

CENTRO PAULA SOUZA
ETEC PHILADELPHO GOUVÊA NETTO

Técnico em Eletroeletrônica

Paulo Rogério Marques Moreira

Plinio Hillebrand Junior

Romário da Silva de Carvalho

Vitor Afonso dos Santos Marciano

TRAVA DE SEGURANÇA ELETRÔNICA

São José do Rio Preto

2026

Paulo Rogério Marques Moreira

Plinio Hillebrand Junior

Romário da Silva de Carvalho

Vitor Afonso dos Santos Marciano

TRAVA DE SEGURANÇA ELETRÔNICA

**Trabalho de Conclusão de Curso
apresentado ao Curso de Técnico em
Eletroeletrônica em 2026 da ETEC
Philadelpho Gouvêa Netto, orientado pelo
professor Mario Kenji Tamura, como
requisito parcial para obtenção do título
de técnico em Eletroeletrônica.**

São José do Rio Preto

2026

DEDICATÓRIA

A todos os professores do Curso Técnico em Eletroeletrônica, que foram importantes na nossa vida acadêmica e no desenvolvimento deste trabalho de conclusão.

AGRADECIMENTOS

A Deus, a fonte de toda força e sabedoria, por ter iluminado cada passo nesta jornada.

Aos meus familiares, pelo apoio incondicional, amor e por serem meu porto seguro durante toda a graduação. Cada incentivo de vocês foi essencial.

Aos professores do curso de Eletroeletrônica, pelo conhecimento compartilhado.

RESUMO

O presente Trabalho de Conclusão de Curso tem como objetivo apresentar o desenvolvimento e a aplicação de uma fechadura eletrônica voltada para o aumento da segurança residencial e comercial, utilizando tecnologias de automação e controle eletrônico. Diante do crescimento da criminalidade e da necessidade de sistemas de proteção mais eficientes, as fechaduras eletrônicas surgem como uma alternativa moderna às fechaduras mecânicas convencionais, oferecendo maior praticidade, controle de acesso e confiabilidade.

O trabalho aborda a evolução histórica dos sistemas de segurança, os principais tipos de fechaduras eletrônicas e as tecnologias empregadas, com destaque para sistemas de autenticação por RFID, senhas, biometria e aplicativos móveis. Também são apresentados os componentes eletrônicos utilizados no projeto, como microcontroladores Arduino, módulos RFID, relés, reguladores de tensão e travas elétricas, além da descrição do funcionamento do circuito eletrônico e do sistema de controle.

A metodologia utilizada baseia-se em pesquisa bibliográfica e no desenvolvimento prático de um protótipo funcional de fechadura eletrônica acionada por RFID, alimentada por fonte de 12 volts com regulador de tensão para 5 volts. Os resultados obtidos demonstram que o sistema desenvolvido apresenta funcionamento eficiente, baixo custo de implementação e potencial aplicação em residências, empresas e instituições de ensino.

Conclui-se que a utilização de fechaduras eletrônicas contribui significativamente para a modernização dos sistemas de segurança, proporcionando maior comodidade, controle e proteção aos usuários, além de demonstrar a importância da integração entre eletrônica, automação e tecnologia da informação no desenvolvimento de soluções inteligentes para a sociedade atual.

Palavras-chave: fechadura eletrônica; segurança residencial; RFID; Arduino.

ABSTRACT

This Course Conclusion Paper aims to present the development and application of an electronic lock focused on improving residential and commercial security through automation and electronic control technologies. Due to the increase in crime rates and the growing need for more efficient protection systems, electronic locks have become a modern alternative to conventional mechanical locks, offering greater practicality, access control, and reliability.

The study discusses the historical evolution of security systems, the main types of electronic locks, and the technologies involved, especially authentication systems using RFID, passwords, biometrics, and mobile applications. It also presents the electronic components used in the project, such as Arduino microcontrollers, RFID modules, relays, voltage regulators, and electric locks, in addition to describing the operation of the electronic circuit and the control system.

The methodology adopted is based on bibliographic research and the practical development of a functional electronic lock prototype activated by RFID, powered by a 12-volt supply with a 5-volt voltage regulator. The obtained results demonstrate that the developed system has efficient operation, low implementation cost, and potential application in homes, companies, and educational institutions.

It is concluded that the use of electronic locks contributes significantly to the modernization of security systems, providing greater convenience, control, and protection for users, while also demonstrating the importance of integrating electronics, automation, and information technology in the development of intelligent solutions for modern society.

Keywords: electronic lock; residential security; RFID; Arduino.

LISTA DE ILUSTRAÇÕES

Fig. 1 – Arduino Uno.....	29
Fig. 2 – Modulo RFID.....	30
Fig. 3 – Fechadura Solenóide.....	30
Fig. 4 – Módulo Buzzer.....	31
Fig. 5 – Regulador de Tensão.....	31
Fig. 6 – Testes componentes I.....	32
Fig. 7 – Testes componentes II.....	33
Fig. 8 – Testes componentes III.....	34
Fig. 9 – Confecção da porta.....	35
Fig. 10 – Pintura da porta.....	36
Fig. 11 – Porta pronta.....	36
Fig. 12 – Fixação da porta.....	37
Fig. 13 – Solda de componentes I.....	37
Fig. 14 – Solda de componentes II.....	38
Fig. 15 – Prototipo pronto frente.....	39
Fig. 16 – Protótipo visão lateral.....	40
Fig. 17 – Prototipo visão parte traseira.....	41
Fig. 18 – Protótipo visão traseira em funcionamento.....	42
Fig. 19 – Diagrama Eletroeletrônico.....	43

SUMÁRIO

1 INTRODUÇÃO – TEMA E PROBLEMATIZAÇÃO	9
2 JUSTIFICATIVA	10
3 OBJETIVOS	11
3.1 Geral	11
3.2 Específicos	11
4 METODOLOGIA DA PESQUISA	12
5 CRONOGRAMA	13
6 DESENVOLVIMENTO	16
6.1 Evolução dos Sistemas de Segurança Residencial e a Sensação de Insegurança	16
6.1.1 Evolução histórica dos sistemas de segurança residencial	16
6.1.2 Dados de segurança pública relacionados a residências	19
6.1.3 Relação entre criminalidade e evolução da segurança residencial	20
6.2 Conceitos de Fechaduras Eletrônicas	22
6.3 Desenvolvimento da Fechadura Eletrônica	28
6.3.1 Planejamento e seleção dos componentes do dispositivo	28
6.3.1.1 Arduino UNO	28
6.3.1.2 Módulo RFID	29
6.3.1.3 Fechadura Solenóide	30
6.3.1.4 Módulo Buzzer	30
6.3.1.5 Regulador de Tensão	31
6.3.2 Testes dos Componentes	32
6.3.3 Montagem do Dispositivo	35
6.3.4 Explicação do Funcionamento da Fechadura Eletrônica com RFID ...	43
6.3.4.1 Alimentação do Sistema	43
6.3.4.2 Comunicação entre RFID e Arduino	44
6.3.4.3 Acionamento do Relé	45
6.3.4.4 Acionamento da Fechadura Solenóide	45
6.3.4.5 Sequência Completa de Funcionamento	46
6.3.4.6 Programação Arduino	46
6.3.5 Comparativo de Custos entre uma Fechadura Eletrônica RFID	

Comercial e o Protótipo Desenvolvido	49
7 CONCLUSÃO	52
REFERÊNCIAS	53

1 - INTRODUÇÃO – TEMA E PROBLEMATIZAÇÃO

A segurança residencial é uma preocupação constante para os moradores de grande e pequenas cidades, e o avanço da tecnologia com a automação residencial e a internet das coisas ajudam a apresentar novas soluções para esta área.

Cerca de 60% dos domicílios tinham algum dispositivo de segurança. Esse percentual foi bem maior para os apartamentos (90,3%) do que para as casas (55,9%) e o mesmo ocorreu na área urbana (64,9%) em relação a rural (28,5%). A grade na janela/porta foi o dispositivo mais usado (35,7% dos domicílios), com destaque para o Centro-Oeste (40,5%). A grade predominava nas casas (35,6%), enquanto os dispositivos na porta (olho mágico, corrente e/ou interfone) estavam em 73,9% dos apartamentos (IBGE, 2021).

Com tecnologia, também é possível dar adeus às tradicionais chaves. O morador pode instalar uma fechadura digital com senha ou biometria a partir de R\$ 300.

Buscando apresentar a sociedade um novo equipamento de segurança para residências, este trabalho propõe o desenvolvimento de uma trava de segurança eletrônica, que visa o baixo custo de fabricação, utilizando princípios de eletroeletrônica incorporados durante o curso.

2 - JUSTIFICATIVA

A segurança patrimonial e pessoal tem se tornado uma preocupação crescente na sociedade contemporânea, especialmente diante do aumento da urbanização e da incidência de furtos e invasões. Nesse contexto, os sistemas tradicionais de segurança, como fechaduras mecânicas convencionais, vêm se mostrando cada vez mais vulneráveis a técnicas de arrombamento e à perda ou duplicação de chaves físicas.

A trava de segurança eletrônica surge como uma solução inovadora, alinhada às demandas atuais de praticidade, confiabilidade e controle de acesso. Esse tipo de tecnologia possibilita maior segurança por meio de métodos de autenticação diferenciados, como senhas, cartões de proximidade, biometria ou integração com dispositivos móveis. Além disso, oferece funcionalidades adicionais, como registros de acesso e possibilidade de integração a sistemas de automação residencial.

Portanto, desenvolver e estudar um protótipo de fechadura eletrônica justifica-se pela necessidade de propor alternativas acessíveis e eficientes para reforçar a segurança em ambientes residenciais, comerciais e institucionais. Além de contribuir para o avanço tecnológico no setor, o projeto também promove a aplicação prática de conhecimentos adquiridos durante a formação acadêmica, integrando conceitos de eletroeletrônica, programação e sistemas de controle.

3 - OBJETIVOS

3.1 GERAL

Desenvolver uma trava de segurança eletrônica funcional, que ofereça maior proteção, praticidade e confiabilidade em relação às fechaduras mecânicas convencionais, aplicando conceitos de eletroeletrônica e automação.

3.2 ESPECÍFICOS

- Pesquisar os principais tipos de sistemas de travas eletrônicas disponíveis no mercado e suas aplicações;
- Projetar o circuito eletrônico adequado para o funcionamento da trava de segurança;
- Implementar o sistema de controle utilizando senha digital/cartão de proximidade/biometria (dependendo da sua escolha de tecnologia);
- Realizar testes de funcionamento para avaliar eficiência, confiabilidade e tempo de resposta da trava;
- Analisar o custo-benefício do protótipo em comparação a sistemas tradicionais e comerciais de segurança;
- Documentar o desenvolvimento do projeto, integrando teoria e prática para aplicação em ambientes residenciais ou comerciais.

4 - METODOLOGIA DA PESQUISA

O desenvolvimento do trabalho será realizado por meio de pesquisa aplicada, de caráter **experimental** e **descritivo**, buscando unir fundamentação teórica e prática, seguindo padrões determinados pela ABNT NBR 14724:2024 . O processo será dividido em etapas:

1. Levantamento bibliográfico

- Pesquisa em livros, artigos científicos, normas técnicas e fontes digitais sobre sistemas de travas eletrônicas, princípios de segurança, componentes eletrônicos e microcontroladores aplicados ao controle de acesso.

2. Estudo de viabilidade

- Definição dos critérios de segurança, praticidade e custo.
- Escolha da tecnologia de autenticação (senha numérica, RFID, biometria etc.) mais adequada ao contexto do projeto.

3. Projeto e desenvolvimento

- Elaboração do esquema elétrico e seleção dos componentes (microcontrolador, sensores, atuadores, fonte de alimentação e mecanismos de travamento).
- Montagem do protótipo em bancada.
- Programação do sistema de controle.

4. Testes e validação

- Realização de ensaios de funcionamento, verificando abertura/fechamento, tempo de resposta, confiabilidade e consumo de energia.
- Identificação de possíveis falhas e ajustes no protótipo.

Canvas(apre s.)					>14								Cada Equipe	
Apresentaçã o Do escopo					>28								Todos	
Revisão final					>05								Todos	
PLANEJAMENTO DE TCC							DESENVOLVIMENTO DE TCC							
Descrição	JUL/ 25	AG O	SE T	OU T	NO V	DE Z	FEV/2 6	MA R	AB R	MAI	JU N	JU L	Responsá vel	
Reinício							> 05							
Revisão das equipes e temas e RESUMOS							>14						Todos	
Follow up1								>07					Por grupo	
Montagem Simulação testes									>04	>08			Todos	
Mostra TCC BANNER													Todos	
Follow up 2								>21					Por grupo	
Follow up 3										>15				
Fup parte escrita									> 24				Por grupo	
Pré-											>09		Todos	

apresentaçã o													
Revisão final parte escrita											>16		Por grupo
Apresentaçã o do TCC (Auditorio)											> 23		Todos
Revisão final											>30		Todos

6 - DESENVOLVIMENTO

6.1 - Evolução dos Sistemas de Segurança Residencial e a Sensação de Insegurança

A segurança residencial, ao longo da história, consolidou-se como um dos pilares fundamentais da organização social, estando diretamente relacionada à preservação da vida, do patrimônio e da privacidade dos indivíduos. No contexto contemporâneo, essa temática adquire maior relevância diante do crescimento urbano, das transformações tecnológicas e das mudanças nas dinâmicas sociais.

A residência, antes percebida como um ambiente naturalmente seguro, passa a ser objeto de constante adaptação frente às novas ameaças e à crescente sensação de insegurança que permeia a sociedade. A acalentada "segurança" do lar é, em parte, uma segurança literal em relação ao medo físico (JACOBS, 2011).

A segurança residencial, ao longo da história, consolidou-se como um dos pilares fundamentais da organização social, estando diretamente relacionada à preservação da vida, do patrimônio e da privacidade dos indivíduos. No contexto contemporâneo, essa temática adquire maior relevância diante do crescimento urbano, das transformações tecnológicas e das mudanças nas dinâmicas sociais. A residência, antes percebida como um ambiente naturalmente seguro, passa a ser objeto de constante adaptação frente às novas ameaças e à crescente sensação de insegurança que permeia a sociedade.

6.1.1 - Evolução histórica dos sistemas de segurança residencial

Inicialmente, os sistemas de proteção residencial eram marcados pela simplicidade e pela dependência de mecanismos naturais de vigilância social. Em comunidades tradicionais, a proximidade entre os indivíduos e o forte senso de pertencimento coletivo funcionava como importantes fatores de prevenção à criminalidade. Nesse cenário, os recursos de segurança restringiam-se a elementos básicos, como portas reforçadas, trancas rudimentares e barreiras físicas simples. A eficácia desses mecanismos estava diretamente associada ao contexto social, no qual o controle informal exercido pela comunidade desempenhava papel essencial.

Com a transição para sociedades urbanizadas, especialmente a partir do século XIX, observa-se uma mudança significativa nesse paradigma. A expansão das cidades, impulsionada pela industrialização, resultou em maior densidade populacional e na

diversificação dos perfis sociais. Esse processo contribuiu para o enfraquecimento das relações comunitárias e para o aumento da desigualdade social, fatores que, combinados, favoreceram o crescimento da criminalidade. Nesse contexto, a segurança residencial passa a demandar soluções mais estruturadas e tecnicamente elaboradas.

Também estão enraizadas na tematização reacionária da “pós-modernidade”, produzida não apenas pelo crime, mas por toda a corrente reacionária cultural e política que caracteriza o presente em termos de colapso moral, de incivilidade, e do declínio da família, exortando a reversão da revolução dos anos 1960 e do movimento de liberação cultural e política que ela deslanchou. A sociedade porosa, móvel, aberta, de estranhos, da pós-modernidade deu causa a práticas de controle do crime que buscam tornar a sociedade menos aberta e menos móvel: fixar identidades, imobilizar os indivíduos, colocar em quarentena setores da população, erguer fronteiras, fechar acessos. Se estas estratégias não são absolutamente determinadas pelo campo social que descrevi, elas são fortemente condicionadas por tal campo e provavelmente inconcebíveis sem ele (GARLAND, 2008).

O desenvolvimento de novos materiais e técnicas construtivas possibilitou a introdução de dispositivos mais resistentes e eficazes. Fechaduras metálicas com sistemas de chave mais complexos, portões reforçados e grades de proteção tornaram-se elementos comuns nas residências urbanas. Posteriormente, com o avanço da eletrificação, surgem os primeiros sistemas de alarme, capazes de emitir sinais sonoros em situações de invasão. Esses dispositivos representam um marco importante na evolução da segurança, pois introduzem o conceito de resposta ativa a eventos suspeitos.

A partir da segunda metade do século XX, o progresso tecnológico promoveu uma verdadeira revolução nos sistemas de segurança residencial. A incorporação da eletrônica e da automação permitiu o desenvolvimento de soluções mais sofisticadas, como sensores de movimento, detectores de abertura de portas e janelas, além de sistemas de monitoramento por câmeras. O circuito fechado de televisão (CFTV) passa a desempenhar papel central na vigilância, possibilitando o registro e o acompanhamento de atividades em tempo real.

Esse é o paradoxo de nosso mundo saturado de dispositivos de vigilância, quaisquer que sejam seus pretensos propósitos: de um lado, estamos mais protegidos da insegurança que qualquer geração anterior; de outro, porém, nenhuma geração anterior, pré-eletrônica, vivenciou os sentimentos de insegurança como experiência de todos os dias (BAUMAN, 2009).

No início do século XXI, com a popularização da internet e o avanço das tecnologias digitais, a segurança residencial atinge um novo patamar. A integração de dispositivos por meio de redes de comunicação possibilita o surgimento de sistemas inteligentes, capazes de operar de forma autônoma e interconectada. A Internet das Coisas (IoT) permite que diferentes equipamentos — como câmeras, alarmes, sensores e fechaduras — sejam controlados remotamente por meio de smartphones e computadores, ampliando significativamente o nível de controle dos usuários sobre suas residências.

A Internet das Coisas, em poucas palavras, nada mais é que uma extensão da Internet atual, que proporciona aos objetos do dia-a-dia (quaisquer que sejam), mas com capacidade computacional e de comunicação, se conectarem à Internet. A conexão com a rede mundial de computadores viabilizará, primeiro, controlar remotamente os objetos e, segundo, permitir que os próprios objetos sejam acessados como provedores de serviços (SANTOS, 2016).

Além disso, tecnologias baseadas em identificação biométrica, como leitura de impressões digitais e reconhecimento facial, vêm sendo amplamente incorporadas aos sistemas de segurança. Esses recursos aumentam a confiabilidade no controle de acesso, reduzindo a dependência de chaves físicas e minimizando riscos associados a perdas ou cópias indevidas. Paralelamente, o uso de inteligência artificial começa a ser explorado na análise de imagens e no reconhecimento de padrões, permitindo a identificação de comportamentos suspeitos de forma automatizada.

Outro aspecto relevante na evolução da segurança residencial diz respeito à integração com sistemas de segurança pública e privada. Empresas de monitoramento oferecem serviços contínuos, nos quais sinais de alarme são transmitidos para centrais de controle, possibilitando respostas rápidas em situações de emergência. Essa integração reforça a ideia de que a segurança residencial não

depende apenas de dispositivos instalados localmente, mas também de redes de apoio externas.

6.1.2 - Dados de segurança pública relacionados a residências

A análise da segurança residencial no Brasil deve considerar os dados de segurança pública, especialmente os crimes patrimoniais, como roubos e furtos. Esses delitos possuem impacto direto na percepção de insegurança, pois atingem o cotidiano da população e o espaço doméstico.

Segundo dados do Instituto Brasileiro de Geografia e Estatística (IBGE, 2021), aproximadamente 2,0% dos domicílios brasileiros tiveram ao menos um morador vítima de roubo em um período de 12 meses, o que representa cerca de 1,5 milhão de residências afetadas. Dentre esses casos, cerca de **11,3%** ocorreram dentro do próprio domicílio, evidenciando que o ambiente residencial não está imune à ação criminosa .

Além disso, dados mais recentes da segurança pública indicam que os crimes contra residências continuam sendo relevantes. No estado de São Paulo, por exemplo, foram registrados aproximadamente 31 mil casos de roubos e furtos a residências em um único ano, sendo a maioria furtos (cerca de 29 mil) e cerca de 1,9 mil roubos, caracterizados pelo uso de violência ou ameaça . Apesar de uma redução de aproximadamente 27% em relação ao período anterior, os números ainda demonstram a frequência desses crimes.

De acordo com Fernando Capez (2023), o crime de roubo diferencia-se do furto pelo emprego de violência ou grave ameaça contra a vítima, enquanto no furto ocorre apenas a subtração do bem sem contato violento. Essa distinção é relevante, pois os roubos tendem a gerar maior impacto psicológico e aumentar significativamente a sensação de insegurança.

No âmbito nacional, dados do Anuário Brasileiro de Segurança Pública indicam que o Brasil ainda registra milhões de ocorrências de crimes patrimoniais anualmente, incluindo roubos e furtos de diferentes naturezas . Mesmo com a tendência de queda em alguns indicadores, os números absolutos permanecem elevados, reforçando a necessidade de medidas de proteção.

Outro aspecto relevante é a tendência de redução de determinados crimes. Em alguns estados, como São Paulo, os roubos apresentaram queda significativa ao

longo dos últimos anos, com reduções superiores a 50% quando comparados a períodos anteriores. Ainda assim, a percepção de insegurança permanece elevada, indicando que a sensação de risco não depende exclusivamente dos dados estatísticos.

6.1.3 - Relação entre criminalidade e evolução da segurança residencial

A evolução dos sistemas de segurança residencial está diretamente relacionada ao comportamento da criminalidade. O aumento dos crimes patrimoniais, especialmente roubos e furtos, impulsionou o desenvolvimento de tecnologias mais avançadas de proteção. Dispositivos como câmeras, alarmes, cercas elétricas e sistemas de monitoramento remoto tornaram-se cada vez mais comuns nas residências brasileiras.

Dados do Fórum Brasileiro de Segurança Pública (2025) demonstram que a incidência de crimes patrimoniais tem incentivado investimentos em sistemas eletrônicos de segurança residencial, como alarmes, monitoramento remoto e fechaduras eletrônicas.

Além disso, observa-se uma mudança no conceito de moradia, que passa a incorporar características de proteção intensiva, como muros altos, portões automatizados e sistemas integrados de vigilância. Esse fenômeno reflete não apenas a necessidade de segurança, mas também a crescente percepção de insegurança por parte da população.

Entretanto, mesmo com a redução de alguns índices de criminalidade, a sensação de insegurança permanece elevada. Isso pode ser explicado por fatores como a ampla divulgação de crimes pela mídia, a experiência pessoal ou indireta com a violência e a desconfiança nas instituições de segurança pública.

Outro fator relevante é a desigualdade social, que influencia diretamente a distribuição da criminalidade. Regiões com menor acesso a recursos e políticas públicas tendem a apresentar maior vulnerabilidade, enquanto áreas com maior poder aquisitivo investem mais em sistemas de segurança privada, ampliando as diferenças na proteção residencial.

A análise da evolução dos sistemas de segurança residencial, associada aos dados de segurança pública, evidencia a complexidade do fenômeno da insegurança. Embora haja avanços tecnológicos significativos e redução em alguns indicadores

de criminalidade, os crimes contra o patrimônio, especialmente roubos e furtos em residências, continuam sendo um problema relevante no Brasil.

Dessa forma, a segurança residencial deve ser compreendida como resultado da interação entre fatores tecnológicos, sociais e institucionais. A adoção de sistemas de proteção é uma resposta direta à criminalidade, mas também à percepção de risco construída socialmente. Para que haja uma efetiva melhoria na sensação de segurança, é necessário não apenas investir em tecnologia, mas também fortalecer políticas públicas, reduzir desigualdades e promover maior integração social.

6.2 - CONCEITOS DE FECHADURAS ELETRÔNICAS

As fechaduras eletrônicas constituem uma importante evolução tecnológica no contexto dos sistemas de segurança e controle de acesso, representando uma alternativa moderna e eficiente às fechaduras mecânicas tradicionais. Com o avanço da eletrônica, da informática e das telecomunicações, esses dispositivos passaram a incorporar múltiplas funcionalidades, ampliando não apenas o nível de segurança, mas também a praticidade e a capacidade de gerenciamento de acessos em diferentes ambientes.

De forma conceitual, as fechaduras eletrônicas podem ser definidas como sistemas eletromecânicos que utilizam sinais elétricos e lógicos para controlar o travamento e destravamento de portas ou acessos físicos. Diferentemente das fechaduras convencionais, que dependem exclusivamente de uma chave física, esses dispositivos operam com base em credenciais digitais previamente cadastradas, permitindo maior flexibilidade e controle sobre os usuários autorizados.

Uma fechadura eletrônica é um sistema microcontrolado que, por meio de um teclado alfanumérico, RFID, *Near Field Communication* (NFC), Bluetooth, Internet e vários outros meios de entrada de informação, pode gerenciar a abertura de uma porta. Após receber a senha do usuário, o microcontrolador faz uma verificação para validá-la e, caso esteja correta, envia um sinal para o sistema de trava eletrônica instalado na porta para que ela seja aberta (KOCIOLEK; KLEMBBA, 2017).

Ou seja, o princípio de funcionamento das fechaduras eletrônicas está fundamentado em um processo de autenticação e validação de dados. Inicialmente, o usuário fornece uma credencial ao sistema, que pode assumir diferentes formas, como um código numérico, um cartão eletrônico, uma característica biométrica ou um comando remoto. Essa informação é capturada por um dispositivo de entrada e encaminhada a um microcontrolador, responsável por processar os dados e compará-los com as informações armazenadas em sua memória interna. Caso a credencial seja validada, o sistema envia um sinal elétrico ao atuador, que realiza o destravamento da fechadura. Em caso de falha na autenticação, o acesso é automaticamente negado, podendo inclusive acionar mecanismos adicionais de segurança, como alarmes ou bloqueios temporários.

Além do processo básico de validação, muitos sistemas modernos incorporam camadas adicionais de segurança, como criptografia de dados, autenticação em múltiplos fatores e registros de acesso (logs), permitindo rastrear entradas e saídas em tempo real. Tais recursos são especialmente relevantes em ambientes corporativos e industriais, onde o controle rigoroso de acesso é essencial. A segurança eficaz não depende de uma única barreira, mas de uma série de defesas redundantes que protegem o ativo (STALLINGS, 2018).

No que se refere aos métodos de autenticação, observa-se uma diversidade de tecnologias aplicadas. A autenticação por senha é uma das mais difundidas, caracterizando-se pela inserção de um código numérico em um teclado digital. Embora seja prática e de baixo custo, sua eficácia depende diretamente da complexidade da senha e do comportamento do usuário. Já a tecnologia RFID (Radio Frequency Identification) permite a identificação sem contato físico, utilizando cartões ou tags que transmitem dados por radiofrequência ao leitor .

A identificação por radiofrequência, ou RFID, é um termo genérico para designar tecnologias que empregam ondas de rádio para identificar automaticamente pessoas ou objetos. Ela vem como complemento a outras tecnologias de identificação automática, como o código de barras, leitor ótico de caracteres e algumas tecnologias biométricas, como o escaneamento de retina, que tem sido usadas para economizar tempo e esforço necessários para a obtenção manual de dados e melhorar sua precisão. A tecnologia de RFID permite que um leitor receba informações de uma etiqueta (tag) e as transmita para um sistema de computação, sem que pessoas se envolvam, otimizando diversos processos, desde checkout em super mercados a controle de qualidade na fabricação de peças. Esta tecnologia aparentemente nova e revolucionária tem suas origens, surpreendentemente, no século XIX, e vem evoluindo até os dias de hoje. Não obstante a manutenção de princípios relativamente simples, ela vem se aperfeiçoando e conquistando cada vez mais espaço; ganhando compreensão quanto aos benefícios de seu uso. Tags RFID tornam-se cada vez mais baratas e presentes em nossas vidas; o que traz tanto comodidades e benefícios (HWANG, 2013).

A biometria, por sua vez, representa um avanço significativo em termos de segurança, pois utiliza características físicas únicas do indivíduo, como impressões digitais, reconhecimento facial ou leitura da íris. Essa abordagem reduz

significativamente o risco de fraudes, uma vez que tais características são praticamente impossíveis de serem replicadas com precisão.

Na atualidade, essa noção de que os corpos possuem uma “senha natural” e as novas conexões que estabelece parece mobilizar uma enormidade de transformações, sentidos e significados característicos do contemporâneo. A ideia que serviu de estopim para os questionamentos aqui presentes foi anunciada na imprensa, e em outros espaços, como um desenvolvimento tecnológico que traria facilidade e segurança para o cotidiano: os equipamentos biométricos de identificação (KANASHIRO, 2011).

Por fim, destaca-se a autenticação por aplicativos móveis, que permite o controle remoto das fechaduras por meio de smartphones. Essa tecnologia está diretamente associada ao conceito de Internet das Coisas (IoT), possibilitando a integração com outros dispositivos inteligentes e sistemas de automação residencial. Dessa forma, o usuário pode monitorar e controlar o acesso mesmo à distância, aumentando o nível de conveniência e segurança.

Segundo Carrion e Quaresma (2019), a interconexão de dispositivos físicos com capacidades computacionais de detecção e comunicação de dados não é uma concepção nova, porém a compreensão da real aplicabilidade de uma Internet das Coisas (*Internet of Things*, ou IoT) ainda é incipiente. A Internet das Coisas descreve o que se observa hoje com o crescente número de dispositivos conectados habilitados à internet. Isto é, um estado onde “coisas”, de pequenos objetos a ambientes e cidades, veem-se capacitados a se comunicar uns com os outros, e consequentemente com os humanos presentes no ecossistema.

O funcionamento eficiente das fechaduras eletrônicas depende da integração harmoniosa entre diferentes componentes eletrônicos e tecnologias digitais, que atuam em conjunto para realizar o controle de acesso de forma segura e confiável.

Os sensores são responsáveis pela captura das informações necessárias para o processo de autenticação. Entre os principais tipos, destacam-se os sensores biométricos, amplamente utilizados em sistemas de reconhecimento de impressão digital, e os sensores magnéticos, que têm a função de detectar o estado físico da porta, indicando se ela se encontra aberta ou fechada. Esses sensores contribuem significativamente para a automação e monitoramento do sistema.

O microcontrolador é considerado o “cérebro” do sistema, sendo responsável por executar as instruções programadas, processar os dados recebidos e tomar decisões com base nas informações armazenadas. Plataformas como o Arduino são frequentemente utilizadas em projetos acadêmicos e protótipos devido à sua acessibilidade, facilidade de programação e ampla documentação disponível. Esses dispositivos permitem o desenvolvimento de sistemas personalizados de controle de acesso com relativa simplicidade.

Um Arduino é um microcontrolador de placa única e um conjunto de software para programá-lo. O hardware consiste em um projeto simples de hardware livre para o controlador, com um processador Atmel AVR e suporte embutido de entrada/saída. O software consiste de uma linguagem de programação padrão e do bootloader que roda na placa (MCROBERTS, 2011).

Os atuadores são dispositivos acionados eletricamente que controlam uma variável física (TOCCI; WIDMER; MOSS, 2011). Os solenoides são amplamente utilizados nesse contexto, pois convertem energia elétrica em movimento mecânico linear, permitindo o acionamento do mecanismo de bloqueio. Motores elétricos também podem ser empregados, especialmente em sistemas mais complexos, nos quais é necessário realizar movimentos rotacionais ou ajustes mais precisos.

Outro aspecto relevante diz respeito às tecnologias de comunicação utilizadas nas fechaduras eletrônicas modernas. O Bluetooth é frequentemente utilizado para comunicação de curto alcance, permitindo a interação direta com smartphones. Já o Wi-Fi possibilita o acesso remoto via internet, sendo essencial em sistemas de automação residencial e controle à distância. A tecnologia RFID, por sua vez, destaca-se pela praticidade e rapidez na autenticação, sendo amplamente empregada em ambientes corporativos, acadêmicos e residenciais (KLAUS; EFRON, 2017).

Além dessas tecnologias, é importante mencionar o uso de protocolos de segurança digital, como criptografia e autenticação segura, que visam proteger os dados transmitidos e evitar acessos indevidos. A integração entre hardware e software é, portanto, fundamental para garantir a confiabilidade do sistema como um todo.

As fechaduras eletrônicas podem ser classificadas de acordo com o tipo de tecnologia empregada e o método de autenticação adotado, apresentando diferentes características, níveis de segurança e aplicações específicas.

A fechadura digital com senha é uma das soluções mais simples e populares. Nesse modelo, o acesso é liberado mediante a inserção de um código numérico previamente cadastrado. Sua principal vantagem reside na praticidade e no baixo custo de implementação. No entanto, a segurança pode ser comprometida caso a senha seja compartilhada ou facilmente descoberta, sendo recomendável a adoção de códigos complexos e sua atualização periódica (STALLINGS, 2018).

A fechadura biométrica destaca-se como uma das opções mais seguras disponíveis atualmente. Ao utilizar características únicas do usuário, como a impressão digital, esse sistema praticamente elimina o risco de acesso não autorizado por terceiros. Além disso, dispensa o uso de chaves ou cartões, reduzindo problemas relacionados à perda ou roubo desses itens (JAIN; FLYNN; ROSS, 2008).

A fechadura com cartão ou tag RFID é amplamente utilizada em ambientes corporativos, hotéis e instituições de ensino. Nesse sistema, o acesso é realizado por meio da aproximação de um dispositivo eletrônico ao leitor, permitindo uma autenticação rápida e eficiente. Uma de suas principais vantagens é a facilidade de gerenciamento, pois cartões podem ser facilmente cadastrados ou desativados conforme a necessidade.

A sigla RFID vem do inglês *Radio Frequency Identification*, que significa Identificação por Radiofrequência. Esta tecnologia é composta por três componentes, que são: antena, responsável por transmitir as ondas de rádio; *transceiver* (transmissor/receptor), responsável por gerar os sinais de rádio para a comunicação; e *transponder* (comumente chamada de *tag* RFID), composta também por uma antena e um microchip, onde são armazenados os seus dados. As *tags* RFID podem ser do tipo leitura ou leitura e escrita, onde a primeira possuem dados gravados de fábrica em seus microchips, e que não podem ser alterados, enquanto que a segunda pode ter seus dados alterados, através de um processo de escrita (FREITAS, 2020).

Por fim, as fechaduras inteligentes, ou *smart locks*, representam o estado mais avançado dessa tecnologia. Integradas a sistemas de automação residencial (IoT),

essas fechaduras permitem o controle remoto via aplicativos móveis, além de oferecer funcionalidades como registro de acessos, notificações em tempo real e integração com assistentes virtuais. Essa tecnologia reflete a crescente tendência de digitalização e conectividade dos ambientes residenciais, proporcionando maior conforto, segurança e controle ao usuário.

6.3 - Desenvolvimento da Fechadura Eletrônica

Abordaremos neste capítulo as etapas que foram executadas para desenvolver o equipamento proposto. A concepção deste projeto executara a seqüência de cada tarefa, conforme desenvolvimento abaixo:

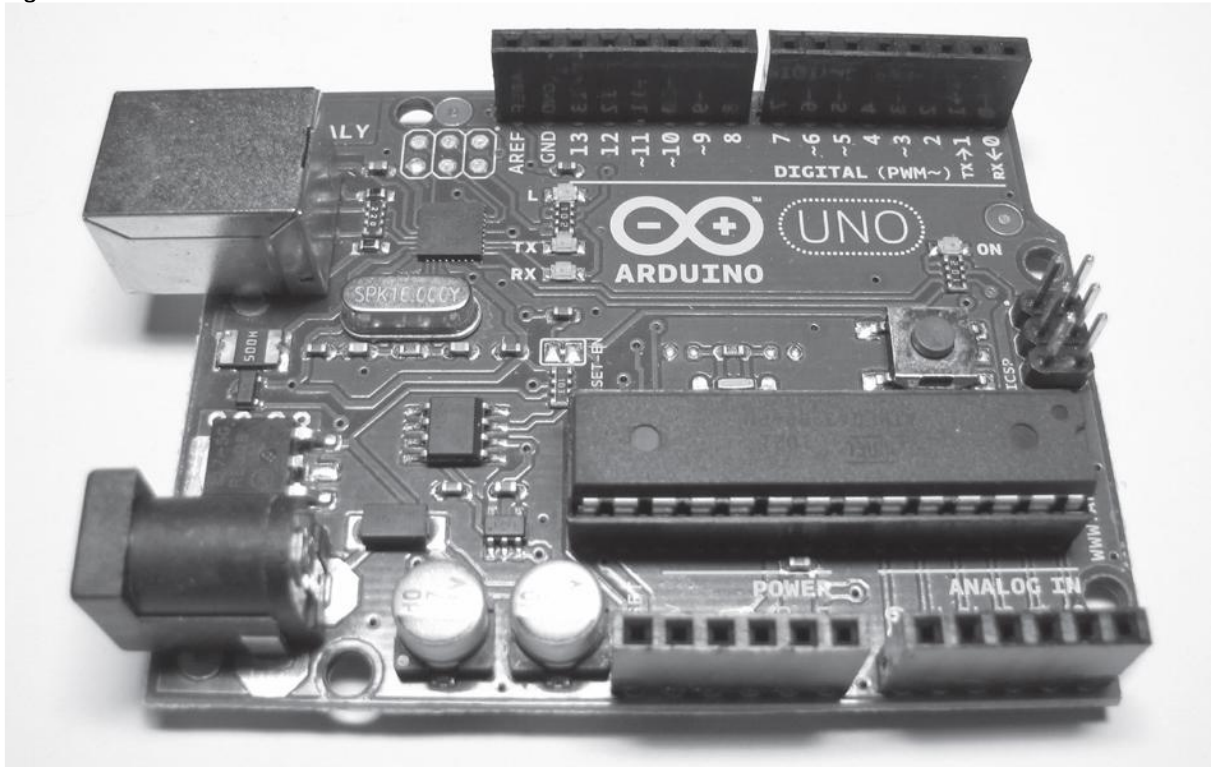
6.3.1 - Planejamento e seleção dos componentes do dispositivo

Foi preciso definir os componentes de hardware que foram empregados nesse protótipo. Para a fechadura esta sendo realizado um estudo para definir qual a melhor fechadura eletrônica que se encaixa com o projeto. Pontos que estão sendo considerados para analisar as fechaduras são: custo da fechadura, voltagem de alimentação, tempo de resposta. Após o estudo da fechadura ser realizado, um rele adequado foi definido para a passagem de voltagem para a mesma, assim como regulador de voltagem e outros componentes elétricos e eletrônicos.

6.3.1.1 - Arduino UNO (R\$ 21,00)

O Arduino UNO é uma placa de desenvolvimento baseada no microcontrolador ATmega328P, projetada para facilitar a criação de protótipos eletrônicos e sistemas embarcados. A plataforma dispõe de entradas e saídas digitais e analógicas, permitindo a integração com sensores, atuadores e dispositivos de comunicação. Sua arquitetura aberta e facilidade de programação tornam o Arduino UNO uma das ferramentas mais utilizadas em projetos educacionais, industriais e de pesquisa tecnológica. (Arduino, 2026).

Fig. 1 – Arduino Uno



Fonte: Google Imagens

6.3.1.2 - Módulo RFID (R\$13,00)

Zhu, Mukhopadhyay e Kurata (2012) explicam que a tecnologia RFID é um composto de um leitor de rádio frequência ligado a um sistema de computador. O *tag* é a parte que coleta de dados em tempo real e em seguida, os transmite via ondas de rádio. As etiquetas são compostas por duas partes: um pequeno chip e uma antena. O chip é utilizado para armazenar e processar os dados, enquanto a antena serve para receber e transmitir a informação.

Fig. 2 – Modulo RFID

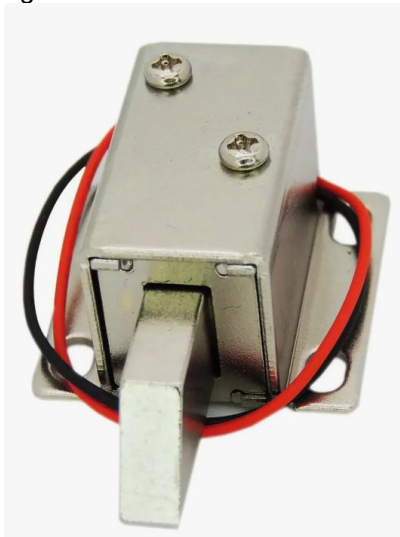


Fonte: Google Imagens

6.3.1.3 - Fechadura Solenóide (R\$19,00)

A fechadura solenoide é um tipo de fechadura eletrônica que utiliza um solenoide, um dispositivo eletromagnético para travar ou destravar portas, portões, gavetas ou armários. É uma solução comum em sistemas de controle de acesso devido à sua discrição e integração com outros dispositivos de segurança (PPA, 2025).

Fig. 3 – Fechadura Solenóide



Fonte: Google Imagens

6.3.1.4 - Módulo Buzzer (R\$5,00)

Os buzzers são dispositivos eletroacústicos que convertem sinais elétricos em ondas sonoras audíveis. Eles são amplamente utilizados para emitir alertas, notificações ou sinais sonoros em uma variedade de dispositivos eletrônicos e sistemas. Esses dispositivos geralmente produzem um som característico, como um zumbido ou

um tom, dependendo do tipo e da aplicação específica. Os buzzers são encontrados em uma variedade de formas e tamanhos, desde pequenos componentes discretos até unidades integradas em dispositivos eletrônicos complexos (MAKERHERO, s.d.).

Fig. 4 – Módulo Buzzer

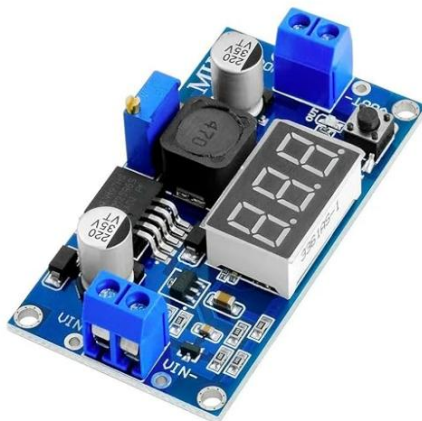


Fonte: Google Imagens

6.3.1.5 - Regulador de Tensão (R\$18,00)

Os reguladores de tensão funcionam controlando a diferença de potencial entre a entrada e a saída do circuito. Eles geralmente utilizam um dispositivo semicondutor, como um transistor, em conjunto com resistores e capacitores, para ajustar a tensão de saída conforme necessário. Quando a tensão de entrada varia, o regulador de tensão ajusta automaticamente sua operação para manter a tensão de saída constante (MAKERHERO, 2026).

Fig. 5 – Regulador de Tensão

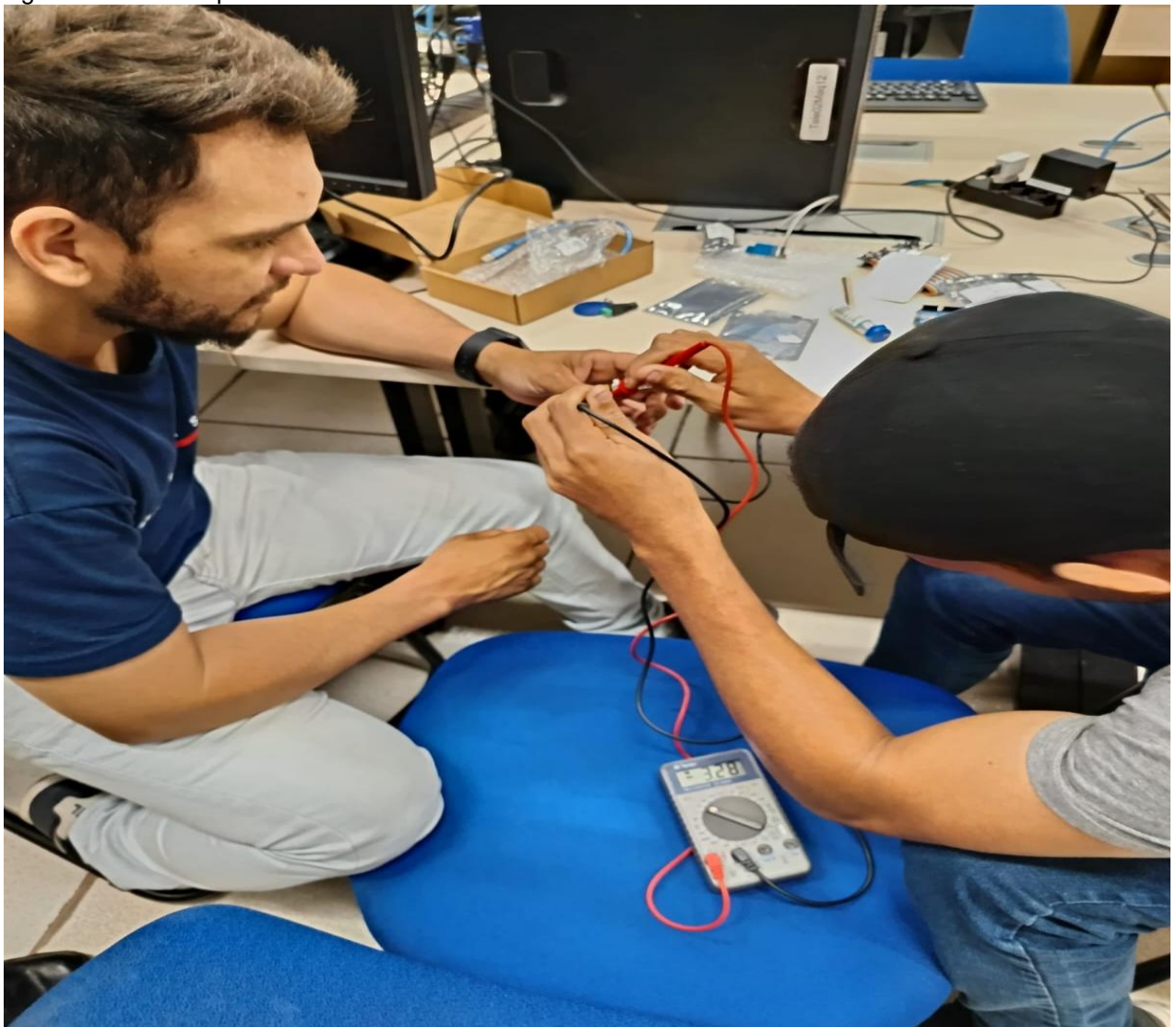


Fonte: Google Imagens

6.3.2 - Testes dos componentes

Apos seleccionar os materiais usados para construir o protótipo, cada componente foi testado para verificar se estão funcionando corretamente. Nesta fase, os componentes elétricos precisam ser analisados para verificar se não estão danificados de alguma forma. Para fazer isso, é necessário verificar se o circuito esta funcionando corretamente, mostrando a corrente e a tensão necessária em cada extremidade, e se as conexões elétricas presentes em cada dispositivo estão boas.

Fig. 6 – Testes componentes I



Fonte: Dos autores

Fig.7 – Testes componentes II



Fonte: Dos autores

Fig.8 – Testes componentes III



Fonte: Dos autores

6.3.3 - Montagem do Dispositivo

Apos as verificações dos materiais usados para o dispositivo, a próxima etapa é montar o dispositivo de fechadura eletrônica que esta sendo proposto. Para realizar a montagem é preciso selecionar onde foram alocados cada componente, para que todas as conexões necessárias entre esses elementos possam ser realizadas e assim a fechadura funcione de forma satisfatória.

Fig. 9 – Confeção da porta



Fonte: Dos autores

Fig.10 – Pintura da porta



Fonte: Dos autores

c



Fonte: Dos autores

Fig.12 – Fixação da porta



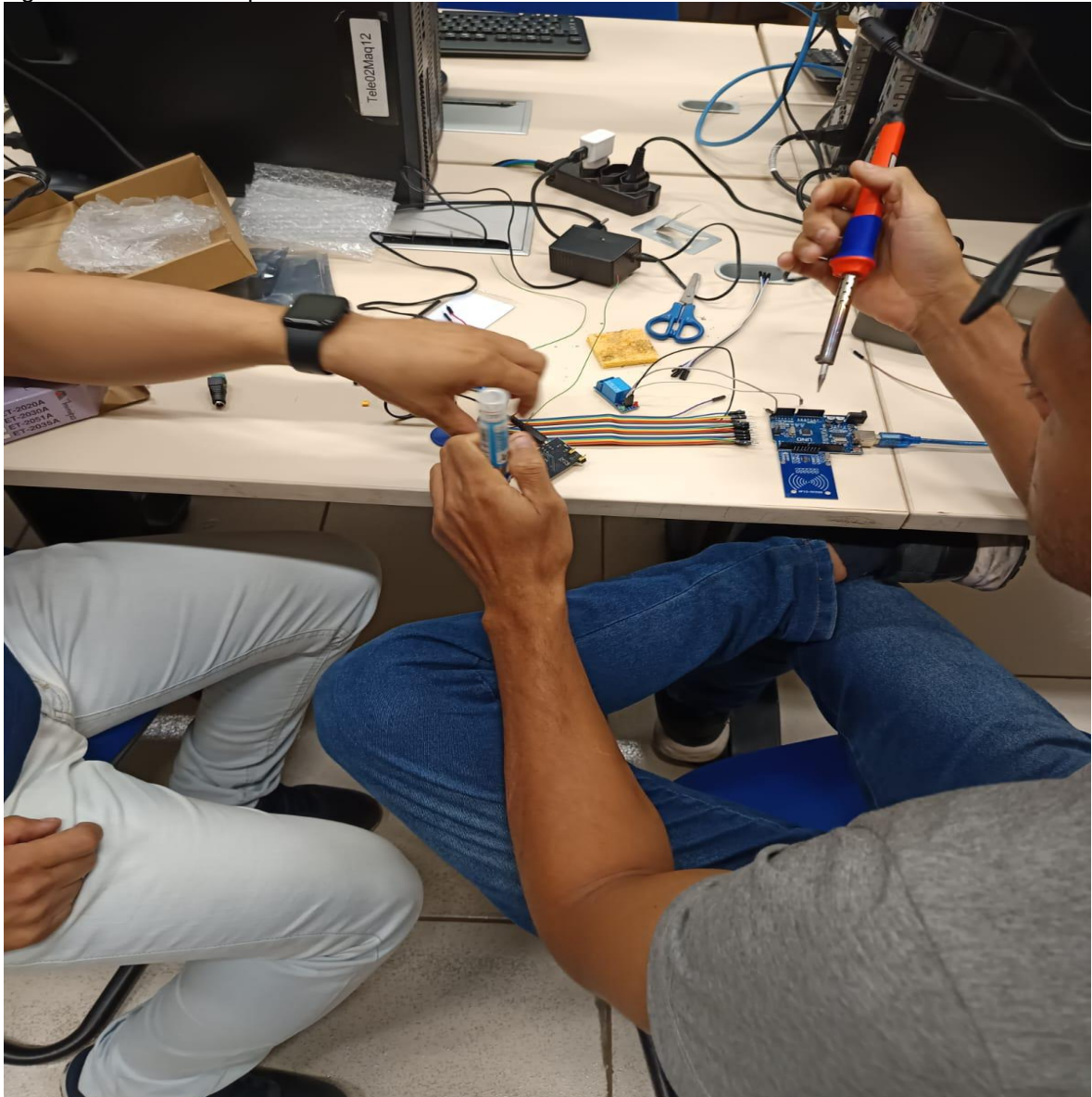
Fonte: Dos autores

Fig.13 – Solda de componentes I



Fonte: Dos autores

Fig.14 – Solda de componentes II



Fonte: Dos autores

Fig. 15 – Prototipo pronto frente



Fonte: Dos autores

Fig. 16 – Protótipo visão lateral



Fonte: Dos autores

Fig. 17 – Prototipo visão parte traseira



Fonte: Dos autores

Fig. 18 – Protótipo visão traseira em funcionamento

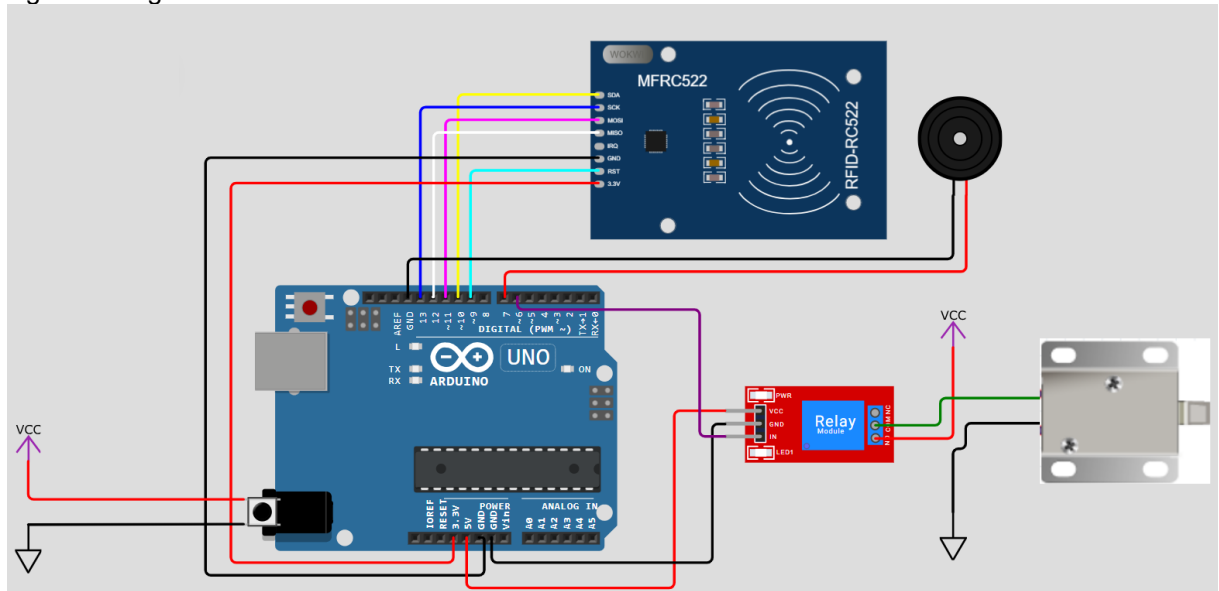


Fonte: Dos autores

6.3.4 - Explicação do funcionamento da fechadura eletrônica com RFID

O sistema é composto por cinco blocos principais: fonte de alimentação, regulador de tensão, Arduino Uno, módulo RFID RC522 e fechadura solenoide acionada por relé, conforme o esquema do diagrama abaixo.

Fig.19 – Diagrama Eletroeletrônico



Fonte: Ferramenta WOWKI

6.3.4.1 - Alimentação do sistema

A alimentação principal é fornecida por uma fonte de 12 Vcc.

A saída da fonte possui duas funções:

1. Alimentar diretamente a fechadura solenoide de 12 V.
2. Alimentar o regulador de tensão LM2596, que reduz os 12 V para 10 V.

Regulador LM2596

O módulo LM2596 recebe:

- IN+ → +12 V da fonte
- IN- → GND da fonte

E fornece:

- OUT+ → 5 V para o Arduino
- OUT- → GND do Arduino

Dessa forma, o Arduino recebe uma tensão adequada para seu funcionamento sem ser exposto aos 12 V direto da fonte.

6.3.4.2 - Comunicação entre RFID e Arduino

O módulo RFID RC522 utiliza comunicação SPI (Serial Peripheral Interface).

As conexões são:

RC522 Arduino Uno

SDA D10

SCK D13

MOSI D11

MISO D12

RST D9

GND GND

3.3V 3.3V

NC Não conectado

Função de cada sinal

SDA (D10)

- Seleciona o dispositivo RFID durante a comunicação SPI.

SCK (D13)

- Fornece o sinal de clock que sincroniza a troca de dados.

MOSI (D11)

- Canal pelo qual o Arduino envia dados ao RC522.

MISO (D12)

- Canal pelo qual o RC522 envia dados ao Arduino.

RST (D9)

- Utilizado para reinicializar o módulo RFID quando necessário.

3.3V

- Alimentação do RC522.
- Importante: o RC522 opera em 3,3 V, não em 5 V.

GND

- Referência comum de tensão entre todos os componentes.

6.3.4.3 - Acionamento do relé

O módulo relé é responsável por isolar eletricamente o Arduino da carga de potência.

As conexões são:

Relé Arduino

IN D7

VCC 5V

GND GND

Funcionamento

Quando o Arduino reconhece uma TAG autorizada:

1. O Arduino coloca o pino D7 em nível alto.
2. O módulo relé é energizado.
3. O contato interno do relé fecha.
4. A tensão de 12 V chega à fechadura solenoide.

6.3.4.4 - Acionamento da fechadura solenoide

A fechadura utiliza alimentação de 12 V.

Ligação típica:

- +12 V da fonte → contato NO do relé
- COM do relé → fechadura
- Outro terminal da fechadura → GND da fonte

Operação

Porta bloqueada

- Relé desligado.
- Não há corrente na bobina da fechadura.

TAG autorizada

- Relé energizado.
- Os 12 V chegam à fechadura.
- A trava é liberada.

Após alguns segundos

- O Arduino desliga o relé.
- A alimentação da fechadura é interrompida.
- A porta volta a ficar travada.

6.3.4.5 - Sequência completa de funcionamento

1. A fonte fornece 12 V ao sistema.
2. O LM2596 reduz os 12 V para 5 V e alimenta o Arduino.
3. O Arduino fornece 3,3 V ao módulo RFID RC522.
4. O usuário aproxima uma TAG RFID.
5. O RC522 lê o código da TAG e envia ao Arduino via SPI.
6. O Arduino verifica se a TAG está cadastrada.
7. Se autorizada, o Arduino ativa o pino D7.
8. O relé fecha seus contatos.
9. A fechadura recebe 12 V e destrava.
10. Após o tempo programado, o relé é desligado.
11. A fechadura volta ao estado travado.

6.3.4.6 - Programação Arduino

```
#include <SPI.h>
```

```
#include <MFRC522.h>
```

```

#define SS_PIN 10

#define RST_PIN 9

MFRC522 mfrc522(SS_PIN, RST_PIN);

void setup()
{
  Serial.begin(9600);
  SPI.begin();
  mfrc522.PCD_Init();
  Serial.println("Aproxime cartao do RFID...");
  Serial.println();
  pinMode(7, OUTPUT);
  pinMode(6, OUTPUT);
  digitalWrite(6, HIGH); //inicia o relé como nivel lógico alto, pois o mesmo aciona com
  nivel lógico baixo
}

void loop()
{
  // Look for new cards
  if ( ! mfrc522.PICC_IsNewCardPresent())
  {
    return;
  } // Select one of the cards
  if ( ! mfrc522.PICC_ReadCardSerial())
  {
    return;
  }
}

```



```

//Mostra UID na serial

Serial.print("UID da tag :");

String conteudo= "";

byte letra;

for (byte i = 0; i < mfrc522.uid.size; i++)
{

Serial.print(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");
Serial.print(mfrc522.uid.uidByte[i], HEX);
conteudo.concat(String(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " "));
conteudo.concat(String(mfrc522.uid.uidByte[i], HEX));

}

Serial.println();

Serial.print("Mensagem : ");

conteudo.toUpperCase();

if (conteudo.substring(1) == "49 AC 2D B3") //UID 1 - TAG com permissão para
acionar a fechadura

{

Serial.println("Acesso Permitido!");

Serial.println();

digitalWrite(7, HIGH); // liga buzzer

delay(100); // espera alguns milisegundos

digitalWrite(7, LOW); // desliga buzzer

delay(100);

digitalWrite(7, HIGH); // liga buzzer

delay(100); // espera alguns milisegundos

digitalWrite(7, LOW); // desliga buzzer

delay(1000);

```

```

digitalWrite(6,!digitalRead(6)); //muda de estado, abre ou fecha a fechadura
}
Else
{
    Serial.println("Acesso Negado!");
    Serial.println();
    digitalWrite(7, HIGH); // liga buzzer
    delay(1000); // espera alguns segundos
    digitalWrite(7, LOW); // desliga o buzzer
    delay(1000);
}
}

```

6.3.5 - Comparativo de Custos entre uma Fechadura Eletrônica RFID Comercial e o Protótipo Desenvolvido

Um dos aspectos mais relevantes na avaliação da viabilidade de um projeto tecnológico é a análise de seus custos em comparação com soluções já disponíveis no mercado. Nesse contexto, foi realizado um comparativo entre o valor de uma fechadura eletrônica com tecnologia RFID comercial e o custo total do protótipo desenvolvido neste trabalho.

As fechaduras eletrônicas RFID disponíveis no mercado utilizam cartões ou tags de proximidade para liberar o acesso, sendo amplamente empregadas em residências, empresas, condomínios e instituições de ensino. Além do mecanismo de abertura, muitos modelos comerciais incluem recursos adicionais, como memória de usuários, alarmes de violação, baterias de emergência, conectividade com aplicativos e sistemas de monitoramento remoto. Em razão dessas funcionalidades, o preço desses equipamentos geralmente varia entre R\$ 180,00 e R\$ 600,00 para modelos básicos e intermediários, podendo alcançar valores superiores em versões mais sofisticadas.

O protótipo desenvolvido neste trabalho foi construído utilizando componentes eletrônicos de baixo custo, incluindo um microcontrolador Arduino, módulo leitor RFID RC522, fechadura solenoide, módulo relé, fonte de alimentação e demais componentes auxiliares. O custo total para a montagem do sistema foi de aproximadamente R\$ 96,00, valor significativamente inferior ao das fechaduras RFID comercializadas no mercado.

Ao comparar os custos, verifica-se que o protótipo apresenta uma economia de aproximadamente 46,7% em relação ao modelo RFID comercial mais barato encontrado no mercado (R\$ 180,00). Quando comparado a equipamentos de valor mais elevado, a economia pode ultrapassar 80%. Esses resultados demonstram que é possível desenvolver um sistema funcional de controle de acesso por RFID utilizando tecnologias abertas e componentes de fácil aquisição, tornando a solução acessível para aplicações acadêmicas, experimentais e de pequeno porte.

Entretanto, é importante destacar que as fechaduras comerciais possuem vantagens relacionadas à certificação do produto, acabamento profissional, resistência mecânica, suporte técnico e garantia do fabricante. Já o protótipo desenvolvido tem como principal objetivo validar o funcionamento da tecnologia RFID aplicada ao controle de acesso, demonstrando sua viabilidade técnica e econômica.

Dessa forma, a análise comparativa evidencia que o sistema proposto alcançou um excelente custo-benefício, oferecendo as funcionalidades essenciais de autenticação por RFID e acionamento eletrônico da fechadura por um investimento reduzido. Isso reforça o potencial da utilização de plataformas de prototipagem eletrônica como ferramenta para o desenvolvimento de soluções de segurança de baixo custo.

Tabela Comparativa de Custos

Solução	Custo Aproximado
Protótipo RFID desenvolvido	R\$ 96,00
Fechadura eletrônica RFID comercial (básica)	R\$ 180,00 a R\$ 300,00
Fechadura eletrônica RFID comercial (intermediária)	R\$ 300,00 a R\$ 600,00
Fechadura RFID comercial avançada	Acima de R\$ 600,00

Portanto o protótipo desenvolvido representa uma alternativa economicamente viável para a implementação de sistemas de controle de acesso por RFID, permitindo a redução dos custos de implantação sem comprometer a funcionalidade básica do sistema.

7 - CONCLUSÃO

O desenvolvimento deste Trabalho de Conclusão de Curso possibilitou a aplicação prática dos conhecimentos adquiridos ao longo do curso técnico em Eletroeletrônica, por meio da construção de uma trava eletrônica de segurança baseada em tecnologias de identificação e controle de acesso. O projeto demonstrou que é possível implementar um sistema de segurança eficiente, de baixo custo e confiável utilizando componentes amplamente disponíveis no mercado, como o microcontrolador Arduino e o módulo RFID.

Durante a execução do trabalho, foram abordados conceitos relacionados à eletrônica, programação, automação e segurança residencial, permitindo a integração entre teoria e prática. Os testes realizados comprovaram o funcionamento adequado do sistema, possibilitando o controle de acesso por meio de cartões ou tags cadastradas, garantindo maior praticidade e segurança em comparação aos métodos convencionais de travamento.

Além dos benefícios relacionados à proteção patrimonial, a solução desenvolvida apresenta potencial para aplicação em residências, escritórios, laboratórios e demais ambientes que necessitem de controle de acesso. O projeto também evidenciou a importância da automação e da Internet das Coisas (IoT) no desenvolvimento de sistemas modernos de segurança, acompanhando as tendências tecnológicas atuais e assim deixa aberto um grande espaço para implementação de novas formas de controle de acesso.

Como sugestão para trabalhos futuros, recomenda-se a implementação de funcionalidades adicionais, utilizando ferramentas e sistemas presentes no mercado, como monitoramento remoto via aplicativo móvel, armazenamento de registros de acesso em banco de dados, integração com sistemas de alarme e envio de notificações em tempo real ao usuário. Essas melhorias podem ampliar significativamente a eficiência e a versatilidade do sistema.

Por fim, conclui-se que os objetivos propostos foram alcançados com sucesso, resultando no desenvolvimento de uma trava eletrônica funcional, segura e economicamente viável, demonstrando a relevância da tecnologia como ferramenta para o aprimoramento da segurança e do controle de acesso em ambientes residenciais e comerciais.

REFERÊNCIAS BIBLIOGRÁFICAS

- ARDUINO. Arduino Uno Rev3. Arduino Documentation, 2025. Disponível em: <https://docs.arduino.cc/hardware/uno-rev3>. Acesso em: 28 maio 2026.
- BAUMAN, Zygmunt. Vigilância Líquida. Rio de Janeiro: Zahar, 2009.
- CAPEZ, Fernando. Curso de processo penal. 30. ed. São Paulo: Saraiva, 2023.
- CARRION, Patricia; QUARESMA, Manuela. Internet da Coisas (IoT): definições e aplicabilidade aos usuários finais. Human Factors in Design, Florianópolis, v. 8, n. 15, p. 49-66, 2019. DOI: 10.5965/2316796308152019049. Disponível em: <https://www.revistas.udesc.br/index.php/hfd/article/view/2316796308152019049>. Acesso em: 6 maio 2026.
- FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. Anuário Brasileiro de Segurança Pública 2025. São Paulo: Fórum Brasileiro de Segurança Pública, 2025.
- FREITAS, R. B. de. Controle e Segurança Patrimonial por RFID no Departamento Acadêmico de Eletrônica da UTFPR Campo Mourão. 2020. 75 f. Dissertação (Pós-Graduação em Inovações Tecnológicas) – Universidade Tecnológica Federal do Paraná, Campo Mourão, 2020.
- GARLAND, David. A cultura do controle: crime e ordem social na sociedade contemporânea. Rio de Janeiro: Revan, 2008.
- HWANG, André. A História do RFID. 2013. Disponível em: https://www.gta.ufri.br/grad/13_1/rfid/cap2_1.html. Acesso em: 6 maio 2026.
- IBGE – INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. Pesquisa Nacional por Amostra de Domicílios Contínua: características gerais dos domicílios e dos moradores 2021. Rio de Janeiro: IBGE, 2021. Disponível em: <https://agenciadenoticias.ibge.gov.br>. Acesso em: 4 maio 2026.
- JACOBS, Jane. Morte e vida de grandes cidades. São Paulo: WMF Martins Fontes, 2011.
- JAIN, Anil K.; FLYNN, Patrick; ROSS, Arun. Handbook of Biometrics. New York: Springer, 2008.
- KANASHIRO, Marta Mourão. Biometria no Brasil e o registro de identidade civil: novos rumos para a identificação. 2011. Tese (Doutorado em Sociologia) –

Faculdade de Filosofia, Letras e Ciências Humanas, Universidade de São Paulo, São Paulo, 2011. DOI: 10.11606/T.8.2011.tde-23042012-120515. Disponível em: <https://teses.usp.br>. Acesso em: 6 maio 2026.

KLAUS, Wolfgang; EFRON, Steven. RFID Handbook: Fundamentals and Applications. 3. ed. Hoboken: Wiley, 2017.

KOCIOLEK, Fabio Tranjan; KLEMBBA, Lucas Laskawski. Trava elétrica acionada por dispositivos de identificação biométrica e RFID. 2017. Trabalho de Conclusão de Curso (Graduação em Engenharia Elétrica) – Universidade Federal do Paraná, Curitiba, 2017.

MAKERHERO. Buzzer: o que é e como funciona? Curitiba: MakerHero, [s.d.]. Disponível em: <https://www.makerhero.com/blog/buzzer-o-que-e-e-como-funciona>. Acesso em: 29 maio 2026.

MAKERHERO. Regulador de tensão: o que é e como funciona. Curitiba: MakerHero, 2026. Disponível em: <https://www.makerhero.com/guia/componentes-eletronicos/regulador-de-tensao/>. Acesso em: 29 maio 2026.

MCROBERTS, Michael. Arduino Básico. São Paulo: Novatec, 2011.

PPA. Manual de instruções: fechaduras de solenóide FES205-2 / FES205-5. Garça, SP: PPA, 2025. Disponível em: https://media.ppa.com.br/files/MANUAL-FECHADURAS-DE-SOLENOIDE-FES205-2-FES205-5_1772107626643.pdf. Acesso em: 29 maio 2026.

SANTOS, Bruno P. et al. Internet das Coisas: da Teoria à Prática. Belo Horizonte: Departamento de Ciência da Computação, Universidade Federal de Minas Gerais, 2016. Disponível em: <https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/internet-das-coisas.pdf>. Acesso em: 4 maio 2026.

STALLINGS, William. Criptografia e Segurança de Redes. 7. ed. São Paulo: Pearson, 2018.

TOCCI, Ronald J.; WIDMER, Neal S.; MOSS, Gregory L. Sistemas Digitais: Princípios e Aplicações. 11. ed. São Paulo: Pearson, 2011.

ZHU, Xiaowei; MUKHOPADHYAY, Samar K.; KURATA, Hisashi. A review of RFID technology and its managerial applications in different industries. Journal of Engineering and Technology Management, v. 29, n. 1, p. 152-167, 2012.