Capítulo I

1. Introdução.

Devido a uma resistência natural a mudanças de hábitos por parte de pessoas mais conservadoras, algumas tecnologias custam a ser assimiladas e por isso podem não ser comercialmente promissoras. Outras são facilmente incorporadas pela sociedade, passando a fazer parte das tarefas cotidianas da população.

Quando esta incorporação é efetivada as tecnologias já não são mais notadas, ou melhor, somente são lembradas com o surgimento de novas necessidades ou quando, por ventura, deixarem de funcionar.

As tecnologias utilizadas para a identificação também passam por este processo, gerando uma sensação de desconfiança inicial como uma reação natural à inovação tecnológica até que gradativamente substituam suas antecessoras e possam ser facilmente utilizadas e assimiladas pela sociedade.

As tecnologias voltadas para a identificação de produtos percorrem um caminho histórico e evolutivo, que compreende desde os códigos de barras até os identificadores por radiofreqüência. Ampliaram sua funcionalidade passando a identificar pessoas, através de biometria e também sendo utilizada em aplicações financeiras por meio da disseminação do uso dos “Smart Cards”.

Estas tecnologias, desde as mais antigas e difundidas até as mais modernas e de pouca difusão, foram e serão assimiladas ao longo do tempo e tornar-se-ão “invisíveis” à medida que cumprirem, satisfatoriamente, suas funções na realização de tarefas rotineiras.

Este trabalho aborda três tecnologias para identificação de objetos que revolucionam a forma como a sociedade realiza diversas tarefas tais como: compra/venda, armazenamento e o transporte de produtos.

Estas tecnologias estão fortemente alinhadas e baseadas a técnicas da computação, que garantem o uso e disseminação através da leitura de códigos de barras, por meio da identificação pela radiofreqüência e do emprego do “Smart Cards” principalmente em movimentações bancárias.

Algumas aplicações voltadas para esta área não apenas requerem a identificação, mas também a autenticação, ou seja, a confirmação dos dados

previamente armazenados. Para isto, lança-se mão de vários mecanismos para ratificação das informações sendo a biometria uma das técnicas.

As tecnologias de identificação abordadas neste trabalho usam componentes de hardware e software que proporcionam segurança e precisão e que impactam as atividades econômicas e sociais da sociedade contemporânea; sendo a principal motivação para o desenvolvimento deste estudo.

Como hipótese principal observa-se que as tecnologias de identificação vieram para transformar culturalmente o modo de vida das pessoas em diversas áreas de atuação. O detalhamento técnico será abordado para esclarecer a dimensão dos limites e recursos computacionais das tecnologias de identificação.

A análise das aplicações de identificação por códigos de barras, radiofreqüência, "Smart Cards" objetiva demonstrar que a evolução tecnológica compreende interseções e complementaridades entre estas tecnologias; de forma a tornar cada uma delas, a tecnologia certa para uma determinada tarefa.

A análise dos impactos positivos e negativos do uso das tecnologias de identificação na sociedade redirecionará os rumos das futuras pesquisas e desenvolvimentos nesta área.

A justificativa deste estudo; como trabalho de fim de curso, é levar novas informações aos discentes do Curso de Ciência da Computação da Universidade Federal de Juiz de Fora, apresentando-lhes as perspectivas tecnológicas que envolvem sistemas de identificação, de forma a motivar o desenvolvimento de pesquisas nessa área de conhecimento.

O trabalho é organizado em capítulos; no capítulo corrente contextualizou-se a motivação e o objetivo do estudo de tecnologias de identificação através de sua importância social. Nos capítulos II, III e IV apresentam-se os aspectos técnicos de identificação por radiofreqüência, "Smart Cards", código de barras e respectivas aplicações e conseqüências para sociedade.

O capítulo V traz uma análise comparativa entre as tecnologias de identificação e um exemplo de caso. O capítulo VI apresenta as considerações finais e perspectivas de continuidade deste trabalho.

Capítulo II

2. RFID - Identificação por Radiofreqüência.

2.1 Breve Histórico.

A maioria das pessoas não imagina o quanto a tecnologia RFID já estava presente nos combates aéreos, entre os pilotos aliados e alemães, durante a 2ª Guerra Mundial.

A Força Aérea da Alemanha utilizou uma forma rudimentar de identificação por radiofreqüência, para ajudar no reconhecimento e não serem confundidos com o inimigo. Pilotos nazistas ao serem captados pelo recém inventado sistema de radar alemão procuravam alterar as imagens na tela do radar atendendo a um pedido via rádio proveniente do solo.

Subseqüentemente houve o desenvolvimento de dispositivos capazes de identificar aeronaves (inimigas ou não) por meio de radar. Tal sistema foi o embrião de todos os IFF, “Identify Friend or Foe” e equipamentos de transponders usados em aeronaves.

Estudos realizados nas décadas de 50 e 60 nos Estados Unidos, Europa e Japão, possibilitaram a utilização da radiofreqüência na identificação remota de objetos.

Na década de 1970, o laboratório nacional de Los Alamos, a pedido do departamento de energia dos EUA, desenvolveu um sistema para rastrear materiais nucleares. Em cada veículo que transportasse esse tipo de material foi colocado um transponder em que seriam armazenados dados de identificação e outros tipos de informações para serem lidas remotamente pelo sistema de Los Alamos.

Na década de 90, foi desenvolvido pela IBM um sistema RFID baseado em UHF, “Ultra High Frequency”, com transferência de dados mais veloz e com maior alcance de leitura. Novas pesquisas continuam a ser desenvolvidas para realizar o rastreamento de itens utilizando de etiquetas de RFID, nas quais um número serial seria gravado em um micro-chip. As figuras abaixo ilustram a evolução dos sistemas de identificação por radiofreqüência.

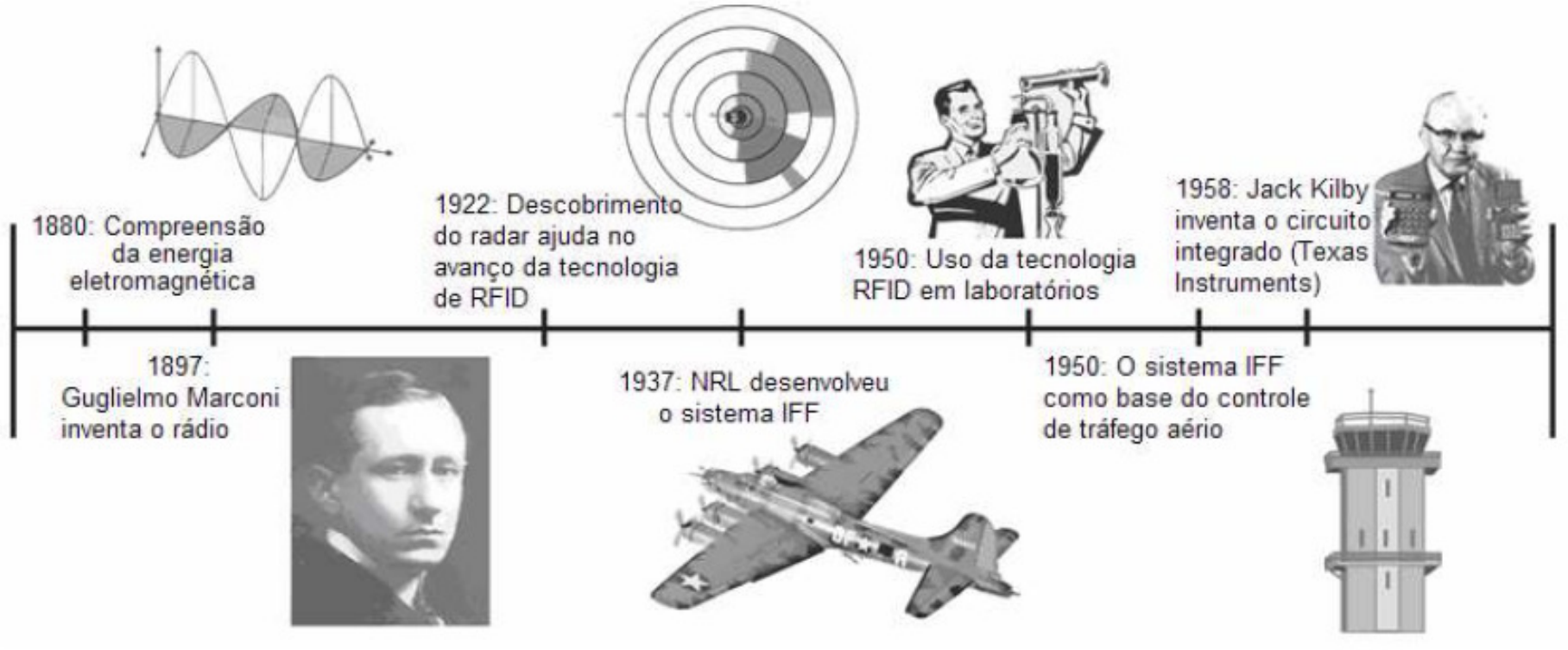


Figura 1 Desenvolvimento dos sistemas de identificação por radiofreqüência [9].

A utilização da energia eletromagnética para comunicação via rádio e no desenvolvimento do radar juntamente com a descoberta do circuito integrado impulsionaram o avanço da tecnologia RFID.

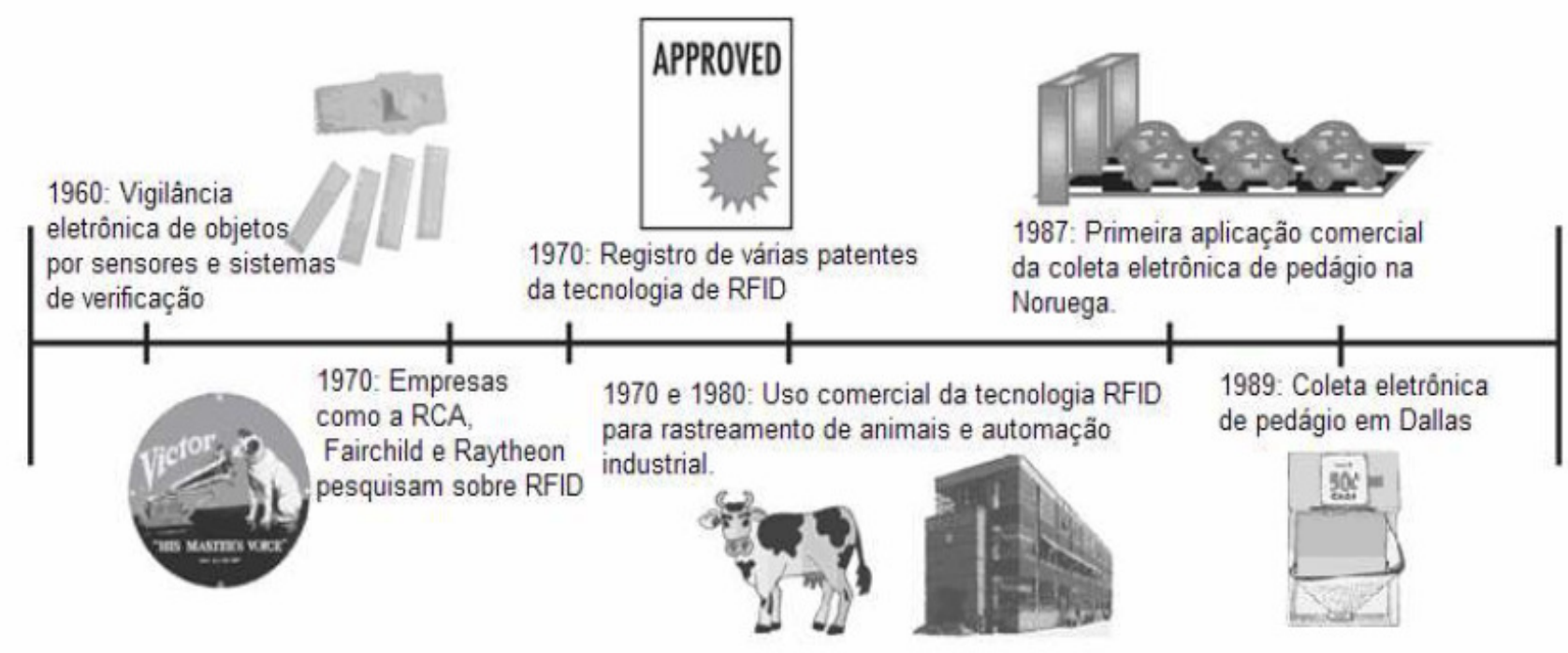


Figura 2 Evolução dos sistemas de identificação por radiofreqüência [9].

Aplicações da tecnologia RFID começaram a ser implementadas na vigilância eletrônica de itens, no rastreamento de animais e produtos e também na coleta eletrônica de pedágio.

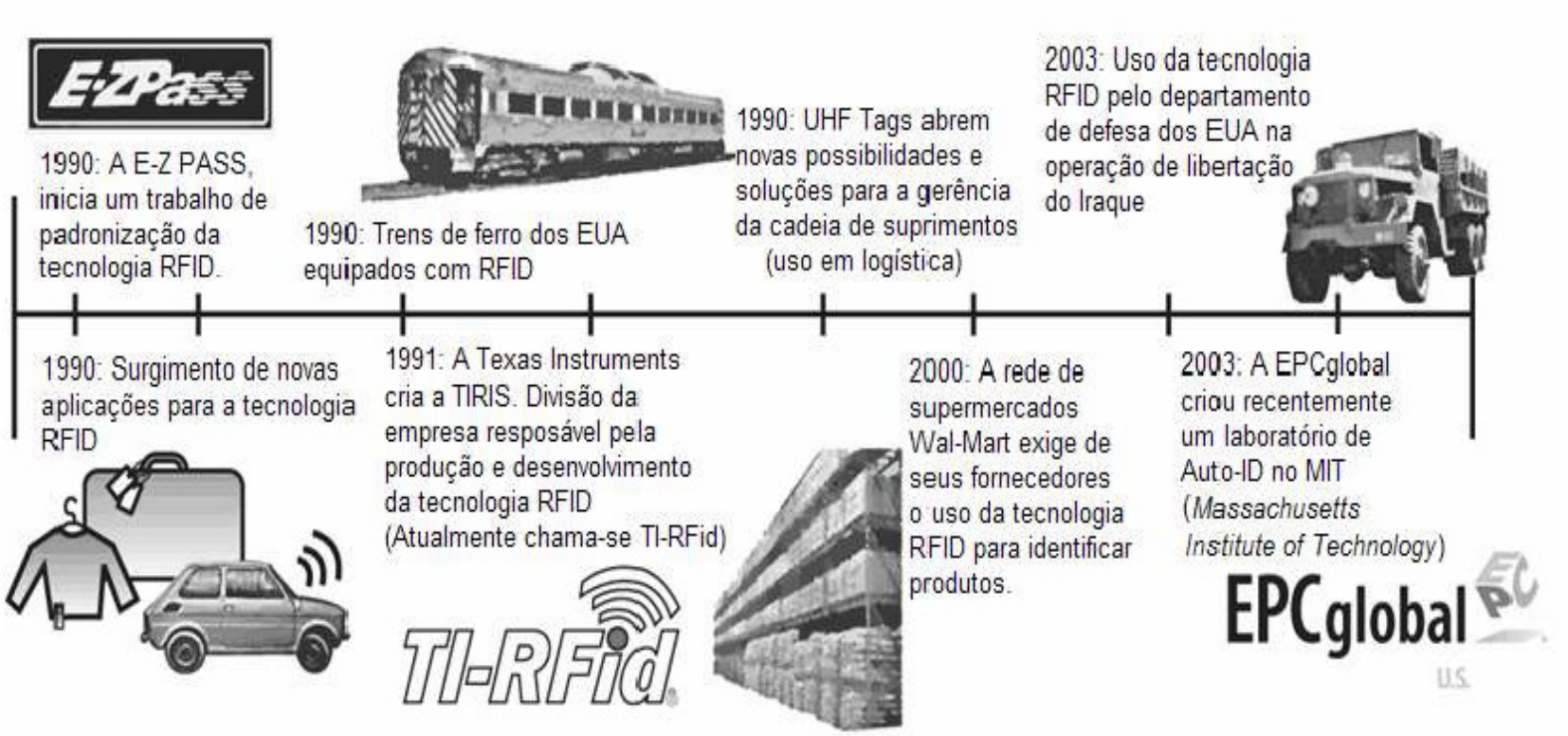


Figura 3 Evolução das aplicações RFID no comércio e na prestação de serviços [9].

Questões quanto à padronização começam a ser levantadas. Novas aplicações são criadas para o controle de veículos, bagagem, itens de vestuário e gerência na cadeia de suprimentos. A rede de supermercados Wal-Mart implanta a tecnologia RFID para a identificação de produtos visando à realização de testes. O Departamento de Defesa dos EUA utiliza RFID na operação de libertação do Iraque.

2.2 Descrição do Sistema RFID.

Um sistema de identificação RFID é basicamente composto por um identificador, um leitor e um software. O identificador (etiqueta inteligente, tag ou transponder) é o dispositivo eletrônico de identificação anexado ao objeto que se deseja rastrear. Este dispositivo pode ou não emitir freqüências de rádio ou variações do campo magnético para ser captado pelo leitor.

O leitor (readers, interrogadores ou transceiver) é um dispositivo que reconhece a presença de identificadores RFID e lê as informações armazenadas neles tratando-os como itens. As informações coletadas pelo leitor devem ser passadas para um computador que utiliza um software para processá-las. Todo este sistema é chamado de middleware RFID; como esquematicamente apresentado na figura 4.

.

Figura 4 Composição Básica de um sistema de identificação de RFID [9].

O dispositivo de leitura emite um campo eletromagnético que sensibiliza os dispositivos de identificação, localizados dentro de sua área de alcance, possibilitando capturar as informações neles armazenadas. Estes dados são transmitidos e processados em um computador remotamente localizado.

2.2.1 Faixas de Freqüência.

Devido ao fato de sistemas RFID produzirem e irradiarem ondas eletromagnéticas, eles são classificados como sistemas de radiofreqüência (RF). Portanto, é necessária a determinação das faixas do espectro de freqüência para que não haja interferências de outros serviços de rádio.

Da mesma forma, o sistema RFID não pode interferir nos sistemas de rádio, celular ou televisão. Na implantação de um sistema de identificação por radiofreqüência, é necessário considerar os espectros de freqüência dos outros sistemas de rádio, pois estes restringem de forma significativa a operação dos sistemas de RFID disponíveis no mercado.

Por esta razão são utilizadas geralmente freqüências que foram reservadas especificamente para aplicações industriais, científicas ou médicas. Tais freqüências são conhecidas como faixa de freqüência ISM, "Industrial-Scientific-Medical" as quais também podem ser utilizadas para aplicações em RFID, conforme apresentado pela figura 5 e pelas tabelas 1 e 2.

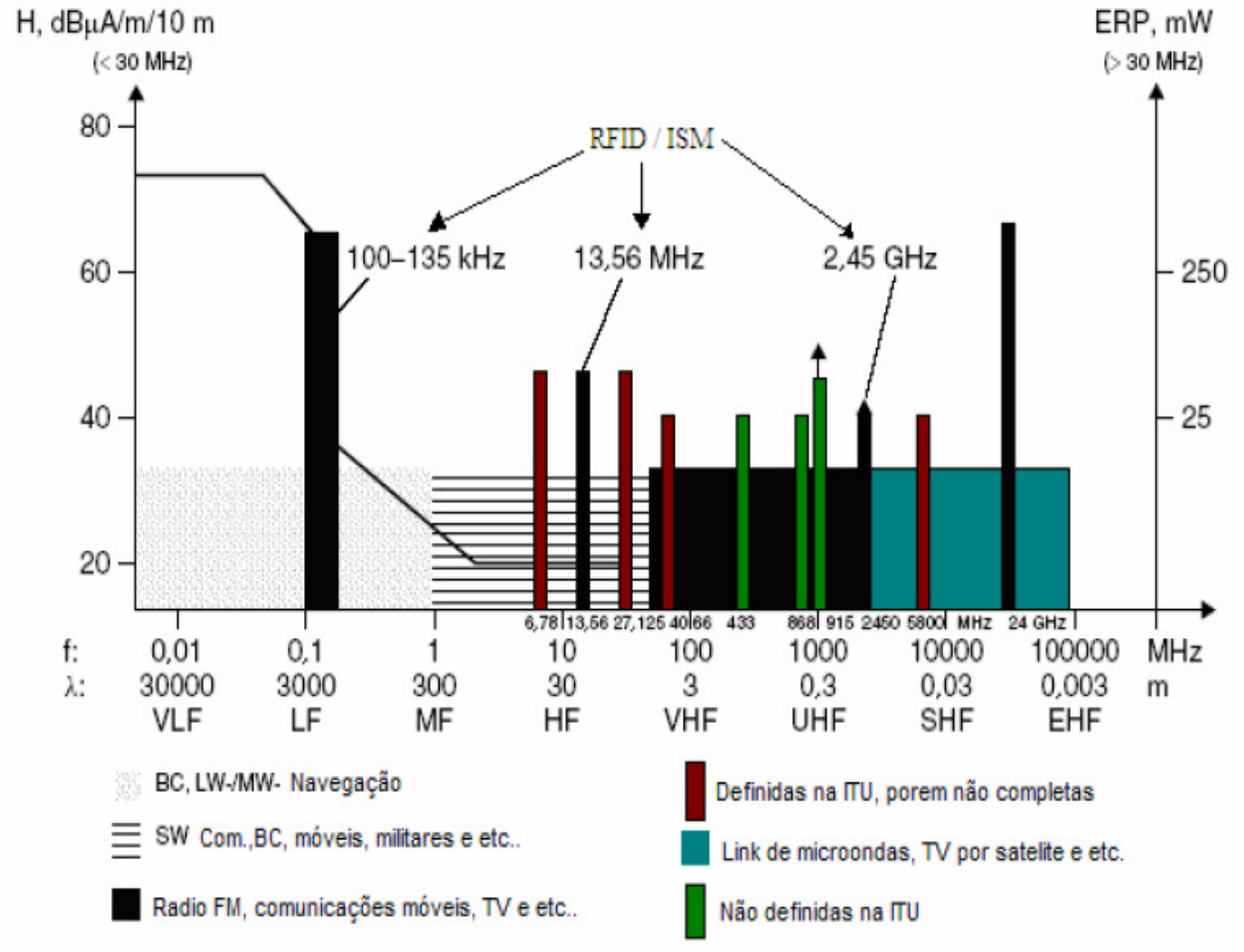


Figura 5 Faixas de freqüências utilizadas por sistemas RFID [9].

Tabela 1 Distribuição das freqüências para sistemas RFID [9].

Freqüência	Descrição
9 a 135 kHz	Low Frequency (LF)
6,78 MHz	ISM Frequency
13,56 MHz	High Frequency (HF)
27,125 MHz	High Frequency (HF)
433,92 MHz	Very High Frequency (VHF)
869 MHz	Ultra High Frequency (UHF)
915 MHz	Ultra High Frequency (UHF)
2,45 GHz	Microondas
5,8 GHz	Microondas
24,125 GHz	Super High Frequency (SHF)

Os sistemas de baixa freqüência (30 kHz a 500 kHz) possuem menor custo e curto alcance para serem utilizados em controles de acesso, identificação de animais ou objetos, rastreabilidade de produtos dentre outros.

Os sistemas de alta freqüência (850 kHz a 2,5 GHz) são utilizados para identificação de objetos em movimento e permitindo maiores distâncias para leitura.

Tabela 2 Faixa máxima típica de leitura por freqüência e aplicações [6].

Freqüência	Faixa máxima típica para identificadores passivos	Algumas aplicações típicas
LF	50 cm	Identificação de animais e leituras próximas de itens com alto conteúdo de água
HF	3 m	Controle de acesso a prédios
UHF	9 m	Caixas e caixotes
Microondas	> 10 m	Identificação de veículos de todos os tipos

Identificadores passivos são aqueles utilizam a energia proveniente do dispositivo de leitura para o seu funcionamento e de acordo com a faixa de freqüência de trabalho são empregados em determinadas aplicações típicas.

2.2.2 Acoplamento.

O mecanismo de acoplamento determina a forma pela qual um circuito no identificador e um circuito do leitor influenciam um ao outro para enviar e receber informações ou energia.

A escolha do mecanismo de acoplamento implica diretamente em qual faixa de leitura o identificador e o leitor irão operar indicando assim a freqüência de trabalho do identificador.

As diferentes faixas de leitura podem ser agrupadas e se classificam como próxima (dentro de 1 cm), remota (de 1cm a 1m) e de faixa longa (mais de 1m), conforme a tabela 3. Acoplamento remoto também é conhecido por "acoplamento de vizinhança".

Os acoplamentos capacitivos e magnéticos são exemplos de acoplamento próximo, o acoplamento indutivo é um tipo de acoplamento remoto e o acoplamento difuso de retorno pode ser remoto ou de faixa longa.

O acoplamento indutivo funciona melhor em LF ou HF. O acoplamento difuso funciona melhor com freqüências mais altas. O acoplamento magnético é mais eficiente de 1 a 10 MHz e o acoplamento capacitivo geralmente é executado em torno de 10 MHz, favorecendo as comunicações e o processamento.

Tabela 3 Resumo das características de aplicação de alguns tipos de acoplamento [6] .

Faixas de leitura	Distâncias	Tipo	Melhor freqüência
Próxima	Dentro de 1cm	Capacitivo Magnético	10 MHz 1 a 10 MHz
Remota	De 1 cm a 1 m	Indutivo Difuso de Retorno	LF ou HF Mais Altas
Faixa Longa	Mais de 1 m	Difuso de Retorno	Mais Altas

Essa tabela mostra de forma resumida as características mais importantes em relação aos tipos de acoplamento.

2.2.3 Identificadores RFID.

É o dispositivo que detém a informação de qualquer item e funciona como uma carteira de identidade. Estão em diversos formatos, conforme a figura 6.

Figura 6 Diversos formatos de um identificador [14].

Os identificadores podem estar inseridos em vários tipos de invólucros ou embalagens de acordo com a necessidade. Podem ser colocados em botões de PVC, frascos de vidro, rótulos de papel, cartões de plástico ou até mesmo em materiais mais resistentes para suportarem à condições adversas.

Possuem diferentes capacidades de armazenamento de informação, podendo variar desde 1 bit até milhares de bytes, conforme as necessidades das aplicações; que vão desde as mais simples, tais como prevenção de furtos até as mais complexas, tais como em uso na linha de montagem de automóveis.

A energia para o identificador se comunicar é proveniente de um campo eletromagnético ou de um pulso de freqüência de rádio emitido pelo leitor quando não é também fornecida por uma bateria junto ao identificador; neste sentido os identificadores podem ser classificados em [6]:

- Passivos, que utilizam a energia proveniente do dispositivo de leitura para o seu funcionamento, conforme a figura 7.

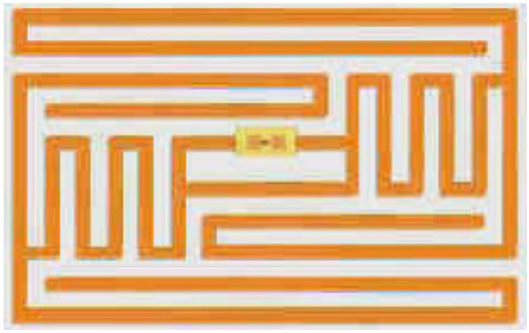


Figura 7 Circuito impresso de um identificador passivo [13].

- Ativos, que fazem uso de fonte de alimentação própria, conforme figura 8.

Figura 8 Exemplo de identificador ativo [13].

- Semi-passivos, que utilizam ambas as formas.

Por possuírem também baixo custo em relação aos demais tipos, os identificadores passivos são os mais comuns sendo largamente empregados em diversas aplicações de sistemas RFID.

2.2.4 Leitores RFID.

Leitores RFID são usados para reconhecer a presença de identificadores RFID dentro de seu raio de ação, conforme figura 9.

Ao transmitir energia RF através de uma ou mais antenas, um identificador próximo capta e a converte em energia elétrica por meio da indução.

Esta energia elétrica é suficiente para energizar o chip semicondutor anexado à antena do identificador, o qual armazena uma identidade. Ao aumentar e diminuir a

resistência da antena, o identificador envia a identidade para o leitor como se fosse um tipo de código Morse.

Outros tipos de identificadores podem trabalhar de forma ligeiramente diferente, porém este é um cenário típico nos quais leitores e identificadores se interagem [6].

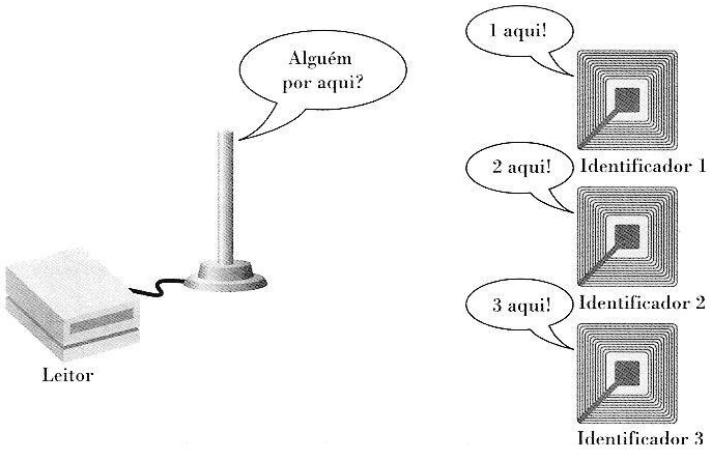


Figura 9 Comunicação entre identificadores RFID e um leitor [6].

Existem leitores RFID em diferentes formas e tamanhos podendo ser fixos ou portáteis, conforme figuras 10 e 11.

Figura 10 Leitor fixo fabricado pela empresa Symbol [13].

Figura 11 Leitor manual fabricado pela empresa Symbol [13].

2.2.5 Antenas.

Realizam a interligação entre os leitores e os identificadores possibilitando a comunicação entre ambos. Normalmente são alimentadas pelo próprio leitor podendo também possuir alimentação própria. Alguns dos vários tipos de antenas são apresentados na figura 12:

Figura 12 Tipos de antenas: A - Desktop ou parede; B - HF; C – Portal [13].

Cada antena destina-se a um uso específico. As antenas Desktop ou de parede são as mais comuns, satisfazendo a maioria das necessidades, uma vez que também podem se agrupar fazendo o papel de antenas de portal.

Uma característica que distingue grandemente as antenas é o seu diagrama de radiação o qual influencia bastante a sua eficiência dependendo do seu modo de utilização [13].

As antenas do tipo Desktop ou de parede possuem um diagrama de radiação lobular como na figura 13, dependendo da polarização utilizada. Obviamente que estes modelos são teóricos e na realidade nunca é perfeito, mas constituem uma aproximação razoável. As antenas captam somente aquilo que estiver na área de abrangência dos lóbulos.

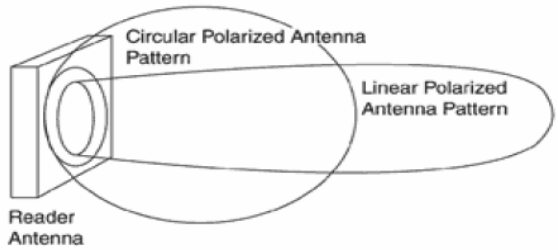


Figura 13 Lóbulos das antenas com polarização linear e circular [13].

Os leitores manuais possuem as próprias antenas incorporadas, normalmente bastante direcionadas, mas dependem das patentes do próprio fabricante, variando sobremaneira de leitor para leitor.

2.2.6 Middleware RFID.

A capacidade de ler milhões de identificadores enquanto eles passam através de uma cadeia de fornecimento e a necessidade de conectar códigos de identificadores a informações significativas, gerará grandes quantidades de dados com inter-relacionamentos complexos.

Um dos principais benefícios do uso de middleware RFID, figura 14, é que ele padroniza as formas de lidar com o fluxo de informação que estes pequenos identificadores produzem.

Além de filtrar eventos, há necessidade também de um mecanismo para se encapsular as aplicações de modo a evitar que elas conheçam os detalhes da infraestrutura física.

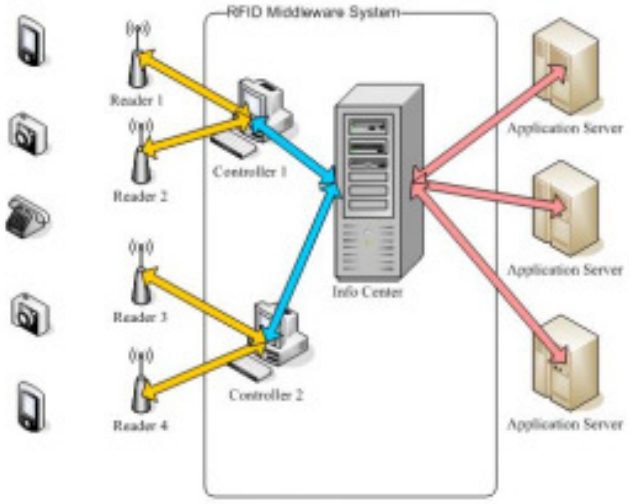


Figura 14 Plataforma de middleware RFID [18].

A fim de que somente as informações relevantes para as aplicações sejam colhidas, existe a necessidade de filtrar, consolidar e transformar observações brutas de leitores RFID, para isso o middleware é impreterível.

RFIDStack, RF²ID, WinRFID, RFID for IBM Websphere e o Sun Java RFID são exemplos de middleware RFID [60].

2.2.7 Padronização e o Código Eletrônico de Produto.

O sucesso da tecnologia RFID está intimamente associado às questões de padronização de seus componentes definindo características de operação e funcionamento de equipamentos para que fabricantes distintos possam produzir dispositivos compatíveis tanto em hardware quanto em software.

Existem muitas soluções proprietárias, mas o que se deseja realmente é que ocorra um esforço conjunto para a padronização de protocolos e regras de utilização visando ao desenvolvimento desta tecnologia.

Algumas organizações como ISO, “International Organization for Standardization”; IEC, “International Engineering Consortium”; EPCglobal que é uma divisão da EAN ,”European Article Number International”; UCC , “Uniform Code Council” e tantas outras estão trabalhando para que isso se torne uma realidade [9].

O EPC, “Electronic Product Code”, ou Código Eletrônico de Produtos é uma forma de identificar itens, conforme a tabela 4, atribuindo a eles um número único que é inserido desde a linha de manufatura e permite que cada companhia faça o rastreamento em sua rede logística dos produtos produzidos até a entrega ao respectivo cliente [9].

A adoção deste sistema como o padrão mundial para a identificação imediata, automática e precisa de qualquer item da cadeia de suprimentos de qualquer empresa, de qualquer setor e em qualquer lugar do mundo é um objetivo desafiador a ser perseguido.

Tabela 4 Tipos de Codificações EPC [6].

Identificador	Nome	Uso Pretendido	Exemplo
SGTIN	Serialized Global Trade Item Number	Rastreamento de itens	Pneus individuais
SSCC	Serial Shipping Container Code	Contêiners de Envio	Um contêiner ISO/intermodal
GLN	Global Location Number	Localizações	Uma antena individual em um depósito
GRAI	Global Retornable Asset Identifier	Itens de biblioteca e aluguel	Um caminhão alugável
GIAI	Global lndividual Asset Identifier	Rastreamento de bens	Uma cadeira de escritório
GID	General Identifier	IDs individuais	Novos esquemas de identificação

2.3 Considerações Finais.

O objetivo deste capítulo foi realizar uma apresentação sucinta a respeito da tecnologia de identificação por radiofreqüência, ou, simplesmente, RFID. Desta forma foi possível a abordagem de vários aspectos como, por exemplo, a conexão entre o identificador e o leitor visando extrair informação realmente útil das inúmeras leituras obtidas.

Como a operação por RFID agrega eficiência, a previsão é de que no futuro tal tecnologia será paulatinamente absorvida pelos mercados. A agilidade dos procedimentos e o incremento no processamento dos dados permitem uma melhor visibilidade dos produtos pertencentes à organização. Isso garante um diagnóstico mais preciso maior lucratividade, menor perda de tempo e mais geração de renda.

Não somente a logística, mas também prestadores de serviços, grandes varejistas e fornecedores perceberão muitas vantagens na instalação de um sistema RFID, entretanto, há ainda um longo caminho para ser percorrido, pois requer que toda a cadeia produtiva e comercial atenda a uma padronização mundial.

Nas Referências Bibliográficas, existem alguns vídeos que traduzem aplicações atuais sobre esta tecnologia como em supermercado [26], na identificação automática de veículos [55], na área da saúde no controle do diabetes [56], em controle de qualidade numa linha de montagem de impressoras [8], em comparação com o código de barras no setor de vestuário [15] e também sobre o Centro de Excelência em RFID da HP [58], localizado em Sorocaba - SP.

Aplicações em sistemas RFID requerem algumas considerações de segurança que são: assegurar a autenticidade das informações armazenadas nos próprios identificadores, assegurar a transmissão de informações entre identificadores e leitores e garantir a segurança geral da aplicação e da infraestrutura.

Há justificadas preocupações quanto à segurança e privacidade com qualquer tipo de tecnologia de identificação e no caso RFID, tem aumentado esse receio entre a população por causa do seu possível impacto sobre a privacidade pessoal.

Há alguma legitimidade nestas preocupações, pois se uma pessoa não autorizada obtiver ou até mesmo alterar informações armazenadas em um identificador RFID seria muito constrangedor no caso de um identificador que não utilize um protocolo seguro e pudesse ser lido por qualquer leitor.

A questão chave para os defensores da privacidade é a possibilidade real de que o rastreamento possa continuar fora de uma determinada loja. Muitos consumidores gostariam de ter quaisquer identificadores RFID desabilitados antes de sair do estabelecimento comercial (tag killing).

Capítulo III

3. “Smart Cards” - Cartões Inteligentes.

3.1 Breve Histórico.

Inicialmente empregado nos Estados Unidos apenas para identificar pessoas e feitos de papel ou papelão os precursores dos “Smart Cards” ganhariam novas funções a partir de sua confecção com PVC - policloreto de vinila. Devido ao baixo custo e a robustez deste material possibilitou-se a produção de cartões mais resistentes e sua utilização desde a década de 50.

Estes cartões ganhariam novas funções tais como servir como credencial de identificação de crédito de seus portadores sendo empregado como mais uma forma de pagamento.

Quase ao mesmo tempo começaram a ocorrer fraudes na utilização dos cartões sendo necessário criar dispositivos de segurança capazes de impedir tal prática nos serviços crediários. Para dificultar a falsificação, o nome do cliente passou a ser aplicado em alto relevo, ou seja, “embossing”. Logo em seguida foi inserido o uso de trilhas magnéticas que permitiam armazenar alguns dados relevantes e houve a criação de um código de acesso para utilização do cartão em máquinas automáticas.

A fragilidade da tecnologia da tarja magnética comprometeu a segurança nas transações, pois o atrito contínuo do cartão com a leitora causava desgaste natural da fita corrompendo as informações gravadas. Além disso, os dados na tarja poderiam ser modificados, apagados, copiados por qualquer pessoa com acesso a uma leitora de cartões com capacidade até mesmo de gerar clones.

Com o progresso da microeletrônica no final da década de 70 foi possível integrar dados e lógica aritmética em um único circuito integrado de silício - “chip”, rodeado de PVC, alcançando um maior grau de segurança na utilização dos cartões como comprovadores de crédito, conforme figura 15.

Os cartões só começaram a ser disponibilizados em escala comercial em 1974 quando na França foram patenteados com o nome de cartões inteligentes, “Smart Cards”. Nesta época, a indústria de componentes eletrônicos já era capaz de fornecer componentes a um preço razoável. Dessa forma, ao se utilizar chips mais poderosos foi

possível armazenar nos cartões dados encriptados com melhores algoritmos de criptografia e ao mesmo tempo restringir o acesso proporcionando assim maior proteção [11].

Figura 15 "Smart Cards" em diversos layouts de chip [19].

3.1.1 Cartões magnéticos.

Por existir uma infraestrutura consolidada para a leitura de cartões magnéticos e por serem de baixíssimo custo, é o tipo mais usado. Durante o período transição de tecnologia os mesmos terminais preparados para lerem "Smart Cards" também foram usados para ler os cartões magnéticos.

A figura 16 apresenta o verso de um cartão com fita magnética que possui uma tarja com três faixas onde as informações são armazenadas, conforme a figura 17. A capacidade e densidade de cada uma delas são mostradas na tabela 5 [22].

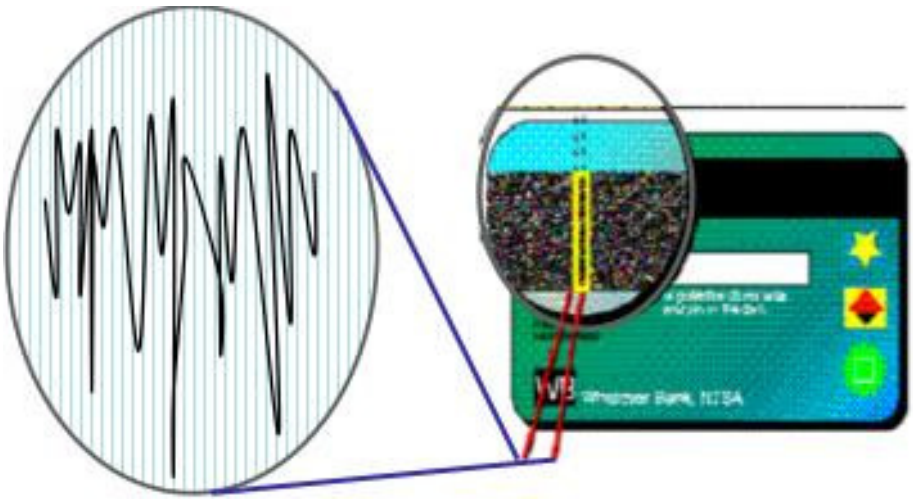


Figura 16 Tarja de um cartão com as partículas magnetizáveis [25].

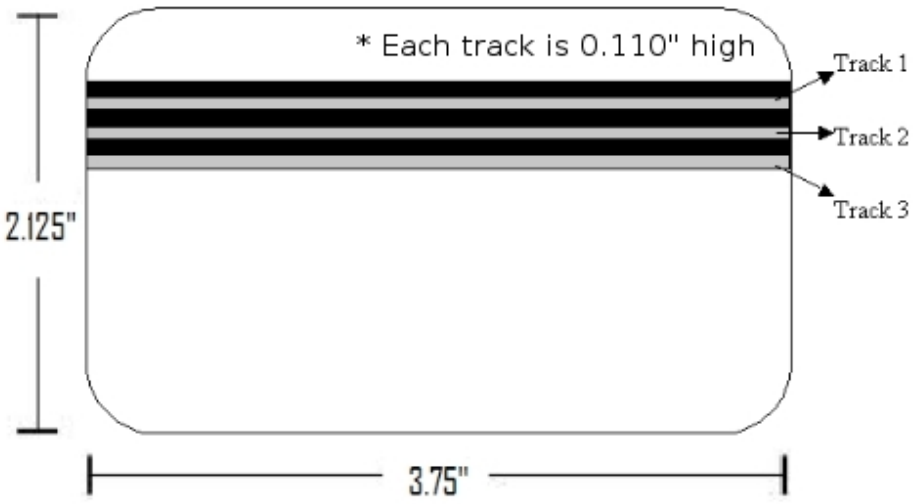


Figura 17 As trilhas de um cartão magnético [24].

Tabela 5 Capacidade e densidade das trilhas da tarja do cartão magnético [22].

	Capacidade	Densidade (bits por polegada)
Faixa 1	79 caracteres	210 bpi
Faixa 2	40 caracteres	75 bpi
Faixa 3	107 caracteres	210 bpi

A leitura das faixas é feita quando o cartão é inserido ou passado em um equipamento que capta os dados gravados. As faixas são de leitura sendo que a faixa três também pode ser de escrita, porém, não é muito utilizada para este fim.

Os cartões magnéticos requerem cuidados redobrados na proteção da tarja magnética, pois um arranhão poderá comprometer a leitura dos dados gravados assim como qualquer exposição a campo magnético eliminam todas as informações existentes.

3.2 “Smart Cards”.

A tecnologia “Smart Card” é representada por um cartão de plástico contendo um chip, conforme a figura 18. Possui uma memória ROM, ”read only memory” onde se encontra o sistema operacional próprio de cada fabricante. Alguns modelos apresentam um microprocessador além da memória.

A capacidade dos cartões varia de alguns bytes até alguns kilobytes, dependendo do chip, do fabricante e do tipo de aplicação. Assemelha-se em forma e tamanho a um cartão de crédito convencional de plástico com tarja magnética [9].

Figura 18 Esquema simples de um “Smart Card” [22].

Além de ser usado em operações bancários e na identificação pessoal, é encontrado também nos celulares GSM, “Global System for Mobile Communications”, conforme figura 19.

Figura 19 Um telefone celular GSM moderno com cartão [20].

Os “Smart Cards” não utilizam fonte de alimentação própria, pois a energia necessária para o seu funcionamento, bem como o relógio de sincronismo para a transmissão de dados, é proveniente do dispositivo de leitura [9].

Possuem uma capacidade de armazenamento maior tendo em vista a disponibilidade no mercado de microchips com mais de 256 Kb de memória sendo possível programar mecanismos de segurança de acordo com as exigências específicas para determinada aplicação. Dessa forma os “Smart Cards” detêm mais vantagens se comparados aos cartões magnéticos.

Algumas características dos “Smart Cards” tornam interessante sua utilização:

- Podem conter várias aplicações diferentes;
- As transações são feitas de forma off-line;
- O próprio cartão autoriza a transação, uma vez que todas as informações necessárias estão contidas nele;
- Segurança alta com o uso de criptografia na autenticação;
- Dificuldade na duplicação de um cartão (reduz, mas não eliminam fraudes);
- Vida útil longa (10 anos);
- Maior robustez em relação a danos externos.

3.2.1 Classificação dos “Smart Cards”.

Uma classificação de “Smart Cards” de acordo com tipo de arquitetura conforme o chip e o tipo de interface dependendo do método de transmissão são representados pela figura 20.

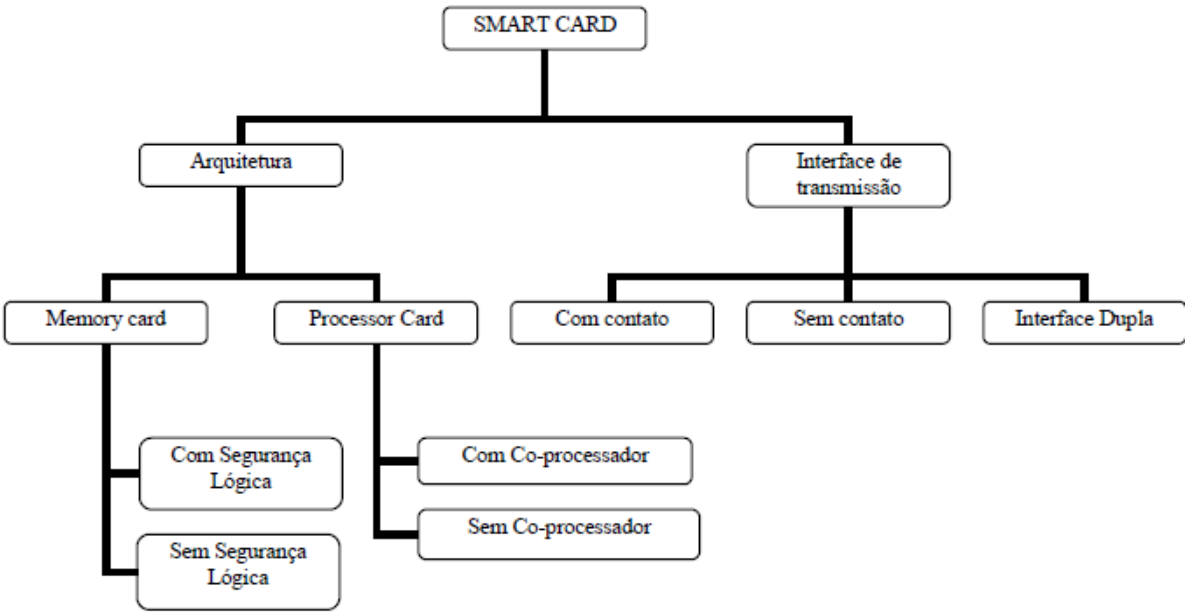


Figura 20 Classificação dos “Smart Cards” [9].

A arquitetura de um “Smart Card” pode ser dos tipos cartão de memória e cartão com microprocessador. O primeiro consiste em cartões de armazenagem de informações e, dependendo da tecnologia empregada, podem ser descartáveis ou reutilizáveis. Os cartões de memória possuem baixo custo de produção e operação, nível de segurança baixo e são utilizados para uma única aplicação simples como telefonia.

O segundo é o "verdadeiro Smart Card", pois contem uma CPU, além da área de memória. Os cartões microprocessados possuem as seguintes características: nível de segurança maior que o cartão de memória; podem ser com contato, sem contato, ou combinados; comporta mais de uma aplicação; e possuem um custo relativamente maior que o cartão contendo apenas memória.

Nos cartões de contato, o acesso aos dados e aplicações do “Smart Card” ocorre através de contato físico com o dispositivo de leitura exigindo que o cartão seja inserido num equipamento, conforme figura 21. Atualmente, seu uso está direcionado a cartões de fidelidade, cartões de crédito dentre outros.

Figura 21 Exemplos de “Smart Cards” com contato sendo utilizado em diversos equipamentos de leitura [28].

O acesso aos dados e aplicações nos cartões sem contato, “contactless” acontece sem contato físico entre o chip e o dispositivo de leitura através de radiofreqüência. São utilizados para aplicações cujas transações devem ser rápidas, como controle de acesso, transporte público e pedágios, conforme figuras 22 e 23.

Figuras 22 e 23 “Smart Card” sem contato sendo utilizado para transporte público no exterior e no Brasil [19] [23].

Os cartões combinados e cartões híbridos possuem os dois tipos de interface conforme figura 24, visando à integração de aplicações de contato e sem contato em um mesmo cartão. A diferença entre eles é que os cartões combinados possuem uma área de memória em comum, enquanto os cartões híbridos têm o mesmo chip.

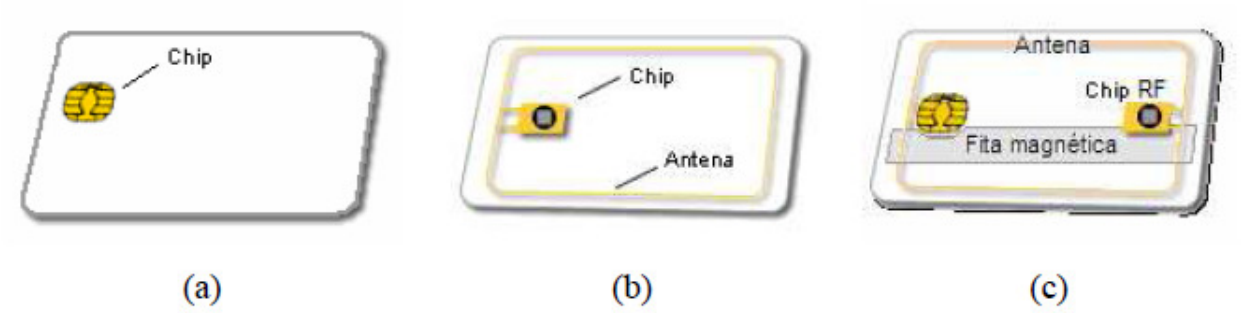


Figura 24 Tipos de Interface dos “Smart Cards”. (a) contato. (b) sem contato. (c) híbrido [9].

3.3 Padronização ISO, “International Organization for Standardization”.

O tamanho do cartão é determinado pelo padrão internacional ISO 7816. Este padrão define também as características físicas do plástico, incluindo faixa de temperatura, flexibilidade do cartão, posição dos contatos elétricos e como o microchip se comunica com o mundo exterior. As principais normas ISO relativas à padronização dos “Smart Cards” são listadas a seguir [9]:

- ISO 7810: disposição de componentes e dimensões do cartão com contato.
- ISO 7811: partes que o cartão de identificação com contato deve conter.
- ISO 7816-1: tamanho do cartão com contato.
- ISO 7816-2: dimensão e local dos contatos no cartão.
- ISO 7816-3: protocolo de sinais e transmissão do cartão com contato.
- ISO 7816-4: formato dos comandos de acesso ao cartão com contato.
- ISO 10536: regulamentam cartões com acoplamento indutivo para distâncias menores que1 cm.
- ISO 14443: regulamentam cartões com acoplamento indutivo para distâncias menores que10 cm.
- ISO 15693: regulamentam cartões com acoplamento indutivo para distâncias menores que 1 m.

Outra forma de classificação é representada pela figura 25 que mostra a distribuição da família de “Smart Cards” de acordo com o tipo de interface conforme o modo de transmissão e quanto faixa de freqüência empregada.

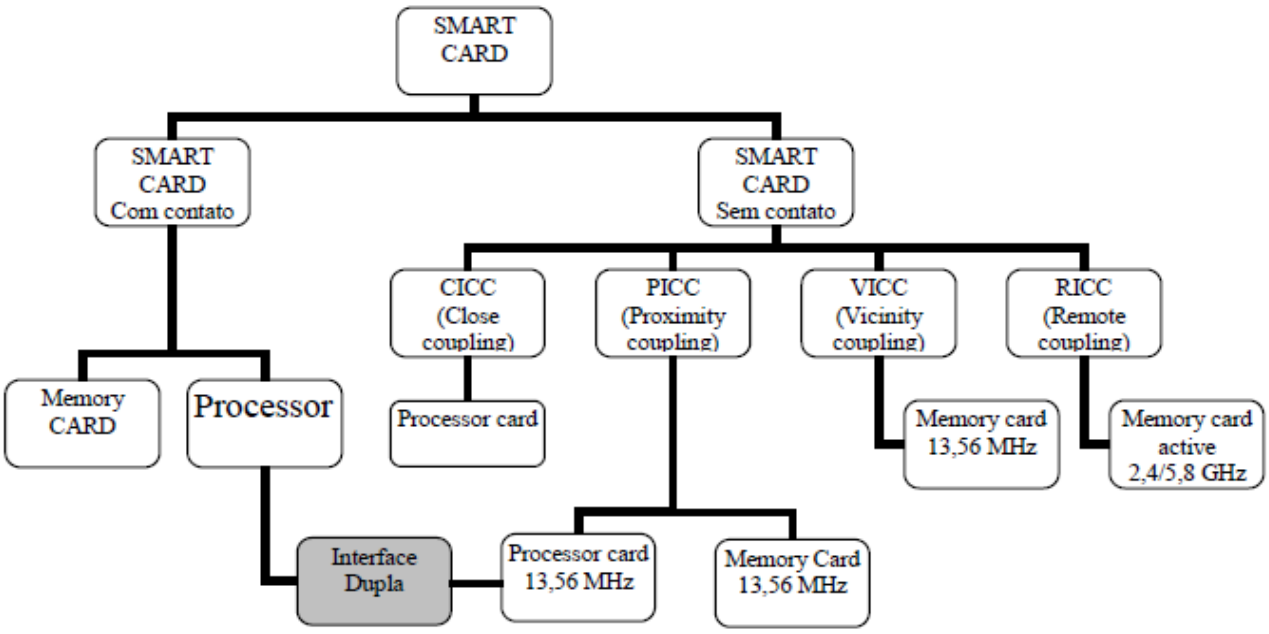


Figura 25 Divisão da família dos “Smart Cards” [9].

3.4 “Smart Card” de contato metálico.

A figura 26 mostra as dimensões de um “Smart Card” de contato metálico conforme a padronização ISO 7816 e ainda regulamenta as seguintes características para o chip:

- 22 mm^2 de área;
- Microprocessador de 8 bits;
- Memória ROM;
- Memória de RAM;
- Memória de armazenamento não-volátil, EEPROM;
- Sistema operacional para rodar e processar os dados de entrada e saída (interno);
- Programas e aplicações (externo);
- Base de dados (externo).

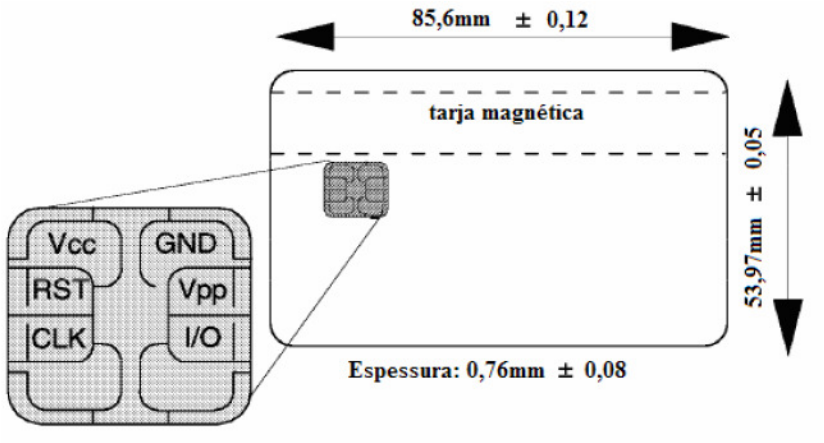


Figura 26 Características físicas do “Smart Card” por contato metálico [9].

A grande maioria dos “Smart Cards” apresenta um módulo com oito contatos metálicos conforme figura 27, sendo que existem módulos com apenas seis.

Figura 27 Módulo com contatos metálicos [22].

As características de operação do chip através dos contatos numerados na figura 27 seguem a seguinte definição:

1. Vcc: a alimentação fornecida pelo dispositivo de leitura, que varia entre + 3v e + 5 v;
2. RST é o pino destinado a efetuar o reset (limpar a memória) no “Smart Card”;
3. CLK é destinado ao sinal de sincronismo (3 MHz a 5 MHz) que é fornecido pelo dispositivo de leitura;
4. Auxiliar 1 : não usado.
5. GND é o ponto de referência ou retorno (terra);
6. Vpp é o pino destinado a escrita na memória EEPROM, “electronic erasable programmable memory”, do “Smart Card”;
7. I/O é a interface serial de entrada e saída responsável pela comunicação de dados do transponder para o dispositivo de leitura e vice versa.
8. Auxiliar 2 : não usado.

3.4.1 Cartão com memória.

A figura 28 mostra o diagrama em blocos de uma arquitetura típica para cartões de contato metálico com segurança lógica e memória. Os dados necessários para a aplicação estão armazenados na memória que geralmente é do tipo EEPROM.

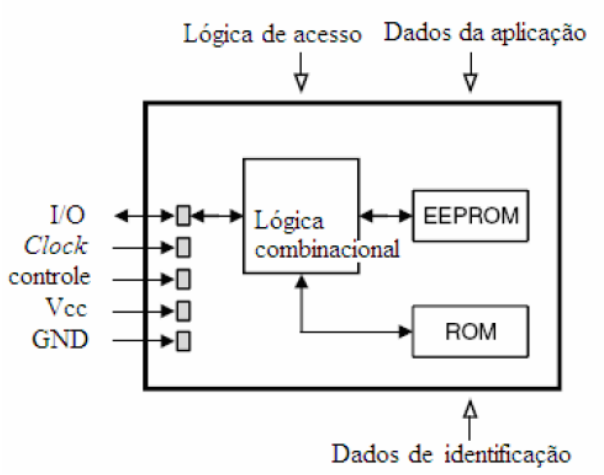


Figura 28 Diagrama de blocos para uma arquitetura típica de cartões com memória por contato metálico [9].

O acesso a memória é controlado por uma lógica de segurança, onde o caso mais simples consiste apenas na proteção para gravar ou apagar os dados da memória.

Há casos em que a lógica de segurança desempenha papel de criptografia, a fim de garantir mais segurança na transmissão dos dados, tanto para leitura quanto para escrita no respectivo bloco de memória do transponder [9].

3.4.2 Cartões microprocessados.

Este tipo de cartão é composto por um microprocessador, uma memória RAM, uma memória ROM e a memória EEPROM. A figura 29 mostra o diagrama de blocos de uma arquitetura típica de um cartão de contato metálico que utiliza microprocessador e memória.

O microprocessador é responsável por gerenciar os demais periféricos por meio de funções a serem executadas de acordo com as entradas que forem fornecidas ao transponder pelo dispositivo de leitura.

A memória ROM é responsável por armazenar o programa que comanda a operação do transponder enquanto a memória RAM, de uso interno do transponder, é

responsável por armazenar resultados e endereços para uso do processador durante o funcionamento do dispositivo.

A memória EEPROM serve para armazenar os dados necessários para a aplicação. Nela é possível ler ou escrever as respectivas informações de acordo com a necessidade e sua capacidade de armazenamento.

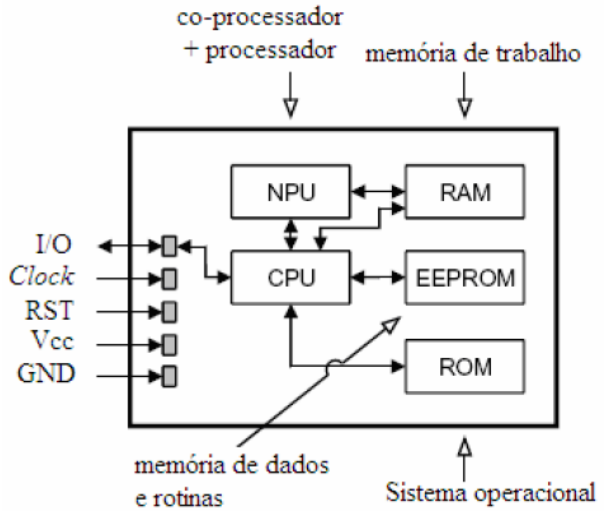


Figura 29 Diagrama de blocos para uma arquitetura típica de cartões com microprocessador por contato metálico [9].

Assim como o cartão com memória, o cartão microprocessado possui a mesma quantidade de pinos na interface. A única diferença está na lógica de entrada que, no cartão de memória, deve receber um sinal de controle e, no cartão microprocessado, a lógica de segurança é toda realizada pelo microprocessador do transponder [9].

3.5 “Smart Card” sem contato.

A figura 30 mostra uma arquitetura típica para “Smart Card” sem contato que em geral utiliza uma memória EEPROM, uma memória ROM e um transmissor de radiofreqüência.

O cartão sem contato possui um transmissor de RF acoplado às portas de entrada e saída do cartão com contato metálico, conforme figuras 30 e 31, não mais havendo a necessidade de contato físico entre o transponder e o dispositivo de leitura.

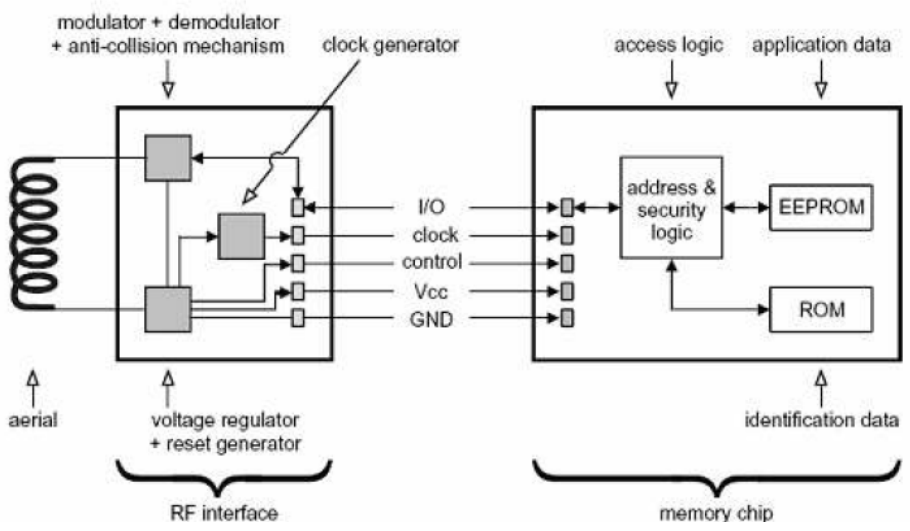


Figura 30 Diagrama de blocos para uma arquitetura típica de "Smart Card" sem contato utilizando lógica de segurança, memória EEPROM e a ROM [9].

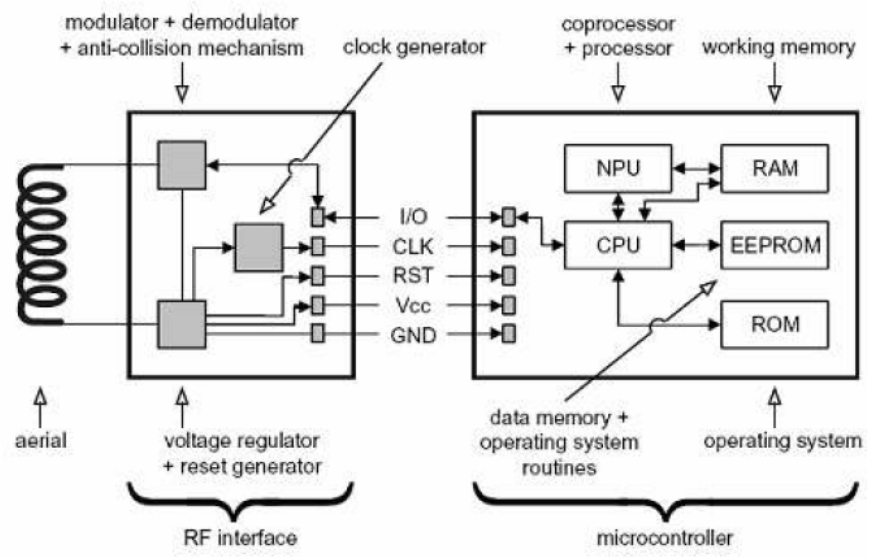


Figura 31 Diagrama de blocos para uma arquitetura típica de "Smart Card" sem contato utilizando microprocessador [9].

A figura 31 mostra a arquitetura típica para um transponder sem contato que utiliza microprocessador. A diferença entre este dispositivo e o da figura 29 está no transmissor de rádio que é acoplado na interface de entrada e saída de dados do transponder.

3.6 “Smart Cards” híbridos.

Os cartões híbridos possuem duas ou mais interfaces para a transmissão e recepção de informações. A transmissão por contato metálico em conjunto com tarja magnética e por meio de radiofreqüência, no caso de sistemas RFID, são as interfaces mais utilizadas.

Encontramos no mesmo “Smart Card” os três tipos de interface de entrada e saída, a tarja magnética, o contato metálico e a transmissão por radiofreqüência. Para o caso de tarja magnética, ao gravar os dados durante a confecção do cartão não mais poderão ser alterados pelo usuário.

A figura 32 mostra o diagrama de blocos de um cartão que não é muito diferente dos cartões apresentados anteriormente, pois somente foi acrescentado um mecanismo para contato físico como dispositivo de leitura. É o sistema híbrido que utiliza a transmissão de radiofreqüência e contato metálico como interfaces de entrada e saída.

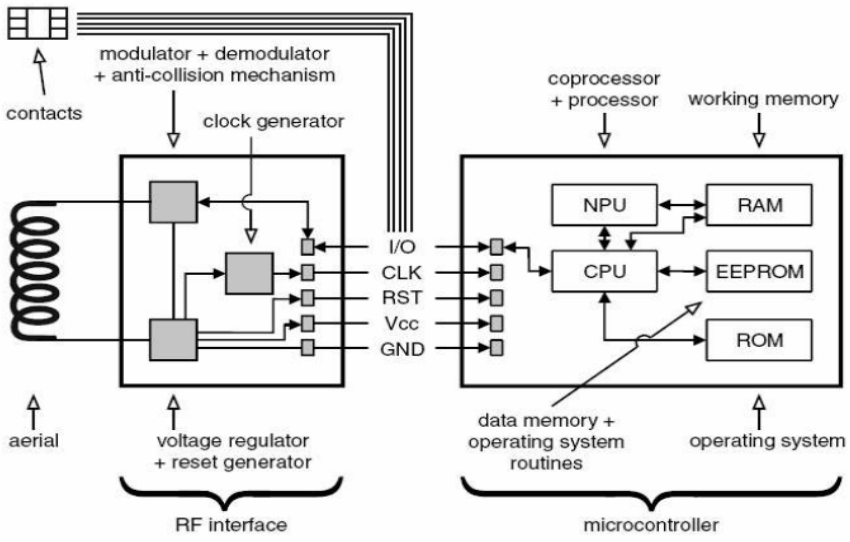


Figura 32 ”Smart Card” híbrido com transmissão de RF e contato metálico [9].

Os cartões híbridos são muito importantes nas fases de transição de uma tecnologia para outra, visto que o custo de substituição de todos os dispositivos de leitura de uma única vez inviabilizaria o uso da nova tecnologia [9].

Está sendo utilizado no mercado brasileiro o cartão com tarja magnética e contato metálico por bancos e outras instituições financeiras. O Banco do Brasil, Visa, Mastercard e o Credicard além de tantos outros estão empregando cartões híbridos para incrementar a segurança e ampliar os serviços ofertados.

3.7 Segurança da tecnologia de “Smart Cards”.

Caracteres em relevo, utilização de senhas, hologramas, micro-impressão, desenhos invisíveis em fibras fluorescentes, assinaturas, algoritmos de criptografia, biometria são algumas formas conjuntas de se trabalhar com os níveis crescentes de segurança quando se trata de cartões inteligentes.

Existem “Smart Cards” do tipo simples bem semelhantes a um cartão magnético até os mais complexos de difícil falsificação. A diferença entre os diversos tipos dependem da forma de funcionamento, preço e nível de segurança que oferecem.

A inserção de senhas em cartões é uma maneira de incrementar a segurança. Em cartões de memória protegidos a informação armazenada somente pode ser acessada após uma senha correta. Caso ultrapasse a quantidade de tentativas incorretas permitidas, o cartão trava e assim os dados armazenados nessas condições se tornam mais seguros do que se estivessem em um cartão de tarja magnética.

Um “Smart Card” roubado é inútil sem a senha de acesso tornando-se mais difícil de ser duplicado que o magnético, porém caso se tenha o conhecimento da senha ainda assim é possível.

A utilização do “Smart Card” tem crescido velozmente, pois conseguem oferecer um nível de segurança alto a um custo razoável por cartão conforme o fabricante.

3.8 Estratégias e técnicas de autenticação de usuários.

Os métodos de autenticação de usuários formam a base dos sistemas de controle de acesso. Mecanismos de autenticação confiáveis são críticos para a segurança de qualquer sistema de informação automatizado. Quando a identidade dos usuários legítimos puder ser verificada com um grau aceitável de certeza são aplicadas técnicas de controle de acesso havendo a liberação aos recursos do sistema em contrapartida são negadas as tentativas sem a devida autenticação.

Várias estratégias de autenticação de usuários estão sendo utilizadas no mercado. Uma prática comum para a questão é o uso da combinação do nome e senha, porém podem ocorrer vários problemas com a autenticação com base neste critério.

Esta maneira de obter a autenticação de um indivíduo é bastante vulnerável, pois se baseia em algo que pode ser copiado, esquecido ou adivinhado por uma pessoa não autorizada e além do mais existem métodos que um intruso pode usar para capturar

senhas como adivinhação da senha, "password guessing*";* ataque do dicionário, "dictionary attack*";* monitoramento do tráfego na rede, "sniffing*";* engenharia social, cavalos-de-tróia e cópia de anotações.

As três categorias de métodos para verificação da identidade de um usuário são baseadas em algo que o usuário sabe tal qual uma senha; algo que o usuário possui tal qual um "token" de autenticação; e alguma característica física do usuário, tal qual a impressão digital ou padrão de voz.

- Autenticação "algo que o usuário sabe", "something you know"**:** Somente a pessoa legítima detem na memória determinada senha ou chave de acesso é o que pressupõe este tipo de autenticação. É utilizada maciçamente em redes, comumente implementada nos próprios servidores e está sujeita a uma grande ameaça caso alguém possa se passar por esta pessoa acarretando prejuízos a segurança.
- Autenticação "algo que o usuário tem", "something you have": O usuário legítimo é a pessoa que porta um determinado dispositivo, cartão ou chave, exatamente como o dono de um carro entra e dá partida por possuir a chave correta. A ameaça em relação à segurança é a de perda deste dispositivo ou a de alguém roubar tal recurso e se passar pelo dono.
- Autenticação "algo que o usuário é", "something you are": Este método baseia-se nas características físicas e biológicas dos indivíduos. Para que funcione realmente bem é essencial a utilização dos dispositivos de reconhecimento biométrico de alto custo. Nos tópicos seguintes serão abordadas questões voltadas sobre este método de autenticação.

3.9 Sistemas Biométricos.

Os sistemas biométricos se baseiam em características fisiológicas e comportamentais de pessoas vivas. As vantagens desses sistemas são que eles não podem ser forjados nem tampouco esquecidos, obrigando que a pessoa a ser autenticada esteja fisicamente presente no ponto de autenticação. A desvantagem reside na falta de padrões, desconforto de usar alguns dispositivos biométricos e custo dos equipamentos extras envolvidos.

Os principais sistemas biométricos utilizados nos dias de hoje são baseados no reconhecimento de face, impressão digital, geometria da mão, íris, retina, padrão de voz, assinatura e ritmo de digitação.

O método de autenticação que parece ser mais interessante para o uso em sistemas biométricos é o reconhecimento de face. Existem dois softwares no mercado que utilizam essa tecnologia, o “TrueFace” e o “FaceIt”, em que uma câmera digital para a captura das imagens é necessário.

Para cada tentativa de acesso a aplicações remotas grava-se uma imagem do usuário para fins de auditoria. Tais sistemas também são capazes de detectar o uso de fotos de usuários autorizados.

Sistemas mais indicados para utilização desktops são os baseados em impressão digital que também funcionam em rede. Outras soluções como o reconhecimento de retina, íris e geometria da mão necessitam de equipamentos extras o que onera o custo de implantação.

Existe uma tendência nos sistemas de identificação para a integração de múltiplos dispositivos biométricos os quais reduzem a possibilidade de fraudes e podem ser usados para superar as limitações individuais. Experimentos utilizando essas técnicas biométricas multimodais obtiveram resultados muito positivos tanto em tempo de resposta, como em precisão.

Uma forma de reduzir custos administrativos associados com a manutenção do banco de dados de modelos para a identificação biométrica é o BioSMART, o primeiro “Smart Card” integrado com um sistema de verificação de impressão digital que fornece um sistema de identificação pessoal portável ao armazenar o modelo do usuário.

3.10 Biometria e “Smart Cards”, uma solução de segurança.

Biometria é mais bem definida como sendo as mensurações fisiológicas e/ou características de comportamento que podem ser utilizadas para verificação de identidade de um indivíduo. Elas são de grande interesse em áreas onde realmente o importante é verificar a real identidade de um usuário [12].

Normalmente, aplicações especializadas de alta segurança empregam essas técnicas. Com o passar do tempo houve uma massificação na utilização desse método de identificação passando a ser encontrado em uma grande e crescente gama de situações do nosso dia a dia. Os principais tipos de dispositivos biométricos são:

- **Scanner de Retina**: Examina os vasos capilares existentes atrás do globo ocular obtendo um contorno distinto e aparentemente mais fácil de ser lido do que uma impressão digital, conforme figuras 33 e 34. Esse dispositivo possui um alto custo sendo utilizado somente em instalações de altíssima segurança.

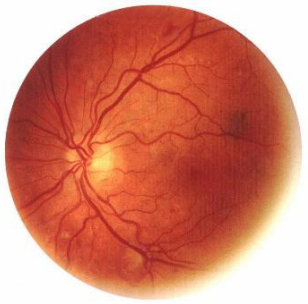


Figura 33 Vasos sangüíneos contidos na retina [29].

Figura 34 Típico scanner de retina [29].

- **Identificação pela leitura da íris**: o indivíduo deve olhar de maneira fixa para um ponto do aparelho enquanto este faz a leitura conforme a figura 35. A identificação pelo olho costuma ser precisa e normalmente é aplicada no controle de acesso a áreas restritas. Trata-se de uma tecnologia cara para ser usada em larga escala.

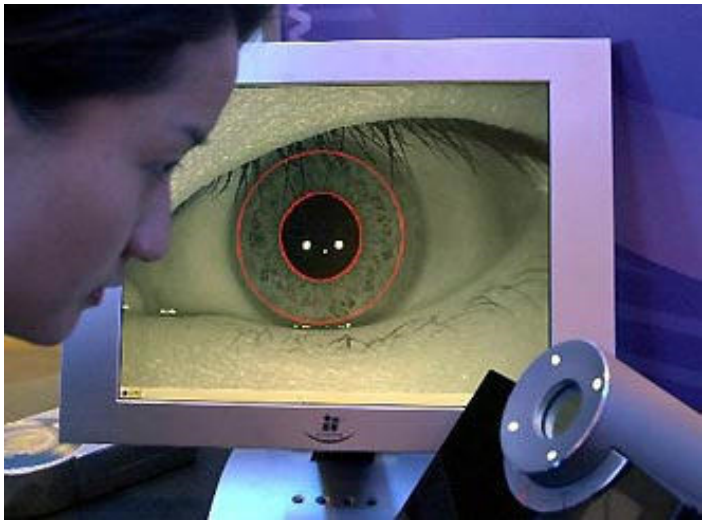


Figura 35 Identificação por leitura da íris [32].

- **Leitores de Impressão Digital**: utilizado com relativo sucesso como forma de identificação policial, nunca foi muito bem sucedido como meio de identificação automatizado conforme figura 36. Existe muita discussão em busca de soluções de menor custo e mais confiáveis.

Figura 36 Leitor de impressão digital [30].

- **Leitores de Impressão Manual**: possuem um menor custo de manutenção, porém não são tão precisos quanto os de impressão digital. Utiliza as dimensões da mão, como o comprimento dos dedos e largura conforme figuras 37 e 38.

Figura 37 Leitor de geometria da mão [31].

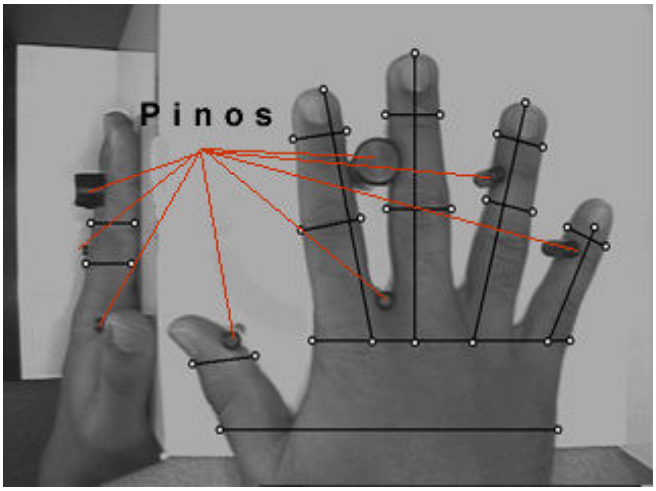


Figura 38 Imagens de perfil e da parte de trás da mão [31].

- **Identificadores de Padrão de Voz**: é possível detectar padrões na freqüência espectral da voz de uma pessoa, conforme a figura 39. São quase tão distintos quanto impressões digitais. A utilização de gravação e possibilidade de alteração nos padrões devido a instabilidade na voz são fatores de risco que comprometem a utilização dessa tecnologia mesmo possuindo um menor custo..

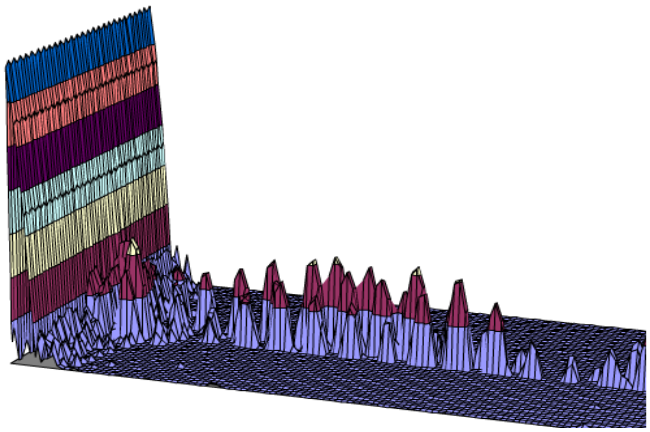


Figura 39 Gráfico de voz [35].

- **Velocidade de Digitação**: a maneira de diferentes pessoas digitarem é bem distinta e experiências foram feitas com identificação baseada em digitação conforme a figura 40. Variações ocasionadas por doenças podem comprometer essa técnica.

Figura 40 Forma de digitação [34].

- **Assinaturas**: maneira clássica de autenticação de pessoas. Reproduzir a habilidade humana de identificar se uma assinatura é efetivamente de uma mesma pessoa é muito complexo, observar a figura 41.

Figura 41 Dispositivo de análise dinâmica de assinatura [33].

- **Reconhecimento de Face**: dispositivos capturam padrões geométricos na face através de uma câmera, com nível razoável de acerto, conforme figura 42. São utilizados em larga escala e possui um baixo custo.

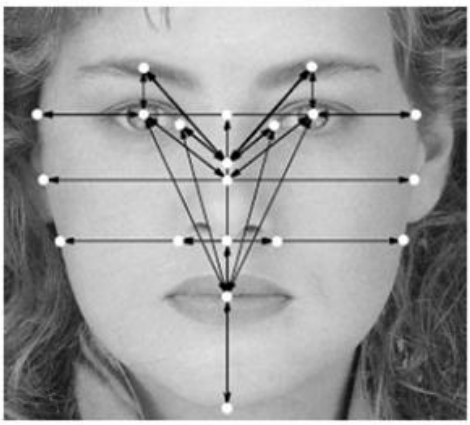


Figura 42 Pontos faciais são utilizados por algoritmos no reconhecimento [28].

Existem duas principais formas de se trabalhar com biometria: a primeira é chamada de captura da imagem biométrica e a segunda de captura de pontos biométricos ou minúcia biométrica.

É necessário obter uma "foto" ou imagem da digital do usuário e armazená-la em um dispositivo. A forma de captura da biometria e os algoritmos aplicados são a grande diferença entre os dois métodos.

No primeiro caso, aplica-se a captura da imagem biométrica ao obter uma imagem da impressão digital do usuário. Essa imagem poderá variar até 70% da imagem original de sua biometria, ou seja, o software de autenticação trabalhará por probabilidades e aproximação da imagem da impressão armazenada.

No segundo caso, aplica-se a captura de pontos biométricos ou minúcia biométrica conforme a figura 43, o software especificará quais são os pontos de biometria que serão utilizados para gerar a identificação do usuário.

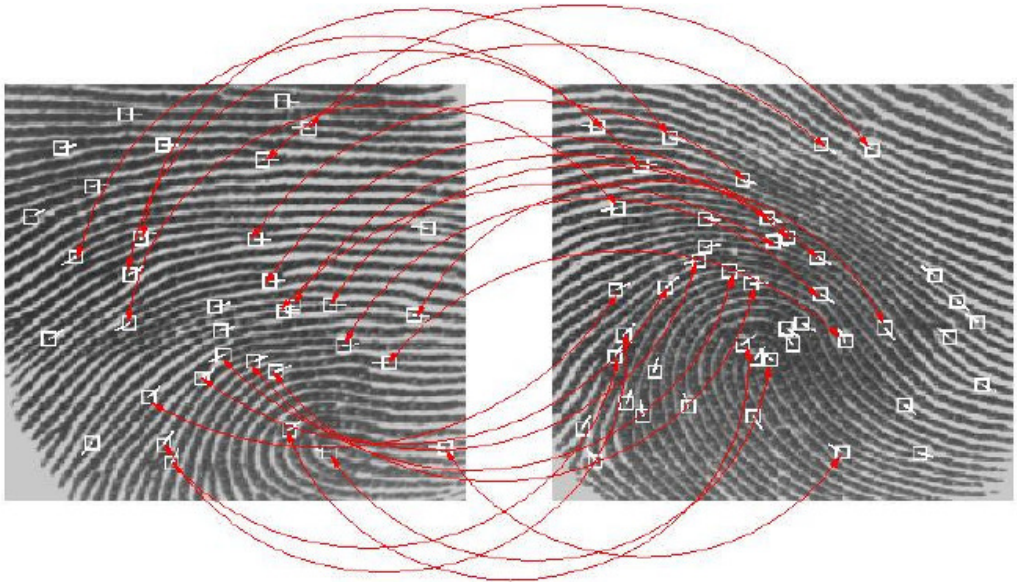


Figura 43 Técnica de comparação de minúcias [36].

Através de um algoritmo matemático tridimensional e gráfico, será possível definir a identidade, mesmo havendo esfolamento. Basta extrair somente as minúcias significativas para composição da identificação.

Ao lidar com uma quantidade maior de usuários em um banco de dados biométricos para autenticação, o processo torna-se lento e inviável para utilização.

3.11 Considerações Finais.

Os “Smart Cards” proporcionam elevado grau de segurança tanto no armazenamento quanto ao acesso aos dados neles inseridos. A informação disponível somente pode ser disponibilizada após passar pelos critérios de segurança já mencionados.

Os cartões inteligentes propiciam portabilidade na movimentação segura de dados tanto no trabalho quanto em domicílio. Dentro de uma organização, o fluxo de informações pode se tornar mais eficiente, ao minimizar o consumo de tempo nas operações. Possibilitam todo o processamento da autenticação sem interferir em outras partes do sistema voltado para as demais aplicações.

Uma vantagem nas aplicações utilizando “Smart Cards” é a característica da EEPROM adicionar ou atualizar as informações armazenadas. O nível de segurança oferecido e a verificação da autenticidade do usuário do sistema são um grande diferencial dessa tecnologia.

Os “Smart Cards” permitem o manejo e controle individualizado das informações neles inseridas de forma segura. Ao combinar tecnologia de fabricação com uma crescente gama de aplicações para o público em geral, é cada vez mais comum sua utilização.

Nas Referências Bibliográficas, existe um vídeo sobre aplicação dessa tecnologia que aborda o novo sistema de identificação a ser implantado no país: o Registro Único de Identificação Civil – RIC [21].

Para a sociedade a utilização desta tecnologia possibilitará a unificação de diversos dados pessoais de identificação em somente um “Smart Card”.

Capítulo IV

4. Código de Barras.

4.1 Breve histórico.

Em 1948 Bernard Silver e Joseph Woodland desenvolveram com base no Código Morse o primeiro código de barras em forma de barras circulares de diferentes espessuras e concêntricas, conforme a figura 44.

Em 1952 foi criado o primeiro leitor de código de barras sendo patenteado em 1958. Somente em 1969 foi desenvolvido um sistema único de identificação de produtos usando a tecnologia de código de barras.

Houve em 1973 nos EUA, a adoção do UPC, “Universal Product Code”, criado por George Laurer, que se baseou nas idéias precursoras de Silver e Woodland.

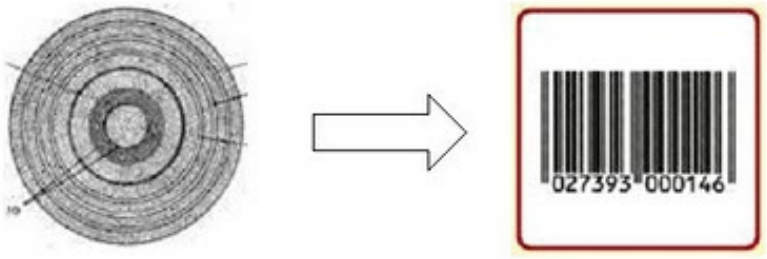


Figura 44 Primeiro Código de barras “bull’s eyes symbol” e sua conversão para o padrão UPC [37].

As mudanças no processo de compra, vendas e estocagem do varejo e da indústria foram constantes e aceleradas a partir da venda do primeiro produto identificado com código de barras nos Estados Unidos em 1974.

Surge em 1977 o EAN – “European Article Numbering System” um sistema único para ser adotado comercialmente por todos os países proposto pela “International Article Numbering Association”, atualmente GS1, uma entidade de âmbito internacional com sede em Bruxelas, na Bélgica.

No Brasil o Decreto nº 90.595, de 29/11/84 da Presidência da República, instituiu como Sistema Nacional de Codificação de Produtos o sistema europeu EAN, conforme consta no Anexo 1 deste trabalho.

4.2 Código de Barras: características e padrões.

É um código binário representado por barras em preto e aberturas em branco arranjadas paralelamente de acordo com um padrão pré-determinado. A seqüência, composta de barras largas e estreitas e de aberturas, pode ser interpretada alfanumérica e numericamente.

Algumas definições encontradas em [39] são importantes para melhor compreender a linguagem usada no estudo dos códigos de barras, conforme a figura 45:

- Barras: representada pela parte escura do código, sendo geralmente preta;
- Espaços: representada pela parte clara do código, em geral, o fundo em que o código está impresso;
- Caractere: cada número ou letra codificado com barras e/ou espaços;
- Caractere inicial ou final: também conhecido como caracteres auxiliar de guarda, é representado por caracteres alfanuméricos ou símbolos especiais, dependendo do tipo de código, indicando ao leitor ótico o início e o fim do código;
- Caractere central: trata-se também de um caractere de guarda, utilizado em alguns códigos de barras para separar o código em lado esquerdo e direito;
- Elemento ou Módulo: representado por uma barra ou espaço mais estreito do código, tendo seu tamanho definido pela densidade do código;
- Zona de silêncio: espaço em branco de tamanho definido, colocado antes do caractere de guarda inicial e depois do caractere de guarda final;
- Densidade: quantidade de caracteres que podem ser codificados por unidade de comprimento.

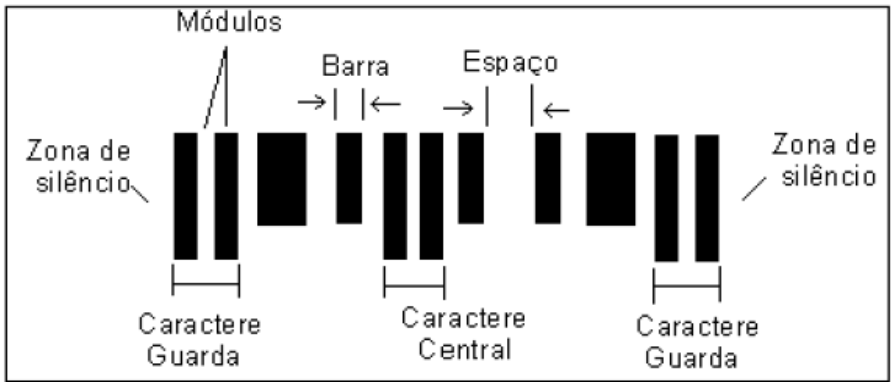


Figura 45 Esquema dos principais elementos de código de barras [39].

A codificação das barras/espaços pode ser feita de duas formas a partir do uso de um código binário e do tipo do código de barras empregado:

- Por largura do módulo: as barras ou espaços estreitos correspondendo ao dígito 0 "zero" e as barras ou espaços largos, ao dígito 1 "um".
- Por refletividade: os espaços refletidos (brancos) correspondendo ao dígito 0 e as barras não refletivas (escuras), ao dígito 1.

Os códigos de barras podem ter seus caracteres formados por um número de barras variável. Na codificação/decodificação quando se consideram os espaços são classificados como discreto caso contrário contínuo.

A leitura é feita pela reflexão diferente de um feixe de laser das barras em preto e das aberturas brancas.

A decodificação do código de barras consiste na conversão das barras e espaços em sinal elétrico proveniente de um leitor de código de barras como, scanner e caneta ótica, conforme a figura 46, traduzindo num caractere correspondente segundo o padrão de código de barras utilizado.

Figura 46 Modelos de diversos leitores a laser de código de barras [40].

A varredura do código de barras por um leitor é iniciada quando um ponto de luz é incidido sobre o código do produto no sentido longitudinal sendo absorvido pelas barras escuras e refletido pelos espaços em branco repassando essa oscilação de sinal ao decodificador, conforme figura 47.

Quanto mais largo for a barra ou o espaço, mais tempo o dispositivo ficará medindo a ausência ou presença de reflexão e, quanto mais fino, menos tempo. Assim o

decodificador compara a variação dos sinais elétricos com os dados de uma tabela interna decodificando o código impresso no produto.

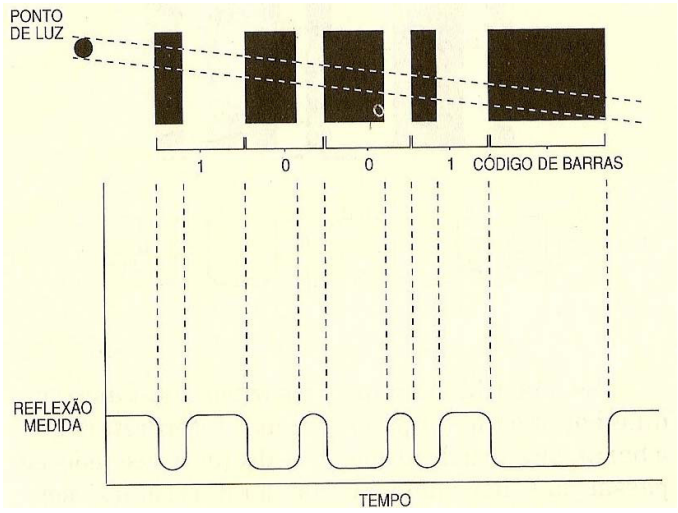


Figura 47 Decodificação de código de barras [39].

Quando houver dígito verificador o leitor ao realizar a varredura refaz os cálculos com base nos outros dígitos do código e compara o valor encontrado com o último dígito de controle detectando erro de leitura se existir.

A característica de leitura bidirecional em códigos de barras está associada com a paridade, ou seja, depende da quantidade de dígito 1 detectada na seqüência da codificação de cada caractere.

Nos códigos UPC e EAN, a paridade de cada seqüência de sete dígitos é determinada segundo as tabelas internas (A, B e C) existente no computador, conforme tabela 6.

Nesse caso, o leitor ao fazer a varredura do código impresso no produto em qualquer uma das direções, se os sinais elétricos lidos apresentarem uma quantidade ímpar de dígitos iguais a 1 ou estar havendo uma alternância nessa quantidade (ora ímpar ora par) significa que a leitura está sendo da esquerda para a direita, mas se apresentar uma quantidade par de dígitos 1, então a leitura ocorre da direita para a esquerda [39].

A paridade no código UPC e EAN somente é possível, porque os caracteres são codificados de maneira diferente quando estão do lado direito ou esquerdo do caractere central [39].

Tabela 6 Verificação de paridade do Código de Barras [39].

DÍGITO	TABELA A ÍMPAR	TABELA B PAR	TABELA C PAR
0	0001101	0100111	1110010
1	0011001	0110011	1100110
2	0010011	0011011	1101100
3	0111101	0100001	1000010
4	0100011	0011101	1011100
5	0110001	0111001	1001110
6	0101111	0000101	1010000
7	0111011	0010001	1000100
8	0110111	0001001	1001000
9	0001011	0010111	1110100

4.3 Código de Barras: tipos, estruturas e funcionamento.

Devido à praticidade, qualidade e rapidez na transmissão de informações proporcionada pelo código de barras, quase sem a necessidade de interferência humana, foram desenvolvidos diversos tipos ou simbologias de códigos, dos quais serão abordados alguns mais utilizados.

4.3.1 Códigos de Barras tipo UPC.

O código UPC (Universal Product Code) foi criado em 1973 nos Estados Unidos para atender aos supermercados e o comércio em geral. Trata-se de um código discreto, numérico e de leitura bidirecional, composto por doze dígitos, cuja distribuição dos dados está apresentada na tabela 7.

Tabela 7 Distribuição de dados no Código de Barras UPC [39].

Prefixo do Sistema	Código do Fabricante	Código do Produto	Dígito de controle
□	□□□□□	□□□□□	□

O prefixo ou número de sistema, localizado à esquerda do código de barras UPC, tem por finalidade caracterizar os tipos de códigos de barras anteriores ao atual, de maneira que se utiliza:

- 0 para os códigos UPC em geral;
- 2 para produtos de peso variável;
- 3 para medicamentos e outros produtos ligados à saúde;
- 4 para códigos sem restrição de marcação na loja;
- 5 para cupons.

Os cincos dígitos posteriores correspondem ao código do fabricante ou empresa, cada qual com seu próprio código estabelecido por um órgão competente. Os outros cinco dígitos, fornecidos pelos próprios fabricantes ou por um órgão responsável, correspondem ao código do item do fabricante e o último dígito é o verificador, usado para dar maior segurança e credibilidade.

No código UPC, a codificação é feita por refletividade, sendo que cada caractere de dado é codificado em sete módulos, de modo que cada módulo ou é uma barra estreita escura (representado pelo dígito 1) ou um espaço estreito em branco (representa pelo dígito 0). Cada barra ou espaço largo pode representar até quatro vezes o valor de um módulo estreito.

Já o caractere de guarda (inicial ou final) é composto por uma seqüência binária de três dígitos (101), o caractere central é composto por uma seqüência de cinco dígitos (01010). No código UPC, assim como no código EAN-13 que será visto mais à frente, é possível perceber que os caracteres de guarda são formados por duas barras e um espaço, cada um dos caracteres de dados se formam a partir de um conjunto de duas barras e dois espaços, ao passo que o caractere central por duas barras e três espaços.

A estrutura do código UPC é composta por caracteres de guarda e de dados, conforme se encontra representado abaixo na tabela 8.

Tabela 8 Estrutura do Código de Barras UPC [39].

Caractere Guarda	Dados (A)	Caractere Central	Dados (C)	Caractere Guarda
▯	▯▯▯▯▯▯	▯	▯▯▯▯▯▯	▯

Observe que na estrutura do código, ocorre a inclusão do primeiro caractere (número de sistema), o qual juntamente com os outros cincos caracteres posteriores são codificados pela tabela A, (vide tabela 6). Os outros seis caracteres restantes, inclusive o

dígito de controle têm sua codificação feita pela tabela C (vide tabela 6), já que estão posicionados à direita do caractere central.

Abaixo conforme figura 48 temos a representação de um código UPC com a codificação de alguns caracteres na parte superior, segundo as tabelas A e C (vide tabela 6) .

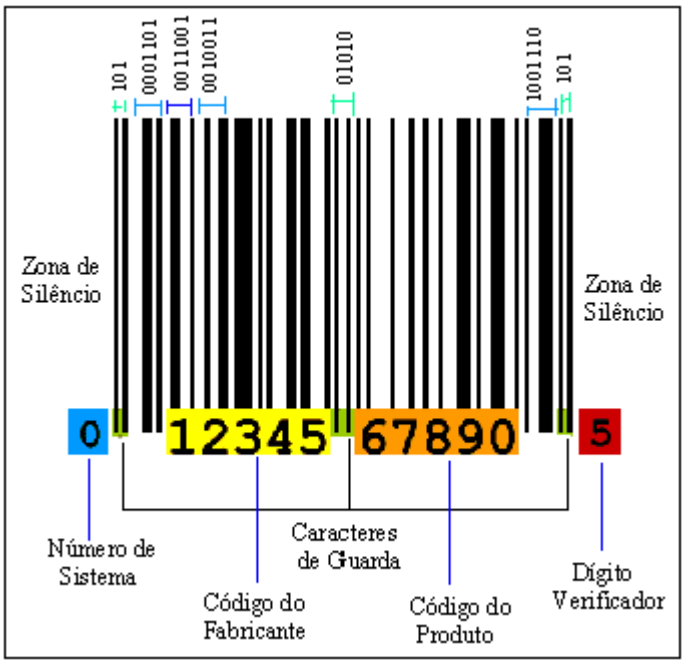


Figura 48 Exemplo de Código de Barras UPC [39].

4.3.2 Código de Barras tipo EAN.

O código EAN (European Article Numbering Association) foi criado em 1977 com base no código UPC e, por isso, apresenta muitas características semelhantes: código discreto, numérico, de leitura bidirecional e codificação por refletividade – o que de certa maneira os tornam compatíveis.

Atualmente, existem duas versões do código EAN:

• EAN-13, composto por treze dígitos e o mais usado internacionalmente;

• EAN-8, uma versão compacta do EAN-13, composto por oito dígitos, restrito às embalagens pequenas (por exemplo, cigarros).

A distribuição dos caracteres de dados que compõe cada uma das versões do código EAN é apresentada conforme a tabela 9.

Tabela 9 Distribuição de dados no Código de Barras EAN [39].

	Prefixo do País	Código do Fabricante	Código do Produto	Dígito de Controle
EAN-13	■■■	■■■■	■■■■■	■
EAN-8	■■■		■■■■	■

Como podemos perceber, no EAN-13, os treze dígitos que compõe o código referem-se a quatro informações: identificação do país (ou região econômica), do fabricante e do produto e, por último, o dígito de controle.

O prefixo do país ou da região econômica, também chamado de bandeira, é determinado pela EAN e conforme a necessidade do país possui dois ou três dígitos, conforme tabela 10.

Tabela 10 Identificação de países ou Regiões Econômicas segundo a EAN [39].

PREFIXO	**PAÍS OU REGIÃO**	**PREFIXO**	**PAÍS OU REGIÃO**	**PREFIXO**	**PAÍS OU REGIÃO**
600 e 601	África do Sul	850	Cuba	750	México
779	Argentina	786	Equador	784	Paraguai
93	Austrália	84	Espanha	775	Peru
789	Brasil	40-44	Germânia	560	Portugal
777	Bolívia	489	Hong Kong	50	Reino Unido
780	Chile	890	Índia	471	Taiwan
690-692	China	899	Indonésia	773	Uruguai
888	Cingapura	80-83	Itália	00-13	EUA e Canadá
770	Colômbia	955	Malásia	759	Venezuela

Quanto à identificação do fabricante, este pode possuir quatro ou cinco dígitos, dependendo da bandeira, e é fornecido pela entidade nacional de cada país (no caso do Brasil, pela ABAC). No caso de empresas com muitos produtos podem ser codificados até cem mil itens diferentes, enquanto que empresas com poucos produtos, até dez mil itens.

Já o código do produto é composto de cinco dígitos e também é fornecido pela entidade nacional responsável. O dígito verificador é calculado de forma semelhante ao do código UPC.

O código EAN-8, diferentemente do EAN-13, não faz referência ao fabricante, desconsiderando o código do mesmo e trabalhando apenas com as outras três informações: bandeira, código do item e dígito de controle, cujo cálculo se dá mesma forma que no EAN-13.

A diferença entre esses dois códigos está no menor número de caracteres de dados e também no processo de codificação dos caracteres, o qual é realizado com o auxílio da tabela 6.

No caso do EAN-13, o primeiro caractere localizado antes do caractere de guarda inicial, não é codificado e dependendo de seu valor, os seis caracteres seguintes a ele, localizados à esquerda do caractere central, serão codificados pela tabela A ou B. Os outros seis dígitos do código, mais o dígito verificador, são codificados pela tabela C conforme a tabela 11 e figura 49.

Tabela 11 Codificação do segundo ao sétimo caractere levando-se em conta o valor do primeiro caractere [39].

DÍGITO INICIAL	CARACTERE					
	2°	3°	4°	5°	6°	7°
0	A	A	A	A	A	A
1	A	A	B	A	B	B
2	A	A	B	B	A	B
3	A	A	B	B	B	A
4	A	B	A	A	B	B
5	A	B	B	A	A	B
6	A	B	B	B	A	A
7	A	B	A	B	A	B
8	A	B	A	B	B	A
9	A	B	B	A	B	A

No código EAN, assim como no código UPC, o caractere de guarda é composto por uma seqüência binária de três dígitos (101), o caractere central é composto por uma seqüência de cinco dígitos (01010), ao passo que os caracteres de dados são constituídos por uma seqüência de sete dígitos.

Figura 49 Exemplo de utilização das tabelas 6 e 11 no código EAN-13 [39].

A seqüência de dígitos 779 representa o número de sistema da Argentina conforme a tabela 10, sendo que o primeiro dígito (sete, no caso) determinará a ordem de codificação dos demais conforme a tabela 11. Assim, para o dígito inicial igual a 7 temos a seguinte ordem para os outros seis caracteres subseqüentes conforme tabela 12 :

Tabela 12 Extrato da codificação do segundo ao sétimo caractere levando-se em conta o valor do primeiro caractere do código EAN-13 [39].

2°	3°	4°	5°	6°	7°
A	B	A	B	A	B

Desta forma, a partir da tabela 6 temos a seguinte codificação do 2° ao 7° caractere numérico:

$7 \rightarrow 0111011$ $9 \rightarrow 0010111$ $1 \rightarrow 0011001$

$2 \rightarrow 0011011$ $3 \rightarrow 0111101$ $4 \rightarrow 0011101$

Como os caracteres à direita do caractere central utilizam apenas a tabela C, então podemos obter facilmente a codificação dos seis caracteres restantes:

$5 \rightarrow 1001110$ $6 \rightarrow 1010000$ $7 \rightarrow 1000100$

$8 \rightarrow 1001000$ $9 \rightarrow 1110100$ $8 \rightarrow 1001000$

No caso do EAN-8, os quatro primeiros caracteres (incluindo o primeiro caractere da bandeira) são codificados pela tabela A e os quatros restantes pela tabela C,

de modo que não é preciso verificar o primeiro caractere do código, como ocorre com o EAN-13.

4.3.2.1 Cálculo do Dígito Verificador do Código de Barras tipo EAN 13.

Exemplo de código: 789105206230X

Somar os números que estiverem na posição ímpar do código de barras multiplicados por 3 (←):

0 (x3) + 2 (x3) + 0 (x3) + 5 (x3) + 1 (x3) + 8 (x3) =

0 + 6 + 0 + 15 + 3 + 24 = 48

Fazer a soma dos números da posição par: 3 + 6 + 2 + 0 + 9 + 7 = 27

Somar tudo: 48 + 27 = 75

O DV é a diferença para o próximo múltiplo de 10, ou seja, para o próximo múltiplo de 10 faltam 5, então o DV é 5 [27].

4.3.2.2 Cálculo do Dígito Verificador do Código de Barras tipo EAN 8.

Exemplo de código: 7891809X

Somar os números que estiverem na posição ímpar do código de barras multiplicados por 3 (←):

9 (x3) + 8 (x3) + 9 (x3) + 7 (x3) =

27 + 24 + 27 + 21 = 99

Fazer a soma dos números da posição par: 0 + 1 + 8 = 9

Somar tudo: 99 + 9 = 108

O DV é a diferença para o próximo múltiplo de 10, ou seja, para o próximo múltiplo de 10 faltam 2, então o DV é 2.

4.3.4 Código de Barras tipo Código 39.

Desenvolvido em 1975, pela empresa Interface Mechanism Inc, o código 39 foi na época adotado por quase todos os órgãos governamentais norte-americanos, principalmente pelo Departamento de Defesa.

Trata-se de um código discreto, alfanumérico e composto por quarenta e quatro caracteres: dez algarismos, vinte e seis letras, um espaço e sete símbolos especiais (travessão, cifrão, ponto, barra, sinal de adição, porcentagem e asterisco).

O último símbolo (asterisco) é usado para indicar as margens de início e fim do código e permitir uma leitura bidirecional. Também é conhecido como “código 3 de

9", pois cada caractere é formado por um conjunto de cinco barras escuras e quatro espaços claros, sendo três mais largos.

A estrutura desse código é composta por caracteres auxiliares (inicial e final) e caracteres de dados, conforme tabela 13.

Tabela 13 Estrutura do Código 39 [39].

Caractere Inicial	Caractere de dados	Caractere Final
▯	N	▯

O fato de não estar definido um número preciso de caracteres de dados no código, deve-se à ausência de restrições quanto à quantidade de informações a serem codificadas.

Como a codificação do código 39 é feita pela largura de módulos, considera-se que os elementos mais largos são, no máximo, três vezes maiores que os estreitos e, ainda, a cada nove módulos (barras e espaços) devem-se usar um espaço estreito para separar um código do outro, sendo que este espaço não entra na codificação.

No caso desse tipo de código, as barras ou espaços largos são representados pelo dígito 1 e os estreitos representados pelo dígito 0, conforme tabela 14.

Tabela 14 Representação de barras e espaços largos no Código 39 [39].

caractere	padrão	barras + espaços	caractere	padrão	barras + espaços
1		100100001	M		101000010
2		001100001	N		000010011
3		101100000	O		100010010
4		000110001	P		001010010
5		100110000	Q		000000111
6		001110000	R		100000110
7		000100101	S		001000110
8		100100100	T		000010110
9		001100100	U		110000001
0		000110100	V		011000001
A		100001001	W		111000000
B		001001001	X		010010001
C		101001000	Y		110010000
D		000011001	Z		011010000
E		100011000	–		010000101
F		001011000	.		110000100
G		000001101	espaço		011000100
H		100001100	*		010010100
I		001001100	$		010101000
J		000011100	/		010100010
K		100000011	+		010001010
L		001000011	%		000101010

*código início/fim

81139-2

O código 39, devido ao seu comprimento variável e capacidade elevada de auto-verificação, não necessita de um dígito de verificação, de modo que a cada 70 milhões de caracteres lidos apresenta um erro de substituição. Entretanto, como se deseja sempre a maior segurança possível em relação à codificação em produtos, existe uma versão do código 39 que utiliza um dígito verificador.

Atualmente, o código 39 é usado em hospitais, bibliotecas, inventários, locadoras e, principalmente, na indústria mecânica, por se tratarem de áreas que necessitam do código alfanumérico no controle de informações. Alguns setores industriais do Brasil utilizam esse tipo de código, conforme figura 50.

Figura 50 Exemplo de um código 39 [39].

4.3.5 Código de Barras tipo Código 25.

Trata-se de um código contínuo, numérico e de comprimento variável devido a quantidade de caracteres ser ilimitada. É considerado o mais simples dos códigos de barras.

Também conhecido como "código 2 de 5", pois cada um de seus caracteres é formado por cincos barras, sendo duas delas largas. É codificado pela largura de módulo em que a informação está contida nas barras escuras, sendo que as largas representam o dígito 1 e as estreitas o dígito 0. Os espaços são usados apenas para separar uma barra da outra, não sendo considerados, conforme figura 51.

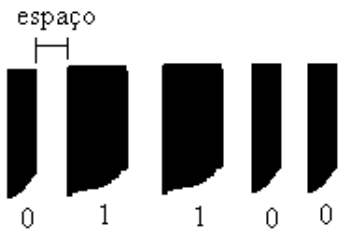


Figura 51 Esquema de representação simbólica do código 25 [39].

O código 2 de 5, é composto em sua estrutura dos seguintes elementos conforme tabela 15 :

Tabela 15 Estrutura do Código 25 [39].

Caractere Inicial	Caractere de dados	Caractere Final
▢	N	▢

Apresenta uma estrutura exatamente semelhante a do código 39, diferenciando-se na consideração ou não dos espaços, conforme figura 52, no processo de codificação e, ainda, quanto aos caracteres auxiliares: enquanto o código 3 de 9 utiliza o asterisco como caracteres inicial e final, o código 2 de 5 possui um caractere inicial e outro final predefinidos, sendo o caractere de início igual a 110 e o caractere final igual a 010, conforme tabela 16.

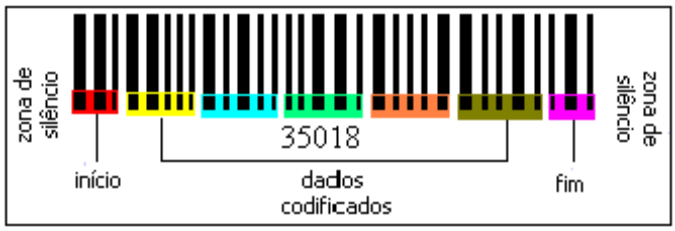


Figura 52 Exemplo da estrutura de um código 25 [39].

Tabela 16 Representação da Codificação dos caracteres de 0 a 9 e de guarda pelo Código 25 [39].

CARACTERE	CÓDIGO 2 de 5	CARACTERE	CÓDIGO 2 de 5
0	00110	**6**	01100
1	10001	**7**	00011
2	01001	**8**	10010
3	11000	**9**	01010
4	00101	**Início**	110
5	10100	**Fim**	010
Observação: 0- barra estreita e 1- barra larga.			

O código 2 de 5 codifica apenas as barras escuras, é muito usado em manuseio de inventário, fichas de compensação, identificação de envelopes de acabamento fotográfico, passagens aéreas, manuseio de bagagens e cargas e muitas outras aplicações.

4.3.6 Código de Barras tipo Código 2 de 5 intercalado.

Consiste em uma versão compactada do código 25, conforme a figura 53. Trata-se de um código contínuo, que não apresenta espaço entre os caracteres, é muito utilizado em boletos bancários e fichas de compensação. No Brasil, a FEBRABAN (Federação Brasileira de Bancos) é responsável por gerenciar e controlar os códigos distribuídos no setor financeiro do país.

Figura 53 Exemplo de um código 2 de 5 intercalado [27].

4.4 Código de Barras Bidimensional (2D).

Os códigos de barra 2D armazenam grande quantidade de dados em uma figura de tamanho pequeno, entretanto sua decodificação torna-se mais custosa em termos de hardware e de tempo.

Existem diferentes padrões e aplicações para o código de barras 2D cuja finalidade é de codificar informações para serem processadas por algum sistema após decodificação.

A leitura desses códigos é feito através de dispositivos de captura com a tecnologia "IMAGER", conforme a figura 54. Realizam uma foto tirada do código que é decodificada pelo equipamento.

Os tradicionais dispositivos com tecnologia de leitura "LASER" não são capazes de efetuar a leitura desses códigos [43].

Figura 54 Dispositivos de captura para leitura de Código Bidimensional [43].

Os Códigos de Barras Lineares possuem a representação simbólica de informações em apenas um eixo. Os Códigos de Barras Bidimensionais representam códigos de barras lineares empilhados um acima do outro com orientação e localização, conforme figura 55.

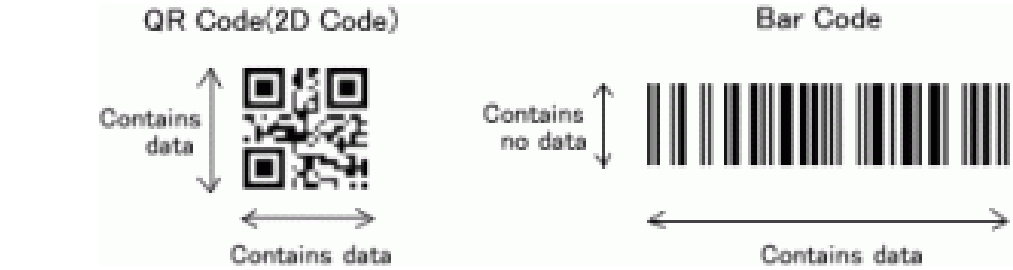


Figura 55 Direções para captura de dados em códigos de barras lineares e 2D [49].

Desenvolvidos recentemente, a utilização de códigos 2D, conforme figura 56, está presente em diversas áreas, tais como [48]:

- Indústrias: utilizado em logística, romaneios, notas fiscais, rastreamento de produtos, identificação de peças;

- Comércios: controle de mercadorias, estoques, clientes;

- Bancos: identificação de cheques, instruções de cobranças em boletos bancários, anti-fraudes em pagamentos;

- Seguradoras: controle de documentos, registro de seguros, laudos técnicos e perícias;

- Hospitais: fichas médicas, credenciais, controle de materiais, exames, diagnósticos, remessas de informações confidenciais;

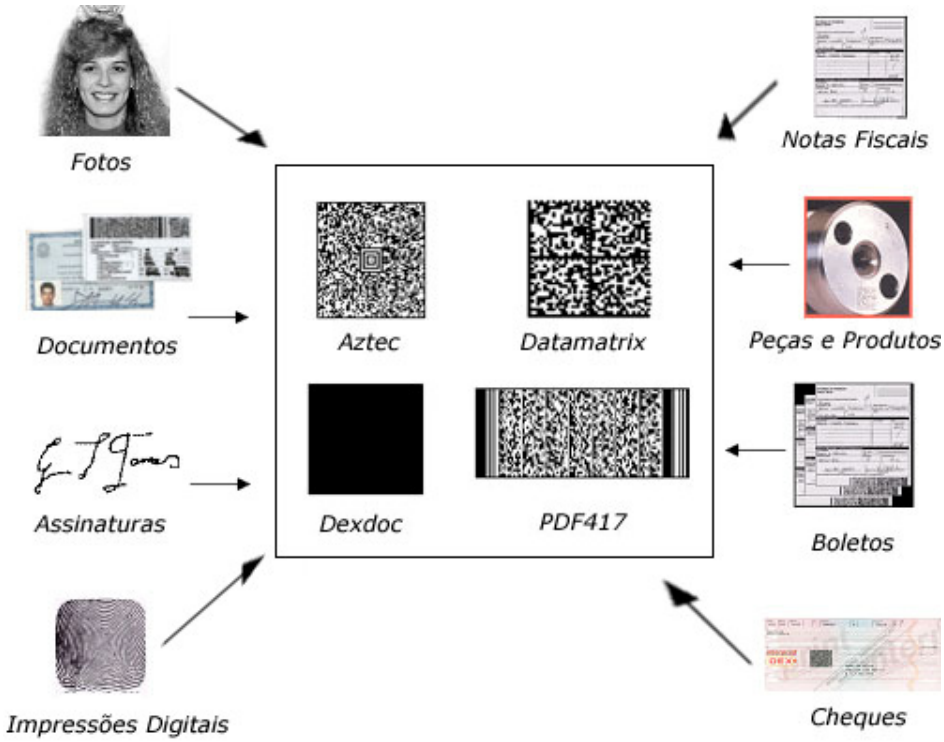


Figura 56 Exemplos de Aplicação para p Código Bidimensional [48].

Algumas características e especificações gerais de um código 2D [48]:

- Geração do código ao mesmo tempo em que está gerando o documento, com total segurança.

- Código de domínio público.

- Rápida leitura, sem falhas com 100% de captura das informações.

- Possibilidade de redundância de até 40%.

- Impressão em papel, metal, plástico, laser, termo transferência e Ink Jet etc.

- Leitura instantânea por Scanners Ópticos.

Alguns tipos de códigos de barras bidimensionais mais comuns serão abordados em seguida.

4.4.1 Código de Barras Bidimensional (2D) tipo Datamatrix.

O Datamatrix é um código bidimensional (2D) , sua codificação é composta por pequenos pontos ou quadrados que unidos formam um símbolo que permite codificar informações alfanuméricas (letras e números), conforme figura 57.

Figura 57 Exemplo código 2D Datamatrix [43].

Recentemente com a Lei aprovada no Brasil todos os medicamentos a partir de 2010 deverão possuir um código Datamatrix com uma numeração única que acompanhará todo o ciclo de vida do medicamento, da sua fabricação até chegar à mão do consumidor, conforme Anexo 2 deste trabalho [43].

4.4.2 Código de Barras Bidimensional (2D) tipo QR Code.

O QR Code é uma matriz ou código de barras bidimensional, conforme figura 58, criado pela empresa Japonesa Denso-Wave, em 1994.

Figura 58 Exemplo de código 2D QR Code [44].

O QR vem de Quick Response, pois o código pode ser interpretado rapidamente, mesmo com imagens de baixa resolução, feitas por câmeras digitais em formato VGA, como as de celulares. O QR Code é muito usado no Japão [44].

Desde 2003, estão sendo desenvolvidas aplicações direcionadas para ajudar os usuários na tarefa de adicionar dados em telefones celulares. São muito comuns também em revistas e propagandas, onde se usam os códigos para guardar endereços e URLs.

O Jornal A TARDE, localizado na cidade de Salvador - Bahia tem usado o QR Code desde 10 de dezembro de 2008. Foi o primeiro jornal impresso no País - reconhecido pela Associação Nacional de Jornais (ANJ) - a utilizar o código em suas páginas como selo integrador de mídias; levando o leitor do papel-jornal ao dispositivo móvel (celular) [44].

4.4.3 Código de Barras Bidimensional (2D) tipo Aztec.

Código Aztec é um tipo de código de barras em matriz bidimensional, inventado por Andrew Longacre, Jr. da Welch Allyn Inc. (correntemente, Hand Held Products Inc.) em 1995.

O símbolo, conforme figura 59, é construído numa grelha quadrada com um padrão "olho de boi" ao centro para colocação do código. Os dados são codificados numa série de círculos ao redor do padrão olho de boi.

Figura 59 Exemplo de código 2D Aztec[45].

Cada círculo adicional circunda completamente o círculo precedente fazendo com que o símbolo cresça em tamanho à medida que mais dados são codificados. Um módulo escuro representa o binário 1 e um módulo claro o binário 0. O código independe de orientação [45].

4.4.4 Código de Barras Bidimensional (2D) tipo Maxi Code.

O formato MaxiCode representado na figura 60, foi desenvolvido pela empresa americana de transportes de mercadorias UPS (United Parcel Service), com intuito de tornar a triagem de mercadorias mais fácil [51].

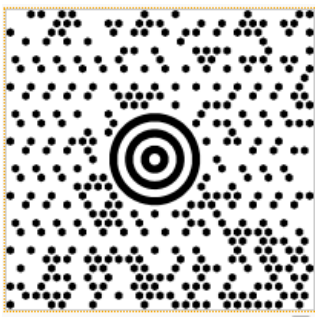


Figura 60 Exemplo de código 2D Maxi Code [47].

O MaxiCode é muito utilizado para rastreamento e controle de embalagens na indústria. No Brasil, é largamente utilizado por companhias de bebida alcoólica. Diferentemente do QR Code, utiliza pontos arranjados em grades hexagonais [50].

4.4.5 Código de Barras Bidimensional (2D) tipo PDF 417.

O formato PDF 417, apresentado na figura 61, foi desenvolvido na década de 90 para as mais variadas aplicações, algumas das quais incluem o controle de transporte de pequenas caixas, identificação militar, renovações de carteiras de motorista, controle de acesso e gestão de armazéns [51].

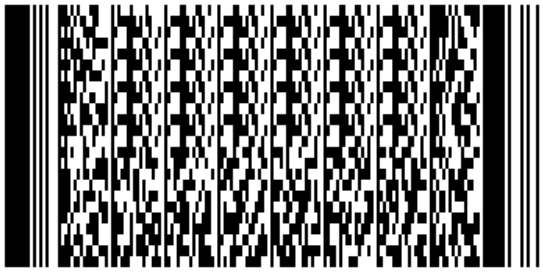


Figura 61 Exemplo de código 2D PDF 417 [46].

Todas estas aplicações ganharam particular importância nos Estados Unidos, onde o formato PDF417 alcançou o estatuto de modelo normalizado dos códigos bidimensionais [51].

4.4.6 Código de Barras Bidimensional (2D) tipo HCCB.

Microsoft Tag - Com esse experimento, a Microsoft colocou no mercado um código em 2D colorido,conforme figura 62.

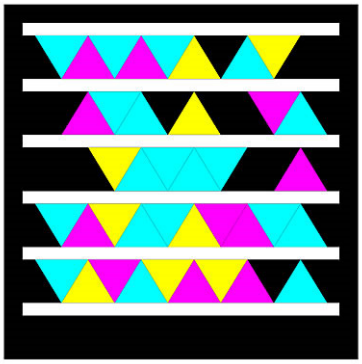


Figura 62 Exemplo de código 2D HCCB [50].

Torna os códigos legíveis para câmeras de baixa qualidade, além de conseguir colocar mais informação em menores imagens. Com esse código, de nome HCCB (High Capacity Color Barcode), também é possível criar imagens codificadas.

4.5 Tecnologias candidatas à substituição dos Códigos de Barras.

A substituição do popular código de barras, que revolucionou a atividade comercial e se estendeu a inúmeras atividades, é só uma questão de tempo. Algumas tecnologias de transição estão sendo desenvolvidas para a ocupação deste espaço. Algumas destas tecnologias serão abordadas em seguida.

4.5.1 Identificação por Rádiofreqüência – RFID (abordado no Capítulo II).

Os códigos de barras serão substituídos por um dispositivo baseado num microchip, conforme figura 63, que armazena dado e se comunica por meio de ondas de rádio com um aparelho de leitura [27].

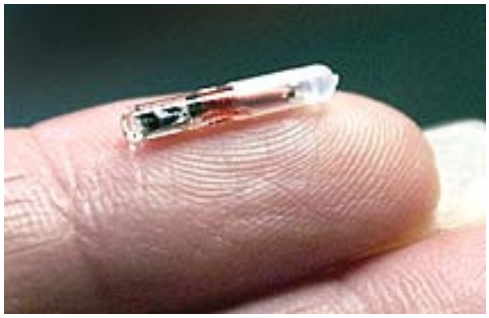


Figura 63 Exemplo de Identificador de RF [27].

4.5.2 Nanotecnologia e Identificação por Rádiofreqüência – RFID.

Ao contrário das conhecidas barrinhas, que possuem um dado único e permanente, as etiquetas RFID conforme figura 64, possuem um chip e memória em seu interior, podendo se comunicar com o exterior por meio de tecnologias de transmissão de dados sem fios.

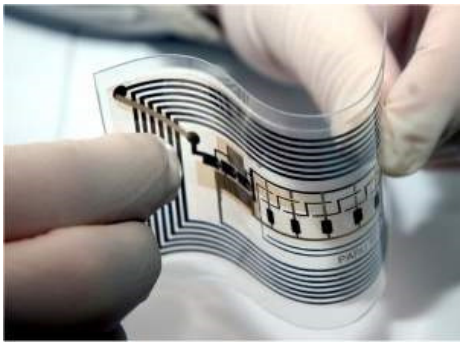


Figura 64 Exemplo de etiqueta inteligente [52].

As etiquetas RFID são caras, porém um novo processo descrito em [52] nas Referências Bibliográficas, permitirá que elas sejam simplesmente impressas, exatamente como os códigos de barras reduzindo o custo conforme figura 65.

Figura 65 Exemplo impressão de etiquetas inteligentes [52].

A técnica utiliza uma tinta na qual estão dissolvidos nanotubos de carbono. Aplicada por uma impressora jato de tinta, a tinta com nanotubos é usada para desenhar os transistores que formam o chip da etiqueta RFID.

No estágio atual, ela pode ser utilizada para imprimir os circuitos eletrônicos sobre papel ou plástico. Este mesmo princípio já foi aplicado para imprimir transitores, células solares e até para imprimir uma bateria de papel.

A técnica é capaz de imprimir também a antena, os eletrodos e as camadas dielétricas, em um processo feito em três etapas. As etiquetas inteligentes resultantes são do tipo passivo, o que significa que elas não precisam de bateria para funcionar.

4.5.3 Bokode.

Bokode é um tipo de etiqueta de dados que mede apenas 3 mm de diâmetro e é capaz de armazenar muito mais informações do que um código de barras, conforme a figura 66.

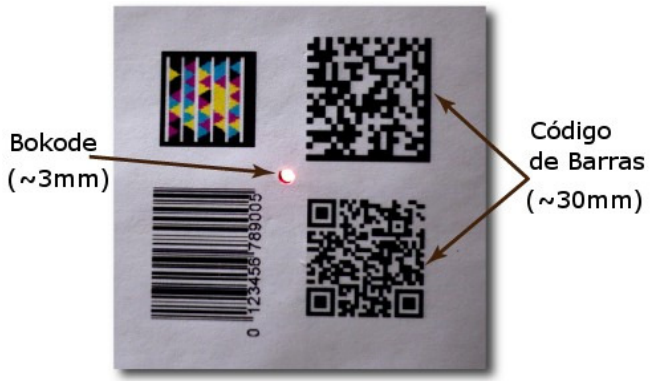


Figura 66 Comparando Bokode com demais códigos [53].

Esta tecnologia foi desenvolvida pelo Media Labs do Instituto de Tecnologia de Massachusetts (MIT), Estados Unidos.

Bokode é uma palavra inventada, criada a partir da junção de duas outras palavras: “bokeh”, palavra em japonês que significa mancha ou borrão, e é um termo técnico da área de fotografia, e “code”, que significa código em inglês. Unindo as duas, Bokode [53].

Esta nova tecnologia já parte na direção dos hologramas e codifica dados na direção angular. Os dados são interpretados de maneiras diferentes de acordo com o posicionamento dos raios de luz que emergem do dispositivo, conforme figura 67 [53].

Figura 67 Exemplo de Bokode ampliado [53].

Seu objetivo então é ocupar menos espaço, armazenar mais informações e facilitar a leitura que poderá ser realizada a uma distância de até 4m por celulares e câmeras além de leitores de códigos padrão.

O Bokode necessita de um LED (Diodo Emissor de Luz) para emitir as luzes necessárias para a leitura e para isso necessitará de uma fonte de energia. Este é um dos principais problemas desta tecnologia para concorrer com o código de barras.

4.6 Considerações Finais.

Este capítulo procurou ilustrar alguns tipos de códigos de barras lineares, bidimensionais e as possíveis tecnologias candidatas para assumir a posição a qual ocupa o código de barras tradicional atualmente.

A tecnologia de código de barras proporcionou o estabelecimento da automação comercial trazendo otimização na organização e no controle da cadeia de suprimentos além de rapidez no atendimento.

Os códigos de barras já estão inseridos no cotidiano da sociedade atual e dificilmente deixarão de permanecer atuantes mesmo com o surgimento de tecnologias promissoras.

Algumas aplicações são comprovadamente inerentes à utilização do código de barras ao se avaliar o custo-benefício da implantação de uma nova tecnologia mais avançada prefere-se permanecer com a utilização daquela que já é largamente empregada e bem assimilada pela sociedade.

Capítulo V

5. Análise Comparativa.

5.1 Comparação.

O uso da tecnologia automática de identificação vem crescendo desde a metade do século passado e está se tornando uma parte indispensável de vida diária. O código de barras foi a base para as tecnologias de auto-identificação.

Encontra-se código de barras em toda parte, desde produtos à prestação de serviços. Embora RFID seja aparentemente novo, não está substituindo o código de barras ou outra tecnologia de identificação, ao menos por enquanto. Cada tecnologia de auto-identificação tem suas vantagens e desvantagens.

Um dos problemas com o código de barras é que se pode fazer a varredura de apenas um objeto de cada vez. Além disso, uma quantidade limitada de dados é armazenada no código deixando de lado informações importantes como número de série original, data de expiração ou validade, ou outra informação pertinente.

O leitor de código de barras necessariamente tem que estar em visada com o código para efetuar sua leitura, logo, ocorrem erros de leitura caso o artigo codificado esteja empoeirado, sujo ou com algum defeito em sua etiqueta de identificação.

Uma grande vantagem da tecnologia de identificação por códigos de barras é o baixo custo de implementação e manutenção, bastando a impressão das etiquetas codificadas e um dispositivo de leitura. Atualmente, tem-se uma boa infraestrutura para essa aplicação.

Em cartões de memória, “memory cards”, geralmente usa-se uma EEPROM, que é acessada usando uma lógica seqüencial. É também possível incorporar algoritmos simples de segurança.

A funcionalidade da memória pode ser otimizada para uma aplicação específica e a flexibilidade da aplicação é altamente limitada, pois um cartão de memória é desenvolvido para determinada aplicação como, por exemplo, para um sistema telefônico sendo que este mesmo cartão não poderá atender a outro sistema como, por exemplo, o de pagamento de passagens em transportes urbanos. Por outro lado, os cartões de memória possuem uma boa relação custo-benefício.

Os cartões microprocessados são muito usados em aplicações que necessitam de uma maior segurança, como os “Smart Cards” para telefones móveis GSM e os cartões de crédito com chip.

A opção de programar os cartões microprocessados facilita a adaptação rápida às novas aplicações que vem surgindo a cada dia, o que representa uma grande vantagem devido a sua flexibilização mesmo com um custo relativamente alto, pois seu tempo de vida é longo.

Um cartão microprocessado assemelha-se a um identificador passivo RFID quando houver a opção sem contato, porém atendendo as normas de padronização em vigor.

Tabela 17 Principais parâmetros para comparação entre tecnologias de auto-identificação [9].

Parâmetros de comparação	Código de Barras	Cartão de contato	RFID - Passivo	RFID - Ativo
Modificação dos dados	Não	Sim	Sim	Sim
Segurança dos dados	Baixa	Alta	Variável (Baixo – Alto)	Alta
Quantidade de dados	- linear: 8-30 caracteres - 2D: 7.200 caracteres	Acima de 8 MB	Acima de 64 kB	Acima de 8 MB
Custo	Poucos centavos de dólar ou fração de centavo por item	Pouco mais de US$1,00 por item	Médio, pouco menos de 25 centavos de dólar por item.	Muito alto, de US$10,00 a US$100,00 por item.
Padronização	Estável e padronizado	Proprietário e não padronizado	Não proprietário e evoluindo para uma padronização	Proprietário e evoluindo para um padrão aberto.
Tempo de Vida	Pequeno	Longo	Indefinido (depende da qualidade do *tag*)	3-5 anos dependendo da bateria de alimentação
Interferência	Barreira óptica - sujeira ou objetos obstruindo a visada do laser	Bloqueio do contato	O meio ambiente pode afetar os campos e a transmissão das ondas de rádio	Barreiras ilimitadas desde que o sinal do *tag* seja forte e livre de ruído.

Na tabela 17, mostra-se uma comparação entre os principais métodos de auto-identificação com relação à quantidade de dados que podem ser armazenados, segurança da aplicação, custo, padronização, vida útil e interferências do meio.

Os benefícios da tecnologia RFID podem ser categorizados quanto ao tempo (curto prazo versus longo prazo) ou quanto à tangibilidade (direta versus indireta).

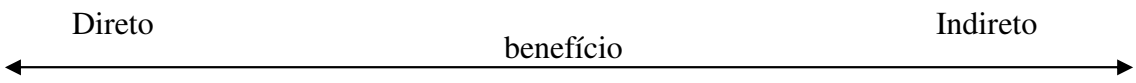
Em alguns casos, como etiquetar gado ou etiquetar uma cadeia de suprimentos, deve-se considerar o efeito de rede, ou seja, o custo da implementação de um sistema RFID pode ser mínimo quando se considera um sistema fechado, como se fossem células isoladas de um circuito fechado de TV com tecnologia proprietária sem interação com os demais usuários da tecnologia, com o único propósito de somente otimizar os próprios processos (criadores de gado ou distribuidores de suprimentos desenvolvem seu próprio sistema RFID).

O custo aumenta significativamente quando se considera um sistema aberto, ou seja, vários criadores ou distribuidores de suprimentos fazem uso de um sistema comum.

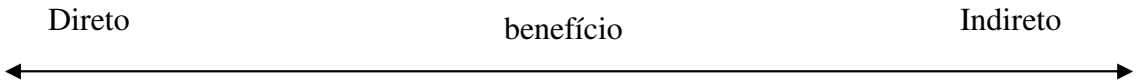
Na tabela 18 verificam-se as vantagens diretas e indiretas relacionadas no período de tempo. Essa comparação é muito importante na tomada de decisão de implementar o uso desta tecnologia no mercado ou indústria.

Tabela 18 Relação tempo x benefício para utilização da tecnologia RFID [9].

Longo Prazo - Direto	**Longo Prazo - Indireto**
Exemplos de Aplicações: - Controle em tempo real da cadeia de suprimento. - Monitorar temperatura e outros atributos de produtos em trânsito. - Controle de estoque da rede Wal-Mart. **Benefícios:** - Melhoria do inventário de produtos e controle de fornecedores. - Redução no custo de estocagem. - Redução no tempo de entrega. - Melhoria na tomada de decisão.	**Exemplos de Aplicações:** - Conformidade com o DoD (Department Of Defense) na cadeia de fornecedores militares. - Trabalho voluntário do FDA (Food and Drug Administration). **Benefícios:** - Melhoria e controle da política de seguros contra perdas e catástrofes nas indústrias. - Responsabilidade Social nas práticas comerciais.



Curto Prazo - Direto	Curto Prazo - Indireto
Exemplos de Aplicações: - Controle de acesso em alguns nichos do mercado. - Coleta de pedágio em rodovias. - Etiquetas em produtos e containers **Benefícios:** - Redução no custo dos trabalhadores. - Alta precisão. - Maior conveniência para o consumidor.	**Exemplos de Aplicações:** - Etiquetas RFID descartáveis (Wal-Mart e DoD). - Etiquetas em remédios e drogas controlados pelo sistema de saúde pública. **Benefícios:** - Melhoria na fiscalização de remédios controlados, e controles de produtos vendidos. - Controle de impostos sobre mercadorias vendidas.



5.2 Exemplo de Caso.

O caso a ser abordado consta em um vídeo presente nas Referências Bibliográficas [8], sobre controle de qualidade e prateleira inteligente numa fábrica em Sorocaba, no estado de São Paulo. Esta mídia mostra de forma sucinta os benefícios alcançados pela utilização da tecnologia RFID na conferência dos itens numa linha de montagem para embalagem de impressoras e também apresenta uma prateleira inteligente capaz de gerenciar cartuchos de impressão.

A fábrica apresenta uma alternativa ainda em fase de testes para substituir o código de barras por meio da utilização de etiquetas inteligentes.

Tal iniciativa possibilita saber todas as informações sobre o produto desde que é fabricado até chegar à casa do consumidor, o que o código de barras não permite, pois somente informa qual é o fabricante e qual o produto.

Com a etiqueta inteligente consegue-se ir além destas informações como identificar o produto de forma única proporcionando verificar se já passou por determinado local dentro da fábrica, por exemplo, ou se já saiu da linha de produção.

A etiqueta inteligente está sendo implantada em uma linha de produção de impressoras, o que permite já na montagem controlar se o produto foi testado, qual o programa de computador usado e a validade do cartucho.

Ao se colocar etiquetas em todos os itens que vão dentro da caixa da impressora, são evitados possíveis erros antes do produto sair da fábrica garantindo assim que nenhum acessório foi esquecido, proporcionando ao consumidor a certeza de que estará levando um produto com todos os itens esperados.

Há também em testes, na fábrica, a prateleira inteligente, na qual leitores monitoram a quantidade de cartuchos de impressoras à venda, à medida que um é retirado, a informação é enviada imediatamente para a central da empresa onde outro dispositivo permite observar em um mapa a localização da máquina responsável pela venda.

Para o caso em pauta, a utilização da tecnologia RFID proporciona algumas vantagens que realmente fazem com que seja bastante promissora sua utilização também em outros setores, em curto espaço de tempo.

A utilização desta tecnologia de identificação permite realizar a leitura de várias etiquetas ao mesmo tempo sem precisar estar em visada com um leitor, checar a situação do estoque de respectivo produto instantaneamente e também obter várias outras informações relativas ao item além de qual fabricante.

Com a etiqueta inteligente obtém-se, por exemplo, o número de série original, data de expiração ou validade, ou outra informação do item permitindo o rastreamento e possivelmente captar dados por onde o produto passou até chegar às mãos do consumidor.

Para a empresa passam a existir muitos subsídios proporcionados pela aplicação desta tecnologia para realizar uma melhor tomada de decisões em relação a aspectos relacionados ao produto.

A quantidade de dados possíveis de serem gravados numa etiqueta inteligente ultrapassa a capacidade do código de barras, sendo esta uma questão vantajosa abordada neste estudo de caso. Além disso, existem condições de realizar a modificação de dados já inseridos na etiqueta inteligente o que não é permitido em código de barras.

A proteção dos dados neste exemplo de caso não requer alto grau de segurança, porém caso fosse necessário poderia ser variado utilizando etiquetas inteligentes, o que não seria viável com código de barras por ser considerado de baixo grau de segurança em relação aos dados.

O tempo de vida de uma etiqueta inteligente depende do material do qual é feito, neste exemplo de caso parece ser recoberta por uma camada plástica transparente retangular o que assegura aparentemente maior proteção.

A padronização da utilização das etiquetas inteligentes não alcançou o patamar ocupado pelo código de barras o qual possui uma infraestrutura instalada estável na sociedade.

No exemplo deste estudo de caso, é desenvolvido um esforço para solucionar problemas encontrados nos testes com a tecnologia RFID, superando entraves técnicos relacionados à transmissão das ondas de rádio, por exemplo, suplantando desafios buscando otimizações e padronizações para a utilização deste sistema.

A utilização de "smart cards" com contato neste exemplo de caso não é o mais apropriado, pois deixaria de viabilizar a dinâmica da linha de produção. A opção sem contato talvez fosse mais pertinente, entretanto o custo para se colocar um "smart card" de acordo com os padrões vigentes, em cada item que compõe o produto seria muito elevado além de indicar uma subutilização dessa tecnologia de identificação.

A adoção de RFID neste exemplo de caso foi a melhor opção para atender as peculiaridades desejadas pela empresa sendo a mais vantajosa em relação ao código de barras e a mais adequada em relação à "smart cards", mesmo havendo certo custo para a implantação desta tecnologia.

Capítulo VI

6. Considerações Finais.

Este trabalho trouxe algumas informações a respeito da Identificação por RFID, “Smart Cards” e Código de Barras onde cada capítulo referente a essas tecnologias procurou transmitir uma noção sucinta para a compreensão de tais assuntos.

No capítulo de Análise Comparativa as tecnologias de identificação foram abordadas por características e aspectos que envolvem vantagens e benefícios de utilização, tendo inclusive um exemplo de caso para um melhor esclarecimento de algumas razões envolvidas para a adoção de uma tecnologia em prol das demais.

Há um apêndice que traz informações sobre uma implementação cuja função é demonstrar a geração de Códigos de Barras lineares e bidimensionais a partir de dados fornecidos. Em seguida alguns anexos fornecem a legislação que ampara as atitudes do governo brasileiro perante as tecnologias de identificação tratadas.

A evolução tecnológica compreende interseções e complementaridades entre estas diversas tecnologias de identificação apresentadas às quais possuem características que permitem atuar de forma combinada ou não, dependendo do tipo de aplicação e do grau de segurança que se deseja.

Cada uma delas possui peculiaridades únicas que indicam ainda um longo tempo de uso na sociedade, pois já se tornou parte indispensável da vida diária. Algumas podem se sobressair em relação a outras, porém depende muito da aplicação, do grau de segurança desejado, custo x benefício e também da assimilação desta tecnologia por parte da sociedade.

Procurou-se demonstrar neste trabalho que estas tecnologias podem se complementar ou que há uma tecnologia mais apropriada para uma determinada tarefa.

O próprio governo brasileiro atualmente executa vários projetos previstos em lei visando aplicações de grande impacto para a sociedade que utilizam as tecnologias de identificação abordadas neste trabalho para otimizar as questões de controle e de segurança em problemas relacionados à identificação quer de pessoas ou não.

Mais uma vez demonstra-se a importância das tecnologias de identificação como elemento profundamente transformador no seio da sociedade ao se propor como solução em vários projetos nacionais a adoção destas tecnologias pelo governo. Desta

forma confirma-se através de sua importância social o estudo destas tecnologias de identificação como objetivo deste trabalho.

Deve-se sempre estar atento quanto à privacidade em razão das possíveis informações que se podem extrair por meio dessas tecnologias de identificação para que não se desviem e sejam utilizadas para outros fins inadequados.

A segurança em geral deve estar também sempre em compasso de evolução com a utilização das tecnologias de identificação para a total preservação da privacidade e da integridade dos dados gravados e acessados por quaisquer dispositivos.

Buscou-se no desenrolar deste trabalho trazer informações sobre as tecnologias de identificação para que fossem despertadas motivações em novas pesquisas nesta área bastante atual e de grande impacto na sociedade.

O contexto desta monografia possibilita muitas opções para implementação. A sugestão para trabalhos futuros é o desenvolvimento de aplicações envolvendo middleware RFID por ser um elemento de suma importância em soluções RFID. Seria bastante interessante e devido ao alto grau de complexidade envolvido não foi explorado em profundidade neste trabalho.

REFERÊNCIAS BIBLIOGRÁFICAS

[1]http://www.suinicultura.com/fpas_info.asp?nr=6&id=1566 acessado em 23 de outubro de 2008.

[2]http://gs1brasil.wordpress.com/2008/04/09/identificacao-de-produtos-e-unidades-logisticas-a-utilizacao-de-padroes-globais/ acessado em 23 de outubro de 2008.

[3]http://www.eanbrasil.org.br/d02_tecn/barcode_pg1.html acessado em 23 de outubro de 2008.

[4]MOURA, Benjamim do Carmo - *Logística: conceitos e tendências*. Vila Nova de Famalicão: Edições Centro Atlântico, 2006. ISBN 978-989-615-019-8

[5]http://pt.wikipedia.org/wiki/C%C3%B3digo_de_barras acessado em 23 de outubro de 2008.

[6]GLOVER, Bill; BHATT, Himanshu. **Fundamentos de RFID**. Rio de Janeiro. Alta Books, 2007.

[7]http://www.gs1brasil.org.br acessado em 23 de outubro de 2008.

[8]http://www.youtube.com/watch?v=IvDsD4U--uE - vídeo sobre RFID HP acessado em 23 de setembro 2010.

[9]OLIVEIRA, Alessandro de Souza; PEREIRA, Milene Franco. Estudo da tecnologia de identificação por radiofreqüência – RFID. Monografia, UnB – Universidade de Brasília, Faculdade de Tecnologia. 2006.
Disponível em: www.ene.unb.br/antenas/Arquivos/Alessandromilene.pdf acessado em 27 de outubro de 2008.

[10]http://pt.wikipedia.org/wiki/RFID acessado em 27 de outubro de 2008.

[11]JÚNIOR , José Fernando Rodrigues. **Sistema para Automatização de Estabelecimentos Gastronômicos com auxílio de Cartões Inteligentes**. São Paulo, 2001.22p. Monografia - Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo. Disponível em: http://gbdi.icmc.usp.br/~junio/Site/Conteudo/Referencias/SV/ProjetoDeEstagio.pdf , acessado em 27 de outubro de 2008.

[12]FONTES, Marcelo Fernandes; DUARTE, Otto Carlos M.B. **Smart Cards para o Controle de Acesso**. UFRJ – Universidade Federal do Rio de Janeiro. Grupo de Teleinformática e Automação. Disponível em : http://inf.upf.tche.br/~52731/CD/Smart_Card_Trab.pdf , acessado em 27 de outubro de 2008.

[13]www.portalrfid.net/documents/EstadoDaArte.pdf acessado em 8 de setembro de 2009.

[14] http://www.hightechaid.com/tech/rfid/rfid_technology.htm acessado em 8 de setembro de 2009.

[15]http://www.rfidjournal.com/videos/view/12 - vídeo sobre Código de Barras x RFID acessado em 27 de janeiro de 2010.

[16]http://www.youtube.com/watch?v=-wdh8WO4TXA – vídeo sobre Código de Barras bidimensional no Controle de Medicamento acesso em 13 de março de 2010.

[17]http://www.ked.com.br/index.php acessado em 23 de fevereiro de 2010.

[18]http://www.dipolerfid.es/productos/software_RFID/middleware_RFID/Default.aspx acessado em 24 de fevereiro de 2010.

[19]http://en.wikipedia.org/wiki/Smart_card acessado em 24 de fevereiro de 2010.

[20]http://pt.wikipedia.org/wiki/Cart%C3%A3o_SIM acessado em 25 de fevereiro de 2010.

[21]http://br.youtube.com/watch?v=MHb1zI0wk8M - vídeo sobre o Projeto RIC acessado em 27 de fevereiro de 2010.

[22] http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2008_2/thiago/smart_cards.html acessado em 27 de fevereiro de 2010.

[23]http://www.macae.rj.gov.br/noticias/mostranot.asp?id=6677 acessado em 07 de março de 2010.

[24]http://www.matthewneely.com/blog/2008/12/22/magstripe-analysis-part-1-introduction-to-magstripe-cards.html acessado em 07 de março de 2010.

[25]http://www.alejandrobarros.com/content/view/211714/Fraude-Electronico-Nueva-barrera.html acessado em 07 de março de 2010.

[26]http://www.youtube.com/watch?v=eob532iEpqk - vídeo sobre RFID Mercado acessado em 03 de novembro de 2010.

[27]http://www.google.com.br/search?q=C_DIGO_DE_BARRAS+s+111&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:pt-BR:official&client=firefox-a acessado em 18 de março de 2010.

[28]http://www.smartcardalliance.org/latinamerica/translations/Logical_Access_Security_Portuguese.pdf acessado em 10 de março de 2010.

[29]http://www.soft2secure.com/2008/03/biometric-and-network-authentication-2.html acessado em 11 de março de 2010.

[30]http://commons.wikimedia.org/wiki/File:Fingerprint_scanner_identification.jpg acessado em 11 de março de 2010.

[31]http://www.gta.ufrj.br/grad/07_2/carlos_eduardo/Produtos.html acessado em 11 de março de 2010.

[32]http://www.infowester.com/biometria.php acessado em 11 de março de 2010.

[33]http://penta.ufrgs.br/pesquisa/fiorese/autenticacaoeadcap2.htm acessado em 11 de março de 2010.

[34]http://www.trgroup.com.br/upload/SISTEMAS_BIOMETRICOS%20DE%20VOZ%20__%20ANDAMENTO_ATE_19JANEIRO20090834.pdf acessado em 11 de março de 2010.

[35]http://www.via6.com/topico.php?tid=109871 acessado em 11 de março de 2010.

[36]http://www.eduardosilvestri.com.br/tecnologia/biometria/palestras/Conceitos%20de%20Biometria%20-%20Silvestri.pdf acessado em 11 de março de 2010.

[37]http://dcm-reality.blogspot.com/2008_01_13_archive.html acessado em 17 de março de 2010.

[38]http://www.fesppr.br/~erico/x%202007%20%20ADMINISTRA%C7%C3O%20-%20ASIG/Trabalhos%20111/EAN%2013%20s%20111.doc acessado em 11 de março de 2010.

[39]http://www.unifieo.br/v2/o_unifieo_cursos/artigo-matema/matematica-codigos-barra.pdf acessado em 28 de março de 2010.

[40]http://www.marcamp.com.br/produtos/11.html acessado em 28 de março de 2010.

[41]http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Lei/L11903.htm acessado em 30 de setembro de 2010.

[42]http://sites.unifra.br/Portals/36/2006/emprego.pdf acessado em 29 de setembro de 2010.

[43]http://oxxcode.com.br/index.php?option=com_content&view=article&id=150&Itemid=150 acessado em 29 de setembro de 2010.

[44] http://pt.wikipedia.org/wiki/QR_Code acessado em 29 de setembro de 2010.

[45]http://pt.wikipedia.org/wiki/C%C3%B3digo_Aztec acessado em 01 de outubro de 2010.

[46] http://en.wikipedia.org/wiki/PDF417 acessado em 01 de outubro de 2010.

[47] http://en.wikipedia.org/wiki/MaxiCode acessado em 01 de outubro de 2010.

[48]http://web.dexbrasil.com.br/index.php?option=com_content&task=view&id=15&Itemid=29 acessado em 02 de outubro de 2010.

[49]http://tec.brq.com/agilizando-captura-de-dados-em-eforms-com-codigo-de-barras-2d/ acessado em 02 de outubro de 2010.

[50]http://br.especiais.yahoo.com/plug-play/artigo/post/tech_noticias/65/Aprenda-mais-sobre-QR-Code.html acessado em 02 de outubro de 2010.

[51] https://repositorio.utad.pt/bitstream/10348/278/1/msc_jfmguedes.pdf acessado em 04 de outubro de 2010.

[52] http://www.metavendasbrazil.com.br/revista/tecnologia/77-nanotecnologia/27-rfid acessado em 04 de outubro de 2010.

[53]http://www.baixaki.com.br/info/2697-bokode-o-novo-concorrente-do-codigo-de-barras.htm acessado em 04 de outubro de 2010.

[54]http://www.abramcet.com.br/Forum_siniav.asp acessado em 04 de outubro de 2010.

[55]http://www.youtube.com/watch?v=QtTWHtGPgrI&NR=1- vídeo sobre SINIAV acessado em 28 setembro de 2010.

[56] http://www.youtube.com/watch?v=GYxRjYOcaA8 - vídeo sobre RFID e Diabetes acessado em 13 março de 2010.

[57] http://www.youtube.com/watch?v=cYO03VaE4JI&feature=related - vídeo sobre Passaporte BR acessado em 22 de setembro de 2010.

[58] http://www.youtube.com/watch?v=EEw-xmx7g1Y - vídeo sobre RFID Coe HP acessado em 28 de setembro de 2010.

[59]http://www2.camara.gov.br/legin/fed/lei/1997/lei-9454-7-abril-1997-349415-publicacao-1-pl.html acessado em 07 de outubro de 2010.

[60] http://www-di.inf.puc-rio.br/~endler/courses/Mobile/Monografias/07/RFID-MW-HubertFonseca-mono.pdf acessado em 24 de fevereiro de 2010.

GLOSSÁRIO

Acoplamento: A forma pela qual um circuito no identificador e um circuito no leitor influenciam um ao outro para enviar e receber informações ou força.

Acoplamento capacitivo: Uma forma de acoplamento na qual o leitor e o identificador possuem cada um patches condutivos que formam um capacitor quando colocados exatamente em paralelo entre si, mas sem se tocarem.

Acoplamento difuso de retorno (disperso): Uma forma de acoplamento que usa a energia refletida do leitor nas comunicações de identificadores.

Acoplamento indutivo: Uma forma de acoplamento na qual o leitor gera um campo magnético com uma antena espiral. O campo guia a corrente através de uma espiral no identificador por indução, muito parecido com a forma pela qual um transformador transfere energia entre duas espirais.

Adivinhação da senha, ”password guessing”: Método que um intruso pode usar para atacar sistemas baseados em senhas.

Algo que o usuário é, “something you are”: Método de autenticação de usuários que compõe a base de sistemas de controle de acesso baseado nas características físicas e biológicas dos indivíduos.

Algo que o usuário sabe, ”something you know”: Método de autenticação de usuários que compõe a base de sistemas de controle de acesso baseada no princípio de que apenas a pessoa legítima conhece uma determinada senha ou chave de acesso.

Algo que o usuário tem, “something you have”: Método de autenticação de usuários que compõe a base de sistemas de controle de acesso baseada no princípio de que o usuário legítimo é a pessoa que tem um determinado dispositivo, cartão ou chave para o acesso.

Ataque do dicionário, "dictionary attack": Método que um intruso pode usar para atacar sistemas baseados em senhas.

Autenticação: Mecanismo crítico para a segurança de qualquer sistema de informação automatizado que checa se a identidade dos usuários legítimos pode ser verificada com um grau aceitável de certeza.

Biometria: Definida como sendo as mensurações fisiológicas e/ou características de comportamento que podem ser utilizadas para verificação de identidade de um indivíduo.

"BioSMART": "Smart Card" integrado com um sistema de verificação de impressão digital fornecendo um sistema de identificação pessoal portável reduzindo os custos administrativos associados com a manutenção do banco de dados de modelos.

"Bokode": É uma palavra inventada, criada a partir da junção de duas outras palavras: "bokeh", palavra em japonês que significa mancha ou borrão, e é um termo técnico da área de fotografia, e "code", que significa código em inglês.

"Bull's eyes symbol": Primeiro código de barras desenvolvido por Bernard Silver e Joseph Woodland em 1948, tendo como base o Código Morse, representado em forma de barras circulares de diferentes espessuras e concêntricas.

Cavalo de Tróia, "**Trojan Horse"**: É um programa que age como a lenda do Cavalo de Tróia, entrando no computador e liberando uma porta para uma possível invasão.

Código Eletrônico de Produtos, **"Electronic Product Code" – EPC**: Define uma arquitetura que utiliza recursos oferecidos pela tecnologia de identificação por radiofreqüência e serve de referência para o desenvolvimento de novas aplicações. O EPC é uma forma de identificar produtos atribuindo a eles um número único que é inserido desde a linha de manufatura.

"Embossing": Cartões com o nome do cliente em alto relevo.

Engenharia Social: São as práticas utilizadas para obter acesso a informações importantes ou sigilosas em organizações ou sistemas por meio da enganação ou exploração da confiança das pessoas.

EPCglobal: A EPCglobal é uma divisão da EAN ,"European Article Number International", e do UCC , "Uniform Code Council". Trata-se de uma organização sem fins lucrativos criada para controlar, desenvolver e promover padrões baseados nas especificações do sistema EPC. Seu objetivo é orientar a adoção deste sistema como o padrão mundial para a identificação imediata, automática e precisa de qualquer item da cadeia de suprimentos de qualquer empresa, de qualquer setor e em qualquer lugar do mundo.

"FaceIt": Software que implementa método de autenticação para o uso em sistemas biométricos por meio de reconhecimento de face no qual é requerida uma câmera digital para a captura das imagens.

Filtro: É uma regra que rejeita alguns eventos ao mesmo tempo em que permite que outros passem.

Identificador: Um transportador de dados que anexa informações a um objeto físico.

"Imager": Tecnologia de leitura que se dá através de uma espécie de foto tirada do código bidimensional que é decodificada pelo equipamento leitor e posteriormente enviada para o sistema.

Leitor: Um sensor que se comunica com identificadores para observar suas identidades e então comunica essas observações a um hospedeiro. No caso de um identificador passivo ou semi-passivo, o leitor também fornece força ao identificador.

Minúcia biométrica: São os pontos de biometria que serão utilizados para gerar a identificação do usuário.

Monitoramento do tráfego na rede, "sniffing": Método que um intruso pode usar para atacar sistemas baseados em senhas.

Nanotecnologia: Um conjunto de técnicas usadas para manipular a matéria na escala de átomos e moléculas.

Nanotubos de carbono: São as "moléculas milagrosas" da nanotecnologia por serem mais resistentes que o aço e seis vezes mais leves e dependendo do método de produção, semicondutores ou isolantes.

Romaneio: Procedimento utilizado entre matrizes e filiais para a transferência de insumos, mercadorias ou produtos que constam em estoque. Também podemos definir como: documento que informa como o produto está organizado (embalado) em relação aos volumes. Ou seja, diz em que volume encontra-se determinado produto, ou ainda, o conteúdo de determinado volume.

"**Smart Cards"**: Consiste em um cartão de plástico com um chip que contem uma memória ROM, "read only memory" e, em alguns modelos, possui, além da memória, um microprocessador.

"Tag killing": Desativação das etiquetas RFID na caixa registradora dos mercados.

"TrueFace": Software que implementa método de autenticação para o uso em sistemas biométricos por meio de reconhecimento de face no qual é requerida uma câmera digital para a captura das imagens.

APÊNDICE 1 – IMPLEMENTAÇÃO EM JAVASCRIPT.

A função desta implementação é a de mostrar a geração de alguns tipos mais comuns de códigos de barras linear e bidimensional abordados nesta monografia a partir de dados fornecidos. Os códigos do programa encontram-se disponibilizados em mídia anexada à monografia.

A tela principal gerada pelo arquivo index1.html, conforme a figura 68, possibilita seguir para vários destinos como ir à página da UFJF; à do professor orientador da monografia; à dos códigos lineares; à dos códigos bidimensionais; à de um aplicativo em JavaScript de um relógio em código de barras e à de outros links interessantes.

Figura 68 Tela principal da implementação.

A tela gerada pelo arquivo implementalinear.html, conforme figura 69, possibilita acessar exemplificações correspondentes aos códigos de barras lineares dos tipos EAN-13, EAN-8, UPC, 39 e 25 intercalado.

Figura 69 Tela sobre alguns tipos de código de barras lineares.

Tela gerada pelo arquivo implementabidimensional.html, conforme figura 70, possibilita exemplificações correspondentes aos códigos de barras bidimensionais dos tipos Datamatrix, QR-Code, PDF-417, Aztec e MaxiCode.

Figura 70 Tela sobre alguns tipos de códigos de barras bidimensionais.

A tela gerada pelo arquivo implementa.html, conforme a figura 71 possibilita gerar código EAN-13 com base nas partes que o compõe. Permite escolher algum país do Mercosul e por meio de funções randômicas fornecem os números correspondentes ao fabricante e produto. Realiza também o cálculo do dígito verificador. A geração da

imagem do código produzido numericamente pode ser obtida através de um gerador local em JavaScript ou por meio de site especializado.

Figura 71 Tela sobre geração de código EAN-13.

A tela gerada pelo arquivo implementa1.html, conforme a figura 72 possibilita gerar código EAN-8 de forma semelhante à tela de geração do código EAN-13. A geração da imagem do código produzido numericamente pode ser obtida por meio de site especializado.

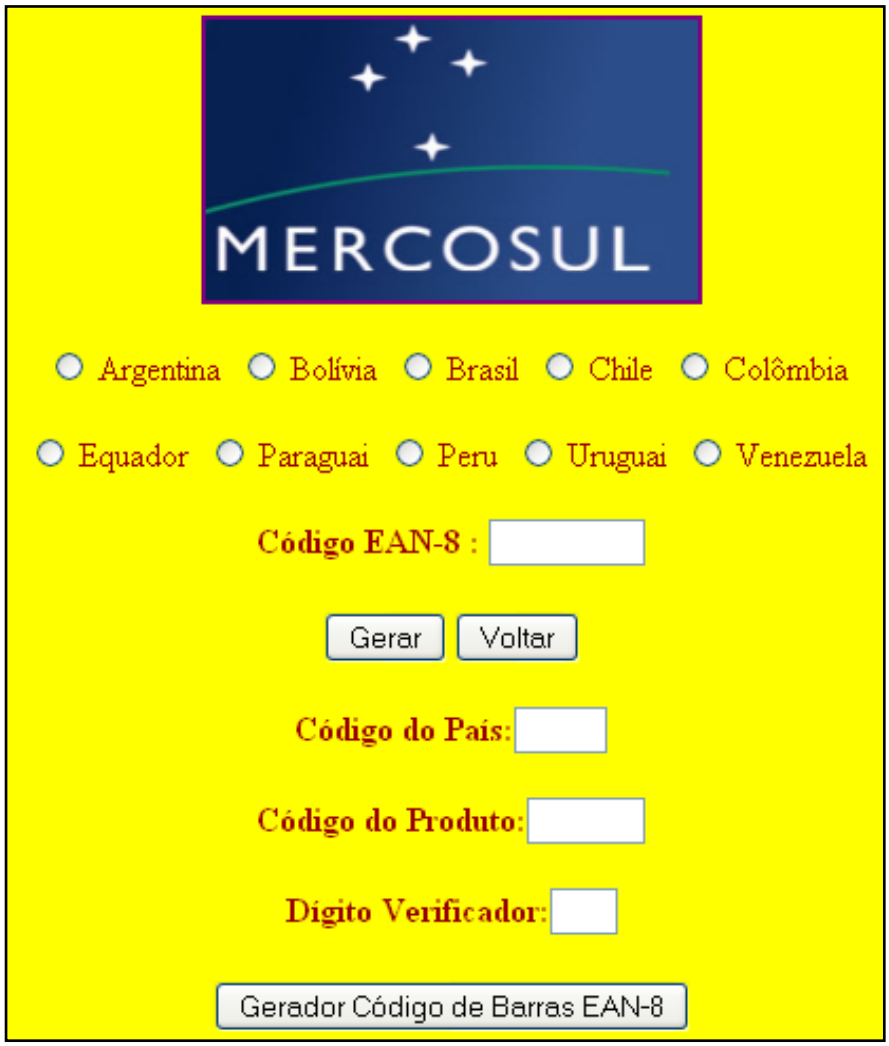


Figura 72 Tela sobre geração de código EAN-8.

A tela gerada pelo arquivo implementa2.html, conforme a figura 73 possibilita a composição numérica do código UPC por intermédio de funções randômicas e de cálculo de dígito verificador. A geração da imagem do código produzido numericamente pode ser obtida por meio de site especializado.

Existe nesta página um exemplo de conversão por passos deste código para o código eletrônico de produto SGTIN-96 utilizado em identificadores RFID o qual pode ser observado por meio da tela gerada pelo arquivo implementa3.html, conforme figura 74.

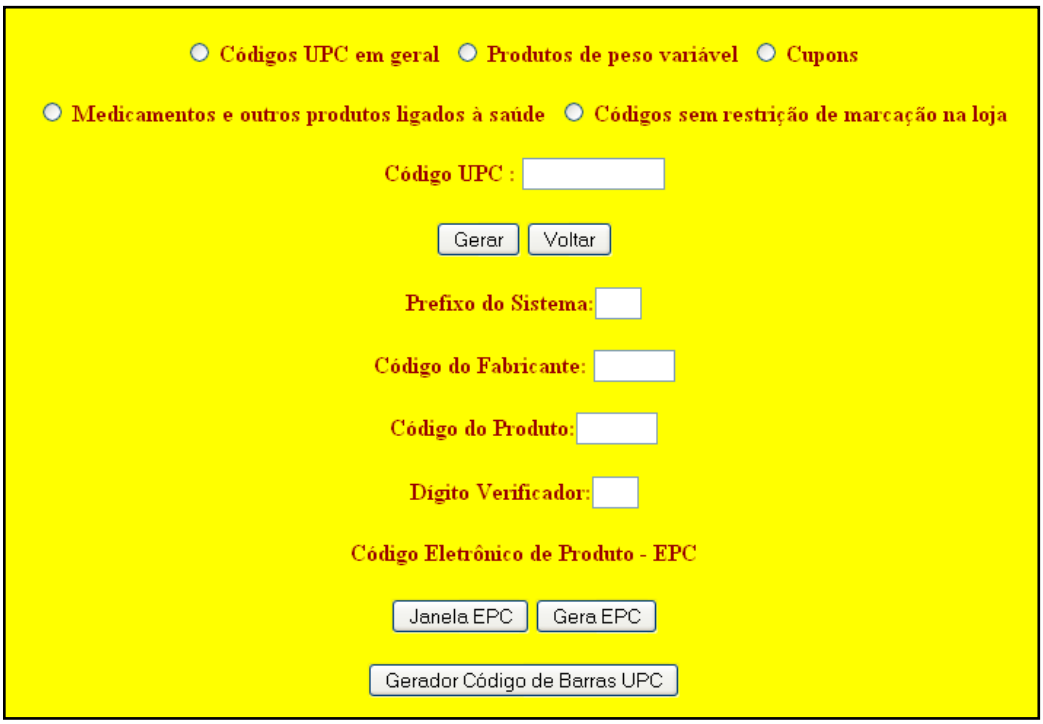


Figura 73 Tela sobre geração de código UPC.

Figura 74 Tela de conversão para código eletrônico de produto EPC-SGTIN.

A tela gerada pelo arquivo implementa4.html, conforme figura 75, nos traz a possibilidade de acessar links interessantes.

Figura 75 Tela sobre acesso a links interessantes.

As opções disponíveis são as páginas da internet especializadas em geração de códigos de barras, aplicativo em JavaScript de geração de um relógio em código de barras, geração local em JavaScript do código EAN-13 e acesso a sites que permitem baixar programas para aparelhos celulares que possibilitam a leitura de códigos de barras bidimensionais dos tipos Datamatrix e QR-Code.

ANEXO 1 - DECRETO E PORTARIA – IMPLANTAÇÃO DO CÓDIGO DE BARRAS NO BRASIL [3].

***DECRETO Nº 90.595 - 29 DE NOVEMBRO DE 1984**

"O Presidente da República, usando das atribuições que lhe confere o artigo 81, inciso III, da Constituição, decreta:

Art. 1º Fica criado o Sistema de Codificação nacional de Produtos, e definido o Padrão Internacional EAN, para todo Território Nacional. Parágrafo único - A Codificação nacional de Produtos de que trata este artigo, visa a identificação de Produtos, por equipamentos de automação, nas operações do Comércio, no Mercado Interno.

Art. 2º O Ministério da Indústria e do Comércio baixará normas complementares sobre implantação do Sistema.

Art. 3º Este Decreto entrará em vigor na data de sua publicação.

Art. 4º Ficam revogadas as disposições em contrário."

***PORTARIA Nº 143 - 12 DE DEZEMBRO DE 1984**

"O Ministro do Estado da Indústria e do Comércio, no uso de suas atribuições e tendo em vista a redação do artigo 2º, do Decreto n. 90.595, de 29 de novembro de 1984, Considerando as conclusões do Grupo de Trabalho criado pela Portaria MIC n. 55, de 1º de agosto de 1984, resolve:

Art. 1º. Conferir à ABAC - Associação Brasileira de Automação Comercial a competência para administrar, em todo Território Nacional, o Código Nacional de Produtos, Padrão EAN, aprovado pelo Decreto n. 90.595, de 29 de novembro de 1984.

Art. 2º. O Conselho de Desenvolvimento Comercial, através de seu Secretário-Executivo ou de seu substituto legal, coordenará a implantação do Sistema de Codificação nacional de Produtos.

Art. 3º. A implantação do Sistema de Codificação nacional de Produtos obedecerá ao Cronograma anexo, que faz parte integrante desta Portaria.

Parágrafo 1º - O Secretário-Executivo, na qualidade de Coordenador da implantação do Sistema, poderá concordar com eventuais alterações no Cronograma de Implantação, desde que motivos relevantes aconselham revisão das metas e/ou prazos nele estabelecidos.

Parágrafo 2º - As normas de que trata o Estágio 05 do Cronograma, serão estabelecidas pelo SINMETRO - Sistema Nacional de Metrologia, Normalização e Qualidade

Industrial, na forma da Lei n. 5.966, de 11 de setembro de 1973, compatibilizando-as com as normas internacionais.

Art. 4º. Esta Portaria entrará em vigor na data de sua publicação. "

ANEXO 2 - LEI – IMPLANTAÇÃO DO SISTEMA DE RASTREAMENTO DA PRODUÇÃO E DO CONSUMO DE MEDICAMENTOS POR MEIO DE TECNOLOGIA DE CAPTURA, ARMAZENAMENTO E TRANSMISSÃO [41].

LEI Nº 11.903, DE 14 DE JANEIRO DE 2009.

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1o É criado o Sistema Nacional de Controle de Medicamentos, envolvendo a produção, comercialização, dispensação e a prescrição médica, odontológica e veterinária, assim como os demais tipos de movimentação previstos pelos controles sanitários.

Art. 2o Todo e qualquer medicamento produzido, dispensado ou vendido no território nacional será controlado por meio do Sistema Nacional de Controle de Medicamentos.

Parágrafo único. O controle aplica-se igualmente às prescrições médicas, odontológicas e veterinárias.

Art. 3o O controle será realizado por meio de sistema de identificação exclusivo dos produtos, prestadores de serviços e usuários, com o emprego de tecnologias de captura, armazenamento e transmissão eletrônica de dados.

§ 1o Os produtos e seus distribuidores receberão identificação específica baseada em sistema de captura de dados por via eletrônica, para os seguintes componentes do Sistema Nacional de Controle de Medicamentos:

I – fabricante (autorização de funcionamento, licença estadual e alvará sanitário municipal dos estabelecimentos fabricantes);

II – fornecedor (atacadistas, varejistas, exportadores e importadores de medicamentos);

III – comprador (inclusive estabelecimentos requisitantes de produtos não aviados em receitas com múltiplos produtos);

IV – produto (produto aviado ou dispensado e sua quantidade);

V – unidades de transporte/logísticas;

VI – consumidor/paciente;

VII – prescrição (inclusive produtos não aviados numa receita com múltiplos produtos);

VIII – médico, odontólogo e veterinário (inscrição no conselho de classe dos profissionais prescritores).

§ 2o Além dos listados nos incisos do § 1o deste artigo, poderão ser incluídos pelo órgão de vigilância sanitária federal outros componentes ligados à produção, distribuição, importação, exportação, comercialização, prescrição e uso de medicamentos.

Art. 4o O órgão de vigilância sanitária federal competente implantará e coordenará o Sistema Nacional de Controle de Medicamentos.

Parágrafo único. O órgão definirá o conteúdo, a periodicidade e a responsabilidade pelo recebimento e auditoria dos balanços das transações comerciais necessários para o controle de que trata o art. 3o desta Lei.

Art. 5o O órgão de vigilância sanitária federal competente implantará o sistema no prazo gradual de 3 (três) anos, sendo a inclusão dos componentes referentes ao art. 3o desta Lei feita da seguinte forma:

I – no primeiro ano, os referentes aos incisos I e II do § 1o;

II – no segundo ano, os referentes aos incisos III, IV e V do § 1o;

III – no terceiro ano, os referentes aos incisos VI, VII e VIII do § 1o.

Art. 6o O órgão de vigilância sanitária federal competente estabelecerá as listas de medicamentos de venda livre, de venda sob prescrição e retenção de receita e de venda sob responsabilidade do farmacêutico, sem retenção de receita.

Art. 7o Esta Lei entra em vigor na data de sua publicação.

Brasília, 14 de janeiro de 2009; 188o da Independência e 121o da República.

LUIZ INÁCIO LULA DA SILVA

Reinhold Stephanes

Márcia Bassit Lameiro Costa

Mazzoli Miguel Jorge

ANEXO 3 – RESOLUÇÃO DO CONTRAN – IMPLANTAÇÃO DO SISTEMA DE IDENTIFICAÇÃO AUTOMÁTICA DE VEÍCULOS (SINIAV) EM TODO TERRITÓRIO NACIONAL [54].

RESOLUÇÀO No 212 DE 13 DE NOVEMBRO DE 2006

Dispõe sobre a implantação do Sistema de Identificação Automática de Veículos – SINIAV em todo o território nacional

O CONSELHO NACIONAL DE TRÂNSITO – CONTRAN, no uso das atribuições que lhe são conferidas pelo art. 12, da Lei nº 9.503, de 23 de setembro de 1997, que instituiu o Código de Trânsito Brasileiro – CTB, e conforme o Decreto nº 4.711, de 29 de maio de 2003, que trata da coordenação do Sistema Nacional de Trânsito;

Considerando o disposto no art. 114, do CTB, que atribui ao CONTRAN dispor sobre a identificação de veículos;

Considerando as atribuições conferidas ao CONTRAN pela Lei Complementar nº 121, de 9 de fevereiro de 2006, que cria o Sistema Nacional de Prevenção, Fiscalização e Repressão ao Furto e Roubo de Veículos e Cargas e dá outras providências;

Considerando a necessidade de empreender a modernização e a adequação tecnológica dos equipamentos e procedimentos empregados nas atividades de prevenção, fiscalização e repressão ao furto e roubo de veículos e cargas;

Considerando a necessidade de dotar os órgãos executivos de trânsito de instrumentos modernos e interoperáveis para planejamento, fiscalização e gestão do trânsito e da frota de veículos;

Considerando as conclusões do Grupo de Trabalho instituído pela Portaria nº 379, de 28 de julho de 2006, do Ministro de Estado das Cidades, publicada no D.O.U. nº 145, seção 2, de 31 de julho de 2006, e o que consta no processo 80000.014980/2006-61

RESOLVE:

Art. 1º Fica instituído em todo o território Nacional o Sistema Nacional de Identificação Automática de Veículos - SINIAV, baseado em tecnologia de identificação por rádio-freqüência, cujas características estão definidas no anexo II desta Resolução.

Parágrafo único. O SINIAV é composto por placas eletrônicas instaladas nos veículos, antenas leitoras, centrais de processamento e sistemas informatizados.

Art. 2º Nenhum veículo automotor, elétrico, reboque e semi-reboque poderá ser licenciado e transitar pelas vias terrestres abertas à circulação sem estar equipado com a placa eletrônica de que trata esta Resolução.

§1º A placa eletrônica será individualizada e terá um número de série único e inalterável para cada veículo.

§2º Os veículos de uso bélico estão isentos desta obrigatoriedade.

Art. 3º Cada placa eletrônica deverá conter, obrigatoriamente, as seguintes informações que, uma vez gravadas, não poderão ser alteradas:

I - Número serial único;

II - Número da placa do veículo;

III - Número do chassi; e

IV - Código RENAVAM.

Parágrafo único – A placa eletrônica de que trata este artigo deverá obedecer também o mapa de utilização de memória constante do Anexo II desta Resolução.

Art. 4º O SINIAV deverá estar implantado em todo o território nacional conforme o cronograma constante do Anexo I desta Resolução.

Art. 5º Cabe aos Órgãos Executivos de Trânsito dos Estados e do Distrito Federal a responsabilidade pela implantação e operação do SINIAV no âmbito do seu território.

Parágrafo único. Fica facultado aos Órgãos Executivos de Trânsito dos Estados estabelecerem convênios com os Municípios visando à implantação do SINIAV.

Art. 6º - As antenas leitoras e as placas eletrônicas deverão ser homologadas pelo DENATRAN, de acordo com as características técnicas especificadas no Anexo II desta Resolução.

Art. 7º - As informações obtidas através do SINIAV e que requeiram sigilo serão preservadas nos termos da Constituição Federal e das leis que regulamentam a matéria.

Art. 8º - O descumprimento do disposto no artigo 2º desta Resolução sujeitará o infrator à aplicação das sanções previstas no Art. 237, do Código de Trânsito Brasileiro .

Art. 9º - Esta Resolução entra em vigor na data de sua publicação, observado o cronograma fixado no artigo 4º .

Alfredo Peres da Silva

Presidente

Fernando Marques de Freitas

Ministério da Defesa – Suplente

Rodrigo Lamego de Teixeira Soares

Ministério da Educação – Titular

Carlos Alberto Ferreira dos Santos

Ministério do Meio Ambiente – Suplente

Valter Chaves Costa

Ministério da Saúde – Titular

Edson Dias Gonçalves

Ministério dos Transportes – Titular

ANEXO 4 – LEI – INSTITUI O NÚMERO ÚNICO DE REGISTRO DE IDENTIDADE CIVIL E DÁ OUTRAS PROVIDÊNCIAS [59] .

Lei nº 9.454, de 7 de Abril de 1997

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º. É instituído o número único de Registro de Identidade Civil, pelo qual cada cidadão brasileiro, nato ou naturalizado, será identificado em todas as suas relações com a sociedade e com os organismos governamentais e privados.

Parágrafo único. (VETADO)

I - (VETADO)

II - (VETADO)

III - (VETADO)

Art. 2º. É instituído o Cadastro Nacional de Registro de Identificação Civil, destinado a conter o número único de Registro Civil acompanhado dos dados de identificação de cada cidadão.

Art. 3º. O Poder Executivo definirá a entidade que centralizará as atividades de implementação, coordenação e controle do Cadastro Nacional de Registro de Identificação Civil, que se constituirá em órgão central do Sistema Nacional de Registro de Identificação Civil.

§ 1º O órgão central do Sistema Nacional de Registro de Identificação Civil será representado, na Capital de cada Unidade da Federação, por um órgão regional e, em cada Município, por um órgão local.

§ 2º Os órgãos regionais exercerão a coordenação no âmbito de cada Unidade da Federação, repassando aos órgãos locais as instruções do órgão central e reportando a este as informações e dados daqueles.

§ 3º Os órgãos locais incumbir-se-ão de operacionalizar as normas definidas pelo órgão central repassadas pelo órgão regional.

Art. 4º. Será incluída, na proposta orçamentária do órgão central do sistema, a provisão de meios necessários, acompanhada do cronograma de implementação e manutenção do sistema.

Art. 5º. O Poder Executivo providenciará, no prazo de cento e oitenta dias, a regulamentação desta Lei e, no prazo de trezentos e sessenta dias, o início de sua implementação.

Art. 6º. No prazo máximo de cinco anos da promulgação desta Lei, perderão a validade todos os documentos de identificação que estiverem em desacordo com ela.

Art. 7º. Esta Lei entra em vigor na data de sua publicação.

Art. 8º. Revogam-se as disposições em contrário.

Brasília, 7 de abril de 1997; 176º da Independência e 109º da República.

FERNANDO HENRIQUE CARDOSO

Nelson A. Jobim