UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

CURSO DE ENGENHARIA ELECTRÓNICA

Proposta de um sistema de controlo de acesso e assiduidade dos trabalhadores da Central Termoeléctrica de Maputo.

Nelton Augusto Muluana

Supervisores:

Supervisor da Faculdade: Eng.º Edson Camilo Fortes

Supervisor da Instituição: Eng.º Berry Machabo

Maputo, 2023

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

CURSO DE ENGENHARIA ELECTRÓNICA

Proposta de um sistema de controlo de acesso e assiduidade dos trabalhadores da Central Termoeléctrica de Maputo.

Nelton Augusto Muluana

Supervisores:

Supervisor da Faculdade: Eng.º Edson Camilo Fortes

Supervisor da Instituição: Eng.º Berry Machabo

Maputo, 2023

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTECNICA

FICHA DE AVALIAÇÃO DA ATITUDE DO ESTUDANTE

(Supervisor da Instituição)

Nome do estudante: Nelton Augusto Muluana

Referência do tema:_____
Data:09/12/2022

Título do tema: **Proposta de um sistema de controlo de acesso e assiduidade dos trabalhadores da Central Termoeléctrica de Maputo.**

Indicador	**Classificação**				
Atitude geral (manteve uma disposição positiva e sentido de humor)	1	2	3	4	5
Dedicação e comprometimento (Deu grande prioridade ao projecto e aceitou as responsabilidades prontamente)	1	2	3	4	5
Independência (realizou as tarefas independentemente, como prometido e a tempo)	1	2	3	4	5
Iniciativa (viu o que devia ter sido feito e fê-lo sem hesitar e sem pressões do supervisor)	1	2	3	4	5
Flexibilidade (disponibilidade para se adaptar e estabelecer compromissos)	1	2	3	4	5
Sensibilidade (ouviu e tentou compreender as opiniões dos outros)	1	2	3	4	5
Criatividade (contribuiu com imaginação e novas ideias)	1	2	3	4	5
Total de pontos (max: 35)					

Valor do classificador	Cotação obtida	Significado
	1	Não aceitável (0 a 9 valores)
	2	Suficiente (10 a 13 valores)
	3	Bom (14 a 16 valores)
	4	Muito Bom (17 a 18 valores)
	5	Excelente (19 a 20 valores)

Total de pontos (max: 35)	

Nota (=Total*20/35)	

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTECNICA

FICHA DE AVALIAÇÃO DA ATITUDE DO ESTUDANTE

(Supervisor da UEM)

Nome do estudante: Nelton Augusto Muluana

Referência do tema:_____
Data:09/12/2022

Título do tema: **Proposta de um sistema de controlo de acesso e assiduidade dos trabalhadores da Central Termoeléctrica de Maputo.**

Indicador	**Classificação**				
Atitude geral (manteve uma disposição positiva e sentido de humor)	1	2	3	4	5
Dedicação e comprometimento (Deu grande prioridade ao projecto e aceitou as responsabilidades prontamente)	1	2	3	4	5
Independência (realizou as tarefas independentemente, como prometido e a tempo)	1	2	3	4	5
Iniciativa (viu o que devia ter sido feito e fê-lo sem hesitar e sem pressões do supervisor)	1	2	3	4	5
Flexibilidade (disponibilidade para se adaptar e estabelecer compromissos)	1	2	3	4	5
Sensibilidade (ouviu e tentou compreender as opiniões dos outros)	1	2	3	4	5
Criatividade (contribuiu com imaginação e novas ideias)	1	2	3	4	5
Total de pontos (max: 35)					

Valor do classificador	Cotação obtida	Significado
	1	Não aceitável (0 a 9 valores)
	2	Suficiente (10 a 13 valores)
	3	Bom (14 a 16 valores)
	4	Muito Bom (17 a 18 valores)
	5	Excelente (19 a 20 valores)

Total de pontos (max: 35)	

Nota (=Total*20/35)	

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉNICA

AVALIAÇÃO DOS SUPERVISORES

Autor: Nelton Augusto Muluana

Proposta de um sistema de controlo de acesso e assiduidade dos trabalhadores da Central Termoeléctrica de Maputo.

Supervisor da Faculdade **Nota**

_____ _____

(Eng.º Edson Camilo Fortes)

Supervisor da Instituição **Nota**

_____ _____

(Eng.º Berry Machabo)

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉNICA

TERMO DE ENTREGA DE RELATÓRIO DO ESTÁGIO PROFISSIONAL

Declaro que o estudante: Nelton Augusto Muluana

Entregou no dia ___/___/20__ as __ cópias do relatório do seu relatório do estágio profissional com a referência: _____

Intitulado: Proposta de um sistema de controlo de acesso e assiduidade dos trabalhadores da Central Termoeléctrica de Maputo.

Maputo, ____ de _____ de 20__

O Chefe de Secretaria

_____

DEDICATÓRIA

Este trabalho eu dedico aos pais, Maria Luíza João Cuamba e Augusto Muluana, por serem a razão da minha existência, por terem feito de tudo por mim e pela minha formação.

AGRADECIMENTOS

Agradeço primeiramente a Deus, pelo dom da vida e por me guardar com saúde sempre, principalmente no período crítico da pandemia da covid-19. Por não ter permitido que momentos de dificuldade e angústia me fizessem desistir dos estudos.

Sou grato a minha namorada Erica Cecília Ofinar Nchussa, por todo suporte e incentivo, pela paciência e compreensão e por ter ajudado toda vez em que precisei. Ao meu cunhado Arsénio Lourenço Nhambongo , por abrir mão de um bem, para que a realização deste trabalho fosse possível e por me suportar e apoiar.

Um agradecimento especial a mim. O qual farei usando um trecho das palavras usadas pelo rapper “Snoop Dogg” em sua música intitulada “*I Wanna Thank Me*”.

“Quero agradecer-me, por acreditar em mim;

quero agradecer-me por fazer todos trabalhos;

quero agradecer-me por nunca desistir;

quero agradecer-me por tentar fazer mais o certo que o errado;

quero agradecer-me por ser eu em todos os momentos.”

EPÍGRAFE

“Nossa maior fraqueza está em desistir.
O caminho mais certo de vencer é tentar mais uma vez.”
(Thomas Edison)

RESUMO

Estudos demonstram a dificuldade em controlar manualmente o acesso dos usuários em diversos ambientes. Estes estudos também apresentam parâmetros relevantes para a escolha do sistema de controlo automatizado, de modo a atender as especificações das áreas de segurança patrimonial e Tecnologia da Informação e Comunicação. Atualmente os sistemas de controlo de acesso possuem dois modos de operação bem característicos: o online, que pode apresentar lentidão no processamento das requisições de acesso; o offline, que pode operar com suas informações desactualizadas devido a demora do servidor em realizar o sincronismo dos dados.

O presente trabalho consiste na elaboração de uma proposta de um sistema para controlar o acesso e assiduidade dos trabalhadores da Central Termoelétrica de Maputo usando a tecnologia RFID e a placa ESP32 para processar as informações de entrada e saída. Este sistema foi implementado utilizando a memória da tag RFID para armazenar dados relevantes a validação do acesso.

Palavras-chave: Controlo de Acesso, Radio-Frequency Identification (RFID), Segurança patrimonial, MFRC522.

ABSTRACT

Studies show the difficulty in manually controlling user access in different environments. These studies also present relevant parameters for the choice of the automated control system, in order to meet the specifications of the property security and Information and Communication Technology areas. Currently, access control systems have two very characteristic modes of operation: online, which can present slow processing of access requests; offline, which can operate with outdated information due to the server's delay in synchronizing the data.

The present work consists in the elaboration of a proposal of a system to control the access and attendance of the workers of the Thermoelectric Power Plant of Maputo using RFID technology and the ESP32 board to process the input and output information. This system was implemented using the RFID tag memory to store data relevant to access validation.

Keywords: Access Control, Radio-Frequency Identification (RFID), Property Security, MFRC522.

INDICE

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

CTM-Central Térmica de Maputo

DHTML- *Dynamic HTML* (HTML Dinâmico);

EDM-Eletricidade de Moçambique

GPIO- General Purpose Input/Output

HTML- *HyperText Markup Language* (Linguagem de Marcação de Hipertexto);

Hz -Hertz

IoT- Internet of Things (Internet das Coisas);

IP- Internet Protocol

LCD-*Liquid Crystal Display* (Tela de Cristal Líquido);

PHP- *Hypertext Preprocessor;*

RF- Rádio Frequência

RFID- Rádio-Frequency Identification

RH- Recursos Humanos.

SPI- Serial Peripheral Interface

SPI-Serial Peripheral Interface

SQL- *Standard Query Language*

TIC- Tecnologia da Informação e Comunicação

CAPíTULO I: INTRODUÇÃO

1.1. Contextualização

Sistemas de controlo de acesso têm se tornado uma ferramenta essencial para garantir a segurança de locais onde existe um considerável número de pessoas circulando. Em alguns casos, além de controlar a entrada e saída de pessoas, é possível inserir funcionalidades diversas como a geração de relatórios de fluxo de pessoas e verificar a presença de indivíduos específicos no ambiente.

O controlo de acesso, por si só, permite aumentar a segurança do espaço físico, não permitindo a entrada de indivíduos estranhos ao local. Proporcionando um ambiente mais seguro e agradável para as pessoas que nele circulam. Essa segurança, obtida por meio do controlo de acesso, é essencial principalmente para CTM. Neste local o controle de acesso se torna uma ferramenta primordial para monitorar a entrada e saída de pessoas. Além de controlar o acesso dos seus trabalhadores, nestes casos, também é possível auditar ou monitorar a presença de visitantes e estagiários, complementando este processo que, normalmente, é feito de forma manual.

Por outro lado, o registo de entrada e saída, registo de ausência, o controle de faltas, marcação de férias é uma necessidade recorrente do sector do RH de inúmeras organizações. Dada a sua importância ao nível de planificação e financeiro este processo deve ser feito de forma eficaz e em tempo útil. No caso da CTM, esta não possui nenhum recurso informático para a gestão do RH, nomeadamente o registo de entradas e saídas. Registo esse que ainda é feito num livro de ponto, que para além de os registos serem manuais estes não têm qualquer controlo de horários e verificação efectiva de horas de entrada e saída.

1.2. Definição do problema

No mundo contemporâneo, quando se fala em segurança nas empresas é muito comum a associação das áreas de segurança patrimonial e tecnologia da informação e comunicação, para elaboração e implantação de um projecto de controlo de acesso e assiduidade dos seus colaboradores. A revolução digital transformou esse segmento, e soluções analógicas passaram a receber dispositivos robustos de identificação e controlo de acesso na virada do milénio. Mas afinal de contas, o que é controlo de acesso? Quais são as vantagens e desvantagens do emprego de um sistema RFID para controlo de acesso?

A assiduidade em um ambiente de trabalho é um dos pontos mais importantes que a empresa percebe em um funcionário. E se este colaborador for premiado por não faltar ao trabalho? Essa situação pode acontecer, por isso, o controlo de assiduidade de pessoal pode ser um grande diferencial no bom desempenho de uma equipa. Nesse sentido, o controlo de assiduidade de pessoal é importante em muitos aspectos, tanto em benefício da empresa quanto do próprio colaborador. Por outro lado, saber o quê e quem entra e sai da empresa é essencial para garantir a segurança, tanto das pessoas no local como dos bens. Uma das soluções mais indicadas para a protecção do património de empresas é o controlo de acesso. Ele padroniza a forma como colaboradores e visitantes acessão os ambientes, além de inviabilizar a circulação de pessoas não autorizadas em locais predeterminados.

Durante o estágio na CTM. levantou-se a questão da não existência de um sitema que controlasse o acesso dos trabalhadores e visitantes. Depois de uma investigação verificou-se que já existiu lá esse sistema e se encontrava avariado. A falta desse sistema, faz com que o controlo seja totalmente dependente das recepcionistas, contribuíndo assim para o mau controlo e gastos de matériais.

Dada esta situação, levantou-se a seguinte questão: das tecnologias existentes para controlo de acesso, qual sería a melhor opção para fazer o controlo de acesso na CTM?

1.3. Relevância da pesquisa

O projecto possui relevância pela necessidade de procurar uma solução para fraquezas no contexto de controlo de acesso e assiduidade dos trabalhadores da CTM. Actualmente, o controlo de acesso é feito por meio de cartão RFID, por outro lado o controlo de assiduidade é totalmente dependente do livro de ponto. Nos dias de hoje, as empresas de uma forma geral, sentem a necessidade de aferir a pontualidade e efectuar o controlo e gestão de acesso e assiduidade dos seus colaboradores. É nesse contexto que o controlo de acesso e assiduidade nas empresas actua como um poderoso aliado dos Gestores.

1.4. Metodologia

A metodologia é o estudo dos métodos, especialmente dos métodos das ciências. É um processo utilizado para dirigir uma investigação da verdade, no estudo de uma ciência ou para alcançar um fim determinado.

O processo de investigação do presente projecto compreenderá duas fases:

1.4.1. Fase Conceptual

- Pesquisas bibliográficas;
- Análise do terreno;
- Escolha e dimensionamento de componentes;
- Programação;
- Estudo de custos de implementação.

1.4.2. Fase Experimental

- Simulação do Sistema;
- Análise da aplicabilidade e possíveis resultados.

1.5. Objectivos

1.5.1. Objectivo Geral

- Projectar a proposta de um sistema de controlo de acesso e assiduidade dos trabalhadores da CTM.

1.5.2. Objectivos específicos

- Apresentar as actividades realizadas durante o estágio e o problema identificado durante o mesmo;
- Identificar as fraquezas de um controle de acesso e assiduidade manual;
- Identificar usuários que fazem parte de uma organização através da tecnologia RFID;
- Controlar entrada e saída dos usuários através de suas identificações RFID;
- Desenvolver um projecto para o controlo de acesso e assiduidade.

1.6. Justificativa

Com o sistema de controlo de acesso ao prédio de administração da CTM avariado, o controlo passa a ser totalmente dependente das recepcionistas, o que contribui para o mau controlo de acesso e assiduidade dos trabalhadores.Criando gastos com material (canetas, livro de ponto, álcool em gel, etc.) para registo de chegada e saída, longas filas na recepção para assinar o livro de ponto tanto na hora de chegada como na de saída dos trabalhadores (o que faz com que os trabalhadores comecem as suas actividades tarde devido a longa fila na entrada).

Por outro lado, sem um Sistema para o controle de acesso a planta de produção de energia, qualquer um que não esteja autorizado pode se fazer a planta, sendo que só os técnicos autorizados devem aceder a planta para trabalhos de manutenção. E isso faz com que tenha sempre um técnico de HST na entrada da planta para controlar o acesso da mesma.

1.7. Estrutura do trabalho

A estrutura do trabalho se divide nos seguintes capítulos:

Capítulo I

Consiste na apresentação do trabalho de forma geral, seus objectivos e metodologia usada.

Capítulo II

Consiste na apresentação das principais atividades realizadas durante o estágio, bem como uma breve descrição da instituição.

Capítulo III

Consiste na apresentação da componente teórica da pesquisa, abrange conceitos e processos relacionados aos sistemas de controlo de acesso, seus componentes e o problema identificado neles.

Capítulo IV

É apresentada a solução para o problema estudado no presente trabalho e avaliação económica do projeto.

Capítulo V

Consiste na apresentação da análise feita dos resultados obtidos após a implementação do sistema.

Capítulo VI

Avalia-se o cumprimento dos objetivos do trabalho e propõe-se recomendações para trabalhos posteriores.

CAPITULO II: VISÃO GERAL DO ESTÁGIO PROFISSIONAL

2. Actividades realizadas no estágio.

O estudante foi integrado no departamento de manutenção, onde trabalhou com engenheiros de instrumentação, em coordenação com outros engenheiros como mecânicos, elétricos, químicos, informáticos, etc.

As actividades realizadas durante o estágio foram as seguintes:

Tabela 1: Actividades realizadas durante o estágio. [Autor]

Semana	Dias	Actividades
1	18/04/22-22/04/22	Chegada às instalações da CTM; Processo de indução; Formação sobre as regras de segurança e valores da empresa.
2	25/04/22-29/04/22	Continuação da formação sobre as regras de segurança e valores da empresa, Formação sobre o funcionamento das unidades da central e do processo em geral.
3	02/05/22-06/05/22	Continuação da formação sobre o funcionamento das unidades da central.

4	09/05/22-13/05/22	Integração no departamento de instrumentação e controlo; Reunião de discussão sobre as fraquezas dos sistemas de alarme na HRSG; Manutenção de Sistemas(CCTV, Alarme, Controlo de Acesso).
5	16/05/20-20/05/22	Investigação do problema de não resposta das bombas da planta de des-salinização aos comandos da IHM do PLC; Configuração de um switch que serviria de sobressalente no equipamento de comunicação da central.
6	23/04/22-28/05/22	Integração no departamento manutenção industrial; Paragem e manutenção da turbina a gás 1; Limpeza de válvulas da planta de tratamento de água.

7	30/05/22-03/06/22	Integração a equipa da eléctrica; Formação sobre o funcionamento das bombas de combate ao incêndio; Formação para o acionamento do gerador principal.
8	06/06/22-10/06/22	Elaboração de procedimentos de de manutenção (preventiva, correctiva e checklist) e relatórios.
9	13/06/22-17/06/22	Substituição de switch na sala do director da central; Substituição de switch no prédio administrativo. Elaboração de relatórios técnicos.
10	20/06/22-24/06/22	Supervisão de sistema DCS e SCADA.
11	27/06/22-01/07/22	Elaboração de relatórios técnicos.
12	04/07/22-08/07/22	Elaboração de planos de calibração de instrumentos de medição.
13	11/07/22-15/07/22	Calibração de instrumentos de medição e sensores(PH, condutividade, indicadores de pressão e transdutores).
14	18/07/22-22/07/22	Elaboração de relatórios técnicos.
15	25/07/22-29/07/22	Diagnóstico de avarías relacionados ao sistema de automação da central;

		Elaboração de relatórios técnicos.
16	01/08/22- 05/08/22	Atribuição do tema para relatório de estágio; Elaboração de relatórios técnicos.

2.1. Apresentação da Central Termoeléctrica de Maputo.

A Central Térmica de Ciclo Combinado a Gás de Maputo está localizada a aproximadamente 6 km a noroeste da baixa da cidade de Maputo, capital de Moçambique. A instalação consiste em dois geradores de turbina a gás (GTG) de 40 MW a gás natural com dois geradores de vapor de recuperação de calor (HRSG), um gerador de turbina a vapor (STG) de 25 MW e seus equipamentos auxiliares.

Figura 1: Localização da Central Térmica de Maputo.[IMPACTO]

Figura 2:Turbina a Vapor. [autor]

A carga normal desta instalação é de aproximadamente 106 MW. A instalação utiliza duas turbinas a gás IHI-LM6000PF com a tecnologia Spray Inter-cooling (SPRINT).

Figura 3: Turbina a Gás. [autor]

A turbina a gás é equipada com tecnologia Dry Low Emission (DLE) para controlar as emissões como NOx e CO para um valor definido referenciado para 15% de oxigénio residual (O2) na chaminé de exaustão.

Para o sistema de ciclo combinado, o gás de exaustão da turbina a gás é direcionado para duas caldeiras, gerador de vapor de recuperação de calor de circulação natural sem ductos (HRSG), onde o calor dos gases de exaustão da turbina a gás é recuperado para gerar vapor.

Figura 4: Caldeira. [autor]

O HRSG está equipado com o sistema Chemical Feed que dosa o fosfato coordenado, antioxidante (não hidrazina) e amina. A turbina a vapor é aplicada para pressão mista, turbina de condensação e tipo multi-estágio. Esta capacidade de gerador de turbina a vapor é projectada para receber vapor HP e LP gerado pelo HRSG.

O tipo de condensador é refrigerado a ar com tubo de aleta. O sistema de condensado e água de alimentação inclui 2 bombas de condensado de 100%, bombas de água de alimentação de 3x50% HP e bombas de água de alimentação de 3x50% LP para dois HRSGS.

Figura 5: Condensador de Vapor. [autor]

O sistema de água de resfriamento para a planta é do tipo de ciclo fechado e inclui várias unidades de ventilador de ar, várias bombas de circulação de água de resfriamento, um tanque de expansão de água de resfriamento, um alimentador de pote químico, tubulação e acessórios. Este sistema de água de resfriamento de ciclo fechado fornece

água de resfriamento para resfriar o ar da GTG, sistemas de amostragem ST / HRSG, compressores de gás combustível, e trocadores de calor com bomba de vácuo. (Maputo 2017)

Figura 6: Fin Fan Coolers. [autor]

O alimentador de pote químico é usado para misturar o inibidor de corrosão e o biocida à água de resfriamento.

O sistema de gás combustível tem skid de medição de gás, dois lavadores de gás, dois filtros/separadores de gás, dois aquecedores de ponto de orvalho, skid de regulação de pressão de gás, três compressores de gás combustível, um tanque de buffer e um analisador de gás.

O sistema de ar comprimido possui dois compressores de ar, dois pré-resfriadores, dois receptores de ar comprimido e dois secadores de ar para fornecer ar de instrumento e ar de serviço à instalação.

Figura 7: Compressores de ar. [autor]

O sistema de protecção contra incêndio é equipado com hidrantes para área da planta e sistema de protecção contra incêndio de CO2 para gabinete de turbina a gás. O Sistema de água de incêndio está equipado com a tubulação para a área da planta. A Instalação é controlada pelo sistema de painel de controle local.

Figura 8: Bombas de combate ao incêndio. [autor]

Os geradores (GTG e STG) produzem uma tensão de 11 KV e são conectados a transformadores elevadores de 66 KV para a linha de distribuição. São também conectados a transformadores de 4 KV para o uso interno nos equipamentos da central e transformadores de 400 V para o uso nos edifícios da central. (Maputo 2017)

A Central possui uma planta de tratamento de água (WTP) e uma planta de desmineralização da água (DWTP), onde são retiradas todas partículas e de seguida a retirada de minerais e do sal onde posteriormente é enviada para o uso nas caldeiras (HRSG).

CAPITULO III: REVISÃO DA LITERATURA

3.1. Sistemas de Controlo de Acesso

Os Sistemas de Controlo de Acesso Electrónico são redes digitais que controlam o acesso a portais de segurança.[1]

Um portal de segurança é uma entrada ou saída de uma fronteira de segurança. A maioria dos Sistemas Eletrónicos de Controlo de Acesso funciona também como um sistema de alarme de intrusão. A partir deste ponto, assumiremos que os sistemas que estamos a discutir têm um elemento de sistema de alarme. Os Sistemas Electrónicos de Controlo de Acesso são compostos por equipamento de campo (sensores e dispositivos controlados), módulos de decisão, uma rede de comunicações, uma ou mais bases de dados, e um ou mais terminais de interface humana (estações de trabalho de computador).[1]

O que não é tão óbvio são os elementos "suaves" do Sistema de Controlo de Acesso. Estes incluem os Utilizadores, Políticas e Procedimentos, a Estrutura de Gestão e Relatórios, e a utilização do sistema para melhorar a avaliação contínua do Programa de Segurança global.[1]

Os elementos mais óbvios de um Sistema de Controlo de Acesso Electrónico são os Elementos de Campo: Portais do Sistema de Controlo de Acesso (para peões ou veículos), sensores de alarme, e quaisquer dispositivos controlados, tais como portas rolantes e luzes.[1]

Estes dispositivos ligam-se a um Painel de Controlo de Acesso, que concede autorizações de acesso baseadas na comparação da credencial apresentada na porta com uma base de dados de credenciais autorizadas. O Painel de Controlo de Acesso comunica com um Servidor através de uma rede informática proprietária ou TCP/IP. O Servidor mantém uma ou mais bases de dados, incluindo a base de dados principal de utilizadores autorizados, registos de configuração do equipamento, grupos de controlo de acesso, e horários. Também inclui eventos de controlo de acesso (pedidos/ autorizações/ cenários) e eventos de alarme. O servidor é operado por uma ou mais

estações de trabalho que são utilizadas para configurações de sistema, acesso interactivo e notificações de alarme, e relatórios.[1]

Todo o sistema deve ser operado de acordo com uma Política de Controlo de Acesso estabelecida.[1]

Existem dois tipos de controlo de acesso:

3.1.1. Controlo de acesso físico

O controlo de acesso físico é toda e qualquer aplicação de procedimento ou uso de equipamentos com o objectivo de proteger ambientes, equipamentos ou informações cujo o acesso deve ser restritos. Esse tipo de controlo envolve o uso de chaves, trancas, guardas, crachás, cercas, vídeos, cartões, biometria e etc.[2]

3.1.2. Controlo de acesso lógico

Aquele que controla acessos e conexões às redes de computadores, arquivos e dados do sistema. .[2]

3.2. Portais

A ideia de um Portal de Controlo de Acessos é central para todo o conceito de Sistemas de Controlo de Acessos. Um Portal de Controlo de Acesso é uma passagem através da qual uma pessoa ou veículo deve passar de um espaço para outro espaço mais controlado ou restrito e no qual só são permitidas pessoas autorizadas. [1]

Tipos de Portais

Existem dois tipos básicos de Portais de Controlo de Acesso: os destinados a peões e os destinados a veículos. Cada tipo tem muitas variações.

Praticamente todos os Portais de Controlo de Acessos têm os seguintes cinco elementos comuns: [1]

- Uma Barricada Operável, com Fecho;
- Um Método ou Dispositivo de Verificação de Identidade;
- Um mecanismo de bloqueio;

- Um dispositivo de sensoriamento de alarme;
- Um Sensor de Requisição de Saída.

Desde a porta de uma só folha mais comum até ao ponto de controlo de segurança de veículos mais complexo, todos têm estes elementos em comum. [1]

Portais comuns: O tipo mais comum de portal pedonal é uma porta de uma ou duas folhas. Esta é uma porta comum com um leitor de credenciais, fechadura electrificada, interruptor de posição da porta (DPS; dispositivo sensor de alarme), e algum tipo de sensor de pedido de saída (botão de pressão, detector de movimento, barra de pânico, etc.). Os tipos comuns de portais incluem portas giratórias, portas automáticas, e Man-Traps. Um Man-Trap é um vestíbulo com uma porta de entrada e saída do vestíbulo, sem saída pelo meio. As Man-Traps típicas requerem uma credencial para entrar e uma credencial para sair. O objectivo principal de uma Man-Trap é assegurar que nenhum utilizador não autorizado possa passar pelo portal enquanto a porta estiver aberta. Outros portais comuns incluem Lobbies de Elevadores, Elevadores, e Portas Automáticas. [1]

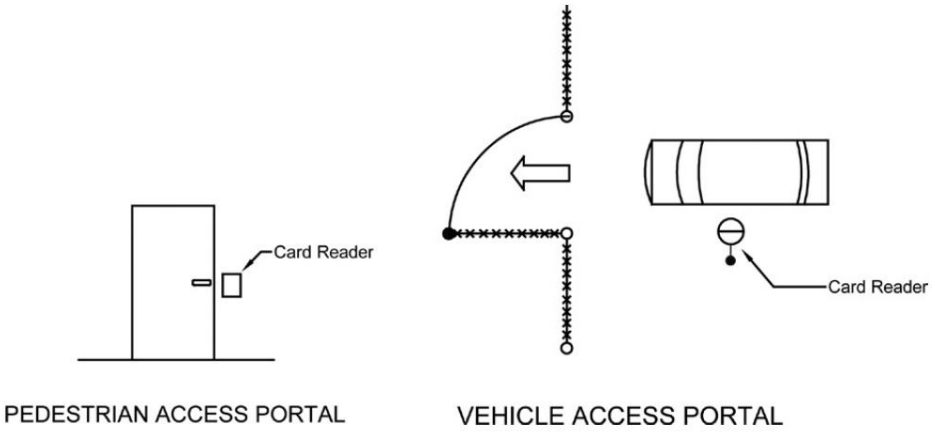

Figura 9: Portais de Controlo de Acesso. [1]

3.3. Métodos de identificação

Um usuário pode ser identificado de três maneiras distintas, onde cada técnica utiliza uma tecnologia diferente, com suas complexidades, vantagens e desvantagens. Sistemas de segurança são, normalmente, compostos por mecanismos para confirmar três fatores:

O que você sabe? O usuário conhece a credencial que irá ter o acesso, um exemplo bem comum e a senha;

O que você possui? O usuário possui uma credencial física que ira utilizar para ter acesso, como exemplo pode se citar o bilhete utilizado no sistema de transporte colectivo;

Quem você é? O usuário é sua própria credencial de acesso, por exemplo o biometria digital.

3.3. Métodos de validação

A análise dos métodos de validação e identificação biométricos é efectuada após uma breve introdução à biometria, nomeadamente o que se entende por biometria (quais os principais conceitos), bem como quais as principais características biométricas utilizadas nos sistemas de controlo de acesso. [3]

Em primeiro lugar irão ser utilizadas tecnologias biométricas como meio de identificação e verificação do utilizador. Posteriormente irão ser apresentadas tecnologias não biométricas ou “convencionais”, ou seja, as que não recorrem à biométrica como meio de identificação e validação do utilizador. [3]

3.3.1. Biométricos

A biometria (a palavra biometria vem do grego “bios” — vida e 'metr' — medir) consiste no reconhecimento dos indivíduos através de uma característica física ou comportamental, que são únicas de indivíduo para indivíduo. Entre as características medidas poderemos ter: [3]

- Face;

- Impressão digital;
- Geometria da mão;
- Íris;
- Voz.

Na biometria é necessário efectuar uma distinção entre identificação, reconhecimento e verificação. [3]

Identificação e reconhecimento são essencialmente sinónimos. Em ambos os processos, uma amostra biométrica é apresentada ao sistema biométrico, o qual tenta descobrir a quem pertence a amostra comparando-a com uma base de dados de amostras, biométricas com esperança de encontrar uma que combine/ coincida. Esta técnica é chamada comparação 1:n. [3]

Verificação é uma técnica de comparação 1:1 na qual o sistema biométrico tenta verificar a identidade de um indivíduo. Neste caso, uma amostra biométrica é capturada e comparada com o "template" (molde/registo) previamente armazenado. Se as duas amostras coincidirem, o sistema biométrico confirma que o indivíduo é quem diz ser. [3]

Os sistemas biométricos são essencialmente constituídos por quatro estados distintos - captura, extracção, comparação e validação, nos quais são igualmente aplicados os conceitos identificação, reconhecimento e verificação, ou seja, existem sistemas biométricos 1:n e 1:1. [3]

A principal distinção entre estes dois conceitos está relacionada com as questões/ perguntas colocadas pelo sistema biométrico e como estas interagem com uma determinada aplicação. [3]

Durante o estado identificação, o sistema biométrico pergunta, "Quem é este?" e estabelece a existência ou não do registo. Caso afirmativo, a identidade do indivíduo é a mesma a quem pertence o registo encontrado. [3]

Durante o estado verificação, o sistema biométrico pergunta, “Este indivíduo é quem diz ser?” e tenta verificar a identidade do indivíduo com o “template” (molde/registo) previamente armazenado. [3]

Figura 10: Métodos de validação biométricos. [4]

3.3.2. Não biométricos “convencionais”

Para além dos métodos biométricos acima mencionados, também é possível encontrar outros tipos de métodos de validação em sistemas de controlo de acessos, tais como o cartão magnético, código de barras ou etiquetas RFID (Figura). [3]

Para estes métodos, uma vez que são suportados com tecnologia convencional, são apresentadas as características estabelecidas de forma normalizada. [3]

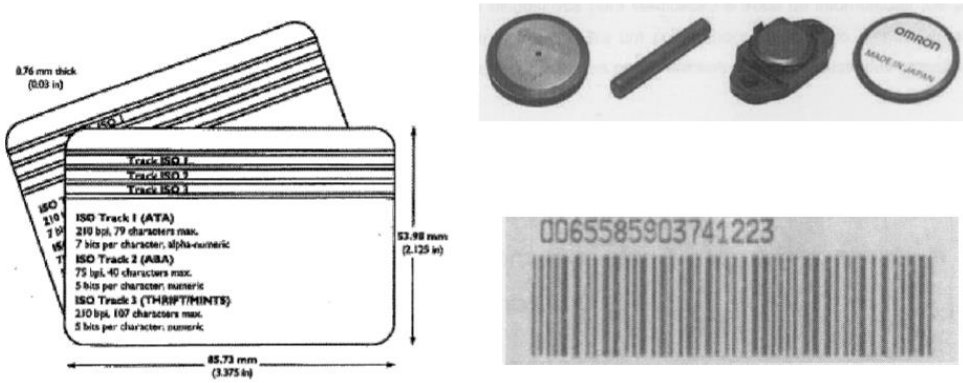

Figura 11: Métodos de validação não biométricos. [3]

3.4. Fraquezas de um sistema de controlo de acesso manual. [5]

Ainda que os métodos de ponto manual sejam rudimentares e antigos, muitas empresas empregam o uso de um ou outro para o registro de ponto de seus colaboradores. A forma mais antiga e suscetível a falhas é chamada Livro de Ponto, ou apenas Livro Ponto.

Nessa técnica de controle de ponto manual, o registro de entrada e saída dos funcionários é realizado por meio de um documento em que tudo é redigido à mão. Como é de se esperar, trata-se de um método extremamente falho, já que conta com a boa fé e competência das pessoas ao assinarem no livro.

O controle de acesso manual dos colaboradores pode gerar diversas complicações, desde consequências leves até as mais graves. Adiante, vamos abordar os principais tipos de problemas causados pela falta de um controlo de acesso eletrônico.

3.4.1. Aumento na carga horária de trabalho.

A evolução tecnológica em qualquer setor tem como um dos principais objetivos diminuir os esforços humanos para a realização de uma tarefa mecânica. Com o Sistema de controlo eletrônico não seria diferente.

A compilação dos dados do controlo manual é demorada e bastante trabalhosa. São várias horas de dedicação exclusiva para apurar todas as marcações de cada trabalhador e, depois, mais algumas horas para fazer os cálculos de horas trabalhadas, horas extras, faltas e saldos de banco de horas.

Com isso, muitas vezes é necessário ter uma quantidade maior de pessoas para conseguir fazer todas as apurações a tempo do fechamento da folha de pagamento, além de sobrecarregar cada uma, impossibilitando-as de exercer outras tarefas dentro da rotina do setor.

3.4.2. Maior risco de erros.

Toda atividade manual tem um risco de erro maior que atividades executadas automaticamente. Isso acontece porque os sistemas computacionais que estão por trás de tudo são elaborados com base em cálculos exatos, nas melhores práticas do mercado.

Além disso, existe o risco de erro nos cálculos em si. Mesmo que todas as informações dos livros de ponto sejam anotadas corretamente, a apuração de ponto manual requer um alto nível de concentração e bons conhecimentos matemáticos para garantir que os valores enviados para a folha de pagamento estejam corretos.

3.4.3. Menor segurança contra adulteração.

Ademais ao caso citado acima, de um erro involuntário dos colaboradores, também não podemos desconsiderar que as pessoas possam adulterar o Livro Ponto ou espontaneamente em benefício próprio, por exemplo, para acobertar um atraso ou ausência.

Da mesma forma, com o método mecânico também existe uma falha de segurança contra profissionais mal-intencionados. No caso de marcação, o que pode ocorrer é que um funcionário esteja marcando para outra pessoa.

3.4.4. Descentralização das informações.

A descentralização das informações no controle das jornadas de trabalho dos colaboradores pode causar muita perda de tempo e das próprias informações pessoais de cada funcionário.

Os cartões de ponto ficam armazenados em um local, as apurações em outro, os pedidos de folga e férias em outro, os comprovantes de justificativas de faltas como atestados médicos em outro. Reunir todas essas informações pode se tornar uma verdadeira jornada épica!

Imagine que um colaborador recebe um desconto por falta na folha de pagamento em um dia em que ele diz ter comparecido ao trabalho normalmente. Sem um controle mais centralizado das informações, fica muito mais difícil comprovar a validade da falta lançada, enquanto o colaborador pode ter diversos meios de confirmar sua presença.

3.5. Arquitetura e Componentes do Sistema de controlo de acesso físico.

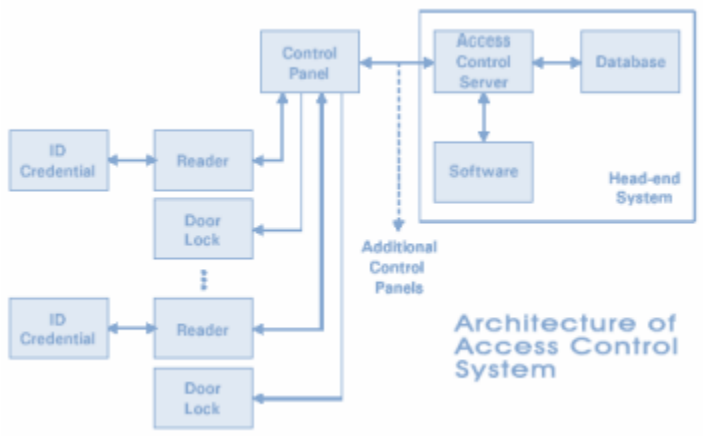

Figura 12: Arquitetura de um sistema de controlo de acessos físico. [6]

3.5.1. Credencial de ID.

A Credencial de ID são múltiplas as tecnologias de ID que podem ser utilizadas em sistemas de controlo de acessos físico. Podem-se apresentar sob uma grande variedade de formatos, sendo utilizadas para o armazenamento de dados que vai permitir a identificação e autenticação da credencial de ID e do seu utilizador.

As credenciais de ID que utilizam este tipo de tecnologia podem armazenar vários tipos de informação, taís como permissões, registos de assiduidade, números de identificação pessoais e templates biométricos que possibilitam a autenticação de factor múltiplo.[7]

Figura 13: Credencial de ID sob a forma de chaveiro de proximidade e Cartão de proximidade.[8]

3.5.2. Leitores.

Os Leitores são o meio de interacção do utilizador com o sistema. Podem ser de diversos tipos: Teclado, Banda Magnética, Proximidade, Códigos de barras, Ópticos e Biométricos (leitura da íris, impressão digital). [9]

Figura 14: Leitor de sistema de Controlo de Acesso. [10]

O leitor no local de acesso ou à entrada dum espaço físico pode ter uma ou mais interfaces, nomeadamente para:

3.5.3. Cartões de Proximidade.

O leitor utilizado para cartões de proximidade actua como um emissor/receptor de baixa potência que transmite ininterruptamente um campo electromagnético de RF. Quando um cartão de proximidade está sob o seu campo de alcance, a energia do campo é recebida através da antena interna do cartão e convertida para activação do seu chip interno que, em seguida, transmite pela antena os dados ao leitor.[11]

3.5.4. Teclados.

Servem para introduzir Códigos de Identificação Pessoal, podendo ser utilizados isoladamente ou em conjunto com outro tipo de leitor.[12]

3.5.5. Biométricos.

Dispositivos com capacidade de reconhecer as características referenciais que caracterizam os utilizadores (os dados biométricos mais utilizados são as impressões digitais, o padrão da íris, a geometria da mão, a voz e as características da face). O leitor biométrico mais conhecido é o leitor de impressões digitais. Este leitor é constituído por uma superfície, onde é colocado o dedo cuja impressão digital se quer analisar, que

contém um sensor capacitivo ou óptico que consegue extrair os detalhes da impressão digital e processá-los internamente através de algoritmos apropriados. .[12]

Figura 15: Leitor biométrico (impressão digital).[11]

3.5.6. Painel de Controlo.

O painel de controle é o ponto de comunicação central num sistema de controle de acessos físico. Interage e comunica com os múltiplos leitores, nos diferentes locais de acesso dos espaços físicos, com os fechos electromecânicos das portas de acesso ou com os mecanismos de desbloqueio dos torniquetes, podendo abri-los ou destravá-los, assim como, com o servidor de controlo de acessos.

Figura 16: Painel de controlo dum sistema de controlo de acessos físico.[13]

O painel de controlo começa por validar o leitor e aceitar os dados transmitidos por este. Em seguida, o processo vai depender do sistema de controlo de acessos ser: Centralizado ou Descentralizado.

Dependendo do sistema, o painel de controlo tanto pode processar os dados provenientes do leitor e do servidor de controlo de acessos e decidir sobre as permissões dos acessos (sistema distribuído), como pode enviar os dados para que o servidor do controlo de acessos tome essa decisão (sistema centralizado).

Por questões de segurança, é importante que seja o painel de controlo e não o leitor a efectuar a gestão do sinal de desbloqueio do fecho da porta do local de acesso. Isto, porque o painel de controlo está localizado no interior da organização, em princípio, numa área ou espaço seguro, enquanto o leitor poderá estar localizado numa área desprotegida ou insegura. [14]

3.5.7. Hosts

Hosts são os sistemas que irão controlar e processar os sinais enviados pelos leitores. Estes hosts podem ser um computador, smartphone, tablet ou qualquer outro dispositivo capaz de processamento. Cabe então ao engenheiro de controlo programar o host para realizar as leituras, processar os sinais e tomar uma acção com base nos dados colectados.[15]

3.5.8. Banco de dados.

Quando se trata de dados, sejam eles coletados de um questionário, de uma pesquisa ou até mesmo de uma TAG RFID, uma das melhores alternativas para se armazenar e manusear os mesmos é a ferramenta chamada banco de dados. Segundo Silberschatz, Sundarshan e Korth (2016, p. 4), "um sistema de banco de dados é uma coleção de dados inter-relacionados e um conjunto de programas que permitem aos usuários acessar e modificar esses dados". A tabela 1 mostra os tipos mais comuns:

Tabela 2: Tipos de sistema de gerenciamento de banco de dados.[16]

Tipos de banco de dados	Descrição
O Oracle Database	É o sistema de gestão de banco de dados mais utilizados no mundo. Trabalha com a linguagem SQL, e garante a segurança e diversos recursos para seus clientes e usuários.

O SQL Server	Criado pela Microsoft, é muito conhecido e utilizado no mercado. A linguagem usada nessa ferramenta é o T-SQL, e oferece recursos avançados e diferenciados para facilitar a actualização de dados e o armazenamento das informações de forma segura e confiável
O MySQL	É um banco de dados relacional que pertence à Oracle. Uma das características mais marcantes desse modelo é o fato de se tratar de um Open Source. Utiliza a linguagem SQL e funciona com as licenças de software comercial e livre.
O PostgreSQL	Também é um gerenciador de banco de dados relacional Open Source, comumente utilizado para sistemas online, como Skype, Apple.
O NoSQL	É um sistema de banco de dados não relacionais. Hoje, esse termo é comumente utilizado por pessoas que produzem conteúdos por dispositivos, redes sociais e outros tipos de funcionalidades web, que exigem a gestão de dados em diferentes formatos.
O MongoDB	É um dos maiores destaques do mercado. Esse banco de dados é Open Source e é um dos mais utilizados por diversas empresas. Seu sistema gira em Windows, Linux e OSX, com linguagem de programação C++.
O Redis	Se tornou um banco de dados popular no mercado, e também funciona como Open Source. Através desse sistema, as informações são armazenadas no formato de chave-valor.

3.5.9. Tecnologias para o Interface.

Para o desenvolvimento do Software Web usa-se uma página em HTML, interpretada pelo navegador de Internet (Microsoft Edge, Google Chrome e outros navegadores), para interagir com o usuário, formando a Camada de Apresentação. Outras tecnologias

podem ser misturadas ao HTML para a construção de uma interface mais poderosa, com um visual mais adequado, além de proporcionar recursos que o HTML isoladamente não é capaz (Costa, 2001).

Tabela 3: apresenta os tipos e a descrição das tecnologias responsáveis pela construção da interface com o usuário.[17]

Tecnologias	Descrição
HTML	É uma linguagem de Marcação padrão usada para construção de páginas WEB. O HTML Utiliza os conceitos do HyperTexto e da Hipermídia para apresentar num mesmo ambiente: dados, imagens e outros tipos de mídia, como vídeos, sons e gráficos. O HTML é um subconjunto do Standard Generalized Markup Language (SGML) e utiliza rótulos (tags) que definem a aparência e o formato dos dados, sendo padronizado pelo Object Management Group (OMG). É interpretado por qualquer navegador, em qualquer plataforma.
DHTML	É um conjunto de técnicas usadas para união das tecnologias HTML e JavaScript para tornar o HTML mais dinâmico. HTML é um termo utilizado para agrupar as tecnologias de script, cascatas de estilo e applets, as quais podem ser utilizadas em conjunto com o HTML tornando as páginas Web mais interactivas e animadas. O uso de tecnologias DHTML é possível graças à concepção do Document Object Model (DOM), que aplica os conceitos da orientação a objectos a todos os elementos de uma página HTML
Applet Java	A linguagem Java da Sun Microsystems, utilizada na forma de applets, é capaz de estender as funcionalidades dos navegadores, adicionando recursos antes impossíveis de serem construídos com o HTML puro. Os applets são miniprogramas executados sob o browser, através da Java Virtual Machine.

Active X	É uma estrutura de software da Microsoft (MSFT) que permite que os aplicativos compartilhem funcionalidades e dados uns com os outros por meio de navegadores da web, independentemente da linguagem de programação em que estão escritos
JavaScript	É uma linguagem de script que pode ser embutida na página HTML, oferecendo algumas formas de controlo da página, como a validação de campos. O JavaScript pode ser usado em quase todos os Navegadores, sendo que o Internet Explorer apresenta diferenças na sintaxe dos comandos, o que dificulta a capacidade multiplataforma das aplicações Web que utilizam o JavaScript.
VBScript	Possui a mesma filosofia do JavaScript, mas utiliza a sintaxe da linguagem Visual Basic da Microsoft, ao invés da sintaxe da linguagem Java
CSS	Permite que os estilos dos elementos da página (espaçamento, cores, fontes, margens, etc.) sejam especificados separadamente da estrutura do documento, facilitando dessa forma, uma futura modificação no estilo da página
XML	É uma linguagem de marcação, tal como o HTML. O XML lida com rótulos (tags) sendo possível definir conjuntos de tags próprios. A definição do padrão de tags, possibilita a criação de documentos num formato XML que podem ser facilmente interpretados pelo Navegador. Diferentemente do HTML, no XML não há tags para a aparência dos dados. O XML é também muito utilizado para padronizar a troca de informações entre sistemas.

3.5.10. Tecnologia RFID.[18]

A tecnologia RFID é uma tecnologia de identificação automática. Os processos de identificação, suportados por este tipo de tecnologias, são significativamente mais fiáveis e menos dispendiosos do que os de tecnologias não automáticas. A tecnologia RFID

representa um considerável avanço tecnológico, a nível da identificação automática, que contém enumeras vantagens, nomeadamente: na comunicação e transmissão de dados, que pode ocorrer sem linha de visão óptica, uma vez que as ondas electromagnéticas de radiofrequência podem atravessar diversos materiais; na velocidade do processo, dado que muitas tags e smart cards podem ser lidos mais rapidamente; na distância de leitura de dados, pois as diversas tecnologias de radiofrequência podem transmitir e receber sinais a maiores distâncias do que outras tecnologias. A capacidade da tecnologia RFID em comunicar sem linha de visão óptica e à distância, sem necessidade de contacto físico, reduz sensivelmente o envolvimento pessoal ou humano no processo de identificação. Além disso, a tecnologia RFID pode também suportar características funcionais, que outras tecnologias não possuem, tais como, memória regravável, funcionalidades de segurança, sensores ambientais.

Tecnologias RFID para o Controlo de Acessos Físico:

Para aplicações de controlo de acessos físico, existem três principais tecnologias de proximidade (RFID):

- 125 KHz;
- ISO 14443;
- ISO 15693.
- Tecnologia 125 KHz.

A tecnologia de 125 kHz é somente de leitura, é a mais antiga e, ainda, utilizada por muitos dos actuais sistemas de controlo de acesso físico baseados em RFID. A tecnologia de 125 kHz permite um único e seguro número de código, que será, depois, transmitido ao sistema do host system com o objectivo de poder ser processado e de se averiguar dos direitos e privilégios associados ao respectivo cartão.

Tecnologias ISO 14443 e 15693

A tecnologia de proximidade dos cartões smart cards está baseada nos standards ISO 14443 e ISO 15693. Os cartões que atendem a estes standards são “inteligentes”, permitem a leitura/escrita, são capazes de armazenar diferentes tipos de dados e de

operarem a diferentes distâncias. Têm capacidade de processamento, tanto para autenticar a identidade de uma pessoa, como para determinar o nível adequado do acesso, tudo isto, a partir dos dados armazenados no chip do cartão. Estes cartões podem, também, incluir factores adicionais de autenticação tais como, modelos biométricos, números de identificação pessoais e outras tecnologias associadas ao cartão, inclusive um chip de contacto, para satisfação de exigências relacionadas com aplicações legadas ou outras, nas quais é mais apropriado a utilização de uma tecnologia diferente.

3.5.10.1. Componentes básicos dos RFID.

O sistema RFID é composto por dois componentes básicos conforme a figura 15, o transponder ou tag, que é o objeto a ser identificado, e a unidade de leitura responsável por realizar a identificação da tag. Dependendo da concepção e tecnologia a unidade de leitura poderá ler e escrever dados na tag. [19]

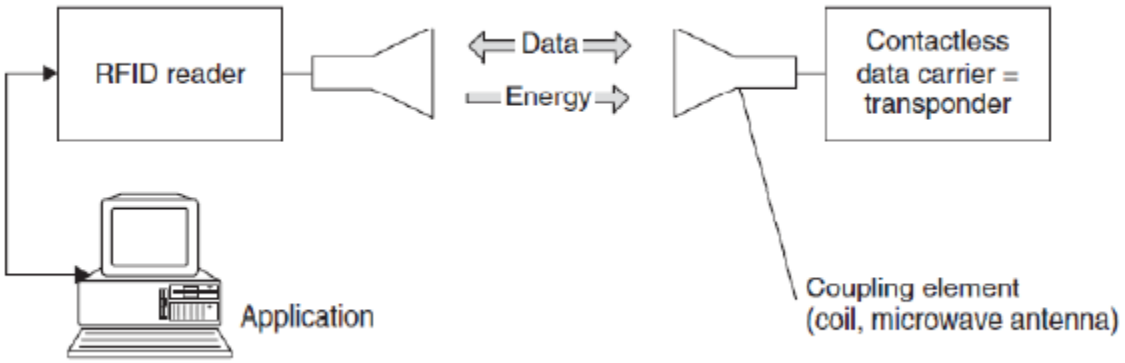

Figura 17: Principais componentes do sistema RFID: Leitor e Tag.[19]

Conforme a figura, a tag é composta por um microchip e uma antena, esta podendo ser de diversos formatos e tamanhos. Suas funcionalidades podem variar das mais simples, como os microchips de uso único que possuem dois estados ativo e não ativo, onde após ser inactivado este deixa de funcionar e a operação é irreversível, passando por outros que permitem a leitura das informações contidas nele, chegando aos mais sofisticados onde é possível realizar leituras e escritas na memória como sendo uma pequena base de dados.

A construção da tags é dinâmica, permitindo que esta possa ser de diversas formas e tamanhos, podendo ser tão pequeno quanto um grão de arroz. Pode ser constituída com materiais que permitem o funcionamento em condições extremas de calor, frio e humidade.[19]

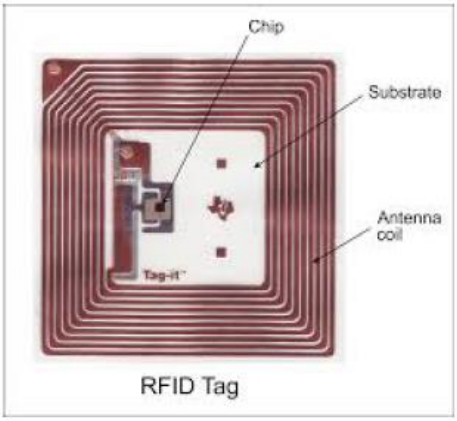

Figura 18:Componentes de uma Tag. [20]

A tag possui três possíveis modos de operação, sendo eles:

Passivo: a energia necessária para alimentação do microchip e todo o processo de comunicação será fornecida pela unidade de leitura, este irá ter seu alcance limitado em alguns poucos metros;

Ativo: possui uma fonte de energia própria, pode iniciar a transmissão dos dados independente da existência de uma unidade de leitura para receber os dados, pode estabelecer a comunicação com algumas dezenas de metros de distância;

Semi-ativo: possui uma fonte de energia própria, porém assim como a tag passiva depende de um estímulo da unidade de leitura para iniciar a comunicação. Seu alcance é superior a tag passiva e inferior a tag ativa.

A unidade de leitura é composta por uma antena para envio do sinal RF e por um chip. Este chip é responsável por gerenciar e controlar a comunicação com as tags, podendo rejeitar dados duplicados, realizar a correcção de erros entre outras funcionalidades. Alguns desses chips podem implementar mecanismos de segurança garantindo a integridade e confidencialidade das informações transmitidas durante o processo de comunicação.[20]

3.6. Vantagens e Desvantagens do emprego de RFID.[20]

Desvantagens:

Os sistemas RFID possuem um alto custo quando comparados aos sistemas de código de barras, e este é o principal obstáculo para seu uso em aplicações de logística. Outro problema enfrentado pela tecnologia é a aplicação em materiais metálicos e condutivos, já que estes afectam o alcance de transmissão. Os consumidores vêem a aplicação desta tecnologia em produtos de consumo como sendo uma invasão de privacidade. Para esse caso existem técnicas de bloqueio do RFID quando o consumidor sai da loja, mas ainda estão com custos elevados.

Vantagens:

Principal vantagem do uso da tecnologia RFID é a facilidade de identificação da tag. A tecnologia permite que seja realizada a leitura sem que seja necessário o contacto ou uma vista direta, sendo assim a tag pode ser aplicada internamente nos produtos ou em suas embalagens.

A tecnologia RFID possui outras vantagens, como o armazenamento de informações e um baixíssimo tempo de resposta, podendo ser inferior a 100 ms. Dessa forma, essa tecnologia torna-se uma boa opção para processos produtivos e para o controle de acessos, onde é necessário ler os dados da tag em movimento, permitindo que o produto carregue seu histórico, facilitando a contagem de estoques e agilizando a autenticação de pessoas.

3.7. Assiduidade no Trabalho.[21]

O dever de assiduidade caminha lado a lado com o de pontualidade. Na verdade, são dois deveres fundamentais para a vida dos trabalhadores, ligeiramente diferentes, mas que muitas pessoas poderão por vezes confundir.

Enquanto a pontualidade é o dever do trabalhador de comparecer ao serviço dentro das horas que forem designadas, a assiduidade é o dever de comparecer de forma regular e continuamente ao serviço.

3.8. Central Termoeléctrica de Maputo

A Central Térmica de Ciclo Combinado a Gás de Maputo está localizada a aproximadamente 6 km a noroeste da baixa da cidade de Maputo, capital de Moçambique. A instalação consiste em dois geradores de turbina a gás (GTG) de 40 MW a gás natural com dois geradores de vapor de recuperação de calor (HRSG), um gerador de turbina a vapor (STG) de 25 MW e seus equipamentos auxiliares.

3.8.1. Sistema de controle de acesso e assiduidade actual.

Atualmente, na CTM, o controle de acesso ao prédio de administração e controlo é feito por meio de cartões RFID e pelas senhoras da recepção, ou seja, os trabalhadores da CTM possuem um cartão que lhes permite ter acesso ao prédio de administração e controlo da central. Durante os quatro meses de estágio, o sistema se encontrava avariado, e as recepcionistas é que controlavam o acesso. Por outro lado, o controlo de assiduidade é totalmente dependente do livro de ponto e das senhoras da recepção para o controlo.

3.8.2. Sistema actual de controlo de acesso a planta de produção

Actualmente não existe nenhum sistema para controlo de acesso a planta de produção de energia eléctrica da CTM.

CAPíTULO IV: DESENVOLVIMENTO DO SISTEMA

A solução escolhida é de um sistema de controlo por RFID, por ser um sistema de baixo custo e de fácil manutenção. Dentre as escolhas principais para realizar este trabalho estavam diferentes microcontroladores. Devido a compatibilidade de integração com banco de dados, graças ao sistema operacional que pode ser instalado em um sistema, o modelo ESP32 foi escolhido. O uso de um sistema operacional, neste caso, pôde facilitar a implementação do software de leitura RFID além de propiciar melhor gerenciamento dos recursos do sistema.

4.1. Princípio de Funcionamento

O objectivo do sistema é acionar um relé através de contactos, que controlam o movimento de uma porta para abrir ou fechar a mesma através de sinal enviado das tags encontrados, através da comunicação SPI de usuário registado na base de dados, e caso este contacto tenha permissão para realizar esta operação os dados relevantes são incorporados e organizados para consulta (identificação, contacto, tipo de operação, data e hora).

Na figura 21, descreve-se a arquitectura do sistema.

No funcionamento do sistema pode-se distinguir três momentos:

- Leitura das TAGs para execução de tarefa;
- Processamento e organização de dados;
- Resposta do sistema e armazenamento de dados.

Leitura das TAGs para execução de tarefa

O usuário aproxima a TAG para módulo MFRC522 que por sua vez faz a leitura da TAG, e este envia sinal de leitura dos bits dos tags encontrados para o microcontrolador, através da comunicação SPI.

Processamento e organização de dados

Nesta fase o sistema faz a verificação e autenticação dos usuários e compila os dados para serem enviados à uma base de dados alojada num servidor e administrada com MySQL. Estes dados são organizados em forma de tabela para melhor visualização principalmente para as mensagens trocadas no serviço USSD.

Resposta do sistema e armazenamento de dados

Dependendo do comando a ser executado a porta deverá abrir ou fechar e em simultâneo, o display mostra para o usuário indicando o estado da operação. Os resultados das operações são armazenados no dispositivo do administrador e no servidor escolhido para tal efeito. Pode-se acessar estes dados através da base de dados criada para especificar identificação, contacto, tipo de operação, data e hora.

4.2. Arquitetura do Sistema

Para projectar um sistema como este, é necessário unificar diferentes subsistemas que permitam Identificar os agentes solicitantes dos acessos, verificar as permissões de acessos, autorizar ou negar acessos, registrar movimentos referentes aos acessos permitidos, alertar e registrar tentativas de acessos não autorizados, permitir consultas e emitir relatórios sobre os acessos concebidos com detalhes da sua movimentação, assim como das tentativas de acessos não autorizadas ao ambiente, armazenar e transferir os dados adquiridos. O sistema foi desenvolvido utilizando o ESP32.

A figura 21 mostra o diagrama de bloco do sistema, que explica de uma forma resumida o funcionamento geral do sistema, o mesmo que será explicado detalhadamente nos passos subsequentes.

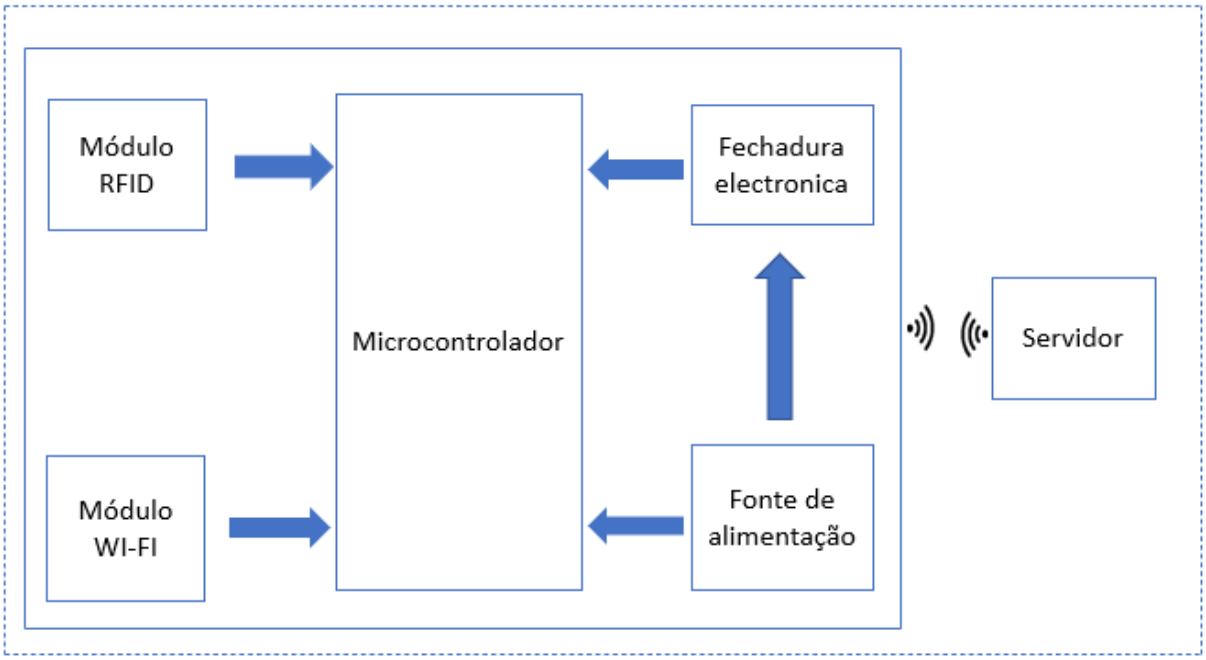

Figura 19: Diagrama de blocos do sistema. [Autor]

4.1.1. Fonte de Alimentação: dispositivo responsável por alimentar o sistema

4.1.2. Módulo RFID: são dispositivos de entrada do sistema, responsáveis pela leitura dos cartões ou tag e enviar os dados para o microcontrolador.

4.1.3. Módulo WiFi: é um dispositivo de entrada, responsável por conectar o microcontrolador a internet.

4.1.4. Fechadura Electrónica: são dispositivos de saída do sistema, responsáveis pelo bloqueio físico.

4.1.5. Microcontrolador: elemento central do sistema, que irá comparar os dados enviados por módulo RFID, Câmera, e dados armazenados no banco de dados.

4.1.6. Servidor: é um software ou computador, com sistema de computação centralizada que fornece serviços a uma rede de computadores, no qual são instalados banco de dados e o módulo principal do software de gerenciamento do sistema.

4.1.7. Terminal/HMI: é uma estação de trabalho e ponto de acesso a rede computacional na qual é instalado o aplicativo de operação do software de controle de acesso.

4.2. Requisitos funcionais do Sistema:

1. Configurar tag do usuário com permissões de acesso, nível de usuário, zona e tempo e validade;
2. Inativar tag do usuário para que o mesmo tenha sua solicitação de acesso negada;
3. Liberar o acesso de usuários previamente cadastrados e sem restrições;
4. Bloquear o acesso de usuários não cadastrados ou irregulares;
5. Indicar ao usuário se foi aceite ou negada a solicitação de acesso;
6. Monitorar estado da porta identificando se está aberta, fechada ou se houve um arrombamento;
7. Registrar log dos acessos de entrada e saída dos usuários em cada um dos dispositivos;

4.3. Especificações Gerais do Sistema

Na tabela 4 pode-se observar as especificações gerais do protótipo, onde o número máximo usuários e sectores foi limitado para permitir que todas as informações sejam armazenadas na memória RAM do ESP32, para permitir uma melhor capacidade de resposta do sistema.

Tabela 4: Especificações Gerais do Protótipo. [16]

Especificações técnicas	**Descrição**
N°. máximo de usuários cadastrados	498 Por Sector
Interface gráfica baseada	Baseada na web centralizada
Controlo de múltiplos sectores	Suportando até 45 sectores simultaneamente
N°. máximo de horários	Até 22.410 (498 por sector)
N°. máximo de registos	500.000 Com armazenamento estendido

4.4. Componentes do sistema

Esta secção apresenta a descrição técnica dos componentes electrónicos que foram usados para a concepção do protótipo.

Microcontrolador

Para a concepção do protótipo foi escolhido o ESP32 ilustrado na figura 22, é microcontrolador CMOS de 32 bits. Projectado com a tecnologia TSMC de ultrabaixa potência e baixo custo, Com Bluetooth e WiFi já integrados. Vide a tabela 6 as especificações técnicas.

Tabela 5: Especificações técnicas do ESP32.

Especificações técnicas	**Descrição**
Microprocessador	*Xtensa* ® Dual-Core 32-bits LX6 com um desempenho de 600 DMIPS
Memória ROM	448 Kbytes
Memória SRAM	Possui 520 KBy da memória *flash*
Clock máximo	240MHz
Memória Flash	4 MB
Wireless padrão	802.11 b/g/n
Conexão Wifi	2.4GHz
Alimentação	2,2 a 3,6 V
Temperatura	- 40°C a 125°C

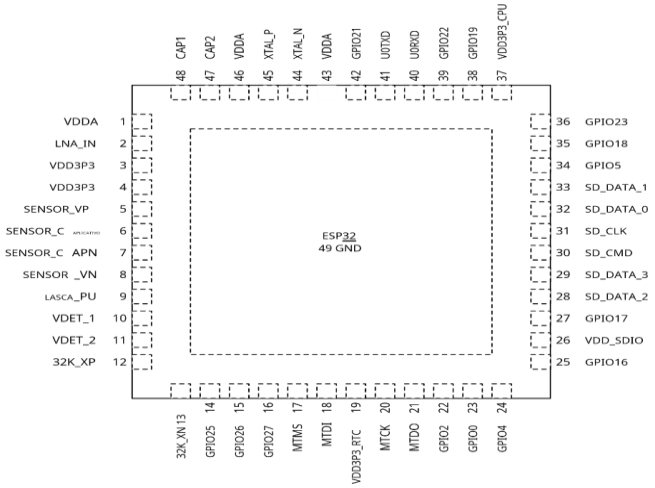

Figura 20: Microcontrolador ESP32.

Fonte de Alimentação

A fonte de Alimentação do Protótipo é o módulo Transformador (Fonte de Alimentação AC-DC 5V 700mA 3.5W Conversor AC 220V para DC 5V) ilustrado na figura 20 de alta qualidade possui um desempenho estável e rentável. A tabela 6 apresenta especificações técnicas

Tabela 6: Especificações da fonte de alimentação

Especificações técnicas	**Descrição**
Tensão de entrada AC	85 a 265V, 50Hz;
Tensão e Corrente de saída DC	5V e 700mA;
Potência:	3,5W;
Temperatura de operação	20ºC a 60ºC;
Humidade relativa:	40-90%
Eficiência de saída:	80%;

Figura 21: Fonte de alimentação.[23]

Modulo RFID

O Leitor RFID-RC522, TAG tipo chaveiro e cartão RFID é baseado no chip MFRC522 da empresa NXP é altamente utilizado em comunicação sem fio a uma frequência 13,56MHz, de baixo consumo e pequeno tamanho, permite sem contacto ler e escrever em cartões que seguem o padrão Mifare.

Tabela 7: Especificações técnicas do MFRC522.[23]

Especificações técnicas	**Descrição**
Frequência de operação	13,56MHz
Alimentação DC	2.5 a 3.3 V
Temperatura de operação	- 20°C a 80°C
Taxa de transferência	10 Mbit/s
Dimensões	8,5 x 5,5 x 1,0cm
Humidade relativa	5% – 95%
Peso	21g
Tipos de cartões suportados	Mifare1 S50, S70 Mifare1, Mifare UltraLight, Mifare Pro, Mifare Desfire

Figura 22: Kit de Modulo RFID baseado no chip MFRC522. [24]

Tela

Para visualização de dados no protótipo foi escolhido o módulo LCD associado a um módulo I2C (vide a figura 10). Para o I2C suportar o LCD é necessário conectar os seus 16 pinos em ordem de expansão para em seguida conectar ao microcontrolador. A tabela 8 apresenta as especificações técnicas do módulo LCD associado com o módulo I2C.

Tabela 8: Especificações técnicas do módulo LCD com o módulo I2C.

Especificações técnicas	**Descrição**
Interface de comunicação	I2C
Comunicação	4bits ou 8bits
Controlador do módulo I2C	PCF8574T
Cor do fundo	Azul
Tensão de Operação DC	4,5V a 5,5V
Número de caracteres (colunas x linhas)	16x2
Dimensões	36mm(L) x 17mm(A) x 83mm(C)
Tamanho da janela (alt. x larg.)	66x16 mm
Iluminação	LED
Cor da iluminação	Branca

Figura 23: Display Lcd 16x2. [24]

Teclado Matricial

Teclado é um dispositivo de entrada pois permite, por meio de botões, inserir dados em um dispositivo.

Internamente são 16 teclas *push-buttons* tipo membrana. Conforme a tecla é pressionada, é feita a conexão entre a linha e a coluna correspondentes. Exemplo de funcionamento, se pressionarmos a tecla A no teclado matricial, será feita a conexão entre os pinos 1 (linha 1) e 8 (coluna 4).

Os pinos das linhas deverão ser configurados como OUTPUT (Saída), e os pinos das colunas como INPUT (Entrada). Nos pinos referente às colunas, devera usar – se 4 resistores *pull-down,* mantendo-as em nível baixo quando não houver accionamento das teclas.[24]

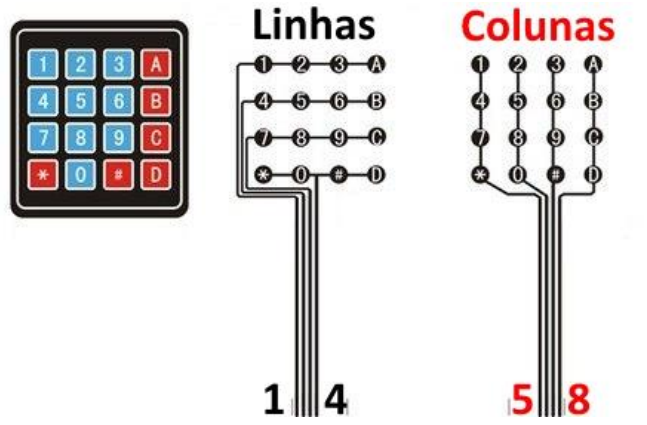

Figura 24: Teclado Matricial. [24]

Modulo Relé

O módulo relé é o dispositivo escolhido para accionar o micro servo, na figura 23 pode – se observar o módulo relé. Ele é equipado com transístores, conectores, leds, díodos e relés de alta qualidade. Cada canal possui um LED para indicar o estado da saída do relé. A tabela 9 apresenta especificações técnicas do módulo relé.

Tabela 9: especificações Técnicas do Modulo relé. [24]

Especificações técnicas	**Descrição**
Modelo	JQC-3FF-S-Z
Tensão de operação	5 VDC
Permite Controlar cargas	220V AC
Tensão máxima de saída	28 VDC a 10ª ou 250VAC a 10A
Dimensões	50 mm x 37 mm x 18 mm
Tempo de resposta:	5~10ms
Pinagem	Normal Aberto, Normal Fechado e Comum
Peso	30g

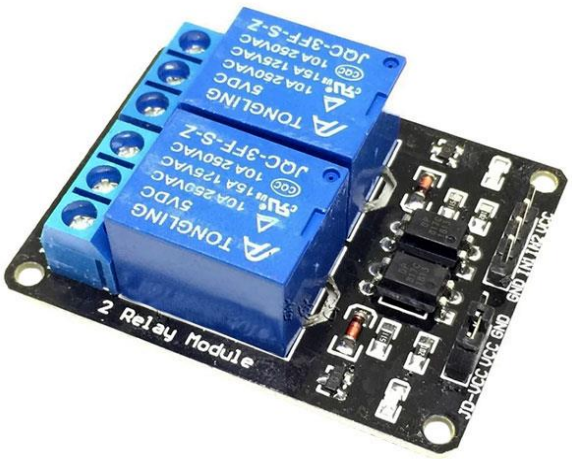

Figura 25: Modulo rele de 2 canais. [24]

4.5. Dimensionamento do projeto.

4.5.1. Esquema elétrico do Sistema.

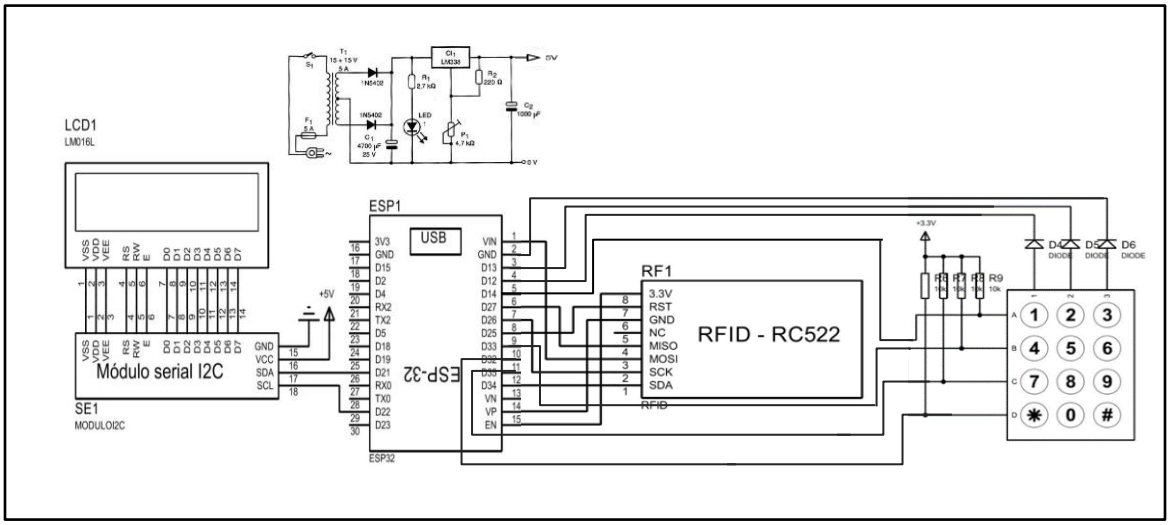

Figura 26: Esquema eléctrico do sistema [elaborado pelo autor]

O elemento central do sistema é o ESP32, que faz o controlo de todos os outros elementos do sistema. Os elementos estão ligados do seguinte modo:

- Ligado aos pinos RST, MISO, MOSI, SCK e SDA encontra-se o módulo MFRC522 conectado ao microcontrolador. Estes enviam sinal de leitura dos bits dos tags encontrados, através da comunicação SPI;
- A alimentação dos dispositivos é feita através de Fonte de Alimentação AC-DC 5VDC;
- Ligados os pinos A, B, C, D, 1, 2 e 3 encontra-se o teclado matricial, que introduz dados no microcontrolador.

Esta proposta integra o circuito de comando do controlador através dos contactos de acionamento, para possibilitar o envio de sinal de abertura ou fecho de porta. O sinal é recebido pelo circuito do operador a partir de uma entrada para relé (NC/ NO), que tem o seu caminho de retorno num ponto de terminação comum. O LCD utilizado neste protótipo é auxiliar para obter informação em relação ao estado de abertura ou fecho da

porta, num caso de produto final real poderia ser substituído por um LED. A luz do mesmo estando ativada indica que a porta se encontra aberta, e fechada para a luz desativada.

4.5.2. Instalação do equipamento.

O sistema proposto pode ser divido em dois blocos: o dispositivo de leitura e servidor.

O sistema será composto por dois dispositivos de leitura para controlar a abertura da porta, e serão instalados um na entrada e um na saída do bloco administrativo da CTM e também na entrada e saída da planta de produção, como pode ser observado na figura 26. O dispositivo de leitura na entrada e saída serão instalados na parede perto da porta a uma altura de 1.1 metro em relação ao chão e a uma distância de 0.2 metro em relação a porta, como pode ser observado na figura 27.

Servidor, onde é instalada a aplicação para gerenciamento, permitindo a realização dos cadastros e auditoria com o auxílio dos registros de acessos será instalado na sala de comandos da CTM.

Descrição:

1. Fechaduras magnéticas;
2. Estação de acesso (composto por teclado e leitor de cartão);
3. Botão de acesso de emergência;
4. Painel de controlo de portas;
5. Painel de controlo principal;
6. PC;
7. Outro painel de controle;
8. Fonte de energia.

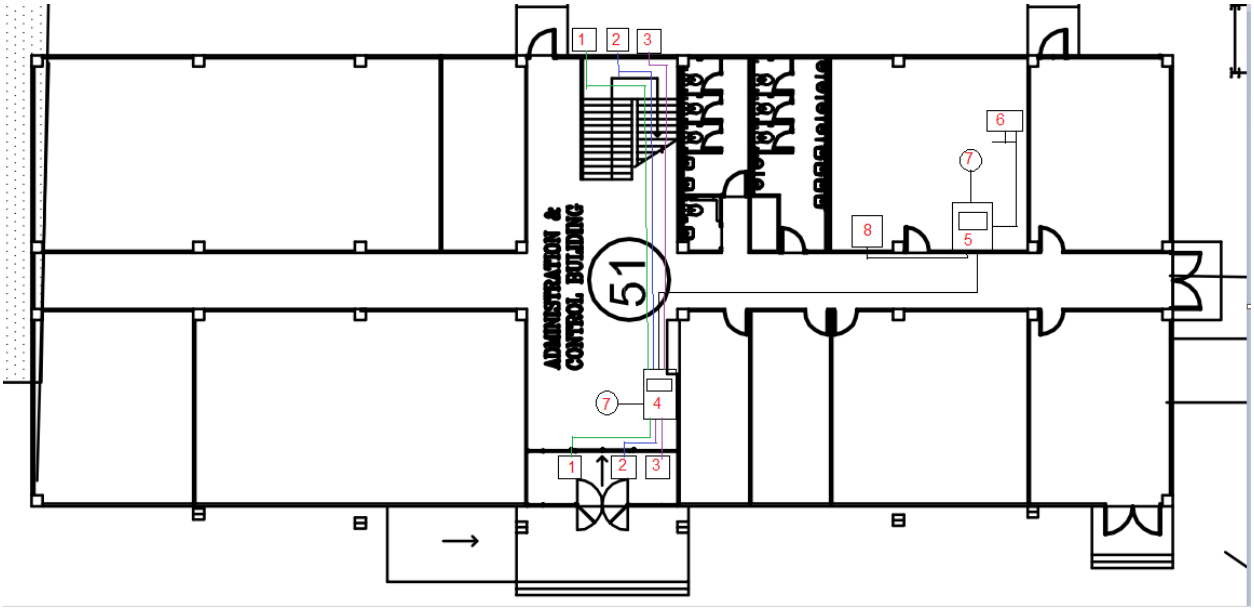

Figura 27: Esquema de Instalação dos equipamentos na planta do bloco administrativo da CTM. [elaborada pelo autor].

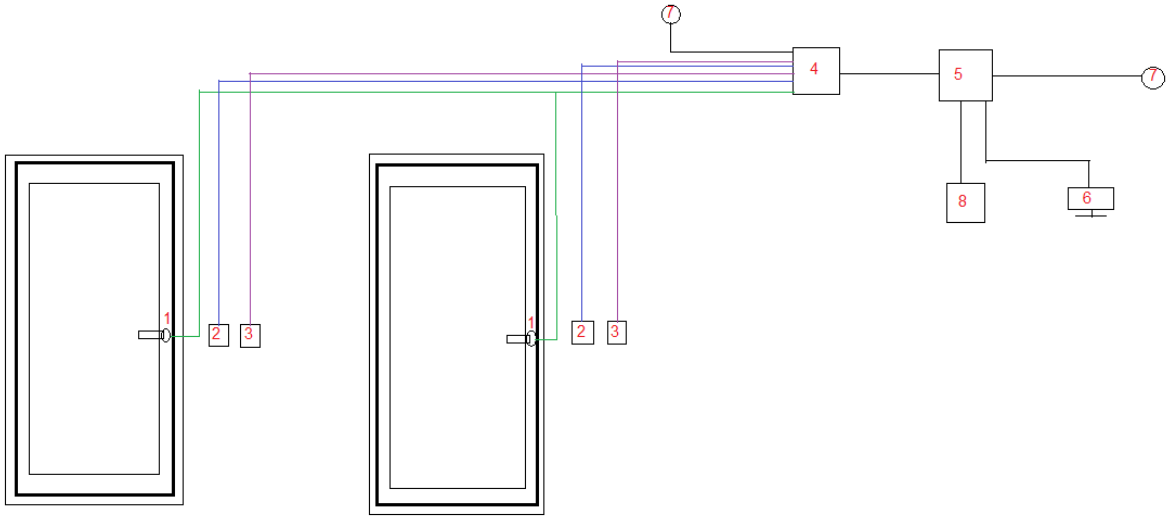

Figura 28: Esquema de Instalação de equipamento de leitura na saída e entrada da porta da CTM. .[elaborada pelo autor].

4.5.3. Programação

Fluxograma

Inicialmente, o sistema conecta - se ao servidor e faz todas as requisições necessárias e activa o módulo MFRC522, para autenticação cadastro, remoção de cartões e actualizar o horário. O usuário aproximará o cartão da unidade de leitura. Deste modo serão lidas as informações armazenadas na tag e processadas. Será constatado que a credencial identificada possui ou não a autorização de acesso, a unidade de controle envia a mensagem de acionamento para a I/O - Acionamento. Em seguida, a unidade de controle realizará o registro do resultado da solicitação de acesso na memória do controlador de acesso.

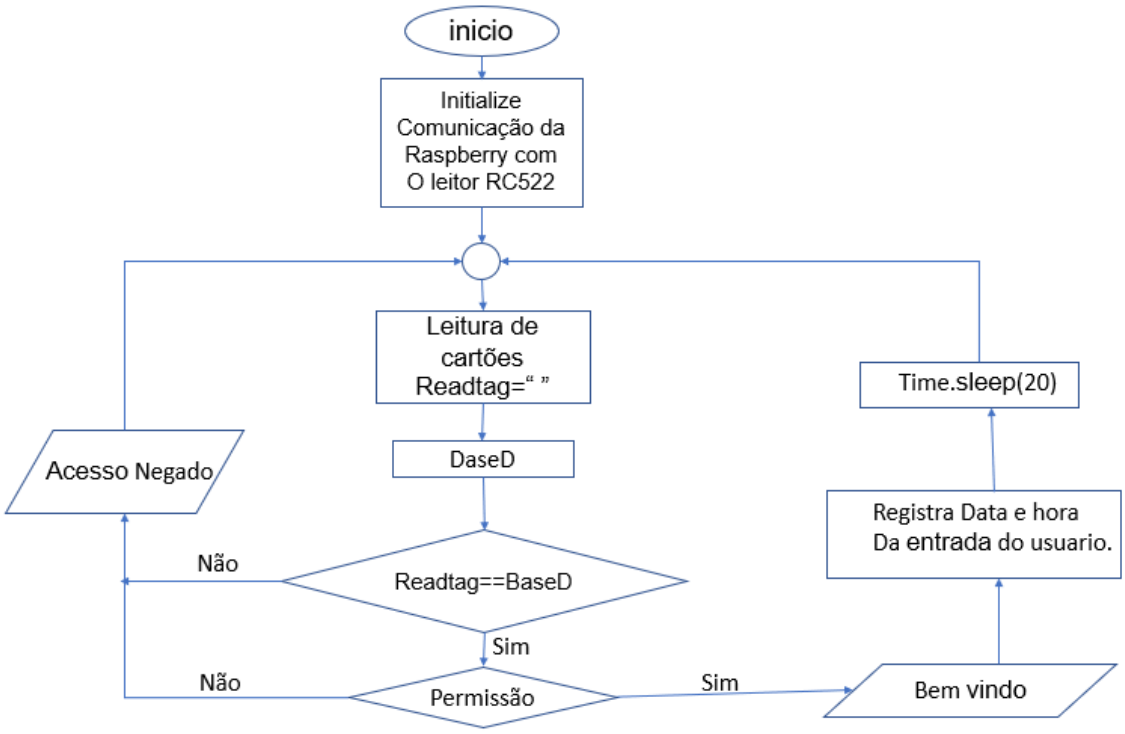

Figura 29: Fluxograma para o controlo de entrada dos usuários. [elaborada pelo autor]

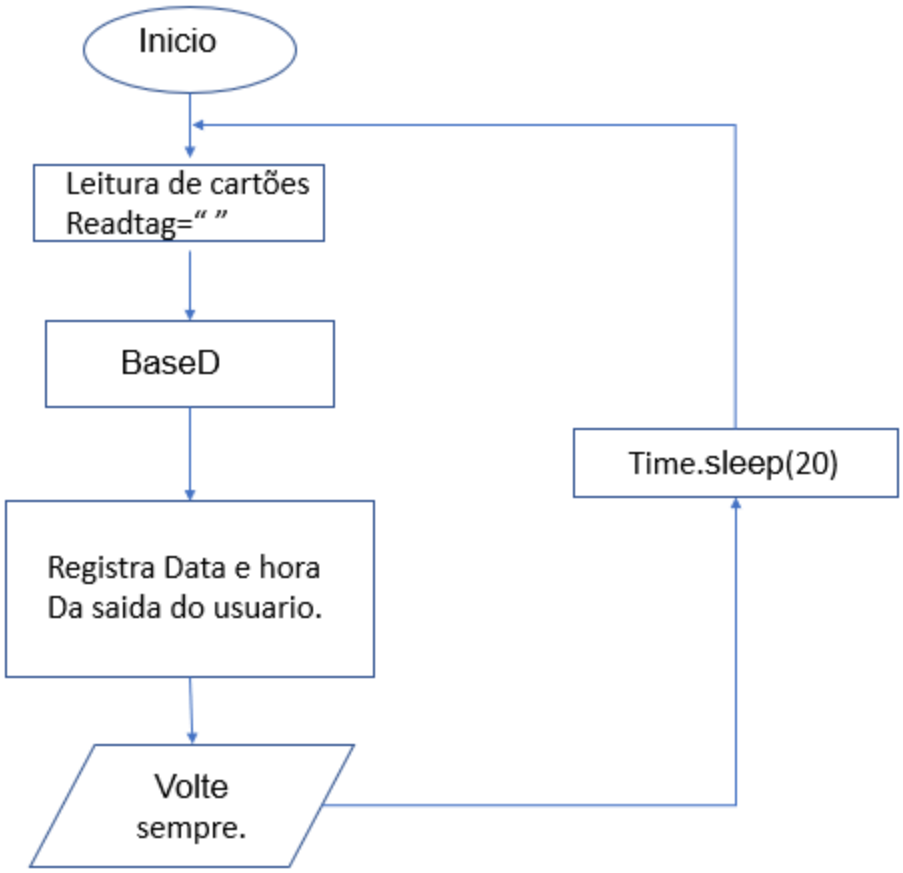

Figura 30: Fluxograma para o controlo de saída dos usuários. [elaborado pelo autor]

Cadastro de Usuários

O registo de dados pode ser feito manualmente por pessoas autorizadas para tal.

Para realizar o cadastro de usuários e suas TAGs no banco de dados foi implementada a lógica explicada no fluxograma da Figura em que seu conteúdo é recebido posteriormente pelo GUI para concluir o cadastro. O usuário passa o seu cartão para autenticação, caso o sistema reconheça o usuário como autorizado para este processo deverá habilitar uma posição na matriz de cadastro, que será introduzido o nome do novo cartão e o UID do próprio cartão. O sistema deverá fazer a verificação/ varrimento destes dados e registar na MySQL.

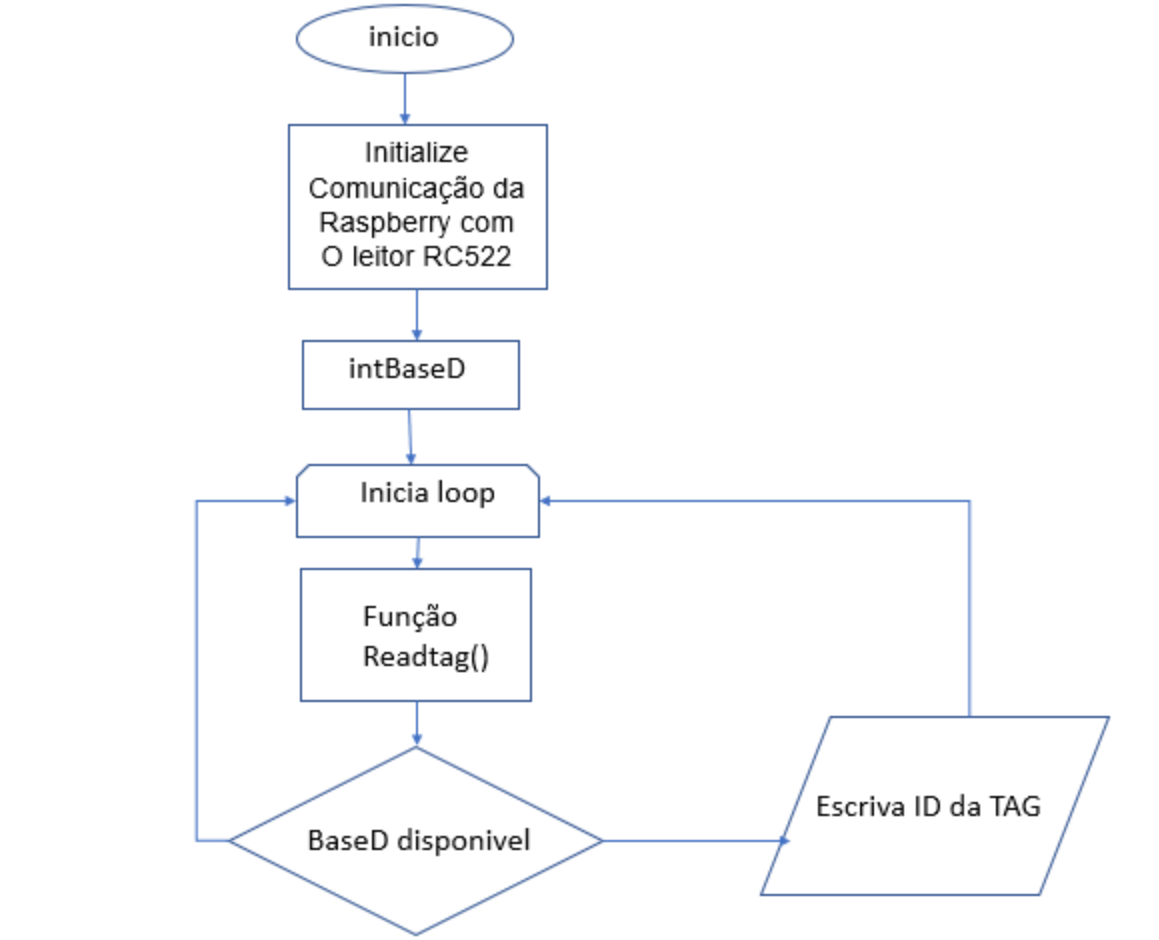

Figura 31: Fluxograma para realizar o cadastro de usuários. [elaborado pelo autor]

O administrador da base de dados também pode a partir dos comandos de MySQL adicionar ou remover um usuário.

Banco de Dados

Para a criação da base de dados foi utilizada a plataforma de gestão de base de dados *MySQL* de código aberto. Passos para criar o *MySQL* e definir a API:

- Instalar o servidor *MySQL*, servidor *web* e *PHP*;
- Criar conta de usuário *MySQL;*
- Criar banco de dados *MySQL*;
- Criar tabela *MySQL*;

- Escrever arquivos de script PHP;

Após a instalação, verificou – se a pasta **C:\xampp\htdocs.** Onde é colocado o código PHP. Abriu – se o painel de controlo do XAMPP, fez – se o *Start* do *MySQL* e *Apache* para habilitar o servidor *Web* e o *MySQL* (vide a figura 17).

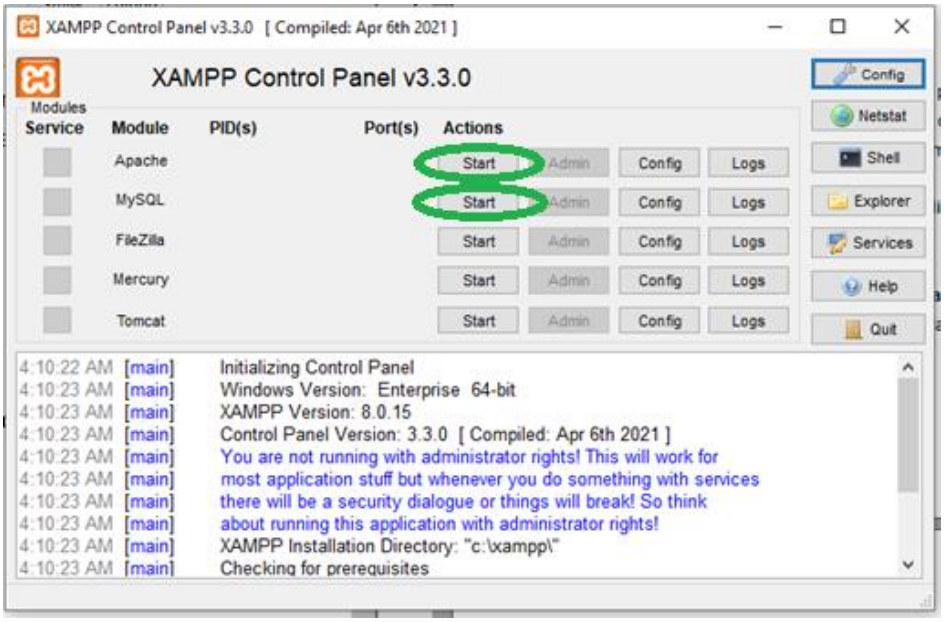

Figura 32: Painel de Controlo XAMPP

Foi Criada a conta *MySQL* com apenas permissões de acesso local, mesmo que os invasores saibam o nome de usuário/senha, eles não podem a cessar o banco de dados *MySQL*. O nome de usuário/senha é usado pelo PHP para se conectar ao banco de dados *MySQL.*

Passos para definir e interfacear o tipo de aplicativo

- Primeiro importa-se a biblioteca Flask para janelas Web que utilizam Python como código de desenvolvimento de aplicativos;
- Configura-se o aplicativo através do nome da base de dados, da senha e do endereço do host;
- Dependo da dinâmica do aplicativo a ser configurado, utiliza-se classes para consultar as tabelas no MySQL: Neste caso específico existe um menu principal

onde são descritas opções para operações do motor de activação da porta e enviadas para a base de dados.

- Utilizando o método @app.route pode-se indicar ao Flask que URL deverá activar a função desejada.

Sequência de criação de tabelas para base de dados

- Criar novo ambiente virtual (virtualenv);

Comando: mkvirtualenv --python=python3.6 myproject

- Entrar no ambiente virtual criado;

Comando: workon myproject

- Instalar pacotes necessários para utilizar SQLAlchemy;

Comando: pip install flask mysqlclient flask-sqlalchemy

- Criar as tabelas e armazenar dados dos usuários;

Comandos:

- CREATE TABLE LOG_USER (id int auto_increment, phone varchar(50),opcao varchar(50) PRIMARY KEY(id));

- *cd C:\xampp\mysql\bin*
- *mysqladmin -u root password YOUR_ROOT_PASSWORD*
- *mysql.exe -u root –p*
- *CREATE USER 'Nome'@'localhost' IDENTIFIED BY 'Senha';*
- *GRANT ALL PRIVILEGES ON *.* TO 'Nome'@'localhost' WITH GRANT OPTION;*
- *FLUSH PRIVILEGES;*

Usou – se o comando o *CREATE DATABASE db_esp32 CHARACTER SET = 'utf8' COLLATE = 'utf8_general_ci';* para criar o banco de dados

- Para visualizar os dados incrementados nas tabelas após acessar a base de dados protegida por uma senha utiliza-se o comando: SELECT* from nome_da_tabela

4.6. Custo estimado do sistema.

Abaixo, são apresentados os custos estimados dos componentes do sistema proposto:

Tabela 10 Custo estimado do sistema

ITEM	DESCRIÇÃO	PREÇO Unitário (MT)	QUANTIDADE	TOTAL (MT)
1	Microcontrolador ESP32	1.500,00	1	1.500,00
2	Modulo Rele De 2 Canais	250,00	1	250,00
4	Capacitor	6,00	10	60,00
5	LM7805	20,00	1	20,00
6	Resistor	5,00	1	5,00
7	Díodo	7,50	10	75,00
8	Kit De Modulo Rfid	270,00	1	270,00
9	Módulo Lcd - I2c	500,00	1	500,00
10	Buzzer	90,00	1	90,00
11	Teclado matricial	170,00	1	170,00
12	bateria	350,00	1	350,00
total				3.290,00

Nota:

A estimativa é válida para o dia 24.11.2023, os preços podem variar. Na estimativa feita não foram adicionados outros custos para cabeamento, estruturas de suporte, etc.

CAPíTULO V:

5. Análise e Discussão dos resultados

Teste de Servidor Web

O servidor web é utilizado não apenas para a interface gráfica do usuário, mas também para a intercomunicação de módulos. Essas melhorias podem ser vistas nos tempos de carregamento das páginas. Ao baixar arquivos grandes (como o arquivo de registos), a

```
Conectando-se a 192.168.12.20:80... conectado.
A requisição HTTP foi enviada, aguardando resposta... 200 OK
Tamanho: 99967 (98K) [text/plain]
Salvando em: “registro.csv”

registro.csv         100%[====================>]  97,62K   307KB/s    em 0,3s
```

velocidade média de download é em torno de 300 KB/s (2,4 Mbps), conforme mostrado na figura.

Tempo de inicialização

O tempo de inicialização do sistema inclui o tempo necessário para:

- Configurar os pinos e componentes do ESP (RFID, RTC e relé);
- Carregar os 4 arquivos de configuração (Rede, sectores, hora e senhas);
- Iniciar o servidor web;
- Carregar os bancos de dados (usuários, sectores, horários);
- Conectar-se à rede Wi-Fi;

Todas essas acções são feitas em 2,3 segundos como mostrado na figura abaixo. Isso significa que, em caso de reinicialização ou restauração de energia, os módulos estarão *online* e funcionando em menos de 3 segundos, um tempo impressionante que foi alcançado após muitas melhorias

```
23:30:34.629 -> Iniciando...
23:30:35.060 -> Lendo configurações de setor...
23:30:35.060 -> Lendo configurações de rede...
23:30:35.159 -> Lendo configurações administrativas e chaves de criptografia...
23:30:35.623 -> Iniciando servidor...
23:30:35.623 -> Coletando usuários...
23:30:35.855 -> Coletando setores...
23:30:35.955 -> Coletando horários...
23:30:36.054 -> Coletando SHA...
23:30:36.783 -> Checando rede... -> 192.168.12.20
23:30:36.783 -> Lendo configurações de data e hora...
23:30:36.883 -> Hora atualizada! -> MDD=1350
23:30:36.916 -> Iniciado!      Tempo de boot: 2298ms
```

Testes de velocidade

Para todos os testes de velocidade desta seção, o sistema está trabalhando em sua capacidade total para garantir que os resultados correspondam ao pior cenário em termos de tamanho de banco de dados. Isso significa que o sistema está utilizando bancos de dados com um total de 498 usuários e 49 sectores.

CAPíTULO VI:

6. Considerações finais

6.1. Conclusão

O presente trabalho teve como tema, Proposta de um sistema de controle de acesso e assiduidade dos trabalhadores da Central Termoelétrica de Maputo**.** Tendo como foco a identificação das permissões de acesso a partir da leitura dos dados armazenados na memória da tag RFID e registrando o log de todos os acessos em banco de dados.

Ao longo do desenvolvimento do sistema foi possível alcançar a validação das funcionalidades, atingindo os objetivos propostos. O controlador de acesso permite o gerenciamento de um ambiente, proporcionando que os usuários realizem o acesso utilizando uma tag RFID, a validação do acesso é realizada a partir da leitura dos dados armazenados em sua memória. Quando é realizado a identificação de uma tag ou efetuado um acionamento no dispositivo esses eventos são registrados em banco de dados.

Foi apresentada toda a base teórica utilizada para poder concretizar as propostas oferecidas no mercado, detalhando como foi implementada passo a passo, mostrando que todos os objetivos propostos foram cumpridos.

Diante do presente trabalho e de acordo com os resultados apresentados, o projeto tem total viabilidade de ser implementado, sendo uma boa solução para automatizar serviços para controlo de acesso.

6.2. Sugestão para trabalhos futuros

Para possíveis trabalhos futuros pode-se melhorar os seguintes pontos no sistema desenvolvido:

- Implentação de leitor biométrico e reconhecimento facial, elevando a segurança;
- Expandir o conceito de acesso para não somente movimentação de pessoas, mas também de béns matérias, que torma muito útil para ambientes que requerem um constante monitóramento;

- Uma outra inovação seria criar uma base de dados mais completa, com uso de métodos de criptografia e um maior detalhamento dos processos.

7. Referências bibliográficas

1. Norman, Thomas, 2012 - Electronic Access Control, Elsevier Inc;
2. https://gestaodeseguranca privada.com.br/sistema-controle-de-acesso-definicoes-como-funciona/#Defini%C3%A7%C3%A3o-controle-acesso, 13 de setembro de 2023;
3. Carneiro, Hugo Miguel Pereira Simões, 2004 - Sistemas de Controlo de Acesso, Porto;
4. Security Pro Solutions Uganda, 2021;
5. https://folhacerta.com/controle-de-ponto-manual-entenda-porque-esse-sistema-esta-obsoleto/. Acesso em 23 de setembro de 2023.
6. Karygiannis, T., Eydt, B., Barber, G., Bunn, L., and Phillips, T. Guidelines for Securing Radio Frequency Identification (RFID) Systems. Special Publication 800-98. National Institute of Standards and Technology (NIST), 2007;
7. Using Smart Cards for Secure Physical Access. Smart Card Alliance, 2003;
8. www.rfidsystems.com.br/ , 13 de setembro de 2023;
9. Gomes, António Augusto Araújo. 2010. Sistemas de Controlo de Acesso. Junho de 2010, pp. 1-14;
10. https://www.topdata.com.br/controle-de-acesso-em-hospitais/, 26 de julho de 2022;
11. Merkert, R. J. Smart Cards and Biometrics in Physical Access Control Systems. Biometric Consortium 2005 Conference. SCM Microsystems, 2005;
12. https://www.apsei.org.pt/sistemas-de-controlo-de-acessos-dispositivos-de-identificacao/, 27 de julho de 2022;
13. Honeywell Physical Access Control Systems, HSPD-12 / FIPS 201 Compliance. White Paper. Honeywell, 2006;
14. Using Smart Cards for Secure Physical Access. Smart Card Alliance, 2003.

15. **Guimarães, André Rolim Almeida. 2013.** Proposta de um sistema de controle de acesso utilizando tecnologia RFID. Setembro de 2013, pp. 1-80;

16. **Souza, Ivan de. 2020.** *Rockcontent.* [Online] 20 de Fevereiro de 2020. [Citação: 16 de Dezembro de 2021.] https://rockcontent.com/br/blog/banco-de-dados/.

17. **Costa, Claudio Giulliano Alves da. 2001.** Desenvolvimento e Avaliação Tecnológica de um Sistema de Prontuário Eletrônico do Paciente, Baseado nos Paradigmas da World Wide Web e da Engenharia de Software. 2001, pp. 1-288.

18. Physical Access Control System Migration Options for Using FIPS 201-1 Compliant Credentials. PAC-07002. Smart Card Alliance Physical Access Council in collaboration with Open Security Exchange, Security Industry Association, and International Biometric Industry Association, 2007;

19. MICROCHIP. microIDr125 kHz RFID System Design Guide. [S.l.], 2004. Ultimo acesso em 23 de novembro de 2022.

20. INTERMEC. Fundamentos da RFID: Entendendo e usando a identificação por radiofrequência. [S.l.], 2007.

21. WIKIPEDIA. Controle de Acesso — Wikipedia, a enciclop ´ edia livre ´ . 2022. https: //pt.wikipedia.org/wiki/Controle_de_acesso. Ultimo acesso em 25 de setembro de 2022.

22. https://www.battery.co.za/products/automotive/passenger-vehicles/, 30 de setembro de 2023;

23. **NXP, Semiconductors. 2016.** MFRC522 Standard performance MIFARE and NTAG frontend. NXP Semiconductors, 27 de Abril de 2016, Vol. Rev. 3.9, pp. 01-95.

24. **Filipeflop. 2021.** Filipeflop. https://www.filipeflop.com/produto/kit-modulo-leitor-rfid-mfrc522-mifare/. 29 de setembro de 2023.

25.

Apêndice: Algoritmo de funcionamento do protótipo na linguagem C++

```
#include <WiFi.h>

#include <HTTPClient.h>

#include <Keypad.h>

#include <LiquidCrystal_I2C.h>

#include <Servo.h>

#include <SPI.h>

#include <MFRC522.h>

#define SS_PIN  5  // ESP32 pin GIOP5

#define RST_PIN 27 // ESP32 pin GIOP27

#define SERVO_PIN  26

#define ROW_NUM     4 // four rows

#define COLUMN_NUM  4 // four columns

const char WIFI_SSID[] = "Nelton";

const char WIFI_PASSWORD[] = "Nelton43";

String HOST_NAME =

String HOST_NAME = String HOST_NAME = String HOST_NAME = tring HOST_NAME = ring HOST_NAME = ing HOST_NAME = ng HOST_NAME = g HOST_NAME = HOST_NAME = HOST_NAME = OST_NAME = ST_NAME = T_NAME = _NAME = NAME = AME = "ME = "hE = "ht = "htt= "http "http://192.168.1.19";

String PATH_NAME   = "/insert_temp.php";

String queryString = "?temperature=30.5";
```

```
MFRC522 rfid(SS_PIN, RST_PIN);

String cat = "";

String jos = "";

Servo servo;

int angle = 0; // the current angle of servo motor

char keys[ROW_NUM][COLUMN_NUM] = {

  {'1','2','3', 'A'},

  {'4','5','6', 'B'},

  {'7','8','9', 'C'},

  {'*','0','#', 'D'}

};


byte pin_rows[ROW_NUM]      = {34, 35, 25, 17}; // GIOP19, GIOP18, GIOP5, GIOP17 connect to the row pins

byte pin_column[COLUMN_NUM] = {16, 4, 0, 2};    // GIOP16, GIOP4, GIOP0, GIOP2 connect to the column pins


Keypad keypad = Keypad(makeKeymap(keys), pin_rows, pin_column, ROW_NUM, COLUMN_NUM );

LiquidCrystal_I2C lcd(0x27, 16, 2); // I2C address 0x27, 16 column and 2 rows


int cursorColumn = 0;

int cursorColumn1 = 0;
```

```
void setup(){
Serial.begin(9600);
 WiFi.begin(WIFI_SSID, WIFI_PASSWORD);
  Serial.println("Connecting");
  while(WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
}
Serial.println("");
  Serial.print("Connected to WiFi network with IP Address: ");
  Serial.println(WiFi.localIP());

  HTTPClient http;

  http.begin(HOST_NAME + PATH_NAME + queryString); //HTTP
  int httpCode = http.GET();

  // httpCode will be negative on error
  if(httpCode > 0) {
    // file found at server
    if(httpCode == HTTP_CODE_OK) {
      String payload = http.getString();
```

```
      Serial.println(payload);
    } else {
      // HTTP header has been send and Server response header has been handled
      Serial.printf("[HTTP] GET... code: %d\n", httpCode);
    }
  } else {
    Serial.printf("[HTTP] GET... failed, error: %s\n", http.errorToString(httpCode).c_str());
  }

  http.end();
}
  lcd.begin(); // initialize the lcd
  lcd.backlight();
  Serial.begin(9600);         // initialize serial
  servo.attach(SERVO_PIN);    // attaches the servo on pin 9 to the servo object
  servo.write(angle);
  SPI.begin(); // init SPI bus
  rfid.PCD_Init(); // init MFRC522

  Serial.println("Tap an RFID/NFC tag on the RFID-RC522 reader");
}

void loop(){
```

```
radioFre();
teclado();
}
void radioFre() {
  if (rfid.PICC_IsNewCardPresent()) { // new tag is available
    if (rfid.PICC_ReadCardSerial()) { // NUID has been readed
      MFRC522::PICC_Type piccType = rfid.PICC_GetType(rfid.uid.sak);
      Serial.print("RFID/NFC Tag Type: ");
      Serial.println(rfid.PICC_GetTypeName(piccType));
      // print UID in Serial Monitor in the hex format
      Serial.print("UID:");
      for (int i = 0; i < rfid.uid.size; i++) {
        Serial.print(rfid.uid.uidByte[i] < 0x10 ? " 0" : " ");
        Serial.print(rfid.uid.uidByte[i], HEX);
      }
      Serial.println();

      rfid.PICC_HaltA(); // halt PICC
      rfid.PCD_StopCrypto1(); // stop encryption on PCD
    }
  }
}
```

```
void teclado (){
   char key = keypad.getKey();


  if (key) {
    lcd.setCursor(cursorColumn, 0); // move cursor to   (cursorColumn, 0)
    lcd.print(key);                 // print key at (cursorColumn, 0)
    cat = key;
    jos = key;
    cursorColumn++;                 // move cursor to next position
    if (cat == "*"){
      lcd.clear();
      cursorColumn = 0;
      cursorColumn1 = 0;
    }
    if(cursorColumn >= 16) {        // if reaching limit, clear LCD
      lcd.setCursor(cursorColumn1, 1);
      lcd.print(key);
      cursorColumn1++;
    }
     if(cursorColumn1 == 16) {
       lcd.clear();
      cursorColumn = 0;
      cursorColumn1 = 0;
```

```
   }
  if (jos == "2") {
  // change angle of servo motor
  if (angle == 0)
    angle = 90;
  else if (angle == 90)
    angle = 0;
  // control servo motor arccoding to the angle
  Serial.print("The button is pressed => rotate servo to ");
  Serial.print(angle);
  Serial.println("°");
  servo.write(angle);
}
}
```