UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ELECTROTECNIA

Curso de Engenharia Electrónica

Relatório do Estágio Profissional

Projecto de sistema de segurança electrónica para Escritório da Oceana Limitada.

Autor: Filipe Salomão Macome

Supervisor da Faculdade: Engº. José Gabriel de Sá Consolo

Supervisor da Empresa: Claude Marcello Champier

Maputo, Setembro 2022

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ELECTROTECNIA

Curso de Engenharia Electrónica

Relatório do Estágio Profissional

Projecto de sistema de segurança electrónica para Escritório da Oceana Limitada.

Autor: Filipe Salomão Macome

Supervisor da Faculdade: Engº. José Gabriel de Sá Consolo

Supervisor da Empresa: Claude Marcello Champier

Maputo, Setembro 2022

Declaração

Eu, Filipe Salomão Macome, declaro por minha honra que este trabalho do estágio profissional do final do curso de Engenharia Electrónica, nunca foi apresentado em nenhuma instituição para obtenção de qualquer nível.

Este trabalho é fruto da minha investigação e de um trabalho colaborativo.

_____

(Filipe Salomão Macome)

Dedicatória

Sem fôlego não há vida e sem vida não estaria nessa posição e nesse local, por isso em primeiro lugar dedico ao dador do Dom da vida, o criador, Alfa e Ómega que permitiu que eu chegasse até aqui.

Em segundo lugar aos meus progenitores Salomão Júlio Macome e Sandra Alberto Massinga, e em especial a minha mãe que foi meu suporte em todos estágios dessa trajectória financeiramente como sentimentalmente e em memória a minha avó materna Beatriz Aurérilo Tembe pelos seus conselhos e ensinamentos.

Em terceiro lugar a minha namorada Felismina Rafael Vilanculos, pelo seu apoio neste último estágio dessa caminha e meus amigos Nielsen Silvestre e Olímpio Mathe pelo seu apoio e seu conselho.

Agradecimentos

Agradeço a todos que me acompanharam ao longo deste percurso e que de alguma forma contribuíram para sua concretização.

Agradeço ao meu bom Deus que me sustentou até que eu chegasse aqui, a minha mãe Sandra Alberto Massinga pelo apoio incondicional pelo suporte que ela me deu momentos de turbulência.

Agradeço ao meu supervisor Engenheiro Gabriel Jose Consolo e Claude Champier, pelas orientações dadas, pela paciência e dedicação concedidas, no decorrer da elaboração do projecto.

Agradeço ao Wolf Tech. LDA e como a Champier.LDA por terem me recebido e permiter que eu fizesse parte da equipe.

Agradeço a todos os professores por todo conhecimento compartilhado ao longo desta caminhada, e pelos conselhos que deles recebi.

Agradeço a todos que foram meus colegas de turma a cada semestre, que compartilharam comigo todas as dificuldades e tornaram esta caminhada mais leve.

Agradeço a toda comunidade da Universidade Eduardo Mondlane, em especial a da Faculdade de Engenharia, que contribuiu para o meu desenvolvimento profissional e pessoal, o meu MUITO OBRIGADO.

Epígrafe

Para tudo há uma ocasião, e um tempo para cada propósito debaixo do céu:
Tempo de nascer e tempo de morrer, tempo de plantar e tempo de arrancar o que se plantou,
Tempo de matar e tempo de curar, tempo de derrubar e tempo de construir,
Tempo de chorar e tempo de rir, tempo de prantear e tempo de dançar,
Tempo de espalhar pedras e tempo de ajuntá-las, tempo de abraçar e tempo de se conter,
Tempo de procurar e tempo de desistir, tempo de guardar e tempo de lançar fora,
Tempo de rasgar e tempo de costurar, tempo de calar e tempo de falar,
Tempo de amar e tempo de odiar, tempo de lutar e tempo de viver em paz.
Eclesiastes 3:1-8

Resumo

O presente relatório referente a disciplina de estágio profissional que foi realizado na empresa Wolf Tech.LDA apresenta projecto de segurança electrónica que foi implementado no escritório da empresa Oceana Limitada sita na avenida da Marginal no prédio Zen, segundo andar que teve como objectivo principal melhorar a segurança do local. Aonde para implementação do projecto foi necessário efectuar um levantamento em termos de utilizador, requisitos e sistemas a instalar.

Foram implementados sistemas de CCTV, sistema de intercomunicação, sistema de alarme e sistema de controlo de acesso, nesse relatório são apresentadas as principais características desse sistemas, como também a planta baixa com a representação dos pontos de instalação das câmeras, dos sensores e como também dos leitores biométricos.

PALAVRA-CHAVE: Segurança electrónica, CCTV, alarme, intercomunicador, controle de acesso.

Abstracts

The present report referring to the professional internship discipline that was carried out at the company Wolf Tech.LDA presents an electronic security project that was implemented in the office of the company Oceana Limitada located on Avenida da Marginal in the Zen building, on the second floor, whose main objective was to improve the site security. Where to implement the project it was necessary to carry out a survey in terms of user, requirements and systems to be installed.

CCTV systems, intercom system, alarm system and access control system were implemented, in this report the main characteristics of these systems are presented, as well as the floor plan with the representation of the installation points of the cameras, sensors and as well as of biometric readers.

KEYWORDS: Electronic security, CCTV, alarm, intercom, access control.

ÍNDICE

Declaração iii
Dedicatória iv
Agradecimentos v
Epígrafe vi
Resumo vii
Abstracts viii
Capítulo 01 1
1. Introdução 1
1.1 Formulação do Problema 2
1.3 Objectivo geral: 3
1.4 Objectivos específicos 3
1.5 Metodologia 3
Capitulo 02 Fundamentação Teórica 4
2. Segurança Patrimonial 4
2.1. Recursos da Segurança Patrimonial 5
2.1.1 Recursos de Gestão Administrativa 5
2.1.2 Recursos da Segurança Física 5
2.1.3 Actividades Inteligência 5
2.2. Segurança Electrónica 6
2.2.1 Tipos de Sistemas Electrónicos de Segurança 6
2.3 Sistema de Intercomunicação 7
2.4 Sistema de Alarme 7
2.4.1 Tipos de Sensores 9
2.4.1.1 Sensor Magnético (Reed Switch) 9
2.4.1.2 Sensor Infravermelho (Passivo) 10
2.4.1.3 Sensor Infravermelho (Activo) 10
2.4.1.4 Sensor por quebra de vidro 11
2.5 Sistema de CCTV 11
2.5.1 Sistemas analógicos 12
2.5.2 Sistemas digitais 12
2.5.3 Constituição de Sistema CCTV 13
2.5.4 Tipo de Câmeras 13
2.5.4.1 Micro-Câmeras 13
2.5.4.2 Câmeras Pin Hole 14
2.5.4.3 Mini Câmeras 14

2.5.4.4 Câmera Bullet 15
2.5.4.5 Câmera Dome 15
2.5.4.6 Câmera Speed Dome 16
2.5.4.7 Câmeras IP 17
2.5.5 Tipos de Equipamentos de Gravação de Imagens 17
2.5.5.1 DVR (Digital Video Recorder) Stand Alone 17
2.5.5.2 NVR (Network Video Record) 18
2.5.5.3 HVR 19
2.5.6 Funções dos Equipamentos de Gravação de Imagens 19
2.6 Sistema de Controle de Acesso 19
2.6.1 Dispositivo de Bloqueio 21
2.6.1.1 Cancelas Automáticas 21
2.6.1.2 Catracas Electrónicas 22
2.6.1.3 Portas, portões e portais 22
2.6.2 Tecnologias de Identificação 23
2.6.2.1 Teclados 23
2.6.2.2 Cartões 24
2.6.2.3 Biometria 25
2.6.2.4 Geometria da mão 25
2.6.2.5 Impressões digitais 26
2.6.2.6 Leitura da Retina ou Íri 27
2.6.2.7 Identificação da face 28
2.6.2.8 Reconhecimento de Voz 28
2.6.2.9 Reconhecimento de Caligrafia 28
2.7 Redes de computadores 29
2.7.1 Tipos de redes de computadores 29
2.7.1.1 PAN 29
2.7.1.2 LAN 29
2.7.1.3 MAN 29
2.7.1.4 WAN 30
2.7.2 Classificação de redes quanto a hierarquia 30
2.7.2.1 Redes ponto-a-ponto 30
2.7.2.2 Redes cliente-servidor 30
2.7.3 Tipos de servidores e serviços de redes 31
2.7.4 Principais dispositivos de uma rede 32
2.7.5 Principais conceitos relacionados às redes de computadores 34

Capítulo 03 35
3.1 Modelo de Sistema de Intercomunicador 35
3.1.1 Configuração e Instalação do VTO e VTH. 37
3.2 Modelo de Sistema de Alarme 38
3.2.2 Configuração e Instalação 39
3.3 Modelo de Sistema CCTV 41
3.3.1 Configuração e Instalação 42
3.4 Modelo de Sistema de Controle de Acesso 43
3.4.2 Leitor Biometrico FR1200 44
3.4.3 ZK4500 45
3.4.4 Fechadura Electrmagnetica 45
3.4.5 Configuração e Instalação 46
Capítulo 04 49
4. Avaliação do impacto da implementação do projecto de segurança nos escritório da OCEANA LIMITADA 49
4.1 Conclusão 51
4.2 Referências Bibliográficas 52
Anexos 54
Anexos 1 – Desenho da Planta Baixa da Área do Escritório 54
Anexos 2 – Desenho da Planta Baixa da Área do Escritório Com Pontos de Instalação de Equipamentos 55
Anexos 3 – Imagem Após Implementação dos Sistemas 56

LISTA DE FIGURAS

Figura 1 - Ilustração do Sensor Reed Switch 9
Figura 2 - Ilustração do Sensor Infravermelho Passivo.....10
Figura 3 - Ilustração do Sensor Infravermelho Activo.....10
Figura 4 - Ilustração do Sensor Quebra Vidro 11
Figura 5 - Ilustração de uma Micro Câmera 14
Figura 6 - Ilustração de uma Pin Hole.....14
Figura 7 - Ilustração de uma Mini Câmeras.....15
Figura 8 - Ilustração de uma Câmera Bullet 15
Figura 9 - Ilustração de uma Câmera Dome.....16
Figura 10 - Ilustração de uma Câmera Speed Dome.....16
Figura 11 - Ilustração de um DVR.....17
Figura 12 - Ilustração de um NVR.....18
Figura 13 - Ilustração de uma Cancela Automáticas.....22
Figura 14 - Ilustração de uma Catraca Electrónica 22
Figura 15 - Ilustração de Teclados.....24
Figura 16 - Ilustração de Leitor Biometrico(Geometria da mão) 26
Figura 17 - Ilustração de Leitor Biometrico(Geometria da mão) 27
Figura 18 - Ilustração de Leitor Biometrico(Íris).....28
Figura 19 - Ilustração de Leitor Biometrico (Identificação Facial) 28
Figura 20 - Ilustração do modelo VTO e VTH.....35
Figura 21 - Illustração do VTO modelo DHI-VTO2111D-WP-S parte frontal e parte traseira.....36
Figura 22 - Ilustração do VTH.....37
Figura 23 - Ilustração da Central Hikivision Modelo DS-PWA32-HR.....39
Figura 24 - Ilustração de um Câmera Modelo IPC-HDBW1235E-W-S2 e DH-IPC-HFW3549E-AS.....40
Figura 25 - Ilustração da Central INBIOS 460.....44
Figura 26 - Ilustração do Leitor Biometrico FR1200.....45
Figura 27 - Ilustração do Leitor Biometrico ZK4500.....45
Figura 28 - Ilustração do Maglocks.....46

LISTA DE TABELAS

Tabela 1 - Equipamentos do Sistema.....48

Capítulo 01 - CONTEXTUALIZAÇÃO DO TEMA

1. Introdução

A disciplina de Estágio Profissional proporciona ao estudante o complemento do aprendizado, pois esta permite aplicabilidade da teoria estudada com prática nas actividades quotidiana de uma empresa.

O presente relatório é referente à disciplina de Estágio Profissional, realizada na empresa WolfTech Industries LDA, sob supervisão do Claude Champier (Empresa) e Engenheiro Gabriel José Consolo (Faculdade de Engenharia).

Este relatório traz informações sobre actividades desenvolvidas durante o período de realização do estágio referente a implementação de projecto de segurança electrónica nos escritório da Oceana Limitada.

A WolfTech Industries LDA é uma empresa de prestação de serviços na área de redes de computadores e de segurança electrónica, sita na Avenida Kwame Nkrumah, o estágio teve início no dia 20 de Abril de 2022 com duração de 3 meses.

Identificação das Actividades de Estágio

Objectivos a serem alcançados

Com a realização do estágio pretende-se que o estágio possa fazer o uso adequado de equipamento de rede, segurança electrónica como também das suas ferramentas: Por em prática o conhecimento adquirido em seus anos de estudos na resolução de problemas diários na area de actuação.

Actividades desenvolvidas no estágio

Acompanhemento no desenvolvimento de projectos de redes de computadores e segirança electronica;

Acompanhemento no processo de instalação de redes de computadores e como também segurança electrónica.

Gestão e manutenção de sistema de redes de computadores e como também de sistema de segurança electronica.

1.1 Formulação do Problema

Neste presente trabalho, visa se a elaborar de um projecto de segurança electrónica para escritórios “Head_Office” da Oceana limitada cita na avenida da Marginal no prédio Zen, que tem como objectivo principal melhorar a segurança do local.

Um sistema é definido como sendo um conjunto de elementos interdependentes de modo a formar um todo e segurança é definido como sendo um conjunto de medidas visando à protecção de riscos, perigos ou perdas a pessoas ou coisas.

Segurança é um termo bastante amplo que está intimamente relacionado a outro termo: “protecção”. Segurança é uma percepção de protecção contra perdas, sejam estas físicas ou materiais.

E se tratando de perda material, surge em seu combate a Segurança Patrimonial. “A área de segurança patrimonial consiste no conjunto de actividades que tem por objectivo zelar pelo património de uma organização pública ou privada.” (CATHO, 2013).

Como foi mencionado no parágrafo anterior segurança é um termo relacionado a protecção, e a segurança electrónica é fazer o uso de meios tecnológicos para garantir a protecção e vigilância de um local.

Sendo o escritório um local aonde circulam diversas pessoas diariamente que para além dos funcionários das empresas outras pessoas se fazem presente nos escritórios em período laboral e como não, o local torna se susceptível à ocorrência de varias infracções como vandalismo, roubo, assalto. Remetendo a seguinte questão de pesquisa: **Como melhor de forma efectiva o sistema de segurança no escritório oceana Limitada?**

1.3 Objectivo geral:

- Elaborar projecto de segurança electrónica para Escritório da Oceana Limitada.

1.4 Objectivos específicos:

- Resume teorico sobre sistemas de controlo de acesso, CCTV, sistema de alarme e intercomunicador;
- Efectuar o levantamento dos requisitos em termos de utilizadores, aplicações dos dispositivos para o Sistema;
- Estruturar e esquematizar o layout físico e lógico do projecto;
- Avaliar o impacto em termo de segurança que projecto trará para o funcionamento da empresa.

1.5 Metodologia

Quanto a Finalidade: Pesquisa Aplicada;

Quanto aos Objectivos: Pesquisa Descritiva;

Quanto a abordagem: Pesquisa Qualitativa;

Quanto ao Método: Método Deductivo;

Quanto Procedimento: Pesquisa Bibliografica, documental e de estudo de caso

1.6 Estrutura do trabalho

O trabalho está dividido em quatro capítulos. No primeiro capítulo é feita a contextualização do trabalho, aonde temos a introdução do trabalho que aborda sobre local e importância do estágio profissional, formulação do trabalho descreve o caso em estudos, os objectivos descritos e a metodologia.

No segundo capítulo é feito o resumo teórico sobre os sistemas que foram implementados isso envolve, sistema de intercomunicação, sistema de alarme, sistema de cctv e sistema de controle de acesso.

No terceiro capítulo são apresentados os meios tecnológicos usado para materialização do projecto, feita descrição técnica, são explicadas formas de configuração e instalação.

No quarto capítulo trata-se “Conclusão”, “recomendações” é feita também avaliação da implementação do projecto e por último é apresenta “referência bibliográfica

Capitulo 02 - Fundamentação Teórica

2. Segurança Patrimonial

Segundo Marcondes (2015) segurança patrimonial é definida como sendo o conjunto de actividades que tem como objectivo prevenir e reduzir perdas relacionadas ao património em uma determinada organização, este património que podem ser activos tangíveis e intangíveis.

Activos tangíveis são bens e valores que existem fisicamente, como instalações, móveis, equipamentos, veículos, dinheiro, stocks, empregados, colaboradores, entre outros, que também integram o património da organização.

Activos intangíveis são bens que a organização possui, mas que não existem fisicamente, licenças, direitos autorais, marca da organização e etc.

Segundo Gil (1995), a segurança patrimonial é um conjunto de medidas de protecção que visa a prevenção, detecção, correcção e restauração das condições de normalidade de bens, em face de ameaças analisadas.

Segundo Silva (2009), o conceito de segurança patrimonial é a aplicação da prevenção, detecção e reacção em proporções distintas em um projecto de segurança.

- Prevenção: deve representar 80% do conjunto e seu foco é antecipar e planejar as medidas preventivas para mitigar acções criminosas;
- Detecção: deve representar 15% do conjunto e seu foco é detectar acções suspeitas com tempo para reacção;
- Reacção: deve representar 5% do conjunto e seu foco é reagir após detectar uma acção suspeita.

Segundo a definição da CIBSE (1991), o projecto de segurança patrimonial de uma edificação deve ter por objectivo minimizar, dentro e ao redor da edificação, os riscos de furto, danos criminosos, vandalismos, ataques pessoais e sabotagens, tanto durante a construção, quanto durante toda a vida útil da edificação.

De acordo com Moreira (2007), a avaliação da segurança patrimonial é realizada mediante uma combinação de factores que incluem a propriedade, a análise de riscos, as vulnerabilidades, as ameaças e os resultados da escolha que ajudarão na determinação do grau de protecção e dos critérios a serem utilizados.

2.1. Recursos da Segurança Patrimonial

Para elaboração de um projecto de segurança patrimonial existem vários factores que devem ser levados em conta, esses factores são identificados com recursos necessários para elaboração de um projecto de segurança patrimonial que podem ser:

- Recursos de Gestão Administrativa;
- Recurso de Segurança Física;
- Actividades de Inteligência.

2.1.1 Recursos de Gestão Administrativa

Os recursos administrativos envolvem:

- Planeamento, Políticas, Planos, Normas e Procedimentos de Segurança;
- Programa de Gerenciamento de riscos;
- Programas de Gestão de Continuidade de Negócios.

2.1.2 Recursos da Segurança Física

Fazem partes dos meios utilizados pela segurança física:

- Barreiras Físicas;
- Iluminação de Protecção;
- Equipe de Vigilância;
- Animais;
- Sistemas Electrónicos de Segurança; e
- Equipamentos de Detecção e Combate a Incêndio.

2.1.3 Actividades Inteligência

Actividade de inteligência refere-se a actividades sistemáticas e especializadas voltadas para a identificação, acompanhamento e avaliação de ameaças reais ou potenciais, bem como, a obtenção, produção e a salvaguarda de

conhecimentos, informações e dados que subsidiem as actividades da segurança patrimonial da organização.

Existem vários recursos para elaboração de um projecto de segurança patrimonial com isso não quer dizer que se deve fazer o uso taxativo de todos os recursos apresentados, pois cada local de implementação de um projecto de segurança patrimonial apresenta suas necessidades únicas, e por vezes já existem certos recursos implementados, mas se busca o aprimoramento dos mesmo ou aplicação de outros recursos inexistente para o melhoramento da eficiência da segurança.

2.2. Segurança Electrónica

Sistemas Electrónicos de Segurança, também conhecido como sistema de vigilância electrónica, é um sistema que faz o uso de equipamentos e sensores electrónicos projectados, desenvolvidos e construídos, para auxiliar a segurança privada nas suas actividades de segurança de pessoas, numerários, eventos, bens, valores, áreas, estabelecimentos e propriedades.

É definido também como sendo equipamentos formados por componentes eléctricos e electrónicos, com o objectivo principal de detectar, captar, processar, armazenar e transmitir dados e informações úteis para prática das actividades da segurança.

2.2.1 Tipos de Sistemas Electrónicos de Segurança

Os sistemas electrónicos de segurança podem ser de vários tipos, com diversas finalidades, dentre elas: para detecção de presença, movimento, som, mudança de temperatura, presença de fumaça, captura de imagem, e outros eventos e estímulos similares de interesse da segurança privada, os sistemas electrónicos podem ser divididos:

Sistema de detecção: são sensores que tem a função de detectar e responder com eficiência algum estímulo do ambiente como: movimento, variação de temperatura e iluminação, pressão, impacto, som, presença de gases e etc.

Sistemas de captura de imagens e som: são compostos pelos vários tipos de câmeras de segurança e captadores de sons existentes;

Sistemas de identificação: cartões electrónicos, sistema de identificação de biometrias;

Sistemas de controlo de acesso: cancelas, portas, fechaduras e portões electrónicos;

Sistema de rastreamento: sistema de rastreamento de numerários, bens e valores; sistema de ronda electrónica;

Sistema de alarme: dispositivos electrónicos que emitem sinais visuais ou sonoros quando accionados.

2.3 Sistema de Intercomunicação

Um sistema de intercomunicação tem função de garantir a comunicação entre dois ou mais compartimentos diferentes de um local, este garante uma comunicação bidireccional que pode ser por meio de transmissão de chamadas de voz ou vídeo, este sistema é útil para escritórios, para residências unifamiliares e como para condomínio, o intercomunicador faz o uso de um microfone que recebe som e o emite por meio de um alto-falante com o finalidade de estabelecer comunicação com uma ou mais pessoas.
Os intercomunicadores podem ser analógicos ou digitais, quando ao meio de transmissão, mas os intercomunicadores analógicos têm vindo a perder espaço para os digitais por vários factores, factores este que incluem modos de instalação, susceptibilidade a interferências e interceptações, e falta de vídeo em modelos analógicos, e também há modelos digitais que fazem uso do protocolo TCP/IP ou UDP/IP este protocolo faz com que seja possível o uso remoto do intercomunicado.

2.4 Sistema de Alarme

O sistema de alarme têm como objectivo proteger um perímetro de um ambiente definido, este é constituído por equipamento electrónicos que devem ter a capacidade de detectar ocorrência de instrução, e emitir sinais de alerta.

Estes dispositivos electrónicos podem ser sensores de movimento, magnéticos, botões de pânico, entre outros, que enviam sinais à central do sistema de

alarme. A central deve emitir sinais acústicos ou ópticos, bem como alertas através da transmissão remota por meio de notificação para endereço pré-programados.

A eficácia destes sistemas depende da sua correcta concepção, instalação e manutenção.

Unidade central de controle - é responsável pelo controlo do funcionamento de todo o sistema. Este elemento recebe a informação proveniente das entradas, e acciona os dispositivos de saída aquando da ocorrência de uma intrusão no espaço protegido. A central de intrusão e os dispositivos podem comunicar através de uma rede de cabos ou via sinal de rádio.

Sensores – são responsáveis pela detecção automática da ocorrência, devendo ser instalados nos pontos passíveis de intrusão, como portas, janelas, etc. Podem ser detectores de movimento, detectores de abertura, detectores de impacto ou vibração, detectores de quebra de vidros.

Botões de pânico – são os dispositivos que permite o accionamento manual um alarme, podendo ser instalados em locais sujeitos a coacção externa.

Dispositivos de alarme – têm como função alertar a ocorrência localmente, podendo ser de sinalização sonorica ou luminosa.

Transmissores de alarme- dispositivos que têm como função transmitir remotamente a existência de um evento.

Comandos externos - são responsáveis pela activação externa de acções complementares.

Dispositivos de Operação – são os meios que permitem a interacção entre o utilizador e o sistema.

Sensores

Os sensores podem ser classificados em alguns grupos:

a) **Sensores volumétricos**: produzem um campo invisível de actuação, têm a capacidade de detectar qualquer movimento que for realizado dentro da do alcance do campo criado.

b) **Sensores de movimento em vídeo**: detectam a invasão por meio da comparação de imagens pré-programadas ou por meio de detecção de calor.
c) **Sensores de barreira**: tem finalidade de fornecer uma barreira física ao invasor e um sistema de sensoriamente para a detecção.

2.4.1 Tipos de Sensores

2.4.1.1 Sensor Magnético (Reed Switch)

Os sensor magnéticos é constituído por dois elementos, um contacto eléctrico e um imã. O contacto eléctrico é formado por duas lâminas metálicas que formam um contacto normalmente aberto, e que se fecham na presença de um campo magnético. O imã tem a função de manter os contactos sempre accionados e quando o mesmo afasta-se, os contactos abrem, enviado um sinal de alarme. São utilizados para proteger elementos móveis, como porta, janelas.

O contacto eléctrico é instalado na parte fixa do elemento móvel , e um imã permanente é instalado na parte móvel, quando ocorre alguma acção que tende distanciar uma parte de sensor da outra que podem ser abertura da porta ou janela, fazendo que o imã permanente se afasta do detector, isso permite que os contactos eléctricos possam desse modo abrirem se, retirando assim a energização de um ponto especifico da unidade de controle de alarme, que interpretara este evento como uma invasão ao local.

Figura 1 - Ilustração do Sensor Reed Switch

Estes sensor magnéticos podem ser instalados com fios, interligando o sensor até a central de controle, ou através de radiofrequência, sem a necessidade de

fios para comunicação com a central, neste segundo caso, é necessário o uso de baterias para alimentação do dispositivo.

2.4.1.2 Sensor Infravermelho (Passivo)

O sensor infravermelho capta a radiação infravermelha gerada por elementos da zona sensoreada e se activa ao variar suficientemente a radiação, e desse modo que detectam a presença de uma pessoa por meio das radiações infrarvermelhas emitido pelo corpo, este tipo de sensor criar um campo de até 6 metros de distância em relação ao seu ponto de fixação.

Figura 2 - Ilustração do Sensor Infravermelho Passivo

2.4.1.3 Sensor Infravermelho (Activo)

O sensor infravermelho activo é composto por um transmissor e receptor, onde o transmissor emite feixe de luz infravermelha invisível para o olho humano, e o receptor detecta os mesmos feixes de luz. Os sensores devem ser colocados frente a frente, em distância predefinida, o alarme quando faz se o uso desse sensor dispara quando ocorre a interrupção da luz, existem modelos de feixe único ou de feixe duplo recomendado para ambientes externos.

Figura 3 - Ilustração do Sensor Infravermelho Activo

O alcance dos feixes pode variar de 20 metros até 1500 metros, dependendo do dispositivo utilizado, no entanto, recomenda-se limitar a distância do receptor ao emissor em no máximo 150 metros, pois uma alta intensidade de

chuva pode afectar o desempenho do dispositivo, e longas distâncias dificultam o alinhamento dos feixe [16].

2.4.1.4 Sensor por quebra de vidro

Sensores por quebra de vidro incorporam um microfone ligado a um circuito composto por um analisador de áudio, e detectam o som típico da quebra de um vidro, ignorando distúrbios ambientais e ruídos externos aleatórios.

Figura 4 - Ilustração do Sensor Quebra Vidro

Os equipamentos mais recentes não necessitam estarem presos a uma janela, podendo dessa forma proteger diversas janelas simultaneamente, a até 6 metros de distância do equipamento. Estes sistemas de segurança podem incluir ajuste de sensibilidade, reduzindo o número de alarmes falsos[16].

2.5 Sistema de CCTV

Quando se trata de um projecto de seguranças electrónica um dos recursos mas usados e indispensável é o monitoramento por câmeras conhecido como CCTV que significa Closed Circuit of Television ou CFTV que significa Circuito Fechado de Televisão, e um sistema de monitoramento digital que tem a capacidade de pode monitar diversos locais, tais como elevadores, corredores, saídas, ambientes fechados entre outras áreas.

CFTV, é um sistema de televisionamento que distribui sinais provenientes de câmeras localizadas em locais específicos, para pontos de supervisão pré-determinados.

O sistema de CCTV não é aplicado somente com propósitos de segurança e vigilância; também é utilizado em outros campos como laboratórios de pesquisa, na área médica, assim como nas linhas de produção de fábricas para controle de processos.

2.5.1 Sistemas analógicos

Um sistema de circuito fechado de televisão analógica tem a finalidade de armazenar as imagens que são capturadas por câmeras analógicas e transmitir estas informações até um gerenciador de imagens.

Os sistemas analógicos de CCTV fazia uso de vários meios para armazenamento e visualização de informação como multiplex, quad, time lapse, e armazenava em fita VHS. Mas actualmente, este equipamento foram agrupados é somente um, adotou-se sigla DVR que significa Digital video Record stand alone pois é equipamento que pode efectuar o gerenciamento das câmeras do sistema sem a necessidade de uso de um computador.

2.5.2 Sistemas digitais

O sistema de gravação digital tem como característica principal monitorar e gravar simultaneamente suas imagens através de um computador. A qualidade das imagens capturadas é superior ao sistema analógico, pois são gerados até 60 quadros por segundo, o que representa o dobro de resolução comparado a um sistema convencional.

O gerenciamento das imagens é feito por meio de software de gerenciamento específicos, e são gravadas em disco duros.

Os sistemas existentes actualmente no mercado podem três configurações distintas, quanto ao requisito de instalação física:

Sistemas interligados a fio, no qual a principal via de comunicação é cabo coaxial. Este sistema normalmente é utilizado em circuitos analógicos;

Sistemas wireless as câmeras se comunicam com as centrais de controle através de rádio-frequência;

Sistemas por endereçamento IP as câmeras possuem comunicação Ethernet incorporada, permitindo assim instalar o equipamento em redes estruturadas de informática.

2.5.3 Constituição de Sistema CCTV

Um típico e simples sistema de CCTV é composto pelos seguintes elementos[9]:

Câmera ou Sensor Vídeo: Esta unidade trata da captação de imagens realçando tal de acordo com as circunstâncias e possibilita o seu transporte para outro destino.

Transmissão: Transporta a imagem para um determinado local (central), onde será apresentada, assegurando a qualidade das imagens.

Controlo: É efectuado pelo operador que pode determinar qual a imagem que ele precisa visionar, bem como direccionar a câmara para um determinado local.

Visualização: É feita através de monitores, a qual pode ser visionada em tempo real ou a posteriori.

2.5.4 Tipo de Câmeras

A existência de diversas necessidades para a implementação de um projecto de CCTV, faz com que existam diferentes modelos de câmeras disponíveis no mercado, cada específica para cada situação. As câmeras de segurança variam em muitos factores área em que será feita a monitoração e às especificações do projecto e suas necessidades.

Entre esses factores deve-se considerar:

- ✓ O tamanho da área de cobertura;
- ✓ A iluminação do local;
- ✓ A resolução de imagem necessária para o projecto;
- ✓ Necessidade de imagens coloridas ou em preto e branco;

O objectivo da vigilância, se é uma monitoração anti-furto, monitoração de processos de trabalho, funcionamento de equipamentos, fluxo viário, etc.

2.5.4.1 Micro-Câmeras

São câmeras de pequeno porte que se caracterizam por ter um custo baixo, facilidade de instalação mas uma qualidade bastante limitadas. Podem ser encontradas em versões preto e branco e coloridas. A qualidade das imagens geradas e o desempenho em áreas muito grandes são as principais

desvantagens. Alguns modelos possuem emissores de luz infravermelho acoplados à câmera para a captação de imagens no escuro, a pequenas distâncias [13].

Figura 5 - Ilustração de uma Micro Câmera

2.5.4.2 Câmeras Pin Hole

São micro câmeras com a característica de possuírem uma lente com tamanho extremamente reduzido, sem prejuízo à captação da imagem. São geralmente utilizadas em aplicações o qual o tamanho deva ser reduzido, como em locais ocultos. Sua aplicação se concentra em residências, consultórios, escritórios e qualquer outro local onde a câmera deva estar escondida, sem que as pessoas percebam sua presença[13].

Figura 6 - Ilustração de uma Pin Hole

2.5.4.3 Mini Câmeras

Seu processo de captura de imagens se assemelha aos das micro-câmeras, com a diferença de que estas possuem a conexão para diversos tipos de lentes convencionais de CFTV, podendo assim ter o controle de foco e captura de imagens ajustada ao ambiente[13].

Figura 7 - Ilustração de uma Mini Câmeras

2.5.4.4 Câmera Bullet

Esse modelo de câmera de segurança é o mais utilizando do mercado. Normalmente são as câmeras utilizadas para monitoramente de ambientes externos, em ruas, postes e áreas públicas, devido principalmente à sua maior resistência e protecção contra certos eventos da natureza como chuva, poeira etc.

Existem uma grande variedade de modelos bullet disponíveis, variado principalmente com relação à aparência e alcance.

Uma característica a ser considerada é que a câmera bullet sempre aponta para uma direcção fixa e por isso é mais utilizada para ambientes abertos.

Figura 8 - Ilustração de uma Câmera Bullet

2.5.4.5 Câmera Dome

São pequeno câmeras em formato de doma, ou cúpula, são utilizadas em ambientes internos, nas paredes ou tectos, devido à sua boa cobertura para esse tipo de ambiente e por ser esteticamente discretas. No entanto, alguns modelos que possuem mais protecção podem ser usados em ambientes externos.

Figura 9 - Ilustração de uma Câmera Dome

Esse modelo de câmeras possuem óptima qualidade de imagem, podendo capturar detalhes de objectos e faces. Outras características são que a direcção em que a câmera está apontando fica oculta, e pode ser ajustada sem muita dificuldade. Muitas vezes essas câmeras CCTV também possuem o recurso de infravermelho.

2.5.4.6 Câmera Speed Dome

Tem sua movimentação motorizada, e conseguem analisar imagens em giros de até 360 graus no eixo horizontal, com movimentações de até 90 graus no eixo vertical. A movimentação de seu posicionamento é feita através de mesas de controle, e é realizada pelo responsável da central, que pode inclusive ampliar a imagem, aproximando a um ponto específico.

Figura 10 - Ilustração de uma Câmera Speed Dome

2.5.4.7 Câmeras IP

As câmeras IP, conhecidas também como network cameras, possuem um servidor Web interno que possibilitam o envio de imagens em tempo real directamente por uma rede intranet ou internet. Podem ser fixas ou móveis, com zoom e movimentos horizontais e verticais, controladas à distância pela rede. Existem modelos que podem se comunicar via wireless, sem a necessidade de conexão física, com excepção de sua alimentação. Os protocolos e as interfaces mais utilizadas e implementados nestes tipos de câmeras são TCP/UDP/IP, RTSP, SMTP, NAT, ARP, Telnet, DHCP, IEEE 802.11g, IEEE 802.11b, IEEE802.3.

2.5.5 Tipos de Equipamentos de Gravação de Imagens

2.5.5.1 DVR (Digital Video Recorder) Stand Alone

DVR significa Digital Vídeo Recorder (Gravador de vídeo digital) é um equipamento aquisição de informação, que tem como função capturar imagem de diversas câmeras analógicas e disponibilizar o acesso a essas imagens ao vivo e também possibilitar a gravação das imagens de todas essas câmeras.

São equipamentos desenvolvidos especificamente para a função de gravação digital em sistemas de CFTV.

Possuem integradas as funções de sequencial, quad, multiplexador e gravador, tendo então a função de centralizar o processamento e gravação. Possui a interface directa para HDs, muitas vezes permitindo a função hot Swap, para retirada e substituição do HD sem a necessidade de desligar o equipamento.

Figura 11 - Ilustração de um DVR

Entradas de vídeo com conectores BNC, saídas em loop, entradas e saídas de alarme, interfaces RS485/RS232, etc.

Possuem também um software completo para gerenciamento das imagens das diversas câmeras do sistema de CCTV, ajustes da qualidade, visualização ao vivo de cada câmera, permite também a gravação das imagens e o acesso a elas com o detalhe de data e hora da informação desejada. Existem modelos de DVR que possibilitam o acesso remoto das câmeras, para tal faz se necessário conectar o DVR a internet e configurar o serviço.

2.5.5.2 NVR (Network Video Record)

NVR significa Network Vídeo Recorder, tem como função gerenciar e gravar imagens de câmeras IP e não possui suporte a câmeras analógicas.

Como se sabe as cameras IP possibilitam o acesso a elas, sem o uso de um equipamento centralizado, mas o uso do NVR é essencial quando se faz o uso diversas câmeras para melhor gerir e guardar informação.

Figura 12 - Ilustração de um NVR

Diferentemente do uso de DVR em que cada câmera é ligada directamente ao DVR através de um cabo coaxial, o uso de NVR com dispositivos IP, permite que todas câmeras sejam conectadas assim como o NVR sejam conectadas a rede de dados, aos switchs, por meio de cabos Ethernet ou via WI-FI. O NVR consegue identificar cada câmera IP ligada à mesma rede e realizar então o gerenciamento e gravação de imagens.

O NVR permite que todas as câmeras IP, instaladas em local sejam visualizadas e geridas por um único ponto e também possui mas recursos do que disponibilizados pelas câmeras.

2.5.5.3 HVR

HVR significa Hybrid video Recorder, consegue gerenciar e gravar imagens de câmeras analógicas e de câmeras IP.

Este equipamento foi criado com o intuito de permitir o aproveitamento de câmeras analógicas com boa qualidade e adicionamento de câmeras IP de um sistema de CCTV, ele serve como um gerenciador central para as duas tecnologias.

2.5.6 Funções dos Equipamentos de Gravação de Imagens

Apesar das diferenças existente entre os dispositivos, as suas funções principais e alguns do seus benefícios são semelhantes, que são:

- ✓ Acesso em tempo real;
- ✓ Gravação das imagens de todas as câmeras em um único dispositivo;
- ✓ Possibilidade de implementação de backups na nuvem ou em HDs externos;
- ✓ Possibilidade de gravações também de áudio;
- ✓ Visualização das imagens e gravações a partir de diferentes pontos da rede da empresa e através da internet;
- ✓ Acesso ao sistema de CCTV através de dispositivos móveis como celulares e tablets;
- ✓ Acesso às gravações de horários e datas específicas;
- ✓ Facilidade de uso e acesso das informações

2.6 Sistema de Controle de Acesso

Sistema de controle de acesso tem como função permitir ou restringir acesso de pessoas ou veículos a determinados locais com ou sem limitação de horários, também regista o momento do acesso ou tentativa deste.

Este sistema torna possível gerenciamento de acesso para pessoa previamente cadastradas, realiza o acesso através da identificação pessoal que pode ser feita de várias maneiras, por cartões de proximidade, biometrias, senhas individuais ou conjuntas, para caso de veículos poderá ser efectuada por meio da leitura de placas, controle remoto.

Este sistemas são integrados de forma informatizada através de uma rede Ethernet ou serial obedecendo a uma série de configurações lógicas de

softwares, além de trabalhar em conjunto com hardwares de controle que fazem interface eléctrica com dispositivos de bloqueio, tais como portas, cancelas ou portões.

O sistema de controle de acesso têm por objectivo proteger o restringir o acesso a um certa área com finalidade de proteger bens institucionais, como também efectuar os registos de eventos que podem ser úteis no controle de movimentação de pessoas ou veículos.

Todos os eventos são registados e armazenados no servidor de controle de acesso. Neste servidor também é feita toda a parametrização do sistema, estas configurações determinam as permissões e restrições dos acessos a determinadas áreas na qual o sistema foi instalado bem como a emissão de relatórios para consultas futuras das operações realizadas.

Os controles de acesso podem ser dividido em três tipo de controle [7]:

- Físico, Lógico e Administrativo.
- ✓ **Físico**: portas, trancas, guardas, travas de acesso a disquetes, sistemas de travamento por cabos para mesas/paredes, circuito interno de TV, retalhadora de papéis e sistemas de controle de incêndios;
- ✓ **Lógico** (Técnico): senhas, permissões para arquivos, listas de controle acesso, privilégios de contas e sistemas de protecção de energia;
- ✓ **Administrativo**: conscientização sobre segurança, revogação de contas de usuários e políticas.

O projecto de um sistema deve seguir alguns critérios básicos para atender seus objectivos, que são:

- ✓ Definir perímetro de controle;
- ✓ Definir critérios de verificação.
- ✓ Registos de todos os eventos decorrentes destas actividades;
- ✓ Armazenar e disponibilizar os eventos para auditoria.

Para além dos critérios usados para elaboração de um projecto de controle de acesso, os sistema de controle de acesso podem ser classificados em:

- ✓ Sistemas manuais;
- ✓ Sistemas semi-automáticos;

- ✓ Sistemas Automáticos.

A diferença entre esses três tipos de sistemas é que num sistema manuais são controlados directamente pela acção humana, desde a verificação e autorização para o acesso.

Sistemas semi-automáticos estes fazem a integração dos recursos humanos com a tecnologia.

Sistemas automáticos são totalmente independentes da acção humana para identificar e autorizar o acesso ao interior das instalações.

2.6.1 Dispositivo de Bloqueio

Dispositivos de bloqueios podem ser definidos como sendo as barreiras físicas utilizadas para separação das áreas controladas das de uso comum, estes podem ser:

- ✓ Cancelas automáticas;
- ✓ Catracas;
- ✓ Portas;
- ✓ Portões, etc;

Estes devem ser seleccionados consoante a área de aplicação, quando estamos perante sistemas semi-automaticos ou automáticos estes dispositivos de bloqueio são controlados por sistemas electrónico de controlo de acesso, que permitem o bloqueio e desbloqueio por meio de circuitos eléctricos e electrónicos.

2.6.1.1 Cancelas Automáticas

As cancelas são dispositivos utilizados para controlar locais onde há um grande fluxo de veículos, como portarias de condomínios e empresas, estacionamentos e pedágios, substitui os portões nesses casos, pois permite o fluxo com rapidez. As cancelas são accionadas por um pulso de contacto seco, desta forma qualquer hardware de controle de acesso pode ser integrado a cancelas [7].

Figura 13 - Ilustração de uma Cancela Automáticas

2.6.1.2 Catracas Electrónicas

As catracas são dispositivos electromecânicos utilizados para controle de passagem de pessoas. São normalmente instaladas em recepções, por não haver necessidade de dividir o ambiente com paredes e portas para restringir a passagem. A vantagem é que por seu controle ser giratório permite que passe uma pessoa por vez evitando que uma pessoa não autorizada aproveite a passagem da pessoa anterior. Normalmente requerem uma actividade anterior como o cadastramento dos visitantes e cadastramento dos funcionários [7].

Figura 14 - Ilustração de uma Catraca Electrónica

2.6.1.3 Portas, portões e portais

São muito utilizadas para separar ambientes que necessitem de mais segurança, e será utilizado como exemplo de aplicação neste trabalho. Para que uma porta funcione em um sistema de controle de acesso é instalada uma fechadura electromagnética para substituir a fechadura existente ou para funcionar em conjunto com a mesma como redundância de segurança. O tipo de porta é projectado de acordo com a área na qual será instalada, os diversos sistemas podem utilizar portas duplas formando uma eclusa na qual uma só

pode ser aberta com a outra fechada, as portas também podem ser giratórias para que passe somente uma pessoa por vez e ainda portais com detectores de metais [7].

2.6.2 Tecnologias de Identificação

Existem diferentes meios para identificação e cada meio apresenta seu nível de segurança, a escolha do meio tecnológico usar deve ser feita levando em conta o nível desejado de segurança do sistema no local de implementação, para além desse aspectos deve ter conta o ambiente de instalação.

Os critérios de verificação da identificação se resumem em[7]:

- ✓ Algo que só o indivíduo sabe;
- ✓ Algo que só o indivíduo possui;
- ✓ Algo que só o indivíduo é.

Algo que só o indivíduo sabe que são senhas pessoais que podem ser alfanuméricas ou numéricas;

Algo que só o indivíduo possui resume se em objectos físicos únicos que permitem a quem possui acesso ao local requisitado;

Algo que só o indivíduo é são características biométricas dos seres humanos que os identificam para os sistemas de controle de acesso.

2.6.2.1 Teclados

Este sistema é indicado para locais com pouco fluxo de pessoas em áreas restritas. O sistema com teclados têm com objectivo permitir acesso após a introdução da senha correcta.

No sistema com teclados uma das desvantagens descrita é facilidade para se copiar a senha e com o tempo o desgaste do teclado facilitará a descoberta das senhas pelas teclas que ficam visivelmente mais desgastados. E também a senha pode ser passada para outras pessoas, desta forma não há garantia de quem acesso somente registados data e horário dos acessos, podemos que uma senha pode ser associada a uma pessoa mas mesmo nesse termo nada impede que outras pessoas possam a conhecer.

Figura 15 - Ilustração de Teclados

2.6.2.2 Cartões

Os cartões de proximidade possuem um protocolo de codificação chamado Wiegand o qual permite codificação dos cartões em 26 ou 32 bits o que torna praticamente impossível a incidência de cartões repetidos e a cópia de cartões é impossível[16].

Os cartões de proximidade utilização tecnologia de identificação por rádio frequência

Esses cartões podem ser activos ou passivos.

Os cartões de proximidade passivos possuem um circuito constituído de bobina entre o substrato plástico que dá a forma do cartão, essa bobina é excitada quando aproximada do leitor o qual emite um campo electromagnético, no mesmo leitor há um receptor que capta o sinal emitido pelo cartão e o envia para placa controladora[16].

Os cartões activos de proximidade possuem uma bateria interna para alimentação de seu circuito o qual emite um sinal sem necessidade de estar muito próximo ao leitor.

Para leitura dos cartões é necessário que sejam instalados leitores em locais estratégicos próximos as áreas de conexão, ou seja, próximo das portas, catracas ou para o caso de veículos ao alcance do motorista. Os leitores são conectados as placas controladoras do sistema os quais farão a interface com o servidor de sistema.

Os leitores conseguem colectar o código dos cartões passivos a uma distância que varia de 10 a 70 centímetros, dependendo do modelo de leitor, quando

maior o alcance maior o custo do mesmo, os cartões de proximidade são extremamente seguros, sendo quase impossível copiá-los[16].

2.6.2.3 Biometria

Biometria pode ser definida como sendo as mensurações fisiológicas e as características de comportamento que podem ser utilizadas para verificação de identidade de um indivíduo.

O controle biométrico é extremamente confiável, pois sua estrutura básica consiste no registo de certas características físicas ou comportamentais de cada pessoa, que são comparadas a um arquivo armazenado em seu banco de dados. Esses sistemas se tornaram possíveis com a evolução das técnicas de processamento digital de sinais, utilizando essas técnicas as características são amostradas, digitalizadas e armazenadas em um banco de dados associada a um código[16].

Para que a leitura de uma característica física ou biológica humana seja caracterizada como biometria, devem ser respeitados os seguintes requerimentos:

- ✓ Universalidade: cada pessoa obrigatoriamente deve possuir a característica em estudo;
- ✓ Distinção: essa característica deve ser suficientemente diferente de uma pessoa para outra, em termos de característica;
- ✓ Permanência: as características devem ser suficientemente invariantes durante certo período de tempo;

Os principais sistemas biométricos existentes são:

- ✓ Geometria da mão;
- ✓ Impressões digitais;
- ✓ Leitura da Retina ou Íris;
- ✓ Identificação da face;
- ✓ Reconhecimento de Voz;
- ✓ Reconhecimento de Caligrafia.

2.6.2.4 Geometria da mão

Este sistema, também chamado de Hand Key, utiliza características das mãos. Reconhecem a geometria da mão, analisando comprimento e largura dos

dedos, e a área da mão. A certeza na forma de identificar um indivíduo por este sistema, é pelo facto que 2 pessoas não possuem a geometria de suas mãos iguais. Consiste na utilização de imagens da geometria da mão, palma e dedos por scanners, para identificar as pessoas[16].

Armazenam comprimento físico das características colectadas e alguns sinais particulares.

Figura 16 - Ilustração de Leitor Biometrico(Geometria da mão)

O sistema de geometria de mão, para realizar o acesso, o usuário deve posicionar sua mão sobre o leitor aonde é efectuada a comparação entre a leitura realizada e os dados armazenados em banco de dados, caso as condições sejam satisfeitas o sistema permite o acesso. É dito como sistema muito confiável, mas com custo elevado, não pode ser instalado em lugares externos sem nenhum meio de protecção e que tenham incidência de luz solar e a mão usada não pode sofrer usado para o aceso não pode sofrer alterações como uso de objectos ou existência de novas cicatrizes.

2.6.2.5 Impressões digitais

As principais técnicas de identificação de uma impressão digital consistem em captura da imagem, por meio de um equipamento específico (scanners), armazenamento desta imagem e posterior identificação de algumas características.

Figura 17 - Ilustração de Leitor Biometrico(Geometria da mão)

Os principais leitores utilizados são[7]:

- ✓ Ópticos: ao colocar-se o dedo em uma base de vidro, uma luz é emitida sobre o dedo, e a imagem é capturada por um scanner óptico;
- ✓ Ultra-som: neste equipamento, a leitura é feita por emissão de ultra-som, e um leitor calcula os tempos de retorno do sinal emitido, transformando estes sinais em imagem;
- ✓ Capacitivos: o dedo é colocado directamente sobre uma pastilha de silício, e um circuito electrónico capta as minúcias do dedo, gerando uma imagem a partir deste detalhamento.

2.6.2.6 Leitura da Retina ou Íris

Escaneiam a íris ou retina. No caso de mapeamento de retina a identificação do individuo é feita pelo escaneamento dos vasos sanguíneos do globo ocular.

Já o mapeamento da íris se baseia sobre os anéis coloridos em torno da pupila. A identificação pela íris é extremamente precisa, pois esta não sofre alterações pelo tempo ou por lesões. Estes métodos de identificação são os mais precisos, mas possuem a desvantagem de ter altíssimo custo e grande desconforto no momento da leitura e é um equipamento que precisa ser sempre higienizado para evitar que haja contaminações de algumas doenças como conjuntivite[7].

Figura 18 - Ilustração de Leitor Biometrico(Íris)

2.6.2.7 Identificação da face

Esta técnica consiste na leitura de pontos delimitadores da face para identificação de tamanhos, proporções, formas e distâncias. Identifica as pessoas mesmo que a face tenha sido alterada por barba, bigodes, sobrancelhas, cor ou cortes de cabelo diferentes. É uma técnica muito nova e que não causa desconforto algum, pois como a captura e leitura é feita por uma câmera o usuário fica a uma distância confortável do ponto de leitura. A principal desvantagem é para o caso de irmãos gémeos[7].

Figura 19 - Ilustração de Leitor Biometrico (Identificação Facial)

2.6.2.8 Reconhecimento de Voz

Reconhece padrões de voz, identificando se o indivíduo é do sexo masculino ou feminino. Não é muito usado em segurança, pois pode ser facilmente burlado.

2.6.2.9 Reconhecimento de Caligrafia

Reconhece a forma com que uma pessoa escreve e posteriormente identifica o individuo que escreveu. Alguns sistemas podem ser burlados de forma que a assinatura e o formato das letras podem ser copiados, porem há tecnologias que não analisam somente a escrita, mas também a forma com que a pessoa escreve (pressão, angulação da caneta ao escrever, tempo de escrita, etc.) ficando assim mais difícil burlar o sistema.

2.7 Redes de computadores

Rede de computadores ou redes de dados, na informática e na telecomunicação é um conjunto de dois ou mais dispositivos electrónicos de computação interligados por um sistema de comunicação digital, guiados por um conjunto de regras conhecidos como protocolo de rede para compartilhar entre si informação, serviços e, recursos físicos e lógicos. Estes podem ser do tipo: dados, impressoras, mensagens (e-mails), entre outros. As conexões podem ser estabelecidas usando mídia de cabo ou mídia sem fio.

2.7.1 Tipos de redes de computadores

- ✓ PAN;
- ✓ LAN;
- ✓ MAN;
- ✓ WAN;

2.7.1.1 PAN

Uma PAN (Personal Area Network) ou Rede de Área Pessoal, constitui-se de uma rede de computadores formada por dispositivos muito próximos uns dos outros.

2.7.1.2 LAN

Uma LAN (Local Area Network), também conhecida como rede local de computadores, corresponde a uma rede que possui uma “cobertura limitada” quanto a extensão geográfica que pode actuar.

Este tipo de rede é geralmente composta por computadores conectados entre si, através de dispositivos tecnológicos (placas de redes, switch, hub, entre outros), possibilitando o compartilhamento de recursos e a troca de informações.

2.7.1.3 MAN

Uma MAN (Metropolitan Area Network) rede de área metropolitana, corresponde a uma rede de computadores que compreende um espaço de média dimensão (região, cidade, campus, entre outros). Geralmente uma MAN está associada a interligação de várias LAN’s e é considerada uma parte menor de uma WAN

2.7.1.4 WAN

Uma WAN (Wide Area Network) ou rede de longa distância, corresponde a uma rede de computadores que abrange uma grande área geográfica, como por exemplo um país, continente, entre outros. As WAN's permitem a comunicação a longa distância, interligando redes dentro de uma grande região geográfica.

2.7.2 Classificação de redes quanto a hierarquia

A classificação das redes de computadores quanto a hierarquia refere-se ao modo como os computadores dentro de uma rede se comunicam. Entre os principais tipos de classificação quanto a hierarquia, estão as redes ponto-a-ponto e as redes cliente-servidor, que veremos a seguir[21].

2.7.2.1 Redes ponto-a-ponto

Uma rede ponto-a-ponto normalmente é utilizada em pequenas redes. Neste tipo de rede os computadores trocam informações entre si, compartilhando arquivos e recursos.

Uma rede do tipo ponto-a-ponto possui algumas características pontuais:

- ✓ É utilizada em pequenas redes.
- ✓ São de implementação fácil e de baixo custo.
- ✓ Possuem pouca segurança.
- ✓ Apresentam um sistema de cabeamento simples.

2.7.2.2 Redes cliente-servidor

Uma rede de computadores do tipo cliente-servidor possui um ou mais servidores, responsáveis por prover serviços de rede aos demais computadores conectados a ele que são chamados clientes. Cada cliente (computador que compõe este tipo de rede) que deseja acessar um determinado serviço ou recurso faz essa solicitação ao servidor da rede, por isso o nome cliente-servidor.

Diversas são as vantagens de se utilizar um servidor em uma rede de computadores, a seguir são citadas algumas delas:

- ✓ Centralização de serviços – ao utilizar-se um servidor, os serviços de rede (que geralmente são mais do que um) ficam centralizados em um mesmo local, o que facilita a tarefa do administrador do servidor.

- ✓ Backup – ao centralizar serviços de rede como um servidor de arquivos, e-mail e banco de dados, tem-se a facilidade de administrar as cópias de segurança (backup), pois todos os serviços, diretórios e arquivos estão centralizados em uma única máquina e não espalhadas por diferentes computadores em uma rede.
- ✓ Acesso remoto – um servidor pode e, geralmente, tem implementado o serviço de acesso remoto. Dessa forma, usuários podem acessar servidores de uma empresa, por exemplo, de qualquer lugar que tenha acesso à internet, seja em casa, numa praça, etc., como se estivessem na mesma rede local (SILVA, 2010).

2.7.3 Tipos de servidores e serviços de redes

Existem, actualmente, diferentes tipos de servidores. Estes servidores são classificados conforme a tarefa que realizam, sendo os principais, listados a seguir [21]:

- ✓ Servidor de arquivos – tem a função de armazenar os dados que são compartilhados entre os diferentes usuários que compõe uma rede de computadores. Entre estes dados estão o armazenamento de arquivos (texto, planilhas e gráficos). Os programas que manipulam os arquivos são instalados e executados individualmente em cada uma das máquinas, não no servidor, que neste caso é responsável por gerenciar eventuais acessos simultâneos.
- ✓ Servidor de impressão – um servidor de impressão processa os pedidos de impressão solicitados pelos usuários da rede e gerencia a ordem de impressão em caso de pedidos simultâneos (prioridades podem ser implementadas, caso necessário). Cotas de impressão podem ser implementadas como forma de limitar a quantidade de páginas impressas por usuários.
- ✓ Servidor de aplicações – é responsável por executar aplicações cliente/servidor, como por exemplo, um banco de dados. Os clientes enviam pedidos ao servidor, que o processa e devolve os dados para serem exibidos em aplicações cliente. A vantagem deste tipo de serviço é que vários usuários podem utilizar uma aplicação ao mesmo tempo.

- ✓ Servidor de e-mail – responsável pelo armazenamento, processamento de envio e recepção de mensagens electrónicas (e-mail).
- ✓ Servidor de backup – responsável por executar, armazenar a actualizar cópias de segurança dos dados armazenados no servidor.
- ✓ Servidor WEB – também conhecido como servidor de hospedagem, armazena as páginas dos usuários que ficarão disponíveis na internet, para acesso pelos clientes via browsers. Vale salientar que muitas vezes um servidor WEB está ligado a outros serviços do servidor como banco de dados, servidores de aplicações server-side, entre outros.
- ✓ Servidor de DNS – estes servidores fazem a tradução dos endereços digitados nas URLs dos browsers em endereços IP e vice-versa. Este servidor exerce uma tarefa de extrema relevância para as redes de computadores, pois sem eles, cada vez que acessássemos um site, por exemplo, teríamos que digitar seu endereço IP correspondente.
- ✓ Servidor proxy – um proxy pode exercer diferentes tipos de serviços a uma rede de computadores. Em geral um proxy está associado a cache, que nada mais é do que o armazenamento local no servidor das páginas da internet mais visitadas. Dessa forma, cada vez que um novo usuário acessar um site já acessado anteriormente, o servidor retornará para este usuário a página armazenada no cache local do servidor, o que se torna muito mais rápido do que abrir uma nova conexão e buscar os dados novamente em um servidor externo.

2.7.4 Principais dispositivos de uma rede

Uma rede de computadores é composta por diferentes dispositivos, cada um com sua função, com o objectivo de dar funcionalidade e organização, bem como, prover a comunicação entre os diferentes componentes de uma rede [21]:

- ✓ Host – equipamento utilizado pelos usuários finais para processamento das aplicações e conexão à rede. Enquadram-se nesta descrição os notebooks, netbooks, computadores pessoais, entre outros.
- ✓ Interface de rede – cada computador, notebook, entre outros dispositivos se conectam à uma rede de computadores através de uma placa de rede. A esta placa de rede é dado o nome de interface de rede. Uma

placa de rede pode ser do tipo Ethernet cabeada (na qual um cabo é conectado a esta placa) ou então Ethernet sem-fios (placas que se comunicam via Bluetooth, ondas de rádio, etc.). Características como velocidade, modo de funcionamento e barramento de conexão, podem variar de uma interface para outra.

- ✓ Hub – o hub (concentrador) é um dispositivo cuja função é interligar os computadores de uma rede local. O funcionamento do hub se difere de um switch, pois o hub simplesmente repassa o sinal vindo de um computador para todos os computadores ligados a ele (como um barramento).
- ✓ Switch – semelhante ao hub, um switch serve de concentrador em uma rede de computadores com a diferença de que recebe um sinal vindo de um computador origem e entrega este sinal somente ao computador destino. Isto é possível devido a capacidade destes equipamentos em criar um canal de comunicação exclusivo (origem/destino). Esta prática diminui consideravelmente o número de colisões e a perda de pacotes na rede
- ✓ Bridge – ponte de ligação entre duas ou mais redes. Como exemplo, podemos citar uma ponte entre uma rede cabeada e uma rede sem-fio.
- ✓ Gateway – sinónimo de roteador na arquitectura TCP/IP, é o equipamento que conecta os hosts à rede. Em outras arquitecturas de redes, um gateway é um dispositivo (hardware ou software) que converte mensagens de um protocolo em mensagens de outro protocolo
- ✓ Roteador – dispositivo de rede que interconecta duas ou mais redes físicas e encaminha pacotes entre elas.
- ✓ Ponto de acesso wireless (access point) – equipamento responsável por fazer a interconexão entre todos os dispositivos móveis em uma rede sem-fio. Uma prática comum é a interligação de um access point a uma rede cabeada, para, por exemplo, prover acesso à internet e a uma rede local de computadores.

2.7.5 Principais conceitos relacionados às redes de computadores

A seguir, separamos alguns dos principais conceitos relacionados as redes de computadores, como forma de entendermos as principais nomenclaturas e quais suas funções no contexto das redes de computadores[21]:

- ✓ Protocolo – um protocolo, em uma rede de computadores, nada mais é do que um conjunto de regras e convenções que definem a comunicação dos dispositivos em uma rede. Um dos protocolos mais conhecidos de rede de computadores e da própria internet é o protocolo TCP/IP.
- ✓ TCP/IP – o protocolo TCP/IP é a junção de dois protocolos diferentes o TCP e o IP. O protocolo TCP (Transmission Control Protocol) é o protocolo padrão que define o serviço de circuito virtual da camada de transporte da arquitetura TCP/IP. Já o protocolo IP (Internet Protocol) é o protocolo padrão que define o serviço de entrega não confiável e não orientado à conexão da camada de rede do TCP/IP.
- ✓ Endereço IP – um endereço IP é um identificador de um dispositivo pertencente a uma rede de computadores. Também conhecido como endereço lógico, pode conter endereços reservados, que são utilizados dentro de uma rede local, também conhecidos como não-roteáveis e endereços IP's válidos, utilizados publicamente, inclusive no acesso à internet.
- ✓ Endereço MAC – um endereço MAC (Media Access Control) também conhecido como endereço físico, é atribuído quando da fabricação de uma interface de rede, por exemplo. Este endereço é único para cada dispositivo de rede.
- ✓ Porta – uma porta em uma rede de computadores corresponde a representação interna do sistema operacional de um ponto de comunicação para envio e recepção de dados. Uma porta é representada por um número, na qual é realizado determinado acesso .

Capítulo 03 – Meios Tecnológicos

3.1 Modelo de Sistema de Intercomunicador

O modelo que foi usado no projecto é um modelo da marca Dahua que é composto por um VTO modelo DHI-VTO2111D-WP-S e um VTH modelo VTH2621G –WP.

Figura 20 - Ilustração do modelo VTO e VTH

O VTO é estação externa do intercomunicador, que pode ser conectada ao VTH que é a parte interna do intercomunicador, VTS é estação mestre do intercomunicador de vídeo, que suporte videochamada entre visitantes do local. O VTO suporta o desbloqueamento por senha ou cartão de acesso, suporta funções de segurança, incluindo chamadas de emergências, publicação de informações e visualização de histórico.

O modelo de VTO usado no projecto é de fácil instalação e manuseamento, este contem

as seguintes especificações:

Parte Frontal do VTO

1- Microfone;

2- Câmera;

3- Leitor de cartão de acesso;

4- Luz indicadora;

5- Botão de chamada;

6- Alto-falantes.

Parte Traseira do VTO

1- Posição do suporte;

2- Alarme à prova de vandalismo;

3- Entrada/saída de alarme Interface;

4- Botão de reset;

5- Porta de rede RJ45;

6- Entrada para alimentação;

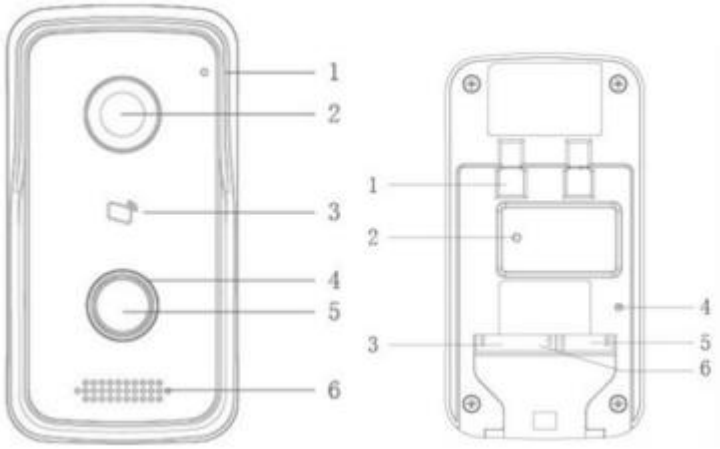


Figura 21 - Illustração do VTO modelo DHI-VTO2111D-WP-S parte frontal e parte traseira.

E o modelo VTH contem as seguintes especificações:

Parte Frontal

1- Ecrã sensível ao toque;

Parte Traseira

1- Porta de alarme;

2- Porta de entrada para alimentação;

3- Porta de rede RJ45.

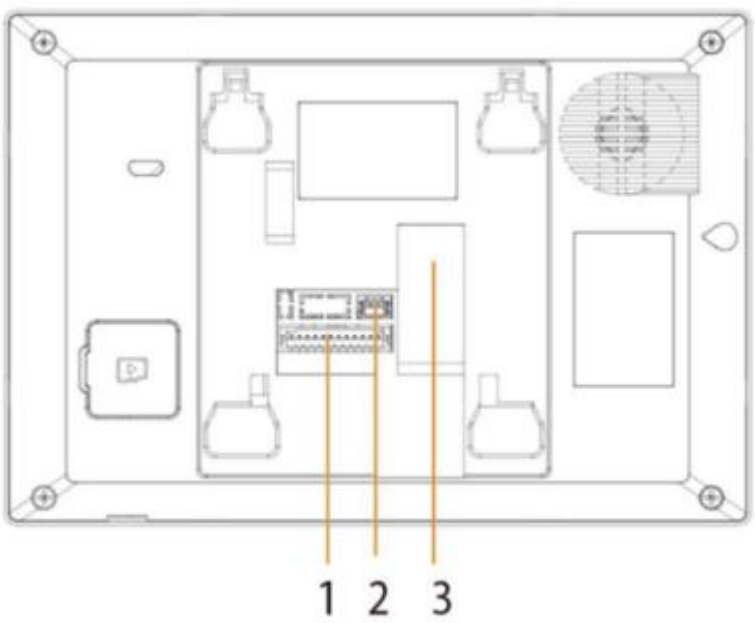


Figura 22 - Ilustração do VTH

No VTO encontramos o microfone este que têm como função de servir como entrada de áudio, câmera de 1.3 Megapixes como entrada de imagens e visualização ou por outros meios, leitor de cartão de acesso para casos em que o VTO esteja ou seja conectado à fechadura magnética para abertura e fechar uma porta, luz de sinalização de seu funcionamento, botão de chamada para inicialização de comunicação por meio do VTH, alto-falantes para que ao se efectuar uma chamada os utentes possam ouvir um ao outro, posição de suporte que serve para fixação seja na parede ou em outro local, alarme a prova de vandalismo que é accionado quando o VTO é removido, interfance para alarme e como Entrada RJ45 para comunicação por meio de uma rede de intranet ou internet.

Algumas das funções do VTO como de áudio, alto-falante, entrada para alarme, existem também no VTH, apesar de não terem sido descritas na figura 1.3, para além dessas funções o VTH é constituído por uma ecrã na sua parte frontal que serve para programação do próprio VTH e como também do VTO.

3.1.1 Configuração e Instalação do VTO e VTH

Para iniciar a configuração da unidade de VTO, temos que se certificar que unidade temos que:

- Verifique se a unidade está conectada à fonte de alimentação adequada;

- Planear a lista de endereços IP e os números de ID para cada unidade VTO e VTH;
- Verifique a posição de implantação do servidor SIP;
- Usar a interface da Web do VTO para definir as informações de VTO e VTH;
- Em seguida, defina o VTH e o VTO informações em cada dispositivo VTH.

Passos para configuração do VTO:

- Inicialize o VTO;
- Configure o número VTO;
- Configure os parâmetros de rede VTO;
- Configurar o servidor SIP;
- Adicione dispositivos VTO ao servidor SIP.

Para configuração do VTH ao ser ligado pela primeira vez é necessário configurar a língua e região, em seguida deve ser seleccionar o modo de funcionamento se é para um apartamento ou um condomínio, após esse dois passos define se a senha e o email de recuperação. Deve se desactivar se o DHCP automático e colocar o IP estático, tanto o VTO e VTH podem servir como servidor SIP mas nessa instalação seleccionou se o VTH como servidor SIP, então o mesmo IP que foi seleccionado no VTO como IP do SIP deve ser o mesmo do VTH, depois dessa configuração os utentes podem desfrutar de todas funcionalidades disponibilizadas no VTH.

3.2 Modelo de Sistema de Alarme

O modelo da central de alarme que foi usado é um modelo da hikivision DS-PWA32-HR(868MHZ) que é uma central sem fio, juntamente com dois sensor, sensor magnético modelo hikivision DS-PD1-MC-WWS (reed switch) e sensor infravermelho passivo modelo DS-PDP15P-EG2-WB.

Figura 23 - Ilustração da Central Hikivision Modelo DS-PWA32-HR

A central de alarme suporta até 32 entradas sem fio, 4 expansores de saída sem fio, oferece dois métodos de configuração que pode ser via cabo de rede LAN e Wi-Fi ou por meio da GSM por meio de um cartão sim, têm dois canais de verificação de área monitorada que têm como função gravação curta vídeo após o accionamento do alarme no canal, comunicação até 800 m em área aberta, suporta armar e desamar passando o cartão com leitor de proximidade embutido

3.2.2 Configuração e Instalação

Para instalação da central deve-se seguir os seguintes passo:

- Permitir a ligação para configuração via GSM (SIM CARD), via ethernet ou por meio de wireless;
- Conecte a bateria ao painel de controle;
- Conecte o adaptador de energia ao painel de controle e em uma tomada elétrica.
- O indicador de alimentação fica verde após cerca de 30 segundos, o que significa que o dispositivo está ligado.

A configuração pode ser feita via três metodos:

- Configuração via app (Hik-conect);
- Configuração via Cliente Web;
- Configurar via Cliente 4200.

Configuração via app

- Acesse a App Store ou o Google Play e insira Hik-Connect para buscar e instalar o cliente para celular;
- Acesse o app com a conta Hik-Connect;
- Selecionar em adicionar dispositivo, fazer leitura do código QR (na etiqueta).
- selecionar em conectar a uma rede. Selecione Conexão sem fio (AP) como modo de conexão.
- Posicione o botão dos modos AP/STA em AP e toque em Confirmar.
- Selecionar em Conectar ao Wi-Fi na janela de aviso. Selecione e conecte a uma rede Wi-Fi estável e clique em Avançar.
- Crie uma senha para ativar o dispositivo.
- Coloque o interruptor de modo AP/STA na posição STA.

Configurar via Cliente Web

- Acesse o Cliente Web
- O endereço IP padrão ao usar o navegador móvel em modo AP é: 192.168.8.1 e o endereço IP padrão ao conectar o cabo de rede directamente no computador é: 192.0.0.64.
- Insira o endereço IP do dispositivo na barra de endereços do navegador da internet. Crie uma senha para ativar o dispositivo e acesse o cliente Web.

Adicione uma câmera para a zona

- Clique em Sistema - Câmera de rede, e você poderá adicionar duas câmeras no painel de controle.
- Clique em Dispositivo sem fio - Zona, selecione uma zona, clique no ícone

Configurar via Cliente 4200

- Baixe e instale o cliente iVMS-4200.
- Entre na página Gerenciamento de Dispositivos, selecione o dispositivo na Lista de dispositivos online, clique em Editar configurações da rede, altere a porta para 80 e clique em adicionar ao cliente.

Para o adicionamento dos sensores é necessário alterar o modo de funcionamento da central pois ela funciona em dois modos receive signal e o send signal, para que este possa reconhecer e adicionar os sensores deve se mudar para o modo send signal. Após a central ser colocado no modo de funcionamento send signal , deve se aproximar a central dos sensor, assim que central estiver próximo dos sensor, alimenta-se os sensor e estes são adicionados a central, cada sensor de forma sequencial, o primeiro a ser adicionado vai para área 1 assim sucessivamente até 32 canais se for necessário. Mas nesse caso somente foram adicionados dois sensor na área 01 o sensor infravermelho e na área 02 o reed switch.

3.3 Modelo de Sistema CCTV

Para o sistema de CCTV foram os usados os seguintes equipamentos:

- NVR;
- Câmeras Dome;
- Câmeras Bullet.

O NVR da marca dahua modelo N42C3P8 apresenta as seguintes especificações:

- Codec duplo Smart H.265+ e Smart H.264+
- Largura de banda de gravação máxima de 160 Mbps
- Resolução de até 8 MP para visualização e reprodução

- Saída de vídeo simultânea HDMI e VGA
- Suporta configuração remota e Gerenciamento de remota de câmeras;
- Suporta Vigilância Remota P2P e Aplicativo Móvel DMSS
- 16 Portas PoE/PoE+

As câmeras pertencem também a marca dahua dome modelo IPCHDBW1235E-W-S2 e Bullet modelo DH-IPC-HFW3549E-AS-LED.

Figure 24 - Ilustração de um Câmera Modelo IPC-HDBW1235E-W-S2 e DH-IPC-HFW3549E-AS

3.3.1 Configuração e Instalação

Para instalação de equipamentos de CCTV deve identificar os locais para instalação das câmeras, este locais devem ser estratégicos, que podem cobrir lugares estratégicos como entradas e saídas dos escritórios.

As câmeras IP dome foram instaladas no interior do escritório e câmeras bullet estas foram instaladas na varanda pra observação do estacionamento. O NVR, como o monitor foram instalada na sala do servidor.

O endereço IP que foi definido para o NVR é o 192.168.1.240. Em seguinda faz se configurações de segurança que implica senhas, email de recuperação e outros dados necessários. Depois desse passos, deve se adicionar as câmeras disponível via wireless. Temos que ir para um campo de pesquisa das câmeras, aonde procura as câmeras e adiciona se, as câmera que usam o meio de transmissão wireless foram aquelas instaladas no interior do escritório que os IP estavam no intervalo de 192.168.1.241-192.168.1.248

Para conectar as câmeras IP a rede, deve se fazer uso de informações disponível na lista de descrição da câmera, que é código da câmera e nome de identificação. Com as duas informações é possível configurar uma câmera IP,

isso nos possibilita alterar o nome como a credenciais das câmeras. As câmeras dome IP, estas podem ser acessadas remotante sem a necessidade do NVR, estas apresentam interface web para sua configuração, nessa interface web pode se efectuar o gerenciamento da câmera. A câmera dome IP, mesmo sem a NVR efectua a gravação das imagens captadas por meio de um cartão SD que lê ate 256GB, no NVR foi instalado um disco duro de 6TB, que possibilitada a gravação de imagens mensais e que depois desse periodo o NVR foi programado para rescrever sobre as imagens existentes. As câmeras Bullet for conectadas ao NVR por meio do Switch, assim como NVR o Switch usado é munido da tecnologia POE que leva alimentação por meio do cabo Ethernet assim sendo o mesmo cabo de transmissão de imagens foi o mesmo cabo que leva alimentação para as câmeras, para adicionar estas câmeras bullet ao NVR é processo simples, como estas estão conectadas por meio do cabo Ethernet para visualização das imagens por meio de NVR foi necessário somente conectar ao NVR. Para visualização remota das câmeras em conjunto o NVR, faz uso de um tecnologia de comunicação Peer to Peer que é comunição ponto a ponto, isso que dizer que não faz necessário o uso de servidor e web para ser ter acesso ao NVR.

3.4 Modelo de Sistema de Controle de Acesso

O modelo do sistema de controle de acesso é o Inbios da Zkteco. A unidade de processamento é o Inbios 460, o dispositivo de identificação para cada entrada é leitores biométricos de impressão digital,este faz leitura da impressão digital de cada usuário que será usado como credencial de identificação e o dispositivo de bloqueio usado é a fechadura magnética.

3.4.1 INBIOS 460

A Inbios 460 é a central do processamento do sistema de controle de acesso com as seguintes especificações:

- CPU de 1,2 GHz de 32 bits de alta velocidade, 128 M de RAM e 256 M de Flash.
- Sistema operacional LINUX embutido;
- Acesso bidireccional de duas portas ou acesso unidireccional de quatro portas.

- Capacidade de impressão digital: 20.000.
- Um máximo de 60.000 portadores de cartão e 100.000 registos de eventos offline
- Suporte de vários formatos de cartão Wiegand e um teclado de senha, compatível com vários tipos de cartas.
- Comunicação dupla de barramento industrial Ethernet e RS485, para comunicações confiáveis.

Figura 25 - Ilustração da Central INBIOS 460

3.4.2 Leitor Biometrico FR1200

FR1200 é um leitor de impressões digitais e cartões RFID 125 kHZ, se comunica através do protocolo RS485. Funciona com controles de acesso stand alone e equipamentos da linha inBio. Captura as impressões digitais, cartões e transfere as informações para o equipamento mestre.

Figura 26 - Ilustração do Leitor Biometrico FR1200

3.4.3 ZK4500

ZK4500 é um scanner de impressão digital estável e excelente. O dispositivo pode capturar a imagem da impressão digital e fazer o upload para o PC pela interface USB.

Figura 27 - Ilustração do Leitor Biometrico ZK4500

3.4.4 Fechadura Electrmagnetica

Um maglock é um dispositivo de travamento electrificado que usa energia de baixa tensão para manter uma entrada segura. Também conhecido como trava electromagnética ou trava magnética, eles consistem em um electroíman e uma placa de armadura. O electroíman é montado na moldura da porta e é conectado de volta a uma fonte de alimentação, enquanto a placa da armadura é montada na porta.

Com energia, o electroíman é energizado, criando um fluxo magnético que atrai a placa da armadura. O resultado é uma acção de travamento, que faz com que a entrada permaneça segura. Como a área da superfície é relativamente grande, a força criada pelo fluxo magnético é forte o suficiente para manter a porta travada sob tensão.

Quando a energia é removida, o maglock é liberado, permitindo que a porta se abra. Essa configuração é conhecida como à prova de falhas, o que significa que, quando a energia falha, a porta permite uma saída segura.

Figura 28 - Ilustração do Maglocks

Existem diferentes tipos de maglock que podem ser classificados segundo a sua disposição e como também a força, esta que pode ser de 250 Kg ou 300kg.

3.4.5 Configuração e Instalação

A central Inbios 460, suporta até 4 portas para controle de acesso no sentido unidireccional e duas portas no sentido bidireccional.

A instalação que foi levada a cabo no local foi configuração no sentido unidireccional, isso quer dizer que somente faz se uso do leitor da impressão digital somente para entrar no local e para saída do local faz se uso de exit button.

As portas em que foram seleccionadas para instalação dos leitores de impressão digital, foi a porta da entrada e da sala do servidor.

A central de controlo foi instalado na sala de servidor, com bateria de backup para o sistema com uma duração 12 horas de tempo, todos componentes do sistemas são alimentados a partir do mesmo power supply, que foi instalado juntamente com a central de controle.

Para diferenciar o leitor biométrico de impressão digital efectua se a codificação de cada um deles por meio de pintos DIP existentes no leitor, isto para que central não os identifique como um só.

Para além dos leitores biométricos de impressão digital foram instalados os Key Switch.

Key Switch são dispositivos que têm a função de destrava maglocks por meio de uma chave este dispositivo é instalado para momento de emergência para permitir abertura da porta, é instalado do lado de fora.

Como outros dispositivo apresentado ao logo do relatório o Inbios 460 também é um dispositivo que permite a ligação a rede por meio do cabo ethernet.

Este também na sua inicialização permite, que seja definidas sua senha mas diferentes dos outros não se define email de recuperação e nem introduz se outros dados, para além da senhas e do nome do administrador.

Para configuração da central é necessário fazer o uso de software, pois apesar de conectar a rede de internet este não possui uma interface web.

Existem vários aplicativos que podem ser usados para a gestão da central, mas o aplicativo que foi seleccionado nesse caso foi o Zkacess 3.5 Security System, que para além do controle pode gerar relatório de presença.

Esta aplicação possibilita o monitoramento em tempo real, aberturas e fechamento de porta remotamente desde que estejamos na mesma rede, gerenciamento das portas configuradas, conexão com base de dados e várias outras funções.

Para efectuar o cadastramentos dos utentes do sistemas deve usar leitor óptico ZK4500, este que têm como função fazer a leitura das impressão digital.

Ao efectuar se o cadastro no software que posteriormente deve se enviar para a central de controle.

Existe a possibilidade de registar os 10 dedos das mãos ou pode seleccionar os dedos que pretende registar para servir como credências para biométrica para abertura da porta.

Como critério de registo proposto foi o registo de dois dedos para cada pessoa que foram registada, estes que podem ser da mão direita ou esquerda.

Para organização é possível criação de departamento e outros meios para identificação, como introduzação de foto, no momento de levantar o monitoramento o sistema disponibiliza cada entrada efectuada

Sendo que cada leitor biométrico é associada a uma área, o leitor biométrico foi associado a área da entrada, e todas impressões cadastradas foram associadas a esse grupo, enquanto para a área da sala do servidor foram seleccionadas somente 3 usuários.

O sistema pode ter mais de um administrador, mas o administrador principal têm possibilidade de criar regras para os outros utentes para que não possam mudar as configurações do sistema.

Tipo de Sistema	Equipamento	Marca	Modelo	Quantidade
Intercomunicador	VTO	Dahua	DHI-VTO2111D-WP-S	1
	VTH	Dahua	VTH2621G –WP	1
Alarme	Central de alarme	Hikivision	DS-PWA32-HR	1
	sensor magnético	Hikivision	DS-PD1-MC-WWS	1
	Sensor Infravermelho	Hikivision	DS-PDP15P-EG2-WB	1
CCTV	NVR	Dahua	N42C3P8	1
	Câmeras a cabo	Dahua	IPC-HDBW1235E-W-S2	8
	Câmeras Wi-fi	Dahua	Dahua DH-IPC-HFW3549E-AS	3
Controle de Acesso	Central de Controle	Zkteco	INBIOS 460	1
	Leitor Biometrico	Zkteco	FR1200	2
	Scanner Biometrico	Zkteco	ZK4500	2
	Botão de Saída	Zkteco		2

Tabela 1 - Equipamentos do Sistema

Capítulo 04 – Avaliação e Conclusão

4. Avaliação do impacto da implementação do projecto de segurança nos escritório da OCEANA LIMITADA

Apesar da existência de uma segurança própria de edifício em questão, esta apresenta vulnerabilidade no seu controle, pois quando alguém acessa ao edifício não são tomadas medidas de percussão no sentido de saber a identidade de quem para aonde vai e o quê pretende fazer, simplesmente a pessoa têm livre acesso ao local.

As câmeras existente no local somente estão instalados no corredor da recepção, depois desse local o individuo esta livre de fazer e proceder com seus intentos.

Com a implementação do projecto pode se notar a melhoria de certos aspectos, pois primeiramente a instalação da câmera de segurança no corrector permite observar as acção que decorrem nesse espaço e capta a imagem de cada invidio que por ali circula a todo momento assim podendo observar qualquer acção suspeita.

Com as câmeras instaladas no interior do escritório, é possível observar as acções de quem encontra se dentro do escritório em dias de expediente como em outras ocasiões, tornam possível identificar o individuo e saber por aonde este circula.

O sistema de alarme apesar de não possui uma sirene de longo alcance em termos sonoricos, este possui o alerta por envio de mensagens pela internet, que envia notificação ao administrador e vários utentes em caso de ocorrer alguma anomalia depois da activação do mesmo, assim como as câmeras possibilitam o acesso remoto após a recebimento do alarme é possível observar o que se acontecer na área que alarme foi emitidos pois estes locais também estão equipados de câmeras.

Como o sistema de controle de acesso, antes da instalação desde a porta permanecia semi aberta, isso para permitir a entrada e saída dos funcionários e

do outros utentes, assim sendo tinha acesso a escritório sem ser necessário respeite nenhum protocolo.

Com instalação do sistema de controle de acesso e também com a instalação do intercomunicador, permitiu uma maior controle para quem busca entrar no escritório, a dependência das chaves para acessar o escritório foi eliminada assim sendo funcionárioscadastrados no sistema tem poder de acessar o escritório dentro do tempo estabelecido.

Pelos motivos descritos pode se concluir que com implementação do projectos, este trouxe um impacto positivo para segurança do escritório

4.1 Conclusão

Após a implementação do projecto de segurança electrónica nos escritórios da Oceana limitada que teve com objectivo principal melhor a segurança do local, pode-se concluir que este objectivo foi alcançado.

Para o alcance desse objectivos foi necessário identificar as necessidades do local e buscar meios tecnológicos de segurança que tivesse capacidade para suprir as necessidades identificadas.

Os meios encontrados foi por implementação de sistema de intercomunicador, sistema de CCTV, sistema de alarme e sistema de controle de acesso. Este sistema que são composto de equipamentos tecnológicos que permitiu uma ligação remota entre o sistema e o usuário do mesmo.

Os sistemas implementados não só melhorou a segurança do local e como também melhorou a fluidez da empresa, melhorando assim a forma de trabalho

A implementação desse projecto não vai eliminar ou impedir na totalidade a ocorrencia de eventos indesejados no recinto de edifício mas se vai melhor a na prevenção.

4.2 Referências Bibliográficas

[1] - Reddick, C. Homeland Security Preparedness and Information Systems: Strategies

for Managing Public Policy. New York: IGI Global.2010.

[2] - Sequesseque, Manuel T.M. O Impacto da Implementação de Segurança da Informação na Usabilidade dos Sistemas de Informação. Instituto Politécnico de Setúbal.2017.

[3] - Rosa, Marisa G. Projeto de Melhoria ao Controle de Acesso e Segurança Eletrônica. Universidade Federal do Paraná. 2011.

[4] - MARTE, Claudio Luiz. Automação predial: a inteligência distruída nas edificações. São Paulo: Carthago, 1995.

[5] - Da Silva, Danielle Simone. Proposta de Um Sistema de Segurança Eletrônica Predial. Universidade Federal do Rio Grande do Norte. 2004.

[6] - Ribeiro, Marco Antonio. Segurança. 1999.

[7] - GALHARDO, Antonio Tadeu. Sistemas Eletrônicos de Controle de Acesso. Universidade São Francisco. 2011.

[8] - BRASILIANO, A.C.R.; BLANCO L. Planejamento Tático e Técnico Em Segurança Empresarial. 1.Ed. Sicurezza: São Paulo, 2003.

[9] - Rodrigues, Ellen.P.T. Proposta de um modelo básico de sistemas de segurança patrimonial obtido por meio da aplicação da ferramenta de análise de risco em condomínios residenciais na Vila Mariana. Instituto de Pesquisas Tecnológicas do Estado de São Paulo:São. 2011.

[10] - User Manual. Invio 160/260/460 Pro Access Control Panel. 2021.

[11] - ZkTeco. Training Lesson. Inbios Series Installation.

[12] - TONN, Fabianna S; CITTOLIN, Guilherme.F; DE SOUZA, V. Desenvolvimento de Um Sistema de Monitoramento e Supervisão Via Web. Universidade Tecnológica Federal do Paraná. 2014.

[13] - BUXEL, Ismael.L. Sistema de Segurança com detecção e Acompanhamento de Movimento automatizado. Centro Universitário Univates. 2015.

[14] - De Souza, Dércia; DE Souza, Carlos; FAJAN, Fernanda. Câmeras de Segurança e seus Sistemas Tecnológicos: Percepções sobre os motivos da utilização. Fatec.

[15] - Garcia, Karla.M. Sistema de Controle de Acesso Veicular Utilizando Tecnologia RFID. Instituto Federal de Educação, ciência e Tecnologia de Santa Catarina. 2013.

[16] - JANES, Ricardo. Estudo sobre sistemas de segurança em instalações elétricas Automatizadas. Universidade de São Paulo. 2009.

[17] - LEGAT. Sistema de controle de Acesso em IOT. Universidade Federal de Santa Caratina.2018.

[18] - Volpato, Luan.C.S. Sistema de Segurança Residencial Integrado com Aplicativo para Smartphone. DAS, CTC, UFSC. 2012.

[19] - PEIXOTO, Thiago Moratori. Sistema de Controle de Acesso Utilizando Dispositivos Embarcados. Universidade Federal de Juiz de Fora. 2013.

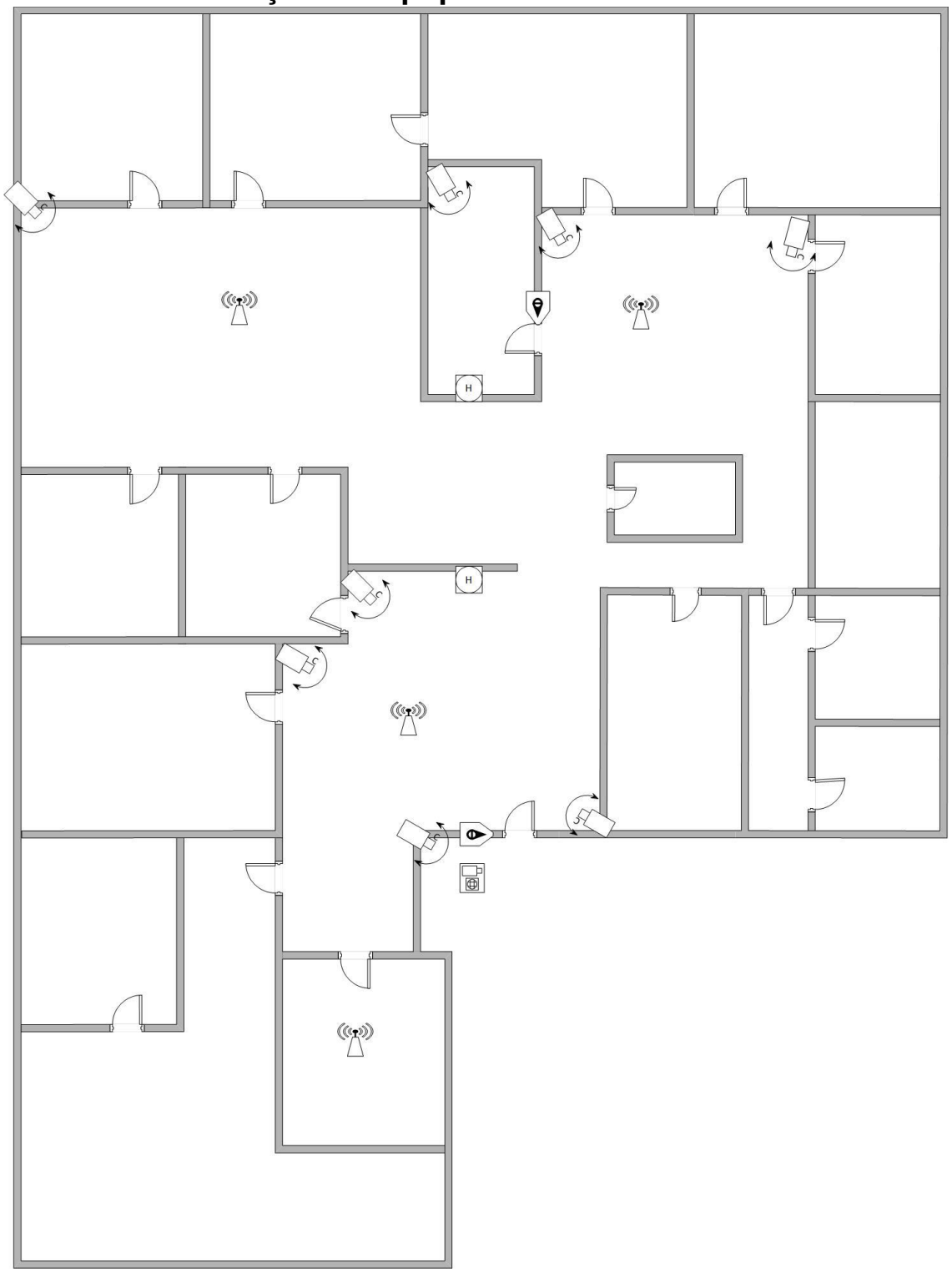
[20] – DA COSTA, João Paulo. Estudo de Viabilidade da Implantação de Um Empresa de Segurança Electrónica em Campina Grande-PB. Universidade Federal de Campina Grande Centro de Humanidades.2017.

[21] – PERLIN, Tiago; FRANCISCATTO, Roberto. Redes de Computadores.2014

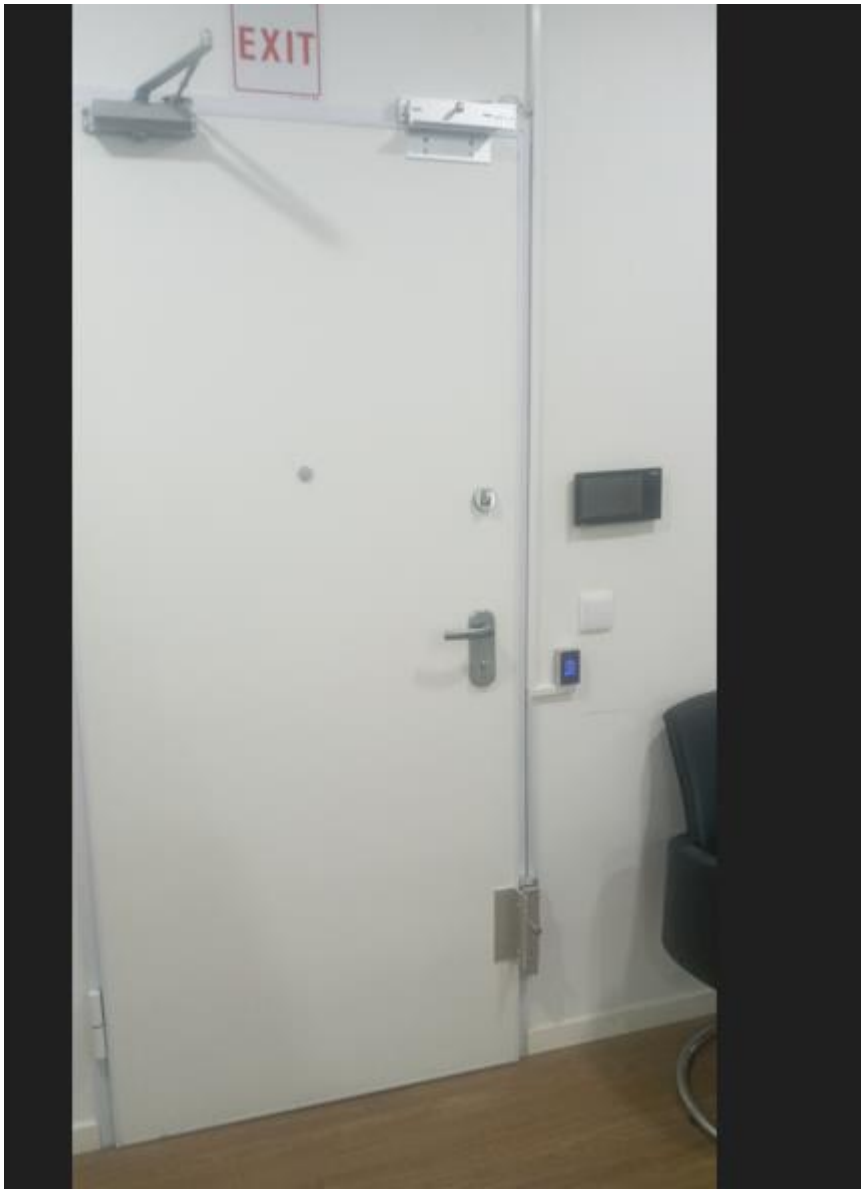
Anexos

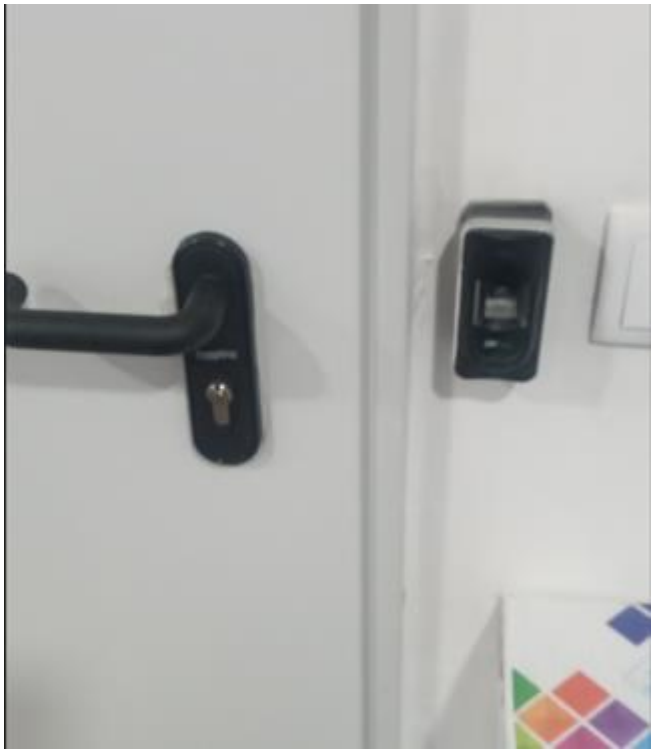
Anexos 1 – Desenho da Planta Baixa da Área do Escritório

Anexos 2 – Desenho da Planta Baixa da Área do Escritório Com Pontos de Instalação de Equipamentos



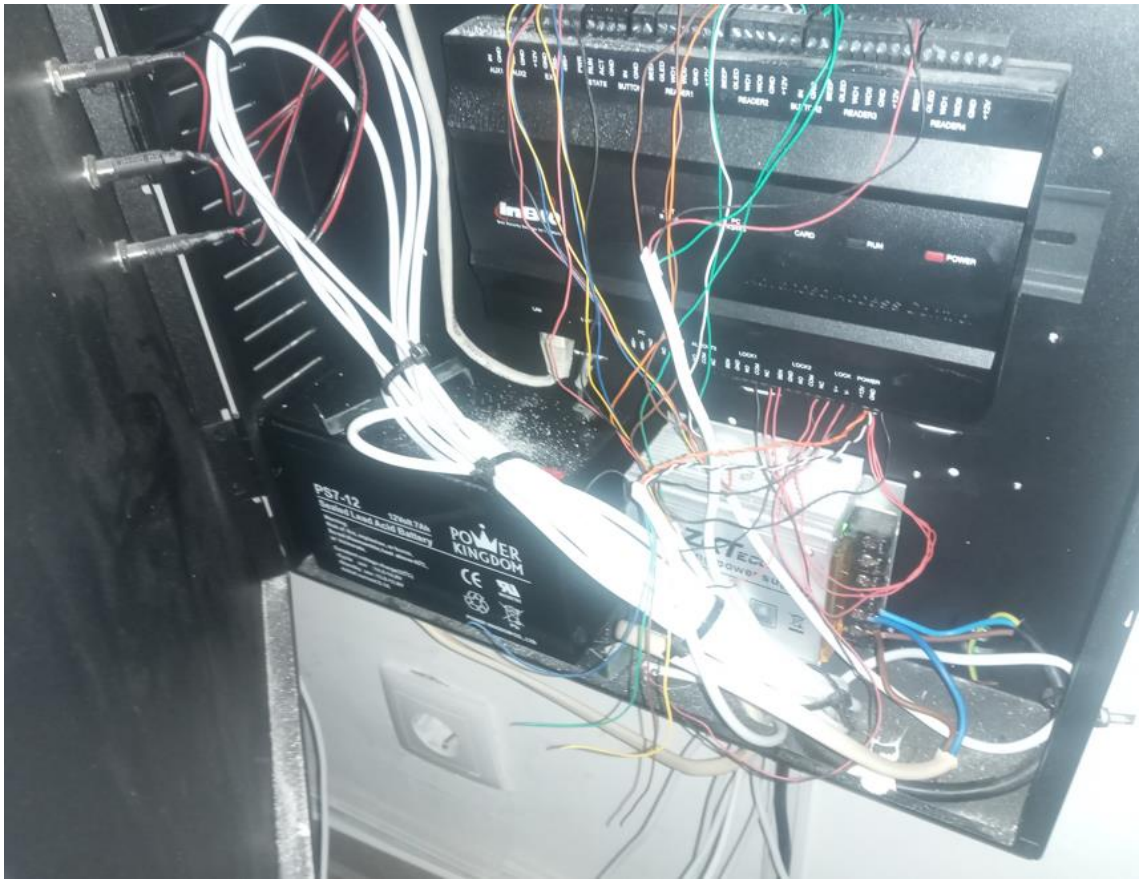
Anexos 3 – Imagem Após Implementação dos Sistemas


EXIT

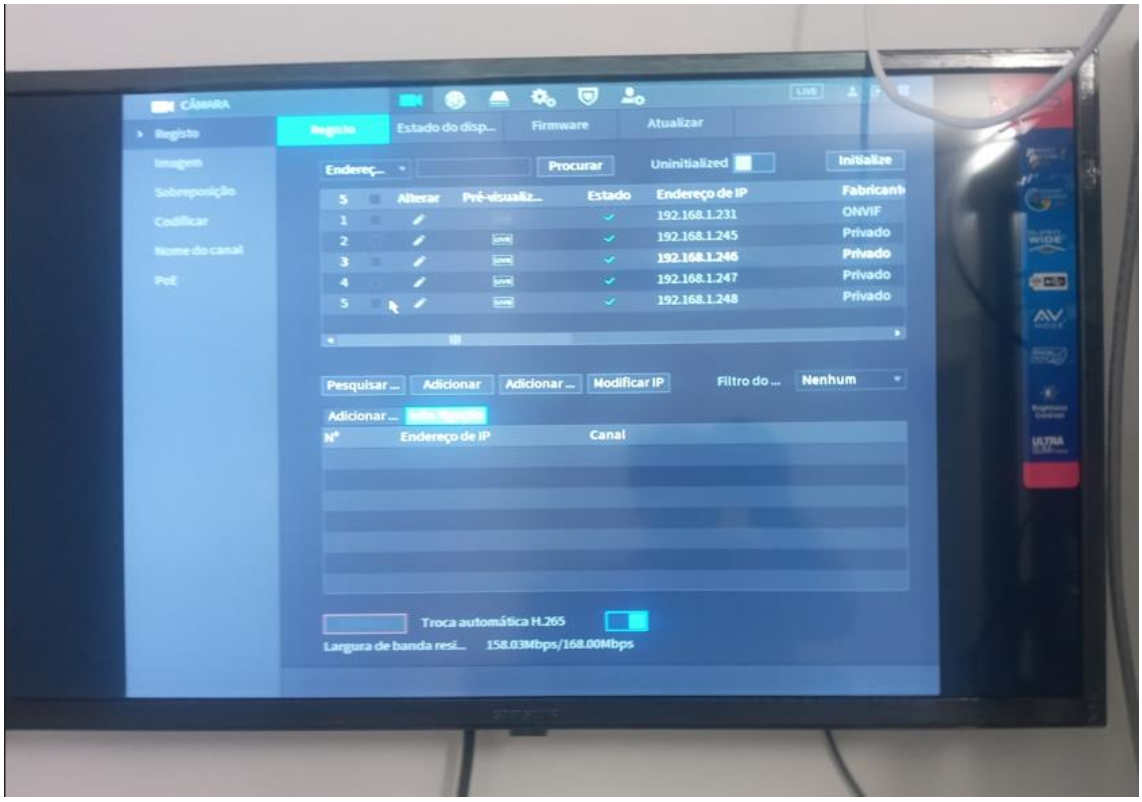



EXIT


ShareCenter
HIKVISION


POWER KINGDOM


Advanced Access Control
RUN
ZKTeco


CÂMARA
Registo
Imagem
Sobreposição
Codificar
Nome do canal
PoE
Registo
Estado do disp...
Firmware
Atualizar
Procurar
Uninitialized
Initialize
Alterar
Pré-visualiz...
Estado
Endereço de IP
192.168.1.231
ONVIF
192.168.1.245
Privado
192.168.1.246
Privado
192.168.1.247
Privado
192.168.1.248
Privado
Pesquisar ...
Adicionar
Adicionar ...
Modificar IP
Filtro do ...
Nenhum
Adicionar ...
Nº
Endereço de IP
Canal
Troca automática H.265
Largura de banda resi...
158.03Mbps/168.00Mbps