



Controle de Acesso:
Sistema Integrado com dispositivos de baixo custo

Vanderlei do Amaral¹

Centro Universitário Academia – UniAcademia, Juiz de Fora, MG

Romualdo Monteiro de Resende Costa²

Centro Universitário Academia – UniAcademia, Juiz de Fora, MG

RESUMO

O presente artigo tem por objetivo realizar o controle de entrada e saída de pessoas utilizando-se para isso as tecnologias de microcontroladores e leitura de cartões ou tags de RFID. No mercado existe inúmeras soluções prontas, como atualização de biometria entre outras, no entanto a aplicação dessas soluções é complexa e requer muito recurso financeiro e tempo de implementação. Na aplicação deste projeto a um cenário real, o uso do cartão funcional dos usuários, aliados ao uso dos hardwares: leitora e microcontrolador ESP32, ambos de baixo custo, foi possível tornar o projeto viável e confiável para o cenário proposto.

Palavras-chave: Controle de acesso, microcontrolador, RFID, ESP32.

ABSTRACT

This article aims to control the entry and exit of people using the technologies of microcontrollers and reading of RFID cards or tags. There are numerous ready-made solutions on the market, such as biometrics updating, among others, however the application of these solutions is complex and requires a lot of financial resources and time to implement. In the application of this project to a real scenario, the use of the functional card of the users, combined with the use of the hardware: reader and ESP32 microcontroller, both of low cost, it was possible to make the project viable and reliable for the proposed scenario.

Keywords: Access control, microcontroller, RFID, ESP32.

1 INTRODUÇÃO

Todos os anos são registrados diversos casos de furto e roubo a estabelecimentos comerciais. De acordo com Secretaria Pública de Minas Gerais, na região da Zona da Mata foram registrados, no ano de 2019, um total de 1.750 casos de furtos em estabelecimentos comerciais sendo que, somente na cidade de Juiz de

¹ Graduando do Curso de Sistema de Informação do Centro Universitário Academia – UniAcademia.

² Docente do Curso de Sistema de Informação do Centro Universitário Academia – UniAcademia. Orientador(a).

Fora, foram 931 casos, o que corresponde a 53% dos casos da Zona da Mata (MINAS GERAIS, 2020).

Devido, principalmente, aos casos de furto e roubo, o gerenciamento de acesso a locais, serviços e recursos é um fator que vem ganhando importância crescente para todas as organizações, sejam elas de pequeno ou grande porte, públicas ou privadas. Independente da área de atuação, certamente, o risco de violações de segurança é um aspecto que merece ser considerado no plano de negócios de uma empresa.

Para o controle do acesso físico pode ser necessário a utilização de dispositivos que facilitem o processamento e a identificação de pessoas. Caso contrário, principalmente em locais de grande circulação, o controle de acessos indevidos pode ser praticamente impossível de ser efetivamente implementado, contribuindo para o aumento nos incidentes de segurança, incluindo os furtos. Diversos dispositivos podem ser encontrados comercialmente com características de restringir e controlar o acesso como dispositivos biométricos, portas giratórias entre outros. Isoladamente, no entanto, esses dispositivos podem não ser adequados para a tarefa de controle de acesso, pois é necessário que sejam corretamente configurados e gerenciados e demandam um aporte de investimento elevado.

Dessa forma, este trabalho tem como foco o estudo de tecnologias que possam ser implementadas em um sistema de controle de acesso, com uso de dispositivos que considerem aspectos de custo, segurança e praticidade, sendo esse último aspecto considerado sobre a possibilidade de integração com sistemas que gerenciem os dados e controlem barreiras físicas que impeçam qualquer acesso não autorizado e que também controlem, para fins de inspeção e auditoria, os acessos que por ventura tenham sido feitos.

O restante deste artigo descreve os detalhes do trabalho proposto. Dessa forma, a próxima seção descreve o ambiente da empresa, com a análise do fluxo de pessoas e da colocação da catraca. Também nessa seção são descritas a arquitetura e as tecnologias propostas para a solução do problema. A seguir, a terceira seção descreve a implementação do problema proposto, seguido pela quarta e última seção descreve as conclusões obtidas com este trabalho.

2 CENÁRIO

Para exemplificar um cenário real, onde, o controle de acesso pode ser necessário e, uma vez implementado, pode auxiliar no controle dos riscos associados ao funcionamento de uma empresa, a empresa ANSAL (Auto Nossa Senhora Aparecida LTDA), que é uma das empresas prestadoras de serviço do transporte público de Juiz de Fora, foi escolhida para análise e propostas de soluções no decorrer deste trabalho. Por se tratar de uma empresa de transporte público, alguns funcionários (cobradores e motoristas), antes de iniciarem os seus trabalhos, comparecem a unidade administrativa, onde guardam os seus pertences pessoais. Por se tratar de um trabalho de escala, é comum que a entrada e saída dos funcionários ocorra nos mais diversos horários ao longo do dia.

No sistema de transporte público de Juiz de Fora é utilizada a bilhetagem eletrônica em que cada usuário dispõe de um cartão. Como todos os funcionários da empresa avaliada possuem esse cartão, a proposta deste trabalho é utilizar esse dispositivo para implementar o controle de acesso, economizando na aquisição de equipamentos.

A empresa atende a oitenta bairros distribuídos nas zonas nordeste, noroeste, leste, sul e centro de Juiz de fora. Para atendimento desses bairros conta com cento e vinte e sete ônibus que são distribuídos em noventa e seis linhas e percorrem um milhão e quinhentos quilômetros mensais transportando três milhões e quatrocentos passageiros por mês. Isso equivale, em média, a cento e quatorze mil passageiros por dia ou quatro mil e setecentos por hora. Para atender essa demanda a empresa dispõem de um mil, duzentos e vinte funcionários entre motoristas e cobradores, que se revezam, diariamente, entre as mil cento e trinta e seis escalas existentes. Assim, considerando as entradas e saídas de todos os motoristas e cobradores são duas mil, duzentas e setenta e duas movimentações diárias, distribuídas durante o dia conforme a Tabela 1.

Tabela 1: Distribuição de funcionários por hora



Fonte: (Relatório de escala de trabalho motorista e cobrador).

O gráfico da Figura 1, obtido através da escala de trabalho dos funcionários, apresenta entre os horários de quatro e cinco horas uma maior concentração de movimentações. Esse é o horário de início da operação de transporte diário, com o respectivo início da jornada de trabalho dos motoristas e cobradores. Ao longo do dia outras movimentações ocorrem, como as rendições em função do término da jornada ou intervalo de repouso para os funcionários em operação. Nos horários entre às nove e às dezessete horas é onde ocorrem as maiores concentrações de trocas e, por conseguinte, a maior concentração de funcionários na unidade.

Em relação a infraestrutura, a entrada da unidade conta com uma porta de entrada que tem a extensão de três metros de comprimento, não contendo nenhum obstáculo físico que impeça a entrada ou a saída. A partir da análise do local, foi identificada a possibilidade de colocação de uma barreira física que direcionou o fluxo para uma catraca conforme a Figura 1. Para identificar possíveis problemas de fluxo de entrada e saída no local foi realizada, inicialmente, a instalação da catraca sem o sistema de controle. Durante o período de quinze dias foi verificado que não houve registro de nenhuma aglomeração significativa de funcionários em razão do controle de acesso ao ambiente, causado pela instalação da catraca.

Figura 1: Instalação da catraca eletromecânica



Fonte: (do autor).

Para controlar a catraca, dispositivos eletrônicos compostos pelo leitor de cartão, microcontrolador e relé de controle de acionamento foram acondicionados em uma caixa plástica próxima à catraca. A descrição da tecnologia associada a esses dispositivos é apresentada nas subseções a seguir.

2.1 RFID

2.1.1 Definição

Segundo (Bhatt & Glover, 2007), RFID (*r*ádio *f*requency *i*dentification ou identificação por radiofrequência) é uma tecnologia para identificação que tem como utilização principal utilizar a frequência de rádio ou variações de campo magnético para a comunicação entre componentes. De acordo com (Mota, 2006), RFID é uma tecnologia que utiliza ondas de radiofrequência para a transmitir dados. Complementarmente, no trabalho escrito por (Ramos & Nascimento, 2007), RFID é definido como um método de identificação automática através de sinais de rádio, onde é possível recuperar e armazenar dados remotamente, através de dispositivos chamados de *tags*.

A tecnologia RFID é constantemente usada nos dias atuais como no controle de acesso a prédios, ambientes corporativos e no ingresso em meios de transportes, normalmente usando cartões de aproximação. Em alguns estabelecimentos já é notável a utilização do RFID em objetos como livros, peças de roupas e até mesmo em alguns de valor alto, buscando evitar o furto dos mesmos (SANTINI, 2008). No

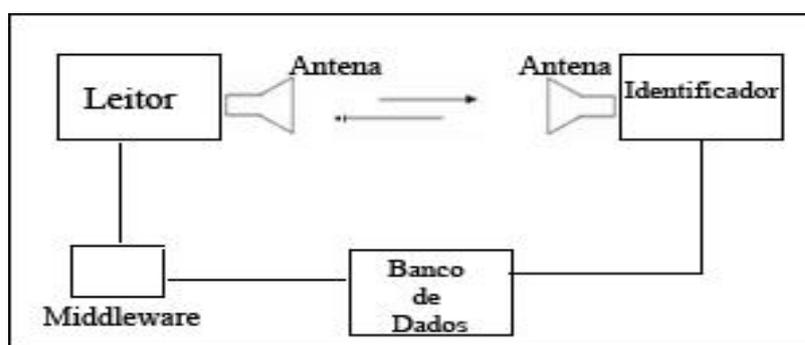
cenário brasileiro, um exemplo da utilização do RFID está nas praças de pedágio das rodovias espalhadas pelos estados, onde um sistema de RFID conhecido como "SEM PARAR" (Almeida, 2011) utilizando um identificador instalado no veículo possibilita a abertura automática da cancela, liberando a passagem (Mota, 2006). A amplitude de utilização de RFID é muito extensa, vai desde o simples registro de bens físicos até o rastreamento de veículos e inclui também a área da logística, com identificação de contêineres e caixas, além do gerenciamento de remessas aos clientes. (Santana, 2005)

2.1.2 Sistema RFID

Conforme (Mota, 2006), apesar de diversos autores concordarem que pode existir um sistema RFID apenas com identificador e leitor, uma conclusão unânime é que todos consideram o banco de dados importante para um sistema completo do ponto de vista prático.

Um sistema simples de RFID tem como composição três componentes principais sendo: identificador, leitor e banco de dados. A Figura 2 ilustra esses componentes na arquitetura proposta por (Mota, 2006) e é uma arquitetura similar que este trabalho pretende seguir.

Figura 2: Sistema RFID



Fonte: Mota, 2006.

Na Figura 2, o leitor se comunica com o Middleware, que é uma camada de software que oferece serviços além daqueles disponíveis pelo sistema operacional. Nesse contexto, o Middleware é o responsável pela comunicação e a integração dos

dispositivos que, na Figura 2, incluem o acesso à base de dados. Ao usar um Middleware, diversas aplicações poderiam ser construídas nessa plataforma, com diferentes objetivos. Neste trabalho, no entanto, como o objetivo de controle é único, uma aplicação é desenvolvida e utilizada no lugar do Middleware. Essa aplicação é embarcada diretamente em um microcontrolador que, além de providenciar o acesso a base de dados também aciona o mecanismo de segurança (catraca). As especificações referentes ao microcontrolador são tratadas na próxima seção.

Ainda na Figura 2, o autor sugere a integração do dispositivo de identificação à base de dados. Neste trabalho os cartões serão cadastrados na base de dados para identificação dos funcionários.

2.2 MICROCONTROLADOR E INTEGRAÇÃO COM OS COMPONENTES

Um microcontrolador é um único circuito integrado que contém os elementos de um sistema microprocessado (interface serial, memória RAM, memória ROM, temporizadores, entre outros). A Unidade de Processamento Central (UCP) é a parte mais importante do microcontrolador (Bertonha, 2007). A Figura 3 mostra um microcontrolador ESP32 (ESP-WROOM-32) que foi escolhido para o projeto. Esse microcontrolador foi escolhido por oferecer uma plataforma de software livre que permite embarcar código na linguagem de programação C/C++³. Dessa forma, o código de controle que se comunica com o leitor RFID e com o banco de dados e que, adicionalmente, controla o acesso através do acionamento da catraca podem ser embarcados nesse microcontrolador. Adicionalmente, esse microcontrolador possui módulo Wi-Fi⁴ integrado e dois núcleos para processamento, além do tamanho reduzido.

Figura 3: ESP-WROOM-32

³ ESPRESSIF. ESP32 Datasheet 2020a. Disponível em: https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf

⁴ ESPRESSIF. ESP32 Datasheet 2020b. Disponível em: https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf



Fonte: www.espressif.com

O microcontrolador ESP32 suporta a integração com outros componentes através de diferentes protocolos de comunicação. Um desses protocolos, é o I2C (Inter-Integrated Circuit)⁵ que é um protocolo de comunicação serial, desenvolvido pela Philips em 1992 que utiliza apenas dois fios. Esse microcontrolador também suporta o protocolo SPI (Serial Peripheral Interface) (Motorola, Inc., 2003) que foi desenvolvido pela Motorola nos anos 80 e é um padrão de comunicação síncrona. Esses protocolos são usados na comunicação com o display LCD e com o leitor de RFID conforme a arquitetura apresentada na próxima seção.

3 DESENVOLVIMENTO DO PROJETO

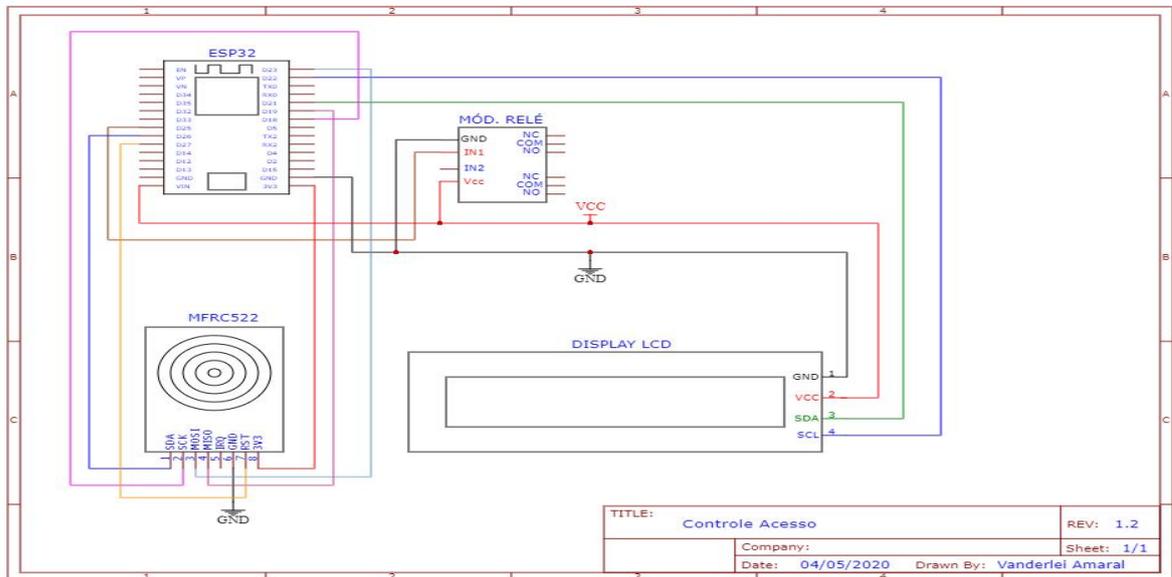
Para realizar o controle de acesso, o leitor de RFID é integrado ao relé que realiza a abertura da catraca. Essa abertura, no entanto, somente é autorizada se o usuário estiver cadastrado e, portanto, se o acesso estiver liberado na base de dados. Para realizar essa operação, o RFID funciona como um dispositivo de entrada de um microcontrolador, onde o código de acesso do usuário é validado. Esse mesmo microcontrolador, caso o acesso do usuário esteja liberado, aciona o relé para a abertura da catraca. Adicionalmente, como dispositivo de saída, que irá informar ao usuário se o acesso está ou não liberado, um display LCD é utilizado.

3.1 ARQUITETURA PARA O CONTROLE DA CATRACA

⁵ NXP. (s.d.). NXP Document on I2C,2014 Disponível em: <http://www.nxp.com/documents/application_note/AN10216.pdf>.

A Figura 4 apresenta a arquitetura dos componentes necessários ao controle da catraca, com detalhes do projeto elétrico necessário à ligação desses componentes.

Figura 4: Arquitetura e projeto elétrico.



Fonte: (do autor).

No pino inferior do microcontrolador ESP32 (VIN), conforme apresentado na Figura 4, está a alimentação de 5 Volts de tensão contínua. A mesma fonte de alimentação fornece a tensão necessária ao funcionamento do módulo relé e do display LCD. Para suportar o consumo desses três componentes, de acordo com a documentação de cada um, optou-se por usar uma fonte de 500 Miliampères. A utilização de uma única fonte de alimentação, além de minimizar o conjunto de componentes necessários à implementação, é a opção mais simples, pois evita a necessidade de sincronização dos componentes. A alimentação do leitor RFID, por outro lado, no valor de 3,3 Volts é fornecida pelo microcontrolador, através do seu pino 3v3, apresentado na Figura 4.

O leitor RFID se comunica com o microcontrolador através do protocolo SPI descrito na seção anterior. Para comunicação desse protocolo são usadas cinco conexões. Os pinos do microcontrolador que fazem esta conexão com o leitor de RFID são respectivamente: 23, 19, 26, 18 e 27, conforme ligação apresentada na Figura 4.

O display LCD informa se o usuário pode passar pela catraca. Caso seja autorizado, o sistema informa o primeiro nome do funcionário e o tipo de

movimentação (entrada ou saída) e, caso não esteja autorizado, a mensagem informada é de acesso negado, seguido pelo número do cartão lido pelo sistema. Na comunicação do microcontrolador com esse display é utilizado o protocolo I2C, apresentado na seção anterior, que necessita de duas conexões. Assim, os pinos SDA (Serial Data) e SCL (Serial Clock) do display estão conectados, respectivamente, nos pinos 21 e 22 do microcontrolador, conforme mostra a Figura 4.

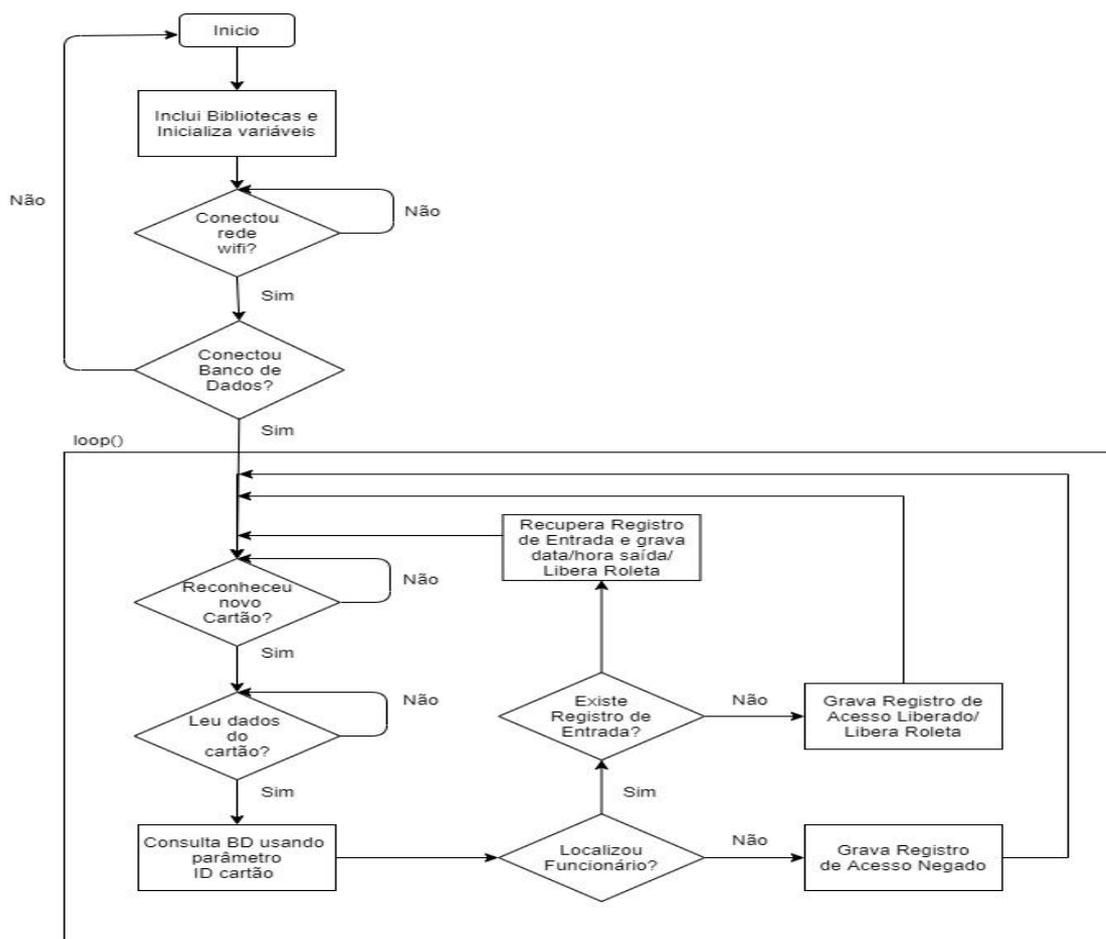
A Figura 4 apresenta também a interligação do relé ao pino 25 do microcontrolador, que é destinado a realizar o controle de acionamento desse componente e, conseqüentemente, de liberação da catraca.

3.2 PROGRAMAÇÃO DO MICROCONTROLADOR

Neste trabalho é utilizada a IDE Arduino para o desenvolvimento do controle do microcontrolador. No programa embarcado, também conhecido como *sketch* (MCROBERTS, 2011) existe duas funções principais, a *setup* e a *loop*. A primeira é executada apenas uma vez, logo após o microcontrolador ser energizado ou quando o *sketch* for carregado. Essa função é utilizada para configuração inicial do ambiente. A segunda é executada infinitamente, enquanto o microcontrolador estiver energizado. Essa função é o cerne do programa.

O Diagrama de Estados, apresentado na Figura 5, permite uma melhor visualização do algoritmo desenvolvido.

Figura 5: Diagrama de estados.



Fonte: (do autor).

Inicialmente o microcontrolador realiza a inclusão das bibliotecas e inicializa variáveis e instancia objetos necessários. Essas operações são realizadas na função *setup*. É importante destacar que as funcionalidades do microcontrolador podem ser extensíveis com uso de bibliotecas, importadas, ou as que já vem por padrão na IDE Arduino. Neste projeto são utilizadas bibliotecas que permitem as comunicações via Wi-Fi, protocolo I2C, protocolo SPI, cliente do SGBD MySQL e leitora RFID

Na sequência, conforme apresentado na Figura 5, o microcontrolador realiza a conexão à rede Wi-Fi e, enquanto não for possível essa conexão, este estado não se altera. Após o dispositivo estar conectado a uma rede, é realizada a conexão com o banco de dados. Caso essa operação não seja possível, o processo é reinicializado.

Sem a comunicação com banco de dados não há como ter o prosseguimento das demais etapas pelo fato de que não haverá como realizar a consulta no banco

de dados para validar o cartão a ser lido assim como qualquer tipo de inserção no banco de dados.

Todos os procedimentos mencionados anteriormente são realizados uma única vez após a inicialização do sistema. Dessa forma, todos eles devem ser implementados na função *setup*. Quando esses processos terminam com sucesso tem início as operações realizadas na função *loop* que, como mencionado, são realizadas repetidamente.

A primeira etapa do processo de repetição é verificar se a leitora identifica um novo cartão capaz de ser lido. O microcontrolador precisa realizar o monitoramento constante da leitora de cartão de RFID que está conectada a ele. Quando a leitora identifica a presença de um novo cartão, o leitor deve ser capaz de ler os dados contidos para que, a partir dessas informações, o microcontrolador realize os procedimentos adequados.

Quando ocorre a identificação de um novo cartão, enquanto houver dados a serem lidos do cartão esse processo não é finalizado. A partir da obtenção do identificador do cartão de RFID, o microcontrolador realiza consulta no banco de dados. Se a consulta não retornar nenhum nome de funcionário, significa que não existe um cartão vinculado a algum funcionário. Nesse caso, o microcontrolador grava no banco de dados o registro de acesso negado. O programa retorna ao início do loop, aguardando novamente a presença de um novo cartão.

Por outro lado, caso a consulta retorne o nome do funcionário, significa que o cartão está vinculado a um funcionário cadastrado no sistema e controles adicionais precisam ser verificados. Em uma consulta adicional ao banco de dados para identificar se existe registro de acesso com status de entrada, pode ser retornado esse registro de entrada, ou nenhum. Caso a consulta não retorne nenhum valor, um novo registro é inserido no banco de dados e o microcontrolador aciona o módulo relé que realiza o destravamento da catraca por 3 (três) segundos. Decorrido esse o microcontrolador trava novamente a catraca e o programa retorna ao início da função *loop* aguardando novamente a presença de um novo cartão. Por outro lado, caso a consulta retorne um registro de entrada, esse registro é alterado no banco de dados e as mesmas operações para a liberação da catraca são realizadas, bem como o reinício do funcionamento do sistema.

Em relação aos procedimentos iniciais, a Figura 6 apresenta a conexão Wi-Fi, utilizando os recursos disponíveis na biblioteca `Wifi.h`⁶ que foi incorporada ao projeto. Em destaque na Figura 6 está a inicialização da conexão com as informações pertinentes, uma estrutura de laço é utilizada para verificar o status da conexão, recorrendo novamente aos métodos disponibilizados pela biblioteca, incluindo o método `WiFi.status()`, que retorna uma constante que será comparada até que retorne conectada. Enquanto não há um retorno dessa conexão haverá um retorno para o usuário através do display LCD mostrando que o sistema está aguardando a realização da conexão.

Figura 6: Métodos conexão rede Wi-Fi

```
while (WiFi.status() != WL_CONNECTED) {  
  lcd.clear();  
  lcd.print("Conectando Wi-Fi ..");  
  lcd.print(SSID_WIFI);  
  delay(500);  
}
```

Fonte: (do autor).

Outra condicionante importante para o sistema é conseguir realizar a comunicação com banco de dados, no programa é utilizada a bibliotecas `Mysql.h`⁷. A Figura 7 apresenta em destaque o método `conn.connect()` fornecido por essa biblioteca. Esse método possui os seguintes parâmetros obrigatórios: o endereço do servidor (IP) onde o banco de dados se encontra hospedado, o número da porta, o usuário e a senha de acesso a esse banco. Essa função tem como retorno um valor verdadeiro, caso consiga conectar com sucesso ao banco de dados, ou falso, caso não consiga a conexão. Caso a conexão ocorra com sucesso, além das informações ao usuário, a função `mensagemInical()` será executada. Caso contrário, ou seja, se a conexão não for possível, o usuário será informado do problema, o sistema aguardará 9 (nove) segundos e, após esse intervalo, a função `esp_restart()`, nativa do microcontrolador, será executada, fazendo com que o microcontrolador reinicie, uma vez que sem conexão ao banco de dados não é possível prosseguir no controle de acesso.

⁶ Arduino. Disponível: www.arduino.cc/en/Reference/WiFi

⁷ Arduino Library. Disponível em: www.arduinolibraries.info/libraries/my-sql-connector-arduino

Figura 7: Conexão ao banco de dados.

```

if (conn.connect(server_addr, 3306, user, password)) {
  lcd.clear();
  lcd.setCursor(1,0);
  lcd.print("Conectado com");
  lcd.setCursor(5,1);
  lcd.print("Sucesso");
  delay(1000);
  lcd.clear();
  mensagemInicial();
}
else {
  lcd.clear();
  lcd.print("Conexao Banco de");
  lcd.setCursor(0, 1);
  lcd.print("Dados - Falhou");
  delay(9000);
  esp_restart();
}

```

Fonte: (do autor).

Após as configurações iniciais, o microcontrolador inicia a execução da função *loop*. A Figura 8 apresenta a primeira condicional a ser verificada nessa função que é realizada através do retorno da função *mfr522.PICC_IsNewCardPresent()*. Essa função, disponibilizada pela biblioteca MFRC522.⁸ tem como objetivo detectar a passagem de um novo cartão na leitora. Logo em seguida à detecção do cartão, é preciso que os dados desse cartão sejam lidos e guardados para uso posterior, nesse caso, outro método da biblioteca é utilizado, o *mfr522.PICC_ReadCardSerial()*.

Figura 8: Métodos da biblioteca.

```

void loop() {

  if ( ! mfr522.PICC_IsNewCardPresent() ) // Verifica se há novo cartão
    return;

  if ( ! mfr522.PICC_ReadCardSerial() ) // Realiza leitura do cartão
    return;
}

```

Fonte: (do autor).

Dos dados lidos pelo método *mfr522.PICC_ReadCardSerial()*, são utilizados o identificador do cartão, conforme a Figura 9. Tento em vista que esse número é armazenado no banco de dados com o tipo texto (*string*), a conversão para esse formato é essencial para comparação com as buscas realizadas no banco de dados.

⁸ Arduino Library. Disponível em: www.arduino-libraries.info/libraries/mfr522

Figura 9: Leitura e conversão do identificador do cartão.

```
for (int i = mfrc522.uid.size; i >=0; i--)  
{  
    uid[i] = mfrc522.uid.uidByte[i];  
    cartao = (cartao << 8) + uid[i];  
}  
  
numCartao = String(cartao);
```

Fonte: (do autor).

Na função *buscaFuncionarioRegistrado()* uma consulta é realizada no banco de dados para retornar o campo com o nome reduzido do funcionário, que nada mais é que o primeiro nome do funcionário. Na Figura 10 apresenta parte do código do programa onde a expressão condicional verifica se a variável *nomeFunc* tem um valor. Neste caso, existe um funcionário associado ao cartão e, portanto, sua entrada está liberada. Neste momento é obtido também o último registro associado a esse funcionário, para determinar se este registro é referente a uma entrada ou saída. A função *buscarUltimoRegistro()*, também apresentada na Figura 10, retorna o último registro do funcionário. Caso não exista um registro, o retorno será um número negativo (-1). Na sequência, o microcontrolador aciona o relé para a liberação da catraca. Esta liberação permanece por 3 (três) segundos para que o funcionário realize a passagem pela catraca e, logo após decorrido esse tempo, o relé volta a seu estado inicial e a catraca permanece travada.

Para o registro do acesso, há duas possibilidades, a primeira, quando se trata de uma entrada, onde um novo registro é criado no banco de dados e, a segunda, quando se trata de uma saída em que o registro de entrada é recuperado para gravação do campo *dat_hora_saida* do banco de dados. Somente nesse caso é utilizada a função *gravaAcesso()*. Por fim, caso o cartão lido não tenha nenhum relacionamento com funcionários existentes no banco de dados, apenas é realizado o registro do cartão no banco de dados através da função *negarAcesso()*. As funções *liberarAcesso()* e *mensagemInicial()*, são apenas para gerar as mensagens no display LCD e criar log no sistema.

Figura 10: Liberar Acesso / Negar Acesso.

```

nomeFunc = buscaFuncionarioRegistrado(numCartao);

if (!nomeFunc.equals("")) {
    int id_registro = buscarUltimoRegistro(numCartao);
    liberarAcesso(nomeFunc, id_registro);

    digitalWrite(RELE, LOW);
    delay(3000);
    digitalWrite(RELE, HIGH);

    if (id_registro <= 0) {
        gravaAcesso(numCartao);
    }else {
        alterarAcesso(id_registro);
    }
    mensagemInicial();
    nomeFunc="";
}
else {
    negarAcesso(numCartao);
    mensagemInicial();
}
}

```

Fonte: (do autor).

3.3 SISTEMA WEB DE GESTÃO

Para realizar a manutenção do cadastro de funcionários e realizar a consulta de relatórios gerenciais foi desenvolvido para os usuários um sistema web de gestão. A Figura 11 apresenta a tela de edição de funcionários do sistema. O emprego de um sistema e gestão é necessário neste projeto pois, sem essa ferramenta, a manutenção das informações dos funcionários tornar-se-iam obsoletas e poderia ser perdido o objetivo do controle de acesso.

Figura 11: Sistema de Gestão de Acesso – Edição de Funcionários.

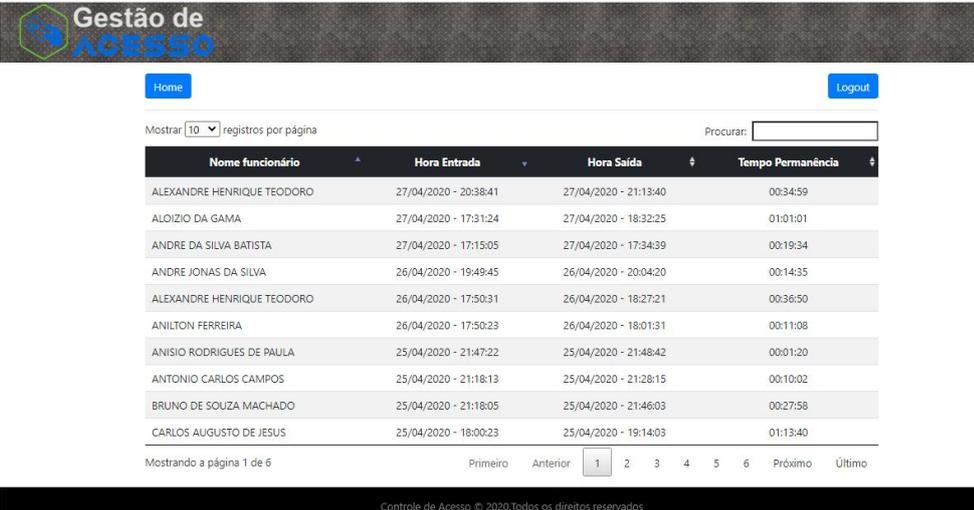
The screenshot displays the 'Gestão de ACESSO' web application. At the top, there are navigation buttons for 'Home', 'Novo funcionário', and 'Logout'. Below these, there is a search bar and a dropdown menu for 'Mostrar 10 registros por página'. The main content is a table with three columns: 'Cracha', 'Nome funcionário', and 'Função'. The table lists several employees, with their names and functions partially obscured by black redaction boxes. The functions listed are 'MOTORISTA' and 'COBRADOR'. At the bottom of the table, there is a pagination control showing 'Mostrando a página 1 de 64' and buttons for 'Primeiro', 'Anterior', '1', '2', '3', '4', '5', '64', 'Próximo', and 'Último'. A footer at the very bottom reads 'Controle de Acesso © 2020. Todos os direitos reservados'.

Fonte: (do autor).

O sistema de gestão foi desenvolvido usando o *framework codeigniter* (Antunes, 2016) que tem como características baixa curva de aprendizado, trabalha sobre o modelo MVC (Antunes, 2016) minimiza a quantidade de código necessário para as tarefas. Também no desenvolvimento, para a arquitetura de *front-end* foi incorporado ao código o *framework bootstrap* (Souza, 2018).

Com a confirmação das credenciais, o usuário pode ter acesso ao relatório de registro de acessos liberados conforme a Figura 12. Neste relatório são apresentados a data e a hora que cada funcionário efetuou a entrada no ambiente, assim como as datas e horas de cada saída.

Figura 12: Listas de acessos realizados.



The screenshot shows a web application interface for 'Gestão de ACESSO'. At the top, there is a navigation bar with 'Home' and 'Logout' buttons. Below the navigation bar, there is a search bar labeled 'Procurar:' and a dropdown menu for 'Mostrar 10 registros por página'. The main content is a table with the following columns: 'Nome funcionário', 'Hora Entrada', 'Hora Saída', and 'Tempo Permanência'. The table contains 12 rows of data, each representing an employee's access record. At the bottom of the table, there is a pagination control showing 'Mostrando a página 1 de 6' and navigation buttons for 'Primeiro', 'Anterior', '1', '2', '3', '4', '5', '6', 'Próximo', and 'Último'. A footer at the very bottom reads 'Controle de Acesso © 2020. Todos os direitos reservados'.

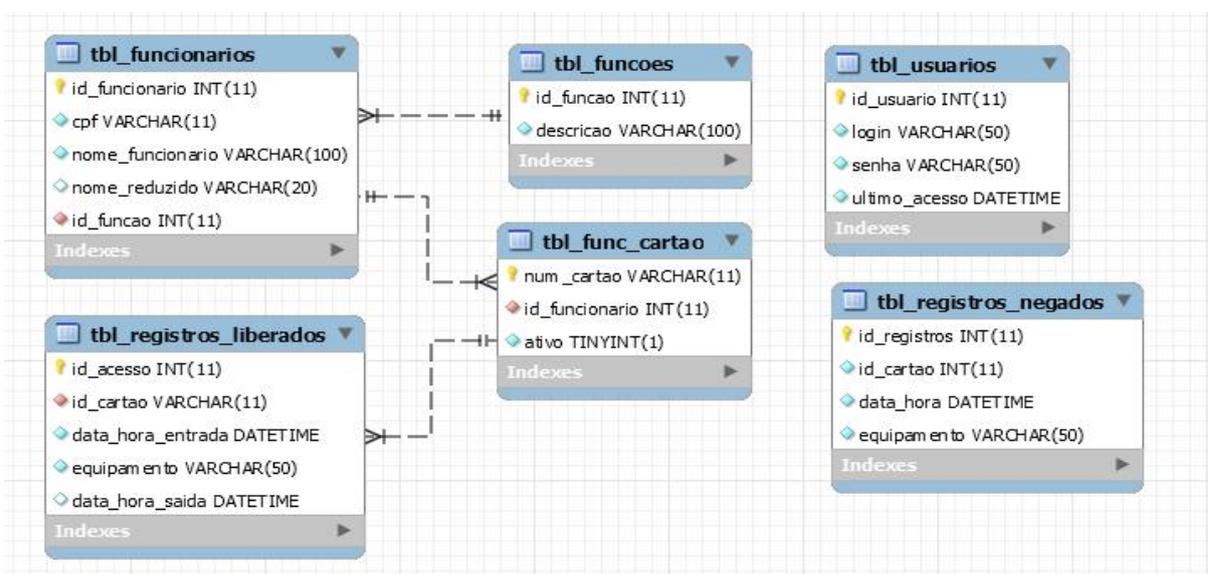
Nome funcionário	Hora Entrada	Hora Saída	Tempo Permanência
ALEXANDRE HENRIQUE TEODORO	27/04/2020 - 20:38:41	27/04/2020 - 21:13:40	00:34:59
ALOIZIO DA GAMA	27/04/2020 - 17:31:24	27/04/2020 - 18:32:25	01:01:01
ANDRE DA SILVA BATISTA	27/04/2020 - 17:15:05	27/04/2020 - 17:34:39	00:19:34
ANDRE JONAS DA SILVA	26/04/2020 - 19:49:45	26/04/2020 - 20:04:20	00:14:35
ALEXANDRE HENRIQUE TEODORO	26/04/2020 - 17:50:31	26/04/2020 - 18:27:21	00:36:50
ANILTON FERREIRA	26/04/2020 - 17:50:23	26/04/2020 - 18:01:31	00:11:08
ANISIO RODRIGUES DE PAULA	25/04/2020 - 21:47:22	25/04/2020 - 21:48:42	00:01:20
ANTONIO CARLOS CAMPOS	25/04/2020 - 21:18:13	25/04/2020 - 21:28:15	00:10:02
BRUNO DE SOUZA MACHADO	25/04/2020 - 21:18:05	25/04/2020 - 21:46:03	00:27:58
CARLOS AUGUSTO DE JESUS	25/04/2020 - 18:00:23	25/04/2020 - 19:14:03	01:13:40

Fonte: (do autor).

3.4 MODELO LÓGICO DOS DADOS

O armazenamento das informações do controle de acesso, ocorrerá através do SGBD MySQL (MANZANO, 2009). que é uma solução de software livre. O banco de dados construído, chamando *db_control_aceso* é composto por seis tabelas, cujo modelo lógico é apresentado na Figura 13.

Figura 13: Modelo Lógico do Banco de Dados.



Fonte: (do autor).

A tabela *tbl_usuarios* armazena as informações dos usuários do sistema de gestão web e tem como campos o id do usuário, login, senha e último acesso. A tabela *tbl_funcionarios* armazena as informações relativas aos funcionários cadastrados, os seus campos são: id do funcionário, cpf do funcionário, nome, nome reduzido ou primeiro nome, id função, na *tbl_funcao* tem como campo id função e a descrição.

A tabela *tbl_registros_liberados* possui os registros dos cartões que tiveram o acesso liberado e, por conseguinte, existe um relacionamento entre o registro dos cartões e dos funcionários, a tabela tem os campos: id acesso, id cartão data e hora de entrada, data e hora de saída e o registro do equipamento onde ocorreu a movimentação.

Na tabela *tbl_registros_negados* são armazenadas as tentativas de acesso que foram negadas, ou seja, os cartões que foram passados no controle da catraca que não estavam cadastrados no banco de dados. Esta tabela tem como campos: id registro, id cartão data e hora e equipamento.

A tabela *tbl_func_cartao* foi definida em razão de que um funcionário pode ter o seu cartão substituído por um novo por quantas vezes forem necessárias ao longo do tempo. É importante observar, no entanto, que um cartão somente pode

pertencer a um único funcionário. Os campos dessa tabela são: número do cartão, id funcionário e status.

3.5 CUSTOS

O projeto proposto leva em consideração o baixo custo de implementação e manutenção. O valor estimado dos componentes utilizados em fevereiro de 2020 foi de R\$ 125,72 como mostra a tabela 2.

Tabela 2: Tabela de custos

Quantidade	Item	Valor R\$
01	ESP32	R\$ 35,90
01	DISPLAY LCD 16X2	R\$ 19,90
01	LEITORA MFRC-522	R\$ 17,58
01	MODULO RELÉ	R\$ 13,90
01	CAIXA PATOLA	R\$ 14,90
01	FONTE ALIMENTAÇÃO	R\$ 10,99
04	PARAFUSOS FIXAÇÃO	R\$ 12,55
VALOR TOTAL:		R\$ 125,72

Fonte: (Elaborado pelo autor).

A catraca eletromecânica não teve custo para o projeto, pois foi retirado de um veículo da frota da empresa que está desativado. Os cartões de RFID também não tiveram nenhum custo, uma vez que já fazem parte do sistema de bilhetagem eletrônica.

4 RESULTADOS E DISCUSSÃO

O protótipo desenvolvido neste trabalho que teve como objetivo o controle de acesso de pessoas a um ambiente, foi testado durante 48 horas e, durante esse tempo, foram processados 2.752 registros de entrada e saída. Nesse tempo foram testados 8 cartões não cadastrados no sistema. Todos os procedimentos foram registrados corretamente no sistema. Os acessos habilitados foram liberados e os cartões inabilitados tiveram seu acesso negado.

Durante o período de testes foi realizado um procedimento intencional para que o microcontrolador perdesse a conexão com banco de dados. Nesse contexto

foi observado que o sistema não conseguiu recuperar a conexão, tendo como comportamento não desejado de não mais validar os cartões, passando todos a terem o status de acesso negado. Esse problema só foi resolvido com a reinicialização do microcontrolador para que o processo de conectividade e conexão com banco de dados fosse restabelecido. Por conta deste problema, foi facilitado o processo de reinício do sistema com a inclusão de um botão próximo da leitora. Nos testes realizados o processo de conexão demorou cerca de 4 (quatro) segundos, o que não contribuiu significativamente para a retenção de pessoas na entrada do estabelecimento.

Nos testes realizados foi utilizada a base de funcionários da empresa, com todos os mil e seiscentos funcionários cadastrados no banco de dados. Nessa base de dados, o tempo de leitura do cartão, consulta no banco de dados e acionamento do modulo relé foi de, em média, sessenta e seis (66) décimos de segundo para os casos em que o acesso estava liberado e de trinta (30) décimos de segundos para os casos onde os acessos foram negados.

Para melhoria do projeto seria interessante desenvolver um mecanismo de recuperação da conexão com banco de dados. Essa funcionalidade permitiria a eliminação da necessidade de reinicialização interativa do sistema de controle nos casos em que essa conexão foi perdida.

REFERÊNCIAS

ALMEIDA, L. C. **Aplicações da Tecnologia de Identificação por Rádio Frequência – RFID** Fortaleza – CE, 2011. – Universidade Federal do Ceará, Departamento de Engenharia de Teleinformática, Fortaleza, 211.

ANTUNES, J. L. **CodeIgniter: Produtividade na criação de aplicações web em PHP**. São Paulo: Casa do Código, 2016

BERTONHA, E. G. **Apostila Microcontroladores 8051**. Departamento Acadêmico de Eletrônica. UTFPR. 2007. 26

BHATT, H.; GLOVER, B. **Fundamentos de RFID**. Rio de Janeiro: Altas Books, 2007.

MANZANO, JOSE AUGUSTO N. G. **Mysql 5 – Interativo: Guia Básico de Orientação e Desenvolvimento**. São Paulo, 2009.

MCROBERTS, MICHAEL **Arduino Básico** 1.ed. São Paulo: Novatec Editora, 2011

MINAS GERAIS, Secretaria de Justiça e Segurança pública de. **Minas em números**
Disponível em: <<http://www.numeros.mg.gov.br/>> Acesso em: 10 de fev. 2020

MOTOROLA, INC. SPI Block Guide V03.06, 2003.

RAMOS, L.F.; NASCIMENTO, **R.G. Redes RFID**. Cuiabá – MT, 2007. – Centro federal de educação tecnológica de Mato Grosso, Departamento de Pós-graduação, Cuiabá, 2007.

SANTANA, S.R.M. **Comunicação via WAP (Wireless Application Protocol) e identificação por radiofrequência**. Praia Grande, 2005. 68 f. *Monografia* (Sistema de informação). FATEC – Faculdade de tecnologia da baixada santista extensão Praia Grande, Praia Grande, 2005.

SANTINI, A. G. **RFID Conceitos, aplicabilidades e impactos** 1.ed. Rio de Janeiro: Ciência Moderna, 2008.

SOUZA, N. **Bootstrap 4: conheça a biblioteca front-end mais utilizada no mundo**. São Paulo: Casa do Código, 2018.