

**CENTRO UNIVERSITÁRIO DO ESTADO DO PARÁ**  
**ÁREA DE CIÊNCIAS EXATAS E TECNOLOGIA**  
**BACHARELADO EM ENGENHARIA DA COMPUTAÇÃO**

**Jellyane da Cruz Rocha**

**Jéssica do Nascimento Campos Gomes**

**Mateus Vieira de Almeida**

**PROJETO DE CONTROLE DE ACESSO UTILIZANDO RFID PARA**  
**INSTITUIÇÕES DE ENSINO**

**Belém**

**2017**

**CENTRO UNIVERSITÁRIO DO ESTADO DO PARÁ**  
**ÁREA DE CIÊNCIAS EXATAS E TECNOLOGIA**  
**BACHARELADO EM ENGENHARIA DA COMPUTAÇÃO**

**Jellyane da Cruz Rocha**

**Jéssica do Nascimento Campos Gomes**

**Mateus Vieira de Almeida**

**PROJETO DE CONTROLE DE ACESSO UTILIZANDO RFID PARA**  
**INSTITUIÇÕES DE ENSINO**

Trabalho de Curso na modalidade Monografia, apresentado como requisito parcial para obtenção do grau em Bacharelado em Engenharia da Computação do Centro Universitário do Estado do Pará – CESUPA, sob orientação da Professora Msc. Michelle Bitar Lelis dos Santos.

**Belém**

**2017**

**Dados Internacionais de Catalogação-na-publicação (CIP)**

**Biblioteca do Cesupa, Belém - PA**

---

Rocha, Jellyane da Cruz.

Projeto de controle de acesso utilizando RFID para instituições de ensino / Jellyane da Cruz Rocha, Jéssica do Nascimento Campos Gomes, Mateus Vieira de Almeida; orientação de Michelle Bitar Lelis dos Santos, 2017.

Trabalho de Conclusão de Curso (Bacharelado em Engenharia da Computação) – Centro Universitário do Pará, Belém, 2017.

1. Radiofrequência. 2. Controle de acesso. I. Gomes, Jéssica do nascimento Campos. II. Almeida, Mateus Vieira de. III. Santos, Michelle Bitar Lelis dos (orient.). IV. Título.

CDD. 23º ed. 005.1

---

**Jellyane da Cruz Rocha**

**Jéssica do Nascimento Campos Gomes**

**Mateus Vieira de Almeida**

**PROJETO DE CONTROLE DE ACESSO UTILIZANDO RFID PARA  
INSTITUIÇÕES DE ENSINO**

**Trabalho de Curso apresentado na modalidade monografia**, apresentado como requisito parcial para obtenção do grau em Bacharelado em Engenharia da Computação do Centro Universitário do Estado do Pará – CESUPA.

**Data da Defesa: 22/06/2017**

Banca Examinadora:

---

**Orientadora Profa. Msc. Michelle Bitar Lelis dos Santos – CESUPA**

---

**Co-orientador Prof. Esp. Cassio Diego Tavares Campos – ESTÁCIO**

---

**Prof. Msc. Johnny Marcus Gomes Rocha – CESUPA**

**Belém**

**2017**

Dedicamos este trabalho às nossas famílias,  
pelos incansáveis momentos em que nos  
apoiaram.

E a todos que direta ou indiretamente  
contribuíram para a conclusão desta etapa de  
nossas vidas.

## **AGRADECIMENTOS**

A Deus, que sempre me deu segurança e forças para contornar as dificuldades encontradas ao decorrer deste trabalho e ao longo da minha vida.

Aos meus pais, Roberto Jancyll Chargas da Rocha e Jeane Aleixo da Cruz Rocha, por cuidado, amor e abdicação do próprio conforto para que eu pudesse concluir essa graduação.

A nossa orientadora, Michelle Bitar, que ficou responsável pela orientação deste trabalho nos acréscimos do segundo tempo, e ainda assim realizou um excelente acompanhamento, mesmo com sua querida pedra no rim e o pouco tempo que teve. Muito obrigada, professora!

Ao nosso coorientador, Cassio Diego, que disponibilizou do seu tempo para auxiliar no desenvolvimento do protótipo. Pelo seu acompanhamento, incentivo e por ter acreditado desde o início que conseguiríamos finalizar. Muito obrigada!

Ao coordenador do curso, Itamar Brito, e todo o corpo docente que sempre buscaram o melhor para o curso, possibilitando o meu conhecimento para chegar até aqui.

As minhas melhores amigas, Jancyelle Rocha e Mayumi Konagano, que escutam meus desabaços desde criança que se intensificaram nesse último semestre com o tão famoso TCC.

Aos meus colegas de TCC, Jéssica Campos e Mateus Almeida, porque juntos conseguimos finalizar este trabalho de conclusão de curso, e pelos quatro anos e meio de graduação.

Jellyane da Cruz Rocha

## **AGRADECIMENTOS**

Agradeço primeiramente a Deus, pelas bênçãos recebidas, por nos conceder perseverança para concluir mais essa etapa em nossas vidas.

Aos meus avós, Maria de Nazaré e João pela presença ao longo do curso, pelos cuidados e pelos sábios conselhos, sempre acreditando no meu êxito sem forçar expectativas, me deixando livre para fazer minhas próprias escolhas ao longo de minha jornada.

Aos meus familiares, pelo suporte, pelos momentos, pela (ampla) paciência, por viabilizar meus estudos e por estarem presentes em todos os momentos da minha vida. Pelos ensinamentos, e principalmente pelo ensinamento de saber rir do próprio momento de dificuldade.

Aos meus amigos que ajudaram a me manter motivada, que entenderam meus momentos de ausência e pelas dicas de formatação que tentaram me passar. Em especial aos amigos do grupo “Quase Engenheiros” que proporcionaram momentos de alegria, tristeza, estresse e companheirismo.

Ao Roberto Guimarães por ser um dos grandes responsáveis por possibilitar a minha permanência na instituição de ensino. Obrigada pelo tempo gasto em bancos esperando eternamente pelo atendimento e por ser meu fiador.

Ao coordenador Itamar Vilhena por todo o esforço voltado para amparar o curso da melhor forma possível e principalmente por estar sempre disponível quando necessário e pela maravilhosa indicação para a orientação desse trabalho.

Aos professores que de alguma forma contribuíram para a realização desse trabalho, seja na correção ou na contribuição em conteúdo, em especial ao professor Cassio Diego pelo tempo disponibilizado e por todo o esforço empregado em nos ajudar com as partes mais críticas do protótipo e, a professora Michelle Bitar por mesmo com um curto prazo a ser respeitado, se disponibilizou a nos ajudar e conseguiu nos motivar a concluir esse desafio.

“Quem diria que um dia a gente estaria aqui...!”

Jéssica do Nascimento Campos Gomes

## **AGRADECIMENTOS**

Primeiramente a Deus, por ter me concedido bênçãos, força e perseverança para continuar até o fim e terminar o curso.

Aos meus pais Robson Almeida e Mônica Vieira que me deram forças e incentivo nos momentos difíceis para levar o curso adiante e, acima de tudo, proporcionaram-me esse momento único custeando o curso com muita luta e suor.

A minha madrastra Tatiana Oliveira e padrasto André Torres, por sempre estarem presentes, em todos esses anos, nos momentos mais importantes dessa caminhada.

Aos meus avós José e Inês Almeida pela força que me deram na reta final do curso.

Aos meus tios Junior Almeida e Glória Dias pela preocupação ao longo de toda a caminhada.

Aos meus irmãos Amanda e Leonardo Vieira que, apesar da distância, são peças cruciais na minha vida e na minha história.

Aos meus primos Krissia Lorena, Ícaro Kalleu e Ítalo Kassiel, que ao longo desses anos me fizeram fugir da rotina quando necessário. Além de me apoiar e estarem comigo a cada passo.

A Jellyane Rocha e Jéssica Campos que, além de serem uma parte indispensável dentro da rotina nesses quatro anos e meio, foram as pessoas que, junto comigo, fizeram este trabalho ser possível.

Aos meus amigos de trabalho, de sala, professores e coordenadores que fizeram parte do meu percurso até o fim dessa jornada.

As amigas Amanda Furtado, Andreza Araújo, Cintia Alice e Maiza Costa que nos momentos mais difíceis fizeram-se presente me apoiando com atitudes e palavras para que eu não fraquejasse em momento algum. Inclusive no período conturbado que foi o final de curso.

A nossa orientadora Michelle Bitar que aceitou assumir um trabalho crítico faltando menos de um mês para a entrega, lutou conosco e nos direcionou no caminho que levasse a aprovação deste projeto. Sem ela e sem nosso co-orientador Cássio Diego, esse trabalho com certeza não seria possível.

Por fim, a todos que fizeram parte da história dessa caminhada me ajudando e contribuindo de alguma forma para a conclusão deste desafio!

Um muito obrigado a todos! Sem vocês, nada disso seria possível!

Mateus Vieira de Almeida

Nunca é tarde demais para começar tudo de novo...

Raul Seixas

## RESUMO

Esta monografia demonstra o uso de RFID (*Radio Frequency Identification*) para aplicações de segurança e controle de acesso, ilustrando como esta tecnologia poderá beneficiar instituições e empresas oferecendo agilidade, tendo como estudo de caso o Centro Universitário do Pará (CESUPA), unidade Governador José Malcher. Comprovar-se-á que o RFID pode ser usado em instituições com grande fluxo de pessoas, não se restringindo às instituições de ensino, uma vez que empresas e outras instituições podem ser bem avaliadas se oferecerem qualidade de atendimento aos seus usuários e clientes, tendo como foco o fator segurança. Outros sistemas semelhantes já apresentaram falhas, porém o RFID tem sido a tecnologia mundialmente reconhecida como eficiente pela sua rapidez ao identificar e processar informações. Na aplicação prática apresenta-se um protótipo da tecnologia RFID para gerenciar o acesso no CESUPA, utilizando *tags* e buscas no banco de dados, visualização e análise via *web*. Na construção do protótipo foram utilizados módulos com antena e leitor RFID, sendo criados dois sistemas em linguagem Java, na IDE NetBeans, o armazenamento no banco de dados *MySQL*, a placa Arduino e desenvolvimento da *web*, realizado na linguagem *Hypertext Preprocessor* (PHP) e a configuração do servidor *web* Apache.

**Palavras-chave:** Tecnologia RFID. Segurança. Controle de Acesso. Protótipo.

## ABSTRACT

This monograph demonstrates the use of RFID (Radio Frequency Identification) for security and access control applications, illustrating how this technology can benefit institutions and companies offering access control agility, having as a case study the University Center of Pará (CESUPA), Governador José Malcher unit. It will be verified that RFID can be used in institutions with large flow of people, not restricted to educational institutions, since companies and other institutions can be well evaluated if they offer quality of service to their users and clients, having as Focus the safety factor. Other similar systems have already flawed, but RFID has been the world-renowned technology as efficient in its speed in identifying and processing information. In the practical application, a prototype of RFID technology is presented to manage the access in organizations with great flow of people, using tags and searches in the database, visualization and analysis via web. In the construction of the prototype were used modules with antenna and RFID reader, being created two systems in Java language, on NetBeans IDE, storage in MySQL database, Arduino board and web development, realized in the language Hypertext Preprocessor (PHP) and The Apache web server configuration.

**Keywords:** RFID technology. Safety. Access Control. Prototype.

## LISTA DE FIGURAS

Figura 1 – Início do RFID. ....	24
Figura 2 – RFID durante os anos 60 a 90. ....	25
Figura 3 – RFID dos anos 90 aos dias atuais. ....	25
Figura 4 – Funcionamento básico do sistema RFID. ....	26
Figura 5 – <i>Tag</i> do sistema RFID. ....	26
Figura 6 – Exemplo de <i>tag</i> ativa. ....	27
Figura 7 – Exemplo de <i>tag</i> passiva. ....	28
Figura 8 – Exemplo de <i>tag</i> semi-passiva. ....	29
Figura 9 – Funcionamento do Leitor. ....	30
Figura 10 – Antena dentro do Sistema RFID. ....	31
Figura 11 – <i>Middleware</i> em um sistema RFID. ....	33
Figura 12 – <i>Scanner</i> FS25 com cartão Mifare. ....	34
Figura 13 – Kimaldi Flexy. ....	35
Figura 14 – Lumen Advance. ....	36
Figura 15 – Aplicação do sistema RFID em pedágios. ....	37
Figura 16 – Pequeno <i>chip</i> RFID utilizado na área da saúde. ....	38
Figura 17 – Pulseiras que utilizam a tecnologia RFID na área da saúde. ....	39
Figura 18 – Componentes do sistema embarcado. ....	44
Figura 19 – Nintendo NES <i>Classic Edition</i> . ....	46
Figura 20 – Dispositivo TeleCare. ....	47
Figura 21 – Amostra de modelos de placas Arduino. ....	48
Figura 22 – Arduino Uno. ....	49
Figura 23 – Módulo MFRC522. ....	52
Figura 24 – Modo de leitura e escrita. ....	53
Figura 25 – <i>Tag</i> chaveiro MIFARE S50 utilizada no protótipo. ....	53
Figura 26 – Esquema da <i>tag</i> MF1S50yyX/V1. ....	54
Figura 27 – Microcontrolador ATmega328P. ....	54
Figura 28 – IDE Arduino. ....	56
Figura 29 – Dados recebidos a porta serial. ....	57
Figura 30 – IDE NetBeans versão 8.1. ....	57
Figura 31 – Esquema eletrônico dos componentes físicos. ....	59

Figura 32 – Interface gráfica do software de cadastro.....	60
Figura 33 – Modelagem do Banco de Dados. ....	61
Figura 34 – Tela de <i>login</i> .....	62
Figura 35 – Tela de Acesso. ....	63
Figura 36 – Busca por matrícula. ....	63
Figura 37 – Gráfico dos acessos mensais. ....	64

## LISTA DE TABELAS

Tabela 1 – Comparação entre as <i>tags</i> . .....	29
Tabela 2 – Faixas de frequência utilizada em alguns países. ....	32
Tabela 3 – Problemas de segurança envolvendo o sistema RFID. ....	41
Tabela 4 – Uso das linguagens de programação em sistemas embarcados. ....	43
Tabela 5 – Dados técnicos do Arduino. ....	50

## LISTA DE SIGLAS

CESUPA	Centro Universitário do Pará
CI	Circuito Integrado
CIOP	Centro Integrado de Operações Policiais
CPU	Unidade Central de Processamento
EEPROM	<i>Electrically-Erasable Programmable Read-Only Memory</i>
GPL	<i>General Public License</i>
HF	<i>High Frequency</i>
I2C	<i>Inter Integrated Circuit</i>
IDE	<i>Integrated Development Environment</i>
IFF	<i>Identify Friend Or Foe</i>
JDBC	<i>Java Database Connectivity</i>
LF	<i>Low Frequency</i>
MIPS	Milhões de Instruções por Segundo
PHP	<i>Hypertext Preprocessor</i>
PWM	<i>Pulse Width Modulation</i>
RADAR	<i>Radio Detection And Rangig</i>
RFID	<i>Radio Frequency Identification</i>
SPI	<i>Serial Peripheral Interface</i>
UART	<i>Universal Asynchronous Receiver Transmitter</i>
UHF	<i>Ultra High Frequency</i>
UID	<i>Unique IDentification</i>
USART	<i>Universal Synchronous Asynchronous Receiver Transmitter</i>
USB	<i>Universal Serial Bus</i>

# SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO</b> .....	18
1.1	JUSTIFICATIVA .....	19
1.2	OBJETIVO GERAL .....	20
1.3	OBJETIVO ESPECÍFICO .....	20
1.4	METODOLOGIA .....	21
1.5	ESTRUTURA DO TRABALHO .....	22
<b>2</b>	<b>TECNOLOGIA RFID</b> .....	23
2.1	SURGIMENTO E EVOLUÇÃO DA TECNOLOGIA .....	23
2.2	COMPONENTES RFID .....	25
2.2.1	<b>Tag</b> .....	26
2.2.1.1	Ativa .....	27
2.2.1.2	Passiva .....	27
2.2.1.3	Semi-Passiva .....	28
2.2.2	<b>Leitor</b> .....	29
2.2.3	<b>Antena</b> .....	31
2.3	MIDDLEWARE .....	32
2.4	RFID X SISTEMA BIOMÉTRICO .....	33
2.5	APLICAÇÕES RFID .....	37
2.5.1	<b>Área automotiva</b> .....	37
2.5.2	<b>Saúde</b> .....	38
2.5.3	<b>Controle de acesso</b> .....	39
2.6	SEGURANÇA E PRIVACIDADE .....	40
2.7	VANTAGENS E DESVANTAGENS .....	41
2.7.1	<b>Vantagens</b> .....	41
2.7.2	<b>Desvantagens</b> .....	42

<b>3</b>	<b>SISTEMAS EMBARCADOS</b> .....	43
3.1	ORIGENS DOS MICROCONTROLADORES .....	44
3.2	FABRICANTES DE MICROCONTROLADORES .....	45
3.3	APLICAÇÕES DE SISTEMAS EMBARCADOS .....	46
3.4	ARDUINO .....	47
3.5	PLACA ARDUINO UNO .....	49
<b>4</b>	<b>APLICAÇÃO DA TECNOLOGIA RFID NO CONTROLE DE ACESSO EM INSTITUIÇÕES</b> .....	51
4.1	COMPONENTES FÍSICOS DO PROTÓTIPO .....	51
4.1.1	<b>Módulo Leitor RFID MFRC522 MIFARE</b> .....	51
4.1.2	<i>Tag MF1S50yyX/V1 (MIFARE S50)</i> .....	53
4.1.3	<b>Microcontrolador</b> .....	54
4.2	AMBIENTE DE DESENVOLVIMENTO INTEGRADO.....	55
4.2.1	<b>IDE Arduino</b> .....	56
4.2.2	<b>NetBeans</b> .....	57
4.3	BANCO DE DADOS .....	58
4.4	DESENVOLVIMENTO E FUNCIONAMENTO.....	59
4.5	SOFTWARES DE CADASTRO E VALIDAÇÃO.....	60
4.6	SISTEMA WEB .....	61
<b>5</b>	<b>CONCLUSÃO</b> .....	65
5.1	DIFICULDADES ENCONTRADAS.....	65
5.2	TRABALHOS FUTUROS .....	66
	<b>REFERÊNCIAS</b> .....	67

# 1 INTRODUÇÃO

A tecnologia de identificação por radiofrequência (*Radio Frequency Identification - RFID*) vem sendo usada desde a década de 40 em diferentes tipos de aplicações, como: automobilística, saúde, controle de acesso, segurança e logística. Uma das áreas em que as vantagens do RFID são plenamente exploradas é no controle de acesso, onde o usuário utiliza *tag* RFID em formato de cartão ou chaveiro para acessar o estabelecimento de forma ágil, apresentando assim segurança aos usuários e ao próprio estabelecimento.

RFID consiste em um mecanismo para identificação automática de itens ou pessoas através de etiquetas sem a necessidade de contato (GLOVER; BHATT, 2006). A primeira aplicação dessa tecnologia ocorreu na segunda guerra mundial, onde era possível identificar aviões aliados por meio do sinal de rádio. Desde então, o recurso de identificação por radiofrequência vem recebendo novas aplicações e atualizações nos departamentos de tecnologia das grandes empresas de pesquisa e desenvolvimento (FINKENZELLER, 2000).

Este trabalho pretende demonstrar o uso de RFID para aplicações de segurança e, como esta tecnologia pode beneficiar instituições oferecendo agilidade no controle de acesso, tendo como estudo de caso o Centro Universitário do Pará (CESUPA). Esta solução pode ser usada em instituições com grande fluxo de pessoas, não restringindo-se às instituições de ensino. Importante observar que essas instituições são avaliadas em diversos fatores, haja vista que além de oferecer ensino de qualidade, há que se destacar a segurança dos estudantes, professores e funcionários. Ressalte-se ainda que é muito comum em universidades e faculdades ocorrer a livre entrada de visitantes, o que pode gerar problemas de segurança, uma vez que a identidade do visitante é desconhecida.

Para controlar esse fluxo de pessoas são implementadas diversas alternativas, como a contratação de seguranças e inspetores. Recursos tecnológicos também são utilizados, câmeras para monitoramento podem ser instaladas, assim como, catracas com sistema biométrico que buscam restringir o acesso aos prédios. O método biométrico consegue identificar usuários de maneira única, entretanto, qualquer alteração na biometria do usuário, como o uso de produtos químicos ou dedos com digitais desgastadas interfere na leitura da impressão digital, gerando falhas no sistema.

Catracas com sistema biométrico é o método de segurança e controle de acesso empregado no CESUPA na unidade da avenida Governador José Malcher. Diariamente percebe-se as limitações dessa tecnologia, pois constatou-se em observações que, alunos,

funcionários e professores precisam muitas vezes passar mais de uma vez sua digital no leitor para acessar a instituição. Essa ausência de precisão nas leituras gera filas, sinônimo de um atendimento inadequado. Em algumas unidades analisadas da instituição, o uso do sistema biométrico é caracterizado pela demora na leitura da digital, o que resulta muitas vezes no desconforto e estresse dos usuários. Além da demora na leitura, ocorrem também diversas manutenções nas catracas. Nesses casos de inatividade do sistema biométrico, algumas pessoas aproveitam para burlar o controle de acesso e adentrar na instituição sem passar a digital, com o objetivo de agilizar o processo. Essa situação pode tornar-se um risco na segurança do CESUPA, pois possibilita a entrada de pessoas desconhecidas.

Como alternativa para solucionar a problemática detectada a partir de pesquisa e observação *in loco*, este trabalho apresenta um estudo sugerindo a utilização de RFID, como melhor opção para controlar o acesso nas unidades de ensino do CESUPA, a partir de um protótipo que será detalhado no decorrer deste estudo. A tecnologia RFID é mundialmente reconhecida pela sua rapidez ao identificar e processar informações, o que motivou seu uso para a realização desta monografia.

Para que o método de identificação por radiofrequência torne-se operacional, é necessário outro recurso computacional, o sistema embarcado e, neste trabalho foi utilizado o Arduino por ser uma plataforma que possui codificação aberta (MCROBERTS, 2011). A utilização do Arduino possibilita o controle da leitura dos dados recebidos pelo módulo RFID. Para ser operante, a placa necessita de códigos desenvolvidos em um ambiente de desenvolvimento integrado (*Integrated Development Environment - IDE*).

## 1.1 JUSTIFICATIVA

Segundo notícia publicada no G1 (portal *online* da Globo), em 02/12/2016, dois homens armados conseguiram acessar uma faculdade particular no Centro de Campina Grande, Paraíba.<sup>1</sup> Conforme informações obtidas pelo Centro Integrado de Operações Policiais (CIOP), os assaltantes conseguiram o acesso à instituição devido suas vestimentas serem similares às dos alunos que frequentavam a faculdade. Ainda de acordo com a polícia, os dois conseguiram roubar cerca de R\$ 1,6 mil, além dos aparelhos celulares dos que estavam presentes no momento. Também em 19/05/2016, o mesmo portal informa que homens armados invadiram a FTC – Faculdade de Tecnologia e Ciências, em Salvador,

---

<sup>1</sup>[1.globo.com/pb/paraiba/noticia/2016/12/assaltantes-se-passam-por-alunos-e-roubam-faculdade-na-paraiba.html](http://1.globo.com/pb/paraiba/noticia/2016/12/assaltantes-se-passam-por-alunos-e-roubam-faculdade-na-paraiba.html), acessado em 11/04/2017.

Bahia. Segundo a Polícia Militar (PM), os alunos estavam na faculdade e os criminosos pegaram de surpresa os usuários em sala de aula.<sup>2</sup> Conforme se constata nos casos apontados, há evidências de que as falhas no controle de acesso a universidades e faculdades podem gerar problemas graves aos usuários, comprometendo seu patrimônio e suas vidas.

Assim sendo, visando garantir um controle de acesso eficiente e eficaz em instituições de ensino e organizações com grande fluxo de pessoas como em academias, prédios empresariais e hospitais, este trabalho tem o propósito de realizar um estudo de caso sobre o uso da tecnologia RFID na agilidade ou implementação de controle de acesso. Desta forma, a tecnologia de radiofrequência poderia atuar como aliada na redução dos eventos gerados pela ausência de segurança, que comprometem a imagem da instituição, a qualidade de vida dos usuários e a proteção do patrimônio empresarial e pessoal dos usuários.

## 1.2 OBJETIVO GERAL

Desenvolver um protótipo fundamentado na tecnologia RFID que gerencie o acesso em organizações com grande fluxo de pessoas. Esse protótipo utiliza *tags* e buscas no banco de dados para efetuar a entrada de pessoas na instituição, de modo que possibilite a visualização e análise via *web*. Assim, pode-se oferecer maior segurança e agilidade no processo de acessar o prédio, já que permite a liberação sem que haja o toque no leitor RFID pelo usuário.

Espera-se também que este trabalho contribua para os estudos de tecnologias em sistemas embarcados que utilizem RFID integrado, e para desenvolvimento de aplicações que funcionem como mediadores entre sistemas embarcados e sistemas gerenciadores de banco de dados.

## 1.3 OBJETIVO ESPECÍFICO

O objetivo deste trabalho, é controlar acessos. Para alcançar esse propósito os objetivos específicos foram divididos em quatro etapas:

- Criar um banco de dados para armazenar as informações dos usuários;

---

<sup>2</sup> <http://g1.globo.com/bahia/noticia/2016/05/homens-armados-invadem-ftc-e-assaltam-alunos-em-sala-de-aula.html>, acessado em 12/04/2017.

- Coletar a identidade das etiquetas por meio da interação do módulo RFID com o Arduino;
- Usar a linguagem Java para integrar o Arduino com o banco de dados;
- Modelar um sistema web para monitorar os acessos no CESUPA.

## 1.4 METODOLOGIA

Como metodologia foram realizadas pesquisas (Bibliográfica e Estudo de Caso) sobre as tecnologias empregadas neste trabalho. A 1ª fase da pesquisa (bibliográfica) foi realizada em livros, *e-books*, artigos, monografias, reportagens e notícias de jornais, em material impresso ou disponível na internet, onde se procurou obter embasamento teórico acerca da temática proposta.

Na 2ª fase da pesquisa constatou-se que o embasamento teórico permitiu o desenvolvimento de um sistema de controle de acesso que representa uma possível solução para o problema de segurança e de lentidão no acesso à instituição escolhida como observado no Estudo de Caso. Para a construção desse protótipo foram utilizados módulos com antena e leitor RFID para obtenção de dados da *tag*. Foram também desenvolvidos dois sistemas em linguagem Java, produzidos na IDE NetBeans, com armazenamento realizado no banco de dados MySQL, além da placa Arduino que funcionou como mediador entre partes físicas e os sistemas desenvolvidos.

A linguagem de programação Java foi escolhida por apresentar melhor integração com as funções desejadas pela equipe durante a produção dos sistemas, e por apresentar grande quantidade de material de apoio disponível e de fácil acesso.

A IDE NetBeans e o banco de dados MySQL foram escolhidos devido a familiaridade GT (Grupo de Trabalho) com o uso de tais ferramentas em experiências externas ao curso. A IDE NetBeans, em particular, teve sua escolha baseada na possibilidade apresentada de desenvolver sistema e interface homem-máquina em uma mesma plataforma.

A placa Arduino, foi escolhida devido a ampla exploração durante o curso e, assim como a linguagem Java, que possui vasto material para auxiliar a construção de códigos, tendo sido uma das escolhas para a construção do protótipo.

A 3ª e última parte da pesquisa foi marcada pelo desenvolvimento do sistema *web*, feito na linguagem *Hypertext Preprocessor* (PHP). Com o fim de realizar a busca das informações já coletadas pelo protótipo no banco de dados e exibir os dados para os

administradores. Como todo sistema *web* precisa de um servidor para ser executável, foi realizada a configuração do servidor *web* Apache HTTP Server.

## 1.5 ESTRUTURA DO TRABALHO

Além deste capítulo introdutório e das considerações finais, este trabalho está organizado do seguinte modo:

O referencial teórico encontra-se nos Capítulos 2 e 3 – “Tecnologia RFID” e “Sistemas Embarcados”, nos quais se mostra o histórico da tecnologia RFID, os componentes, *middleware*, diferenças entre código de barras e RFID, aplicações, segurança e privacidade e as vantagens e desvantagens de seu uso. Quanto ao Capítulo 3 “Sistemas Embarcados”, priorizou-se a origem dos microcontroladores, a menção aos fabricantes, as aplicações dos sistemas, com ênfase à placa Arduino Uno. Assim sendo, trabalhou-se para reconstituir a história, as características, o funcionamento e as aplicações do sistema.

O Capítulo 4 descreve a “Aplicação da tecnologia RFID no controle de acesso às instituições”, tendo como foco o detalhamento do protótipo, a caracterização dos componentes físicos, o banco de dados, a descrição do ambiente de desenvolvimento integrado, bem como o funcionamento do protótipo.

A sessão de testes comprovou que o protótipo funcionou de acordo com as expectativas, conforme apresentado na descrição das provas realizadas e nas "Considerações Finais" deste trabalho.

## 2 TECNOLOGIA RFID

Com base na problemática de segurança e comodidade no acesso às instituições, foi realizada uma pesquisa sobre as diferentes tecnologias que podem ser utilizadas para solucionar essa questão. Entre as tecnologias analisadas, o sistema RFID foi a que se mostrou mais eficiente, pois apresenta rapidez e precisão na leitura de dados, e seu custo de manutenção é considerado baixo. Esse sistema permite a identificação automática de itens para controle de acesso ágil, rastreamento de animais, controle de estoque, dentre outras aplicações.

Em casos de controle de acesso, que é o objetivo deste trabalho, podem ser utilizados, por exemplo, cartões, pulseiras ou chaveiros para restringir a entrada de pessoas autorizadas à determinadas festas, instituições, cinemas, campos de futebol, entre outros. A utilização de cartões para ingressar em estabelecimentos privados tornou-se parte da rotina de muitos usuários e, geralmente, quando alguém usufrui desse mecanismo, está utilizando a tecnologia de identificação por radiofrequência ou RFID.

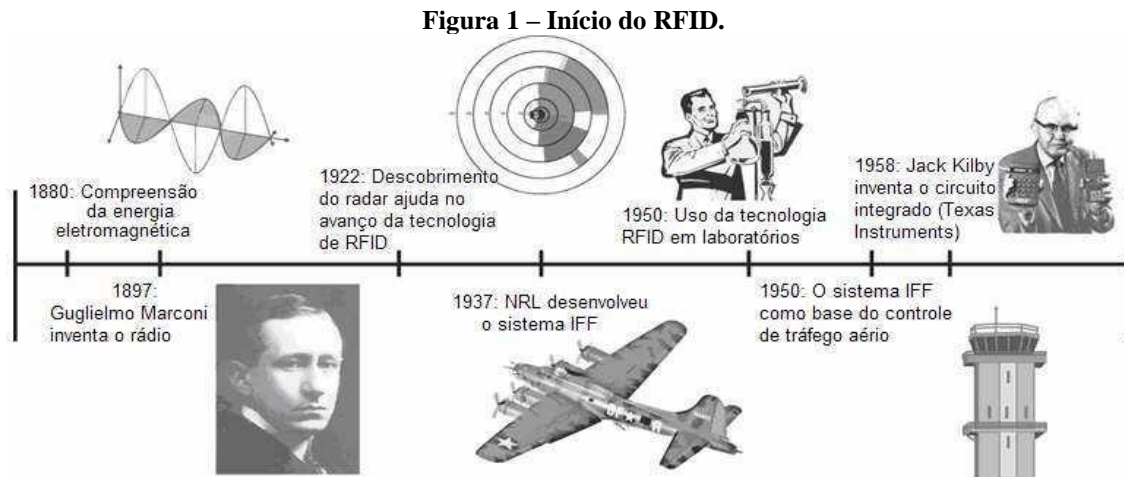
O RFID é um sistema de identificação por rádio frequência, utilizado na construção de etiquetas eletrônicas, que permitem o controle de produtos em lojas, de estoques, validade de produtos, localização de equipamentos, entre outros. Pode possuir área de cobertura limitada, mas com excelente rastreabilidade (CUNHA, 2006, p. 20).

Para muitos especialistas, a tecnologia RFID tende a ser a melhor opção de uso entre outros sistemas já existentes no mercado que utilizam identificação por ondas eletromagnéticas, como o código de barras. O que muitos desconhecem, é que essa tecnologia não é nova e sua aplicação foi registrada ainda na Segunda Guerra Mundial para detectar aviões por meio das ondas de rádio (BERNARDO, 2004; VIOLINO, 2005).

### 2.1 SURGIMENTO E EVOLUÇÃO DA TECNOLOGIA

A história do RFID tem seu início em 1922 quando o escocês *Sir* Robert Alexander Watson Watt inventou a Detecção e Telemetria por Rádio ou como é comumente conhecido, radar (*Radio Detection and Rangig* – RADAR). Este dispositivo realiza a localização de objetos que emitem sinais por meio de ondas eletromagnéticas e, já na Segunda Guerra Mundial, era utilizado para a identificação de aviões inimigos ou amigos a partir do sinal de rádio. É dessa forma que a invenção do Radar contribuiu para o avanço da tecnologia RFID,

conforme mostra a Figura 1. Também são apontadas algumas datas marcantes do início da tecnologia, como a utilização da identificação por radiofrequência no controle de tráfego aéreo britânico. (BHUARTANI; MORADPOUR, 2005; VIOLINO, 2005; SANTOS, 2017).



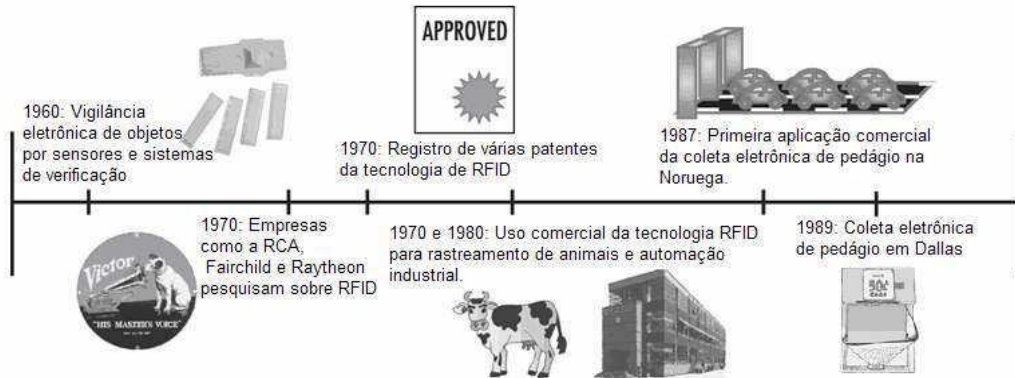
Fonte: Bhuptani e Moradpour (2005, p. 40).

O VIOLINO (2005) afirma que os primeiros sistemas RFID foram desenvolvidos pelos alemães e britânicos, onde:

- Sistema Alemão: Os alemães descobriram que se seus aviões realizassem um giro antes de chegar à base, este enviaria um sinal diferente de rádio ao radar. Dessa forma, seria possível a identificação de um avião aliado. Este método de identificação ficou conhecido como sistema passivo de RFID;
- Sistema Britânico: Chamado de Identificação de Amigo ou Inimigo (*Identify Friend Or Foe – IFF*) e sob o comando de *Sir Robert*, essa aplicação consistiu na implementação de transponders nos aviões britânicos que, ao receberem o sinal emitido pelo radar da base, emitiam um sinal de resposta diferente, que o identificavam como avião amigo. Posteriormente este sistema ficou conhecido como sistema ativo de RFID, justamente pela utilização de transponders.

Como ilustra a Figura 2, que aponta avanços na utilização da tecnologia RFID até os anos 90, foi só em 1973 que Mario W. Cardullo e Charles Walton receberam as primeiras patentes para um sistema ativo e passivo de RFID, respectivamente. Ainda na década de 70, o governo norte-americano realizava projetos para o rastreamento de materiais radioativos e de gado (BHUARTANI; MORADPOUR, 2005; 2º CONGRESSO BRASILEIRO DE RFID E INTERNET DAS COISAS, 2011).

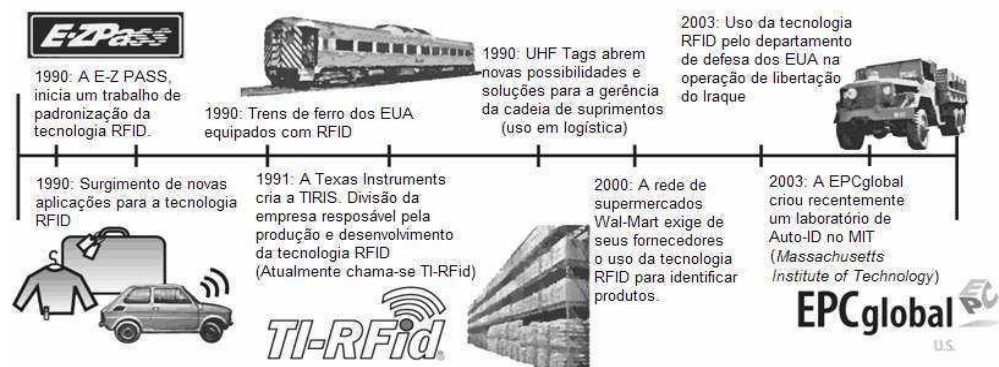
**Figura 2 – RFID durante os anos 60 a 90.**



Fonte: Bhuptani e Moradpour (2005, p. 42).

Desde então, o RFID alcançou vários adeptos ao redor do mundo, reduziu o custo de sua implementação e aumentou sua aplicabilidade em outros setores industriais. Dessa forma, o que antes era monopolizado por grandes empresas e militares, passou a ser acessível e ter um alcance mundial, fazendo com que autoridades governamentais e não-governamentais passassem a investir para estabelecer algum tipo de padronização na frequência de operação, conforme mostra a Figura 3. Sendo assim, essa tecnologia sofreu diversas evoluções em seu sistema e componentes (OLIVEIRA; PEREIRA, 2006).

**Figura 3 – RFID dos anos 90 aos dias atuais.**



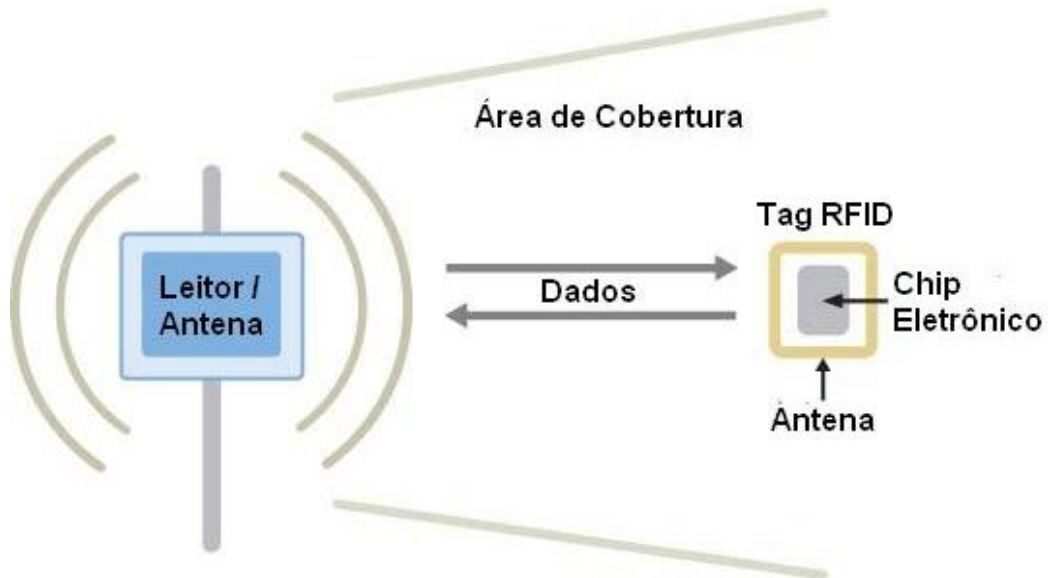
Fonte: Bhuptani e Moradpour (2005, p. 44).

## 2.2 COMPONENTES RFID

O sistema básico do RFID é composto por três componentes: *tag*, leitor e antena. Tais componentes trabalham juntos da seguinte forma: a antena, quando conectado ao leitor, emite um sinal de radiofrequência dentro de uma determinada área de cobertura solicitando informações para o leitor. Esses dados, geralmente, estão presentes em *tags*, que apresentam

em sua memória interna informações que serão enviadas ao leitor, conforme ilustra Figura 4 (LIMA JUNIOR, 2006; CARVALHO JUNIOR, 2008).

**Figura 4 – Funcionamento básico do sistema RFID.**

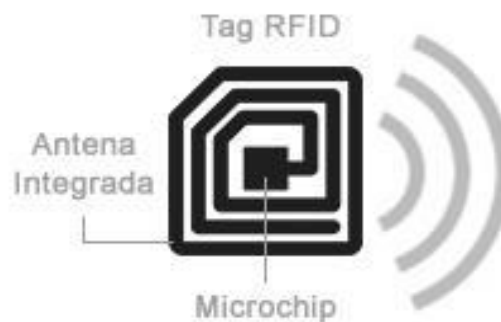


Fonte: Adaptado de RFIDBr – Portal Brasileiro sobre RFID (2011, online).

### 2.2.1 Tag

É o componente que armazena dados para transmitir e responder ondas de radiofrequência emitidas pelo leitor. Conforme ilustra a Figura 5, essas *tags* são compostas por um *chip* de silício, antena e, dependendo da *tag*, de uma bateria. Seus tamanhos variam de acordo com os tipos ativas, passivas e semi-passivas. (REVISTA INTRALOGISTICA, 2010; QUEIROZ; ARAÚJO; HORTA, 2014).

**Figura 5 – Tag do sistema RFID.**



Fonte: AfixCode (2014, online).

### 2.2.1.1 Ativa

Maiores e mais resistentes, a *tag* ativa, conforme ilustra a Figura 6, apresenta dois componentes específicos em sua composição: bateria e um circuito transmissor.

- Bateria: responsável por energizar o circuito da *tag*, este componente permite a etiqueta iniciar a comunicação com o leitor sem precisar de um sinal eletromagnético para ativação;
- Circuito Transmissor: permite a *tag* realizar uma operação em alcance maior (CARVALHO JUNIOR, 2008; QUEIROZ; ARAÚJO; HORTA, 2014).

Figura 6 – Exemplo de *tag* ativa.



Fonte: Smiley (2016, online).

LIMA JUNIOR (2006) afirma que os primeiros sistemas RFID utilizavam as *tags* ativas. Já nos dias de hoje, são usadas somente quando as *tags* passivas não conseguem atender as necessidades da aplicação desejada. Além disso, algumas características dos sistemas ativos de RFID são pontuadas, tais como:

- Capacidade de utilização de sensores pelas *tags*;
- Alta velocidade de resposta;
- Tempo de vida útil definido.

### 2.2.1.2 Passiva

As *tags* passivas, conforme mostra a Figura 7, consistem nas etiquetas que não apresentam alimentação interna. Diferentemente das etiquetas ativas, a energização das *tags* passivas são feitas através da indução magnética, em outras palavras, esse tipo de etiqueta necessita apenas do campo magnético emitido pelo leitor para realizar sua função (CUNHA, 2006; LIMA JUNIOR, 2006).

**Figura 7 – Exemplo de *tag* passiva.**



Fonte: Smiley (2016, online).

O funcionamento do sistema passivo de RFID segue alguns passos:

- A antena da *tag* recebe o sinal do leitor;
- A antena transmite o sinal recebido para o circuito integrado (CI) da *tag*;
- Parte da energia eletromagnética recebida do leitor é transferida para o funcionamento do CI;
- O CI recebe o sinal e envia uma resposta para o leitor (CARVALHO JUNIOR, 2008).

Atualmente as *tags* passivas possuem maior visibilidade por apresentarem alguns fatores favoráveis, como: vida útil e, principalmente, custo reduzido. Dessa forma, o sistema passivo de RFID é o mais utilizado em aplicações como a automação industrial, monitoramento de produtos e controle de acesso (LIMA JUNIOR, 2006; QUEIROZ; ARAÚJO; HORTA, 2014).

### 2.2.1.3 Semi-Passiva

Considerada como intermediária entre as *tags* ativas e passivas, as semi-passivas, como mostra a Figura 8, apresentam bateria própria que, além de permitir a aplicação da *tag* com antenas que emitem baixa intensidade de campo magnético, permite o funcionamento dela sem grandes interferências externas. No entanto, as *tags* semi-passivas servem somente para receber dados e não são capazes de gerar um novo sinal de radiofrequência (CUNHA, 2006; GOMES, 2007).

**Figura 8 – Exemplo de tag semi-passiva.**



Fonte: Smiley (2016, online).

CARVALHO JUNIOR (2008) apresenta uma comparação entre as tags passivas, semi-passivas e ativas, conforme mostra a Tabela 1.

**Tabela 1 – Comparação entre as tags.**

<b>CARACTERÍSTICAS DA TAG</b>	<b>PASSIVO</b>	<b>SEMI-PASSIVO</b>	<b>ATIVO</b>
<b>FONTE DE ENERGIA</b>	Recebe a energia do leitor.	Bateria Interna.	Bateria Interna.
<b>COMUNICAÇÃO</b>	Comunicação iniciada somente pelo leitor.	Comunicação iniciada somente pelo leitor.	Iniciada tanto pelo leitor quanto pela tag.
<b>TAMANHO</b>	Pequena.	Média.	Grande.
<b>ALCANCE</b>	Curto.	Médio.	Grande.
<b>TIPO DE MEMÓRIA</b>	Leitura; Escrita somente uma vez; Escrita/Leitura.	Leitura; Escrita somente uma vez; Escrita/Leitura.	Leitura; Escrita somente uma vez; Escrita/Leitura.
<b>CAPACIDADE DE MEMÓRIA</b>	Variam de 128bits a 64KB.	Até de 8MB.	Mais de 8MB.
<b>CUSTO</b>	Baixo.	Intermediário.	Caro.

Fonte: Adaptado de Carvalho Junior (2008, p. 28).

### 2.2.2 Leitor

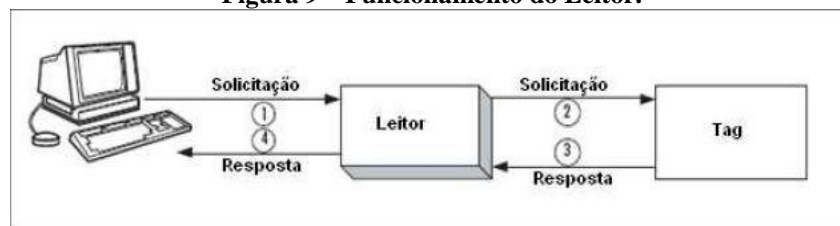
Também chamado de interrogador, o leitor é o componente do sistema RFID responsável pela captura e processo dos dados contidos nas tags. É ele que realiza essa comunicação com as tags por meio de uma antena que emite sinais de radiofrequência. Tais comunicações variam conforme o tipo de leitor:

- O leitor que faz somente a leitura é utilizado junto com as *tags* passivas, sendo responsável por receber os dados das etiquetas energizadas;
- O leitor que é capaz de realizar leitura e escrita é utilizado com os dois tipos de etiquetas, pois pode receber e enviar dados (BHUPTANI; MORADPOUR, 2005; QUEIROZ; ARAÚJO; HORTA, 2014).

Responsável pela conexão entre o computador e as *tags*, o funcionamento do leitor para coletar dados das *tags* pode ser explicado em quatro passos, conforme ilustra Figura 9:

- I. O computador solicita uma informação ao leitor;
- II. O leitor envia a solicitação de tal informação para as *tags* que estão na zona de leitura;
- III. As *tags* respondem as informações solicitadas pelo leitor;
- IV. O leitor recebe as informações e as transfere ao computador (CARVALHO JUNIOR, 2008).

**Figura 9 – Funcionamento do Leitor.**



Fonte: Carvalho Junior (2008, p. 31).

De acordo com GRUCHINSKI (2007), o tempo para realizar essa sequência de instruções equivale a um décimo de segundo, ou seja, todas as etiquetas que passarem pelo campo de leitura serão lidas, gravadas e decodificadas pelo leitor, em tempo real.

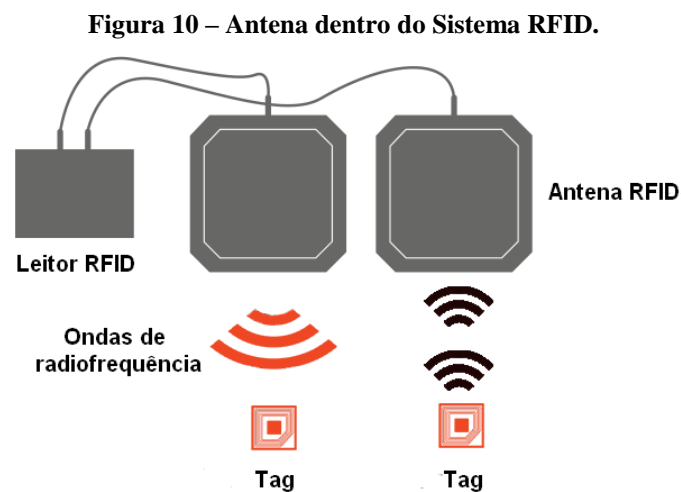
A escolha do leitor deve ser analisada de acordo com o tipo, que é designado por meio de sua mobilidade. Esta decisão deve ser feita com base na aplicação que será implementada. Os tipos de leitores são:

- Fixo: Os leitores fixos alcançam as maiores distâncias em termos de leitura por apresentarem um desempenho otimizado se comparado com o sinal de radiofrequência que emite. Estes tipos, também são capazes de realizar uma conexão direta com uma rede de computadores ou com um microcomputador através de suas interfaces;

- Móveis: Por apresentar um campo de leitura menor que os leitores fixos, os leitores móveis necessitam estar próximos da *tag* para fazer a leitura. Este tipo de leitor utiliza as baterias dos equipamentos que está conectado, pois não apresenta uma boa fonte de alimentação interna;
- Embarcado: O leitor embarcado é a mais nova tendência do mercado, especialmente na área da logística. O maior objetivo dos setores que usam este tipo de leitor, é em relação a junção das funcionalidades dos equipamentos que realizam as movimentações de cargas nos depósitos, portos ou centros de distribuições (LIMA JUNIOR, 2006; CARVALHO JUNIOR, 2008).

### 2.2.3 Antena

Por serem a base da comunicação sem fio, as antenas apresentam um papel fundamental na área de telecomunicações e, conseqüentemente, dentro do sistema RFID. Sendo um componente importante na identificação por radiofrequência, é função da antena emitir e transformar a energia irradiada ou guiada durante uma comunicação entre a *tag* e o leitor, conforme ilustra a Figura 10 (NARCISO, 2008; QUEIROZ; ARAÚJO; HORTA, 2014).



Fonte: Smiley (2014, online).

Como as *tags* e os leitores apresentam quatro faixas de frequência distintas, a antena deve ser escolhida de forma que seja compatível com a mesma frequência utilizada no sistema elaborado. As faixas mais comuns utilizadas pelo sistema RFID e a frequência em que operam são:

- Baixa Frequência (*Low Frequency* – LF): 125 KHz – 134 KHz ou menos;
- Alta Frequência (*High Frequency* – HF): 13,56 MHz;
- Ultra Alta Frequência (*Ultra High Frequency* – UHF): 860 MHz – 930 MHz;
- Microondas: 2,45 GHz (CARVALHO JUNIOR, 2008).

Por ainda não apresentarem uma padronização definida, o sistema RFID acaba sendo regulamentado como dispositivo de rádio. Dessa forma, para as faixas LF, HF e Microondas, formou-se um padrão mundial de frequência a ser utilizado. Já no caso da UHF, por ser considerada uma faixa nova e ainda não apresentar um padrão, cada país adota sua própria padronização. Na Tabela 2 é mostrada as faixas de frequência utilizada por alguns países (CARVALHO JUNIOR, 2008; LOPES et al., 2009).

**Tabela 2 – Faixas de frequência utilizada em alguns países.**

PAÍSES	LF	HF	UHF	MICROONDAS
USA	125, 134 kHz	13,56 MHz	902-928 MHz	2,40-2,48 GHz; 5,72-5,85 GHz
EUROPA	125, 134 kHz	13,56 MHz	868-870 MHz	2,45 GHz
CHINA	125, 134 kHz	13,56 MHz	N/A	N/A
ÍNDIA	125, 134 kHz	N/A	865-867 MHz	2,40 GHz
JAPÃO	125, 134 kHz	13,56 MHz	950-956 MHz	2,45 GHz
CINGAPURA	125, 134 kHz	13,56 MHz	923-925 MHz	2,45 GHz

Fonte: Carvalho Junior (2008, p. 34).

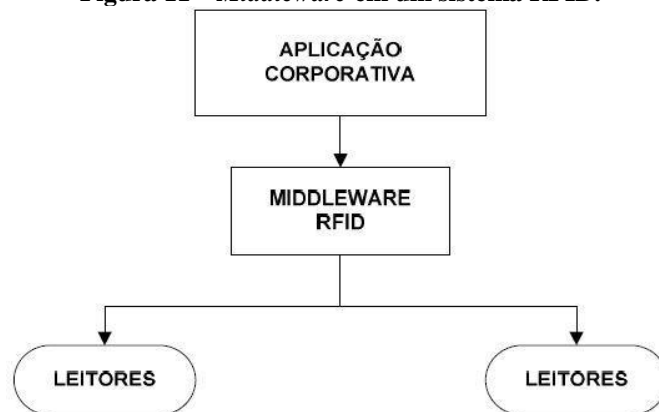
### 2.3 MIDDLEWARE

Para que o sistema RFID torne-se útil, é necessária uma camada intermediária capaz de receber, organizar e processar as informações coletadas pelo leitor. Essa camada responsável pela análise e interpretação dos dados é um sistema de *software*, chamada comumente de *middleware*. (DRESCH JR; EFROM; GRUMOVSKI, 2008).

O *middleware* é o elo entre os dados contidos nas etiquetas e o sistema que necessita desses dados. É ele que recebe, seleciona e altera as informações significativas coletadas das *tags*, deixando-as legíveis para a aplicação (NARCISO, 2008; REVISTA INTRALOGISTICA, 2010).

Em termos de mercado, LOPES et al. (2009) afirma que seria difícil os desenvolvedores de sistemas RFID criarem um *middleware* que abrangesse todo os tipos de leitores disponíveis no mercado. Por este motivo, os *middleware* são introduzidos no sistema posteriormente, entre os leitores e as aplicações necessárias, conforme mostra Figura 11.

**Figura 11 – Middleware em um sistema RFID.**



Fonte: Lopes et. al (2009, p. 25).

## 2.4 RFID X SISTEMA BIOMÉTRICO

Como já explicado no trabalho, o RFID utiliza ondas de rádio para identificação de objetos ou seres vivos portadores de *tags* que pertencem ao sistema. Dessa forma, este se inclui em uma categoria de tecnologias conhecida como identificação automática que, como o próprio nome sugere, é composta por toda tecnologia que identifica itens automaticamente, como o código de barras, os leitores ópticos e o reconhecimento biométrico (LIMA JUNIOR, 2006; LOPES et al., 2009).

Das tecnologias que realizam a identificação automática, o sistema biométrico é a tecnologia utilizada para controlar o acesso no CESUPA. Para tanto, foram selecionadas algumas empresas afim de realizar uma comparação entre seus produtos que utilizam do RFID e da biometria como método de monitoramento de acesso em estabelecimentos com grande fluxo de pessoas. Tais empresas e seus produtos são:

- Computer ID® e CIS®

A Computer ID® é uma empresa que apresenta um foco em produtos e soluções com biometria. No entanto, em uma das suas principais linhas de produtos, a linha Futronic, já disponibiliza equipamentos que utilizam mutuamente do sistema biométrico e do sistema RFID, como o *Scanner FS25*

com cartão Mifare, conforme é mostrado na Figura 12 (COMPUTER ID, 2017).

**Figura 12 – Scanner FS25 com cartão Mifare**



Fonte: Computer ID (2017, online).

Ainda de acordo com a referência previamente citada, este equipamento tem como objetivo realizar a autenticação de dois fatores, na qual é associada a digital do usuário junto com os dados contidos no cartão Mifare que, nada mais é do que um cartão que utiliza da tecnologia RFID. Dessa forma, a vantagem deste equipamento é que ele disponibiliza uma solução para casos em que o armazenamento da digital venha a infringir a privacidade dos usuários.

“O FS25 é a solução para este problema, pois ele pode identificar um indivíduo usando impressão digital sem o armazenamento de dados de impressões digitais no sistema e sim no cartão que ele possui.” (COMPUTER ID, 2017, online).

Atualmente, a CIS®, que é uma empresa especializada em produtos de automação bancária e comercial, também fornece produtos biométricos da linha Futronic (CIS, 2017);

- **Kimaldi®**

A Kimaldi® é uma empresa que atua na venda de produtos destinados na identificação de pessoas para diversos setores comerciais onde, diferentemente da CIS® e da Computer ID®, apresenta produtos baseados tanto no sistema RFID quanto no sistema biométrico (KIMALDI, 2016).

Ainda de acordo com a Kimaldi (2016), seu principal produto, desenvolvido pela própria empresa, o Kimaldi Flexy, conforme ilustra Figura 13, utiliza de ambas tecnologias para realizar o controle de acesso. No entanto, neste equipamento, as tecnologias não trabalham de forma simultânea. Deixando para o usuário a escolha da forma mais adequada para a aplicação desejada.

**Figura 13 – Kimaldi Flexy.**



Fonte: Kimaldi (2016, online).

- Henry®

Por fim, uma das empresas analisadas foi a Henry®, que é a empresa fornecedora das catracas que realizam o controle de acesso no CESUPA. A Henry® é uma das empresas referência no mercado de controle de ponto e acesso, disponibilizando produtos que utilizam do sistema RFID, da biometria e do código de barras (HENRY, 2017).

Um dos seus produtos de destaque é a Lumen Advance, conforme mostra a Figura 14, na qual pode ser operada nas três tecnologias que realizam a identificação automática. Em nosso estudo de caso, esse equipamento é utilizado somente com o sistema biométrico.

Figura 14 – Lumen Advance.



Fonte: Adaptado de Dataponto (2017, online).

Dessa forma, analisando o cotidiano do CESUPA, informações sobre a catraca utilizada na instituição e os estudos sobre a tecnologia RFID, destacamos algumas vantagens do sistema de identificação por radiofrequência para o sistema biométrico, tais como:

- Precisão

Pela utilização das ondas de radiofrequência para a identificação das *tags*, o RFID se torna mais eficiente ao identificar a identidade das etiquetas que apresentam os usuários;

- Agilidade

Devido a precisão na identificação dos dados contidos nas *tags*, a liberação no acesso do usuário a instituição é realizada de forma mais ágil ao comparada com a leitura da biometria, levando em consideração o grande fluxo de pessoas;

- Manutenção

O tempo de manutenção das catracas que utilizam RFID é menor do que nas catracas que utilizam da biometria, o que implica em um menor custo para a manutenção e diminuição nos períodos de inatividade das catracas;

- Limitações de usuários

O RFID, por necessitar apenas da identificação da *tag*, pode apresentar um número ilimitado para o cadastro de usuários no banco de dados. Enquanto que, em equipamentos biométricos, como o utilizado no CESUPA, é disponibilizado o gerenciamento com eficiência para apenas 15.000 usuários (LIMA JUNIOR, 2006; HENRY, 2017).

## 2.5 APLICAÇÕES RFID

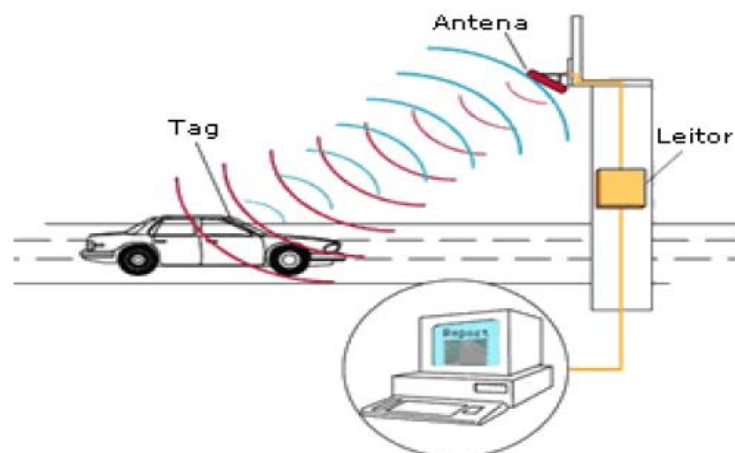
Com o crescimento na utilização da tecnologia RFID, especialistas na área afirmam que as etiquetas inteligentes, cedo ou tarde, estarão presentes em produtos de diversos setores, como em sistemas de rastreamento, gerenciamento, identificação, pedágios, antifurto, acesso, entre outros (BERNARDO, 2004). Nas subseções seguintes, serão exemplificadas algumas áreas que usufruem da aplicação do RFID.

### 2.5.1 Área automotiva

Em termos automotivos, duas grandes aplicações envolvendo o sistema RFID destacam-se. São elas:

- Sistema Antifurto: Consiste na aplicação das *tags* em chaveiros ou na parte plástica da chave. Dessa forma, o veículo só consegue dar partida quando a chave é inserida no contato e a *tag* acoplada na chave envia um código ao leitor que, por sua vez, encaminha tal código a um sistema que o irá reconhecer e permitirá que o carro dê a partida;
- Pedágios: Este tipo de aplicação consiste na implementação de etiquetas no para-brisa de veículos e antenas nas cabines de cobrança, conforme mostra Figura 15. Assim, as antenas ao reconhecerem as etiquetas autorizadas liberam a passagem do veículo (OLIVEIRA; PEREIRA, 2006; NARCISO, 2008; LAZARO; NASCIMENTO, 2011).

Figura 15 – Aplicação do sistema RFID em pedágios.



Fonte: Lazaro e Nascimento (2011, p. 7).

Um grande exemplo de aplicações do RFID dentro do setor automotivo no Brasil é em pedágios, com o Sem Parar. Projeto que teve início em São Paulo e atualmente já expandiu para outros estados, o Sem Parar é um sistema de pagamento eletrônico que utiliza da tecnologia RFID e permite ao usuário passar em pedágios sem a necessidade de manusear em dinheiro ou cartão de crédito para efetuar o pagamento. Recentemente, alguns estacionamentos de *shoppings* também aderiram ao Sem Parar, uma vez que todas as despesas viriam em fatura única (LEWGOY, 2017).

## 2.5.2 Saúde

Na área da saúde, a aplicação do sistema RFID de mais destaque mundial, consiste na implementação de pequenos *chips* sob a pele de pessoas, conforme ilustra a Figura 16. Nesses *chips* constam informações de pacientes, como seu tipo sanguíneo e os detalhes de sua condição de saúde. Basicamente, todos os dados de registros e saúde dos pacientes poderiam ser acessados pela leitura das informações contidas na etiqueta (OLIVEIRA; PEREIRA, 2006; NARCISO, 2008).

**Figura 16 – Pequeno *chip* RFID utilizado na área da saúde.**



Fonte: Narciso (2008, p. 55).

Ainda segundo os autores previamente citados, este tipo de aplicação RFID ainda gera bastante divergências e discussões de opiniões entre instituições acadêmicas, autoridades governamentais e não governamentais, pois nem todos os países aceitam este tipo de implementação. Atualmente, esses tipos de *chips* são aplicados em pacientes que apresentam cuidados especiais, como portadores da doença de *Alzheimer*, diabetes, entre outras doenças que necessitam de um tratamento complexo.

TOMAZ (2009) afirma que o sistema RFID também pode ser utilizado na área da saúde como forma de pulseira, conforme mostra a Figura 17. Dessa forma, pacientes, remédios e equipamentos seriam etiquetados para auxiliar na administração do hospital, contribuindo no aumento da segurança e na diminuição de erros.

**Figura 17 – Pulseiras que utilizam a tecnologia RFID na área da saúde.**



Fonte: Tomaz (2009, p. 3).

### **2.5.3 Controle de acesso**

O uso da identificação por radiofrequência no controle de acesso é uma das suas aplicações mais utilizadas no mundo. Como o próprio nome sugere, consiste na permissão do acesso de pessoas autorizadas em locais privados e, por utilizar banco de dados para o armazenamento das informações dos usuários, podem ser aplicadas em diversos setores, como edifícios comerciais, eventos, instalações, sala de controles, cofres de bancos, instituições de ensino, entre outros (OLIVEIRA; PEREIRA, 2006; CARVALHO JUNIOR, 2008).

A exemplo do uso do RFID na área da saúde, uma das aplicações no controle de acesso consiste no implante de *chips* no corpo humano. Já este com o intuito de identificação de fraudes, dando maior segurança em acessos a locais privados e, se combinado com alguns outros sensores, tais *chips* podem analisar as condições de medo e *stress* da pessoa, realizando até mesmo o armazenamento de tais informações, por exemplo (OLIVEIRA; PEREIRA, 2006; LAZARO; NASCIMENTO, 2011).

Outro modo de aplicação utiliza apenas de *tags* como chaveiros, cartões ou pulseiras para permissão de acesso em locais como instituições de ensino, cinemas, estádios de futebol,

etc. A utilização deste tipo de etiquetas pode aumentar a rapidez e segurança no acesso das pessoas nesses locais. Este tipo de aplicação é a ideia base para a implementação do projeto realizado neste trabalho (LAZARO; NASCIMENTO, 2011; MARTINS NETO; RODRIGUES, 2016).

## 2.6 SEGURANÇA E PRIVACIDADE

Assim como nas redes de computadores, os sistemas RFID têm como um dos objetivos armazenar e proteger dados de usuário que, muitas vezes, estão expostos em termos de segurança e privacidade. Mesmo explicados de forma indistintas por muitos autores, é necessário entender que existe uma distinção entre a violação de segurança e a violação de privacidade:

- Violação de segurança: São as violações que giram em torno da vulnerabilidade e proteção de dados confidenciais quanto ao acesso e manipulação não autorizada;
- Violação de privacidade: Os problemas de privacidade consistem no mal-uso de dados de terceiros por usuários autorizados, levando à violação e invasão da privacidade de uma pessoa ou empresa (BHUARTANI; MORADPOUR, 2005; ANDRELO JUNIOR, 2007).

Dessa forma, devido à evolução na utilização do sistema RFID em áreas que exigem alto nível de segurança, a tecnologia de radiofrequência pede cada vez mais um processo eficaz na segurança e privacidade dos dados de pessoas ou empresas (ANDRELO JUNIOR, 2007).

Observamos que embora as preocupações com privacidade *individual* sejam mais frequentemente discutidas e debatidas publicamente, as *empresas* também se preocupam com as violações da segurança que resultam em acesso não autorizado e possível manipulação dos dados corporativos privados ou confidenciais (BHUARTANI; MORADPOUR, 2005, p. 167).

MOTA (2006) mostra que existem alguns problemas específicos e corriqueiros dentro do sistema RFID, como os físicos, de plágio, interceptação de dados, negação de serviço e privacidade de localização, conforme mostra Tabela 3. Cada problema funciona de forma

distinta e, na grande maioria, podem ser resolvidos com esquemas de autenticação, de segurança físicas ou de pessoas, por exemplo.

**Tabela 3 – Problemas de segurança envolvendo o sistema RFID.**

<b>TIPO</b>	<b>COMO FUNCIONA</b>	<b>ABORDAGEM</b>
<b>FÍSICO</b>	O intruso pode realizar ataques físicos às <i>tags</i> .	Esquemas de segurança física de objetos, como contratação de seguranças, sistemas de câmeras, etc.
<b>PLÁGIO OU FALSIFICAÇÃO (FABRICAÇÃO)</b>	O intruso pode realizar consultas às <i>tags</i> e responder consultas a leitores legítimos.	Sistemas de autenticação para o controle de acesso.
<b>INTERCEPTAÇÃO (E MODIFICAÇÃO)</b>	O intruso captura os quadros que trafegam no ar, também chamado de espionagem.	Criptografar os dados que são enviados entre o leitor e <i>tag</i> .
<b>NEGAÇÃO DE SERVIÇO (INTERRUPÇÃO)</b>	O intruso atrapalha as difusões interferindo nos sinais de radiofrequência.	Muito difícil de serem evitados e por isso são bastante danosos.
<b>PRIVACIDADE DE LOCALIZAÇÃO (RASTREAMENTO)</b>	O intruso faz leituras nas <i>tags</i> que o usuário carrega podendo rastrear a localização do usuário.	Sistemas de autenticação para o controle de acesso.

Fonte: Mota (2006, p. 26).

## 2.7 VANTAGENS E DESVANTAGENS

Como toda tecnologia, o sistema RFID apresenta alguns benefícios e limitações quanto a sua utilização, como o custo elevado de alguns componentes e a durabilidade das etiquetas. Dessa forma, algumas vantagens e desvantagens serão pontuadas neste tópico (OLIVEIRA; PEREIRA, 2006; QUEIROZ; ARAÚJO; HORTA, 2014).

### 2.7.1 Vantagens

- Capacidade de armazenamento, leitura e envio de dados para *tags* ativas;
- Detecção sem necessidade do contato com a leitora para o reconhecimento dos dados;

- Alta vida útil da *tag*, com possibilidade de reutilização;
- Elevado grau de controle e fiscalização;
- Contagem de estoque instantânea;
- Precisão nas informações coletadas;
- Prevenção de roubos e falsificação de produtos;
- Coleta de dados de animais presentes no campo;
- Encapsulamentos especiais para *tags* que são usadas com materiais metálicos afim de contornar o problema de alcance de transmissão;
- Operação segura em ambientes úmidos, molhados, sujos, corrosivos, de altas e baixas temperaturas, com vibração ou choque;
- Etiquetas de vários formatos e tamanhos (BERNARDO, 2004; ANDRELO JUNIOR, 2007; GRUCHINSKI, 2007; CARVALHO JUNIOR, 2008; LAZARO; NASCIMENTO, 2011).

### 2.7.2 Desvantagens

- Custo elevado dos componentes se comparado a outros meios de identificação;
- Interferências eletromagnéticas;
- Uso do sistema com materiais metálicos que podem afetar o alcance de transmissão;
- A ausência de padronização das frequências para que os produtos possam ser lidos pela indústria de maneira uniforme;
- Conflitos causados pela transmissão simultânea de informações de várias *tags*;
- Posição da antena para a recepção do sinal da *tag*;
- Riscos quanto à segurança dos dados que trafegam entre os componentes do sistema RFID;
- Alcance das antenas dependendo da frequência utilizada pelos componentes;
- Invasão da privacidade de consumidores por conta da monitoração das etiquetas colocadas nos produtos (BERNARDO, 2004; PRADO; PEREIRA; POLITANO, 2006; GRUCHINSKI, 2007; CARVALHO JUNIOR, 2008; LAZARO; NASCIMENTO, 2011).

### 3 SISTEMAS EMBARCADOS

No mundo atual as pessoas estão fortemente dependentes da tecnologia, desde o uso de computadores pessoais a aparelhos eletrodomésticos como geladeira, fogão, TV e máquina de lavar roupa. Já se fala em um mundo totalmente conectado, onde cada indivíduo não consegue viver sem seu *smartphone*, *tablet* ou *laptop*, em outras palavras, sem a tecnologia.

Para que alguns eletrodomésticos mais sofisticados em termos de tecnologia computacional possam ser usados, é indispensável um sistema inteligente de controle para gerenciar todos os periféricos que são vitais para a interação do equipamento com o meio ambiente. Sendo assim, é necessária uma unidade de processamento de dados e memória para armazenar informações de forma temporária ou permanente.

O micro-ondas, por exemplo, precisa de um sistema para gerenciar as funções de aquecer o alimento no tempo exato escolhido pelo usuário da forma mais eficiente possível. Assim, dentro do micro-ondas há um programa embutido dentro de um microcontrolador. Processo este que é denominado de sistema embarcado.

Um Sistema Embarcado (ou Sistema Embutido) é um sistema microprocessado no qual a unidade de processamento (CPU) é completamente dedicada ao dispositivo ou sistema que ele controla. Diferente de computadores de propósito geral, como um computador pessoal ou notebook, um sistema embarcado realiza um conjunto de tarefas predefinidas, geralmente com requisitos bem especificados. (OLIVEIRA JUNIOR; DUARTE, 2010, p. 09).

De acordo com Taurion (2005), a limitação do uso de sistemas embarcados em equipamentos do cotidiano ou de nível industrial é somente a criatividade e, para o funcionamento desses sistemas, é necessário desenvolver linhas de código geralmente escritas em linguagens de programação estruturadas como a linguagem C, já que a maioria dos softwares não adota conceitos como orientação a objetos. As linguagens utilizadas para o desenvolvimento dos sistemas embarcados podem ser observadas na Tabela 4.

**Tabela 4 – Uso das linguagens de programação em sistemas embarcados.**

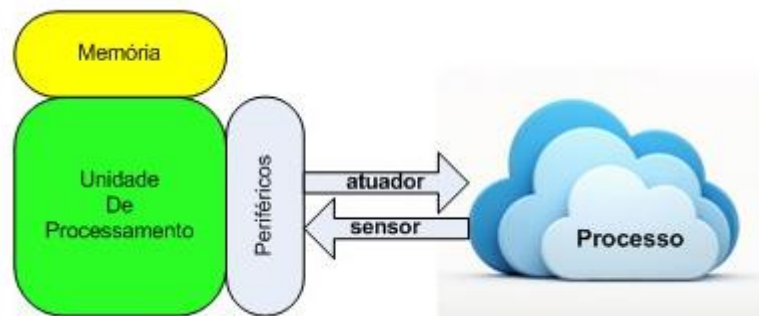
LINGUAGEM	USO (%)
C	51
C++	30
ASSEMBLY	8
JAVA	3
BASIC	1
UML, MATLAB OU OUTRA LINGUAGEM DE MODELAGEM	3
LAB VIEW	2
OUTRAS	5

Fonte: Freitas (2013, p. 35).

O desenvolvimento de sistemas embarcados é projetado principalmente utilizando microcontroladores. Segundo Watanabe (2011), microcontroladores são circuitos digitais programáveis compostos de um microprocessador, memórias e periféricos de entrada e saída, acoplados em um único *chip*. São usados para aplicações na engenharia e na solução de problemas específicos.

O sistema embarcado é composto por unidade de processamento, memória e periféricos, sendo que esses periféricos realizam a interação com o ambiente através de sensores e atuadores, representado na Figura 18. Além do hardware há também o software gravado dentro do microcontrolador.

**Figura 18 – Componentes do sistema embarcado.**



Fonte: Delai (2013, p. 3).

### 3.1 ORIGENS DOS MICROCONTROLADORES

Para que a origem dos microcontroladores possa ser compreendida, será apresentada uma breve abordagem sobre microprocessador.

O microprocessador surgiu em um projeto realizado no ano 1969, por uma empresa japonesa chamada BUSICOM, para a criação de um *chip* que foi implementado em calculadoras eletrônicas. A empresa, naquele momento, encaminhou para os Estados Unidos uma equipe de engenheiros japoneses à procura de Marcian Hoff, representante da Intel®, que possuía uma ampla experiência em computadores e observou que esse projeto poderia ser extremamente valioso. Então, teve a ideia de desenvolver um *chip* que não só realizasse as funções de calculadoras eletrônicas, mas também pudesse realizar qualquer outra operação e que funcionasse em qualquer equipamento, modificando apenas a programação interna (MATIC, 2010).

Em 1971, dois engenheiros da Texas Instruments® desenvolveram o microcontrolador, tornando realidade a ideia de Marcian Hoff em relação ao

microprocessador solicitado pela BUSICOM. Ainda nesse mesmo ano, a Intel® decidiu comprar a licença da empresa japonesa, e obtendo assim os direitos de comercialização do *chip* (INTEL®, 2017).

### 3.2 FABRICANTES DE MICROCONTROLADORES

Desde a sua primeira geração lançada no início dos anos 70 pela Texas Instruments® o mercado de microcontroladores, que antigamente era dominado pela própria empresa, vem crescendo sempre. Após quase cinco décadas de comercialização, a *Microchip*® provavelmente se tornou líder mundial na fabricação de microcontroladores e soluções de sistemas relacionados com a compra da Atmel®.

Entre outros diversos fabricantes que possuem uma rentabilidade considerável destacam-se: Atmel®, Freescale®, *Microchip*®.

- Texas Instruments®

Empresa americana que desenvolve aplicações para sistemas de computadores e semicondutores. Encontra-se entre os maiores fabricantes de semicondutores do mundo, junto com a Intel® e Samsung®. É a maior fornecedora de circuitos integrados para telefones móveis. E também possui outra área de atividade que incluem o circuito para o RFID (TEXAS INSTRUMENTS®, 2017);

- Intel®

Fundada em 1968 pelos físicos Robert Noyce e Gordon Moore, a Intel® é uma empresa multinacional conhecida pelo desenvolvimento de circuitos integrados como microcontrolador e outros *chipsets*. Muito famosa também pelo seu microprocessador 8080 que possuía uma capacidade de endereçamento de memória de 64KB (INTEL®, 2017);

- Freescale®

A corporação Freescale® teve seu início a partir da divisão por setores da Motorola® e ficou responsável pelos semicondutores. Ela é voltada para o mercado de sistema embarcado e comunicações para seus *chips*. Em 2004 tornou-se uma empresa de capital aberto, após mais de 50 anos como parte da Motorola. Atualmente fundiu-se com a NXP Semicondutores (FREESCALE®, 2017);

- **Microchip® e Atmel®**

A **Microchip®** é uma empresa americana que desenvolve semicondutores analógicos e microcontroladores. Em sua linha de produção estão inclusos os microcontroladores da família PIC e em 2016 foi introduzida a família AVR, justamente quando a **Microchip®** adquire a **Atmel®** por 3,56 bilhões de dólares (**MICROCHIP®**, 2017);

Já a **Atmel®** é uma empresa de semicondutores, fundada em 1984, sua linha de produtos inclui microcontroladores, como o 8051, arquitetura ARM e a arquitetura **Atmel® AVR**, desenvolvida pela própria empresa. Essa é a arquitetura usada no Arduino, memórias EEPROM e Flash, RFID e outros componentes eletrônicos. Seus microcontroladores oferecem uma rica combinação de designs integrados (**ATMEL®**, 2017);

Em abril de 2016, a **Microchip®** concluiu a aquisição da empresa **Atmel®**.

### 3.3 APLICAÇÕES DE SISTEMAS EMBARCADOS

Sistemas embarcados estão presentes em milhares de equipamentos do cotidiano. Às vezes, são tão comuns que chegam a passar despercebidos aos usuários.

Podem-se destacar alguns tipos de aplicações, tais como:

- **Propósito Geral**

São aplicações que se assemelham aos computadores pessoais, porém, realizando uma função específica. Videogames são ótimos exemplos desse tipo de aplicação, que normalmente possuem uma forte interação homem-máquina, representado na Figura 19 (**CHASE**, 2007);

**Figura 19 – Nintendo NES Classic Edition.**



Fonte: Autores (2017).

- Automobilística

Na área de automóveis há uma alta demanda na precisão dos softwares, pois realizam operações críticas como controlar a frenagem e aceleração de veículos. Esse sistema é altamente complexo e, uma falha em seu comando pode ocasionar danos irreversíveis ao usuário (LAMB, 2015);

- Aplicação na medicina

TeleCare, conforme ilustra a Figura 20, é um equipamento da Atmel® que permite às pessoas idosas uma vida de maneira mais independente em suas residências, fornecendo assistência e monitoramento da saúde remotamente. A tecnologia Atmel® fornece uma plataforma para equipamentos com capacidade de detecção de quedas, uma aplicação promissora que pode alertar os serviços de emergência automaticamente. (ATMEL®, 2017).

**Figura 20 – Dispositivo TeleCare.**



Fonte: Atmel (online, 2017).

### 3.4 ARDUINO

Outra aplicação de sistemas embarcados está altamente relacionada com o Arduino, que é uma placa de prototipagem para o desenvolvimento de aplicações embarcadas.

Criado em 2005 por Massimo Banzi, David Cuartielles, Tom Igoe, Gianluca Martino e David Mellis, o Arduino era um projeto que tinha o objetivo de ser desenvolvido como um dispositivo que fosse fácil de programar, de baixo custo e funcional. Inicialmente pensado para o âmbito educacional, com o passar dos anos foi conquistando novos públicos por ser acessível aos que não tinham conhecimento aprofundado em eletrônica e programação (EVANS; NOBLE; HOCHENBAUM, 2013; THOMSEN, 2014).

No projeto inicial, foi criada uma plataforma de prototipagem eletrônica, baseada no microcontrolador da Atmel® e que contém, além do microcontrolador, circuitos de entrada e saída. Para a construção de projetos mais elaborados, o Arduino pode contar com expansões de hardware, sendo elas pequenas placas com sensores, chamadas de módulos, ou pode ser combinada com outros Arduinos, chamados de *shield* (THOMSEN, 2014; ARDUINO, 2017).

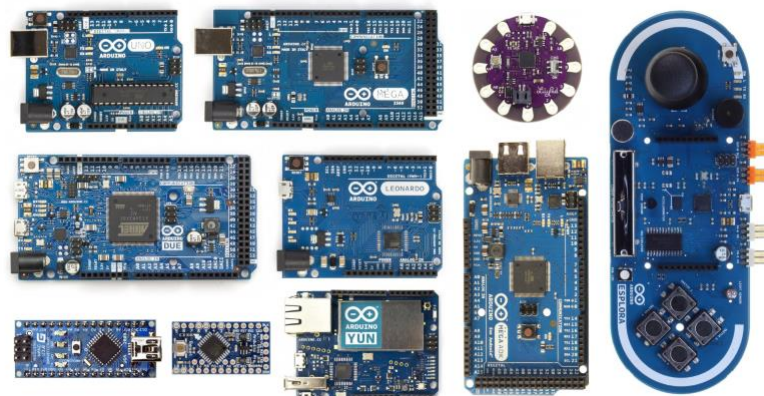
Para a construção de projetos mais elaborados, o Arduino pode contar com expansões de hardware, que são:

- Módulos: pequenas placas com sensores que acrescentam maior interação entre periféricos e sistema;
- Shields: placas com circuitos eletrônicos específicas para o Arduino, capazes de adicionar novas funções (EVANS; NOBLE; HOCHENBAUM, 2013; THOMSEN, 2014).

Compondo a construção de um protótipo, é necessário programar um conjunto de instruções. Essa programação pode ser facilmente transmitida para a placa Arduino através de sua IDE que utiliza as linguagens C e C++ para desenvolver os códigos. A facilidade de transmissão se dá pela necessidade de usar apenas um cabo USB para realizar a emissão de dados para o Arduino.

A IDE utilizada para a programação das placas é única, independentemente do modelo de placa Arduino empregada. Conforme ilustra Figura 21, o Arduino dispõe de vários modelos que variam na capacidade de processamento, no tamanho, número de portas de entrada e saída, entre outros. Essa variação permite ao projetista escolher a placa que melhor se adapte com as necessidades que o projeto apresenta (EVANS; NOBLE; HOCHENBAUM, 2013).

**Figura 21 – Amostra de modelos de placas Arduino.**



Fonte: Thomsem (2017, online).

De acordo com Arduino (2017), entre os modelos existentes, destaca-se a placa Arduino UNO, por ser a mais utilizada da família Arduino e por apresentar uma grande quantidade de documentação sobre projetos com esse modelo na internet.

### 3.5 PLACA ARDUINO UNO

A placa ilustrada na Figura 5, é baseada no microcontrolador ATmega328P. Esta placa é constituída pelos seguintes componentes:

- Pinos de entrada e saída digital, dentre eles 6 pinos com saída *Pulse Width Modulation* (PWM);
- Pinos para entradas analógicas;
- Pinos de alimentação para módulos e *shields* que possam vir a ser conectados com a placa;
- Conexão *Universal Serial Bus* (USB);
- Botão de *reset* (ARDUINO, 2017).

Utilizado no protótipo desenvolvido pela equipe, o modelo Arduino UNO, ilustrado na Figura 22, trabalha em conjunto com módulo RFID e com componentes eletrônicos menores para compor sua modelagem. A conexão USB disposta pelo Arduino em questão, funciona tanto como canal de comunicação serial para a transmissão de dados emitidos pela IDE, como fonte de alimentação. Essa alimentação serve para a placa Arduino, seus componentes, e para o módulo conectado com a placa.

**Figura 22 – Arduino Uno.**



Fonte: Arduino (online, 2017).

Na Tabela 5 é possível observar os dados do Arduino Uno fornecidos pelo fabricante.

**Tabela 5 – Dados técnicos do Arduino.**

<b>MICROCONTROLADOR</b>	<b>ATMEGA328P</b>
<b>VOLTAGEM DE OPERAÇÃO</b>	5 V
<b>VOLTAGEM DE ENTRADA (RECOMENDADA)</b>	7-12 V
<b>VOLTAGEM DE ENTRADA (LIMITE)</b>	6-20 V
<b>PINOS DE ENTRADA/SAÍDA DIGITAIS</b>	14 (Dos quais 6 são de saída <i>PWM</i> )
<b>PINOS DE ENTRADA/SAÍDA DIGITAIS PWM</b>	6
<b>PINOS DE ENTRADA ANALÓGICA</b>	6
<b>SRAM</b>	2 KB (ATmega328P)
<b>EEPROM</b>	1 KB (ATmega328P)
<b>MEMÓRIA FLASH</b>	32 KB (ATmega328P) Desses, 0.5 KB usados pelo <i>bootloader</i>
<b>COMPRIMENTO</b>	68.6 mm
<b>LARGURA</b>	53.4 mm
<b>PESO</b>	25g

Fonte: Arduino (2017, online).

## **4 APLICAÇÃO DA TECNOLOGIA RFID NO CONTROLE DE ACESSO EM INSTITUIÇÕES**

A partir da percepção de uma deficiência na segurança e agilidade de acesso presente no CESUPA unidade José Malcher, foi desenvolvido o protótipo para gerenciar e monitorar os acessos na instituição. Utilizando a tecnologia RFID para identificação automática e eficiente dos usuários e seus horários de entrada, este protótipo conta com interação homem-máquina por meio de interfaces gráficas, sendo expansível para outros estabelecimentos que apresentam grande fluxo de pessoas.

### **4.1 COMPONENTES FÍSICOS DO PROTÓTIPO**

No presente projeto, os componentes físicos utilizados são responsáveis pela identificação dos usuários, processo de entradas e saídas de dados e exibição do resultado da validação de tal identidade capturada. Os componentes físicos empregados no protótipo foram: 4 *tags* RFID, um módulo leitor RFID como periférico para interagir com as *tags* e um Arduino, ou mais precisamente o seu microcontrolador ATmega328P. As especificações dos componentes utilizados são:

#### **4.1.1 Módulo Leitor RFID MFRC522 MIFARE**

Eficiente para o propósito do projeto e com baixo custo em relação aos concorrentes com maior alcance, esse módulo, ilustrado na Figura 23, recebe a função de obter a identificação dos usuários cadastrados a partir da leitura das *tags* que entram no campo de percepção.

**Figura 23 – Módulo MFRC522.**



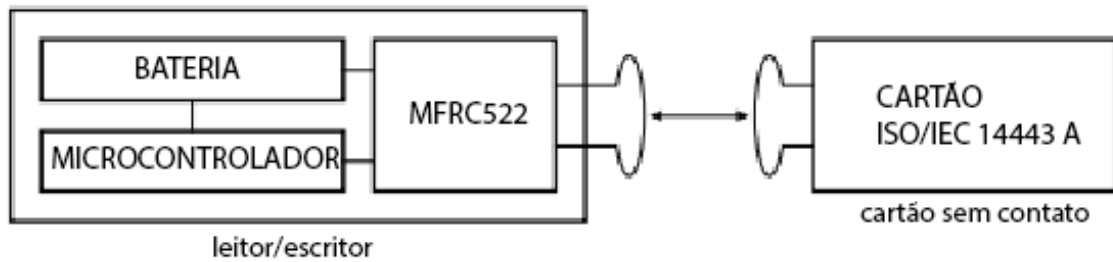
Fonte: Autores (2017).

Baseado no chip da NXP Semicondutores, o módulo segue um padrão sugerido pela NXT onde dispõe de antena e leitor em uma única placa. Dessa forma, resulta em um dispositivo mais compacto e de fácil programação das instruções necessárias para funcionamento. Trabalhando em alta frequência, garante alcance suficiente para o uso no protótipo. Entre as informações cedidas pelo fabricante do *chip*, destacam-se as seguintes especificações:

- Opera na frequência 13,56 MHz;
- Utiliza as padronizações ISO/IEC 14443, tipo A/MIFARE e NTAG;
- Suporta interfaces de comunicação serial SPI (*Serial Peripheral Interface*), UART (*Universal Asynchronous Receiver Transmitter*) e I2C (*Inter Integrated Circuit*), entretanto, devido às facilidades de programação oferecidas pela biblioteca presente no Arduino, foi utilizado a interface SPI;
- Com o uso do SPI obtêm-se uma taxa de transferência de 10 Mbit/s;
- Alcance de leitura e escrita definidos em 50 mm, cabendo alterações de acordo com o tamanho da antena e configuração do Arduino;
- Alimentação da placa variante entre 2,5 V e 3,3 V;
- Leve e compacto, o módulo utilizado apresenta as dimensões: 8,5x5,5cm e pesa 21g (NXP, 2016).

Ainda com base no datasheet da NXP (2016), o módulo necessita de uma fonte de energia e de um microcontrolador para terminar a composição em conjunto com o *chip* MFRC522, o esquema de leitura e escrita está representado na Figura 24, onde exibe de forma genérica um módulo e uma *tag* para exemplificar o sistema RFID.

**Figura 24 – Modo de leitura e escrita.**



Fonte: NXP (2017, online).

#### 4.1.2 Tag MF1S50yyX/V1 (MIFARE S50)

Originalmente chamada de *Unique IDentification* (UID), a *tag* MIFARE S50 utilizada neste projeto e ilustrada na Figura 25, é compatível com a frequência do módulo leitor e possui uma identificação única que representa cada usuário com acesso na instituição.

**Figura 25 – Tag chaveiro MIFARE S50 utilizada no protótipo.**



Fonte: Autores (2017).

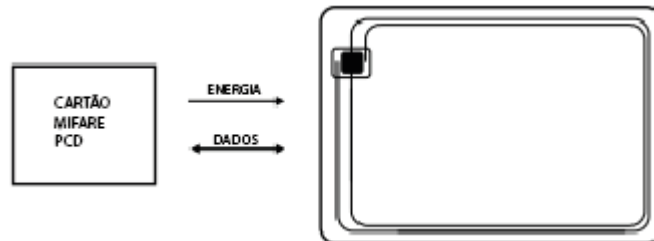
Presente no projeto para interagir com o leitor e prover dados sobre seu portador, a *tag* escolhida apresenta a possibilidade de regravar a memória e assim adicionar mais informações sobre o usuário além da sua identidade, além de tornar a *tag* reutilizável. Visando futuros problemas de leitura, a *tag* inclui um algoritmo de anti-colisão que possibilita a leitura de mais de uma *tag* simultaneamente, diminuindo os riscos de interferência no sistema. As especificações mais relevantes levantadas sobre a *tag* são:

- Obedece ao padrão ISO/IEC 14443 tipo A;
- Opera na frequência 13,56 MHz;
- 1 kB de EEPROM (*Electrically-Erasable Programmable Read-Only Memory*), organizados em 16 setores de 4 blocos (cada bloco com 16 *bytes*);
- Possui um algoritmo de anti-colisão que permite a utilização de múltiplas *tags* em um mesmo campo sem causar interferência na leitura;

- Modelado para oferecer comodidade ao usuário, apresenta tempo de transmissão de dados de 100 ms;
- Alcance de 100 mm, podendo variar de acordo com a configuração do leitor e o formato da antena (NPX, 2016).

É sugerido um modelo geral de funcionamento para as *tags*, conforme mostra a Figura 26. Tal modelo pode ser implementado em diversas formas e materiais, onde para o projeto foram adotadas as formas cartão e chaveiro. Essas formas apresentam material à prova d'água, e não divergem em alcance, velocidade de transmissão e memória, pois seguem o mesmo modelo, portanto as mudanças na disposição antena dentro da *tag* não são relevantes.

Figura 26 – Esquema da *tag* MF1S50yyX/V1.

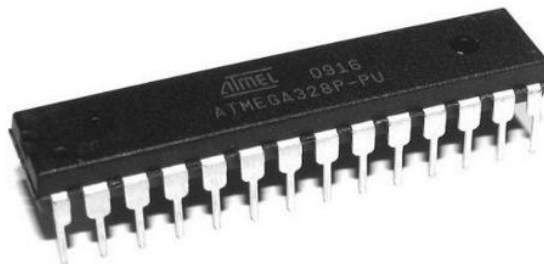


Fonte: NXP (2017, online).

### 4.1.3 Microcontrolador

Componente principal da placa Arduino, o microcontrolador ATmega328P, ilustrado na Figura 27, vem embutido na plataforma, processa as informações obtidas das *tags* e disponibiliza entradas e saídas, sendo essas digitais e analógicas, empregadas para receber os dados do módulo leitor e controlar as respostas enviadas aos *leds* (ATMEL, 2016; ARDUINO, 2017).

Figura 27 – Microcontrolador ATmega328P.



Fonte: Arduino (2017, online).

Viabilizando a construção de projetos com mais funcionalidades, devido à grande quantidade de entradas e saídas disponíveis para interagir com o meio onde o microcontrolador se encontra e, um vasto poder de processamento para poder executar grandes quantidades de instruções, o microcontrolador oferece uma excelente combinação desempenho e eficiência quanto ao uso de energia. Além dessas características, possui as seguintes especificações:

- Opera com a tensão de alimentação entre 1,8 V e 5,5 V;
- Apresenta núcleo AVR e barramento de dados de 8 bit;
- Memória *Flash* de 32 KB;
- EEPROM 1 KB;
- RAM 2 KB;
- Apresenta velocidade de processamento de 20 MIPS (Milhões Instruções por Segundo);
- Frequência máxima operacional de 20 MHz;
- Suporta as interfaces de comunicação serial SPI, USART (*Universal Synchronous Asynchronous Receiver Transmitter*) e I2C (ATMEL, 2016).

## 4.2 AMBIENTE DE DESENVOLVIMENTO INTEGRADO

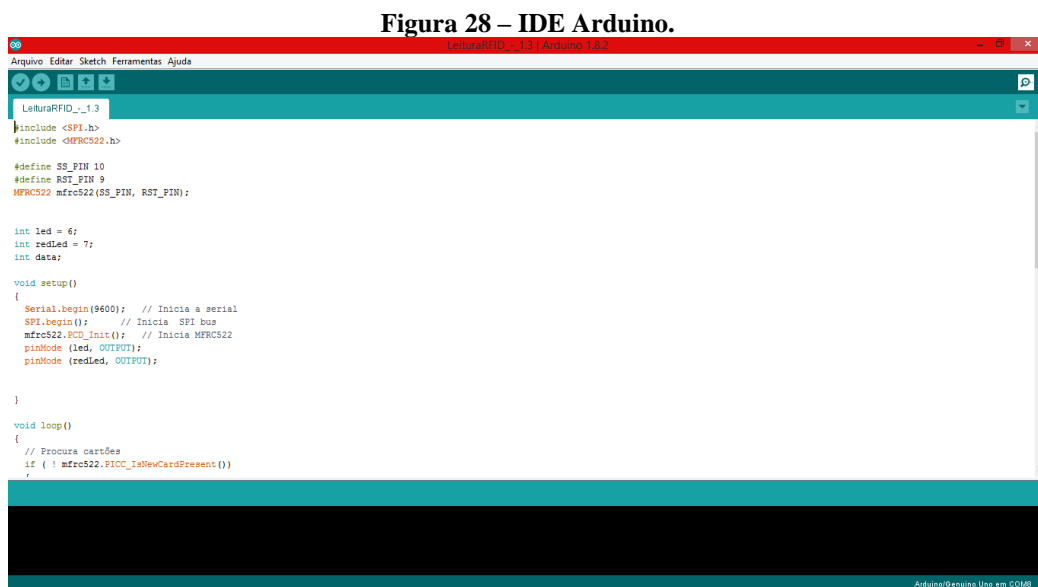
IDE, *Integrated Developer Environment*, se refere à um ambiente de desenvolvimento integrado. É o programa que reúne várias ferramentas necessárias para a criação de *softwares*, auxiliando o seu processo de desenvolvimento do. Além da capacidade de editar o código, o IDE possui compilador, ou interpretador, para gerar e executar o programa criado, apontando eventuais erros (DEITEL, 2005).

Pode suportar várias linguagens de programação, desde as mais simples até as mais robustas com maior estrutura, no entanto, é interessante destacar a linguagem Java. Constituindo mais de 50% do protótipo, devido a construção dos softwares e sistemas necessários para o seu funcionamento, Java é uma linguagem de programação e plataforma computacional lançada pela *Sun Microsystems* em 1995, atualmente essa linguagem pertence a Oracle (JAVA, 2017). Faz-se pertinente observar que é uma linguagem orientada a objetos, facilitando e deixando mais rápido o processo de alterar os sistemas desenvolvidos, além de permitir a criação de softwares estruturados e apresenta compatibilidade com várias plataformas, podendo ser executados em diferentes sistemas operacionais (DEITEL, 2005).

De forma específica, foram utilizados no desenvolvimento do protótipo, os IDE's Arduino e NetBeans, possibilitando interações entre os componentes escolhidos e o usuário final.

#### 4.2.1 IDE Arduino

Atualmente em sua versão 1.8.1, ilustrada na Figura 28, este IDE é disponibilizada pelos mesmos fabricantes da placa Arduino. Permite a gravação de códigos no microcontrolador de forma mais fácil e eficiente, devido usarem o mesmo padrão de comunicação. É baseado em *wiring*, projeto que antecede o do Arduino, porém conserva algumas características como apresentar fonte aberta e ser um programador de microcontroladores (ARDUINO, 2017).



Fonte: Autores (2017).

Ainda de acordo com ARDUINO (2017), este ambiente utiliza as linguagens C e C++ para o desenvolvimento de códigos, que são transferidos para o microcontrolador através da porta USB e, faz uso a interface de comunicação serial SPI.

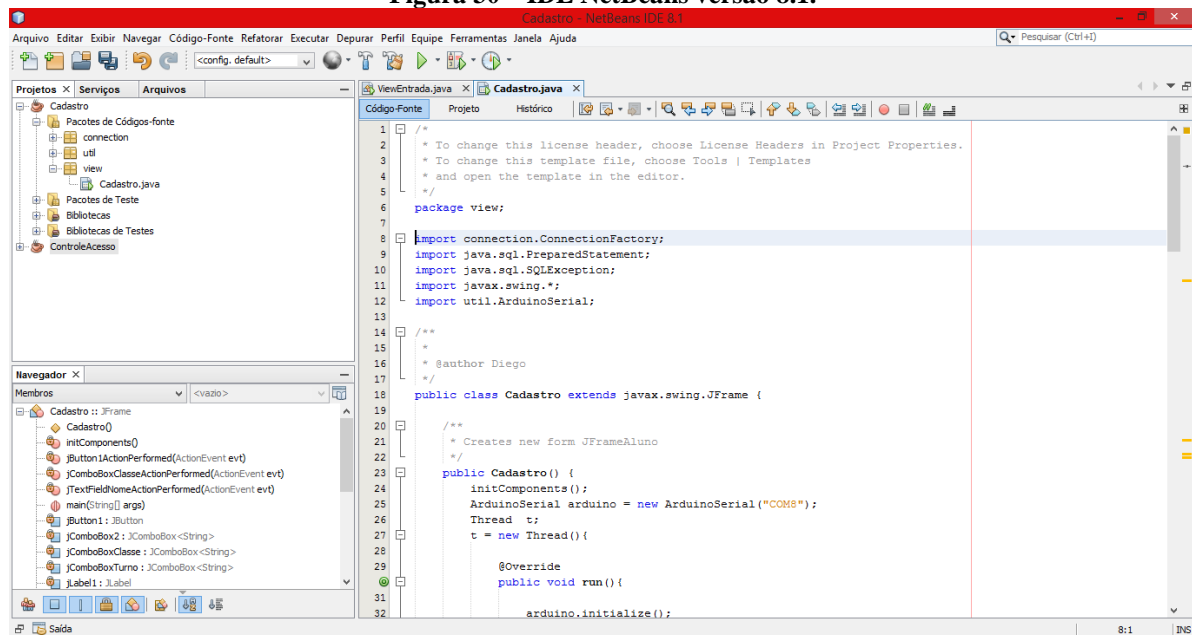
Esta interface é suportada por todos os componentes físicos, viabilizando a transferência sem maiores problemas de compatibilidade de comunicação. Os dados enviados e recebido através da porta serial da placa, podem ser exibidos para o programador por meio da ferramenta presente na IDE, chamada Monitor Serial como ilustra a Figura 29.

**Figura 29 – Dados recebidos a porta serial.**

Fonte: Autores (2017).

## 4.2.2 NetBeans

O NetBeans, conforme mostra a Figura 30, é um IDE atualmente na sua versão 8.2, criado e mantido pela Oracle. Foi empregado no projeto como plataforma para o desenvolvimento dos *softwares* de validação e cadastro de usuários usando a linguagem Java. Foi utilizado também para desenvolver o sistema web na linguagem PHP, responsável pelo monitoramento dos acessos registrados no sistema (NETBEANS, 2017).

**Figura 30 – IDE NetBeans versão 8.1.**

Fonte: Autores (2017, online).

Ainda baseado na referência anterior, este IDE apresenta ferramentas para facilitar o desenvolvimento de códigos e indica a localização de possíveis falhas na programação, capacidade de permitir o desenvolvimento de uma interface gráfica de forma simples e rápida na mesma plataforma do software desenvolvido é uma das mais importantes qualidades do NetBeans e, apresenta também bibliotecas que auxiliam a conexão com outros softwares que possam enriquecer o programa desenvolvido. Para este protótipo foi importada através do IDE a biblioteca RXTX, desenvolvida e mantida por Trent Jarvi. Esta tem como finalidade a conexão com a placa Arduino, realizando a obtenção e envio de dados. O driver JDBC (*Java Database Connectivity*) foi empregado para realizar a conexão com o banco de dados responsável por armazenar dados do usuário e sua identificação.

### 4.3 BANCO DE DADOS

O banco de dados utilizado no projeto é o MySQL 5.5, que hoje faz parte da linha de produtos da Oracle. Este o banco de dados é de código aberto e ainda é o conhecido do mundo em aplicações na internet. Atua como software livre com base na GPL (*General Public License*). O MySQL é representado pelo modelo relacional (MYSQL, 2017).

O modelo relacional representa o banco de dados como uma coleção de relações. Informalmente, cada relação é semelhante a uma tabela de valores ou, até certo ponto, a um arquivo plano de registros. Ele é chamado de arquivo plano porque cada registro tem uma simples estrutura linear ou plana [...] (ELMASRI; NAVATHE, 2004, p. 44).

A escolha deste banco de dados se deu pela sua facilidade de uso, compatibilidade com Java, PHP, desempenho e confiabilidade. O MySQL tornou-se a principal opção para aplicações na internet, como Facebook®, Google® e Adobe®, por ser uma ferramenta que armazena dados relacionados. Esses dados, utilizados no protótipo, são informações do mundo real que podem realizar uma, ou algumas, das quatro operações básicas: *create*, *retrieve*, *update* e *destroy*, conhecido como CRUD.

- *Create*: para a criação de novas entradas de dados;
- *Retrieve*: Ler, recuperar ou visualizar dados existentes;
- *Update*: Atualizar dados existentes, caso exista necessidade;
- *Destroy*: Excluir dados que não são mais necessários (MYSQL, 2017).

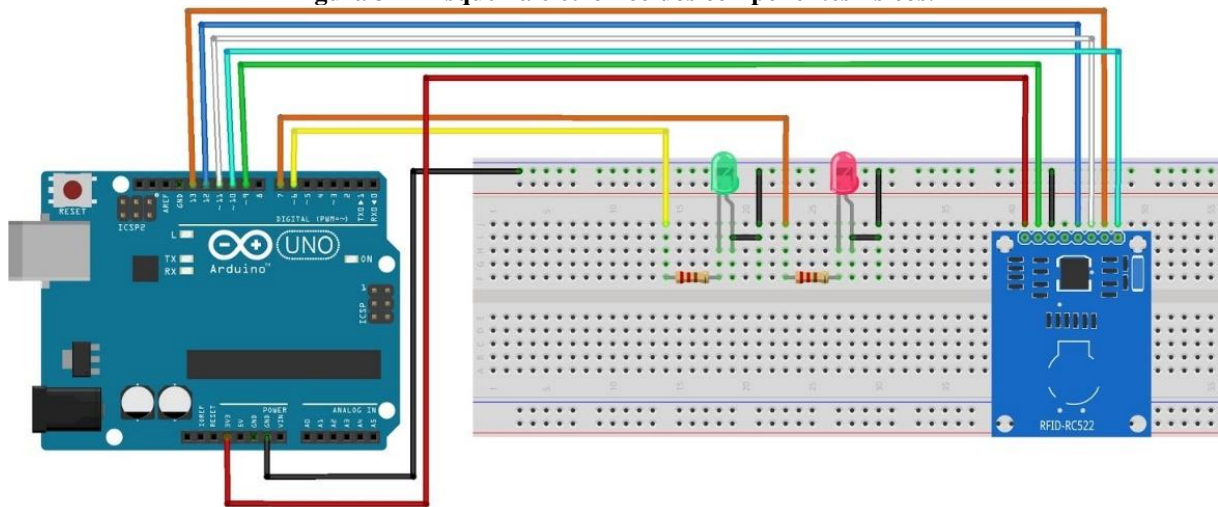
No protótipo, cabe ao banco de dados armazenar todas as informações dos usuários cadastrados a fim de disponibilizar os dados necessários para que o sistema *web* e o *software* de validação possam ser executados com sucesso.

#### 4.4 DESENVOLVIMENTO E FUNCIONAMENTO

A integração dos componentes físicos, softwares e sistemas apresentados neste capítulo têm como propósito auxiliar a compreensão do funcionamento do protótipo desenvolvido.

A princípio, fez-se a montagem dos componentes físicos, onde houve a junção da placa Arduino com o módulo Leitor RFID, para poder realizar as leituras das *tags* disponíveis. Dispondo de quatro *tags*, sendo duas encapsuladas em cartão e duas em chaveiro, a interação dessas *tags* foi realizada com o Arduino e o módulo, dispostos de acordo com a Figura 31.

**Figura 31 – Esquema eletrônico dos componentes físicos.**



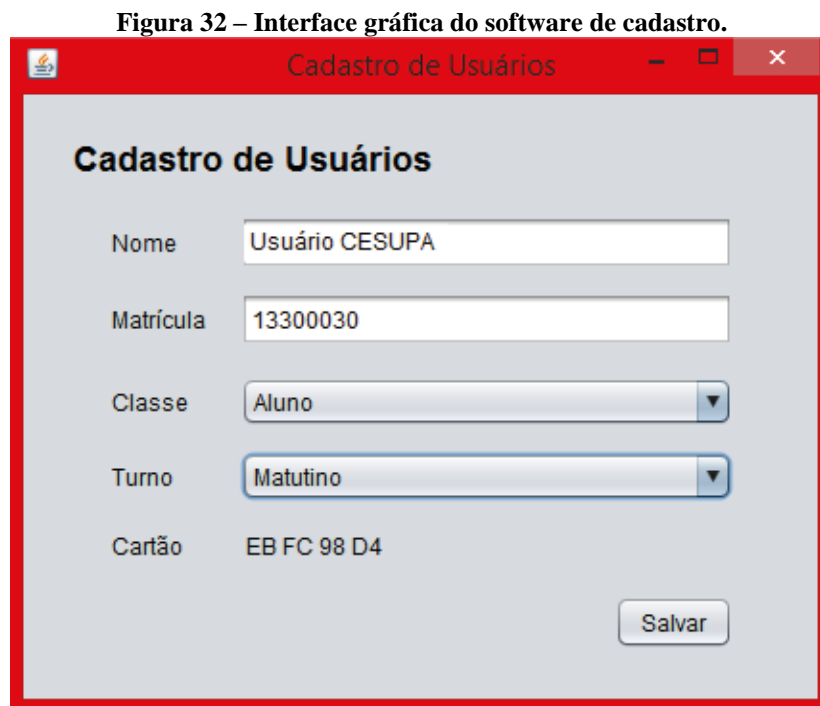
Fonte: Autores (2017).

Com os componentes físicos já montados, foi desenvolvida e transmitida através da IDE do Arduino a programação responsável pela identificação dos usuários, onde o código contém duas rotinas. A primeira rotina apresenta as instruções necessárias para fazer com que o leitor sempre busque por novas *tags*, execute a leitura e deixe a UID da *tag* lida disponível na porta serial. A segunda rotina recebe a resposta enviada pelo software de validação, sendo uma vez recebida uma resposta positiva, há a liberação de acesso do portador da *tag*.

## 4.5 SOFTWARES DE CADASTRO E VALIDAÇÃO

Os softwares foram desenvolvidos com linguagem Java na plataforma NetBeans, fazendo uso da possibilidade de comunicação com os componentes físicos através da porta serial e, da criação facilitada de interfaces homem-máquina que pudessem ser ponte entre a captura dos dados do usuário via radiofrequência e o banco de dados.

No intuito de inserir os dados dos usuários e a sua respectiva *tag* correspondente, o *software* de cadastro captura a UID disponível na porta serial do Arduino, a exibe na interface gráfica desenvolvida, ilustrada na Figura 32, e a armazena no banco de dados, assim como os dados inseridos na interface.



Fonte: Autores (2017).

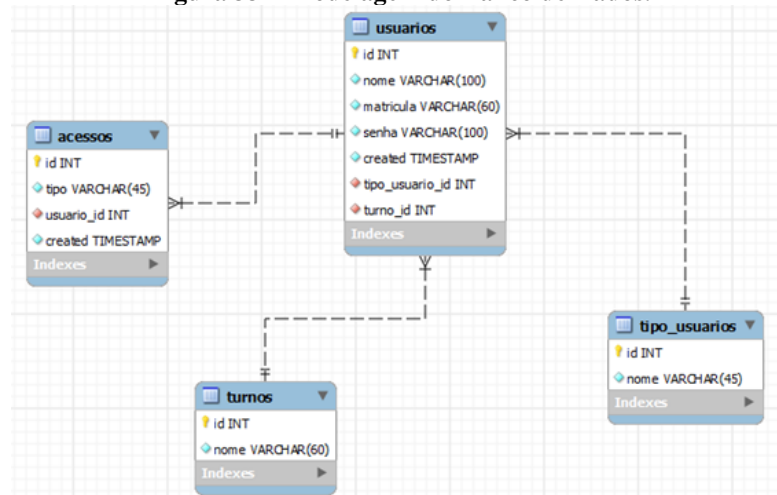
No software de validação é efetuada a comparação da UID capturada com as que estão presentes no banco de dados. Assim como para cadastrar novos usuários no sistema, utiliza-se o driver *Java Database Connectivity (JDBC)* para auxiliar a conexão com o banco de dados preenchido com os dados dos usuários, incluindo a identificação da *tag* de cada um deles.

A comparação realizada pelo software verifica se a *tag* lida existe no banco de dados, dessa forma, se houver tal cadastro, é registrado no banco o horário do acesso e a *tag* que foi utilizada na comparação. Em conjunto com o registro do acesso uma resposta é emitida via porta serial para o Arduino, responsável por acionar um *led* de cor verde assim permitindo a

entrada do usuário. Caso a UID da *tag* lida não esteja cadastrada, a resposta emitida para o Arduino impossibilita a passagem do usuário e aciona o *led* vermelho como resposta visual para a invalidação da *tag*. Para a saída dos usuários é apenas apresentado uma divergência em relação ao sistema supracitado, sendo ela a ausência do acionamento de leds, dispondo somente da validação da tag e registro do horário de acesso no banco de dados.

Para suprir as necessidades de armazenamento dos usuários e dos acessos da instituição, foi criado um banco de dados em MySQL com a relação predominante de 1:N, que nada mais é do que a relação de um para muitos. Isso pode ser observado na Figura 33 com a leitura das tabelas (*tipo\_usuarios*) e (*usuarios*) onde cada usuário terá apenas um tipo de usuário e um tipo de usuário poderá conter vários usuários.

**Figura 33 – Modelagem do Banco de Dados.**



Fonte: Autores (2017).

## 4.6 SISTEMA WEB

A linguagem utilizada para o desenvolvimento do sistema web foi o PHP por ser muito usado em desenvolvimentos na *web*, gerar páginas com conteúdo dinâmico e coletar dados de formulários. Além disso, também é conhecido por suportar uma ampla variedade de banco de dados. Essas características o tornam ideal para o sistema de monitoramento deste projeto (PHP, 2017).

Ainda de acordo com a referência previamente utilizada, o PHP é uma linguagem de programação gratuita e de código aberto, ou seja, ele pode ser instalado em qualquer máquina sem nenhum custo e independentemente da plataforma (Windows, Linux ou Mac). A

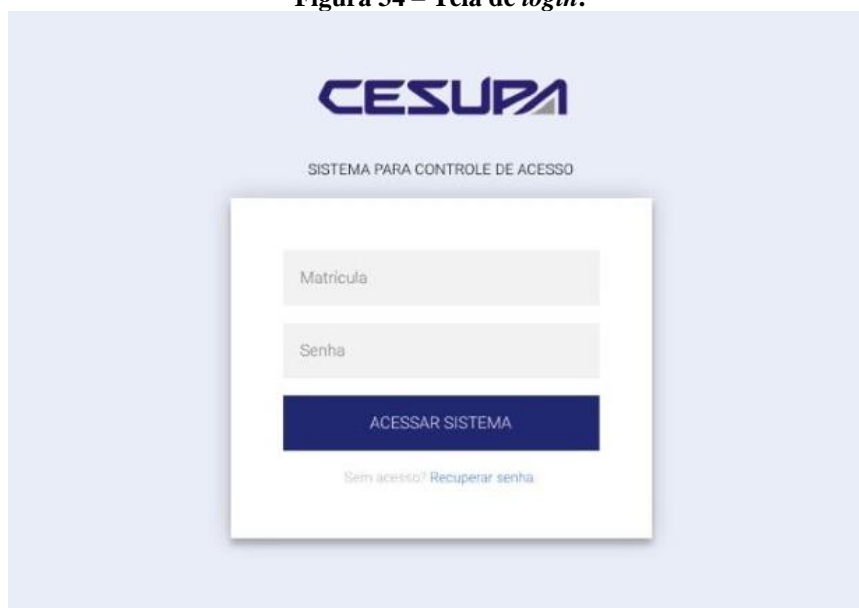
linguagem possui estilo de tipagem dinâmica, com uma curva de aprendizado reduzida para iniciantes, sem contar que é semelhante às linguagens já consagradas como C e Java.

O banco de dados utilizado no protótipo, o MySQL, estão armazenados todos os cadastros de usuários (alunos e funcionários) e os acessos à instituição. Os acessos estão separados por período: matutino, vespertino, noturno e integral.

O CakePHP 2.3 é um *framework* livre, de código aberto e escrito em PHP. Tem como objetivo oferecer estrutura para programadores PHP desenvolverem aplicações seguras e robustas. Esse *framework* orientado a objetos fornece uma estrutura organizacional básica que usa padrão de projeto dividido em três camadas: *model*, *controller* e *view*, também conhecido por MVC (CAKEPHP, 2017). Executado sob o servidor Apache 2.2, que também é livre e fornece implementações robustas e comerciais para diversos consumidores que vão desde pessoa física até empresas (APACHE, 2017).

Utilizando as ferramentas descritas, foi desenvolvido o sistema *web* escrito na linguagem PHP, usando padrão de projeto MVC e desenvolvido na IDE do NetBeans. O sistema *web* tem como objetivo monitorar os acessos no CESUPA, gerando relatórios por mês ou por matrícula. A tela de acesso, ilustrada na Figura 34, demonstra que apenas usuários credenciados são capazes de realizar o *login* do sistema e visualizar o conteúdo disponibilizado.

**Figura 34 – Tela de login.**



A imagem mostra a interface de login do sistema CESUPA. No topo, há o logotipo 'CESUPA' em azul escuro. Abaixo dele, o texto 'SISTEMA PARA CONTROLE DE ACESSO' em cinza. O formulário principal é branco e contém dois campos de entrada: 'Matrícula' e 'Senha', ambos com bordas arredondadas e fundo cinza claro. Abaixo dos campos, há um botão azul escuro com o texto 'ACESSAR SISTEMA' em branco. Na base do formulário, há um link em cinza que diz 'Sem acesso? Recuperar senha'.

Fonte: Autores (2017).

Como mostra Figura 35, podem ser observados os relatórios dos acessos que estão armazenados no banco de dados e foram importados para uma interface homem-máquina.

Ainda nela, estão presentes o número de matrícula do usuário que acessou à instituição por meio do cartão RFID, o dia e hora desse acesso.

**Figura 35 – Tela de Acesso.**

ID	Usuário	Matrícula	Tipo de acesso	Data e Hora
2	Administrador	000	Entrou	15/05/2017 12:34:12
10	Jellyane da Cruz Rocha	13300030	Entrou	15/05/2017 08:50:47
11	Mateus Vieira de Almeida	13300022	Entrou	15/05/2017 08:50:55
12	Jessica do Nascimento Campos Gomes	13300032	Entrou	15/05/2017 08:50:58
13	Jellyane da Cruz Rocha	13300030	Saiu	15/05/2017 13:24:53
14	Jessica do Nascimento Campos Gomes	13300032	Saiu	15/05/2017 13:24:58
15	Mateus Vieira de Almeida	13300022	Saiu	15/05/2017 13:25:03

Fonte: Autores (2017).

Esse relatório pode ser filtrado utilizando a pesquisa por matrícula, como pode ser observado na Figura 36, onde é exibido apenas o relatório dos acessos encima da matrícula digitada.

**Figura 36 – Busca por matrícula.**

ID	Usuário	Matrícula	Tipo de acesso	Data e hora
10	Jellyane da Cruz Rocha	13300030	Entrou	15/05/2017 08:50:47
13	Jellyane da Cruz Rocha	13300030	Saiu	15/05/2017 13:24:53
16	Jellyane da Cruz Rocha	13300030	Entrou	16/05/2017 09:53:27
19	Jellyane da Cruz Rocha	13300030	Saiu	16/05/2017 13:00:43
22	Jellyane da Cruz Rocha	13300030	Entrou	17/05/2017 08:01:17

Fonte: Autores (2017).

Finalizando o sistema *web* foi desenvolvido um gráfico para a exibição dos acessos por mês, como é demonstrado na Figura 37. A fim de representar o monitoramento dos acessos de maneira mais dinâmica.

Figura 37 – Gráfico dos acessos mensais.



Fonte: Autores (2017).

## 5 CONCLUSÃO

O objetivo deste trabalho é realizar melhorias no controle de acesso do CESUPA. Essas melhorias são divididas em maior agilidade no fluxo de entrada, influenciando na segurança dos seus usuários, e adicionar a possibilidade de monitorar os horários de entrada desses usuários.

Por meio de estudos sobre identificação por radiofrequência e os componentes que auxiliam seu funcionamento, tal como o sistema embarcado, foi possível alcançar o objetivo estipulado a partir do desenvolvimento de um protótipo de controle de acesso que conta com partes físicas e partes virtuais. As partes físicas fazem uso da tecnologia RFID para identificar os usuários e da placa Arduino para o processamento dos dados obtidos via radiofrequência. A parte virtual é composta pelos *softwares* desenvolvidos em Java para validar e cadastrar usuários assim como, o sistema *web* feito na linguagem PHP que disponibiliza o registro dos acessos.

Conclui-se que para o propósito de controle, gerência e monitoramento de acesso, a tecnologia RFID torna-se grande aliada devido a velocidade na captura e transmissão de dados, apesar de suas desvantagens nos custos de aparelhos com grande alcance. Se trabalhado com baixo alcance de leitura, o RFID se torna pouco dispendioso e de fácil configuração, criando possibilidades de implantação em maior escala, em outras instituições, não necessariamente de ensino, e com maiores funcionalidades.

### 5.1 DIFICULDADES ENCONTRADAS

Durante o desenvolvimento deste trabalho, alguns obstáculos foram encontrados. Em relação a monografia, a principal dificuldade foi conseguir acesso a referências bibliográficas sobre o RFID, pois, em nossa região, essa tecnologia é explorada vagarosamente. O que justifica a ausência de livros em grande parte das bibliotecas de Belém, porém, com a busca de trabalhos na Internet, conseguimos contornar essa situação.

Já em relação ao protótipo, mais de uma dificuldade pode ser destacada:

- A primeira dificuldade encontrada foi quanto ao uso do banco de dados que, por não termos conhecimento aprofundado sobre o assunto, nos levou a convidar um profissional em banco de dados para auxiliar no protótipo. Uma

vez com o banco de dados criado, a dificuldade seguinte foi realizar a conexão com o Arduino;

- Outra dificuldade relevante do projeto ocorre pelo mesmo motivo da que foi encontrada no desenvolvimento da monografia: a tecnologia RFID possui um progresso lento na região. Então, para obter os equipamentos necessários ao protótipo, tivemos que solicitar fora do estado.

## 5.2 TRABALHOS FUTUROS

Mesmo que o projeto tenha chegado ao seu fim, ainda há sugestões para o avanço no controle de acesso, seja ele em instituições ou em qualquer outro tipo de empresa.

Com o intuito de aumentar o nível de controle, a adição de uma restrição de tempo para um novo ingresso de uma mesma *tag* seria a providência a ser tomada de imediato. Onde um usuário poderia acessar a instituição novamente somente após 20 minutos do registro da sua saída, diminuindo a possibilidade de burlar o sistema através de empréstimos de etiquetas a terceiros.

Desenvolver no sistema de monitoramento *web* um gráfico com os horários que os alunos de cada curso se encontram com maior frequência na instituição fora do seu turno original. Com esses resultados, poderia ser realizada uma análise para a criação de novas turmas nos horários com maior fluxo de alunos fora do turno usual.

Além dessas sugestões, pode-se destacar outros tópicos:

- Implementação de catracas;
- Cartão curinga para visitantes;
- Melhoras na segurança do cartão.

## REFERÊNCIAS

2º CONGRESSO BRASILEIRO DE RFID & INTERNET DAS COISAS. **RFID "Identificação por frequência de rádio"**. Disponível em: <<http://web.archive.org/web/20130809192534/http://congressorfid.com.br/rfid/>>. Acesso: 02 abril de 2017.

ANDRELO JUNIOR, Joel. **RFID – identificação por radiofrequência**. Monografia. Faculdade de Tecnologia de Praia Grande. Informática para Gestão de Negócios. São Paulo: Praia Grande, dez.2007. Disponível em: <[www.monografias.com](http://www.monografias.com)>, acessado em 23/03/2017.

ARDUINO. **Overview**. Disponível em: <<https://www.arduino.cc/en/main/arduinoBoardUno>>. Acesso: 03 maio de 2017.

ATMEL. Produtos. **Microcontroladores**. Disponível em: <<http://www.atmel.com/pt/br/products/microcontrollers/default.aspx>>. Acesso: 25 março de 2017.

BERNARDO, Cláudio Gonçalves. A tecnologia RFID e os benefícios da etiqueta inteligente para os negócios. **Revista Eletrônica UNIBERO de Produção Científica**. São Paulo, set.2004.

BHUPTANI, Manish; MORADPOUR, Shahram. **RFID: Implementando o Sistema de Identificação por Radiofrequência**. São Paulo: IMAM, 2005. 250p.

CAKEPHP. **Welcome**. Disponível em: <<https://book.cakephp.org/2.0/en/index.html>>. Acesso: 03 maio de 2017.

CARVALHO JÚNIOR, José Regivaldo. **RFID Aplicação no controle de acesso**. UEPE/Escala Politécnica de Pernambuco/Departamento de Engenharia Elétrica. Monografia, Recife, nov.2008.

CHASE, Otávio. **Sistemas Embarcados**. [www.sbajovem.org](http://www.sbajovem.org). SBA Jovem, 2010. 12/2007. Disponível em: <[www.lyfreitas.com.br/ant/pdf/embarcado.pdf](http://www.lyfreitas.com.br/ant/pdf/embarcado.pdf)>. Disponível em: 29 maio de 2017.

CIS. **CIS Eletrônica**. Disponível em: <<http://www.cis.com.br/>>. Acesso: 28 junho de 2017.

\_\_\_\_\_. **Leitores Biométricos**. Disponível em: <<http://www.cis.com.br/index.php/digiscan-fs-25>>. Acesso: 28 junho de 2017.

COMPUTER ID. **Empresa**. Disponível em: <<http://computerid.com.br/empresa/index.php?id=1>>. Acesso: 28 junho de 2017.

\_\_\_\_\_. **Produtos**. Disponível em: <[http://computerid.com.br/produtos/produtos\\_view.php?c=2&s=1&l=29&p=39](http://computerid.com.br/produtos/produtos_view.php?c=2&s=1&l=29&p=39)>. Acesso: 28 junho de 2017.

CUNHA, Alessandro F. Novas Tecnologias. **RFID. Etiquetas com eletrônica de ponta**. Revista Saber Eletrônica, nº 401, jun.2006, p.20 a 25.

DATAPONTO. **Catracas Lumen Advance**. Disponível em: <<http://www.dataponto.com.br/catracas-sp/catracas-lumen-advance.php>>. Acesso: 28 junho de 2017.

DEITEL, Harvey M. **JAVA – Programar**. São Paulo: Person Prentice Hall, 2005. Ed. 6. 1152p.

DELAI, Andre Luiz. **Sistemas Embarcados: a computação invisível**. Guia do Hardware.net. 16/mai/2013.

DRESCH JUNIOR, Antonio; EFROM, Danny R.; GRUMOVSKI, Dieison. Sistema de Controle de Patrimônio via RFID. **Revista E-Tech: Atualidades Tecnológicas para Competitividade Industrial**. Florianópolis (SC), v. I, n. 1, p.47-57, 1º Sem/2008.

ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistema de banco de dados**. São Paulo. Pearson Education, 2010. Ed. 6. 808p.

EVANS, M.; NOBLE, J; HOCHENBAUM, J. **Arduino em Ação**. São Paulo: Novatel, 2014.

FREESCALE. **Products**. Disponível em: <<https://www.freescale.com/transweb>>. Acesso: 22 março de 2017.

FREITAS, Stéfani Antonelli Goerck. **Desenvolvimento de um sistema de controle embarcado para a equipe de futebol de robôs Araranguá Intruders**. Monografia de TCC. Araranguá (SC): UFSC, fev.2013, 74p.

GOMES, Hugo Miguel Cravo. **Construção de um sistema de RFID com fins de localização especiais**. Portugal: Universidade de Aveiro, Departamento de Engenharia Eletrônica, Telecomunicações e Informática. Dissertação de Mestrado, 2007, 104p.

GRUCHINSKI, Marlei Rute. **Protótipo de um sistema único de identificação pessoal baseado em tecnologia RFID**. Blumenau (SC), Universidade Regional de Blumenau, 2007, TCC, 64p. [www.mf.furb.br/~pericos/orientações](http://www.mf.furb.br/~pericos/orientações). Centro de Ciências Exatas e Naturais.

HENRY. **Institucional**. Disponível em: <<http://www.henry.com.br/institucional>>. Acesso: 28 junho de 2017.

\_\_\_\_\_. **Lumen Advance com cofre**. Disponível em: <<http://www.henry.com.br/catracas/lumenadvancecofre>>. Acesso: 28 junho de 2017.

INTEL. **A History Of Innovation**. Disponível em: <<https://www.intel.com.br/content/www/br/pt/history/historic-timeline.html>>. Acesso: 27 março de 2017.

\_\_\_\_\_. **The Story Of The Intel® 4004**. Disponível em: <<https://www.intel.com/content/www/us/en/history/museum-story-of-intel-4004.html>>. Acesso: 27 março de 2017.

JAVA. **O que é a Tecnologia Java e porque preciso dela**. Disponível em: <[https://www.java.com/pt\\_BR/download/faq/whatis\\_java.xml](https://www.java.com/pt_BR/download/faq/whatis_java.xml)>. Acesso: 13 abril de 2017.

KIMALDI. **Início**. Disponível em: <<http://www.kimaldi.com/po/>>. Acesso: 28 junho de 2017.

\_\_\_\_\_. **Controle de Acesso Kimaldi Flexy**. Disponível em: <[http://www.kimaldi.com/po/produtos/sistemas\\_biometricos/controlo\\_de\\_acesso\\_biometrico/controlo\\_de\\_acesso\\_kimaldi\\_flexy](http://www.kimaldi.com/po/produtos/sistemas_biometricos/controlo_de_acesso_biometrico/controlo_de_acesso_kimaldi_flexy)>. Acesso: 28 junho de 2017.

LAMB, Frank. **Automação Industrial na prática**. AMGH Editora, 2015. Série Tekne. McGraw Hill Education.

LAZARO, Ewerton Costa; NASCIMENTO, Thais Pedruzzi. **RFID – IDENTIFICAÇÃO POR RÁDIO FREQUÊNCIA.** Disponível em: <<https://pt.scribd.com/document/136943818/Trabalho-RFID-pdf>>. Acesso: 07 abril de 2017.

LEWGOY, Julia. **Sem Parar ou ConectCar. Qual vale mais a pena para você?.** Revista Exame.com, 23.jan.2017.

LIMA JUNIOR, Levi Ferreira. **A tecnologia de RFID no padrão EPC e soluções para implementação desta tecnologia em empilhadeiras.** Monografia de Pós-Graduação. MBIS, PUC/SP, 2006.

LOPES, Alexandre Ricardo; COSTA, Douglas Tudeia; GONÇALVES, Gustavo Lourencetti; PONTES, João Orlando; ALMEIDA, Nicelio Alves. **Controle de acesso através da identificação por radiofrequência.** Santos André (SP) 2009, Centro Universitário Fundação Santo André/Faculdade de Engenharia Eng. Celso Daniel/Engenharia Eletrônica – Telecomunicações. Monografia. 50p.

MARTINS NETO, Antonio; RODRIGUES, Wagner José Wanzeler. **Controle de Fluxo Utilizando Tecnologia RFID.** Monografia de TCC. Belém (PA): CESUPA, jun.2016, 66p.

MATIC, Nebojosa. **PIC Microcontrollers.** Picbook. USA: 04/02/2003. Disponível em: <<http://www.islavici.ro/cursuriold/conducere%20sist%20cu%20calculatorul/PICbook/picbook.htm>>. Acessado em: 14 abril de 2017.

MCROBERTS, Michel. **Arduino básico.** Apostila. São Paulo: Novatec Editora Ltda., 2011. Disponível em: <[www.caiobarbosa.com.br/wp-content/uploads/2015/11/apostila\\_arduino.pdf](http://www.caiobarbosa.com.br/wp-content/uploads/2015/11/apostila_arduino.pdf)>, acessado em 15/04/2017.

MICROCHIP. **Microchip Technology, Inc. Acquires Atmel.** Disponível em: <<http://www.microchip.com/announcements/microchip-technology-inc-acquires-atmel>>. Acesso: 25 março de 2017.

MOTA, Rafael Perazzo Barbosa. **Mecanismos para a melhoria do desempenho de sistemas RFID passivos.** Tese de doutorado. USP, 2006.

MYSQL. **General Information.** Disponível em: <<https://dev.mysql.com/doc/refman/5.7/en/introduction.html>>. Acesso: 10 abril de 2017.

NARCISO, M.G. Aplicação da tecnologia de identificação por radiofrequência (RFID) para controle de bens patrimoniais pela Web. **Revista Science Global Science Technology**, vol.1, nº 7, p.50a59, dez/mar 2008.

NETBEANS. **NetBeans IDE**. Disponível em: <<https://netbeans.org/features/index.html>>. Acesso: 15 abril de 2017.

NPX SEMICONDUCTORES. **MF1S50yyX/V1**. Disponível em: <[http://cache.nxp.com/documents/data\\_sheet/MF1S50YYX\\_V1.pdf](http://cache.nxp.com/documents/data_sheet/MF1S50YYX_V1.pdf)>. Acesso: 15 abril de 2017.

ODA, Glauco. **O que é RFID: Etiquetas RFID no Controle Patrimonial**. AfixCode. 3.out.2014.

OLIVEIRA JÚNIOR, Marconi; DUARTE, Ricardo de O. **Apostila sobre Introdução ao Projeto de Microcontroladores e Programação de Periféricos**. Belo Horizonte: UFMG/DELT, dez.2010, 115p.

OLIVEIRA, Alessandro de Souza; PEREIRA, Milene Franco. **Estudo da tecnologia de identificação por radiofrequência – RFID**. Brasília: Faculdade de Tecnologia/Departamento de Engenharia Elétrica. 2006.

PHP. **O que é o PHP?**. Disponível em: <[https://secure.php.net/manual/pt\\_BR/intro-what-is.php](https://secure.php.net/manual/pt_BR/intro-what-is.php)>. Acesso: 03 maio de 2017.

PRADO, N; PEREIRA, N.; POLITANO, P. **Dificuldades para a adoção de RFID nas operações de uma cadeia de suprimentos**. Anais, 2006.

QUEIROZ, Eduardo Luiz; ARAÚJO, Tairone Ádamo; HORTA, Mário Marcos Brito. RFID e o seu uso na indústria. **Revista Semana Acadêmica**. Fortaleza, ano MMXIV, nº 000063, 26/11/2014.

REVISTA INTRALOGISTICA. **Fundamentos sobre RFID**. Disponível em: <[http://www.imam.com.br/consultoria/artigo/pdf/fundamentos\\_sobre\\_rfid.pdf](http://www.imam.com.br/consultoria/artigo/pdf/fundamentos_sobre_rfid.pdf)> Acesso: 07 abril de 2017.

**RFID Essentials.** Theory in Practice. O'Reilly Network. GLOVER, Biel; BHATT, Himanshu. Media, USA, 2006, ISBN 0.596.00944.5.

**RFID Handbook: Radio-Frequency Identification Fundamentals and Applications.** FINKENZELLER, K. Wiley, UK, 2000, ISBN 9780471988519.

RFIDBR. **Definindo RFID.** Disponível em: <[http://www.rfidbr.com.br/index.php/definindo\\_rfid.html](http://www.rfidbr.com.br/index.php/definindo_rfid.html)>. Acesso: 03 abril de 2017.

SANTOS, Marco Aurélio da Silva. **"Radar"**. Brasil Escola. Disponível em <<http://brasilecola.uol.com.br/fisica/radar.htm>>. Acesso em: 14 março de 2017.

SEUFITELLI, Claudia Boechat; HENRIQUE, Daniele Fontes; ROSA, Sérgio Inácio; CARVALHO, Rogério Atem. Tecnologia RFID e seus benefícios. **VÉRTICES.** Campos dos Goytacazes (RJ), v. 11, n. 1/3, p.19-26, jan./dez. 2009.

SMILEY, Suzanne. **Active RFID vs. Passive RFID: What's the Difference?.** RFID INSIDER. Tracking The RFID Industry. 4.mar.2016.

\_\_\_\_\_. **Monostatic vs Bistatic RFID System.** RFID INSIDER. Tracking The RFID Industry. 18.jul.2014.

TAURION, Cezar. **Software Embarcado: a nova onda da Informática.** São Paulo: Brasport, 2005.

TEXAS INSTRUMENTS. **Por que TI?.** Disponível em: <<http://careers.ti.com/whyti/>>. Acesso: 19 março de 2017.

THE APACHE SOFTWARE FOUNDATION. **Supporte Apache.** Disponível em: <<https://www.apache.org>>. Acesso: 01 maio de 2017.

THOMSEM, Adilson. **Programando um Arduino Pro Mini com Arduino UNO.** Blog filipeflop.com, 9.jan.2014.

TOMAZ, Laurence Smanhotto. **RFID(Radio-Frequency IDentification).** PUC/PR, Curitiba, nov.2009.

VIOLINO, Bob. **"The history of RFID Technology"**. RFID Journal, 16.jan.2005.

WATANABE, Ana T. Y. **O Universo HCS08QG8. Teoria, Linguagem Assembly, atividades de laboratório e projetos.** Santa Catarina: UDESC, Joinville, 2011.