixa de 30 kHz e 30 GHz. Nas próximas seções serão apresentados os principais componentes e classificações do sistema de RFId.

### 2.3.1 Tag

A tag, também chamada de *transponder*, identificador ou etiqueta RFId, é formada basicamente por um *microchip* de silício e uma antena, como mostra a Figura 2.5.

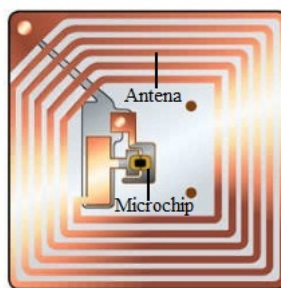


Figura 2.5: Exemplo de uma tag.  
FONTE: (SANTINI, 2006) (Modificada)

Normalmente, as tags estão envoltas em plástico, podendo ser encapsuladas em diversos formatos, como ilustra a Figura 2.6. Dependendo da utilização das tags a escolha do formato é fundamental, levando-se em conta a durabilidade, resistência a mudanças de temperatura e acessibilidade (HECKEL, 2007).



Figura 2.6: Modelos de tags.  
FONTE: (CUNHA, 2005)

O objetivo de uma tag é identificar o ser vivo, objeto, ou local ao qual está anexada devido ao seu número único de identificação (que também pode ser composto por *strings*): o EPC.

Há vários tipos de tags disponíveis no mercado que satisfazem às diversas necessidades das aplicações. Logo, as tags podem ser classificadas por suas diferentes características, como: a utilização da bateria, forma de encapsulamento, frequência, acoplamento e capacidade de armazenamento.

#### **2.3.1.1 Utilização da Bateria**

A fonte de energia é o principal fator de classificação das tags. Quanto à forma de energia que utilizam, segundo (GREFF, 2009), elas podem ser classificadas em passivas, semi-passivas e ativas.

##### **2.3.1.1.1 Tag Passiva**

A tag passiva contém, normalmente, memória do tipo *Read Only Memory* (ROM) e apenas responde ao sinal emitido pela antena ligada ao leitor. Ela opera sem bateria, sendo que sua alimentação é fornecida pelo próprio leitor através de ondas eletromagnéticas. Este tipo de tag possui alcance médio menor e durabilidade teoricamente infinita, uma vez que sua vida útil só tem como fator limitante o seu bom uso (FAHL, 2005).

Por trabalhar numa frequência mais baixa, essas tags são mais suscetíveis a ruídos e a perdas de sinal em relação a fatores climáticos, barreiras e outras imposições. Contudo, o custo dos modelos passivos é bem inferior, e tem uma vida útil bem mais elevada, se comparado aos modelos ativos.

##### **2.3.1.1.2 Tag Semi-passiva**

A tag semi-passiva é muito similar à passiva, porém, incorpora uma pequena bateria que permite que o circuito integrado de leitura seja constantemente alimentado; e tem um tempo de resposta mais rápido, pois é mais potente em seu raio de leitura. Este tipo de tag não possui um transmissor ativo, fato este que o diferencia das tags ativas.

Este tipo de tag é utilizado em sistemas de tempo real para rastreamento de materiais de alto valor ou equipamentos dentro de uma fábrica. Outra aplicação da tag semi-passiva é nos sensores de controle de temperatura, pressão, umidade relativa do ar, aceleração, vibração, movi-

mento e altitude em produtos que exijam esse monitoramento. Ela possui melhor capacidade de leitura quando anexada à materiais opacos e absorventes (GREFF, 2009).

#### **2.3.1.1.3 Tag Ativa**

A tag ativa é alimentada por uma bateria interna, o que torna seu tempo de vida limitado. Este tipo de tag tem a característica de transmitir o próprio sinal, operando em altas frequências. Isto faz com que não seja necessária a utilização de várias antenas para cobrir um espaço, já que seu raio de alcance é maior.

As principais vantagens da tag ativa são: realizar processos de escrita e leitura, maior capacidade de memória e tolerância a ruídos e a perdas de sinal. Suas grandes desvantagens são: alto custo (em relação às tags passivas), tamanho e tempo de vida finito da bateria.

#### **2.3.1.2 Forma de Encapsulamento**

As tags podem ser colocadas em botões, cartões de plástico, rótulos de papel, cápsulas de vidro, relógios, pulseiras, brincos, chaveiros, chaves, etc. Podem ser fixadas em produtos ou embalagens, presas a peças de roupa, colocadas em animais ou até mesmo em pessoas.

Dependendo da utilização das tags, a escolha do formato é fundamental, levando-se em conta: durabilidade, resistência, mudanças de temperatura e acessibilidade. De acordo com (HECKEL, 2007), as principais formas de encapsulamento são:

##### **2.3.1.2.1 Botões, Discos e Moedas**

São utilizadas quando a resistência do material é importante. Normalmente são feitas de plástico, como a da Figura 2.7, ou PVC e suportam temperaturas mais altas.



Figura 2.7: Tag em formato de botão.  
FONTE: (SANTINI, 2006)



### 2.3.1.2.2 Cartões

São utilizadas em *smart cards*, como o da Figura 2.8, que são cartões que não precisam de contato. Estes cartões, ou crachás, costumam ser utilizados em controle de acesso.

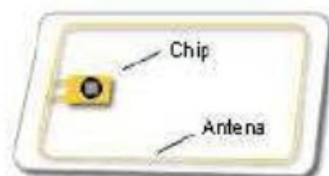


Figura 2.8: Exemplo de um *smart card*.  
FONTE: (OLIVEIRA; PEREIRA, 2006)

### 2.3.1.2.3 Rótulos de Papel

Estas tags, também chamadas de *smart labels*, são semelhantes aos códigos de barra e geralmente são aplicadas diretamente em caixas. São tags passivas (não possuem bateria), por isso seu tamanho é reduzido; e são ativadas apenas quando entram na área de cobertura do leitor. Este deverá ser o tipo de tag utilizado nos casos em que o RFId possa substituir o código de barras. Uma tag em formato de rótulo de papel pode ser visualizada na Figura 2.9.



Figura 2.9: Exemplo de uma tag em formato de rótulo de papel.  
FONTE: (SANTINI, 2006)

### 2.3.1.2.4 Cápsulas de Vidro

As tags no formato de cápsulas de vidro são ideais para realizar implantes em seres humanos, como o da Figura 2.10. Este formato tem grande perspectiva de crescimento e popularização no mercado, pois ele pode ser usado para abrir a porta de casa ou ligar o carro sem a

necessidade de chaves, pelo simples balançar do braço. “Os implantes em seres humanos geralmente são feitos na parte frontal da mão, sobre o músculo adutor do polegar, entre o músculo interósseo dorsal I, normalmente o tamanho desta tag é de 1 cm”. (SANTINI, 2006, p. 20).



Figura 2.10: Tag de vidro implantada em uma pessoa.  
FONTE: (HECKEL, 2007)

### 2.3.1.3 Frequência

As tags RFId também podem ser classificadas de acordo com a frequência em que operam. A frequência é um fator muito importante na adoção de um sistema de RFId, pois, de acordo com ela, haverá um maior ou menor raio de alcance. Além disso, para (GLOVER; BHATT, 2007, p. 53) “diferentes frequências possuem diferentes propriedades. Sinais de frequência mais baixos são mais capazes de viajar pela água, enquanto que frequências mais altas podem carregar mais informações.” Outro fator no qual a frequência influencia é a taxa de transferência de dados: quanto maior a frequência, maior é a taxa de transferência de dados.

Diferentes frequências são utilizadas em diferentes aplicações. As faixas de frequência nas quais as tags operam são:

#### 2.3.1.3.1 Low Frequency (LF)

A faixa de baixa frequência (LF) inclui frequências entre 30 kHz e 300 kHz, não sendo necessária a regulamentação. Uma vantagem desta faixa é que ela penetra na maioria dos materiais, como metais, água e na própria pele do corpo humano. Sua maior desvantagem é a interferência que pode ser causada por motores elétricos em ambientes industriais (MOROZ,

2004). A frequência de 125 kHz é a mais utilizada em sistemas de RFId, embora também existam aplicações que utilizem a frequência de 134 kHz.

As tags LF possuem a mais baixa taxa de transferência de dados dentre todas as frequências utilizadas em RFId e geralmente são usadas para armazenar uma pequena quantidade de dados. A área de cobertura deste sinal pode atingir de poucos centímetros até 1,5 m, porém, essas tags geralmente são mais caras que as demais. Exemplos de aplicação: identificação de animais, identificadores anexados em materiais com grande umidade ou próximos a metais, controle de acesso, controle de automóveis, imobilizadores de veículos, etc.

#### **2.3.1.3.2 High Frequency (HF)**

A faixa de alta frequência (HF) inclui frequências entre 3 MHz e 30 MHz, sendo que as tags HF operam tipicamente em 13.56 MHz. Como vantagem sobre as tags que operam em LF, estas tags transmitem dados mais rapidamente e podem armazenar um maior número de dados. Como desvantagem, a faixa HF é mais suscetível a interferências quando as tags estão próximas a metais, e por este motivo, seu custo é inferior. As tags HF geralmente são passivas, e tem alcance de leitura de até 1,5 m. Exemplos de aplicação: *smart cards*, cartões de crédito, livros, bagagem aérea, bibliotecas, passaportes eletrônicos (*e-passaportes*), etc.

#### **2.3.1.3.3 Ultra High Frequency (UHF)**

A faixa de ultra alta frequência (UHF) inclui frequências entre 300 MHz e 3 GHz, sendo que apenas as frequências de 433 MHz e de 860 MHz à 960 MHz são utilizadas para aplicações de RFId. A primeira é utilizada por tags ativas e a segunda por tags passivas ou semi-passivas. Esta faixa é utilizada quando os leitores precisam ler tags a uma distância maior do que as obtidas pelas faixas LF e HF. Estas tags podem ser facilmente acopladas à diversos tipos de materiais. Seu processo de fabricação é relativamente simples, contribuindo para baixar seu custo. Todos os protocolos na faixa UHF oferecem capacidade anti-colisão, permitindo que várias etiquetas sejam lidas simultaneamente. Exemplos de aplicação: identificação de caixas, rastreamento especial de animais e logística.

#### **2.3.1.3.4 Microwave Frequency (MF)**

A faixa de micro-ondas (MF) inclui frequências entre 2 GHz e 30 GHz, sendo que apenas a frequência de 2,45 GHz é utilizada em aplicações de RFId. As tags MF alcançam distâncias maiores que as demais e podem ser utilizadas por tags passivas, semi-passivas e ativas. As tags passivas são menos comuns no mercado, pois são mais caras que as tags passivas UHF e compartilham as mesmas vantagens e desvantagens; as semi-passivas são usadas no controle de acesso de longo alcance para veículos, identificação de frota e coleta de pedágios em rodovias; e as ativas são utilizadas para sistemas de localização em tempo real (GREFF, 2009).

#### **2.3.1.4 Acoplamento**

A forma de acoplamento é o modo como as tags irão se comunicar com os leitores, podendo ser alimentadas por eles no caso de tags passivas. Cada uma das formas de acoplamento utiliza uma frequência específica e são recomendadas de acordo com a distância entre leitor e tag.

Os tipos de acoplamento mais utilizados, segundo (HECKEL, 2007), são:

##### **2.3.1.4.1 Difuso de Retorno**

O acoplamento difuso de retorno, também chamado de *backscatter*, é utilizado em algumas tags ativas e em tags passivas que precisam ser alimentadas pelo leitor. As tags que utilizam este tipo de acoplamento refletem a frequência do leitor para gerar energia, que varia de poucos microwatts até alguns miliwatts. Conforme descrevem (GLOVER; BHATT, 2007), o *chip* existente na tag controla um resistor que pode refletir o sinal do leitor numa amplitude menor, assim pode ser criado um sinal *Amplitude Shift Keying* (ASK) modulado para transmitir o número de Identificação (ID) único armazenado na memória do *chip*.

##### **2.3.1.4.2 Indutivo**

O acoplamento indutivo é considerado um acoplamento remoto e também é utilizado em tags passivas que precisam da energia dos leitores. O dispositivo de leitura gera um campo eletromagnético nas frequências de 135 KHz ou 13,56 MHz, que penetra na área da bobina da tag e induz uma tensão que é retificada e utilizada para alimentar o *chip*, que enviará o seu ID para o dispositivo de leitura. Seu funcionamento ocorre quando a tag está na área de cobertura do leitor (zona de interrogação) e sua frequência de ressonância corresponde a frequência do dispositivo de leitura. A modulação dos dados pode ser feita por ASK, *Frequency Shift Keying*

(FSK) ou *Phase Shift Keying* (PSK). “A faixa de leitura das tags que utilizam esse modo de acoplamento é de cerca de 10 cm, podendo ser aumentada conforme o tamanho das antenas utilizadas.” (HECKEL, 2007, p. 49)

A Figura 2.11 exemplifica o acoplamento indutivo de uma tag e uma antena de um sistema RFId passivo. O princípio é similar ao de um transformador, onde a antena transfere energia e os dados são trocados entre os dois elementos.

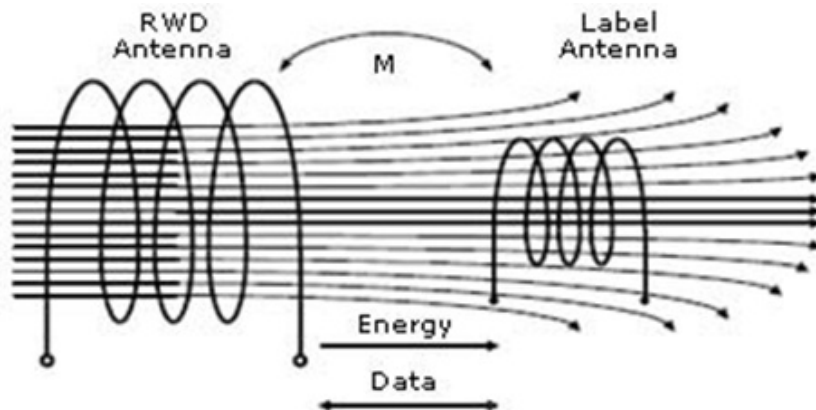


Figura 2.11: Acoplamento indutivo entre antena e tag.  
FONTE: (MARTINS, 2005)

#### 2.3.1.4.3 Magnético

O acoplamento magnético é muito parecido com o indutivo, com a diferença de que a antena do leitor de acoplamento magnético é em forma de ‘U’. A distância entre o leitor e a tag não deve passar de 1 cm. Este tipo de acoplamento, conforme explicam (SANTOS; JÚNIOR, 2003, p. 13), “se baseia no princípio de proximidade eletromagnética e necessita que a área do tag em ‘contato magnético’ seja máxima, (...) o fluxo eletromagnético deve fluir por toda a ‘antena’ do tag, caso contrário este não recebe energia suficiente para entrar em operação”.

#### 2.3.1.5 Capacidade de Armazenamento

As tags também podem ser classificadas quanto à capacidade de armazenamento. Deve-se analisar cada caso para decidir qual o melhor tipo de tag a ser utilizada, pois quanto maior a disponibilidade de memória maior também será o custo. Segundo (HECKEL, 2007), as tags podem ter de um bit até alguns bytes e podem ser classificadas em:

#### 2.3.1.5.1 *Eletronic Article Surveillance*

As tags *Eletronic Article Surveillance* (EAS) ou tags de vigilância eletrônica de artigos, também chamadas de ‘1 bit *transponder*’, são passivas e podem possuir *microchips* (OLIVEIRA; PEREIRA, 2006) . Elas apenas podem comunicar se estão ligadas (através de um bit de valor 1) ou se estão desligadas (bit igual a 0) (RFID-GET-STARTED, 2011). É o tipo de tag mais barata e também a mais utilizada no mercado. Sua principal aplicação é no controle de objetos e seus locais comuns de utilização são: bibliotecas, locadoras de filmes e lojas comerciais.

#### 2.3.1.5.2 *Surface Acoustic Wave*

As tags *Surface Acoustic Wave* (SAW) ou tags de onda acústica de superfície, possuem um ID único que vem gravado de fábrica. Estas tags não têm baterias ou *microchips*, operam através de micro-ondas e seu ID não pode ser modificado.

Para (GLOVER; BHATT, 2007, p. 63):

“(...) a antena recebe o pulso de micro-ondas do leitor e o alimenta. O transdutor possui um cristal piezelétrico que vibra quando recebe o pulso de micro-ondas. Esta vibração cria uma onda acústica que viaja através da tag, encontrando tiras de refletor (à direita). As tiras refletem a parte de trás da onda, fazendo com que o cristal vibre novamente criando uma reflexão de difusão de retorno. O número e o espaçamento das tiras de refletor determinam o número e o tempo dos pulsos enviados de volta para o leitor, e também determina o número representado pelo identificador. Restrições práticas de tamanho também limitam os identificadores SAW a uma capacidade de 32 bits. (...) Identificadores SAW representam determinado número que o leitor ‘ilumina’ de forma que ele se torne visível.”.

A Figura 2.12 exemplifica uma tag SAW.

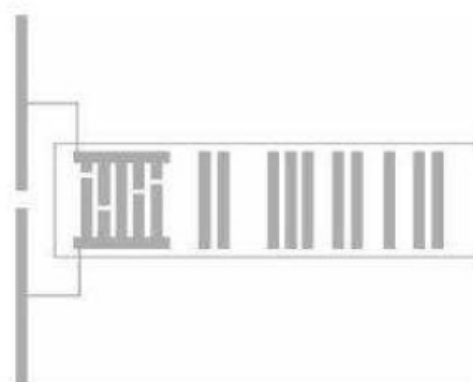


Figura 2.12: Exemplo de tag SAW.  
FONTE: (GLOVER; BHATT, 2007)

#### 2.3.1.5.3 N-bit Transponder

As tags n-bit *transponder* podem possuir mais informações que um simples ID. Para permitir a utilização de informações adicionais, pode-se utilizar a memória *Electrically-Erasable Programmable Read-Only Memory* (EEPROM). Estas tags são mais complexas que as demais, algumas delas utilizam criptografia e técnicas anti-colisão quando estão agrupadas com outras tags. Elas podem ser passivas ou ativas (normalmente são ativas), podendo ter microprocessadores completos.

A memória EEPROM é responsável, nas aplicações de RFId, por armazenar os dados na tag. Precisa ser não volátil para assegurar que os dados fiquem guardados quando o dispositivo está em seu estado de *standy-by* (repouso). Seu conteúdo pode ser apagado e regravado diversas vezes eletricamente. (SANTOS; JÚNIOR, 2003).

### 2.3.2 Antena

A antena, também chamada de bobina, realiza a comunicação dentro do sistema de RFId. Seu papel é definir como o campo eletromagnético será gerado, realizando de maneira confiável a troca de informações entre o leitor e a tag. A antena emite um sinal de rádio que ativa a tag, realizando a leitura ou escrita de dados, que depois de lidos são enviados ao *middleware* do sistema. Essa emissão de ondas de rádio é difundida em diversas direções e distâncias, dependendo da potência e da frequência utilizada. O tempo decorrido nesta operação é inferior a um décimo de segundo, portanto, o tempo necessário de exposição da tag é bem pequeno. As antenas são oferecidas em diversas formas e tamanhos, conforme a exigência operacional da

aplicação. Exemplos de antenas podem ser vistos na Figura 2.13.



Figura 2.13: Modelos de antenas RFId.  
FONTE: (CUNHA, 2005)

Tanto o leitor quanto as tags devem possuir uma antena para poder realizar a troca de informações. Contudo, a antena pode ser considerada um elemento a parte nos sistemas de RFId, já que em muitas aplicações, onde se exige uma maior mobilidade, as antenas são acopladas aos *transceivers*, sendo chamadas de leitores (CUNHA, 2005).

#### 2.3.2.1 Leiaute das Antenas

A característica mais importante das antenas é o leiaute que podem possuir junto aos leitores. Segundo (GLOVER; BHATT, 2007), estes leiautes podem ser de:

##### 2.3.2.1.1 Portal

São antenas e leitores projetados para reconhecer itens identificados. Geralmente, são colocados estrategicamente nas entradas e saídas de locais como depósitos, bibliotecas e estabelecimentos comerciais para identificação de produtos e segurança. São muito utilizadas no sistema EAS para vigilância eletrônica de artigos. Uma antena em formato de portal pode ser visualizada na Figura 2.14.





Figura 2.14: Exemplo de antena em formato de portal.  
FONTE: (HECKEL, 2007) (Modificada)

#### 2.3.2.1.2 Túnel

De acordo com (GLOVER; BHATT, 2007, p. 103), “um túnel é como um pequeno portal com a vantagem de que um túnel também pode incluir escudo RFId, que absorve a energia RF mal direcionada ou refletida que poderia interferir com outros leitores e antenas próximos.” Estas antenas são utilizadas em esteiras de linhas de montagem, como na Figura 2.15.

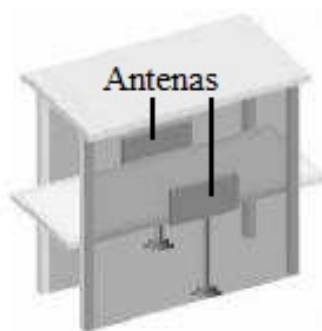


Figura 2.15: Exemplo de antena em túnel.  
FONTE: (DOBKIN, 2008) (Modificada)

#### 2.3.2.1.3 Portátil

Nos casos em que é inviável levar os itens até a antena, pode-se utilizar leitores móveis com antenas integradas, como o da Figura 2.16. “Alguns desses leitores podem ler tanto tags RFId

quanto códigos de barra, neste caso a praticidade é a maior vantagem” (HECKEL, 2007, p. 57).



Figura 2.16: Exemplo de um leitor (RFId e código de barras) portátil com antena integrada.  
FONTE: (DUARTE, 2005)

#### 2.3.2.1.4 Empilhadeira

São leitores com antenas integradas acoplados a empilhadeiras, assim como na Figura 2.17, para realizar a identificação de itens, geralmente caixas ou *containers*. Geralmente, são utilizados em fábricas e em portos.

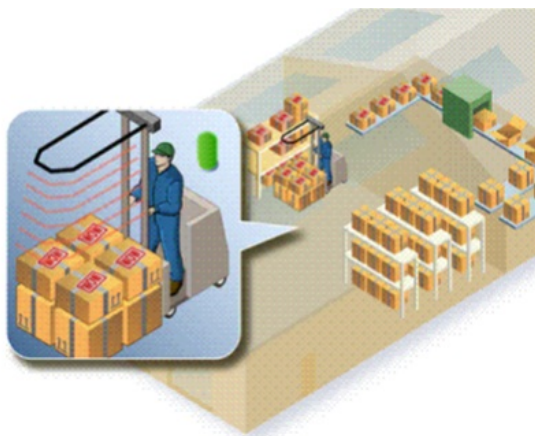


Figura 2.17: Exemplo de antena em uma empilhadeira.  
FONTE: (HECKEL, 2007)

#### 2.3.2.1.5 Prateleira

As chamadas prateleiras inteligentes, como a da Figura 2.18, são adaptadas a antenas que monitoram constantemente o fluxo de mercadorias. Através de sua utilização é possível acompanhar o estoque de produtos em tempo real e controlar características importantes, como a data de validade do produto (SANTINI, 2006).

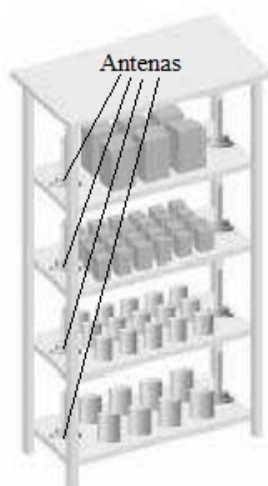


Figura 2.18: Ilustração de uma prateleira inteligente.  
FONTE: (GLOVER; BHATT, 2007) (Modificada)

### 2.3.3 Leitor

O leitor, também chamado de *transceiver*, *reader* ou interrogador, é o componente de comunicação entre o sistema de RFId e os sistemas externos de processamento de informação. A complexidade dos leitores depende do tipo de tag e das funções a serem aplicadas. Os leitores mais sofisticados apresentam funções de verificação de paridade de erro e correção de dados. Uma vez que os sinais do receptor sejam corretamente recebidos e decodificados, algoritmos podem ser aplicados para decidir se o sinal é uma transmissão de resposta de uma tag.

Os leitores emitem ondas de radiofrequência para alimentar as tags, que por sua vez retornam as informações solicitadas. (SANTANA, 2005) explica que quando a tag passa pela área de cobertura da antena, o campo magnético é detectado pelo leitor, que decodifica os dados codificados na tag, passando-os para o *middleware* realizar o processamento. A comunicação de dados entre tags e leitores é realizada sem contato físico, como mostra a Figura 2.19.



Figura 2.19: Exemplo de leitor RFId.  
FONTE: (HECKEL, 2007)

### 2.3.3.1 Estrutura dos Leitores

Para (SANTINI, 2006), os leitores possuem duas estruturas gerais: as partes física e a lógica.

#### 2.3.3.1.1 Parte Física

Os principais componentes físicos de um leitor RFId são: antena, controlador e interface de rede. A antena serve para realizar o acoplamento da energia de *Radio Frequency* (RF) entre o leitor e a etiqueta. Ela não precisa estar acoplada ao leitor, mas todo leitor deve possuir, no mínimo, uma antena. Um leitor pode controlar antenas remotas, estando sempre atento à atenuação do sinal.

O controlador tem como função gerenciar os protocolos de transmissão da tag e do leitor, e dentro dele encontram-se os componentes lógicos. Caso seja coletada uma informação importante pelo leitor, o controlador é quem tem a função de analisar e enviar essa mensagem para a interface de rede (SANTINI, 2006).

A interface de rede serve para interligar o leitor com outros dispositivos. “É através da interface de rede que os leitores externalizam as informações, por uma interface serial, rede ou até mesmo via wireless, dispositivos recebem as informações do leitor para serem tratadas.” (HECKEL, 2007, p. 54). A Figura 2.20 mostra os diferentes componentes físicos de um leitor.

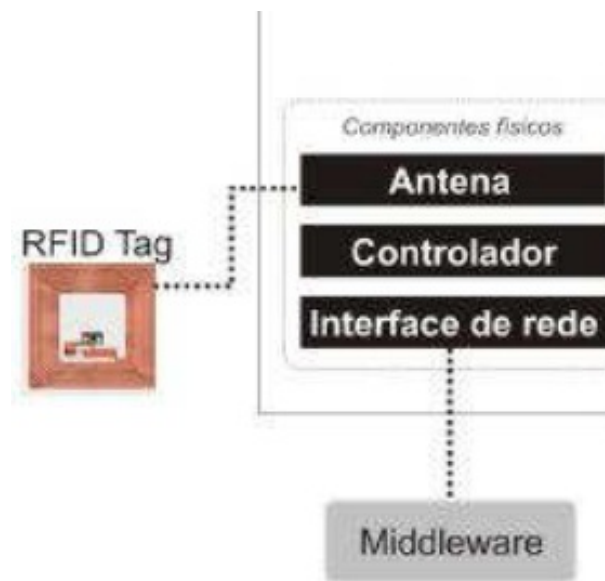


Figura 2.20: Componentes físicos de um leitor.  
FONTE: (SANTINI, 2006)

### 2.3.3.1.2 Parte Lógica

Os principais componentes lógicos de um leitor RFId são: *Application Programming Interface* (API) do leitor, subsistema de comunicações, subsistema de gerenciamento de eventos e subsistema da antena.

A API permite que outras aplicações solicitem informações das tags, monitorem a situação do leitor ou controlem as configurações, como níveis de energia e o tempo corrente. Ela é responsável por realizar a transição de informações entre o *middleware* e o leitor.

“O subsistema de comunicação lida com os detalhes da comunicação sobre qualquer protocolo de transporte que o leitor possa usar para se comunicar com o *middleware*. Este é o componente que implementa Bluetooth, Ethernet ou um protocolo proprietário para enviar e receber as mensagens que constituem a API.” (GREFF, 2009, p. 32-33).

O gerenciador de eventos é quem identifica se uma tag na zona de interrogação de um leitor já foi **observada** ou se é considerada um novo **evento**, que é separado dos demais pela **filtragem de eventos**. É este componente que avalia a importância de determinado **evento**, e se é relevante para ser colocado em um relatório ou transmitido imediatamente pela interface de rede.

O subsistema da antena consiste da interface e da lógica que permite aos leitores RFId interrogar as tags e controlar as antenas físicas (GLOVER; BHATT, 2007).

### 2.3.4 Módulo de *Middleware*

O módulo de *middleware*, também chamado de aplicação ou *software* final, é o dispositivo de interface que controla todo o sistema periférico de RFId (leitor e tags) além da comunicação com os outros componentes do sistema. Ele é desenvolvido para a integração entre aplicações de RFId e muitas vezes passa despercebido por rodar em *background* no sistema. O *middleware* é o responsável por filtrar o grande número de dados coletados pelos leitores, pela depuração das informações recebidas pelas antenas e por converter essas informações em algo que o sistema do usuário possa interpretar.

Para (GLOVER; BHATT, 2007), há três motivos para se utilizar *middleware* RFId: encapsular as aplicações das interfaces de dispositivos; processar as informações brutas capturadas pelos leitores de modo que as aplicações só vejam eventos significativos; e para obter uma interface em nível de aplicação para gerenciar leitores e consultar observações do sistema de RFId.

O desenvolvimento do *middleware* varia de acordo com o *hardware* de cada fabricante e exige um alto grau de conhecimento técnico, pois a maioria dos leitores simplesmente capta todos os dados que estão na sua área de interrogação e cabe ao *middleware* organizar esses dados e os transformar em informações.

## 2.4 Padrões

A necessidade de interoperabilidade de sistemas RFId fez com que fossem adotados padrões para se trabalhar com identificadores de radiofrequência. Os principais identificadores existentes seguem os padrões *Electronic Product Code* (EPC) ou *International Organization for Standardization* (ISO), e cada um deles trabalha com diferentes leitores. Por este motivo, é importante conhecer esses diferentes padrões e analisar a escolha do leitor ideal dependendo de cada aplicação.

“A finalidade da padronização e de normas é definir as plataformas em que uma indústria possa operar de forma eficiente e segura. Os maiores fabricantes de RFId oferecem sistemas proprietários, o que resulta numa diversidade de protocolos de sistemas de RFId numa mesma planta industrial” (MARTINS, 2005, p. 4). Como organizações mais conhecidas, envolvidas na luta de padronização de protocolos RFId, podem-se destacar as internacionais EPC Global e ISO; e a nacional Brasil-ID.

### 2.4.1 EPC Global

Segundo (SANTANA, 2005, p. 2):

“(...) na década de 80 quando o MIT, juntamente com outros centros de pesquisa, iniciou o estudo de uma arquitetura que utilizasse os recursos das tecnologias baseadas em radiofrequência para servir como modelo de referência ao desenvolvimento de novas aplicações de rastreamento e localização de produtos. Desse estudo, nasceu o Código Eletrônico de Produtos - EPC (*Electronic Product Code*). O EPC definiu uma arquitetura de identificação de produtos que utilizava os recursos proporcionados pelos sinais de radiofrequência, chamada posteriormente de RFId (*Radio Frequency Identification*).”.

Em 2005, a EAN, a UCC e a *Global System 1* (GS1) formaram a EPC Global, que segundo (GLOVER; BHATT, 2007, p. 64), “define um método combinado de classificação de identificadores que especifica frequências, métodos de acoplamento, tipos de chaveamento e modulação, capacidade de armazenamento de informações e modos de interoperabilidade de sistemas RFId”.

A EPC Global definiu uma arquitetura de identificação de produtos que utilizavam os sinais de radiofrequência, que vieram a ser chamados de RFId. (HECKEL, 2007, p. 59) afirma que: “Um EPC estabelece um número único para determinado produto, similar a um *MAC Address* de uma placa de rede”.

A estrutura do formato básico de um número EPC pode ser analisada na Figura 2.21.

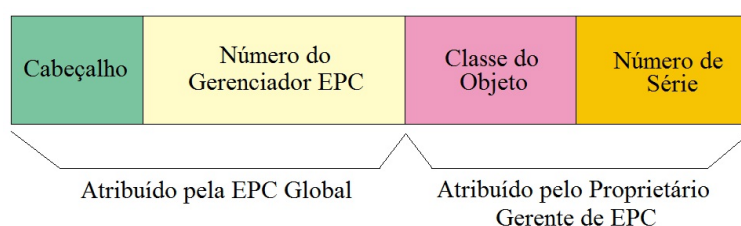


Figura 2.21: Estrutura de um número EPC.  
FONTE: (SANTINI, 2006)

O campo **cabeçalho** indica o comprimento, tipo, estrutura, versão e geração do EPC; o campo **número do gerenciador EPC** é a entidade responsável por manter as partições subsequentes; a **classe do objeto** identifica a classe do objeto ao qual a tag está anexada; e o **número de série** identifica a instância. As diferentes classes definidas pela EPC Global estão listadas na Tabela 2.1.

Tabela 2.1: Classe de tags reconhecidas pela EPC Global

Classe	Descrição
0	Passivas, apenas de leitura
0+	Passiva, grava uma vez, mas usando protocolos da classe 0
I	Passiva, grava uma vez
II	Passiva, grava uma vez com extras, como criptografia
III	Regravável, semi-passiva (chip com bateria, comunicações com energia do leitor), sensores integrados
IV	Regravável, ativa, identificadores podem conversar com outros identificadores, energizando suas próprias comunicações
V	Podem energizar e ler identificadores das Classes I, II e III e ler identificadores das Classes IV e V, assim como atuar como identificadores da classe IV

FONTE: (HECKEL, 2007)

O esquema de armazenamento de dados em uma tag pode ser observado na Figura 2.22.



Figura 2.22: Armazenamento de dados em uma tag.

FONTE: (GLOVER; BHATT, 2007)

O campo **Cyclic Redundancy Check (CRC)** é uma forma de detectar erros de armazenamento ou transmissão. Ele é enviado com a mensagem original e verificado no receptor com o objetivo de comprovar que não houve alterações. O campo **EPC** é o código da tag e o **password** (senha) é o campo responsável por desabilitar a tag, destruindo-a permanentemente.

### 2.4.2 ISO

Como os primeiros sistemas de RFID eram utilizados somente para controle interno, não havia preocupações em relação à uma padronização para a tecnologia. Segundo (MOROZ, 2004), o primeiro setor a solicitar uma padronização foi o da pecuária, para a aplicação de identificação de animais.

(GLOVER; BHATT, 2007) explicam que em fevereiro de 2005, a especificação EPC foi submetida a ISO, esperando-se que com isso se resolvam alguns conflitos entre as duas abordagens.



### 2.4.3 Brasil-ID

Sobre a padronização no Brasil, (KAMINSKY, 2009) explica que em 2009, o Ministério da Ciência e Tecnologia (MCT), o Ministério da Fazenda e as Secretarias de Fazenda de todos os estados brasileiros assinaram um acordo de cooperação para a criação do Brasil-ID (BRASIL-ID, 2011): Sistema de Identificação, Rastreamento e Autenticação de Mercadorias.

O sistema é baseado na tecnologia de RFId e de comunicação sem-fio. O projeto visa estabelecer um padrão único de Identificação por Radiofrequência a ser utilizado em qualquer tipo de produto em circulação pelo país; e a estruturação de serviços de rastreamento e verificação de autenticidade de todo tipo de mercadoria que poderá ser desenvolvido pelos setores público e privado em atendimento às necessidades do mercado.

O objetivo do Brasil-ID é promover a segurança do comércio e circulação de mercadorias no país através de tecnologia confiável e padronizada. Portanto, além de uma fiscalização de trânsito de mercadorias muito mais ágil, o contribuinte poderá utilizar a tecnologia para seu próprio benefício logístico, de garantia de autenticidade e de proteção contra a circulação de bens roubados.

## 2.5 Aplicações RFId

O desenvolvimento de novos produtos de RFId, a regulamentação e a redução de custos têm provocado o surgimento de novas aplicações nas mais diversas áreas, como na pecuária, segurança, medicina, etc. A seguir são citados alguns exemplos.

### 2.5.1 Identificação de Animais

Uma das primeiras aplicações comerciais de RFId foi na área de identificação de animais, utilizando tags passivas. Este tipo de sistema utilizado na identificação de animais ajuda no gerenciamento dos mesmos entre as companhias, no controle de epidemias e garantia de qualidade e procedência.

A identificação animal por sistemas de RFId pode ser feita de quatro maneiras diferentes: colares, brincos, injetáveis ou ingeríveis (*bolus*). Os colares são fáceis de serem aplicados e podem ser reutilizados em outros animais. Os brincos são as tags mais baratas, e podem ser lidas a uma distância de até um metro. As tags injetáveis são colocadas sob a pele do animal com uma ferramenta especial, como se fosse uma injeção. A tag ingerível, também chamada de

*bolus*, é um grande comprimido de forma cilíndrica, revestido por material cerâmico resistente a ácido, e pode ficar no estômago do animal por toda sua vida.

O rastreamento de animais está cada vez mais exigido para a entrada de carne em mercados que prezam pela rastreabilidade de alimentos, e a tecnologia de RFID atende perfeitamente a estas exigências, pois permite rastrear o animal desde o seu nascimento até o abate.

### 2.5.2 Sistema Antirroubo de Carros

Nos anos 90, o roubo de carros apresentou um grande crescimento, fazendo com que os mercados de segurança para carros, alarmes e sistemas de imobilização se tornassem muito promissores. Os controles de alarme comuns são pequenos transmissores de rádio frequência que operam na frequência de 433.92 MHz. Neste tipo de sistema de segurança para carros, é somente este controle que pode destravar o carro, fazendo com que ele seja aberto sem que o alarme seja acionado. Porém, se o controle que destrava o carro for quebrado, este ainda pode ser aberto através das chaves, por um processo mecânico, mas não há como o sistema reconhecer se a chave inserida é genuína, permitindo que uma ferramenta específica ou uma chave-mestra possa abrir o veículo.

A tecnologia das tags de RFID age justamente neste ponto: no sistema antirroubo de ignição dos carros. Neste sistema, um leitor é colocado na barra de direção do veículo e uma tag é colocada em sua chave, “assim, se o número de identificação que o leitor está programado para reconhecer não for o mesmo da chave do carro que deve estar na ignição o automóvel não liga” (HECKEL, 2007, p. 57).

### 2.5.3 Smart Cards

De acordo com (HECKEL, 2007, p. 68), “Os primeiros smart cards ou cartões inteligentes foram desenvolvidos na França na década de 70, mas sua utilização se tornou viável e em maior escala apenas a partir da década de 90. Estes cartões são de plástico e possuem uma memória ROM, alguns, inclusive, possuem microprocessadores”.

Os *smart cards* possuem muitas vantagens em relação aos cartões de tarja magnética convencionais. As mais importantes são a sua maior capacidade de armazenamento e a maior variedade de mecanismos de segurança disponíveis (criptografia), conforme exigências específicas de cada aplicação. (OLIVEIRA; PEREIRA, 2006).

Os cartões inteligentes podem ser classificados quanto a presença de memória e micropro-

cessador e se são cartões de contato. Os *smart cards* sem contato não necessitam de uma visada direta com a antena, pois possuem um transmissor de radiofrequência. Estes cartões são usados principalmente para controle de acesso em *shoppings*, condomínios residenciais, comerciais e empresariais entre outras áreas restritas; e para controle de pagamentos.

### 2.5.4 Implantes em Humanos

Implantes de tags *chips* RFId podem ser utilizados em humanos como um método de identificação de fraudes, aumento de segurança, controle de acesso, banco de dados de medicamentos, iniciativas antissequestro, entre outros. Combinado com sensores para monitorar as funções do corpo, o dispositivo pode monitorar pacientes em hospitais. Conforme (CARDOSO, 2000, p. 8), “tal sistema pode dar suporte à gerência hospitalar, permitindo a analisar, tanto a funcionalidade de setores, quanto o fluxo e o acesso de pessoal, podendo contribuir assim, no estudo e controle da infecção hospitalar.” Esta é uma área polêmica já que implantes de tags RFId constituem uma ameaça à segurança e a privacidade das pessoas.

Implantes de tags RFId são utilizados por casas noturnas da Europa, implantando as tags em alguns de seus frequentadores para identificar os *Very Important Persons* (VIPs); por empresas do México, colocando em seus funcionários para controlar o acesso a lugares restritos; e por hospitais dos Estados Unidos para monitorar seus pacientes.

### 2.5.5 Bibliotecas

As tags RFId podem ser utilizadas para identificação de acervo em bibliotecas e centros de informação, possibilitando a leitura e o rastreamento dos exemplares físicos das obras. Algumas aplicações desta tag são: autoatendimento, devolução, empréstimo, estatística de consulta local, leitura de estante para inventário do acervo, localização de exemplares indevidamente ordenados no acervo, localização de exemplares em outras bibliotecas da rede e re-catalogação.

Neste sistema, uma tag RFId adesiva de dimensões reduzidas é fixada na contracapa dos livros, dentro de revistas e sobre materiais multimídia para ser lida à distância. Esta tag contém no centro um *microchip* e ao redor deste uma antena metálica em espiral. Um conjunto com sensores especiais e dispositivos possibilitam a codificação e leitura dos dados da tag referentes aos livros, principalmente o código identificador, que antes era registrado em códigos de barras (NOGUEIRA, 2003).

### 2.5.6 Supermercados

Algumas das redes de supermercados mais famosas no mundo, como por exemplo a norte-americana *Wall Mart*, tem inovado tecnologicamente investindo na tecnologia de RFId.

Neste tipo de aplicação, cada carrinho do supermercado tem um minicomputador com um sensor que, através das tags, capta e registra o preço dos produtos que são colocados no carrinho. Ao passar no caixa, o cliente não precisa registrar novamente os produtos, basta registrar o que está computado na tela do carrinho.

Essa tecnologia facilita muito a vida dos clientes e o trabalho no supermercado. Algumas lojas do Wall Mart nos EUA, do MetroGoup da Alemanha, e até da rede brasileira Pão de Açúcar já possuem um certo número de produtos com a tag RFId, funcionando como teste para futuras implementações (MANSUR, 2010).

## 2.6 Vantagens e Desvantagens da Tecnologia de RFId

Como qualquer tecnologia emergente, deve-se analisar com cuidado e saber dos riscos e benefícios que a tecnologia de RFId pode trazer. Dentre algumas das vantagens e benefícios, podem-se citar as seguintes:

- Permite realizar a leitura de tags remotamente;
- Os dados das tags são coletados de forma mais rápida;
- O tempo de vida (durabilidade) das tags passivas é muito grande;
- As tags passivas, teoricamente, não tem nenhuma necessidade de manutenção;
- As tags podem ser reutilizadas;
- As tags ativas têm capacidade de armazenamento, leitura e escrita;
- As tags de RFId podem ser utilizadas em locais sujeitos à alterações climáticas e outras diversidades;
- A tecnologia de RFId pode ser utilizada na prevenção de roubos e falsificação de mercadorias;
- A utilização da tecnologia de RFId permite a contagem instantânea de estoque, facilitando os sistemas empresariais de controle de inventário e

- A utilização da tecnologia de RFID pode contribuir na melhoria do reabastecimento com eliminação de itens faltantes ou com validade vencida;

Como desvantagens e riscos do sistema de RFID, podem-se apresentar, entre outros, os seguintes itens:

- O custo elevado da tecnologia de RFID em relação aos sistemas de código de barras;
- O preço final dos produtos, pois a tecnologia não se limita à tag anexada ao produto. Por trás da estrutura estão antenas, leitores, ferramentas de filtragem das informações e sistemas de comunicação;
- O uso em materiais metálicos e condutivos relativos ao alcance de transmissão das antenas. Como a operação é baseada em campos magnéticos, o metal pode interferir negativamente no desempenho;
- Problemas de padronização, principalmente das faixas de frequência, para que os produtos possam ser lidos por toda a indústria de maneira uniforme e
- Possíveis problemas quanto a segurança e, principalmente, a invasão da privacidade dos consumidores. Por causa da monitoração das tags coladas nos produtos.

## **2.7 Segurança e Privacidade**

Como a área de RFID é considerada nova e em ascensão, ela provoca muita discussão em relação a segurança das informações e privacidade dos usuários. As modernas tags RFID podem trazer grandes problemas aos seus usuários, pois elas não contêm nenhuma rotina ou dispositivo para proteger seus dados. Mesmo as tags passivas, que tem raio de ação de poucos metros, podem sofrer interceptação e extravio de suas informações. Pensando em tags ativas, o problema pode se tornar ainda mais crítico.

### **2.7.1 Segurança**

Assim como qualquer dispositivo de comunicação sem fio, a tecnologia de RFID está sujeita à falhas de segurança, já que as informações trafegam pelo ar. Portanto, a implantação desta tecnologia sem um tratamento cuidadoso de segurança pode acarretar em graves problemas aos seus usuários. Medidas preventivas devem ser tomadas a fim de evitar ataques inesperados. Para (PINHEIRO, 2005), os principais problemas quanto a segurança em RFID são em relação a violação da integridade, cópia e monitoramento das tags.

A seguir serão citados alguns exemplos de problemas que possivelmente trarão complicações as pessoas, caso a tecnologia de RFID seja implantada em larga escala e sem ter o devido cuidado com segurança. Também serão descritos exemplos de ocorrência destes problemas e possíveis soluções para eles (GLOVER; BHATT, 2007).

**Problema:** Violação da Integridade Física. Uma tag possui dados específicos do material ao qual está localizada. Se esta for colocada em outro material, pode causar danos ao seu usuário.

**Exemplo:** Se um ladrão trocar a tag de um produto caro pela de um produto barato, poderá lesar o estabelecimento, causando prejuízos a ele.

**Possível Contramedida:** Monitorar as pessoas que estejam próximas às tags; ou anexá-las em lugares estratégicos; ou em invólucros resistentes e difíceis de serem removidos. Assim, poderiam ser evitadas possíveis fraudes, pois a tag ficaria livre de interceptações quando não estivesse em uso.

**Problema:** Cópia (Clonagem) de Tags. Uma pessoa que possua o conhecimento de criação de tags, copia, de maneira mal intencionada, dados das tags usando um leitor, e utilizada estes dados para criar uma idêntica.

**Exemplo:** Alguns carros fabricados atualmente possuem um dispositivo RFID que faz com que não seja necessário o transporte da chave. Se um ladrão conseguir copiar os dados da tag deste dispositivo, poderá facilmente roubar o carro.

**Possível Contramedida:** Criptografar as tags, fazendo com que somente emissor e receptor (leitor e tag) tenham acesso a informação nela contida. Qualquer pessoa que queira obter esses dados ilicitamente terá que decifrar o código.

**Problema:** Monitoramento de Tag. Invasão da rede sem fio em que o leitor esteja situado (já que a comunicação entre tag e leitor dificilmente pode ser criptografada), para obtenção de dados das tags para uso indevido.

**Exemplo:** Um *hacker*, beneficiando-se desta falha de segurança, intercepta a comunicação e obtém acesso à troca de informações entre transmissor e receptor.

**Possível Contramedida:** Leitor requerer autenticação apropriada.

**Problema:** Vazamento de Informações Pessoais. Acesso não autorizado aos programas que fazem o processamento das informações dos leitores.

**Exemplo:** Um *hacker* pode obter os dados bancários de uma pessoa através do banco de dados e, sabendo que ela possui grande quantia em dinheiro, obrigá-la a sacá-lo no caixa eletrônico.

**Possível Contramedida:** *Firewalls*, IDs e outras ferramentas para prevenir ataques na rede interna e externa (caso os computadores tenham acesso a Internet).

## 2.7.2 Privacidade

Existem muitas preocupações em relação a invasão da privacidade das pessoas com o desenvolvimento da tecnologia de RFID. Alguns problemas já existem e muitos outros podem surgir com o crescimento da computação pervasiva e da interoperabilidade entre diferentes dispositivos, entretanto, muitas preocupações são apenas mitos sem fundamento. Um destes mitos é o de que as pessoas que portam tags RFID passivas, provenientes de algum produto comprado em uma loja, podem ser rastreadas de alguma forma. Este rastreamento é impossível, pois o alcance do leitor, no caso das tags RFID passivas usadas nos produtos, é de no máximo alguns metros.

Contudo, de acordo com (HECKEL, 2007, p. 64):

“(...) caso uma pessoa compre determinada peça de roupa com uma tag anexada e passe por uma zona de leitura de alguém que possua um leitor, pode-se saber até mesmo o preço da roupa adquirida por ela. Por isso é que se estuda internacionalmente uma forma de legislação para regulamentar sistemas RFID. Uma possível solução é que após a compra a pessoa peça para um funcionário da loja desativar a tag de sua peça de roupa (...).

As tags ativas, que possuem um alcance maior, dificilmente podem vir a se tornar um grande problema, já que, por enquanto, são muito maiores que as tags passivas, além de serem mais caras, sendo inviável de se utilizá-las em objetos comuns. A prática de colocar tags diretamente em objetos também não é usual, normalmente são as embalagens que deverão conter as etiquetas, minimizando assim o problema da invasão de privacidade.”.

Para (GLOVER; BHATT, 2007), todos os identificadores EPC devem suportar a destruição remota e permanente de um identificador individual usando uma senha.

Conforme (GLOVER; BHATT, 2007), Simson Garfinkel apresentou um artigo abordando que uma possível solução para estes problemas seria propor uma **Declaração de Direitos RFID**,

que deveria possuir as seguintes cláusulas:

- O direito de o consumidor saber quais itens possuem identificadores RFId;
- O direito de remover ou desativar o identificador RFId assim que um produto seja comprado;
- O direito a produtos e serviços, mesmo se um consumidor escolher não usar identificadores RFId;
- O direito de saber onde, quando e por que um identificador RFId está sendo lido;
- O direito de saber quais informações estão sendo armazenadas em um identificador RFId.

## **2.8 RFId Versus Código de Barras**

O conceito *Automatic Identification and Data Capture* (AIDC) engloba um conjunto de métodos para identificar objetos, recolher informações sobre eles e fornecer essa informação a sistemas de tratamento de dados de forma automática. Este conceito engloba, entre outras, as tecnologias de código de barras e de RFId.

As tecnologias de código de barras e de RFId são análogas. A primeira utiliza leitores ópticos que transformam as informações contidas em uma etiqueta, com um código de barras impresso, em sequências de sinais elétricos correspondentes e proporcionais aos dados nela contidos. Enquanto a segunda utiliza um leitor de radiofrequência que alimenta as chamadas etiquetas inteligentes, fazendo com que elas respondam com o seu número de identificação.

O sistema de RFId, apesar de não ser uma unanimidade devido a falta de padronização e as supostas ameaças de invasão de privacidade, aspira a substituir a tecnologia de código de barras, pois é mais completo e acrescenta novas funcionalidades e facilidades, como as apresentadas na Tabela 2.2.



Tabela 2.2: Comparativo entre uma etiqueta de código de barras em uma tag RFId passiva

	<b>Etiqueta de Código de Barras</b>	<b>Tag RFId passiva</b>
Capacidade de Informação	Pequena	Grande
Custo da Etiqueta	Insignificante	Significante
Custo de Manutenção	Alto	Baixo
Custo dos Equipamentos	Baixo	Alto
Dados Modificáveis	Não	Sim
Distância de Leitura	Muito Pequena	Grande
Durabilidade	Pequena	Indefinida
Formatos	Etiquetas	Variados
Contato Visual com o Leitor	Necessita	Não Necessita
Padronização	Definida	Em definição
Resistência Mecânica	Baixa	Alta
Reutilização	Não	Sim

De acordo com (NISHIDA, 2008), o código de barras é uma boa solução para coletar informações em processos bem estruturados e projetados, onde se tem acesso direto ao produto. Já as tags RFId são mais eficientes na coleta de informações de recursos móveis (sem visada direta) e de processos de negócios não estruturados, oferecendo para estes ambientes um controle mais sistemático e eficiente.

Para (MARTINS, 2005, p. 2):

“(...) a tecnologia RFId não é um substituto do código de barras, pelo menos por enquanto. O custo da impressão de um código de barras é insignificante no custo da embalagem se comparado ao custo de um tag de RFId, por mais simples que este seja. A grande vantagem do RFId é a sua capacidade de obter maior número de informações, identificando vários itens ao mesmo tempo, não exigindo leitura-em-linha, o que representaria, no caso de uma aplicação num supermercado, uma redução de custos operacionais na hora do *check-out* das compras.”.

Na verdade, ao invés de substituir o código de barras, a tendência é que ambas as tecnologias deverão coexistir, aplicando-se uma ou outra conforme conveniência da aplicação. (RFID-GET-STARTED, 2011).

## 2.9 Futuro do RFId

A maior preocupação sobre o futuro da tecnologia de RFId é em relação a falta de segurança, a invasão de privacidade e as pragas digitais. Atualmente, a tecnologia de RFId está sendo am-

plamente utilizada por grandes indústrias, empresas multinacionais e até órgãos do governo. Por isso, é necessário tomar precauções em relação à segurança das informações que estão sendo confiadas a este sistema, para que a adoção da tecnologia seja feita de forma consistente e que não traga incertezas e mitos sobre a sua eficiência.

A tecnologia de RFId também poderá ter grande influência no desenvolvimento da computação ubíqua e pervasiva. A computação pervasiva poderá utilizar a tecnologia de RFId para rastrear e monitorar objetos ou pessoas em um ambiente inteligente. As mais diversas aplicações podem ser desenvolvidas para aumentar a interação entre o usuário e o sistema computacional a sua volta. Através das tags RFId, todo o ambiente pervasivo fica ciente da localização do usuário, possibilitando prever suas ações através da análise do seu histórico de movimentações (BOLZANI, 2004).

Outro problema é em relação ao custo da tecnologia. Atualmente, muitas aplicações RFId não são implementadas devido ao alto custo, não apenas das tags, mas de todo o sistema. Porém, com o crescimento deste mercado, espera-se que ocorra o barateamento da tecnologia, e que em um futuro próximo o investimento financeiro inicial deixe de ser um problema tão grande nesta área.

No próximo capítulo será abordado o desenvolvimento de um aplicativo de controle de fluxo de pessoas que demonstra a viabilidade de um sistema de RFId; e um experimento gerenciando o registro de fluxo de pessoas em um laboratório do IFSC, que exemplica como esta tecnologia pode ser inserida, de forma simples, nas instituições.

### 3 *Aplicativo de Controle de Fluxo de Pessoas*

Este trabalho tem como objetivo demonstrar como a tecnologia de RFId pode ser facilmente inserida no cotidiano do ser humano. Para melhor ilustrar este potencial tecnológico, um aplicativo com base na tecnologia de RFId, o de controle de fluxo de pessoas foi escolhido para ser desenvolvido.

Dentro da estrutura do sistema de RFId, este aplicativo se refere ao componente módulo de *middleware* e sua função é depurar e filtrar os dados coletados pelos leitores e os transformar em informações que o sistema do usuário possa compreender. Após fazer esta comunicação entre os componentes do sistema, o aplicativo trata e realiza o processamento das informações recebidas; e cadastra os dados relevantes em um banco de dados para posterior consulta ou geração de relatórios.

Com estes procedimentos, o aplicativo possibilita registrar os horários de entrada e saída dos usuários do sistema, controlando o fluxo de pessoas e podendo funcionar também como um ponto eletrônico.

#### 3.1 Ambiente

O aplicativo de controle de fluxo de pessoas foi desenvolvido para controlar o acesso a áreas restritas de instituições, podendo funcionar também como um ponto eletrônico. Para ambos os casos, o ambiente deverá ser constituído da seguinte forma:

Cada usuário possuirá uma tag RFId, que será a sua forma de identificação com o sistema. Esta tag poderá ser de qualquer formato, o importante é que o usuário esteja sempre de posse da mesma. No caso do aplicativo ser utilizado para ponto eletrônico em empresas, o recomendado seria a utilização das tags no formato de crachá.

Em todos os locais aonde a instituição deseje controlar o acesso, deverá ser colocado um

leitor RFId, ou outro equipamento capaz de alimentar as tags, receber os dados enviados por elas e disponibilizá-los ao *middleware*. Este equipamento deverá ser colocado em um lugar estratégico, preferencialmente na(s) via(s) de acesso deste local, para que ele possa reconhecer a tag assim que o usuário entre ou saia.

Sempre que a tag portada pelo usuário entrar na área de cobertura do leitor, ela será alimentada e irá transmitir seu número único de identificação (ID). O leitor irá receber este ID e irá disponibilizá-lo ao *middleware*, que definirá a funcionalidade deste sistema de RFId.

## 3.2 Especificação

Para desenvolver e testar o aplicativo, foram utilizados:

### 3.2.1 Hardware

Os equipamentos citados a seguir podem ser visualizados na Figura 3.1.

#### 1 Microcomputador:

Processador: Intel Celeron D CPU 3.06GHz

Conexão com o Leitor: Porta serial RS-232.

Memória: 1Gb.

#### 1 Leitor RFId:

Marca: Akiyama

Modelo: DE210-R2/C

Antena: Antena integrada

Frequência: 125 kHz

Dimensões: 240 x 240 x 50 mm

Distância Máxima de Leitura: 1000 mm

Tempo de Resposta e Decodificação: Abaixo de 100 ms

Alimentação: +12 v linear DC e 200 mA típico, 300 mA máx.

Interface: RS232

**Cartões de Proximidade RFId:**

Marca: Akiyama

Modelo: TP Clamshell Personalité

Antena: Enrolamento de cobre

Frequência de Operação: 125 kHz

Dimensões: 85,60 x 53,98 x 1,90 mm

Alcance de Leitura: 70 mm

Material: ABS (Acrilonitrila Butadieno Estireno)

Códigos pré-gravados: Decimal, ASC II e Wiegand

**Classificação da Tag:**

Alimentação: Tag passiva (alimentada pelo leitor)

Tipo de Encapsulamento: Cartão

Frequência: LF

Acoplamento: Indutivo

Capacidade de Armazenamento: SAW



Figura 3.1: *Hardware utilizado*

### 3.2.2 Software

Para desenvolver e testar o aplicativo, foram utilizados:

Sistema Operacional: Ubuntu Linux 10.04

Plataforma de Desenvolvimento: Netbeans 6.9 com JDK 6

Comunicação Serial: API Java Communications

Banco de Dados: MySQL Community Server 5.5 com Conector/J

Geração de Relatórios: JasperReports 4.0.2 com plugin iReport 3

O Anexo ‘Controle de Fluxo de Pessoas Usando RFId - Tutoriais de Instalação’ é um documento referente à informações e a instalação destes *softwares*.

## 3.3 Aplicativo

Foram desenvolvidos dois *softwares* utilizando a linguagem de programação Java: O *Software* de Monitoramento e o *Software* de Gerenciamento. Estes *softwares* fazem o registro e a manipulação de informações através de conexões com tabelas de um banco de dados. A seguir, serão descritos os modos de funcionamento e funções destes *softwares* e tabelas.

### 3.3.1 Software de Monitoramento

Este é o *software* de monitoramento do sistema de RFId. A primeira ação relevante que este *software* irá realizar é a abertura da porta serial. Após esta ação, o *software* irá aguardar que o leitor disponibilize um ID na porta de comunicação, ou seja, que uma tag RFId entre na área de cobertura do leitor e transmita seu número de identificação. Assim que este evento ocorrer, o *software* irá tratar o ID. Este tratamento é realizado para retirar os dados de controle inseridos pelo leitor na *String* do ID. É como se fosse uma ‘limpeza’ desta *String*.

Na segunda tomada de decisão do *software*, ele irá consultar o banco de dados para identificar se já existe algum usuário cadastrado com o ID que foi disponibilizado pelo leitor. Em caso negativo, o *software* irá ignorar este ID, pois ele não pertence ao sistema, e irá aguardar que o leitor disponibilize um novo ID.

Caso a busca ao banco de dados retorne uma indicação positiva em relação ao cadastro, o *software* irá para a próxima tomada de decisão. Esta também envolve uma consulta ao banco de dados, desta vez para descobrir quanto tempo se passou desde o último registro do ID. Caso este

tempo seja menor que dez segundos, ele não será registrado, e o *software* irá voltar ao ponto de espera por um novo ID.

Não deve ser permitido mais de um registro de um mesmo ID em um curto intervalo de tempo. Isto se deve a possibilidade de, por um pequeno descuido do usuário, o leitor ler duas vezes a sua tag, registrando sua entrada e em seguida sua saída em uma mesma passagem. Neste exemplo, este intervalo de tempo foi configurado para dez segundos, mas pode ser configurado com um tempo diferente.

Se o ID não houver sido registrado nos últimos dez segundos, o *software* irá registrar este horário de passagem da tag pelo leitor. Após realizar o registro, ele irá cadastrar este evento (entrada ou saída) no banco de dados, assim como outros dados que serão processados pelo *software* (como tempo de permanência no local), de acordo com o evento.

Após o evento ser cadastrado no banco de dados, o *software* irá exibir uma mensagem na tela, relativa ao último evento ocorrido. Esta mensagem faz a interface com o usuário, e sua utilidade será explicada posteriormente. Após a exibição desta mensagem, o *software* voltará a aguardar que o leitor disponibilize um ID na porta de comunicação, para realizar todo o processo novamente e indefinidamente.

É importante destacar que os registros do aplicativo são armazenados em um mesmo banco de dados. Por exemplo: caso o usuário entre passando por um leitor de acesso e, posteriormente, passe por outro, sua saída não será registrada. Entretanto seria, se este acesso fosse registrado no aplicativo e os leitores RFID fossem controlados por computadores distintos ou fossem registrados em bancos de dados diferentes.

O fluxograma do *software* de monitoramento pode ser visualizado na Figura 3.2:

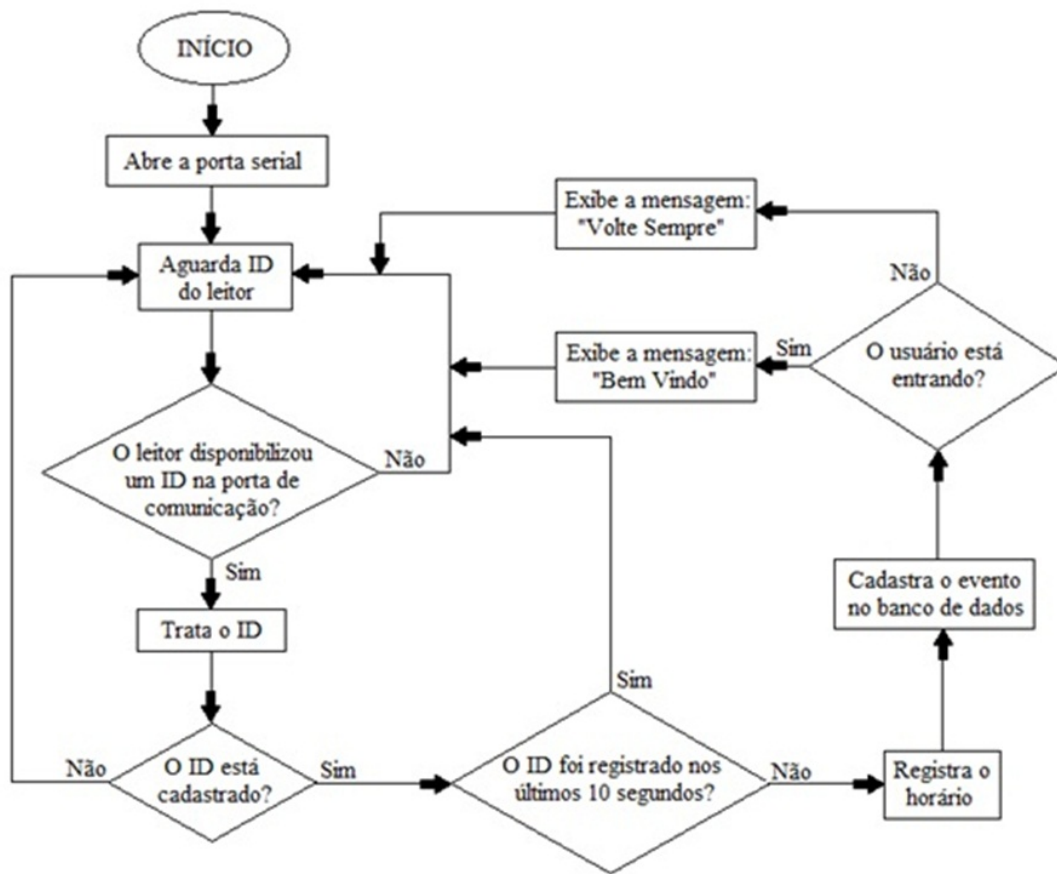


Figura 3.2: Fluxograma do *software* de monitoramento

### 3.3.1.1 Funções do *Software* de Monitoramento

A seguir, serão apresentadas as funções deste *software*:

**Comunicação Serial:** Abre e configura a comunicação com a porta serial

**Tratamento de Dados:** Analisa e faz as modificações necessárias nos dados enviados pelo leitor.

**Registro de Horários:** Registra o horário de entrada e saída do usuário.

**Cálculo de Horários:** Calcula o tempo de permanência do usuário no local.

**Interface com o Usuário:** Exibe mensagens de 'Boas-Vindas'.

**Conexão com o Banco de Dados:** Faz a conexão da aplicação com o banco de dados.

**Comunicação com o Banco de Dados:** Insere e consulta informações no banco de dados.



### 3.3.2 Software de Gerenciamento

Este é o *software* de gerenciamento do sistema de RFId. Para entender o seu funcionamento, primeiro deve ser compreendido o sistema de banco de dados que foi criado:

#### 3.3.2.1 Banco de Dados

O banco de dados armazena em tabelas todas as informações que são enviadas pelo aplicativo de controle de fluxo. Isto faz com que os dados fiquem armazenados de maneira estruturada e possam ser consultados pelo aplicativo através da linguagem *Structured Query Language* (SQL). A seguir, serão descritas as funções e o modo básico de funcionamento destas tabelas:

##### 3.3.2.1.1 Tabelas do Banco de Dados

As tabelas do banco de dados registram as informações dos usuários do sistema, como eventos (entrada, saída, cadastro) e horários em que ocorreram. Estes registros pode ser feitos em formatos que sejam facilmente assimiladas pelo ser humano, como um tempo no formato HH:MM:SS para ser colocado em um relatório, ou em formatos que sejam melhor adequados para o processamento de dados, como um tempo em milissegundos para cálculos. As quatro tabelas utilizadas pelo aplicativo são:

**Tabela Acesso:** Possui o registro dos usuários cadastrados que podem ter acesso ao *software* de gerenciamento e suas senhas.

**Tabela FuncionárioX:** é a tabela individual de cada usuário. O X é um número que é incrementado a cada nova tabela criada, ou seja, o nome da tabela do primeiro usuário cadastrado será Funcionário1, a do segundo usuário será Funcionário2, a do terceiro Funcionário3 e assim por diante. Nesta tabela estão registradas informações como: nome, eventos, datas, horários, tempos de permanência parciais e totais para a geração de relatórios individuais; e outras informações específicas para a realização de cálculos de horários e outros tipos de processamentos de dados.

**Tabela Listagem de Funcionários:** esta tabela armazena apenas os nomes dos usuários e seus respectivos IDs, linha após linha. Desta forma, eles podem ser listados adequadamente na Tela de Cadastro.

**Tabela Geral:** é a tabela comum a todos os usuários. Ela possui as informações de todos

os nomes, eventos, datas, horários, tempos de permanência parciais e totais para a geração de relatórios gerais.

Na Figura 3.3 podem ser visualizadas as conexões do *software* com as tabelas do banco de dados.

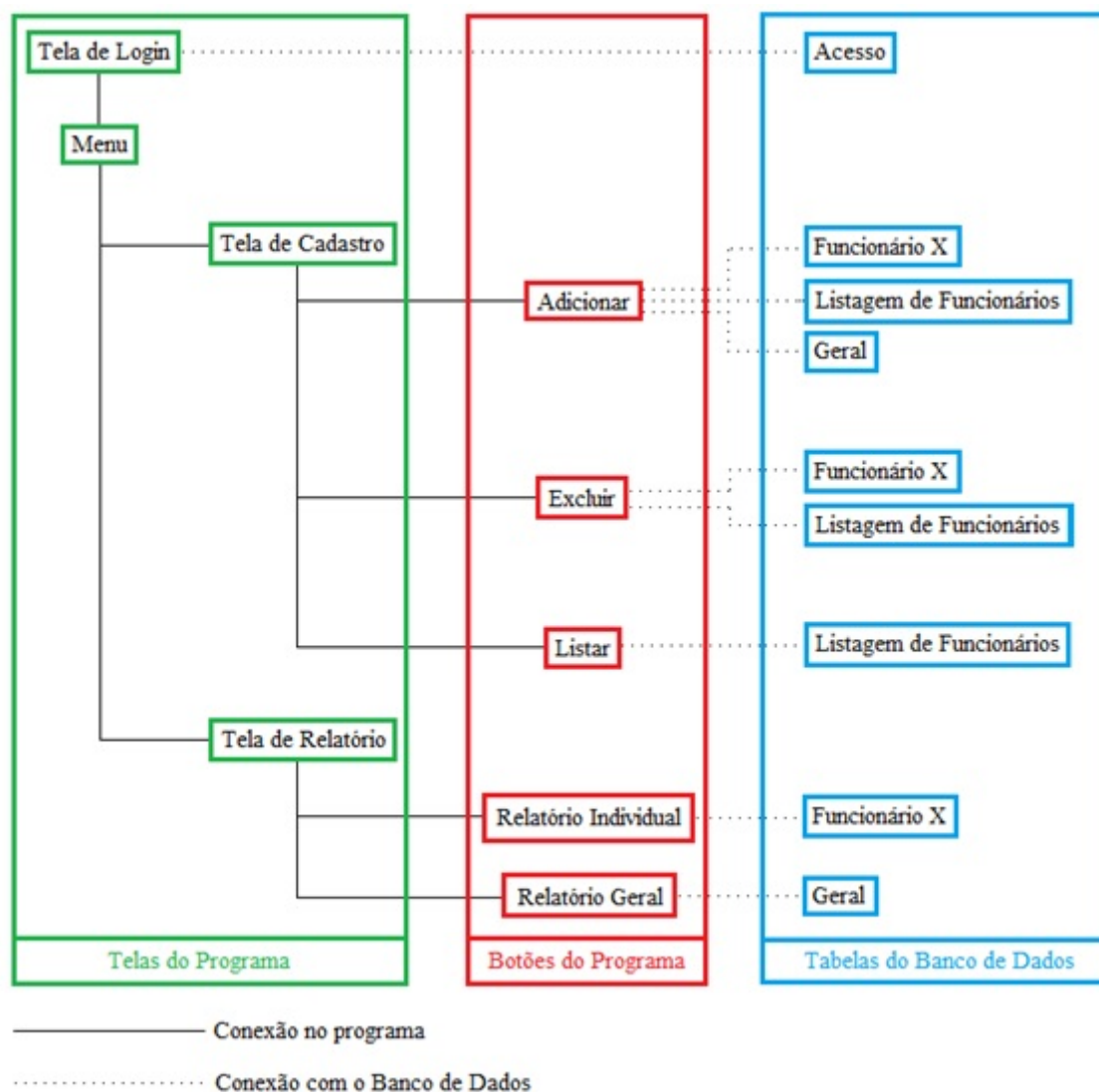


Figura 3.3: Ilustração da comunicação do *software* de gerenciamento com as tabelas do banco de dados

A primeira consulta ao banco de dados é realizada através da Tela de *Login*. Ela realiza uma consulta a Tabela Acesso para verificar se o usuário e senha fornecidos estão cadastrados e possuem autorização para acessar o *software* de gerenciamento.

A Tela de Cadastro realiza interações com o banco de dados através de três botões:

**Adicionar:** O botão Adicionar cria a tabela FuncionárioX; adiciona o nome e o ID deste usuário cadastrado na tabela Listagem de Funcionários; e adiciona o evento cadastro, assim como data

e horário em que foi realizado nas tabelas FuncionárioX e Geral.

**Excluir:** O botão Excluir exclui a tabela FuncionárioX respectiva ao usuário que se deseja eliminar do sistema; e exclui este usuário e ID da tabela Listagem de Funcionários.

**Listar:** O botão Listar lista na Tela de Cadastro os dados registrados na tabela Listagem de Funcionários, que são os nomes dos usuários e seus respectivos IDs.

A Tela de Relatório realiza interações com o banco de dados através de dois botões:

**Relatório Individual:** O botão Relatório Individual consulta a tabela FuncionárioX e utiliza seus dados para gerar o relatório individual, com os dados dos eventos do usuário requisitado.

**Relatório Geral:** O botão Relatório Geral consulta a tabela Geral e utiliza seus dados para gerar o relatório geral, com os dados dos eventos de todos os usuários.

### 3.3.2.2 Funções do *Software* de Gerenciamento

A seguir, serão apresentadas as funções deste *software*:

**Privacidade:** Solicita *login* e senha para acesso ao *software* de gerenciamento. Este *software* permite acesso direto ao conteúdo do Banco de Dados, e para garantir a segurança das informações nele contidas, ele realiza esta requisição para verificar a autorização do usuário. A Tela de Login pode ser visualizada na Figura 3.4.



Figura 3.4: Tela de Login

**Cadastro:** Adiciona e exclui usuários. A Tela de Cadastro permite adicionar um usuário ao banco de dados, associando-o a um ID. Este ID é o número único de identificação (EPC) da tag portada pelo mesmo. Assim, quando este ID for disponibilizado pelo leitor ao aplicativo, ele irá consultar os registros e identificar a qual usuário ele pertence. Esta tela também permite excluir usuários, sendo necessário apenas informar o ID. A Tela de Cadastro pode ser visualizada na

Figura 3.5.

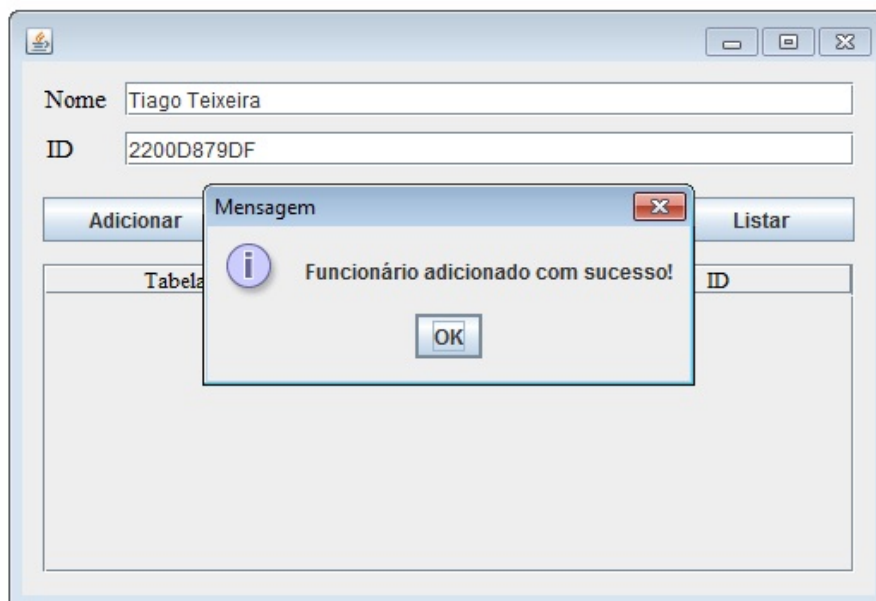


Figura 3.5: Tela de Cadastro

**Listagem:** Lista os usuário e IDs cadastrados. A Tela de Cadastro também permite listar todos os usuários cadastrados e seus respectivos IDs. A Tela de Cadastro listando os usuários e IDs cadastrados pode ser visualizada na Figura 3.6.



Figura 3.6: Tela de Cadastro listando os usuários e IDs cadastrados

**Interface com o Usuário:** Através de janelas. Permite a interação com o usuário através de interfaces gráficas como a Tela de Menu. Esta tela pode ser visualizada na Figura 3.7.

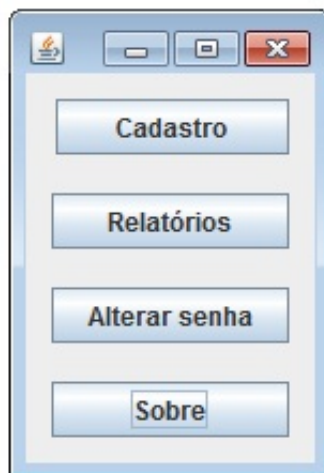


Figura 3.7: Tela de Menu

**Geração de Relatórios:** Gera relatórios individuais e gerais dos usuários. A Tela de Geração de Relatórios permite gerar relatórios individuais, através do fornecimento do nome do usuário cadastrado, ou gerar relatórios gerais, relativos a todos os usuários. Nestes relatórios, constam: os eventos (cadastro, entrada ou saída do usuário) em ordem cronológica; a data e horário em que eles ocorreram (no formato DD/MM/AAAA - HH:MM:SS); o tempo de permanência referente a última passagem do usuário pelo local; e a soma de todas as permanências, ou seja, o tempo total de permanência do usuário no local. A Tela de Geração de Relatórios pode ser visualizada na Figura 3.8.



Figura 3.8: Tela de Geração de Relatórios

**Conexão com o Banco de Dados:** Faz a conexão da aplicação com o banco de dados.

**Comunicação com o Banco de Dados:** Cria tabelas, insere e consulta informações no banco de dados.

Após compreender o modo de funcionamento de ambos os *softwares*, pode-se entender o modo de interação entre eles. O *Software* de Monitoramento monitora a porta serial à espera de um ID. Quando este ID é disponibilizado pelo leitor, é realizado o seu tratamento, assim como alguns testes para verificar a sua validade. Após realizados estes testes, este *Software* cadastra o evento no banco de dados e volta a monitorar a porta serial. Enquanto isso, o *Software* de Gerenciamento pode ser executado para, por exemplo, cadastrar um usuário, associando um ID ao seu nome. Imediatamente após este cadastro ter sido efetuado no banco de dados, a tag poderá ser utilizada pelo usuário para acessar o local, pois o *Software* de Monitoramento irá consultar o banco de dados e irá identificar que o ID agora pertence ao sistema. Com isto, pode-se notar que a interação entre *softwares* distintos é realizada através da comunicação com um mesmo banco de dados.

### 3.4 Etapa de Testes

Para verificar a consistência dos *softwares* desenvolvidos, foi realizada uma etapa de teste de campo. Esta etapa de teste foi realizada no Laboratório de Iniciação Científica (LabIC) do Instituto Federal de Santa Catarina (IFSC) Campus São José, que é o mesmo laboratório no qual o aplicativo foi desenvolvido. Esta etapa contou com a colaboração dos usuários do mesmo (bolsistas) e consistiu em monitorar o acesso destes ao laboratório, funcionando também como um ponto eletrônico.

A etapa de testes foi realizada durante um período de nove semanas, aproximadamente, e contou com a participação de seis bolsistas. Para facilitar a avaliação inicial do sistema, nas primeiras quatro semanas de teste foram cadastrados apenas três bolsistas. Entretanto, para aumentar o nível de complexidade dos testes e variar as possibilidades de situações imprevistas ocorrerem, mais três bolsistas foram cadastrados.

A arquitetura deste sistema de RFID para teste pode ser visualizada na Figura 3.9. Ela é formada por um leitor, localizado estrategicamente próximo a porta, e por tags RFID (cartões de proximidade) portadas pelos bolsistas. O leitor está conectado a um computador, onde está sendo executado o *software* (*middleware*). Sempre que uma pessoa portando um cartão RFID entrar na área de cobertura do leitor, o horário exato deste evento é registrado pelo *software*.

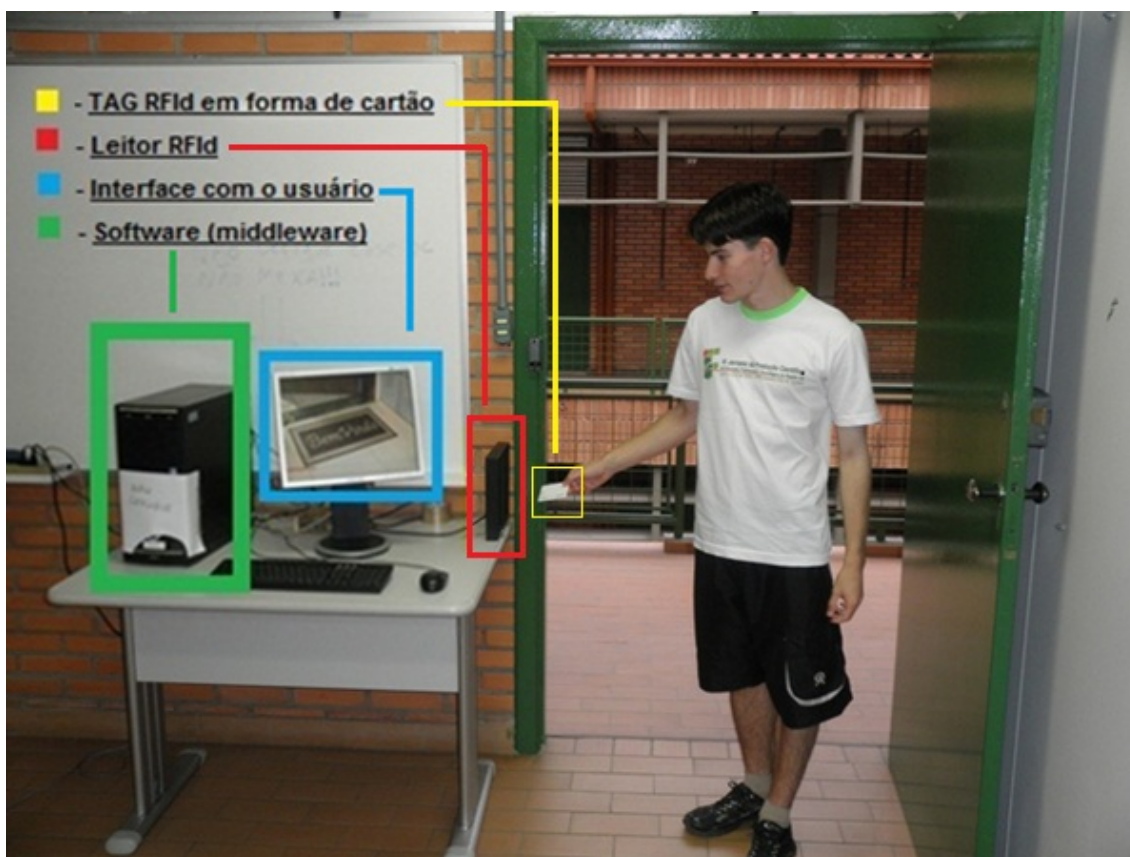


Figura 3.9: Sistema de RFID para testes

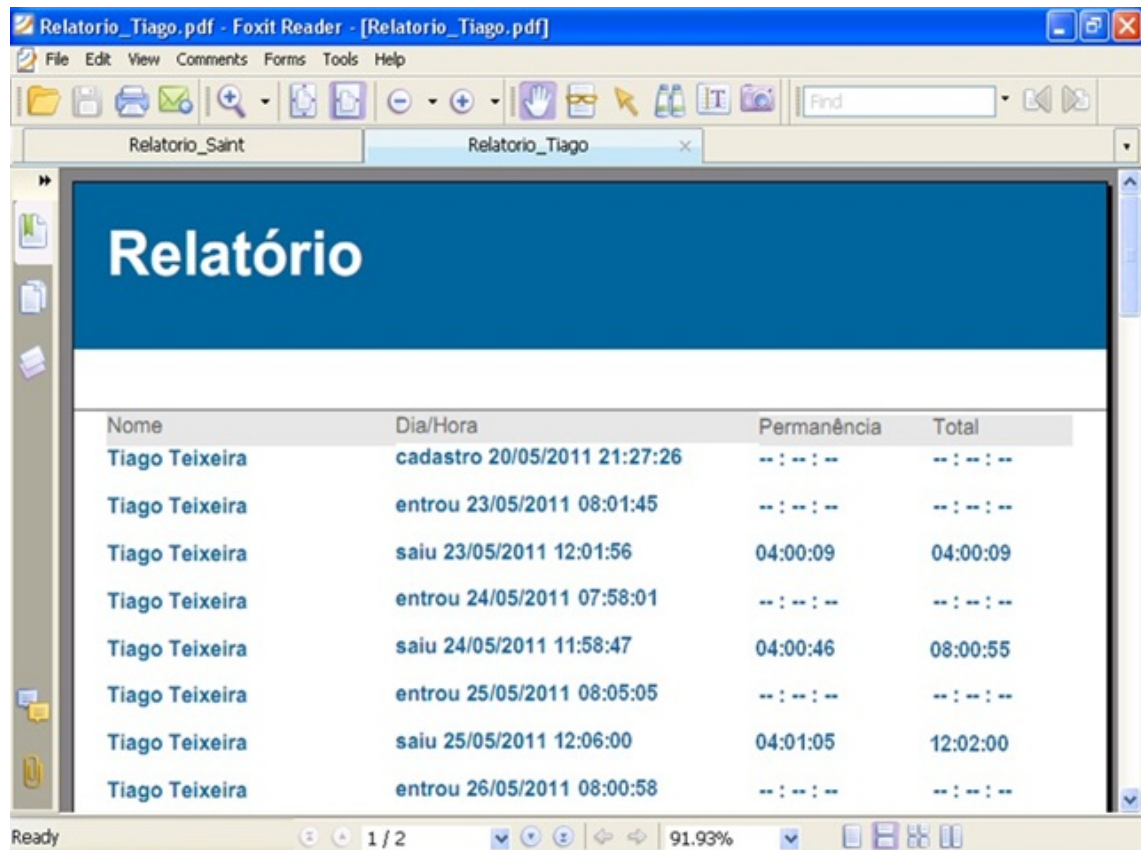
O leitor foi posicionado com as suas faces de maior alcance de irradiação, em relação a suas arestas e não ao centro (devido ao formato do leitor), noventa graus ( $90^\circ$ ) em relação à parede na qual estava a porta de entrada para o laboratório. Posicionando o leitor desta forma, uma de suas faces de maior alcance de irradiação estava posicionada também a noventa graus ( $90^\circ$ ) em relação à direção do fluxo de pessoas que entravam no laboratório através desta porta. O leitor foi colocado sobre uma mesa com altura aproximada de um metro. Esta altura foi considerada muito próxima da ideal para realizar os testes, pois a maioria dos bolsistas portava a tag em um dos bolsos laterais da calça.

Assim, considerando-se a posição do leitor, a direção do fluxo de pessoas através da porta e o local onde os bolsistas portavam as tags, avalia-se que os componentes leitor e tag estavam posicionados de forma ótima, um em relação ao outro, durante o fluxo de pessoas pela porta. Este posicionamento contribuiu para diminuir a possibilidade de uma passagem de tag pela porta não ser reconhecida pelo leitor.

Através do aplicativo é gerado um relatório como o da Figura 3.10, com todos os horários de passagem (entrada e saída) dos bolsistas pela entrada do laboratório e também o tempo exato que cada um deles permaneceu dentro dele. Para que estes horários sejam registrados



corretamente, o bolsista não pode entrar ou sair sem o cartão, pois sem ele, o aplicativo não registra o horário de passagem pela entrada, e com isso, não calcula corretamente o seu tempo de permanência no laboratório.



The screenshot shows a Foxit Reader window displaying a PDF report titled 'Relatório'. The report contains a table with the following data:

Nome	Dia/Hora	Permanência	Total
Tiago Teixeira	cadastro 20/05/2011 21:27:26	-- : -- : --	-- : -- : --
Tiago Teixeira	entrou 23/05/2011 08:01:45	-- : -- : --	-- : -- : --
Tiago Teixeira	saiu 23/05/2011 12:01:56	04:00:09	04:00:09
Tiago Teixeira	entrou 24/05/2011 07:58:01	-- : -- : --	-- : -- : --
Tiago Teixeira	saiu 24/05/2011 11:58:47	04:00:46	08:00:55
Tiago Teixeira	entrou 25/05/2011 08:05:05	-- : -- : --	-- : -- : --
Tiago Teixeira	saiu 25/05/2011 12:06:00	04:01:05	12:02:00
Tiago Teixeira	entrou 26/05/2011 08:00:58	-- : -- : --	-- : -- : --

Figura 3.10: Exemplo de relatório gerado pelo *software*

## 3.5 Resultados dos Testes

Foram avaliados na etapa de testes: o desempenho do sistema de RFID proposto e a consistência do *software* desenvolvido.

### 3.5.1 Consistência do *Software*

Em relação à consistência do *software*, foram identificados e corrigidos *bugs* e outros problemas que sem a etapa de testes, poderiam passar despercebidos e causar problemas no futuro, quando o *software* fosse submetido a situações reais.

Os principais problemas apresentados pelo *software* durante a etapa de testes foram: ‘*too many connections*’, ‘*communications link failure*’ e ‘*java heap space*’. Os dois primeiros são



problemas referentes ao uso de variáveis do banco de dados MySQL e foram facilmente identificados e solucionados. O terceiro é referente à memória *Heap*<sup>1</sup> utilizada no Java, esse problema exigiu um estudo sobre a utilização e os tipos de memórias do Java e uma revisão no código para diminuir a possibilidade desse erro voltar a acontecer. Após a constatação deste problema, o valor da memória *Heap* passou a ser monitorado nos testes.

Durante os testes, sentiu-se a necessidade de uma forma de interação com o usuário. Por este motivo, foram implementadas telas de ‘Boas Vindas’ no programa para informar ao usuário se sua entrada ou saída foi corretamente registrada pela aplicação. Esta simples interação evita vários problemas, pois pode acontecer de o leitor não enviar os dados para o programa, e com isso, o usuário não ter seu horário de passagem pelo leitor registrado. Porém, com a tela de ‘Boas Vindas’, o usuário sempre saberá se sua passagem foi corretamente registrada.

**Avaliação:** Após corrigidos os *bugs* do programa e supridas as necessidades referentes a interação com o usuário, o *software* se mostrou estável; e os relatórios gerados passaram a ser reconhecidos como registros dos horários de entrada e saída de cada bolsista.

### 3.5.2 Desempenho do Sistema de RFId

Em relação ao sistema de RFId, não foi necessária nenhuma modificação relevante na arquitetura, nos componentes ou no posicionamento destes. Todos funcionaram adequadamente e não apresentaram nenhum problema de desempenho. O único atenuante que pôde ser observado foi o fato da distância máxima de leitura do leitor utilizado ser de, aproximadamente, trinta e seis centímetros ao redor do centro do equipamento, sendo que, segundo a especificação do produto, esta distância máxima de leitura poderia chegar a um metro. Contudo, a distância máxima de leitura de trinta e seis centímetros foi considerada suficiente para a realização dos testes.

**Avaliação:** O sistema de RFId apresentou um ótimo desempenho na etapa de testes. Rapidamente, os usuários se adaptaram ao sistema e o aplicativo passou a não apenas controlar o fluxo de pessoas no laboratório, mas também funcionar como um ponto eletrônico extraoficial para os bolsistas.

---

<sup>1</sup>A memória *Heap* armazena todos os objetos que são utilizados em um programa. Quando um objeto é instanciado, ele e seus respectivos parâmetros são automaticamente alocados na *Heap*. Quando um método que utiliza o objeto é finalizado, uma exceção ocorre, ou o número de referências ao objeto cai a zero, ou *threads* que utilizam o mesmo são finalizadas. Então, o objeto fica passível de ser coletado pelo *Garbage Collector*

## 3.6 Considerações Finais

Para que um sistema de controle de fluxo de pessoas usando a tecnologia de RFID seja utilizado pelas instituições sem causar problemas e com o máximo de aproveitamento do seu potencial, existem algumas mudanças de conduta ou inclusões de hábitos que podem ser recomendados aos usuários. Respeitando-se estas recomendações e fazendo bom uso do equipamento, pode-se garantir o funcionamento adequado do sistema. As principais recomendações são em relação à:

**Porte da tag:** O usuário do sistema deve estar sempre de posse da sua tag RFID, pois sem ela, o leitor não poderá identificar a sua passagem.

**Uso da tag:** O usuário não pode trocar ou emprestar a sua tag, pois enquanto um ID estiver cadastrado no sistema associado a um nome, a tag deve ser de uso pessoal e intransferível.

**Leitura da tag:** O usuário deve sempre se certificar de que a sua tag realmente foi lida pelo leitor. Esta verificação pode ser efetuada através de mensagens visuais ou avisos sonoros. Pode ocorrer de o leitor demorar alguns segundos para reconhecer a tag, por uma interferência momentânea por exemplo. Caso a tag não seja reconhecida pelo leitor, o registro do acesso no banco de dados não será realizado.

O sistema de RFID não causará grande impacto ou mudanças de rotina na vida das pessoas. Uma aplicação de controle de fluxo usando RFID tem como características a discrição e a praticidade. Após instalados os equipamentos e cadastrados os usuários, estes irão usufruir da tecnologia muitas vezes sem perceber. Um funcionário de uma empresa poderá passar por leitores localizados nos corredores, registrando a sua movimentação através da leitura de sua tag, e ao final do mês, este funcionário poderá consultar um relatório com o seu histórico de movimentações pela empresa. Já a questão da praticidade se deve ao fato de que a possibilidade de uma má leitura, fazendo com que o usuário tenha que repetir o procedimento de identificação, é muito menor na tecnologia de RFID, comparando-se com outras tecnologias utilizadas no controle de acesso disponíveis no mercado, como código de barras e biometria.

## 3.7 Futuro do Aplicativo

Alguns aprimoramentos poderão ser implementados no aplicativo futuramente. Melhorias como: enviar os relatórios individuais para cada usuário através de *e-mail*; adicionar alarmes relativos à faltas, atrasos, hora-extras, excesso de entradas e saídas, acesso a áreas consideradas restritas, etc; configuração manual do banco de dados para abatimento de horas, férias, ou

até mesmo caso o usuário não registre seu horário corretamente com o cartão; inclusão de uma tela personalizada de identificação (com foto por exemplo) para cada usuário; entre outros aperfeiçoamentos que deverão ser realizados conforme exigência de cada tipo de aplicação.

Um possível futuro local de aplicação para um sistema de RFId como o da fase de testes, seria a portaria de escolas. Inclusive, o próprio IFSC poderia ter muitos benefícios utilizando a tecnologia de RFId. Se os alunos do Instituto utilizassem carteirinhas RFId, ao invés das convencionais, e um leitor fosse colocado na portaria, os horários de entrada e saída de cada aluno seriam registrados automaticamente pelo aplicativo de controle de fluxo. Os leitores RFId também poderiam ser colocados na portas das salas de aula, registrando a presença dos alunos nas aulas.

Alguns benefícios desta implementação no IFSC seriam:

- Não haver a necessidade dos alunos apresentarem a carteirinha ao porteiro. A identificação dos alunos poderia ser feita por uma tela de identificação personalizada com seu nome, foto, curso, etc;
- Não haver a necessidade de realização de chamadas nas aulas. Os alunos poderiam registrar sua presença passando sua carteirinha RFId pelo leitor localizado na porta da sala;
- Geração de relatórios com os horários de entrada e saída de cada aluno no Instituto e nas salas de aula;
- Geração de relatórios da movimentação dos alunos pelo campus, dependendo de onde forem colocados os leitores RFId;
- Ponto eletrônico para os profissionais que trabalham no IFSC, como professores, servidores, bolsistas, estagiários, etc;

Com estes exemplos, pode-se notar que existem muitas vantagens que um aplicativo de controle de fluxo como o que foi desenvolvido pode trazer para as instituições nas quais ele for aplicado e que, dependendo do tipo de aplicação específica, determinadas melhorias poderão ser feitas no aplicativo com o objetivo de trazer ainda mais benefícios.

## 4 *Conclusões*

A promissora tecnologia de RFId implementa um método automático de identificação de objetos, locais ou até seres vivos, de maneira remota através da rádio frequência. Embora já seja amplamente utilizada, esta tecnologia ainda se mostra com muito potencial inovador, pois frequentemente surgem novas aplicações nas mais variadas áreas. As principais barreiras para a expansão desta tecnologia são: deficiência na segurança dos dados, falta de padronização e alto custo para determinadas aplicações. Após solucionados estes problemas, o RFId tende a se popularizar ainda mais.

Um sistema de controle de fluxo de pessoas utilizando a tecnologia de RFId deve se adequar tão bem a situações reais quanto se adequou a etapa de testes. Este sistema pode ser muito útil aonde vir a ser utilizado, pois através do aplicativo de controle de fluxo que foi desenvolvido, é possível controlar o acesso à áreas restritas, registrar o horário de entrada e saída de cada usuário e até o deslocamento deles pela empresa.

Entretanto, o sistema RFId tem algumas desvantagens em relação aos sistemas convencionais e, se não for utilizado corretamente, pode trazer prejuízos aos seus usuários. As principais desvantagens são descritas a seguir:

**Alto Investimento** – Como já foi citado, o custo é um dos principais obstáculos para implementação da maioria dos aplicativos de RFId e, para um sistema de controle de fluxo de pessoas não é diferente. Caso a aplicação seja apenas na portaria de uma instituição ou em suas áreas restritas, o custo não é proibitivo. Contudo, se houver a necessidade de controlar o fluxo em muitos locais, como em uma aplicação que controle o deslocamento dos usuário pela instituição, o custo seria muito elevado, pois seriam necessários vários leitores, ou leitores com maior alcance, e portanto, mais caros.

**Manutenção** – Embora a durabilidade das tags esteja sujeita exclusivamente ao seu bom uso, o mesmo não se pode afirmar sobre o restante do sistema. Por exemplo: os leitores, como o que foi utilizado nos testes, diminuem sua área máxima de alcance de leitura proporcionalmente ao seu tempo de utilização e certamente, com o passar dos anos, irão precisar de manutenção,

troca de peças ou até mesmo aquisição de outro equipamento.

**Porte da Tag** – Os usuários de um sistema de controle de fluxo usando a tecnologia de RFID sempre devem estar, obrigatoriamente, de posse da tag. Caso isto não ocorra, o leitor não poderá registrar os horários em que o usuário passou por ele, e isso irá comprometer a veracidade do conteúdo dos relatórios gerados pelo sistema. Esta obrigatoriedade pode se tornar incômoda para os usuários, dependendo do tipo de aplicação e do formato da tag.

**Privacidade** – O excesso de controle sobre horários e deslocamento pode ser tornar uma invasão da privacidade dos usuários. Dependendo do local onde for aplicado e, principalmente, de seus administradores, o sistema de controle de fluxo poderá ser utilizado para monitoração excessiva e até mesmo perseguição de pessoas devido a sua grande eficiência em registro de horários.

**Segurança** – Com a utilização do sistema de controle de fluxo, haverá uma grande quantidade de informações sigilosas de usuários armazenada no banco de dados. Pessoas mal intencionadas poderiam apagar, modificar ou utilizar este conteúdo para fins inescrupulosos caso obtivessem acesso a ele. Por este motivo, deverá haver um maior controle e investimento em segurança de dados.

Contudo, se for corretamente utilizado e administrado por pessoas responsáveis, o sistema de controle de fluxo de pessoas com certeza trará muitos benefícios aos seus investidores. Seu método de funcionamento é extremamente eficiente e seus resultados aparentam ser muito satisfatórios. Muitos lugares no futuro poderão fazer uso de um aplicativo de RFID no controle de fluxo de pessoas, como por exemplo: empresas, hospitais, escolas, estabelecimentos comerciais, condomínios e qualquer outro local que possa ter uma área restrita.

De acordo com (HECKEL, 2007, p. 67): “Os sistemas RFID vieram para ficar, visto que grandes empresas já utilizam a tecnologia para melhor controlar seus processos, resta saber se a tecnologia vai realmente superar os problemas e virar uma tendência no processo de identificação de objetos.” e de pessoas.

Finalizando, o aplicativo de controle de fluxo que foi desenvolvido demonstrou como a tecnologia de RFID pode ser inserida nas instituições de uma maneira simples e a etapa de testes comprovou a fiabilidade deste aplicativo, submentendo-o a uma situação real de utilização na qual ele mostrou ótimo desempenho. Após implementadas algumas melhorias, que serão exigidas para cada tipo específico de aplicação, e mais alguns testes de campo, o aplicativo poderá ser utilizado comercialmente e provavelmente demonstrará a mesma consistência que demonstrou nos testes.

## *Lista de Abreviaturas*

**AIDC** *Automatic Identification and Data Capture*

**API** *Application Programming Interface*

**ASK** *Amplitude Shift Keying*

**CRC** *Cyclic Redundancy Check*

**EAN** *European Article Number*

**EAS** *Eletronic Article Surveillance*

**EEPROM** *Electrically-Erasable Programmable Read-Only Memory*

**EPC** *Eletronic Produte Code*

**FSK** *Frequency Shift Keying*

**GS1** *Global System 1*

**HF** *High Frequency*

**ID** *Identificação*

**IFSC** *Instituto Federal de Santa Catarina*

**ISO** *International Organization for Standardization*

**LabIC** *Laboratório de Iniciação Científica*

**LF** *Low Frequency*

**MCT** *Ministério da Ciência e Tecnologia*

**MF** *Microwave Frequency*

**MIT** *Massachusetts Institute of Technology*

**PSK** *Phase Shift Keying*

**RF** *Radio Frequency*

**RFId** *Radio Frequency Identification*

**ROM** *Read Only Memory*

**SAW** *Surface Acoustic Wave*

**SQL** *Structured Query Language*

**UCC** *Uniform Code Council*

**UHF** *Ultra High Frequency*

**VIP** *Very Important Person*

## *Referências Bibliográficas*

AHSON, S.; ILYAS, M. *Applications, Technology, Security, and Privacy*. [S.l.]: Taylor & Francis Inc, 2008.

BOLZANI, C. A. M. *Computação Pervasiva e Sistemas de Identificação*. Dissertação (Mestrado) — Escola Politécnica da Universidade de São Paulo, São Paulo, 2004.

BRASIL-ID. Sistema nacional de identificação, rastreamento e autenticação de mercadorias. In: MINISTÉRIO DA CIÊNCIA E TECNOLOGIA. 2011. Disponível em: <<http://www.brasil-id.org.br/>>. Acesso em: 05 ago. 2011.

CARDOSO, F. de S. *Contribuição ao Desenvolvimento de um Sistema de Identificação por Rádio Frequência para Aplicações Hospitalares*. Dissertação (Mestrado em Engenharia Biomédica) — Área de Instrumentação Biomédica, Universidade Federal da Paraíba, João Pessoa, 2000.

CUNHA, R. P. *O Uso da Tecnologia RFId no Gerenciamento de uma Cadeia de Suprimentos*. Dissertação (Bacharelado) — Engenharia da Computação, Faculdade de Engenharia de Sorocaba, Sorocaba, 2005.

DOBKIN, D. M. *The RF in RFId Passive UHF RFId in Practice*. [S.l.]: Elsevier, 2008.

DUARTE, J. A. M. Automação do sistema de ordem de serviço e formação de trens em pátios. In: REVISTA FERROVIÁRIA. 2005. Disponível em: <<http://www.revistaferroviaria.com.br/maxion2005/trabalhos/>>. Acesso em: 05 ago. 2011.

FAHL, C. R. *Um estudo sobre a Viabilidade de Implantação de Etiquetas Inteligentes como Vantagem Competitiva em um Centro de Distribuição*. Dissertação (Monografia) — Instituto Paulista de Ensino e Pesquisa - Centro de Pós-graduação, Gestão de Negócios em Logística e Transportes, Campinas, 2005.

GLOVER, B.; BHATT, H. *Fundamentos de RFID*. [S.l.]: Alta Books, 2007.

GREFF, P. de A. *Especificação de um Sistema para Monitoramento de Atividades de Natação usando RFId*. Dissertação (Tecnólogo) — Curso Superior de Tecnologia em Sistemas de Telecomunicações, Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina - Campus São José, São José - SC, Outubro 2009.

HECKEL, A. P. *Identificação por Radiofrequência (RFId) Estudo Teórico e Experimentação Via Simulação*. Dissertação (Bacharelado) — Ciência da Computação, Centro Universitário Feevale, Novo Hamburgo, Novembro 2007.



- KAMINSKY, O. Ministérios assinam acordo de cooperação para a criação do brasil-id. In: INTERNETLEGAL. 2009. Disponível em: <<http://www.internetlegal.com.br/2009/09/ministerios-assinam-acordo-de-cooperacao-para-a-criacao-do-brasil-id/>>. Acesso em: 05 ago. 2011.
- MANSUR, M. Rfid nos supermercados. In: TURMA 4A. 2010. Disponível em: <<http://turma4a201001.bligo.com/content/view/774347>>. Acesso em: 05 ago. 2011.
- MARTINS, V. A. Rfid (identificação por radiofrequência). In: TELECO. 2005. Disponível em: <<http://www.teleco.com.br/tutoriais/tutorialrfid/default.asp>>. Acesso em: 05 ago. 2011.
- MOROZ, R. Understanding radio frequency identification (rfid). (passive rfid). In: RFIDCANADA. 2004. Disponível em: <<http://www.rfidcanada.com/rfid.html>>. Acesso em: 05 ago. 2011.
- NISHIDA, J. K. *Identificação por Radio Frequência (RFId)*. Dissertação (Bacharelado) — Engenharia Elétrica Telemática, Universidade do Sul de Santa Catarina, Florianópolis - SC, Junho 2008.
- NOGUEIRA, I. C. Gerenciando a biblioteca do amanhã: tecnologias para otimização e agilização dos serviços de informação. 2003.
- OLIVEIRA, A. de S.; PEREIRA, M. F. *Estudo da tecnologia de identificação por radiofrequência - RFID*. Dissertação (Projeto de Graduação) — Faculdade de Tecnologia – Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, 2006.
- PINHEIRO, J. M. S. Técnicas de modulação em redes de telecomunicações. *Projeto de Redes*, Fevereiro 2005.
- RFID-GET-STARTED. What is rfid? In: RFID JOURNAL. 2011. Disponível em: <<http://www.rfidjournal.com/article/view/1339>>. Acesso em: 05 ago. 2011.
- SANTANA, S. R. M. Rfid - identificação por rádio frequência. In: WIRELESSBR. 2005. Disponível em: <<http://www.wirelessbrasil.org/wirelessbr>>. Acesso em: 05 ago. 2011.
- SANTINI, A. G. *RFID*. Dissertação (Mestrado) — Curso de Sistemas de Informação, Centro Universitário de Votuporanga, Votuporanga, 2006.
- SANTOS, K. T. dos; JÚNIOR, L. G. R. *Identificação por Rádio Frequência*. Dissertação (Projeto de Conclusão de Curso) — Universidade Federal de Goiânia, Graduação em Engenharia Elétrica, Goiânia, 2003.
- SHAHAM, M.; MANISH, B. *RFID Field Guide: Deploying Radio Frequency Identification Systems*. [S.l.]: Prentice Hall PTR, 2005.