

**UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO”
FACULDADE DE ENGENHARIA
CÂMPUS DE ILHA SOLTEIRA**

VINICIUS DE ALMEIDA LONGO

Uma abordagem das tecnologias, dispositivos e aplicações de sistemas eletrônicos de segurança

**Ilha Solteira - SP
2022**

VINICIUS DE ALMEIDA LONGO

Uma abordagem das tecnologias, dispositivos e aplicações de sistemas eletrônicos de segurança

Trabalho de graduação apresentado à Faculdade de Engenharia de Ilha Solteira – Unesp como parte dos requisitos para obtenção do título de Engenheiro Eletricista.

Carlos Antonio Alves
Orientador

Ilha Solteira - SP
2022

FICHA CATALOGRÁFICA

Desenvolvido pelo Serviço Técnico de Biblioteca e Documentação

L856a Longo, Vinicius de Almeida.
Uma abordagem das tecnologias, dispositivos e aplicações de sistemas eletrônicos de segurança / Vinicius de Almeida Longo. -- Ilha Solteira: [s.n.], 2022
86 f. : il.

Trabalho de conclusão de curso (Graduação em Engenharia Elétrica) - Universidade Estadual Paulista. Faculdade de Engenharia de Ilha Solteira, 2022

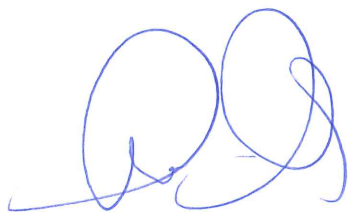
Orientador: Carlos Antonio Alves
Inclui bibliografia

1. Controle de acesso. 2. CFTV. 3. Segurança. 4. Sensores.

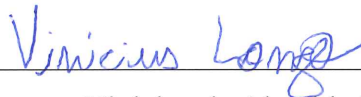

Raiane da Silva Santos

ATA DE DEFESA DE TRABALHO DE GRADUAÇÃO

Aos dezoito dias do mês de Julho do ano de dois mil e vinte e dois, o discente **Vinicius de Almeida Longo**, matriculada sob o nº 142053619, tendo como banca examinadora o seu orientador, o *Prof. Dr. Carlos Antônio Alves*, o *Doutorando Lucas do Carmo Yamaguti* e o *Doutorando Rodrigo Daltin*, apresentou o Trabalho de Graduação intitulado "**Uma abordagem das tecnologias, dispositivos e aplicações de sistemas eletrônicos de segurança**", obtendo a nota 9.0 (NOVE) e conceito APROVADO.



Prof. Dr. Carlos Antônio Alves
- Orientador -



Vinicius de Almeida Longo
- Discente -



Doutorando Lucas do Carmo Yamaguti
- Membro da Banca -



Doutorando Rodrigo Daltin
- Membro da Banca -

DEDICATÓRIA

Aos meus pais, por todo amor, compreensão e confiança integral durante estes 26 anos.

AGRADECIMENTOS

Aos meus pais, Edson e Rosilene, pelo apoio incondicional desde que me conheço, nunca me senti sozinho ou desacreditado por um segundo sequer, tenho realizado sonhos que por vezes acreditei impossíveis graças a tudo que ambos fizeram por mim. Ao meu irmão Tiago e meu primo Leonardo, pelo suporte integral e por todas as alegrias compartilhadas até então. A todos meus familiares, que sempre fizeram o possível para que me sentisse amado, acolhido e me suportaram sempre para que pudesse seguir meus sonhos. À minha namorada, Barbara, por todo o suporte e companhia durante o último ano. A todos os meus amigos, de diferentes lugares, que em momentos chave da minha vida sempre estiveram ao meu lado para compartilhar momentos bons e ruins, tive o grande privilégio de cultivar amizades incríveis por todos os vários lugares em que passei, sinto saudade de todos e sem dúvidas foram fundamentais para que construísse o que tenho e sou até aqui.

A todos meus professores da UNESP pela dedicação e pelo conhecimento compartilhado, são os grandes responsáveis pelos resultados extremamente gratificante que obtive neste início de carreira profissional, graças a toda paciência e troca que tivemos, sempre me senti competente e capaz de aprender ou realizar qualquer tarefa ou projeto proposto. Em especial, agradeço o professor Dr. Carlos Alves, por toda a atenção e dedicação que teve comigo seja, seja como no PET, orientador de estágio e também do trabalho de graduação, passos fundamentais para meu desenvolvimento acadêmico.

A todos meus colegas de turma por toda a troca durante os anos de graduação. A todo que fizeram parte das experiências incríveis que tive nos grupos de extensão da faculdade, que me trouxeram grandes amigos, desafios e aprendizados essenciais, seja no PET, na empresa júnior Potencial ou no centro acadêmico.

Meu agradecimento também e todos os cidadãos que contribuíram, muitas vezes mesmo sem desfrutar do mesmo retorno que eu, com o ensino público, gratuito e de qualidade. Me comprometo retornar todo o esforço e credibilidade de todos de alguma forma.

Por fim, agradeço a banca pela atenção, disponibilidade e contribuição com meu Trabalho de Graduação, passo fundamental em minha vida acadêmica e experiência de grande contribuição para meu desenvolvimento acadêmico e profissional.

RESUMO

Serão examinados neste estudo os pilares de um sistema eletrônico de segurança, começando pelas tecnologias de controle de acessos, serão abordados os mecanismos de identificação por meio de senhas, cartões e biometria, a fim de controlar os fluxos de pessoas e autenticação em áreas protegidas. Em sequência, aborda-se os métodos de detecção de intrusão por meio de sensoramento, analisando os sensores de detecção por infravermelho ativo, passivo, sensores de contato magnético e finalizando o estudo com os sensores sísmicos. Os sistemas de monitoramento por câmeras também são abordados, detalhando as tecnologias de registro de imagem, métodos utilizados para armazenamento de imagens, operação e análise e também as tecnologias existentes voltadas para monitoramento inteligente e vídeo analítico. Por fim desenvolveu-se um projeto de segurança para exemplificar como opera um sistema de controle de acesso, detecção de intrusão, monitoramento e integração utilizando placas controladoras, detalhando aspectos de aplicação e instalação de dispositivos disponíveis no mercado, aplicando na prática os conceitos teóricos abordados inicialmente.

Palavras-chave: Controle de acesso; CFTV; Detecção; Segurança; Sensores.

ABSTRACT

The pillars of an electronic security system will be analyzed in this work, starting with access control technologies, identification mechanisms through passwords, cards and biometrics will be addressed in order to control personnel flows and authentication in protected areas. In sequence, the methods of intrusion detection by sensors are approached, analyzing the following intrusion detection sensors: active and passive infrared, magnetic contact sensors and finally the seismic sensors. Camera monitoring systems were also addressed, detailing image recording technologies, methods used for image storage, operation and analysis, as well as existing technologies aimed at intelligent monitoring and analytical video. Finally, a security project was developed to illustrate in practice how an access control system, intrusion detection, monitoring and integration through controller boards operates, detailing aspects of application and installation of devices available on the market, applying in practice the theoretical concepts initially addressed.

Keywords: Access control; Detection; CCTV; Security; Sensors.

LISTA DE FIGURAS

Figura 1	- Elementos básicos de um sistema de segurança.....	15
Figura 2	- Sistema de detecção de entrada.....	15
Figura 3	- Teclado simples para validação de senha.....	18
Figura 4	- Cartão de banda magnética comum.....	19
Figura 5	- Cartão magnético e respectivas pistas.....	20
Figura 6	- Zona de inflexão.....	20
Figura 7	- Polarização da banda magnética.....	21
Figura 8	- Leitura na banda magnética.....	22
Figura 9	- Classificação dos cartões.....	23
Figura 10	- Padrão para tamanho de cartões.....	24
Figura 11	- Pinagem definida pela norma ISO78816.....	24
Figura 12	- Diagrama de blocos da interface de contatos de um chip de memória.....	25
Figura 13	- Diagrama de bloco da interface de contato de um chip com microcontrolador.....	26
Figura 14	- Diagrama de blocos básico de um sistema RFID.....	27
Figura 15	- Variedade de <i>tags</i> RFID.....	28
Figura 16	- <i>Tags</i> RFID passivas, semi passivas e ativas.....	29
Figura 17	- Construção de uma <i>tag</i> RFID.....	30
Figura 18	- Sistema RFID com interrogador à esquerda.....	31
Figura 19	- Espectro de radiofrequência.....	32
Figura 20	- <i>Tags</i> RFID passivas para frequências baixas, altas e ultra altas.....	33
Figura 21	- Leitura por meio do sensor óptico e capacitivo.....	35
Figura 22	- Terminações de cume (à esquerda) e bifurcações (à direita) ...	36
Figura 23	- Processo de armazenamento de impressão digital.....	36
Figura 24	- Diagrama de blocos de processo de validação de uma impressão digital.....	37
Figura 25	- Amostra capturada por um scanner de mão.....	39
Figura 26	- Amostra de mão com os pontos definidos para cálculo dos parâmetros.....	39

Figura 27	- Referenciamento dos pontos da mão e pontos referência para altura e largura.....	40
Figura 28	- Pontos utilizados para medir distância e parâmetros finais indicados.....	40
Figura 29	- Identificação da íris no olho humano.....	41
Figura 30	- Íris humana com parâmetros identificados, imagem monocromática a 35 cm de distância.....	42
Figura 31	- Imagem pré-normalização.....	43
Figura 32	- Imagem normalizada.....	43
Figura 33	- Construção física do <i>reed switch</i>	46
Figura 34	- Espectro eletromagnético e temperatura.....	47
Figura 35	- Princípio de funcionamento do sensor piroelétrico.....	48
Figura 36	- Diagrama de circuito do sensor infravermelho ativo.....	49
Figura 37	- Modelo de sensor ultrassônico HC-SR04 tradicionalmente utilizado no arduino.....	51
Figura 38	- Operação do sensor ultrassônico.....	52
Figura 39	- Deformação de um fio sob tração.....	54
Figura 40	- Extensômetros elétricos de resistência.....	55
Figura 41	- Esquema de confecção dos extensômetros.....	55
Figura 42	- Diagrama esquemático de uma câmera convencional.....	58
Figura 43	- Ilustração da primeira tentativa de reproduzir uma imagem digital.....	59
Figura 44	- Representação do pixel no eletrodo de silício.....	60
Figura 45	- Comportamento das cargas armazenadas ao variar a tensão do eletrodo.....	61
Figura 46	- Registro das informações recebidas pelo CCD sequencialmente por meio de linhas.....	62
Figura 47	- Ilustração do fluxo de elétrons pelo eletrodo através da variação de carga.....	62
Figura 48	- Solução possível: dividir os componentes da luz em três CCDs diferentes.....	63
Figura 49	- Adição do filtro de cor e estimativa por meio de algoritmo no processamento da imagem digital.....	64
Figura 50	- Organização das placas do sistema.....	72

Figura 51	-	Associações de resistores nas entradas das placas.....	75
------------------	---	--	----

LISTA DE TABELAS

Tabela 1	- Tamanhos mais comuns e suas respectivas aplicações.....	24
Tabela 2	- Comparação de métodos de biometria.....	44
Tabela 4	- Lista de dispositivos.....	67
Tabela 5	- Sensores da controladora 1.....	72
Tabela 6	- Sensores da controladora 2.....	73
Tabela 7	- Programação dos relés das sirenes.....	73
Tabela 8	- Controladoras de controle de acesso.....	74
Tabela 9	- Definições das áreas existentes.....	77

LISTA DE SIGLAS E ABREVIATURAS

CCD	<i>Charge Coupled Device</i> (Dispositivo de Carga Acoplada).
CFTV	Circuito Fechado de Televisão.
CMOS	<i>Complementary Metal-Oxide-Semiconductor</i> (Semicondutor de Óxido de Silício Complementar).
CPTED	<i>Crime Prevention Through Environmental Design</i> (Prevenção de Crimes Pela Arquitetura do Ambiente).
CPU	<i>Central Processing Unit</i> (Unidade Central de Processamento).
DPI	<i>Dots Per Inch</i> (Pontos por Polegada).
DVR	<i>Digital Video Recorder</i> (Gravador de Vídeo Digital).
ECC	<i>Elliptic Curve Cryptosystems</i> (Sistemas de Criptografia Elípticos e Curvados)
EEPROM	<i>Electrically Erasable Programmable Read Only Memory</i> (Memória de Somente Leitura Programável e Apagável Eletricamente).
FAR	<i>False Acceptance Rate</i> (Taxa de Falsa Aceitação).
FRR	<i>False Rejection Rate</i> (Taxa de Falsa Rejeição).
HF	<i>High Frequency</i> (Alta Frequência).
ISO	<i>International Organization for Standardization</i> (Organização Mundial para Padronizações).
LF	<i>Low Frequency</i> (Baixa Frequência).
NA	Normalmente Aberto.
NF	Normalmente Fechado.
NPU	<i>Number Processing Unit</i> (Unidade de Processamento Numérico).
NVR	<i>Network Video Recorder</i> (Gravador de Vídeo na Rede).
PIN	<i>Personal Identification Number</i> (Número de Identificação Pessoal).
PIR	<i>Passive Infrared Sensor</i> (Sensor de Infravermelho Passivo).
RFID	<i>Radio Frequency Identification</i> (Identificação por Rádio Frequência).
RGB	Vermelho, Verde e Azul.
RO	<i>Read Only</i> (Somente Leitura).
ROM	<i>Read Only Memory</i> (Memória de Somente Leitura).
RSA	Rivest, Shamir e Aldeman.
RW	<i>Read/Write</i> (Leitura e Escrita).
UHF	<i>Ultra High Frequency</i> (Frequência Ultra Alta).

SUMÁRIO

1. INTRODUÇÃO	14
2. SISTEMAS DE CONTROLE DE ACESSO	17
2.1 VALIDAÇÃO POR SENHA	17
2.2 CARTÕES MAGNÉTICOS	18
2.2.1 Gravadores de cartões magnéticos	20
2.2.2 Leitores de cartões magnéticos	21
2.3 CARTÕES INTELIGENTES	22
2.3.1 Cartões com chip	22
2.3.2 Sistemas RFID	26
2.3.2.1 Tags RFID	27
2.3.2.2 Leitores e controladores RFID	31
2.3.2.3 Escolha da frequência de operação	31
2.4 VALIDAÇÃO POR BIOMETRIA	33
2.4.1 impressões digitais	34
2.4.2 Geometria das mãos	37
2.4.3 Reconhecimento da íris	41
2.4.4 Biometria: considerações adicionais	43
3. SISTEMAS DE DETECÇÃO DE INTRUSÃO	45
3.1 SENSORES MAGNÉTICOS	45
3.2 SENSORES DE DETECÇÃO DE PRESENÇA	47
3.2.1 Sensor infravermelho passivo	47
3.2.2 Sensor infravermelho ativo	49
3.2.3 Sensor ultrassônico	51
3.3 SENSOR SÍSMICO	53
3.3.1 Extensômetro	53
4. SISTEMAS DE CFTV	57
4.1 PRINCÍPIO DE FUNCIONAMENTO	58
4.1.2 Definição de cores na imagem	62
4.2 CLASSIFICAÇÃO DE CÂMERAS POR CONEXÃO	64
4.3 CÂMERAS COMO DETECÇÃO DE INTRUSÃO	65
4.3.1 Vídeo analítico	65
5. PROJETO DE UM SISTEMA DE SEGURANÇA	67
5.1. CONSIDERAÇÕES SOBRE OS EQUIPAMENTOS ESCOLHIDOS	68

5.2 CABEAMENTO E INFRAESTRUTURA	70
5.2 ENDEREÇAMENTO DE SENSORES E ATUADORES NAS PLACAS	70
5.3 CONEXÃO DOS DISPOSITIVOS NAS PLACAS	74
5.4 MECANISMOS CONFIGURADOS	76
5.5 CÔMODOS E POSICIONAMENTO DOS DISPOSITIVOS	77
5.5.1 Recepção	77
5.5.2 Salas controladas 1 e 2	78
5.5.3 Sala de controle	78
5.5.4 Escritórios, copa e sala de reuniões	79
5.5.5 Corredor principal	79
6. CONCLUSÃO	80
REFERÊNCIAS	81
APÊNDICE A – LEGENDA DO PROJETO	84
APÊNDICE B – INSTALAÇÃO DE UM SISTEMA DE SEGURANÇA	85

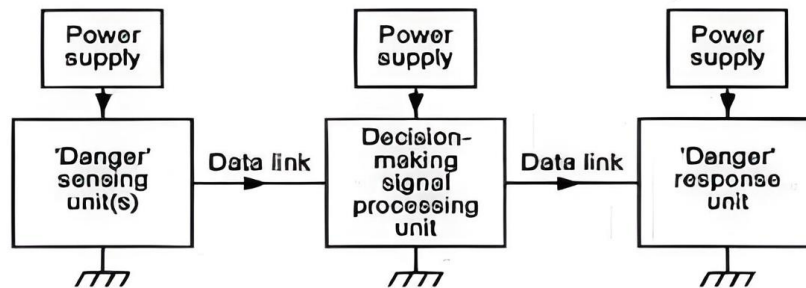
1. INTRODUÇÃO

Os sistemas de segurança são mecanismos que têm como objetivo afastar ou minimizar riscos inerentes a qualquer bem material ou pessoal desejado. Para isto emprega-se recursos para dissuadir, detectar, atrasar e defender-se da ameaça em prazo que atenda às necessidades do projeto. Considera-se então alguns pilares para garantir um sistema de segurança eficaz, são eles: pessoas, ambiente, procedimentos e infraestrutura. (PURPURA, 2011).

Os recursos humanos de um sistema de segurança são as equipes de profissionais de segurança contratados para rondas, postos de vigia, monitoramento de sistemas ou resposta a crises. Os recursos do ambiente são pautados nos conceitos do CPTED, que emprega arquitetura, engenharia e análise social para aprimorar a segurança, garantindo pontos importantes como visibilidade, difícil acesso físico, redução de esconderijo, compreensão dos riscos sociais do ambiente, entre outros; Já os procedimentos, buscam garantir que restrições e protocolos estratégicos para a segurança do local sejam observados, empreendendo revistas, proibição de alguns materiais, limitação de acesso, entre outros. O último pilar refere-se à infraestrutura instalada, contemplando desde cercas, portas, portões e muros até os dispositivos elétricos e eletrônicos.

Denomina-se sistema eletrônico de segurança como uma estrutura na qual as ações são totalmente dependentes de um circuito eletrônico, seja ele um alarme de porta, fechadura com teclado eletrônico ou até mesmo um simples alarme antirroubo (MARSTON, 1998). Os principais elementos de um sistema eletrônico de segurança são ilustrados na Figura 1.

Figura 1 - Elementos básicos de um sistema eletrônico de segurança

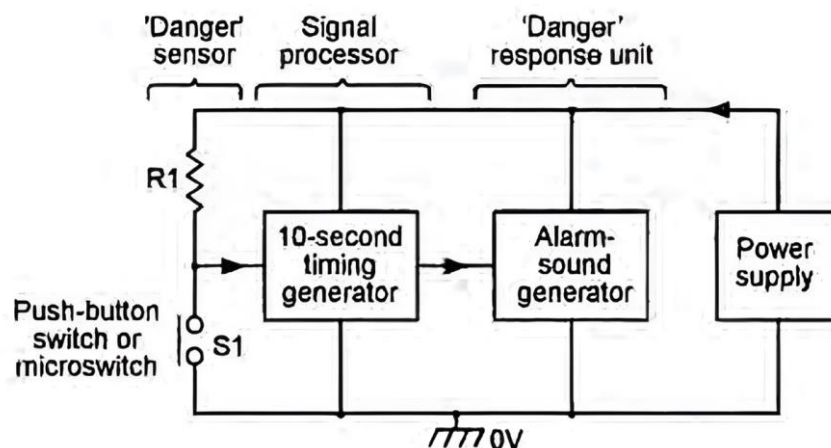


Fonte: MARSTON, 1998.

Todos os sistemas de segurança são compostos pelos elementos ilustrados na Figura 1, da seguinte forma: uma ou mais unidades de sensoriamento ficam dispostas na entrada do sistema, sendo responsáveis por gerar algum tipo de sinal elétrico como saída sempre que algum perigo for identificado. A saída da unidade de sensoriamento é enviada para uma unidade de processamento que, por sua vez, analisa a entrada, toma uma decisão e aciona, por meio de um segundo sinal elétrico, a unidade de “resposta à ameaça”, que interligada a dispositivos eletromecânicos ou alarmes, fica responsável pela atuação do sistema para conter o risco detectado.

Um exemplo prático para ilustrar a composição de um sistema eletrônico de segurança é o sistema de detecção de entrada simples com alarme, apresentado na Figura 2.

Figura 2 - Sistema de detecção de entrada



Fonte: MARSTON, 1998.

Neste caso, a chave S1 opera como unidade de detecção do sistema, enviando um sinal para a unidade simples de controle toda vez que for fechada. A unidade de processamento, por seu turno, envia um pulso com duração de 10 segundos para o alarme, que desempenha o papel de atuador eletromecânico do sistema. Com os exemplos, define-se de forma como uma unidade de sensoriamento, que emite sinal elétrico como saída quando detecta uma ameaça, esta é analisada por uma unidade de tomada de decisão, que responde ao sinal adequado ao elemento atuador, que pode ser um dispositivo elétrico, eletromecânico ou eletrônico.

Além de sensores de intrusão e atuadores, tecnologias mais recentes possibilitaram novos conceitos de controle dos sistemas de segurança, passaram então a fazer parte deste também os mecanismos de controle de acesso e monitoramento. Métodos de validar se um indivíduo realmente está autorizado a entrar em determinada área sem a necessidade de validação humana tornaram-se fundamentais e amplamente utilizados, contando com autenticações por senhas, cartões codificados e até mesmo por características biométricas, tornando possível não só eliminar riscos e custos relacionados a pessoas, mas também monitorar o fluxo dos locais de forma autônoma e inteligente. Os conceitos de controle de acesso serão detalhados abordando os métodos de validação por cartões magnéticos, inteligentes, *tags* RFID biométrica, bem como a combinação destes mecanismos para dificultar acessos indevidos.

O avanço nas áreas de eletrônica e computação permitiram também que recursos de captação, gravação e processamento de imagens também fossem integrados como parte fundamental de um sistema de imagens, servindo como base dos sistemas modernos de monitoramento. O uso estratégico de câmeras digitais e algoritmos de análise permitem que uma grande área seja monitorada por apenas um operador, que se preocupará apenas em tratar os eventos alertados pelos algoritmos do sistema, uma vez que estes fazem as análises necessárias, dessa forma, os CFTV (Circuitos Fechados de Televisão) também passaram a ocupar um papel determinante nos sistemas de segurança modernos. Este trabalho tem como foco abordar as tecnologias de controle de acesso, detecção de intrusão e monitoramento por CFTV e integrá-las, ilustrando em um projeto prático quais são os requisitos, desafios e recursos disponíveis para construir um projeto de sistema de segurança.

2. SISTEMAS DE CONTROLE DE ACESSO

Os sistemas de controle de acesso são os responsáveis por garantir que apenas pessoas autorizadas sejam permitidas a entrar ou sair das áreas controladas. Este controle é realizado por meio de cercas, portões, portas com trava eletrônica ou até mesmo um vigia que realiza o controle de acesso de forma manual. Como meio de validação, é possível utilizar senhas, cartões codificados e até mesmo características biométricas para garantir a autenticidade no momento do acesso. É fundamental combinar ao menos duas das três autenticações possíveis, exigindo alguma informação que só o solicitante saiba (senha), a posse de um item individual de validação (cartões ou *tags*) ou comprovar quem realmente é, por meio de biometria (PURPURA, 2011).

Tecnologias existentes para atender as combinações mencionadas serão abordadas neste capítulo, iniciando pela validação por senhas (validação mais simples), é possível combiná-la com alguns cartões com tecnologias de codificação/autenticação seja por tarja magnética, *chips* inteligentes ou até mesmo circuitos de autenticação por radiofrequência. Por fim, coloca-se como alternativa adicional os tipos mais comuns de controle de acesso por meio da biometria, seja por meio da detecção dos dedos, geometria da mão ou pela íris.

2.1 VALIDAÇÃO POR SENHA

O método básico de identificação para sistemas de controle de acesso eletrônicos é a validação por meio de uma senha digitada em uma simples leitora de 12 dígitos, contendo número de 0 até 9 e os símbolos * e #, conforme ilustrado na Figura 3. A maior vantagem desse tipo de leitora é que elas são muito simples de utilizar, além de muito baratas.

Figura 3 - Teclado simples para validação de senha



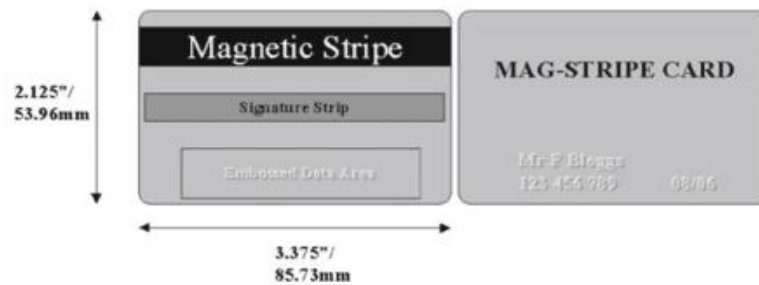
Fonte: NORMAN, 2007.

A grande desvantagem é que pode ser relativamente fácil para alguém que deseje acessar indevidamente o local espiar algum código válido sendo digitado e utilizá-lo posteriormente. Neste caso pode ter um conflito na base de dados de controle de acesso, pois duas pessoas podem acessar utilizando o mesmo código, não sendo possível saber realmente se a pessoa que acessou tem o acesso permitido. Ressalta-se então a importância de combinar pelo menos dois tipos de verificação de acesso para obter um sistema minimamente seguro (NORMAN, 2007). Outras tecnologias para combinação com as senhas serão descritas a seguir.

2.2 CARTÕES MAGNÉTICOS

Os cartões com tarja magnética ainda são amplamente utilizados em várias aplicações principalmente devido ao seu baixo custo e pela facilidade que apresentam para leitura e escrita. É uma tecnologia que surgiu em meados dos anos 70 e deu início a uma nova era na forma de venda para o varejo, acelerando o processo e dando maior controle para os empresários sobre transações financeiras e estoques (MOURA, 2006). A Figura 4 ilustra um modelo de cartão magnético convencional.

Figura 4 - Cartão de banda magnética comum

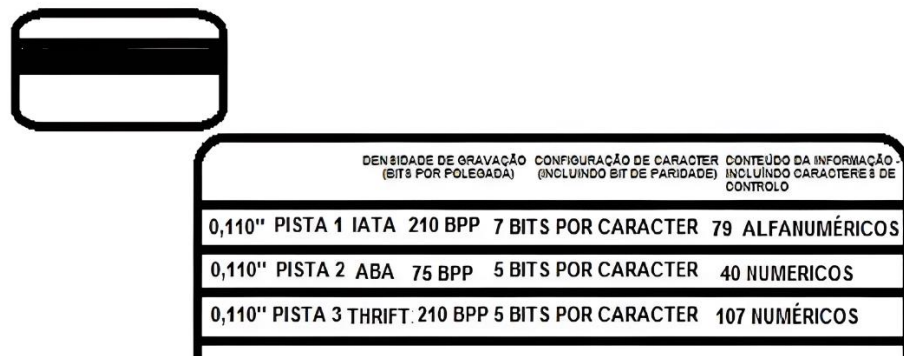


Fonte: MAYNES e MARKANTONAKIS, 2017.

Para entendimento do processo de gravação e leitura em mídias magnéticas, é necessário recorrer ao ferromagnetismo, mecanismo responsável por transformar certos materiais em ímãs permanentes. Um pedaço de ferro, por exemplo, possui em seu interior uma série de momentos magnéticos distribuídos ao longo de seu volume, cada um destes por ser representado por um pequeno ímã. Quando se aplica um campo magnético sobre um material ferromagnético, estes ímãs tendem a se alinhar com o campo, modificando assim sua configuração magnética. Dessa forma, é possível atribuir ao material um valor de magnetização, que é definido como o seu momento magnético por unidade de volume (ASTRATH, 2019).

Materiais ferromagnéticos são capazes de manter este novo estado magnético total ou parcialmente mesmo quando todo o campo magnético externo é removido, assim é possível codificar a informação na configuração magnética do material, os estados dos momentos magnéticos gravados geram um campo magnético nas proximidades do material, de forma que possa ser identificado e a informação armazenada lida. A banda magnética pode ser de dois tipos, de cor preta (chamadas de HiCo – “*High Coercivity*” ou Alta Coercividade), constituídas por óxido de ferro ou de cor castanha (chamadas de LoCo – “*Low Coercivity*” ou Baixa Coercividade), constituídas por ferrite de bário. A coercividade é medida em Oersteds (Oe), e traduz a dificuldade que a banda magnética apresenta na escrita da informação. Existe uma norma definida pela ISO, que determina a forma com que os dados devem ser armazenados na banda magnética dos cartões financeiros, a norma é a ISO 7813 e divide a banda em 3 pistas, como ilustrado na Figura 5.

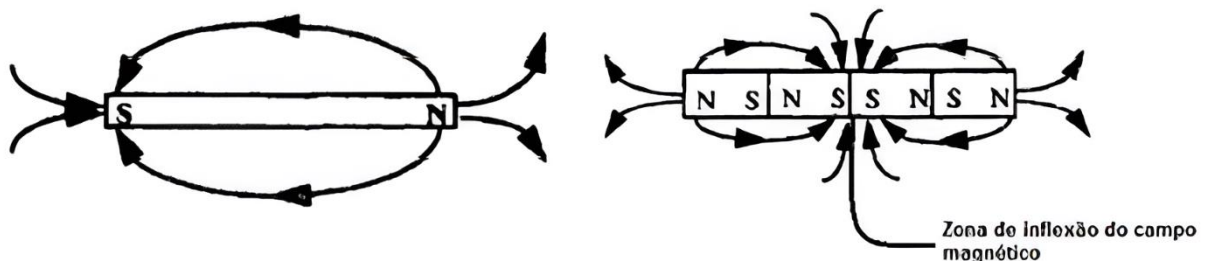
Figura 5 - Cartão magnético e respectivas pistas



Fonte: KUMAR, 2019.

Cada pista da banda magnética é constituída por elementos com capacidade de magnetização e permanência da condição de polaridade que lhe foi atribuída, de forma que pólos opostos se atraem e pólos iguais repelem-se. Se partículas adjacentes forem polarizadas com pólos iguais, ocorre uma zona de inflexão de polos, que são zonas de maior concentração de campo magnético. A Figura 6 ilustra a ocorrência da zona de inflexão.

Figura 6 - Zona de inflexão



Fonte: KUMAR, 2019.

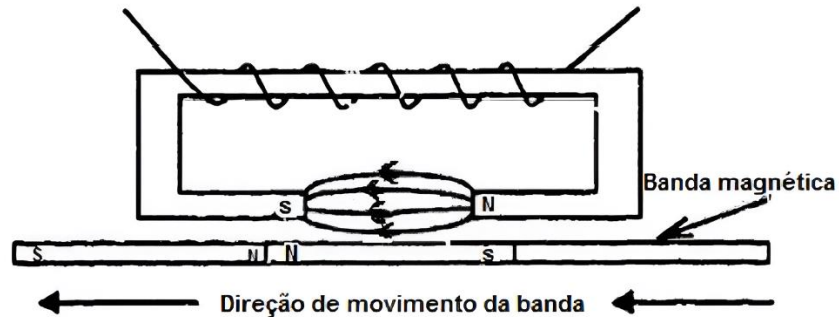
Dessa forma, determina-se um método binário para modelar os dados, de forma que as zonas de inversão representam o bit 1 e as regiões normais o bit 0 (KUMAR, 2019).

2.2.1 Gravadores de cartões magnéticos

Para gravar um cartão magnético, utiliza-se um circuito magnético semelhante ao descrito na figura abaixo, apresentando uma determinada polaridade de campo magnético e a banda magnética passando por baixo do entreferro, que polariza as

partículas de acordo com a informação que se pretende, caso seja necessário gravar o bit 1, magnetiza-se duas partículas adjacentes com a mesma polaridade, criando uma zona de inflexão. A Figura 7 representa um circuito gravador e o movimento do cartão no momento da gravação.

Figura 7 - Polarização da banda magnética



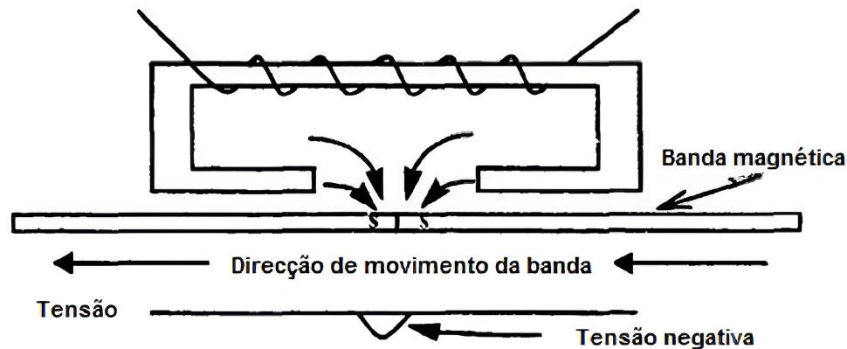
Fonte: KUMAR, 2019.

Importante ressaltar que é possível inverter o sentido do campo magnético invertendo a corrente na bobina ou invertendo a direção de deslocamento da banda, conforme ilustrado.

2.2.2 Leitores de cartões magnéticos

Para realizar a leitura é necessário identificar as zonas de inflexão do fluxo, neste caso, o circuito magnético não é percorrido por uma corrente. Ao passar a banda magnética pelo entreferro, é possível notar fluxos gerados no circuito magnético, devido as zonas de inflexão, que apresentam maior intensidade. Consequentemente induz-se uma corrente na bobina e através da leitura dos pulsos de tensão, é possível identificar e decodificar a informação gravada na banda magnética, o processo é ilustrado na Figura 8.

Figura 8 - Leitura na banda magnética



Fonte: KUMAR, 2019.

É importante ressaltar que a leitura só é possível devido ao fluxo magnético variável que acontece durante o movimento do cartão, sem esse movimento não há corrente induzida e seria impossível medir alguma tensão nos terminais da bobina.

2.3 CARTÕES INTELIGENTES

Cartões inteligentes são amplamente utilizados para validação de acesso devido a seu custo e praticidade, geralmente são embarcados com microprocessador, memória, circuito de comunicação e uma bateria, além de contatos centrais que possibilitam a comunicação do microprocessador com uma leitora. Estes também permitem as funções de proximidade e criptografia, tornando a tecnologia aplicável em diversas frentes, uma das aplicações mais conhecidas é seu uso em transações financeiras.

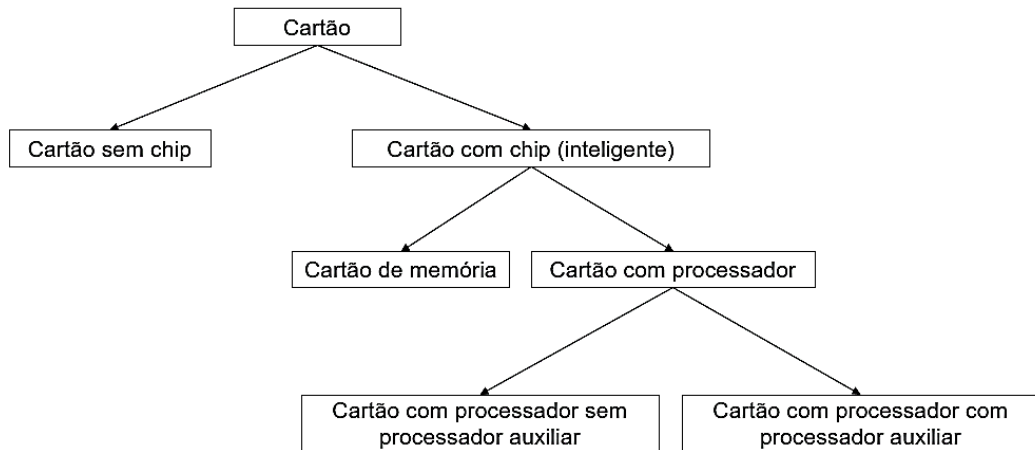
Existem alguns critérios para classificar os cartões inteligentes do ponto de vista tecnológico, como por exemplo: Possuir um identificador único, ser capaz de realizar uma transação eletrônica automatizada, ter como foco o adicional de segurança, oferecer alta resistência para ser clonado ou falsificado, ser capaz de armazenar dados de forma segura e por fim, ser capaz de executar algoritmos versáteis e funções de segurança (MAYNES E KONSTANTINOS, 2017).

2.3.1 Cartões com chip

As aplicações com chip, devido à sua capacidade e recursos, são classificadas como cartões inteligentes, tendo como elemento de distinção a aplicação de seu chip: este pode ser um cartão de memória ou um microcontrolador, chamados de cartões

processadores. Podem ser divididos entre cartões com ou sem processadores auxiliares, capazes de executar algoritmos de criptografia mais modernos, como por exemplo RSA ou ECC. A divisão descrita está diagramada na Figura 9.

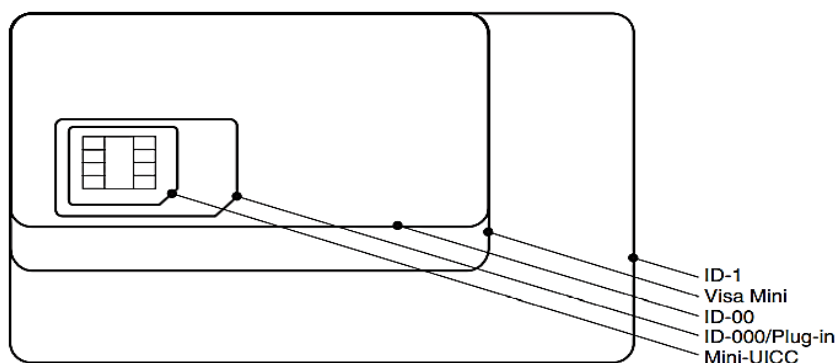
Figura 9 – Classificação dos cartões



Fonte: RANKL, 2007.

Para algumas aplicações a banda magnética é suficiente e não há a necessidade do chip no cartão, para aplicações de *chips*, pode-se ter apenas uma memória embarcada ou então um processador, que pode ou não contar com um auxiliar, dependendo da necessidade de criptografias mais avançadas na aplicação (RANKL, 2007).

Para que todos os cartões produzidos possam ser lidos pelas leitoras, definiu-se uma norma padrão para os tamanhos, materiais, terminais, aplicações entre outros aspectos que devem ser levados em consideração durante o processo de fabricação de um cartão para as mais diversas áreas. A norma em questão é a ISO 7816, o padrão é ilustrado na Figura 10.

Figura 10 - Padrão para tamanhos de cartões

Fonte: RANKL, 2007.

Os tamanhos Visa Mini são amplamente utilizados por bancos e empresas para aplicações em sistemas de pagamento, já as versões menores, ID-000/Plug-in e Mini-UICC são muito comuns nos setores de telecomunicações, como por exemplo para habilitação de rede de internet em aparelhos celulares. Para contextualização dos tamanhos, a Tabela 1 indica a altura e comprimento de cada modelo padrão.

Tabela 1 – Tamanhos mais comuns e suas respectivas aplicações

Modelo	Largura (mm)	Altura (mm)	Aplicação
ID-1	85,6	54	Formato padrão mais conhecido
Visa mini	65,6	40	Sistemas de pagamento.
Plug-in, ID-000	25	15	Telecomunicações.
Mini-UICC	15	12	Telecomunicações.

Fonte: RANKL, 2007.

Conforme abordado, por motivos de compatibilidade, as fabricantes devem seguir o padrão definido pela norma ISO 7816 para posicionamento dos contatos do chip, de acordo com a figura e descrição da Figura 11:

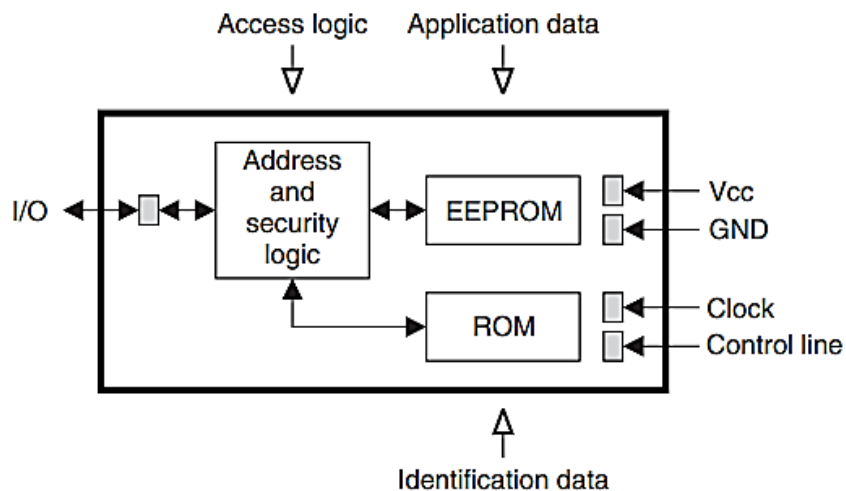
Figura 11 - Pinagem definida pela norma ISO7816

Fonte: BENADJILA et al, 2019.

Onde C1 – VCC é o terminal de alimentação, C2 – RST o reset do chip, C3 – CLK o terminal de clock, C4 está reservado para aplicações futuras C5 – GND é o terminal de aterramento, C6 é Bit reservado para que o fabricante adicione aplicações diferenciais/opcionais, C7 é o terminal de entrada/saída de dados (barramento bidirecional) e C8 também está reservado para aplicações futuras.

Embora a tecnologia de cartões inteligentes com microcontroladores tenha avançado bastante, ainda se utiliza bastante os cartões embarcados apenas com capacidade de armazenamento, com circuitos lógicos fixos construídos pelos fabricantes de semicondutores. A Figura 12 ilustra o funcionamento dos grupos desse tipo de chip.

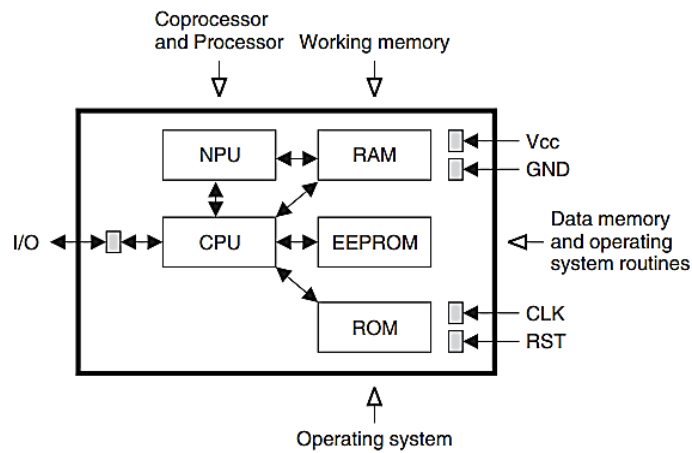
Figura 12 - Diagrama de blocos da interface de contatos de um chip de memória



Fonte: RANKL, 2007.

A memória ROM armazena dados sobre o tipo do chip, já a EEPROM prove a área de armazenamento para um número único de identificação exclusivo do chip e dados armazenados na área de leitura e escrita. A lógica de segurança varia de acordo com o chip, monitorando o acesso aos dados. Um exemplo comum de validação é exigir um PIN correto antes de conceder acesso de escrita no chip. Microcontroladores para cartões tem muito mais funções que os cartões de memória simples, como identificado na Figura 13.

Figura 13 - Diagrama de bloco da interface de contato de um chip com microcontrolador



Fonte: RANKL, 2007.

A CPU é uma unidade de controle livremente programável que executa as instruções da máquina do sistema operacional, que está localizada na ROM. A CPU é auxiliada por um coprocessador numérico (NPU) para cálculos numéricos, particularmente aqueles que lidam com criptografia. Esses processadores especiais combinam desempenho extremamente alto com baixo consumo de energia.

As extensões do sistema operacional, aplicativos reais e os dados associados são armazenados na EEPROM. Assim como em um computador pessoal, a RAM serve como memória de trabalho para armazenar dados durante a operação. O principal tipo de memória não volátil utilizadas nos controladores de cartões inteligentes são as ROM, caso o dado na memória que está operando precise ser utilizado, neste caso, utiliza-se a EEPROM ou a Flash, que também é muito utilizada por ter dimensões menores e também atender a demanda do chip (RANKL, 2007).

2.3.2 Sistemas RFID

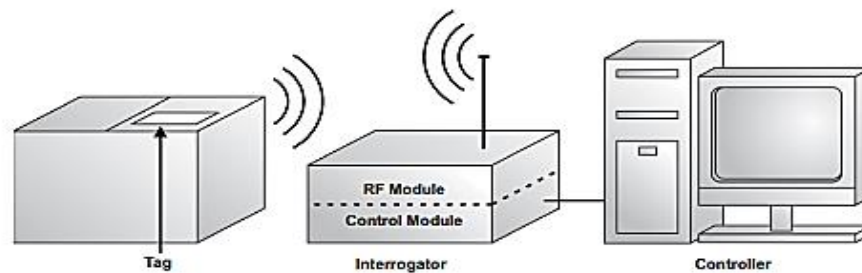
O RFID é uma tecnologia que permite a comunicação sem fio entre um item receptor e um sistema de validação por meio de rádio frequência. Um sistema de RFID possui 3 componentes básicos para funcionamento, são eles:

1. Uma *tag*, que é composta por um chip semicondutor, uma antena receptora e muitas vezes uma pequena bateria.

2. Um dispositivo de leitura e gravação (conhecido como leitor), composto por uma antena, um módulo eletrônico de radiofrequência e um módulo eletrônico de controle.
3. Um controlador, chamado de *host*, que pode ser um computador ou uma estação de trabalho responsável por executar a base de dados e o *software* e controle do sistema RFID.

A *tag* e o dispositivo de leitura comunicam-se por meio de ondas de rádio, quando a *tag* entra na zona de alcance do leitor, este faz com que a ela transmita de volta a informação que está armazenada. Quando o leitor recebe de volta a mensagem, é realizada a validação por meio do controlador do sistema, que pode utilizar a mesma para uma variedade de aplicações. Os componentes principais de um sistema RFID descritos acima estão ilustrados na Figura 14.

Figura 14 - Diagrama de blocos básico de um sistema RFID



Fonte: HUNT et al, 2007.

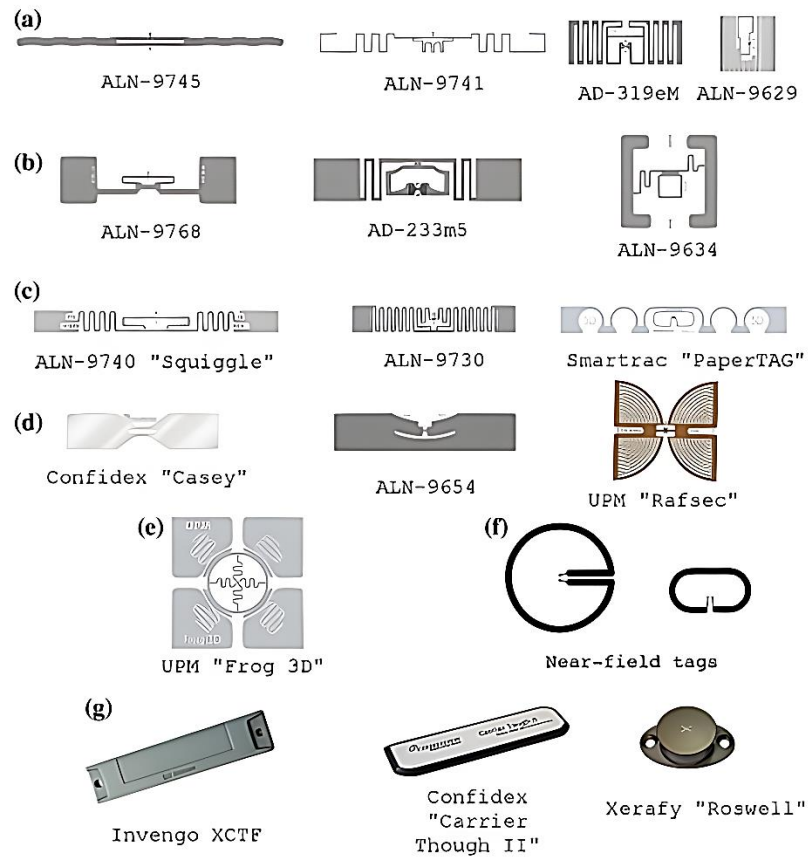
O sistema RFID pode ser composto por diversos leitores dispostos por uma área na qual a validação de acesso é necessária em diversos pontos, como por exemplo: uma central de concentração de estoque, uma linha de produção, entre outros. Suportando o uso de várias *tags* ao mesmo tempo em diversos pontos, é possível desde que todos os leitores estejam logicamente conectados a um mesmo sistema controlador (HUNT, 2007).

2.3.2.1 Tags RFID

A função básica das *tags* é armazenar dados necessários e transmiti-los para o leitor, como foi mencionado, ela é composta por um chip e uma antena. Geralmente os *chips* possuem uma memória na qual os dados podem ser armazenados, lidos e

muitas vezes também gravados. As *tags* podem ser classificadas como ativas ou passivas, a característica determinante é a presença ou não de bateria (HUNT, 2007). A Figura 15 ilustra a variedade de *tags* disponíveis no mercado.

Figura 15 - Variedade de *tags* RFID



Fonte: ZUFFANELLI, 2018.

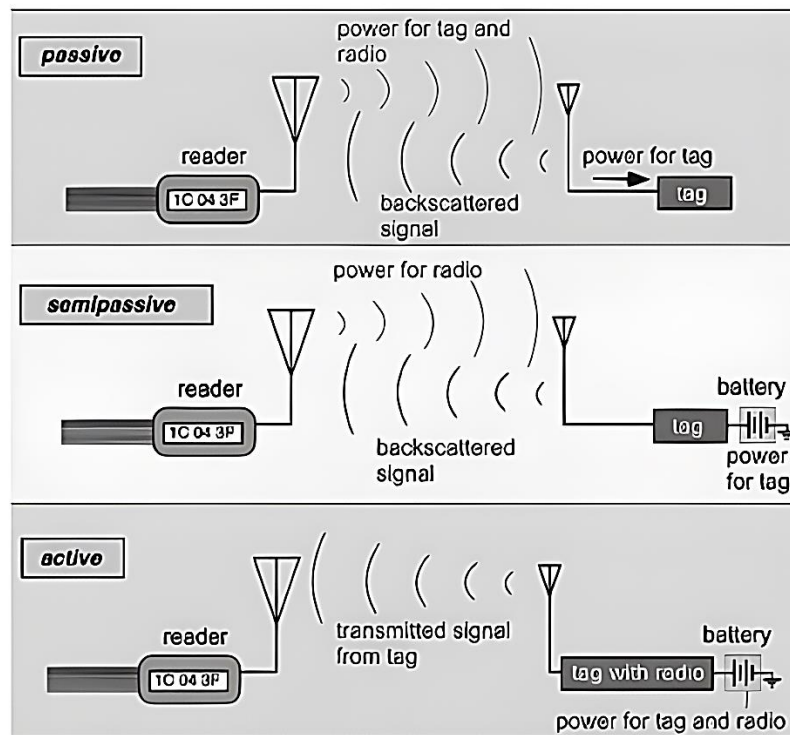
São consideradas *tags* ativas aquelas que possuem uma fonte de alimentação própria, neste caso, quando a *tag* precisa transmitir dados de volta para o leitor, ela utiliza essa fonte de energia para transmissão. Por esse motivo, as *tags* ativas são capazes de se comunicar com leitores menos potentes e transmitir informações por mais tempo e por distâncias muito maiores. Outro ponto importante é que as baterias das *tags* ativas têm uma duração satisfatória, variando entre 2 e 7 anos. Por outro lado, as *tags* ativas são maiores e mais caras para produzir do que as *tags* passivas, que serão descritas a seguir.

As *tags* passivas não possuem fonte de alimentação acoplada, em vez disso elas derivam a potência do sinal enviado pelo leitor (por meio de uma antena em espiral, que gera um campo magnético com a energia enviada da leitora e alimenta seus

circuitos), evidentemente com um sinal de retorno muito menos potente. Por conta disso, elas são bem mais baratas que as ativas e possuem um alcance efetivo muito menor, muitas vezes abaixo de 60cm, exigindo então um leitor muito mais poderoso para captação do sinal.

Existe também um classe de *tags* passivas alimentadas por uma pequena bateria, porém apenas para alimentação dos componentes eletrônicos embarcados, e não para auxiliar na transmissão do sinal, um exemplo dessa aplicação é quando há a necessidade de monitorar a temperatura de uma mercadoria no estoque por meio da *tag*, neste caso, o sensor de temperatura embarcado precisa da alimentação de uma bateria para funcionamento (HUNT, 2007). A Figura 16 mostra a diferença de montagem entre os dois tipos discutidos.

Figura 16 – Tags RFID passivas, semi passivas e ativas



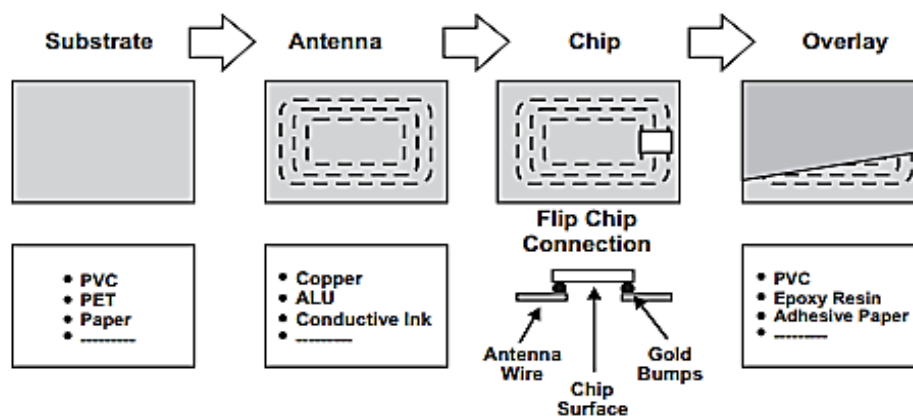
Fonte: ZUFFANELLI, 2018.

Conforme ilustrado, as *tags* passivas recebem e derivam parte da potência do sinal do leitor para alimentar seu circuito e assim retornar a informação codificada de volta. Na segunda linha estão as semi-passivas, que também realizam a derivação da potência do sinal recebido para operar, porém contam com uma bateria para alimentação de circuitos específicos. Na última faixa por fim estão as *tags* ativas, que são

equipadas com uma fonte de alimentação própria e provê a energia necessária para que seu circuito se comunique com a leitora (ZUFFANELLI, 2018).

Na Figura 17 observa-se a composição de uma *tag* RFID, construída sobre um substrato de PVC, PET ou papel, a antena de cobre, alumínio ou tinta condutora sobrepondo a primeira camada, um chip é conectado fisicamente à antena por meio de contatos de ouro e por fim, é feita a sobreposição do circuito com PVC, resina epoxy ou papel adesivo.

Figura 17 - Construção de uma *tag* RFID



Fonte: HUNT et al, 2007.

Outro fator de diferenciação das *tags* é seu tipo de memória, que pode ser de somente leitura (RO) ou de leitura e escrita (RW). As memórias de somente leitura são programadas apenas uma vez pelo fabricante e a partir daí não podem mais sofrer alterações, sendo assim análoga a um CD-ROM, que não pode sofrer alterações de dados após a gravação. Essas *tags* geralmente são utilizadas quando deseja-se armazenar uma quantidade pequena de dados que sempre serão estáticos, como por exemplo um número de série de uma peça ou uma breve descrição de um produto, são facilmente integradas com sistemas de código de barras. Já as *tags* RW (classificadas como inteligentes), têm como característica a capacidade de armazenar uma grande quantidade de dados de forma que sua memória endereçável permite que estes sejam facilmente alterados, permitindo que os dados da *tag* RW sejam apagados e reescritos milhares de vezes, de acordo com a necessidade do sistema de controle, possuindo infinitas aplicações em todos os tipos de indústrias e sistemas (HUNT, 2007).

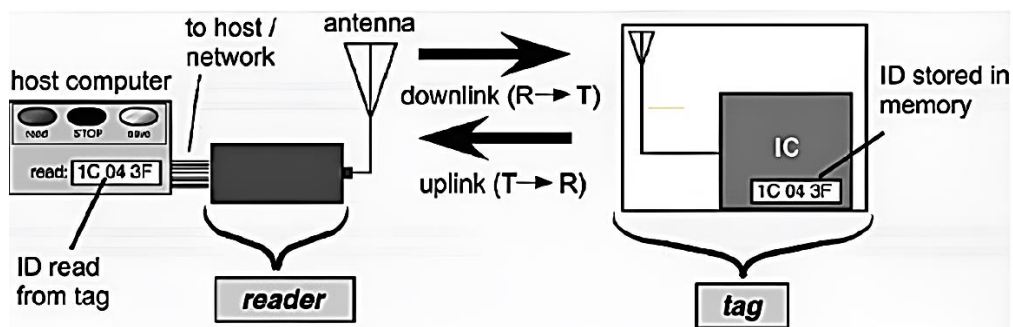
2.3.2.2 Leitores e controladores RFID

O leitor RFID atua como uma ponte entre a *tag* e o controlador, para executar esta função possui algumas funções básicas, são elas:

- Ler os dados contidos em uma *tag* RFID;
- Escrever dados em *tags* inteligentes;
- Retransmitir dados de e para o controlador;
- Alimentar as *tags* passivas.

Na Figura 18 está descrito o esquema de um Leitor (*Reader*) interagindo com uma *tag*, recebendo suas informações e comunicando de volta ao controlador.

Figura 18 - Sistema RFID com leitor à esquerda

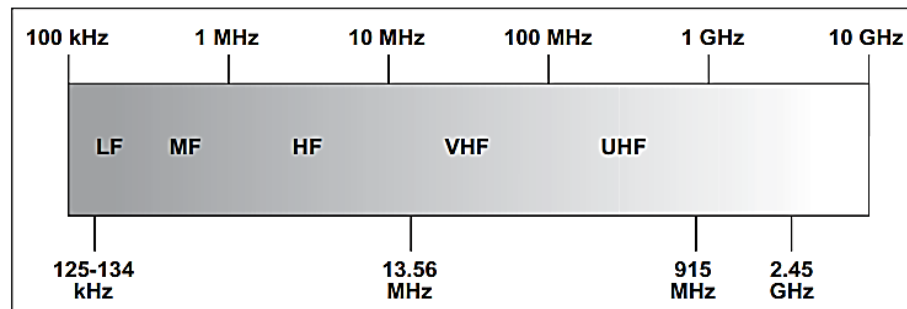


Fonte: ZUFFANELLI, 2018.

Leitores são compostos por uma antena, um módulo eletrônico de radiofrequência para transmissão/recepção de sinais da *tag* via antena e um módulo eletrônico de controle, responsável pela comunicação com o controlador do sistema. Os controladores são responsáveis por conectar vários integradores em rede e processar as informações de forma centralizada. Normalmente é um computador ou um servidor executando um *software* e um banco de dados para fazer as validações lógicas referentes ao sistema de controle de acesso RFID (HUNT D, 2007).

2.3.2.3 Escolha da frequência de operação

Um fator muito importante para a operação de um sistema RFID é sua frequência. Assim como os sinais de transmissão de TV, os sistemas de RFID podem operar em diferentes bandas de comunicação, como indicado na Figura 19:

Figura 19 - Espectro de radiofrequência

Fonte: HUNT et al, 2007.

Para RFID tanto altos valores de radiofrequência quanto baixos são utilizados, são classificados da seguinte forma.

Bandas RFID de baixa frequência:

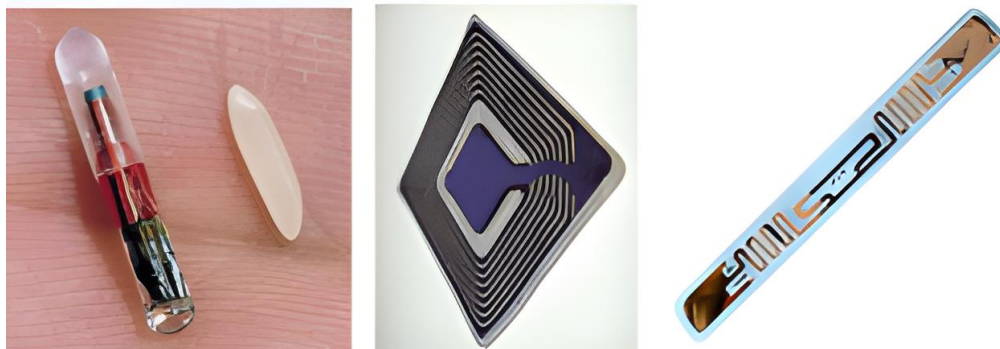
- Baixa frequência: 125 – 134 kHz
- Alta frequência: 13.56 MHz

Bandas RFID de alta frequência:

- Frequência ultra-alta: 860 – 960 MHz
- Microondas: acima de 2.5 GHz

Nas bandas de frequência mais baixas, os raios de leitura de *tags* passivas são menores que um metro, devido principalmente ao baixo ganho da antena. Em baixas frequências, os comprimentos de onda são muito altos, da ordem de vários quilômetros às vezes, muito maiores do que as dimensões das antenas integradas em etiquetas RFID. Como o ganho da antena é diretamente proporcional ao tamanho da antena em relação ao comprimento de onda, o ganho da antena nessas frequências é muito baixo. A Figura 20 ilustra as *tags* utilizadas para diferentes frequências

Figura 20 - Tags RFID passivas para frequências baixas, altas e ultra altas (da esquerda para direita)



Fonte: ZUFFANELLI, 2018.

Em frequências mais altas, o alcance de leitura normalmente aumenta, especialmente onde etiquetas ativas são usadas. No entanto, as bandas de alta frequência representam alguns problemas de saúde e preocupações para os seres humanos, a maioria dos órgãos reguladores, define limites de energia em sistemas UHF e micro-ondas, isso reduziu o alcance de leitura desses sistemas de alta frequência de 3 a 10 metros em média no caso de etiquetas passivas (HUNT, 2007).

2.4 VALIDAÇÃO POR BIOMETRIA

A última tecnologia de controle de acesso que será descrita neste trabalho é a biometria, definida como a validação de uma ou mais características físicas ou pessoais de um indivíduo, como por exemplo: Impressões digitais, geometria das mãos, voz, escrita e vasos sanguíneos retinais são amplamente utilizados como validação de acesso (PURPURA, 2011).

Vários fatores contribuem para a popularidade da tecnologia de impressão digital em relação a outras biometrias: ela é reconhecida como uma representação legal da assinatura de uma pessoa e sua confiabilidade como padrão de impressão digital não muda ao longo da vida. Outro fator importantíssimo é o baixo custo de hardware necessário e a alta portabilidade — são necessários apenas 120 Byte a 180 Byte (~1 kbit) de memória para armazenar um conjunto de recursos exclusivos (minúcias) que representam uma impressão digital (HSU, 2016).

A validação biométrica é a mais segura que pode ser utilizada como ferramenta de autenticação, uma vez que não pode ser emprestada, esquecida ou nem mesmo roubada. A autenticação biométrica é única e individual, uma vez que as impressões

digitais são uma análise dos padrões encontrados nas pontas dos dedos de um indivíduo (LIU e SILVERMAN, 2001).

Existem dois métodos de análise de biometria por meio da impressão digital: o primeiro deles faz o reconhecimento espirais, loops e inclinações da impressão digital referenciada, que é armazenada em uma representação digitalizada da imagem e comparada com a impressão digital da pessoa que está realizando a tentativa de entrada. Já a segunda alternativa é realizar uma comparação das terminações, pontos de ramificações de cristas e vales da impressão digital que está sendo inserida com os mesmos parâmetros da armazenada na base de dados (PURPURA, 2011).

2.4.1 impressões digitais

Nesta seção serão exploradas as tecnologias de leitura de impressões digitais, na qual são explicados alguns métodos existentes para leitura e obtenção de dados. A primeira descrita conta com o apoio de leitores ópticos. Com sensores ópticos, o dedo é colocado ou empurrado em uma placa e iluminado por uma fonte de luz LED (KEUNING, 2000).

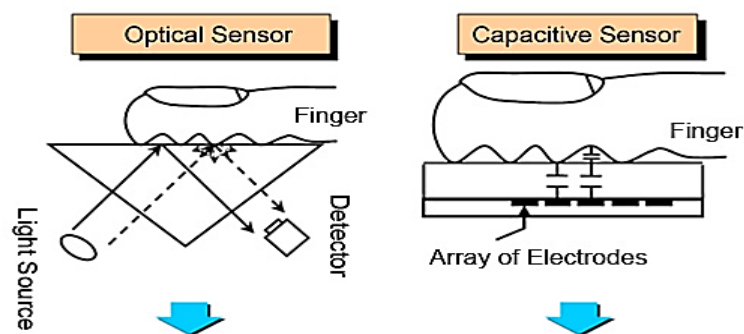
- **Leitura por sensores ópticos** – Através de um prisma e um sistema de lentes, a imagem é projetada em uma câmera. Pode ser uma câmera do tipo CCD ou, seu sucessor moderno, uma câmera CMOS. Usando técnicas de captura de frames, a imagem é armazenada em uma base de dados e fica disponível para leitura e processamento no sistema desejado.
- **Sensores ultrassônicos** – As técnicas ultrassônicas foram descobertas quando se percebeu que havia uma diferença na impedância acústica da pele (as cristas em uma impressão digital) e ar (nos vales de uma impressão digital). Os sensores utilizados nestes sistemas não são novos, eles já estavam sendo implantados há muitos anos no mundo médico para realização de exames do tipo “eco”. A faixa de frequência que esses sensores usam, é de 20 kHz a vários Giga-hertz. As frequências superiores são necessárias para poder fazer uma digitalização da impressão digital com uma resolução de cerca de 500 pontos por polegada (DPI). Esta resolução é necessária para situações em que é necessário obter detalhes minuciosos da impressão digital.
- **Sensores de campo elétrico** – Por meio de um sensor com tamanho semelhante a um carimbo, é criado um campo elétrico em que sua variação quando

o dedo é pressionado, resultado das cristas (na pele) e vales (no ar) da impressão digital, resulta em uma matriz de *pixels*.

- **Sensores capacitivos** – Semelhantes em tamanho com os sensores de campo elétrico, os sensores capacitivos também definem uma matriz de *pixels* quando o mesmo é pressionado por uma impressão digital, isso é possível por conta da variação de capacitância entre os vales e cristas da impressão digital. Esse método é possível devido à diferença de capacitância medida entre ar – sensor e pele – sensor.
- **Sensores de temperatura** – Sensores que medem a temperatura de uma impressão digital podem ser menores do que o tamanho de um dedo. Embora a largura ou a altura devam exceder o tamanho do dedo, a outra dimensão pode ser bastante pequena, uma vez que uma varredura de temperatura pode ser obtida passando o dedo sobre o sensor. O sensor contém uma matriz de *pixels* de medição de temperatura que faz uma distinção entre a temperatura da pele e a temperatura do ar.

Um modelo de leitura de impressão digital por meio de um sensor óptico (à esquerda) e capacitivo (à direita) estão representados na Figura 21.

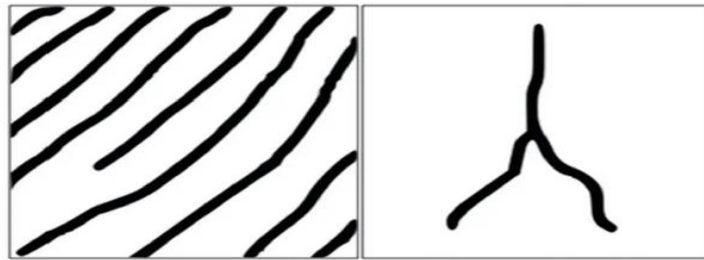
Figura 21 - Leitura por meio do sensor óptico e capacitivo



Fonte: HSU, 2016.

Em todos os casos, uma vez que os dados da digital são processados, chega-se a pontos chaves, identificados como bifurcações e terminações de cume das digitais, gerando pontos de identificação únicos para cada leitura, conforme a Figura 22.

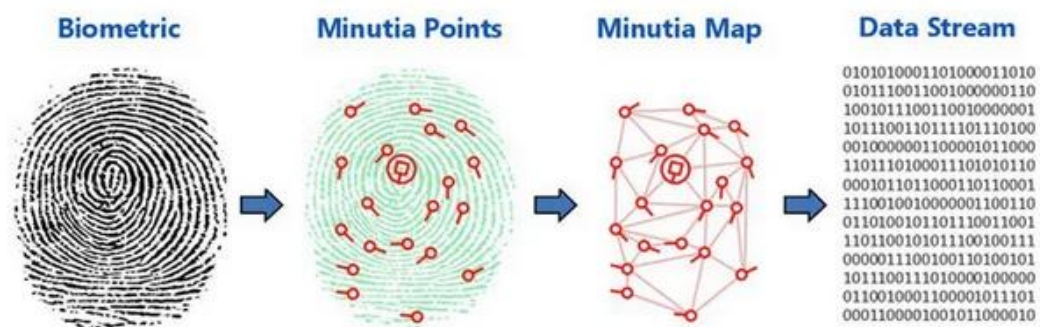
Figura 22 - Terminações de cume (à esquerda) e bifurcações (à direita)



Fonte: HSU, 2016.

Um mapa desses pontos chave são armazenados em uma base de dados, gerando uma representação da impressão digital, na Figura 23 está um exemplo do processo de tratamento dos pontos até o armazenamento:

Figura 23 - Processo de armazenamento da impressão digital

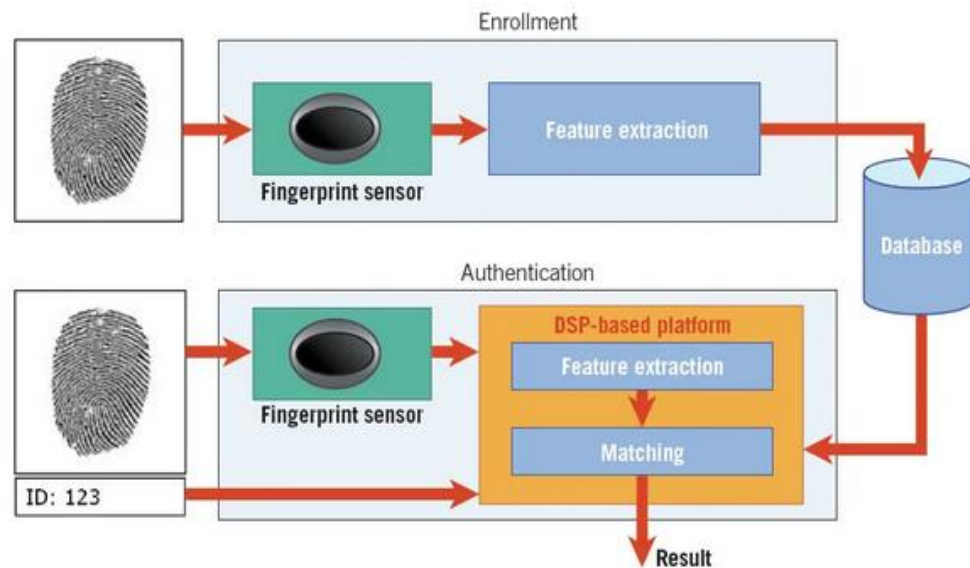


Fonte: HSU, 2016.

De acordo com o Sistema de Classificação de Henry, apenas 13 pontos chave são necessários para identificar uma impressão digital (única). Transformada em formato digital, isso é equivalente a aproximadamente de 120 a 180 bytes de dados, tornando-a um recurso de validação muito leve e versátil (HSU, 2016).

Na Figura 24 verifica-se o procedimento necessário padrão para implementação do sistema de autenticação biométrica por meio da impressão digital, inicialmente passando pelo processo de cadastro da impressão em um banco de dados e posteriormente a busca e validação do dado obtido para validação antes da confirmação do acesso.

Figura 24 - Diagrama de blocos do processo de validação de uma impressão digital



Fonte: HSU, 2016.

Após a captura da impressão digital, é necessário cadastrar o modelo biométrico em uma central de armazenamento de dados, de forma que possa ser utilizada em futuras validações de acesso. Uma vez armazenada, quando inserida novamente no sistema de controle de acesso, é realizado seu processamento e comparação com todos os modelos já armazenados pelo sistema e retornando enfim a liberação do acesso, caso encontrada a equivalência na base de dados. Devido ao custo relativamente baixo das leitoras de impressões digitais, seu tamanho pequeno e a facilidade de integração com sistemas eletrônicos, a validação por impressões digitais são amplamente utilizadas e são uma ótima opção para combinação com sistemas de senha ou cartões inteligentes para compor um sistema de dupla autenticação (HSU, 2016).

2.4.2 Geometria das mãos

Outro recurso de validação por meio de é a captura e análise de parâmetros geométricos das mãos para validação biométrica, parâmetros como o comprimento dos dedos, largura, espessura, curvatura e localização relativa são capazes de distinguir qualquer ser humano de outro. A técnica é considerada suficiente para sistemas que demandam segurança em nível médio ainda apresenta várias vantagens com relação a outros métodos (VARCHOL e LEVICKÝ, 2007), como por exemplo:

- Custo não tão elevado, uma vez que demanda apenas de uma plataforma de apoio e um leitor ou câmera de média resolução;

- Utiliza algoritmos que demandam baixo processamento computacional, o que permite alta velocidade do sistema;
- A amostra armazenada é pequena, a ordem de 352 a 1209 *bytes*, o que reduz a demanda por armazenamento;
- Muito prático para os usuários, resultando em uma boa aceitação.

A disponibilidade de processadores de baixo custo e recursos de eletrônica que atendem a demanda do sistema disponível, fez com que fosse possível produzir leitores de leitura de mãos a um custo acessível no mercado de dispositivos e sistemas de controle de acesso. Além disso, variáveis fora de controle como tempo seco ou problemas na pele, como ressecamento, por exemplo, não interferem na eficácia do método. Por outro lado, o mecanismo pode apresentar dificuldades para ler a mão de pessoas que utilizam anéis grandes, apresentam inchaço ou alguma deficiência, como por exemplo a falta de algum dedo.

Assim como os outros métodos de autenticação biométrica, a validação da geometria das mãos passa inicialmente pelo processo de cadastro da amostra em uma base de dados e posteriormente uma validação comparativa. Para cadastrar uma amostra são necessárias várias capturas da mão em uma determinada posição (geralmente orientada por meio de uma plataforma com indicações), uma vez obtidas as imagens, é realizado o processamento para extração dos parâmetros utilizados para validação, neste momento é obtida a amostra final, chamada de *template*. No método apresentado, apenas uma imagem é capturada no momento da validação, esta é comparada aos *templates* armazenados na base de dados, o resultado retornado pelo sistema é “autorizado” ou “não autorizado” (VARCHOL e LEVICKÝ, 2007). Na Figura 25 está representado o primeiro procedimento para extração de uma amostra da geometria da palma da mão.

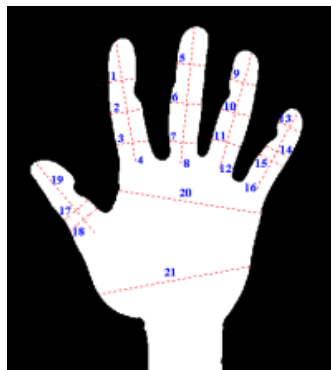
Figura 25 - Amostra capturada por um scanner de mão



Fonte: VARCHOL e LEVICKÝ, 2007.

Uma vez que uma amostra semelhante à ilustrada na Figura 25 é obtida, realiza-se o pré-processamento, a fim de obter os parâmetros desejados. O primeiro passo é converter a imagem obtida em binários, de forma que 0 indica *pixels* mais escuros que um valor pré-determinado e 1 para os demais. O resultado do processamento é a Figura 26, já trata e com os pontos necessários para determinação dos parâmetros que serão utilizados para reconhecimento no sistema já identificados (VARCHOL e LEVICKÝ, 2007).

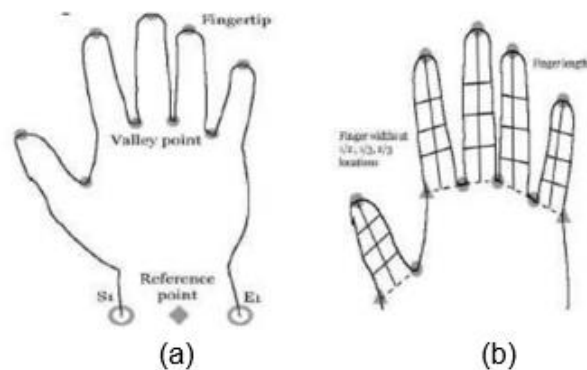
Figura 26 – Amostra de mão com os pontos definidos para cálculo dos parâmetros



Fonte: VARCHOL e LEVICKÝ, 2007.

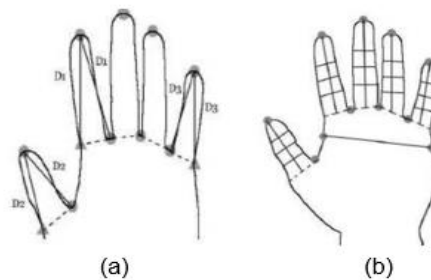
Uma metodologia semelhante será utilizada para descrever os próximos passos necessários para tratar a amostra obtida e obter os parâmetros mencionados. As Figuras 27 e 28 ilustram quais são os pontos de referência utilizados nas mãos e as distâncias que serão utilizadas como parâmetros de validação.

Figura 27 – (a) Referenciamento dos pontos da mão. (b) Pontos referência para altura e largura



Fonte: DUBEY et al, 2013.

Figura 28 - (a) Pontos utilizados para medir distâncias (b) Parâmetros finais indicados



Fonte: DUBEY et al, 2013.

Alguns métodos numéricos são abordados por ambos os trabalhos referenciados para atingir os valores das distâncias finais, porém ainda é necessário colocar à prova a confiabilidade do sistema, os resultados podem variar de acordo com o método numérico empregado, a qualidade do equipamento utilizado para obtenção e processamento das imagens, o posicionamento da mão no momento da captura e, conforme mencionado, as condições de inchaço das mãos.

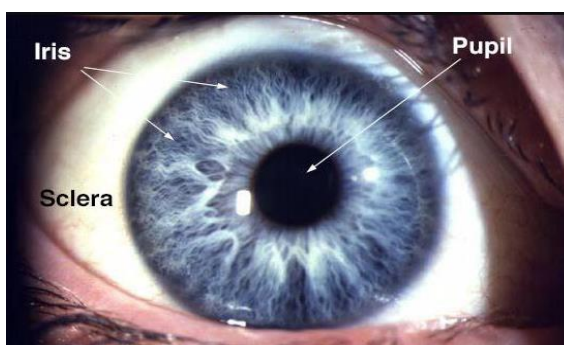
Para avaliar o desempenho dos sistemas de validação biométrica, os índices de avaliação de acurácia do sistema mais comum são o FRR (*False Rejection Rate*) e o FAR (*False Acceptance Rate*), o primeiro consiste no percentual de pessoas autorizadas têm o acesso invalidado pelo sistema e o segundo indica qual o percentual de pessoas não autorizadas têm acesso liberado (DUBEY, 2013).

Ambos os trabalhos analisados apresentam uma taxa de confiabilidade no sistema de 98% e avaliam que o método é válido como uma alternativa para sistemas que demandam uma segurança de nível médio e custo relativamente baixo. Uma alternativa amplamente utilizada e recomendável é utilizar, além da leitura biométrica, um controle de acesso com dupla autenticação por meio de senhas, cartões ou *tags*, conforme já foi discutido neste trabalho.

2.4.3 Reconhecimento da íris

A biometria baseada na leitura da íris utiliza como referência para validação biométrica os parâmetros encontrados nas cores do anel de tecido que envolve a pupila, sendo o método menos intrusivo disponível para validação biométrica realizada por meio do olho, utiliza um modelo de câmera bastante convencional e não exige que a leitora esteja muito próxima do usuário (LIU e SILVERMAN, 2001). A Figura 29 separa as partes do olho humano a fim de definir a região que será utilizada neste método.

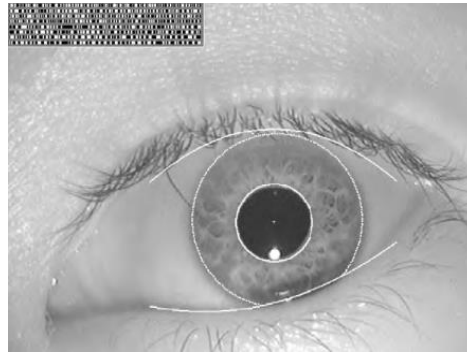
Figura 29 - Identificação da íris no olho humano



Fonte: ALAOUI et al, 2002.

A íris disponibiliza um alto nível de estabilidade e também de distinção, além de cada indivíduo possuir uma íris única, existindo diferenças até mesmo entre gêmeos ou entre os olhos direito e esquerdo da mesma pessoa além de praticamente não sofrer alterações durante a vida (ALAOUI, 2002). A íris começa a se formar a partir do terceiro mês de gestação e atinge sua estrutura completa já no oitavo mês. Mesmo tendo sua pigmentação alterada ao longo do tempo, ela mantém preservados uma série de parâmetros, como arqueadura dos ligamentos, sulcos, cumes, criptas, coroa, sardas e um colarinho em ziguezague, conforme ilustra a Figura 30 (BOVIK, 2009).

Figura 30 - Íris humana com parâmetros identificados, imagem monocromática a 35 cm de distância

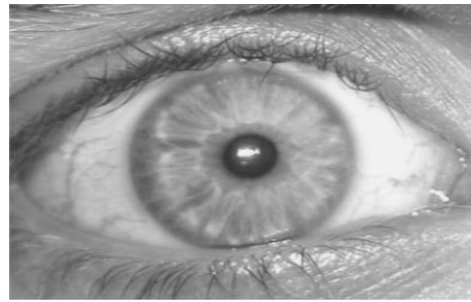


Fonte: BOVIK, 2009.

Também pode-se notar na Figura 30 os primeiros passos realizados para extração dos parâmetros da íris, inicialmente transforma-se a imagem do olho em escalas de cinza e trabalham para determinar qual região da imagem representa a íris que será analisada, uma vez que partes como pupila, cílios, esclera e pálpebras não serão utilizados na análise. Este processo é chamado de pré-processamento da imagem e logo em seguida executa-se a localização da íris (demarcações na Figura 30), também é realizada a normalização da imagem.

Como as imagens podem ser capturadas sob diferentes condições (como por exemplo, com dilatação da pupila, movimentação do olho e inclinação da cabeça), após a localização dos limites da íris, obtém-se uma representação retificada da imagem para que imagens diferentes possam ser processadas e comparadas da mesma maneira (isto é, as imagens passam a ser representadas da mesma forma, com o mesmo número de *pixels*). Esta retificação é obtida mapeando os valores dos *pixels* da imagem da íris originalmente em coordenadas cartesianas $I(x,y)$ para um sistema de coordenadas polares $I(r, \theta)$ (redefinido como $I(r, \theta)$). Este processo de retificação da forma circular da íris é também chamado de normalização, pois mapeia a imagem original da íris usando N_r raios e N_θ ângulos, formando uma imagem retificada de $(N_r \times N_\theta)$ *pixels*. O resultado do processo de normalização mencionado é ilustrado na Figura 31 e na Figura 32 (GUIMARÃES et al, 2008).

Figura 31 - Imagem pré-normalização



Fonte: GUIMARÃES et al, 2008.

Figura 32 - Imagem normalizada



Fonte: GUIMARÃES et al, 2008.

Uma vez obtida a representação normalizada, realizou-se a extração das características relevantes da imagem da íris, que são representadas através de um conjunto de dados. Nos trabalhos mencionados (BOVIK, 2009 e GUIMARÃES et al, 2008), a abordagem comum foi utilizar diferentes métodos de transformações de imagens, que geram novos espaços de representação e a partir deles, são obtidas as estatísticas que formam um vetor final de características da imagem, que é utilizado para diferenciação das imagens processadas. Nos trabalhos analisados, identificou-se o uso da função de Gabor bidimensional, ferramenta matemática utilizada para identificar padrões de frequência em uma região de uma determinada imagem e também da transformada de Haar, também utilizada para compreensão de dados e análise de sinais.

2.4.4 Biometria: considerações adicionais

Existem ainda outros tipos de validações biométricas em estudo e amplamente difundidas no mercado, como por exemplo: reconhecimento facial por câmeras, validação por meio da leitura da retina, validação por meio da análise da assinatura e também reconhecimento de voz. Todas estas, além das mencionadas acima, possuem características específicas que devem ser consideradas de forma particular para cada tipo de projeto, levando em consideração o nível de segurança, usuário final,

investimento desejado, entre outros (LIU e SILVERMAN, 2001). Alguns pontos relevantes para classificar as tecnologias de validação biométrica a fim de mostrar a comparação e facilitar essa análise estão definidos na Tabela 2:

Tabela 2 - Comparação de métodos de biometria

Característica	Digitais	Geometria das mãos	Retina	Iris	Face	Assinatura	Voz
Praticidade	Alta	Alta	Baixo	Média	Média	Alta	Alta
Risco	*	Cortes e idade	Óculos	Baixa iluminação	**	Mudança na assinatura	***
Acurácia	Média	Alta	Muito alta	Muito alta	Alta	Alta	Alta
Aceitação	Média	Média	Média	Média	Média	Muito alta	Alta
Segurança	Alto	Médio	Alto	Muito alto	Médio	Médio	Médio
Estabilidade	Alta	Média	Alta	Alta	Média	Média	Média

* Ressecamento, higienização e idade.

** Iluminação, idade, óculos e cabelo.

*** Barulho, clima e saúde.

Fonte: LIU e SILVERMAN, 2001.

De acordo com a Tabela 2, conclui-se que embora alguns métodos apresentem maior acurácia, alguns fatores como aceitação dos usuários, praticidade e taxa de variação ao longo do tempo devem ser levados em consideração ao instalar um sistema de validação de acesso por meio da biometria. Outro fator importante é o custo da tecnologia, porém, as milhares de opções disponíveis no mercado nos mais diversos níveis de acurácia dificultam uma análise genérica. Cada projeto deve levar em consideração seus custos, usuários e demandas de segurança para definir qual a melhor ferramenta disponível.

3. SISTEMAS DE DETECÇÃO DE INTRUSÃO

Os dispositivos de detecção de intrusão são os responsáveis por informar imediatamente a central de controle caso identifique alguma ameaça na região protegida, para isto, são utilizadas algumas tecnologias que permitem com que estes dispositivos sejam capazes de reconhecer uma anormalidade ou alteração de estado, seja uma abertura indevida de portas e janelas ou até mesmo a presença de uma pessoa em uma área de acesso restrito. Além de prover confiabilidade ao sistema de segurança da área, as tecnologias de detecção de intrusão reduzem consideravelmente os custos, uma vez que o investimento em dispositivos eletrônicos é muito mais vantajoso a longo prazo do que a contratação de vários vigilantes durante todos os turnos, que além de um custo muito elevado, agregam ao sistema preocupações como falhas de atenção, coação, corrupção, sono, necessidade de treinamentos constantes, entre outros. NORMAN (2007) classificou os dispositivos de detecção em três classes:

- Detectores pontuais: chaves posicionadas em portas e janelas, sensores de quebra-vidro, interruptores de coação, etc.
- Detectores volumétricos: infravermelhos, micro-ondas, ultrassônicos, etc.
- Detectores lineares: sensores sísmicos, de pressão de capacitância, etc.

Algumas das tecnologias presentes nos detectores mencionados serão detalhadas a seguir.

3.1 SENSORES MAGNÉTICOS

São amplamente utilizados em sistemas de segurança principalmente devido ao baixo custo e também pela eficiência e facilidade de integração no sistema e instalação. É a melhor escolha para monitoramento de portas, janelas e portões, uma vez instalado, permite com que seja acompanhado em tempo real se uma porta foi aberta ou violada, emitindo um sinal imediato para uma central, que pode utilizar este estado para a análise que for conveniente, como contagem do período em que ficou

aberta, por exemplo. O sensor pode funcionar em dois estados, dependendo da finalidade, operando como NA, caso a condição anormal seja o fechamento do dispositivo ou NF, mais comum, utilizado quando deseja-se se saber se houve a abertura de uma janela, retirando o sensor da posição NF e acionando um alarme.

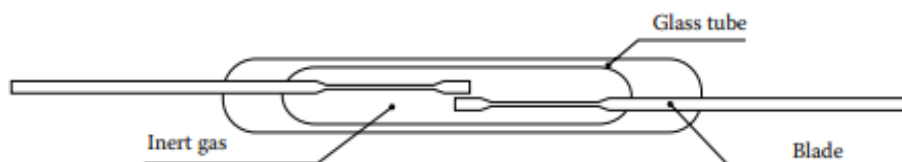
O componente eletrônico chave para a construção de um sensor magnético é o *reed switch*, como um par de lâminas em um material magnético, como liga 52 (Ni 52%, Fe Bal), selado em um tubo de vidro junto com um gás inerte, conforme descrito na figura a seguir. O campo magnético de uma bobina ou ímã induz um pólo norte ou sul em uma lâmina, e a força atrativa induzida resulta no contato dos dois metais, atuando como uma chave fechando o circuito nela conectado. Quando o campo magnético é removido, a elasticidade das palhetas de metal faz com que se afastem, resultando na abertura do circuito (SLADE, 2014).

São feitas ainda as seguintes considerações sobre o *reed switch*:

1. Como os contatos, juntamente com um gás inerte, são hermeticamente fechados em um tubo de vidro, a operação está livre da influência do ambiente externo.
2. Uma vez que o *reed switch* não sofre operações desnecessárias por te poucas peças mecanicamente móveis, possui uma vida útil muito longa.
3. Como os componentes móveis são leves e com alta frequência de ressonância, estes se abrem e fecham de forma muito rápida.

A Figura 33 ilustra a construção física do componente:

Figura 33 - Construção física do *reed switch*



Fonte: SLADE, 2014.

Sensores magnéticos baseados no *reed switch* estão disponíveis no mercado em modelos com fios e também em módulos com circuitos eletrônicos, permitindo que o dispositivo se comunique por meio da rede sem fio com a central de alarmes. Os

preços deste sensor variam de acordo com as funcionalidades, partindo de R \$20,00 (vinte reais) e podendo chegar até R \$200,00 (duzentos reais) com os recursos de comunicação sem fio (valores referentes a 2022). Dessa forma, sensores magnéticos são uma ótima solução para monitoramento de portas, janelas e painéis elétricos e eletrônicos, uma vez que apresentam uma taxa de alarmes falsos baixíssima e uma ótima durabilidade (SLADE, 2014).

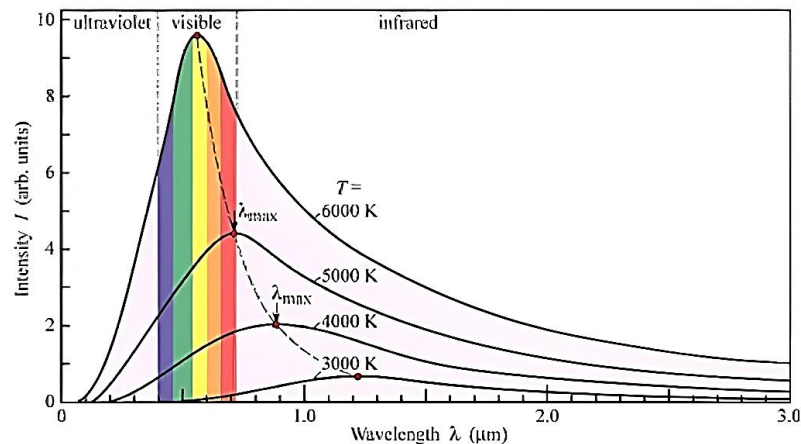
3.2 SENSORES DE DETECÇÃO DE PRESENÇA

Caso não seja possível eliminar uma ameaça por meio da dissuasão, o próximo princípio fundamental de um sistema de segurança que entra em ação é a capacidade de detecção deste. Só é possível atrasar ou atuar sobre uma possível tentativa de invasão a partir do momento em que se detecta a ameaça, para isto, existem sensores que empregam tecnologias voltadas para detecção de intrusão por meio de sensoria-mento da área, os mais comuns são os sensores de infravermelho ativo, passivo e também os sensores ultrassônicos.

3.2.1 Sensor infravermelho passivo

Sabe-se que qualquer carga que esteja sofrendo variação de velocidade emitirá uma onda eletromagnética. Estendendo este conceito a outros corpos com temperaturas acima do zero absoluto, nos quais identifica-se movimentação de elétrons (com campos elétrico e magnéticos associados), observa-se a irradiação de ondas eletro-magnéticas com comprimento fora do denominado espectro visível, classificadas en-tão como infravermelhas. À direita da Figura 34 está referenciada a região infraver-melha do espectro, região do gráfico que apresenta um comprimento de onda muito acima da região visível.

Figura 34 - Espectro eletromagnético e temperatura

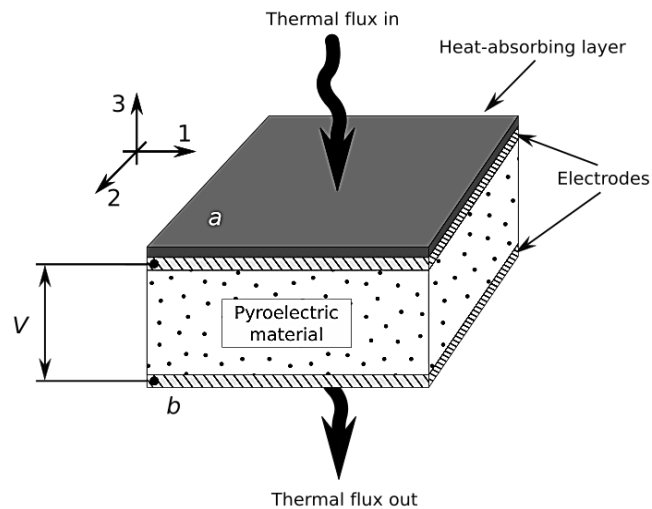


Fonte: CAMPERI, 2021.

Conclui-se que o corpo humano emite radiação eletromagnética na região do infravermelho, mesmo não sendo possível enxergar, torna-se possível identificar estas radiações por meio de sensores construídos para esse propósito, que são amplamente utilizados não só nos sistemas de segurança, mas também para automações em diversas áreas (BRITTO e GARCIA, 2020).

A piroeletricidade, conceito importante para compreensão e sensores infravermelhos, é definida como a capacidade de geração de um dipolo elétrico em um material isolante devido a uma mudança homogênea na temperatura. Um material piroelétrico gera momentos de dipolo elétrico, e isso, por sua vez, gera uma corrente proporcional à variação da temperatura do cristal. Portanto, materiais piroelétricos são na prática cristais detectores térmicos de alta frequência que são utilizados para detectar radiação por meio da variação de temperatura (HOSSAIN e RASHID, 1991). A Figura 35 ilustra o esquema de um sensor piroelétrico, apresentando como o fluxo térmico é captado por este e entra em contato com o material piroelétrico responsável pelo acionamento.

Figura 35 - Princípio de funcionamento do sensor piroelétrico



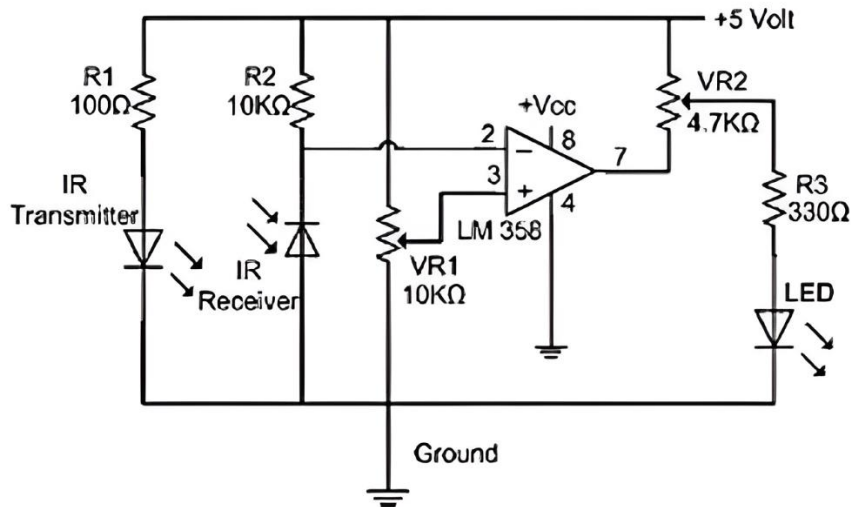
Fonte: FILHO e MOREIRA, 2016.

O sensor piroelétrico é construído a partir de um material cristalino capaz de gerar um potencial elétrico em sua superfície quando exposto a calor emitido na forma de radiação infravermelha, a carga do sensor muda de acordo com a quantidade de radiação que recebe, dessa forma é possível mensurar esta quantidade. Por conta dessa capacidade, uma das grandes aplicações deste sensor é o sensor detector de movimentos, uma vez que as propriedades piroelétricas de alguns cristais fornecem o recurso de identificar variações de temperatura em determinada área, é possível construir um sistema de controle que trate o sinal de variação de temperatura gerado como uma possível presença inesperada ou tentativa de invasão na área monitorada (FILHO e MOREIRA, 2016).

3.2.2 Sensor infravermelho ativo

O sensor de infravermelho ativo, ao invés de detectar as ondas eletromagnéticas na região do espectro infravermelho, possui uma fonte de radiação infravermelha ativa e um fotodetector, ou seja, um diodo emissor de luz e um receptor. Dessa forma, assim que um objeto se aproxima do sensor, a luz infravermelha é refletida e detectada pelo receptor, constatando então a presença de um corpo nas proximidades do sensor. Na Figura 36 está ilustrado um diagrama do circuito eletrônico de um sensor infravermelho completo, com transmissor, receptor, comparador e potenciômetro.

Figura 36 - Diagrama de circuito do sensor infravermelho ativo



Fonte: AGARWAL, 2013.

Para construção de um sensor infravermelho ativo comum é necessário um par formado por um diodo emissor de luz e um fotodetector, de forma que o diodo emissor de luz alimentado pela fonte de tensão e polarizado diretamente permanece emitindo radiação infravermelha de forma constante. O fotodetector está com um dos terminais aterrado e o outro conectado diretamente à entrada do comparador (entrada 2 na Figura 36), este será polarizado apenas quando identificar a presença de luz em sua superfície.

No momento em que identificar a luminosidade refletida pelo objeto que se aproxima, o fotodetector “*IR Receiver*” entrará em condução e consequentemente o comparador LM358 identificará a mudança de estado no terminal 2. A saída do comparador (terminal 7) depende também do valor da resistência variável (potenciômetro $VR1$) que tem a função de determinar a sensibilidade do dispositivo proporcionalmente ao valor de sua resistência. Quando a condição de polarização do fotorreceptor e condução do comparador LM358 forem atendidas, um LED será aceso no circuito em questão, mas o diagrama ilustrado possui inúmeras aplicações não só na segurança, mas também na indústria devido à sua capacidade de identificação de objetos de forma rápida e de baixo custo.

3.2.3 Sensor ultrassônico

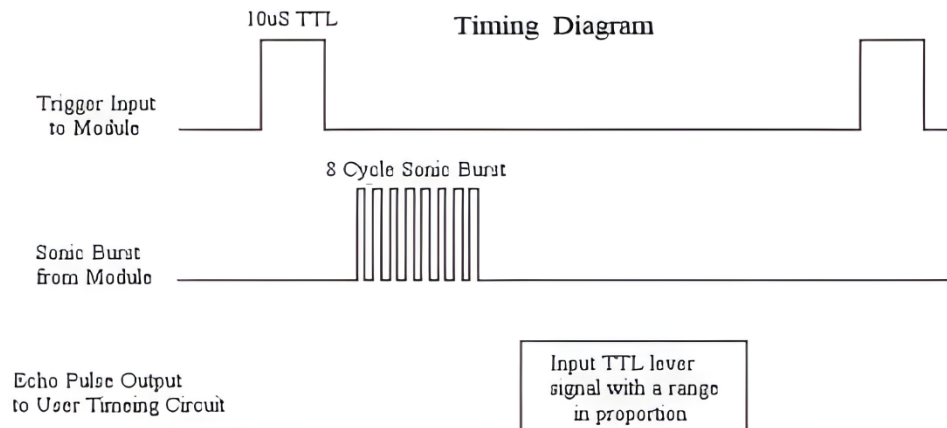
Os sensores ultrassônicos são usualmente utilizados para detectar a presença de objetos e até mesmo substâncias em diversos estados. Seu funcionamento é através de radiação não sujeita a interferência eletromagnética de forma totalmente limpa, o que pode ser muito importante para determinadas aplicações. O comprimento de onda utilizado é muito importante nesse tipo de sensor, pois ele determina as dimensões mínimas do objeto que pode ser detectado. Só ocorre reflexão em intensidade suficiente para se obter um bom sinal, quando o objeto tem dimensões próximas ou maior que o comprimento de onda. Um sensor ultrassônico é formado por um emissor e um receptor, que podem estar fixados ou separados, dependendo do posicionamento desejado (FERREIRA et al., 2017). Um modelo bastante comum de sensor ultrassônico está ilustrado na Figura 37.

Figura 37 - Modelo de sensor ultrassônico HC-SR04 tradicionalmente utilizado no arduino



Fonte: MORGAN, 2014.

O sensor HC-SR04 utiliza a tecnologia de detecção por meio de sinal ultrassônico e é muito utilizado para projetos nos quais é necessário realizar a detecção de presença ou aproximação de um objeto, contando não apenas com o recurso de detecção, mas também com o cálculo da distância entre o sensor e objeto a ser detectado. O sensor conta com terminais de alimentação, aterramento, disparo de pulsos (*trigger*) e tempo de retorno do sinal emitido (*echo*). O funcionamento e método de detecção será apresentado na Figura 38.

Figura 38 - Operação do sensor ultrassônico

Fonte: MORGAN, 2014.

Identifica-se no HC-SR04 a presença de um emissor (TX) de sinais ultrassônicos e um receptor (RX). No início do processo, o transmissor envia um pulso de 10µs, para marcar o início da transmissão e logo em seguida são enviados em sequência 8 pulsos de 40 kHz. A partir desse momento o sensor começa então a aguardar o retorno do sinal ultrassônico enviado e determinar então o tamanho do pulso mostrado na terceira linha, que será retornado ao sistema por meio da saída ECHO do sensor. Este valor de saída será uma medida temporal, porém uma vez em que é conhecida a velocidade de um sinal ultrassônico, é possível utilizá-la para calcular então a distância que foi percorrida por este pulso considerando o tempo que levou para que atingisse o objeto saindo de TX e retornando a RX, como demonstrado na equação (1).

$$D = \frac{t_{\text{retorno}} \cdot V_{\text{som}}}{2} \quad (1)$$

Onde:

D: Distância percorrida pelo sinal ultrassônico em metros.

t_{retorno}: Tempo para que o sinal atinja o objeto e retorne a RX em segundos.

V_{som}: Definido como $340 \frac{m}{s}$.

Dessa forma, é possível calcular por meio de um algoritmo ou operação no sistema do microcontrolador que gerencia o sistema de alarmes qual é a distância segura que um objeto pode aproximar-se de determinada área e acionar os devidos

alarmes e atuadores que instalados para informar a intrusão indevida no local e mitigar os riscos de uma possível invasão no perímetro protegido (MORGAN, 2014).

3.3 SENSOR SÍSMICO

Outro mecanismo muito eficiente para monitorar portas, janelas, portões, muros e até mesmo o solo de áreas muito sensíveis é a detecção de vibração nas superfícies. Outros sistemas de detecção de intrusão podem ser desativados por técnicos ou chavesiros experientes em atividades minuciosas, que podem colocar o funcionamento do sistema em risco sem que ocorra a detecção, um contato magnético, por exemplo, como foi apresentado, não dispara mesmo que o dispositivo todo se mova ou seja inspecionado, se seus contatos magnéticos permanecerem colados, nenhuma atuação de alarme é enviada ao sistema.

Para resolver este problema e proporcionar ao sistema de segurança uma alternativa mais eficiente contra possíveis invasores que tentam desativar ou sabotar a área protegida, uma ótima alternativa são os sensores de detecção de vibração, conhecido como “sensores sísmicos”.

Existem vários tipos de sensores de vibração, cada um deles com suas particularidades de detecção, custos e vantagens para cada tipo de aplicação, que vão desde detecção de funcionamento inadequado de maquinários na indústria até a detecção de terremotos. Alguns tipos destes sensores são: extensômetros, acelerômetros, de corrente de Foucault, deslocamento a laser, giroscópios e sensores de microfone (UPKEEP, 2019). A seguir, serão discutidos com um pouco mais de detalhes os sensores de vibração denominados de extensômetros.

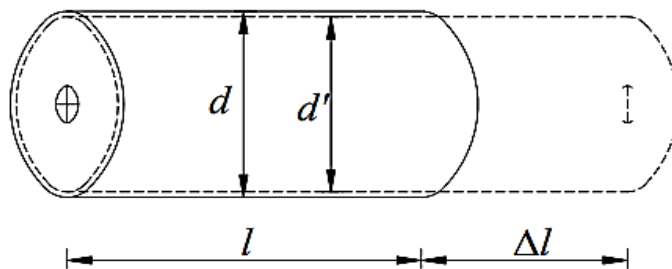
3.3.1 Extensômetro

O sensor de vibração do tipo extensômetro consiste em uma lâmina com uma grade com capacidade de condução elétrica que é aplicada diretamente na superfície monitorada. À medida que a grade é esticada ou comprimida, em casos em que o material sofre alguma perturbação, sua resistência elétrica sofre alteração, e são essas oscilações que servem de referência para a medição de vibrações em uma superfície. Uma breve definição é que o extensômetro é baseado no fato de que os metais mudam sua resistência elétrica quando sofrem uma deformação. O extensômetro

deve ser muito bem fixado à estrutura em que realizará a medição e uma vez instalado, o sistema que o utiliza tem o potencial de converter toda a deformação nela causada em tensão, de forma que o sinal de tensão pode ser amplificado e enviado para leitura e tratamento em um local remoto, que pode ser a central de monitoramento do sistema de segurança (ANDOLFATO, 2004).

Para analisar o princípio de funcionamento de um extensômetro, podemos analisar um fio metálico antes e após uma deformação, conforme a Figura 39.

Figura 39 - Deformação de um fio sob tração



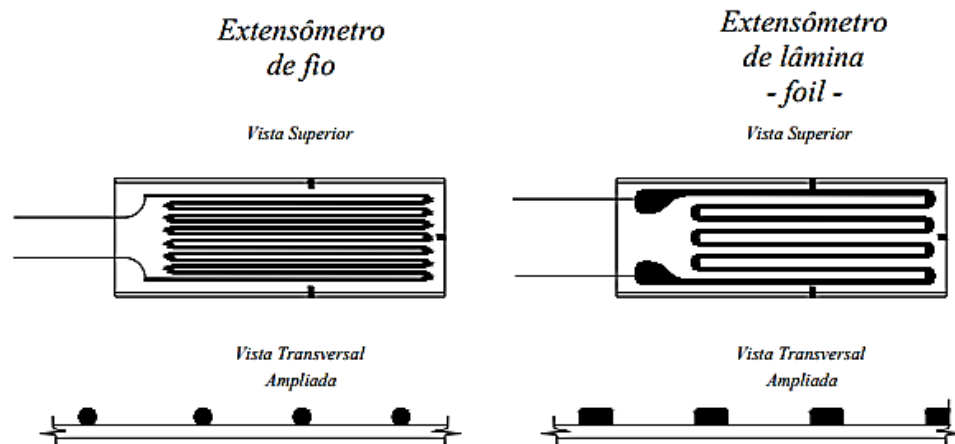
Fonte: ANDOLFATO et al, 2004.

Na figura, l representa o comprimento original do fio antes da deformação e nas condições iniciais o fio apresenta uma resistência inicial R . Analisando a linha pontilhada, verifica-se que o fio metálico está alongado após uma perturbação e consequentemente seu comprimento nestas condições será representado por $l + \Delta l$, de forma que a resistência também sofrerá alteração e passará a ser representada por $R + \Delta R$. Sabe-se que a resistência elétrica R de um material é dada pela equação (2):

$$R = \rho \cdot \frac{l}{A} \ (\Omega) \quad (2)$$

Onde A é a área da seção transversal do fio e ρ é a resistividade do material do fio. Nota-se então que perturbações na área ou no comprimento do material utilizado para fabricação do extensômetro resultará diretamente em uma variação na resistência elétrica do circuito do sensor. Na Figura 40 estão representações de extensômetros fabricados em forma de fios e de lâminas:

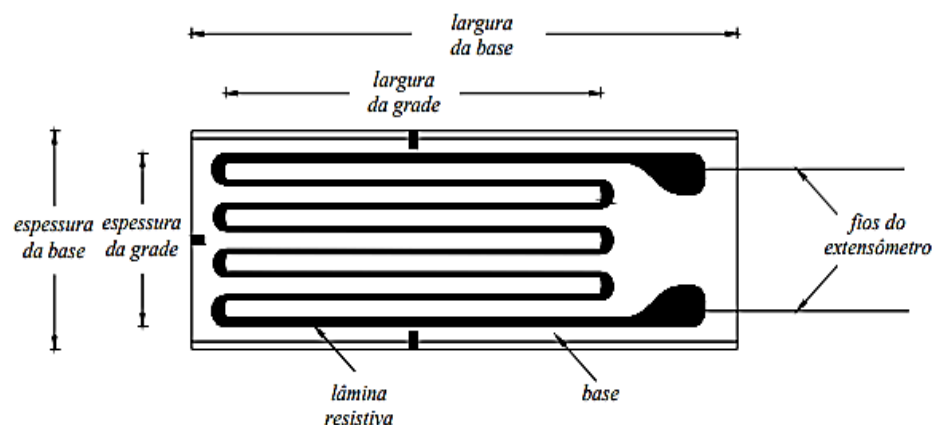
Figura 40 - Extensômetros elétricos de resistência



Fonte: ANDOLFATO et al, 2004.

Para a fabricação de extensômetros tradicionais, uma lâmina metálica resistiva de alguns micro é fixada em um material eletricamente isolado chamado de base de forma que porções desnecessárias do material da lâmina são eliminadas pelo processo de foto gravação, de acordo com o padrão desejado para o extensômetro, posteriormente os fios de saída são soldados. As configurações mais comuns são de resistência de 120 Ω , mas existem extensômetros disponíveis no mercado com resistência de 350 Ω , 500 Ω e até 1000 Ω (ANDOLFATO, 2004). A Figura 41 descreve quais são as partes componentes durante a confecção de um extensômetro elétrico de resistência:

Figura 41 - Esquema de confecção dos extensômetros



Fonte: ANDOLFATO et al, 2004.

Além dos com a tecnologia descrita, existem extensômetros de diversos tipos de materiais e suas e com diversas tecnologias para construção, porém os conceitos de funcionamento e aplicações seguem os mesmos e as vantagens variam de acordo com a necessidade do projeto, não apenas o tipo de extensômetro. A tecnologia dos sensores de vibração pode ser mais eficaz, porém com as informações acima é possível ter uma referência das aplicações da tecnologia.

4. SISTEMAS DE CFTV

Os CFTV são sistemas de vídeo vigilância aplicados a um delimitado perímetro, como dentro e fora de construções, locais públicos, entre outros. Permite que vários locais sejam observados por uma única pessoa a milhares de milhas de distância em centros de operações, celulares ou laptops. O CFTV consiste em um sistema de monitoramento por imagens de televisão que transmitem os sinais recebidos de câmeras localizadas em locais específicos, nos quais é interessante monitorar as atividades. O posicionamento das câmeras é algo subjetivo e deve ser levado em consideração qual é o bem ou região que deve ser foco de seu monitoramento, seja um cofre, uma porta, uma entrada de veículos, entre outros. No caso de entrada de veículos, por exemplo, é interessante enfatizar alguns pontos, como placa do carro, modelo e vista do comportamento do motorista, as câmeras têm limitações de amplitude de cobertura e também de resolução, fatores como iluminação, anteparos naturais e distância do objeto a ser monitorado sempre devem ser levados em consideração (PURPURA, 2011).

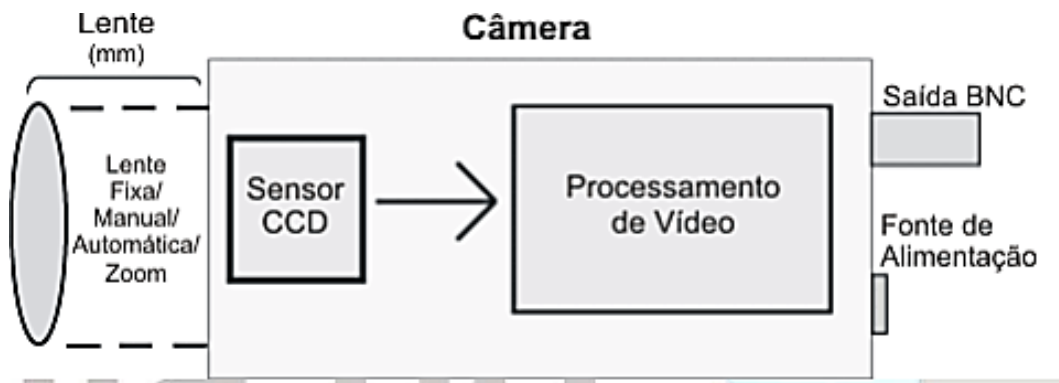
Um circuito de câmeras bem posicionado e ajustado permite que apenas uma pessoa faça o monitoramento de uma grande área por meio de alguns monitores dispostos de forma inteligente e um bom *software* de gerenciamento de vídeo, além da possibilidade de antecipar incidentes de segurança através do monitoramento de atitudes suspeitas, também é de extrema importância na investigação de eventos já ocorridos, sejam da área de segurança ou não, alguns bons exemplos são áreas técnicas em que pode-se identificar alguma falha por meio monitoramento e também acompanhamento de tráfego, desastre naturais, ou qualquer outro risco ou ameaça que esteja presente.

Além de uma ferramenta importantíssima para monitoramento, existem diversos tipos de tecnologias de câmeras que podem ser utilizadas na detecção de intrusão por meio de algoritmos de vídeo analítico, que podem ser aplicados em diversas áreas, uma vez que permitem distinguir objetos, cores, tipos de veículos entre outros. Algoritmos de processamento de imagem também permitem que um sistema de câmeras identifique situações específicas de acordo com a necessidade do sistema e emite alarmes, forneça base de dados para estudos estatísticos entre outras aplicações, como será detalhado posteriormente.

4.1 PRINCÍPIO DE FUNCIONAMENTO

O funcionamento da câmera parte da conversão de níveis de iluminação e cor em sinais elétricos seguindo padrões determinados. Para isso, toda câmera possui sensores, que têm a finalidade de serem atingidos pela luz, sendo então o ponto de início do sistema de visualização. Dessa maneira, as câmeras criam imagens através dos níveis de iluminação capturados do ambiente através de suas lentes e também do sensor de imagem CCD. A imagem capturada é então processada e transmitida para o sistema de controle ou para um dispositivo de armazenamento de vídeo. Atualmente existem diversos tipos de câmeras projetadas para aplicações e ambientes específicos. Há micro câmeras para aplicações simples, câmeras profissionais para aplicações de maior segurança ou exigência, câmeras *speed domes* (de alta performance) para aplicações de grande porte e grande versatilidade, entre outras (PERES, 2004). O sistema descrito é ilustrado na Figura 42.

Figura 42 - Diagrama esquemático de uma câmera convencional



Fonte: PERES, 2004.

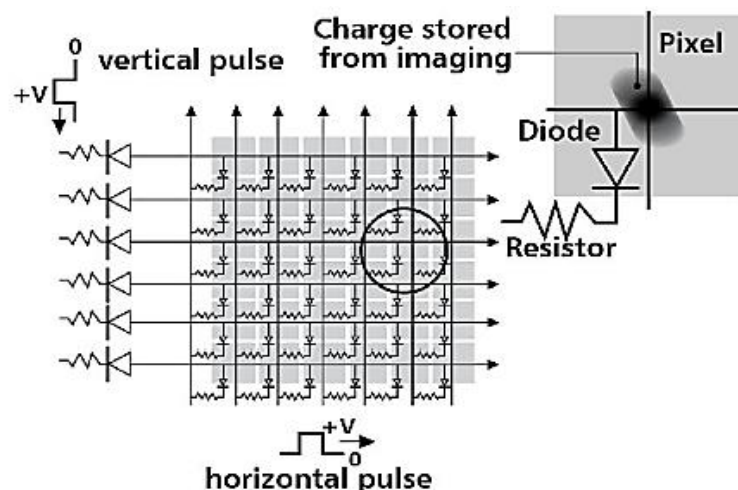
A tecnologia mais complexa presente nas câmeras é o sensor de carga acoplada: sem ele, não seria possível converter a iluminação do ambiente em sinais elétricos e construir uma imagem em *pixels* como conhecemos.

Quando analisamos, atualmente, uma câmera convencional, nos deparamos com duas funções principais: a captação das imagens por meio de um CCD sensível à luz e o armazenamento dos sinais elétricos captados por meio de circuitos eletrônicos. Sabe-se que uma imagem é composta por milhares de fragmentos unificados e que cada um destes pequenos fragmentos é popularmente conhecido como *pixel*. O

desafio que surge no processo de captação e armazenamento de imagens reside exatamente em como relacionar cada microfragmento com uma pequena região do CCD. A forma com que este registra e posiciona cada um desses *pixels* é a chave para o entendimento da imagem digital (HAMMACK et al, 2012).

O primeiro passo para reproduzir uma imagem é a absorção da luminosidade de um objeto, armazenando-a de alguma forma. Tal processo só se tornou possível a partir da descoberta do efeito fotoelétrico, conceito que assume que alguns materiais produzem corrente elétrica quando recebem algum tipo de luz. Na prática, o silício totalmente subdividido presente no CCD armazena elétrons de acordo com a quantidade de luz que incide sobre este, convertendo, assim, a luz em cargas elétricas durante sua extensão. Partindo dessa premissa, seria possível construir uma câmera organizando vários componentes de silício sensíveis à luminosidade de forma similar a uma matriz de *pixels*, como se observa em uma imagem digital convencional. A primeira tentativa de prova deste conceito foi realizada conectando os *pixels* em uma matriz x-y por meio de fios (IDEM). Como se observa na Figura 43, a cada *pixel* foi adicionado um *gate* eletrônico com o intuito de controlar o fluxo da carga do *pixel*. As cargas armazenadas, segundo essa ideia, fluíram verticalmente e horizontalmente pela grade, possibilitando então a leitura de cada *pixel* individualmente.

Figura 43 - Ilustração da primeira tentativa de reproduzir uma imagem digital



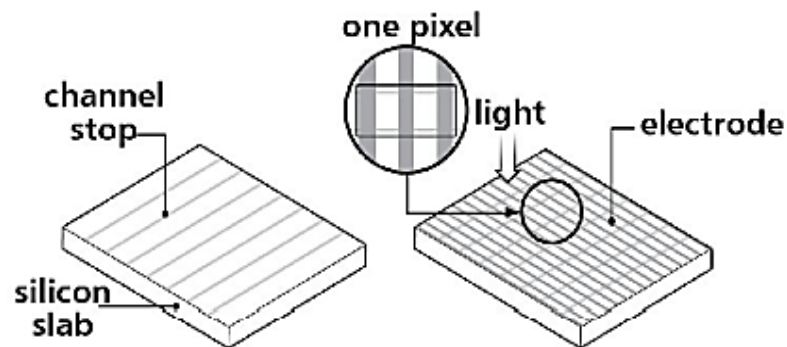
Fonte: HAMMACK et al, 2012.

Este método, porém, apresentou um grave problema: todos os pequenos componentes conectados entre cada *pixel* possuíam uma capacitância individual, de forma

que quando o sinal percorre a matriz, ele acumula a carga (chamada de acoplamento capacitivo) de cada um dos *pixels* pelos quais passou, o que resulta em uma distorção significativa no resultado final do sinal de imagem obtido. Mesmo que a carga de cada *pixel* seja pequena, a somatória do acoplamento capacitivo compromete cada vez mais o sinal resultante quanto maior a resolução da matriz de *pixels*. Para resolver a questão da distorção do sinal por conta do acoplamento capacitivo, a solução do CDD é não contar com nenhum fio conectado em seu sistema (HAMMACK et al, 2012).

Ainda em análise à orientação dos autores, o CCD possui 5 mm de comprimento por 4mm em sua aplicação atual nas câmeras convencionais, e é formado por apenas uma placa de silício. O que faz do silício o material ideal para a construção do CCD é sua capacidade de operar como condutor, isolante ou semicondutor, de acordo apenas com a dopagem em que é aplicada. Tirando vantagem dessa versatilidade do silício e para atender a construção do CCD, são construídas seções isolantes que servem para delimitar os *pixels*. Conforme se extrai da Figura 44, um *pixel* é identificado em uma pequena seção do silício constituído por duas limitações de silício isolante na horizontal e três tiras de metal na vertical (HAMMACK et al, 2012).

Figura 44 - Representação do pixel no eletrodo de silício

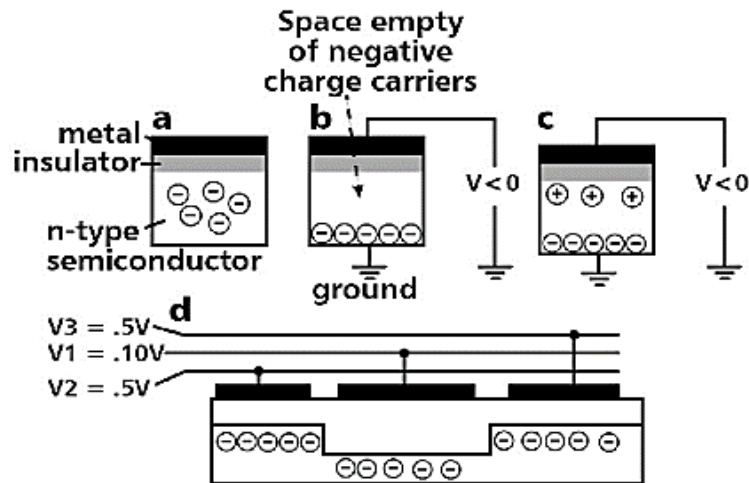


Fonte: HAMMACK et al, 2012.

Dando continuidade ao processo, uma vez expostas à luminosidade dos objetos que serão registrados, as cargas são produzidas em cada *pixel* do CCD: a esse ponto, o desafio é transitar com essas cargas a fim de realizar o armazenamento. As cargas registradas devem ser então movidas linha por linha pela matriz de *pixels* até o momento em que chegam no registrador eletrônico da câmera. Para captar os elétrons referentes às cargas armazenadas, o CCD conta com uma cobertura de eletro-

dos metálicos, que variando sua tensão, cria uma armadilha de elétrons com três estágios, captando, dessa forma, as cargas dos *pixels* que compõem a imagem. A Figura 45 demonstra como é possível mover os elétrons armazenados por meio da variação de tensão do eletrodo presente.

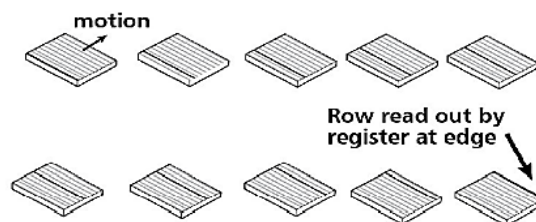
Figura 45 - Comportamento das cargas armazenadas ao variar a tensão do eletrodo



Fonte: HAMMACK et al, 2012.

A oscilação de tensão no eletrodo faz com que as cargas migrem da região de menor tensão para a de maior tensão. Dessa maneira, torna-se possível fazer com que as cargas passem de forma sequencial pelos eletrodos até que atinjam o registrador eletrônico da câmera, possibilitando o registro de cada linha de carga (que compõe a imagem) de forma sequencial. A Figura 46 ilustra o fluxo das cargas até o momento em que chegam na posição em que é realizado o armazenamento pelo registrador eletrônico da câmera.

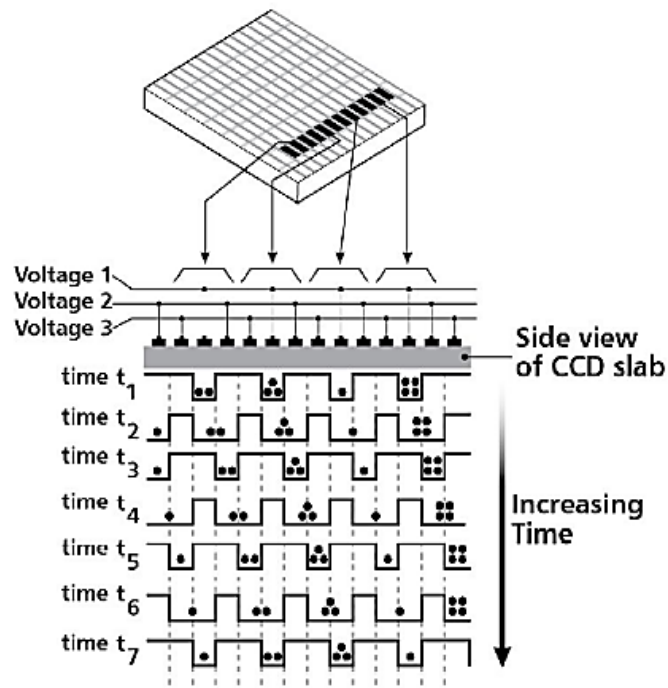
Figura 46 – Registro das informações recebidas pelo CCD sequencialmente por meio de linhas



Fonte: HAMMACK et al, 2012.

Na Figura 47 é possível verificar de forma mais detalhada como é possível efetuar a transição de cargas da matriz de eletrodos até o registrador por meio da variação de tensão no eletrodo.

Figura 47 – Ilustração do fluxo de elétrons pelo eletrodo através da variação de carga



Fonte: HAMMACK et al, 2012.

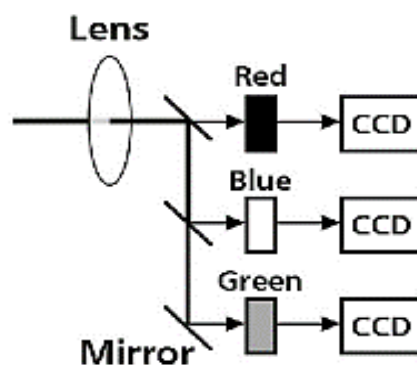
Mediante o uso da técnica de captação de elétrons, estes se aproximam ou se repelem de acordo com a tensão aplicada, sendo possível então que transitem pela matriz de *pixels* do CCD até o registrador da câmera (HAMMACK et al, 2012).

4.1.2 Definição de cores na imagem

A tecnologia de captação de imagens descrita até agora pormenoriza como é possível formar a imagem em uma câmera; porém, como foi mencionado, o método até este ponto capta apenas a intensidade da luz por meio das cargas, deixando um importante detalhe quando se trata de imagens: a cor. Por meio das cargas captadas pelos *pixels* no CCD é possível constituir uma imagem em preto e branco, uma vez que é conhecida a intensidade da luz que incidiu sobre os *pixels* de silício, mas nenhuma diferenciação de cores foi realizada até então. Uma das possíveis soluções para este problema é separar o espectro da luz por meio de um prisma e armazenar

em três CCDs diferentes as matrizes de *pixels* dos vermelhos, verdes e azuis para posteriormente combiná-los e obter, finalmente, uma imagem colorida. Um problema nítido para essa solução é o custo: o CCD, por conta de sua composição e tecnologia, é um componente bastante caro. A manutenção de 3 (três) deles em funcionamento eleva o custo de uma câmera de forma significativa. Na Figura 48, é possível observar a ilustração da solução proposta de dividir a luz recebida em três CCDs diferentes.

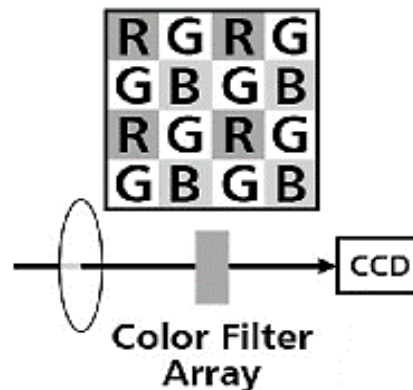
Figura 48 - Solução possível: dividir os componentes da luz em três CCDs diferentes



Fonte: HAMMACK et al, 2012.

Por conta da contrariedade citada, foi proposta outra solução para integrar cor às imagens digitais: adicionou-se um filtro de cor em forma de matriz na entrada de luz, juntamente com o CCD, assim como indicado na Figura 49. Essa matriz foi então dividida em pequenas seções proporcionais ao tamanho dos *pixels*, de forma que algumas possuem filtro vermelho, verde ou azul. Obtém-se então, na saída do CCD, uma imagem resultante da combinação de diversas cores. No entanto, para obter nitidez na imagem final, é necessário aplicar um algoritmo para estimar quais os percentuais dos outros componentes RGB (Vermelho, Verde e Azul) de cada pixel. Tal informação pode ser estimada pelo algoritmo por meio da análise das cores predominantes nos *pixels* adjacentes e suas intensidades (HAMMACK et al, 2012).

Figura 49 - Adição do filtro de cor e estimativa por meio de algoritmo no processamento da imagem digital



Fonte: HAMMACK et al, 2012.

Dessa forma, por intermédio de algoritmos, possibilita-se o tratamento dos *pixels* obtidos e filtrados para obtenção de uma estimativa para compor a imagem digital utilizando-se apenas um CCD, reduzindo, assim, o custo de fabricação das câmeras digitais (HAMMACK et al, 2012).

4.2 CLASSIFICAÇÃO DE CÂMERAS POR CONEXÃO

Outro ponto importante é a classificação das câmeras utilizadas no sistema com base na tecnologia aplicada. Para este fim, são utilizadas as câmeras analógicas e também as chamadas IP. As analógicas, por definição, têm como saída um sinal analógico que pode ser reproduzido de forma instantânea ou convertido e tratado por meio de conversores analógico-digitais para fins de armazenamento, não sendo capazes de comunicar-se diretamente com a rede de internet. Já as câmeras IP possuem essa capacidade, sendo de fácil instalação, uma vez que não precisam de conversor de sinais e de melhor transmissão, tendo em vista que na rede a imagem pode ser visualizada por qualquer pessoa autorizada em qualquer lugar. Poupam-se, assim, investimentos como cabeamento e conversão, viabilizando qualidade de imagem superior.

Por outro lado, as câmeras IP são totalmente dependentes da rede de internet, necessitando assim de uma redundância para garantir que a gravação não seja afetada, além de fornecer um ponto de acesso local na rede, facilitando o acesso de *hackers* (caso tenham acesso ao cabo da câmera), uma vez que a conexão é direta.

Neste contexto, as câmeras analógicas são recomendadas para casos em que os vídeos serão acompanhados apenas em um site, ou em que se faça necessário integrar a imagem de um ponto crítico à rede. Nesse caso, é possível gravar o local não seguro com uma câmera analógica (sem expor um ponto de acesso) e fazer a conversão do sinal e integração com a internet já em uma área protegida.

4.3 CÂMERAS COMO DETECÇÃO DE INTRUSÃO

Os sistemas de CFTV são essenciais não só como facilitadores do monitoramento de perímetros, mas também como suporte em investigações de eventos de segurança, como elemento de dissuasão e ferramenta de detecção de intrusão por meio de tecnologias de análise de variação de movimento e vídeo analítico.

A análise de variação de movimento verifica a escala de *pixels* das imagens e, com base nos quadros anteriores, calcula a variação e avalia se foi significativa; se sim, causa um alarme direto na central de monitoramento. Já o vídeo analítico, por meio de algoritmos e processamento digital de sinais, verifica se a variação nos *pixels* foi significativa a ponto de representar uma atividade anormal para o sistema. Tal tecnologia utiliza sistemas mais sofisticados de análise de imagem a fim de evitar falsos alarmes para a central de monitoramento. Diferentemente da detecção de movimento, comporta uma inteligência embarcada capaz de promover a filtragem da imagem gravada.

4.3.1 Vídeo analítico

Conforme introduzido, o vídeo analítico implementa *firmwares*, tecnologias de processamento digital de sinais e algoritmos com capacidade de aprendizado em câmeras, processadores, servidores e em gravadores de vídeo (NVR) com a finalidade de potencializar a capacidade de monitoramento e análise do sistema de monitoramento. Com o apoio das tecnologias mencionadas, é possível que uma única pessoa monitore até mesmo centenas de câmeras, uma vez que o sistema inteligente fará o tratamento das imagens de forma automatizada e retornará ao operador apenas os alarmes e notificações de vídeo relevantes, que podem representar alguma ameaça concreta, acompanhando em apenas uma tela o relatório e seleção de imagens mais relevantes naquele momento, eliminando, então, a necessidade de várias pessoas

analisarem múltiplas telas e eliminando possíveis falhas de observação por cansaço ou outras falhas de atenção por parte dos operadores (BHATTACHARYYA, 2009).

Deve ser ressaltado que a definição de atividade suspeita ou movimentação irregular pode variar muito de acordo com os objetivos do sistema de vigilância, porém alguns exemplos característicos podem ser mencionados, como o cruzamento de limites de espaço, a presença de veículos ou pessoas parados por muito tempo no mesmo local, objetos deixados ou esquecidos em local de risco, aglomerações de pessoas ou carros, entre outros. Exemplos como os citados em uma área com centenas de câmeras poderiam facilmente passar despercebidos pelos operadores; todavia, o sistema de vídeo analítico desempenha a detecção destes eventos de forma automática (pré-definida de acordo com as prioridades do sistema) e os reporta por meio de alarme ou notificação.

Além da análise em tempo real, é possível aplicar as mesmas tecnologias de detecção sobre as imagens registradas dos últimos dias ou meses, que normalmente ficam armazenadas em uma central de armazenamento de rede (NVR) ou digital (DVR), trazendo assim de volta à situação em que se deseja investigar sem que seja necessário que alguém assista e busque um único evento em centenas de horas de gravação. Para pontuar alguns exemplos, pode-se citar a investigação de um momento específico em que determinada pessoa cruzou um limite da imagem da câmera, ou um carro vermelho passou pela rua, uma pessoa com camiseta azul passou por determinada porta, resultando na perda de diversas horas ou até mesmo dias para apurar o ocorrido. Neste mesmo contexto, o sistema de vídeo analítico é capaz de apresentar, em segundos, o resultado pretendido, utilizando apenas um único operador treinado para manejar as ferramentas de análise.

5. PROJETO DE UM SISTEMA DE SEGURANÇA

Foi elaborado um projeto para detalhar a instalação e aplicação real de um sistema eletrônico de segurança, incluindo dispositivos envolvidos, materiais necessários para instalação, possíveis configurações e boas práticas de segurança. Criou-se uma planta fictícia para ilustração dos conceitos e fornecimento de uma aplicação prática dos conceitos teóricos discutidos nos capítulos anteriores. O objetivo deste projeto é construir um sistema eletrônico de segurança para uma planta de um escritório comercial, cobrindo o controle do fluxo de pessoas, monitoramento de atitudes suspeitas, detecção de tentativas de intrusão e viabilização de investigações de eventos importantes.

O projeto se encontra disponível no Apêndice B – Projeto de instalação de um sistema de segurança bem como no Apêndice A – Legenda do projeto, encontra-se a legenda dos dispositivos empregados no projeto.

Na Tabela 4 estão listados os dispositivos utilizados, quantidades, modelos e estimativa de preços de mercado, disponíveis em sites de lojas convencionais de tecnologia, eletrônica e materiais para construção.

Tabela 4 - Lista de dispositivos

Dispositivo	Modelo	Quantidade	Preço unitário (R\$)	Preço total (R\$)
Leitora com teclado	Leitora com Teclado Numérico HID RK40 6130	4	1.300,00	5.200,00
Leitora sem teclado	Leitor HID iClass SE RM40	4	900,00	3.600,00
Ímã	Fechadura Eletroímã 300 Kgf com sensor	4	500,00	2.000,00
Botoeira de emergência	Caixa Quebra Vidro Emergência Abertura De Porta	4	130,00	520,00
Sensor de contato	Sensor de abertura magnético com fio	15	15,00	225,00
Sensor infravermelho passivo	Intelbras IVP 1000 PET SMART	3	50,00	150,00
Sirene de alarme	Sirene Intelbras SIR 1000	3	35,00	105,00
Sensor infravermelho ativo	Intelbras IVA 9100 TRI	2	500,00	1.000,00
Câmeras IP	AXIS M3045-V Network Camera	13	1.000,00	13.000,00
Placa controladora IP	Lenel LNL-3300 <i>Intelligent System Controller</i>	1	5.000,00	5.000,00
Placa controladora para leitoras	Lenel Series 1320 <i>Dual Reader Interface Module</i>	4	3.000,00	9.000,00
Placa controladora com relés	Lenel LNL1100 <i>Input Control Module</i>	2	1.000,00	2.000,00
Switch com gravador	<i>Network Video Recorder</i> Intelbras NVD 3116	1	2.000,00	2.000,00

Fonte de alimentação	Fonte Chaveada 12V 10 A Ultra Bivolt 110/220 V	2	50	100,00
Bateria	Bateria 12 V Para Central De Alarme	1	70,00	70,00
Cabo IP	Cabo de rede	70	2,00	140,00
Conector RJ-45	Conector RJ-45	28	1,00	28,00
Cabo de controle	Cabo Manga 12 Vias 26AWG (12x26AWG) - Com Blindagem	100	15,00	1.500,00
Eletroduto	Conduíte Eletr. Corrugado 3/4	100	2,00	200,00
Caixas de passagem	Caixa para Condulete 3/4" 4x2 sem Rosca PVC Tigre	15	27,00	405,00
Codificador de vídeo	AXIS P7304	1	2.000,00	2.000,00
Câmera analógica	Camera de Vigilancia Moto- rola Analogica Image 1080P Bullet Metal Lente 2.8MM IR20M/OSD/IP66-L	2	200,00	400,00
TOTAL				R\$ 51.643,00

Fonte: Elaborado pelo autor.

Os produtos listados na Tabela 4 podem ser substituídos por outros modelos de acordo com os recursos disponíveis, precisão e nível de segurança desejado, já que estão disponíveis no mercado produtos de diversos preços e níveis de segurança/confiabilidade. É possível manter todas as características do sistema gastando menos e concentrando os investimentos nos dispositivos mais críticos para o sistema em questão, o que demonstra a importância do estudo das tecnologias aplicadas e também a análise do contexto em que a instalação será realizada.

5.1. CONSIDERAÇÕES SOBRE OS EQUIPAMENTOS ESCOLHIDOS

Por se destinar a escritório comercial, o controle de acesso para entrada e monitoramento foram os pontos enfatizados no projeto, uma vez que se trata de um ambiente com grande fluxo de pessoas. Por esta razão, investiu-se em placas controladoras, leitoras de cartão de acesso e sistema de câmeras de maior qualidade.

Com relação aos mecanismos de detecção de intrusão, optou-se por sensores de presença de custo reduzido e focados em pontos estratégicos da planta, para que cubram as áreas em que há painéis de controle e salas privativas. Por não haver previsão de materiais ou estoques de alto valor patrimonial, optou-se então pela instalação de sensores magnéticos de contato para supervisionar aberturas indevidas de portas e janelas. Tais sensores, além de possuírem baixo custo, apresentam uma baixíssima taxa de falsos alarmes, cumprindo muito bem a função de detecção de

intrusão por portas e janelas e evitam investimentos muito mais altos. Caso fosse necessário cobrir todas as áreas com sensores sísmicos e infravermelhos, que apresentem taxa considerável de falsos alarmes em áreas movimentadas, além do custo mais elevado de compra e instalação, seria necessária uma equipe de operação para analisar e atuar nos alarmes ocorridos.

Os painéis de controle de alarmes e integração do sistema de CFTV possuem com uma fonte de alimentação 12V e 10 A, suficiente para alimentar o sistema (que conta apenas com equipamentos de baixa potência), além de bateria de 12V como redundância de alimentação, que fica ligada em paralelo com saída da fonte e serve para manter o sistema funcionando temporariamente caso ocorra uma queda de energia.

Outro fator importante são os eletroímãs utilizados como fechaduras das portas: apesar de funcionarem muito bem associados aos sistemas de controle de acesso, possuem a característica negativa de abrir a porta caso ocorra falta de energia por período maior do que a bateria suporta. Uma alternativa de solução é a utilização de fechaduras mecânicas das portas como redundância em períodos fora de horário comercial, garantindo que estas permaneçam sempre fechadas e sem impactar a operação do local.

Com relação às câmeras, para os ambientes internos optou-se pelas câmeras IP, pois são facilmente integradas na rede existente e possuem uma qualidade de imagem superior. Algumas delas foram posicionadas para que monitorem entradas e saídas nas portas, demandando então mais foco e menos visão panorâmicas e outras para cobertura de cômodos completos e corredores, estas com um campo de visão mais aberto, pois seu objetivo é atingir a máxima cobertura com a resolução disponível. Já para as áreas externas de porta de entrada e acesso às janelas por meio do estacionamento, optou-se pela instalação de câmeras analógicas por questões de segurança, já que uma câmera IP nestas posições forneceria um ponto de acesso direto à rede do estabelecimento em um ponto externo, tornando-se uma ameaça crítica de invasão por hackers. Instalando uma câmera analógica nessas posições faz com que um invasor não acesse nenhum dado, uma vez que apenas o cabo analógico ficará exposto. Apesar de elevar a segurança, isto também resulta em custo adicional, uma

vez que para integrar esta câmera no sistema é necessário de um codificador posicionado já dentro do painel de controle, que receberá então o sinal analógico e converterá para digital, de forma que possa ser normalmente integrado na rede e armazenado no NVR.

5.2 CABEAMENTO E INFRAESTRUTURA

Para conectar os dispositivos de segurança nas placas controladoras é necessário criar um circuito de segurança interligando todos os periféricos até o painel de controle central. Com este fim, passa-se um cabo de controle, que possui em seu interior diversos pares de fios para conexão de eletrônicos, compatíveis com os dispositivos e com a placa controladora. Os dispositivos que serão utilizados consomem uma corrente muito baixa (menor que 1 A) e tensão de 12 V, a limitação para adição de periféricos será limitada pela quantidade de entradas disponíveis nas placas controladoras.

Para o sistema de CFTV é necessário construir um segundo circuito interligando todas as câmeras instaladas ao *switch* de rede que realizará o gerenciamento dos respectivos IPs conectando estas ao sistema de rede do local, tornando possível o gerenciamento via *software*. Diferentemente do sistema de alarmes, este circuito será construído com cabos de rede padrão com conectores RJ-45 nas extremidades do *switch* e das câmeras.

Para ambos os circuitos, é necessário analisar quais são os riscos de exposição do cabeamento instalado, já que um cabeamento exposto acima do forro, além de permitir cortes e atos de sabotagem, podem degradar com muito mais facilidade, apesar do custo inferior. O cenário ideal é utilizar eletrodutos de metal com caixas de passagem nas proximidades, de preferência nas extremidades dos sensores e câmeras, a fim de cobrir todo o trecho do cabeamento. As caixas de passagem de alumínio devem ser preferencialmente lacradas, dificultando ainda mais os acessos indevidos.

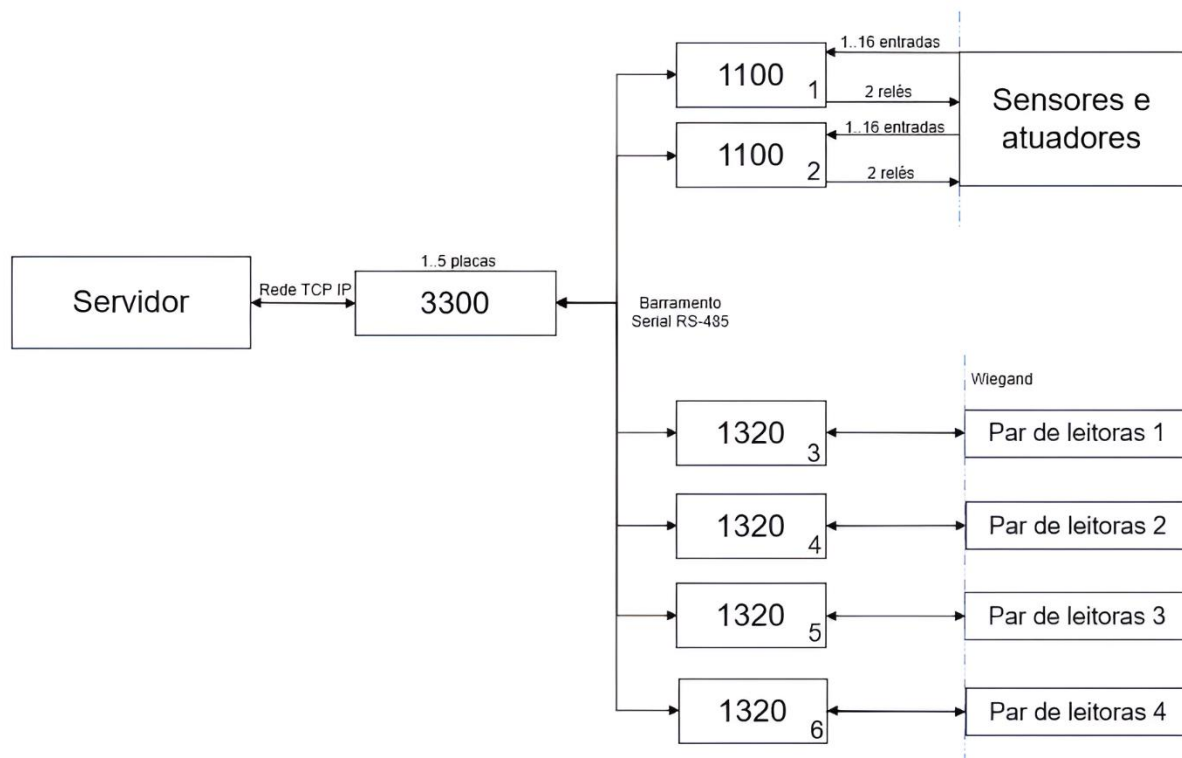
5.2 ENDEREÇAMENTO DE SENSORES E ATUADORES NAS PLACAS

Foram empregados 3 tipos de placas para controlar o sistema de segurança projetado. Como controladora do sistema utilizou-se a placa *Lenel 3300*, que se comunica com a rede local por meio do protocolo TCP/IP, sendo possível então obter dados do servidor para diversas finalidades, como por exemplo para atualização de credenciais

e níveis acesso. Já para o gerenciamento das demais placas, esta conta também com a capacidade de comunicação serial RS-485, sendo possível então endereçar manualmente até 32 placas de controle de acesso (*Lenel 1320*) ou gerenciadoras de relés (*Lenel 1100*) conectadas a ela, as placas mencionadas serão descritas a seguir.

As placas *Lenel 1320* tem a característica de comunicar-se com as leitoras de crachás, sendo então necessário uma destas para cada par de leitoras instaladas, considera-se o par pois é necessária uma para validação de entrada e outra para saída. Apesar de contar também com 4 entradas para alarmes e 2 relés atuadores, sua principal função é comunicar-se com as leitoras de crachás, obter os dados de acesso e transmiti-los para a controladora central por meio da comunicação serial para que esta faça a validação com o servidor, uma vez que é a única do sistema com acesso a rede IP, e responde então a validação do acesso, a ativação de um relé de abertura de trava magnética de porta, ou qualquer outra função que foi programada. Alguns eventos de acesso programados estão vinculados à comunicação descrita, são eles: acesso liberado (seguido do acionamento do relé para abertura de porta), nível de acesso indevido (não autorizado, ativa o relé do *led* de acesso negado), senha errada (ativação do relé do *led* de acesso negado) e crachá inválido (ocorre quando o crachá aproximado está fora da faixa de frequência definida pela leitora).

Por fim, as placas *Lenel 1100* são as responsáveis pela recepção dos sinais de alarme a atuação de sirenes e abertura de portas por meio dos relés. Sua principal função é monitorar o estado dos dispositivos do alarme do sistema e comunicar a controladora, também pela comunicação serial, quando um evento indevido é detectado. A controladora, por sua vez, retorna o comando referente à atuação, acionando o relé correspondente a atuação pré-definida quando cada uma das entradas é acionada. A Figura 50 ilustra a organização das placas bem como suas conexões e interações.

Figura 50 - Organização das placas do sistema

Fonte: Elaborado pelo autor.

Nota-se que as duas controladoras que recebem os sensores receberam os endereços 1 e 2 e as placas que gerenciar as leitoras de crachás atendem por 3, 4, 5 e 6. Na Tabela 5 estão descritos quais foram os dispositivos relacionados à controladora com endereço 1, bem como os atuadores relacionados a cada sensor.

Tabela 5 - Sensores da controladora 1

Área	Endereço na placa	Sensor	Atuador relacionado
Recepção	1	Sensor de presença	Sirene recepção
Recepção	2	Contato magnético da porta	Sirene recepção
Recepção	3	Unidade quebra vidro	Sirene recepção
Banheiro masculino	4	Contato magnético de janela	Sirene da sala de reuniões
Banheiro feminino	5	Contato magnético de janela	Sirene da sala de reuniões
Sala de reuniões	6	Contato magnético de janela	Sirene da sala de reuniões
Sala controlada 2	7	Contato magnético de janela	Sirene recepção
Sala controlada 2	8	Unidade quebra vidro	Sirene recepção
Sala controlada 1	9	Contato magnético de janela	Sirene do corredor
Sala controlada 1	10	Unidade quebra vidro	Sirene do corredor
Área externa 1	11	Infravermelho ativo (emissor)	Sirene recepção
Área externa 1	12	Infravermelho ativo (receptor)	Sirene recepção

Fonte: Elaborado pelo autor.

A controladora de endereço 2 também seguiu a mesma lógica de programação, na Tabela 6 estão os dispositivos nela instalados.

Tabela 6 - Sensores da controladora 2

Área	Endereço na placa	Sensor	Atuador relacionado
Sala de controle	1	Sensor de presença	Sirene do corredor
Sala de controle	2	Contato magnético da porta	Sirene do corredor
Sala de controle	3	Unidade quebra vidro	Sirene do corredor
Sala de controle	4	Contato magnético de janela	Sirene do corredor
Corredor	5	Sensor de presença	Sirene do corredor
Copa	6	Contato magnético de janela	Sirene do corredor
Banheiro	7	Contato magnético de janela	Sirene do corredor
Escritório 1	8	Contato magnético de janela	Sirene do corredor
Escritório 2	9	Contato magnético de janela	Sirene do corredor
Escritório 3	10	Contato magnético de janela	Sirene do corredor
Área externa 2	11	Infravermelho ativo (emissor)	Sirene do corredor
Área externa 2	12	Infravermelho ativo (receptor)	Sirene do corredor

Fonte: Elaborado pelo autor.

Também é necessário endereçar os relés de cada placa, de forma que sejam ativados de acordo com as detecções dos sensores listados nas Tabelas 5 e 6. A Tabela 7 descreve os relés de ambas as placas.

Tabela 7 - Programação dos relés das sirenes

Endereço da placa	Área	Endereço do relé na placa	Atuador
1	Recepção	1	Sirene recepção
1	Sala de reuniões	2	Sirene sala de reuniões
2	Corredor	1	Sirene do corredor

Fonte: Elaborado pelo autor.

Da mesma forma, as controladoras responsáveis pelas leitoras de crachás também foram endereçadas e tiveram seus relés relacionados aos eletroímãs instalados conforme descrito na Tabela 8, sendo responsáveis então pela desmagnetização destes quando o acesso for validado.

Tabela 8 - Controladoras de controle de acesso

Endereço da placa	Local do par de leitoras	Relé
3	Recepção	Fechadura eletroímã
4	Sala controlada 1	Fechadura eletroímã
5	Sala controlada 2	Fechadura eletroímã
6	Sala de controle	Fechadura eletroímã

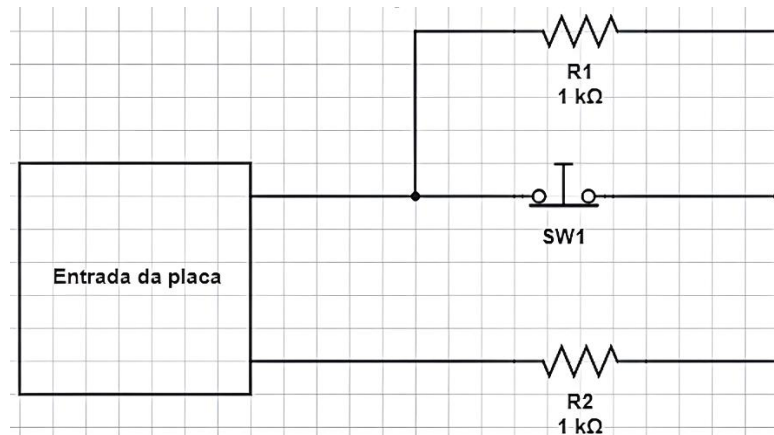
Fonte: Elaborado pelo autor.

Com base nas tabelas anteriores, sabe-se exatamente como devem ser feitas as conexões nas placas controladoras bem como os eventos que devem ser logicamente relacionados a cada sensor na hora de programá-las, facilitando não só a instalação, mas também a manutenção de dispositivos ou expansões futuras do sistema.

5.3 CONEXÃO DOS DISPOSITIVOS NAS PLACAS

Outro fato importante da instalação é a conexão entre os sensores do sistema nas placas controladoras *Lenel 1100*, a interpretação dos estados de alarme varia de acordo com a aplicação, para este caso utilizou-se o estado de saída comum dos sensores (entrada da placa) como circuito normalmente fechado com supervisão de resistores. Esta configuração por si só já é suficiente para classificar como um estado de alarme qualquer tentativa de corte nos fios dos dispositivos, nota-se que caso seja decidido pela configuração normalmente aberto, qualquer dano na infraestrutura entre o sensor e a placa não será perceptível, uma vez que circuito aberto seria o estado padrão.

Para elevar a segurança foi a instalação de uma associação de resistores de supervisão (fechados com plástico termo retrátil) entre o dispositivo e a placa, de forma que só será identificado o estado de alarme se nos terminais de entrada for medido um valor de resistência de 2 k Ω . A Figura 51 representa como será realizada a conexão.

Figura 51 - Associações de resistores nas entradas das placas

Fonte: Elaborado pelo autor.

Percebe-se na Figura 51 que a chave SW1 representa a saída de um dispositivo de alarme com estado normal em normalmente fechado, situação em que a placa identificará em seus terminais de entrada uma resistência de 1 kΩ. Quando o sensor em questão entra em estado de alarme, a chave SW1 será aberta, elevando então a resistência de entrada para 2 kΩ. Outras situações serão descritas a seguir:

- Resistência medida de 1 kΩ: Estado normal da entrada, circuito normalmente fechado com um resistor de supervisão.
- Resistência medida de 2 kΩ: Estado de alarme, circuito normalmente fechado com a associação de resistores na supervisão do alarme indicando 2 kΩ.
- Resistência medida de infinito: Indica que há circuito aberto em algum trecho do cabeamento.
- Resistência medida de 0: Indica que há um curto circuito em algum trecho do cabeamento.

Nota-se que com a implementação da supervisão com resistores nas saídas dos dispositivos se torna muito mais difícil sabotar o sistema, uma vez que mesmo que o indivíduo mal intencionado saiba exatamente qual a resistência exata em que o sistema entra em estabilidade, o que já é um grande desafio, ainda não conseguira inserir sua associação de resistores falsa sem cortar o cabeamento ou alterar a configuração do circuito temporariamente, o que gerará um estado de alerta no sistema.

5.4 MECANISMOS CONFIGURADOS

Para que um visitante tenha seu acesso liberado, é necessário que este digite sua senha e aproxime seu crachá da leitora. Caso o crachá seja válido e a senha esteja correta, o relé da placa controladora é aberto e desmagnetiza o ímã da porta em questão por alguns segundos, liberando então a passagem. Porém, para que o sistema não seja sabotado, é importante garantir que logo após a passagem a porta retorne à posição inicial e o ímã volte a funcionar. Para tanto, é implementada uma função de alarme conhecida como “porta mantida aberta”, possibilitando a supervisão deste evento pela placa controlada por meio de um sensor de contato magnético instalado entre a porta e a estrutura da parede acima, acionando a sirene em situações que permaneça aberta por mais de 1 minuto após o acesso liberado.

O mesmo sensor de contato de porta também é fundamental para detecção de tentativas de intrusão por meio do forçamento da porta. Caso alguém tente empurrar a porta sem liberação do acesso, este sensor será desalinhado e a reação da placa controladora será o imediato acionamento da sirene de alarme, que é conhecida como alarme de porta forçada. É importante também que o acionamento de botoeiras de emergência seja configurado para gerar alarmes de porta forçada, uma vez que um acionamento silencioso desmonetiza o ímã e pode ser um facilitador para acesso indevido.

Outra ameaça comum aos sistemas de controle de acesso é a prática conhecida como “carona”, ou seja, quando uma pessoa com acesso abre a porta e permite a passagem de uma segunda pessoa que não foi autorizada a entrar no local. A fim de mitigar o risco de intrusão por meio de caronas, as leitoras de crachás atuam não só como contadoras de fluxo de entrada e saída, mas também mantendo controle da posição lógica de cada indivíduo por meio da transição nas áreas configuradas. Deste modo, se uma pessoa entra na área 1, o único passo seguinte permitido é a saída desta área, forçando que o crachá sempre seja utilizado para entrar ou sair de uma sala. Caso ocorra uma inconsistência lógica, ou seja, a tentativa de acesso não esteja de acordo com a área do indivíduo no sistema, é gerado um alarme de “bloqueio de entrada ou saída”. As câmeras posicionadas em ambos os lados das portas são fundamentais para garantir que não ocorram práticas indevidas, além dos procedimentos

de acesso individual, que devem ser informados a todos os usuários do sistema e sinalizados nas portas que contam com este tipo de supervisão.

As áreas lógicas configuradas para monitoramento de entrada e saída este projeto estão descritas na Tabela 5.

Tabela 9 - Definições das áreas existentes

Área	Cômodos relacionados	Requisitos
Área comum	Recepção, corredor, sala de reuniões, escritórios e copa	Qualquer pessoa que precise acessar o prédio, acesso apenas a áreas de fluxo comum, nível de acesso menos restrito.
Sala controlada 1	Sala controlada 1	Acesso à sala controlada 1, onde podem ser armazenados materiais de valor ou podem ser realizadas atividades confidenciais.
Sala controlada 2	Sala controlada 2	Acesso à sala controlada 2, onde podem ser armazenados materiais de valor ou podem ser realizadas atividades confidenciais.
Sala de controle	Sala de controle	Acesso permanente restrito a poucas pessoas e acesso temporário para técnicos de manutenção e inspeção.

Fonte: Elaborado pelo autor.

Além dos eventos de alarmes envolvendo o controle de acesso, também existem os alarmes ativos, causados pelo acionamento de algum sensor no momento em que não esteja inibido. O sistema projetado conta com alarmes de intrusão detectadas pelo sensor infravermelho, presença detectada pelo sensor de movimento quando a contagem de pessoas na área em questão for zero e também desalinhamento dos sensores magnéticos de detecção posicionados nas janelas para detectar aberturas indevidas.

5.5 CÔMODOS E POSICIONAMENTO DOS DISPOSITIVOS

Para cada área delimitada no projeto é aplicado um nível de segurança diferente, variando os níveis de acesso, dispositivos instalados e cobertura por câmeras, seguindo as demandas de segurança e riscos assumidos para cada local.

5.5.1 Recepção

A fim de facilitar o controle sobre o fluxo de pessoas, o ambiente possui apenas uma entrada e saída, reduzindo a necessidade de novos pontos de controle de acesso e monitoramento intensivo. A recepção conta com um par de leitoras de crachá, de

forma que para entrar no ambiente é necessária a combinação de um crachá com acesso à área permitido e também uma senha de 4 dígitos que apenas o dono do crachá possui ciência, combinando então duas camadas de segurança para acesso ao local, algo que apenas o portador do crachá saiba (além da efetiva posse do crachá).

Para saída, não é vantajosa a dupla autenticação, pois além do visitante já ter validado a senha na entrada, realizar o mesmo procedimento na saída pode causar congestionamento em horários de alto fluxo no local. A porta ainda conta com suporte de câmeras para monitorar entrada e saída, além de um sensor de presença posicionado de forma a cobrir a recepção, parte do corredor principal e saída de banheiros e sala de reuniões. Por ser uma área com alta quantidade de acessos, a sirene foi posicionada próxima à porta para enfatizar que o evento foi disparado nesta.

5.5.2 Salas controladas 1 e 2

Contam com sistema de controle de acesso similar ao da recepção, podendo ser utilizadas como estoques com acesso restrito a apenas algumas pessoas ou até mesmo como escritórios privativos de segurança elevada. Contam com monitoramento de câmeras tanto na entrada quanto na saída e detecção de intrusão nas janelas. Já a área externa para as janelas destas duas salas conta com um sistema de detecção de intrusão por infravermelho acima do muro, de forma que qualquer tentativa de invasão pelas janelas possui duas camadas de identificação antes que seja possível acessar o ambiente.

5.5.3 Sala de controle

Concentra o painel central com as placas de controle do sistema de segurança, que integram os cabeamentos de sensoriamento e acionamento de todos os dispositivos instalados, além de abrigar o *switch* que recebe os sinais de todas as câmeras instaladas e também o gravador de vídeo que armazena as imagens. Por ser uma sala crítica, de onde é possível desativar ou sabotar todo o sistema de segurança instalado, conta com um controle de acesso permanente que deve ser restrito a poucas pessoas, com a possibilidade de acessos temporários para técnicos de manutenção ou inspeções periódicas. Além do controle de acesso, conta com câmeras monitorando entrada e saída do local, além de um sensor de presença dedicado à

sala e um sensor de contato magnético para monitorar a abertura da janela. Assim como nas salas controladas, a área externa possui um sensor de infravermelho ativo instalado para detectar tentativas de intrusão pelo muro.

5.5.4 Escritórios, copa e sala de reuniões

Consideradas como áreas comuns, não contam com sistema de controle de acesso, apenas com monitoramento com câmeras e sensores de contato para intrusão nas janelas. Dessa forma, qualquer pessoa com acesso liberado à única entrada do prédio poderá utilizar estes cômodos.

5.5.5 Corredor principal

Por ser uma área de grande circulação e com acesso a todas as salas, conta com duas câmeras nas extremidades, além de um detector de presença posicionado no corredor, a fim de detectar qualquer possível intrusão por meio de telhado ou solo antes que seja realizado o acesso a qualquer área crítica.

6. CONCLUSÃO

Partindo dos sistemas de controle de acesso e posteriormente passando aos dispositivos de detecção de intrusão, além das tecnologias de imagem para monitoramento, observou-se como estão presentes as áreas eletrônica, elétrica e de computação na segurança, tornando acessíveis sistemas de segurança para diferentes aplicações. Reduz-se, assim, a presença humana e os riscos, além de tornar viável a aplicação de sistemas de segurança funcionais sem altos investimentos. Verificou-se a importância da aplicação de pelo menos 2 (dois) tipos de validação de acesso, às possibilidades de monitoramento do trânsito de pessoas em áreas críticas e diversas tecnologias, como cartões inteligentes, *tags* RFID e validações biométricas para solucionar este problema. Também foi abordada a importância de detecção de intrusão no perímetro de uma área protegida por meio de sensoramento, seja por meio de infravermelhos, ultrassom ou até mesmo captação de perturbações mecânicas. Foram detalhados os mecanismos que permitem com que fotorreceptores captem uma imagem real e armazene em dispositivos de memória, a fim de monitorar, registrar eventos e até mesmo utilizar a inteligência artificial para interpretação automática em tempo real das imagens captadas. Por fim, desenvolveu-se um projeto com aplicação prática dos métodos e tecnologias abordados no trabalho, detalhando a instalação, aplicações, posicionamento e custo benefício de cada um dos equipamentos. Concluiu-se que para construir um sistema eletrônico de segurança confiável é necessário analisar o contexto de cada projeto para tirar o maior proveito das tecnologias disponíveis, focando os recursos nos pontos de maior risco e explorando soluções de baixo custo para áreas menos críticas.

REFERÊNCIAS

- AGARWAL, T. **What is an IR Sensor: Circuit Diagram & It's Working**. **ELPROCUS**, 2013. Disponível em: <<https://www.elprocus.com/infrared-ir-sensor-circuit-and-working/#comment-250362>>. Acesso em: 10 maio. 2021
- ALAOUI, M. *et al.* **IRIS RECOGNITION**. Marrakesh: IEEE, 2002.
- ANDOLFATO, Rodrigo *et al.* **Extensometria Básica**. 1. ed. Ilha Solteira: UNESP, 2004.
- ASTRATH, Nelson *et al.* Princípios de gravação magnética e registro de som em fios. **Revista brasileira do ensino de física**, v. 1, n. 1, 2019.
- BENADJILA, Ryad *et al.* The Lab Embedded ISO7816 Analyzer A Custom Smart-card Reader for the ChipWhisperer. **SSTI**, v. 2, n. 1, 2019.
- BHATTACHARYYA, Shuvra; KISACANIN, Branislav; CHAI, Sek. **Embedded Computer Vision: Advances in Pattern Recognition**. 18. ed. London: Springer, 2009.
- BOVIK, Al. **The Essential Guide to Image Processing**. Burlington: Elsevier, 2009.
- BRAGA, N. C. **Sensores magnéticos de alarmes (ART265)**. Disponível em: <https://www.newtonbraga.com.br/index.php/como-funciona/1796-art265.html>. Acesso em: 03 set. 2021.
- BRITTO, Rodrigo; GARCIA, Dorotéa. Análise da Aquisição do Sinal de um Sensor Infravermelho Passivo-PIR. **Unisanta Science and Technology**, v. 9, n. 1, 2020.
- CAMPERI, A. **How to use a PIR Sensor**. **Kisi Academy**, 2021. Disponível em: <<https://www.getkisi.com/academy/lessons/how-to-use-a-pir-sensor>>. Acesso em: 5 nov. 2021
- DUBEY, Neelesh *et al.* HAND GEOMETRY: A New Method for Biometric Recognition. **International Journal of Soft Computing and Engineering (IJSCE)**, v. 2, n. 2231-2307, 2013.
- FERREIRA, D.; XIMENES, R.; SANTOS, T. Desenvolvimento de um Sistema para Visualização de Obstáculo Utilizando Sensor Ultrassônico. *In*: SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES, 3DC, [s. l.],. **Anais [...]**. [S. l.: s. n.], 2017.
- GUIMARÃES, Anderson; NAKATANI, Alessandro; NETO, Vicente. MEDIÇÃO COM SENSOR ULTRASSÔNICO HC-SR04. *In*: 3RD INTERNATIONAL CONGRESS ON MECHANICAL METROLOGY (3RD CIMMEC), 2014, Gramado. **3rd International Congress on Mechanical Metrology (3rd CIMMEC)**. [S. l.: s. n.].
- HAMMACK, Bill *et al.* **Eight Amazing Engineering Stories: Using Elements to Create Extraordinary Technologies**. 1. ed. rev. Urbana: Articulate Noise Books, 2012.

HOSSAIN, Akram; RASHID, Muhammad. Pyroelectric Detectors and Their Applications. **IEEE Transactions on Industry Applications**, v. 27, n. 5, 1991.

HSU, D. **Fingerprint Sensor Technology And Security Requirements** (D. HSU, Ed.) **Semiconductor Engineering**, 3 nov. 2016. Disponível em: <<https://semiengineering.com/fingerprint-senor-technology-and-security-requirements/>>. Acesso em: 17 out. 2021

HUNT, Daniel; PUGLIA, Albert; PUGLIA, Mike. **RFID - A guide to Radio Frequency Identification**. New Jersey: Wiley, 2007.

KEUNING, Jeroen; PUTTE, Ton van der. **Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned**. Boston: IFIP International Federation for Information Processing, 2001.

KUMAR, Ram. **GRAVADOR DE CARTÕES MAGNÉTICOS ISO**. 2019. Dissertação de Mestrado — Universidade Nova de Lisboa, Lisboa, 2019.

LIU, Simon; SILVERMAN, Mark. A Practical Guide to Biometric Security Technology. **IEE**, v. Security, n. 1, 2001.

MAYNES, Keith; MARKANTONAKIS, Konstantinos. **Smart Cards, Tokens, Security and Applications**. Egham: Springer, 2017.

MOREIRA, Benjamin; FILHO, Pedro. NOVO SENSOR DE PRESENÇA PARA ACIONAMENTO AUTOMÁTICO DE LUMINÁRIAS. *In*: CONGRESSO TÉCNICO CIENTÍFICO DA ENGENHARIA E DA AGRONOMIA, 2022, Foz do Iguaçu. **Congresso Técnico Científico da Engenharia e da Agronomia**. [S. l.: s. n.].

MORGAN, E. **HCSR04 Ultrasonic Sensor**, 16 nov. 2014. Disponível em: <<https://kysungheo.com/wp-content/uploads/2022/03/HC-SR04-ETC.pdf>>

NORMAN, Thomas. **Integrated Security Systems Design**. Burlington: Elsevier, 2007.

PERES, Marcelo *et al.* **Guia do CFTV: Curso básico**. 1. ed. rev. [S. l.]: ACADEMIA, 2006.

PURPURA, Philip. **Security, an introduction**. New York: CRC, 2011.

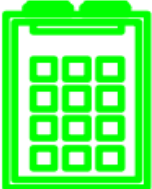
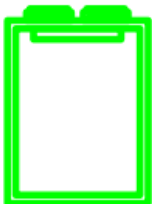
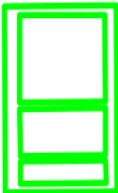
RANKL, Wolfgang. **Smart Card Applications - Design models for using and programming smart cards**. Chichester: Wiley, 2007.

SLADE, Paul. **Electrical Contacts - Principles and Applications**. 2. ed. Boca Raton: CRC Press, 2014.

VARCHOL, Peter; LEVICKÝ, Dušan. Using of Hand Geometry in Biometric Security Systems. **Radioengineering**, v. 16, n. 4, 2007.

ZUFFANELLI, S. **Antenna design solutions for RFID tags based on metamaterial-inspired resonators and other resonant structures**. Cham: Springer, Cop, 2018.

APÊNDICE A – LEGENDA DO PROJETO

Dispositivo	Descrição
	Leitora de crachás por RFID com teclado numérico para senha: Realiza a dupla autenticação para entrada no ambiente e comunica-se com as placas controladoras para validar o nível de acesso e permitir a desmagnetização do ímã para abrir a porta.
	Leitora de crachás por RFID sem teclado numérico: Uma vez que a dupla autenticação já foi realizada na entrada, não é necessário que seja feita novamente na saída, possui a mesma função de controle e validação da leitora com teclado, porém apenas a aproximação do crachá já é suficiente para validação.
	Ímã para fechamento de portas: É conectado à placa controladora, que envia o comando para que seja desmagnetizado em situações de acesso liberado ou acionamento de dispositivo de emergência.
	Botoeira de emergência: Conhecida como “Unidade quebra-vidro”, utilizada para abertura imediata da porta em casos de emergência, desmagnetizando o ímã e liberando o acesso instantaneamente e acionando um alarme de porta forçada, posicionada sempre do lado interno para garantir a segurança do local.
	Sensor de contato magnético: Supervisiona a abertura de portas e janelas, emitindo um alarme caso seja aberto ou desalinhado em tentativas de abertura sem acesso liberado.
	Sensor de presença: Detecta qualquer presença na área monitorada, acusando intrusões por meio do telhado ou subsolo. Geralmente é programado para ser inibido quando alguém está presente no ambiente, as leitoras auxiliam a placa controladora a monitorar a contagem de pessoas na sala e ativa este sensor quando a sala está vazia.
	Sirene de alarme: Integrada com os relés de saída das placas controladoras, é responsável pelo sinal sonoro quando algum sensor de alarme é disparado.



Sensor infravermelho ativo: Responsável pela detecção de intrusão pelo muro, causando um alarme caso alguém cruze a linha de luz infravermelha emitida pelo dispositivo no perímetro do muro.



Câmera IP: Ficam distribuídas por todo o ambiente e posicionadas de acordo com o foco desejado, seja para portas, janelas, visão panorâmica ou periférica. Ficam conectadas a um switch que integra as imagens em um *software* de monitoramento, relacionando-as com o sistema de alarmes.

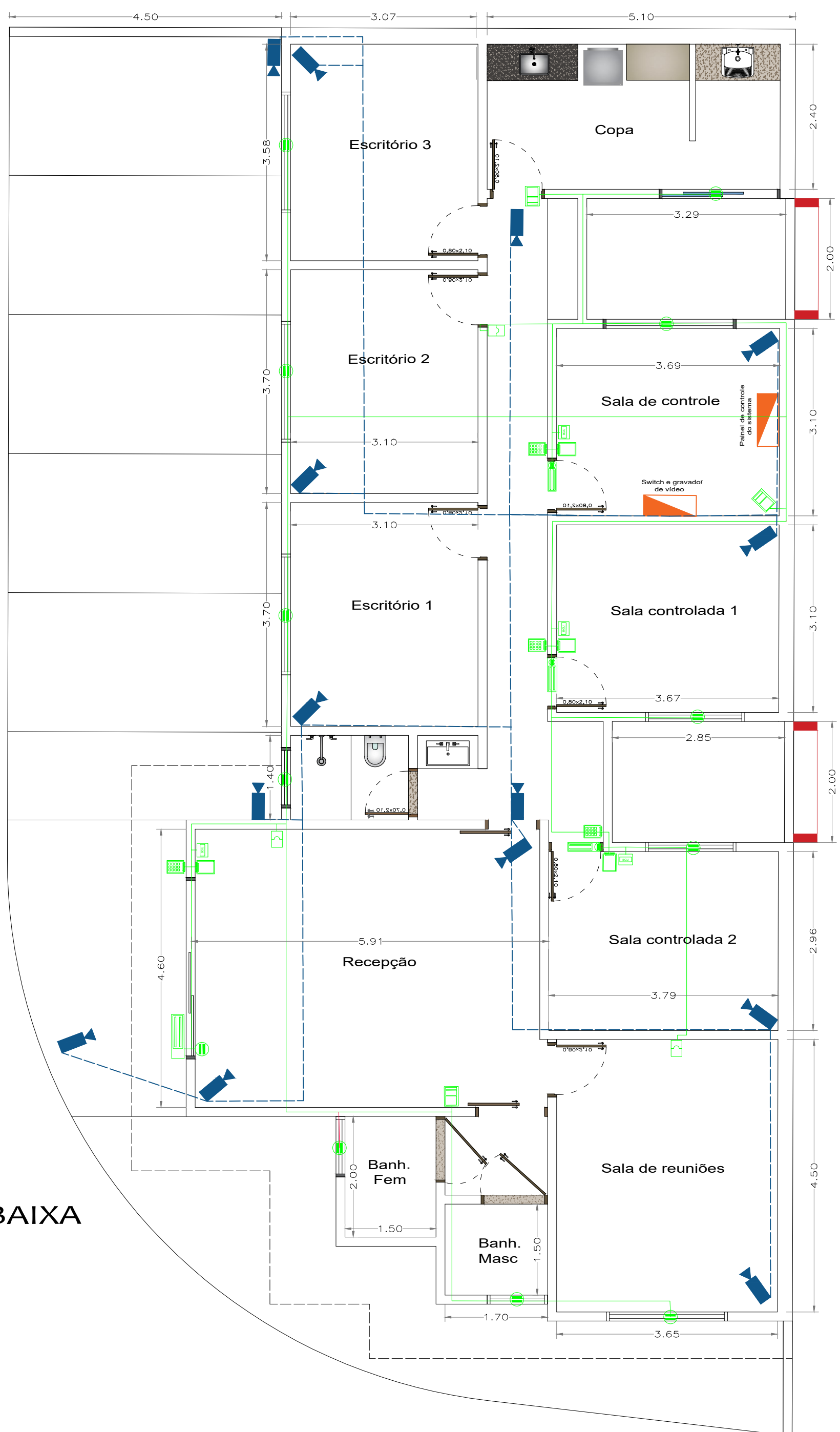


Painel de controle do sistema: Acomoda todas as placas controladoras responsáveis pelo controle de acesso, recepção de sinais de alarme dos sensores e acionamento de relés de ímãs e sirenes de alarme. Este painel deve ficar em uma área segura e monitorada, contando também com uma fonte de alimentação e uma bateria para manter o sistema de segurança funcionando em caso de quedas de energia.



Switch e gravador de vídeo: Painel que recebe todos os sinais de câmera do sistema, integrando todos os cabos com um “switch” e armazenando as imagens pelo tempo desejado por meio de um DVR (Gravador de Vídeo Digital), que pode ser integrado com o sistema de segurança a fim de relacionar as imagens com os eventos de alarmes e sensores.

APÊNDICE B – INSTALAÇÃO DE UM SISTEMA DE SEGURANÇA



PLANTA BAIXA
ESC. S/E