



**UNIVERSIDAD NACIONAL AUTÓNOMA  
DE MÉXICO**

---

**FACULTAD DE INGENIERÍA**

**DISEÑO Y CONSTRUCCIÓN DE  
UN DISPOSITIVO CON  
TECNOLOGIA RFID**

**T E S I S**

**QUE PARA OBTENER EL TÍTULO DE:**

**INGENIERO MECÁNICO ELECTRICISTA  
(AREA ELÉCTRICA ELECTRÓNICA)**

**P R E S E N T A :**

**ARMANDO LOPEZ VILLELA**

**DIRECTOR DE TESIS:**

**M. I. JORGE VALERIANO ASSEM**

**México D.F. 23 de Marzo de 2006**





Universidad Nacional  
Autónoma de México



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

## ***AGRADECIMIENTOS***

### ***A la Memoria de mi Padre***

Por tu ejemplo, tu apoyo y sobre todo por tu cariño que me ha impulsado a seguir adelante y enfrentar los retos.

### ***A mi Madre***

Por tu gran amor que mantengo siempre conmigo.

### ***A mis Hermanas y Hermanos***

Por su apoyo y estímulo que me han ayudado a llegar hasta aquí.

### ***A Leticia Villagómez***

Por tu profesionalismo, tu dedicación y paciencia.

### ***A Ivette***

Por convertirte en la luz de mi vida, por estar junto a mí impulsándome y amándome. Gracias por la felicidad que llegó contigo.

## INDICE

|  |           |
|--|-----------|
| <b>INTRODUCCION.....</b>   | <b>1</b>  |
| <b>CAPITULO I. SISTEMAS DE IDENTIFICACIÓN AUTOMÁTICA.....</b>        | <b>2</b>  |
| I.1. Sistemas de código de barras.....                               | 4         |
| I.1.1. Historia.....   | 4         |
| I.1.2. Tipos de Código de Barras.....                                | 6         |
| I.1.3. Aplicaciones.....   | 6         |
| I.2. Reconocimiento Óptico de Caracteres (OCR). ....                 | 11        |
| I.2.1. Historia.....   | 11        |
| I.2.1. Tipos de OCR.....   | 12        |
| I.2.3. Aplicaciones.....   | 14        |
| I.3. Banda Magnética.....  | 15        |
| I.4. Tarjetas Inteligentes.....                                      | 17        |
| I.4.2. Tipos de Tarjetas Inteligentes.....                           | 18        |
| I.4.2.1. Tarjeta Inteligente de Contacto.....                        | 18        |
| I.4.2. Tarjeta Inteligente sin Contacto.....                         | 19        |
| I.5. Sistemas Biométricos.....                                       | 19        |
| I.5.1. Técnicas Biométricas.....                                     | 21        |
| I.5.2. Aplicaciones.....   | 23        |
| I.6. Identificación por Radiofrecuencia.....                         | 24        |
| <b>CAPITULO II. FUNDAMENTOS DE LA TECNOLOGÍA RFID.....</b>           | <b>28</b> |
| II.1. Diferencias Fundamentales en los Sistemas RFID.....            | 29        |
| II.2. Tipos de Sistemas RFID.....                                    | 32        |
| II.2.1. Sistemas de 1 bit.....                                       | 33        |
| II.2.1.1. Radiofrecuencia.....                                       | 33        |
| II.2.1.2. Microondas.....  | 34        |
| II.2.1.3. Divisor de Frecuencia.....                                 | 36        |
| II.2.1.4. Electromagnético.....                                      | 36        |
| II.2.1.5. Acústico.....  | 37        |
| II.2.2. Sistemas de $n$ -bits.....                                   | 39        |
| II.2.2.1. Procedimiento Full y Half Duplex.....                      | 40        |
| II.2.2.2. Sistemas de Procedimientos Secuenciales.....               | 48        |
| II.4. Normalización.....   | 50        |
| II.3.1. Identificación de Animales.....                              | 50        |
| II.3.2. Tarjetas Inteligentes Libre de Contacto.....                 | 51        |
| II.3.3. ISO 69873 – Portadores de Datos para Herramientas.....       | 52        |
| II.3.4. Identificador de Contenedores.....                           | 52        |
| II.3.5. VDI 4470 –Sistemas Antirrobo de Bienes.....                  | 52        |
| <b>CAPITULO III. COMPONENTES DE HARDWARE DE UN SISTEMA RFID.....</b> | <b>53</b> |
| III.1. Dispositivo Lector.....                                       | 54        |
| III.1.1. Componentes de un Lector.....                               | 55        |
| III.1.1.1. Interfaz de Alta Frecuencia.....                          | 55        |

|   |            |
|---|------------|
| III.1.1.2. Unidad de Control.....   | 59         |
| III.1.2. Tipos de Lector.....   | 60         |
| III.1.2.1. Lectores OEM.....  | 60         |
| III.1.2.2. Lectores para Uso Industrial.....  | 61         |
| III.1.2.3. Lectores Portátiles.....   | 61         |
| III.2 Transponder.....  | 62         |
| III.2.1. Transponder con Función de Memoria.....  | 66         |
| III.2.1.1. Interfaz HF.....   | 66         |
| III.2.1.2. Lógica de Direcciones y Seguridad.....   | 67         |
| III.2.2. Transponder con Microprocesador.....   | 69         |
| III.2.3. Tecnología de Memoria.....   | 70         |
| III.2.3.1. RAM.....   | 70         |
| III.2.3.2. EEPROM.....  | 71         |
| III.2.3.3. FRAM.....  | 71         |
| <b>CAPITULO IV. ANALISIS DE LOS COMPONENTES DE HARDWARE UTILIZADOS<br/>EN EL SISTEMA.....</b> | <b>73</b>  |
| IV.1. Requerimientos y definición del Sistema.....  | 74         |
| IV.2. Transponder.....  | 77         |
| IV.3. Lector.....   | 80         |
| IV.4. Dispositivo <i>Handheld</i> .....   | 84         |
| IV.5. Fuente de Poder.....  | 89         |
| <b>CAPITULO V. ANALISIS Y DISEÑO DEL SOFTWARE DEL SISTEMA.....</b>                            | <b>93</b>  |
| V.1. Requerimientos del Sistema.....  | 94         |
| V.2. Protocolo de Comunicación con el Lector.....   | 97         |
| V.3. Plataforma de Desarrollo.....  | 100        |
| V.3.1. <i>JAVA Micro Edition (J2ME)</i> .....   | 101        |
| V.3.2. <i>.NET Compact Framework</i> .....  | 105        |
| V.4. Módulo de captura de datos.....  | 114        |
| V.5. Módulo de Almacenamiento de Datos.....   | 115        |
| <b>CAPITULO VI. CONSTRUCCION Y RESULTADOS.....</b>  | <b>117</b> |
| VI.1. Construcción del Dispositivo.....   | 118        |
| VI.2. Pruebas y Resultados.....   | 122        |
| <b>CONCLUSIONES.....</b>  | <b>124</b> |
| <b>APÉNDICE 1. Comandos Disponibles en el SIRIT ST-200.....</b>                               | <b>125</b> |
| <b>APÉNDICE 2. Códigos de Error del SIRIT ST-200.....</b>                                     | <b>127</b> |
| <b>BIBLIOGRAFIA.....</b>  | <b>128</b> |

## INTRODUCCION

El Laboratorio de Microsoft cuenta en éste momento con 20 equipos de cómputo que probablemente se incrementarán en un período cercano y además cuenta con otros dispositivos como impresora, puntos de acceso y dispositivos móviles. En cada uno de éstos equipos hay una etiqueta adherida que es inspeccionada visualmente para obtener y asentar manualmente el número de inventario.

Esta actividad es realizada por lo menos una vez al año ya que la DGSCA (Dirección General de Servicios de Cómputo Académico) solicita periódicamente un inventario que generalmente es necesario realizar en un plazo corto, lo que agrega una presión de tiempo a ésta tarea y que fácilmente puede provocar errores en la realización de la misma.

**El presente trabajo consiste en el diseño y construcción de un dispositivo que utilice la tecnología RFID (Identificación por Radiofrecuencia) para realizar inventarios en el Laboratorio de Microsoft de la Facultad de Ingeniería. Este dispositivo será capaz de:**

- **Realizar el inventario de manera rápida sin que exista necesariamente línea de vista entre el dispositivo y los bienes.**
- **Leer y escribir en las tarjetas de RFID, utilizadas para identificar los bienes.**
- **Será utilizado fácilmente en cualquier área de la Facultad de Ingeniería para la realización de Inventarios.**
- **Portátil.**
- **Localizar un bien en particular, indicándolo mediante una alarma audible y/o visual.**

La utilización de un método para realizar inventarios que no involucre la participación humana en la lectura y escritura de datos, con las características de rapidez, efectividad y confiabilidad adecuadas, permite que los errores se minimicen considerablemente con consecuencias positivas en el ahorro de recursos.

El gasto inicial en un sistema de éstas características se ve amortizado rápidamente por los beneficios tangibles de ahorro, tanto de tiempo como de dinero, así como los beneficios intangibles que se obtienen con una mejor planeación y aprovechamiento de los recursos existentes.

La realización de un proyecto que involucre sistemas de identificación automática, implicará dar un paso importante en la utilización de nuevas tecnologías en la Facultad de Ingeniería. Esto se sumará a otros esfuerzos que en el mismo sentido son realizados en distintas áreas y coadyuvará con el propósito de mantener nuestra Institución a la vanguardia en el uso de nuevas tecnologías.

# **Sistemas de Identificación Automática**

I.1 Código de Barras

I.2 Reconocimiento Óptico de Caracteres (OCR)

I.3 Banda Magnética

I.4 Tarjetas Inteligentes

I.5 Sistemas Biométricos

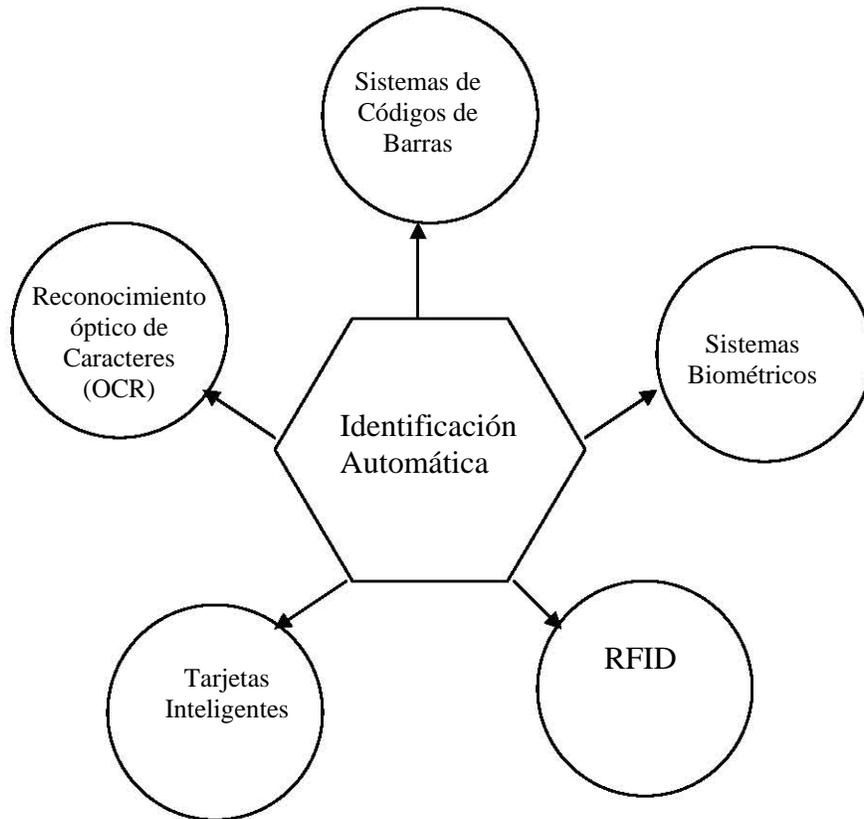
I.6 Identificación por Radiofrecuencia (RFID)

## **Capítulo 1**

## CAPITULO I. SISTEMAS DE IDENTIFICACIÓN AUTOMÁTICA

Los sistemas de identificación automática han tenido un crecimiento notable en los últimos años, principalmente a partir del uso extensivo que se le ha dado a los códigos de barras para la identificación de productos. Ha sido también notorio el desarrollo de diferentes tecnologías y la aplicación de otras ya existentes en la solución de problemas específicos de identificación.

En la figura I.1 se muestran algunos de los procedimientos de identificación automática más comunes. Estos procedimientos utilizan tecnologías de diferente tipo, entre las que se encuentran las telecomunicaciones, semiconductores, manufactura y hasta criptografía que juntos conforman soluciones efectivas de identificación.



[1] *Figura I.1. Procedimientos más importantes de identificación automática.*

[1] Finkenzeller, K. *RFID Handbook*. Segunda Edición. 2004. John Wiley & Sons, Ltd. West Sussex. UK. 2.

## I.1. SISTEMAS DE CODIGO DE BARRAS

Conocidos hoy por una buena parte de la humanidad, los códigos de barras son una técnica de entrada de datos (tal como la captura manual, el reconocimiento óptico y la cinta magnética), con imágenes formadas por combinaciones de barras y espacios paralelos, de anchos variables (figura I.2). Representan números que a su vez pueden ser leídos y descifrados por lectores ópticos o *scanners*.

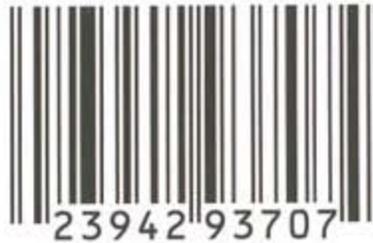


Figura I.2. Código de Barras típico.

El código sirve para identificar los productos de forma única pues cuenta con información detallada del artículo o del documento que los contiene, a través de una asociación con una base de datos.

### I.1.1. Historia

En 1948 una empresa norteamericana se acercó al Drexel Institute of Technology en Filadelfia buscando una solución para leer información automáticamente. Aunque la Universidad declinó el proyecto, Bob Silver y Norman Joseph Woodland lo tomaron en sus manos.

Ellos llegaron a varias soluciones, incluyendo un código de barras lineal y un “bull’s eye code” el cual consistía en una serie de círculos concéntricos y además trabajaron en un prototipo para leerlos. En 1952 Silver y Woodland lograron una patente por sus ideas, pero después de recibir varias ofertas la vendieron a *Philco Corporation*, quien después la vendió a *RCA Corporation*.

En 1961 aparece el primer escáner fijo de códigos de barras instalado por *Silvana General Telephone*. Este aparato leía barras de colores rojo, azul, blanco y negro identificando vagones de ferrocarriles.

En 1967 la Asociación de Ferrocarriles de Norteamérica aplica códigos de barras para control de tránsito de embarques. El proyecto no duró mucho por falta de mantenimiento adecuado de las etiquetas conteniendo los códigos. En ese mismo año, como respuesta a un llamado realizado por la Asociación Nacional de cadenas de Alimentos (NAFC), la RCA instaló el primer cajero que leía automáticamente los códigos de producto utilizando el “bull’s eye code”.

Sin embargo, hubo problemas con el código RCA y se reconoció la necesidad de que la industria llegara a un acuerdo de codificación estándar abierto a todos los fabricantes de equipo. En respuesta se estableció un consorcio que estableciera los lineamientos para el desarrollo del código de barras.

Por esa época, George Laurer de IBM, basado en las ideas de Woodland, inventó un código de barras rectangulares. Como resultado se formó un comité especial para escuchar las posiciones de RCA e IBM, encontrando que el código de IBM presentaba menos distorsión y que el tamaño podía ser reducido.

El 3 de Abril de 1973, éste comité liberó el CODIGO Universal de Producto (UPC), con pocas modificaciones a la propuesta de IBM. Europa se hace presente con su propia versión de UPC en 1976, con el código EAN (European Article Number). La figura I.3 muestra ejemplos de éstos códigos:



Figura I.3. Códigos de barras UPC-A, UPC-E, EAN-8 y EAN-13.

Los adelantos tecnológicos traen la aparición del primer sistema de verificación de barras por medio de láser en 1978 y el uso de CCD (Charge Coupled Device) en 1981. Éste último en la actualidad tiene bastante difusión en el mercado asiático, mientras que el láser domina el mundo occidental.

En 1987 el Dr. Allais desarrolla el primer código bidimensional, el código 49. Le sigue Ted Williams (*Laser Light Systems*) con el código 16K (1988).

En 1990 se publica la especificación ANS X3.182, que regula la calidad de impresión de códigos de barras lineales. En ese mismo año, Symbol Technologies presenta el código bidimensional PDF417 (figura I.4).



*Figura 1.4. Código de barras PDF417.*

### **I.1.2. Tipos de Códigos de Barras**

Actualmente hay una gran variedad de simbologías de códigos de barras, que se puede dividir básicamente en dos categorías: Lineales, que son llamadas así porque son hechos por una serie de líneas de diferente ancho, y bidimensionales en las cuales como su nombre lo indica, la información se codifica en un plano de dos dimensiones.

Las diferentes simbologías tienen diferentes capacidades para almacenar datos. Por ejemplo, la simbología para identificar productos al menudeo siempre contiene 12 dígitos numéricos mientras que el propósito general de las simbologías del código 39 o del código 128 pueden codificar una longitud variable de datos alfanuméricos de hasta 30 caracteres.

Las nuevas simbologías de códigos de barras bidimensionales como el PDF417, el código Azteca y el Data Matriz poseen la capacidad de codificar miles de bytes de datos en un simple símbolo de código de barras incluyendo texto o datos binarios.

### **I.1.3. Aplicaciones**

Las aplicaciones de los códigos de barras son muy variadas ya que su utilización se ha generalizado principalmente en las dos décadas pasadas. En la actualidad vemos los códigos de barras prácticamente en cada producto que compramos y en ocasiones en la correspondencia que recibimos.

La utilización más generalizada por el volumen que se maneja, es la identificación de productos que se venden al menudeo en tiendas y supermercados. En este caso el tipo de simbología más utilizado son el UPC-A y el EAN-13.

También existen aplicaciones muy especializadas como la mensajería o la correspondencia. En éste caso, en los estados unidos se utiliza la simbología Postnet, el cual se puede apreciar en la figura 1.5.



Figura 1.5. Código de barras Postnet.

En la tabla I.1 se resume la información de algunas de las simbologías lineales y bidimensionales.

| Código de Barras | Tipo   | Caracteres        | Longitud  | Checksum  | Aplicación /Comentarios   |
|------------------|--------|-------------------|---|-----------|---|
| EAN-13           | Lineal | Números Solamente | 12 dígitos de datos y 1 dígito de verificación; 2 o 5 dígitos suplementarios opcionales | Requerido | Mundialmente en venta de productos al menudeo.  |
| EAN-8            | Lineal | Números Solamente |   | Requerido | Mundialmente en venta de productos al menudeo; código comprimido para productos con espacio limitado en la etiqueta |
| EAN Bookland     | Lineal | Números Solamente |   | Requerido | Uso especial de la simbología EAN-13 para codificar números ISBN en libros.   |

Tabla I.1 Comparativo de Simbología de Códigos de Barras

| Código de Barras                         | Tipo   | Caracteres        | Longitud  | Checksum                     | Aplicación /Comentarios  |
|--|--------|-------------------|---|------------------------------|--|
| UPC-A                                    | Lineal | Números Solamente | 11 dígitos de datos y 1 dígito de verificación; 2 o 5 dígitos suplementarios opcionales | Requerido                    | Marcación de productos al menudeo en USA y Canadá  |
| UPC-E                                    | Lineal | Números Solamente |   | Requerido                    | Productos al menudeo en USA y Canadá; código comprimido para productos con espacio de etiqueta limitado.         |
| UPC Shipping Container Code (ITF-14)     | Lineal | Números Solamente | 13 dígitos de datos y 1 dígito verificador  | Requerido                    | Uso especial del código ITF (Interleaved 2 de 5) para marcar envíos que contienen productos con codificación UPC |
| UCC/EAN Shipping Container Code (SCC-14) | Lineal | Números Solamente | 13 dígitos de datos y 1 dígito verificador  | Requerido                    | Uso especial del código 128 para marcar envíos que contienen productos con codificación UPC.                     |
| Code 11                                  | Lineal | Números Solamente | Variable  | 1 Requerido<br>2 Recomendado |  |
| Interleaved 2 of 5                       | Lineal | Números Solamente | Variable  | Opcional                     | Muy compacto. Codifica dígitos en pares de manera que la longitud total debe ser un número impar de dígitos.     |
| Industrial 2 of 5                        | Lineal | Números Solamente | Variable  | No definido                  | Tipo de código antiguo   |
| Standard 2 of 5                          | Lineal | Números Solamente | Variable  | No definido                  | Tipo de código antiguo   |

Tabla I.1 Comparativo de Simbología de Códigos de Barras (continuación)

| Código de Barras                   | Tipo                          | Caracteres  | Longitud                                   | Checksum    | Aplicación /Comentarios   |
|------------------------------------|-------------------------------|---|--|-------------|---|
| Codabar (USD-4, NW-7, 2 of 7)      | Lineal                        | Números: 0-9;<br>Símbolos: - : . \$ / +<br>Caracteres Start/Stop: A, B, C, D, E, *, N, or T | Variable                                   | No definido | Código antiguo; utilizado con frecuencia en librerías y bancos de sangre.                 |
| Plessey                            | Lineal                        | Números Solamente   | Variable                                   | Requerido   | Etiquetas de estante de tiendas al menudeo  |
| MSI (MSI Plessey)                  | Lineal                        | Números Solamente   | Variable                                   | Requerido   | Etiquetas de estante de tiendas al menudeo  |
| OPC (Optical Industry Association) | Lineal                        | Números Solamente   | 9 dígitos de datos y 1 dígito verificador  | Requerido   | Uso especial del código ITF (Interleaved 2 of 5) para marcar productos ópticos al menudeo |
| Postnet                            | Codificado de Altura de Barra | Números Solamente   | 5, 9, or 11 dígitos y 1 dígito verificador | Requerido   | Código Postal USA (código ZIP)  |
| Code 39                            | Lineal                        | Letras Mayúsculas A-Z<br>Números 0-9<br>Espacio - . \$ / + %                                | Variable                                   | Opcional    | De uso amplio para muchos tipos de aplicaciones   |
| Code 93                            | Lineal                        | Letras Mayúsculas A-Z<br>Números 0-9<br>Espacio - . \$ / + %                                | Variable                                   | Opcional    | Un primo compacto del código 39, aunque no tan ampliamente utilizado                      |

Tabla I.1 Comparativo de Simbología de Códigos de Barras (continuación)

| <b>Código de Barras</b> | <b>Tipo</b>   | <b>Caracteres</b>  | <b>Longitud</b>   | <b>Checksum</b>     | <b>Aplicación /Comentarios</b>   |
|-------------------------|---------------|--|---|---------------------|--|
| Extended Code 39        | Lineal        | Todos los Caracteres ASCII y Códigos de Control          | Variable  | Opcional            | Utiliza pares de caracteres para codificar símbolos no estándar con mucho desperdicio de espacio.                      |
| Code 128                | Lineal        | Todos los Caracteres ASCII y Códigos de Control          | Variable  | Requerido           | Ampliamente utilizado, excelente para muchos tipos de aplicaciones   |
| UCC/EAN-128             | Lineal        | Todos los Caracteres ASCII y Códigos de Control          | Variable  | Requerido           | Emisión especial del código 128 que define formatos de datos para especificaciones de comercio                         |
| LOGMARS                 | Lineal        | Letras Mayúsculas A-Z; números 0-9; espacio - . \$ / + % | Variable  | Opcional            | Mismo que el código 39, ésta es la especificación del gobierno norteamericano  |
| PDF-417                 | Bidimensional | Todos los caracteres ASCII                               | Variable, hasta 1850 caracteres ASCII o 2725 caracteres numéricos | Corrección de error |  |
| DataMatrix              | Bidimensional | Todos los caracteres ASCII                               | Variable hasta 2335 caracteres ASCII                              | Corrección de error |  |
| Maxicode                | Bidimensional | Todos los caracteres ASCII                               | 93 caracteres ASCII   | Corrección de error | Desarrollado por la empresa de mensajería UPS para el codificado de destinos en la selección automática de paquetería. |
| QR Code                 | Bidimensional | Todos los caracteres ASCII                               | Variable, hasta 1520 caracteres ASCII o 2509 caracteres numéricos | Corrección de error |  |

Tabla I.1 Comparativo de Simbología de Códigos de Barras (continuación)

Es de suponer que dadas las características de bajo costo y fácil implantación de los sistemas de códigos de barras, su utilización está asegurada por un largo período, ya que las tecnologías alternas presentan todavía dificultades técnicas y costos superiores.

## **I.2. RECONOCIMIENTO ÓPTICO DE CARACTERES**

EL reconocimiento óptico de caracteres (OCR) consiste en tomar información de una fuente de entrada, convertirla en señales electrónicas que puedan ser almacenadas y procesadas en una computadora y obtener una salida en un momento determinado.

La información a ser tratada puede ser un documento escrito a mano, mecanografiado o impreso en papel. Las diferentes fuentes de entrada son, entre otras, un escáner óptico para el reconocimiento de caracteres (OCR), video digitalizado o información residente en un archivo.

### **I.2.1 Historia**

Los intentos de Ingeniería por lograr un sistema de reconocimiento automatizado de caracteres impresos iniciaron antes de la segunda guerra mundial. Pero no fue hasta los inicios de la década de 1950 que fue identificada una necesidad comercial que justificara la recaudación de fondos para financiar la investigación y el desarrollo de ésta tecnología. Éste ímpetu lo proporcionó la Asociación Americana de Banqueros y la Industria de Servicios Financieros. Ellos retaron a los mayores fabricantes de equipos que llegaron a un “lenguaje común” para procesar cheques automáticamente. Después de la guerra, el procesamiento de cheques se había convertido en aplicación más grande de proceso de papel en el mundo. Aunque la industria bancaria eventualmente escogió el Reconocimiento de Caracteres por Tinta magnética (MICR), algunos fabricantes habían propuesto el reconocimiento óptico de caracteres. Sin embargo, en ése momento el OCR estaba en las primeras etapas de desarrollo y no funcionó tan aceptablemente como el MICR.

El lector de los primeros equipos OCR utilizaba espejos, luces, aberturas fijas para la luz reflejada y un disco movable con rendijas adicionales. La imagen reflejada se rompía en bits discretos de datos en blanco y negro, presentado a un tubo foto-multiplicador y convertido en bits electrónicos.

El procesador lógico requería de la presencia o ausencia de bits de datos “negro” o “blanco” a intervalos regulares. Esto permitía conocer un juego de caracteres muy limitado que tenía que ser especialmente diseñado.

Para lograr esto, las unidades requerían de transportes muy sofisticados para los documentos que eran procesados. Era necesario también que los documentos pasaran a velocidad constante y los datos impresos estuvieran en una posición fija.

La siguiente generación de equipos, introducida de mediados hasta finales de la década de 1960, utilizaban un tubo de rayos catódicos, un lápiz de luz y fotomultiplicadores en una técnica llamada "Seguimiento de curva". Estos sistemas ofrecían mayor flexibilidad tanto en la posición de los caracteres como en el diseño de los mismos o el tipo de letra que sería leído. Fue ésta técnica la que introdujo el concepto de que los caracteres manuscritos podían ser leídos automáticamente, particularmente si se utilizaban ciertas restricciones.

La tercera generación de dispositivos de reconocimiento introducida a principios de 1970, consistía en arreglos de fotodiodos. Estos pequeños sensores estaban alineados en un arreglo de manera tal que la imagen reflejada de un documento pasaría a una velocidad determinada.

Concurrentemente con la tecnología de los microprocesadores, la tecnología OCR dio un paso de gigante a finales de los 70 y principios de los 80. La nueva generación de los escáneres OCR permitía leer distintos estilos de tipo de letra comúnmente utilizados en una oficina, tales como los Courier 10, Pica, Prestige Elite, Letra Gótica, etc. Mejoró la precisión de la exploración, así como el nuevo software añadido para el proceso adicional por pasos, aplicable a un amplio rango de condiciones.

Actualmente, los sistemas de reconocimiento óptico de caracteres son capaces de leer y reconocer textos manuscritos o escritos a máquina, de imprenta o de impresora, convirtiéndolos a texto ASCII, editable por el usuario con cualquier programa de tratamiento de textos convencional.

En teoría, un buen OCR es capaz de leer texto de imprenta en varios tipos de letra, en distintos formatos (columnas, cuadros, etc) y con caracteres especiales (acentos, signos ortográficos, etc.). Hasta hace relativamente poco tiempo, los OCR eran muy imprecisos propensos a múltiples errores. En éstos momentos se emplean sistemas inteligentes que aprenden sobre la marcha o con ayuda del usuario, que además consultan diccionarios y se corrigen a sí mismos.

La precisión que se obtiene de éstos sistemas es bastante alta, aunque es difícil alcanzar el 100%.

### **I.2.2 Tipos de OCR**

La tecnología inicial de OCR requería que el soporte para la exploración estuviera impreso en un papel especial utilizando fuentes de caracteres específicas. La fuente OCR-A fue la primera desarrollada para este propósito, siendo diseñada para ser legible por una máquina, resultando ligeramente difícil para la lectura directa por una persona. La figura I.6 muestra la tipografía OCR-A.

ABCDEFGHIJKLMNOP  
 QRSTUVWXYZÀÁÉÎÏÕØÜ  
 abcdefghijklmnop  
 qrstuvwxyzàáéíõøü&  
 1234567890(£. , ! ? )

*Figura 1.6. Tipografía OCR-A*

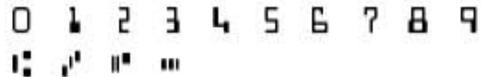
Al inicio de los años 70, una alternativa a la anterior fue utilizar un pequeño código de barras colocado debajo de caracteres normales escritos a máquina; el código de barras era explorado y los caracteres así codificados, una vez capturados, eran procesados. Este método, como el OCR-A, estaba limitado a una única fuente y un hardware especial diseñado para leer los caracteres de esta forma codificados.

A finales de los 70, una nueva fuente, el OCR-B, alcanzó un uso mucho más extendido. Era más fácil de leer y se parecía a un tipo de letra conocido como letra gótica. Sin embargo, tenía muchas limitaciones ya que el hardware existente sólo permitía leer documentos preparados con esa fuente especial. La precisión de los escáneres OCR no era la suficiente por lo que los documentos tenían que ser verificados y corregidos en pantalla, antes de poder ser usados. La figura 1.7 muestra la tipografía OCR-B.

ABCDEFGHIJKLMNOP  
 QRSTUVWXYZ , ÁÉÎÏØÜ  
 abcdefghijklmnop  
 qrstuvwxyzàáéíõøü&  
 1234567890(\$£. , ! ? )

*Figura 1.7. Tipografía OCR-B.*

El reconocimiento de caracteres por tinta magnética o MICR, es una clase especial de la tecnología OCR que fue adoptada por la industria bancaria para facilitar el procesamiento de cheques. Casi todos los cheques en México incluyen caracteres MICR en la parte inferior del papel en una fuente conocida como E-13B (figura 1.8).



*Figura 1.8 Tipografía MICR E-13B*

El problema general de la tecnología OCR es que está limitado en su utilidad al grado de seguridad en el reconocimiento. A través del uso de caracteres especialmente diseñados y tinta magnética, la tasa de error para la lectura de los números en la parte inferior de un cheque típico es menor que los sistemas usuales de OCR. Las letras son leídas con un dispositivo similar a la cabeza de un grabador de cintas magnéticas y su confiabilidad es mayor que el procesamiento a mano, siendo por lo tanto altamente útil en su dominio.

### **I.2.3. Aplicaciones**

La tecnología OCR ha sido utilizada para introducir datos a computadoras automáticamente para su diseminación y procesamiento. Los primeros sistemas estaban dedicados a entradas de datos variables de alto volumen siendo el primer uso mayor del OCR el procesamiento de recibos de venta de gasolina con tarjetas de crédito. Esta aplicación proporcionaba el reconocimiento del comprador desde el número de cuenta estampado en la tarjeta de crédito y la introducción de la transacción. Los primeros dispositivos estaban acoplados con unidades que hacían pequeñas perforaciones para ser leídos por la computadora. A medida que las computadoras y los dispositivos OCR se hicieron mas sofisticados, los escáners proporcionaron acceso directo al CPU. Estas dos son aún las mayores aplicaciones de OCR.

Con el tiempo evolucionaron otras aplicaciones. Cualquier forma o documento estándar con datos variables repetitivos sería un candidato para una aplicación OCR. Algunas aplicaciones muy imaginativas. Quizá la más innovadora era el escáner Kurzweil que leía para los ciegos ya que con éstos dispositivos las páginas eran convertidas en palabras.

### I.3 BANDA MAGNÉTICA

La banda magnética es similar a un pedazo de cinta magnética de un casete musical. Su misión es almacenar cierta información, como el nombre del titular, el número del titular, el número de su cuenta, el tipo de tarjeta y el PIN (número de identificación personal). Básicamente se puede decir que identifica al usuario con la máquina con la que se pone en contacto y esta máquina o dispositivo, conectándose en línea con otros dispositivos, gestiona una serie de operaciones y guarda cierta información de cada transacción.

La banda magnética está adherida al reverso de la tarjeta en una línea horizontal de extremo a extremo, como se muestra en la figura I.9. Esta franja tiene media pulgada de ancho y está siempre a una distancia fija del borde superior o inferior.



Figura I.9 Tarjeta típica con Banda Magnética

La información en una banda magnética, al contrario de lo que ocurre con otras formas de almacenaje de información, puede ser re-escrita y actualizada. La cantidad de información incorporada a una banda magnética es de aproximadamente 134 bytes y es estática, por lo que la relación entre el usuario de la tarjeta y el emisor es unidimensional, es decir, únicamente se actualiza cuando se interactúa a través de hardware especializado.

Pero estas cintas no son inmunes al trato al que les podemos someter diariamente. Uno de los peligros que las acecha es la desmagnetización, con la consecuente pérdida de la información. Sin embargo existen materiales que protegen a las cintas magnéticas de este peligro; se trata de los denominados materiales de alta coercitividad (Hi-Co).

La coercitividad es una propiedad física que se define como la resistencia de los materiales magnetizados que determina precisamente la resistencia del material a la pérdida de información, en este caso a la desmagnetización. Un material con alto nivel de coercitividad, necesitará un campo magnético más intenso para alterar la orientación de sus partículas. Por otro lado, una banda magnética de baja coercitividad (LO-CO) necesita un campo magnético relativamente débil para ser codificada. Lógicamente, también requiere un campo débil para desmagnetizarla o borrar la información. Por esta razón estas tarjetas son más vulnerables a posibles campos magnéticos en las proximidades.

El valor estándar de la coercitividad en una tarjeta de baja, se ha fijado en 300 Oe (Oersted). El valor para una tarjeta de alta coercitividad puede variar de 2750 a 4000 Oe, dependiendo de las características particulares de cada banda magnética. En realidad no existe un valor estándar en la industria para las bandas magnéticas de alta coercitividad. Para estas cintas Hi-Co, una vez grabadas, su decodificación es prácticamente imposible.

Por otro lado, las cintas magnéticas son también susceptibles a daños físicos y también a daños causados por el medio ambiente. La mejor forma de conservarlas es en un medio limpio, seco y frío. El polvo o la humedad, por ejemplo, pueden acumularse sobre la banda magnética y causar errores en el proceso de lectura. Las temperaturas excesivas podrían alterar la magnetización de la cinta, ya que la transferencia de energía al material magnético podría ser lo suficiente como para agitar térmicamente el material haciéndole perder su orientación magnética y con ello, su estado de magnetización. Las temperaturas típicas de almacenamiento oscilan entre -40 y 80 °C, siendo las temperaturas típicas de operación entre 0 y 55 °C.

Las tarjetas de banda magnética se pueden reproducir y grabar con demasiada facilidad. Antes, un lector codificador de tarjetas magnéticas no era fácil de conseguir y podría tener un costo muy elevado. En la actualidad es mucho más fácil conseguir un codificador a buen precio. Ante esto, las tarjetas de banda magnética intentan sobrevivir protegiéndose con marcas de agua, hologramas y todo tipo de recursos de seguridad que solamente eluden el problema y que, en opinión de los expertos, no lo resuelven.

La banda más utilizada es de un ancho de ½ pulgada, y su colocación viene especificada en la norma estándar ISO-7811-2.

La información de la banda magnética se almacena en tres tracks o pistas que se ubican en partes específicas de la banda como se puede apreciar en la figura I.10. La capacidad de grabación de la banda varía en función de los tracks.

Track 1: Acepta 76 caracteres alfanuméricos útiles.

Track 2: Acepta 37 caracteres numéricos útiles.

Track 3: Acepta 104 caracteres numéricos útiles.

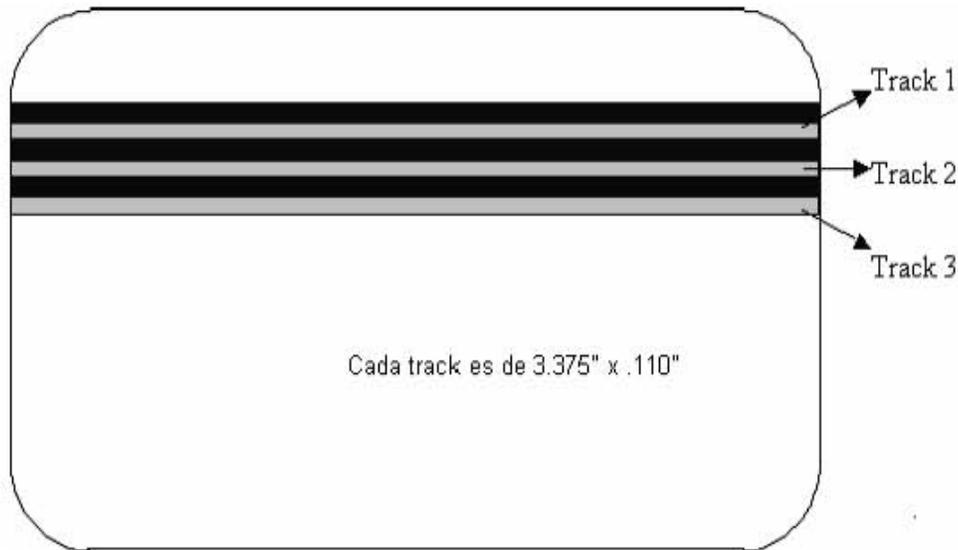


Figura I.10 Ubicación de los tracks en una banda magnética

La mayor aplicación de las bandas magnéticas es en las tarjetas bancarias y las credenciales de identificación. Actualmente su uso se encuentra extendido por todo el mundo y existen también una gran cantidad de fabricantes, tanto de la banda magnética como de equipo para colocarla y también para grabar la información en ella.

#### I.4 TARJETAS INTELIGENTES

Aunque el nombre Tarjeta Inteligente captura la imaginación, tal término es ambiguo y es utilizado en muchas formas diferentes. ISO (*Internacional Standard Organization*) utiliza el término *Integrated Circuit Card* ICC o Tarjeta con Circuito Integrado lo cual comprende todos aquellos dispositivos donde un circuito integrado está contenido en una tarjeta de plástico ISO 1. La tarjeta presenta las mismas dimensiones que las tarjetas de crédito que tienen una banda magnética y que se utiliza como medio de pago por medio de muchas instituciones financieras.

Una tarjeta inteligente contiene un microprocesador con su CPU, su RAM y su ROM, su forma de almacenamiento puede ser EPROM o EEPROM, el programa ROM consta de un sistema operativo que maneja la asignación de almacenamiento de la memoria, la protección de accesos y maneja las comunicaciones del bus interno entre los elementos. Es totalmente inaccesible desde afuera del chip de silicón mismo, por ello la única manera de comunicarse está totalmente bajo control de sistema operativo y no hay manera de poder introducir comandos falsos o requerimientos inválidos que puedan sorprender las políticas de seguridad.

Las tarjetas inteligentes dependen de tres zonas fundamentales:

- Zona Abierta: Contiene información que no es confidencial. (el nombre del portador y su dirección).
- Zona de Trabajo: Contiene información confidencial. (Aplicaciones bancarias: cupo de crédito disponible, el número de transacciones permitidas en un periodo de tiempo).
- Zonas Secretas: La información es totalmente confidencial. El contenido de estas zonas no es totalmente disponible para el portador de la tarjeta, ni tiene por que conocerlo la entidad que la emite ni quien la fabrica.

Las tarjetas se activan al introducirlas en un lector de tarjetas. Un contacto metálico, o incluso una lectura láser, como en un CD-ROM, permite la transferencia de información entre el lector y la tarjeta, actualmente comienzan a existir casas comerciales cuyos productos permiten leer una tarjeta inteligente desde la propia computadora personal.

Las comunicaciones de las tarjetas inteligentes se rigen por el estándar ISO 7816/3, la tasa de transferencia de datos es de 9600 bauds en modo asíncrono.

## **I.4.2. Tipos de Tarjetas Inteligentes**

### **I.4.2.1. Tarjeta Inteligente de Contacto**

Estas tarjetas son las que necesitan ser insertadas en una terminal con lector inteligente para que por medio de contactos pueda ser leída, Existen dos tipos de tarjeta inteligente de contacto: Las sincrónicas y las asincrónicas.

**Tarjetas Inteligentes Sincrónicas:** Son tarjetas con solo memoria y la presentación de esta tarjeta inteligente y su utilización se concentra principalmente en tarjetas prepagadas para hacer llamadas telefónicas.

Estas tarjetas contienen un chip de memoria que se utiliza generalmente para el almacenamiento de datos, dentro de esta categoría existen dos tipos de tarjeta:

**Memoria Libre:** Carece de mecanismos de protección para acceder a la información.

**Memoria Protegida:** que necesita de códigos y pasos previos para tener acceso a la información.

Estas tarjetas son desechables cargadas previamente con un monto o valor que va decreciendo a medida que se utiliza, una vez se acaba el monto se vuelve desechable, se utilizan a nivel internacional para el pago de peajes, teléfonos públicos, máquinas dispensadoras y espectáculos.

**Tarjetas Asincrónicas:** Son tarjetas inteligentes con microprocesador, esta es la verdadera tarjeta inteligente, tiene el mismo tamaño y grosor de una tarjeta de crédito y el mismo grosor, pueden tener un cinta magnética en la parte posterior. Dentro del plástico se encuentra un elemento electrónico junto con la memoria RAM, ROM y EEPROM en el mismo chip

#### **I.4.2.2 Tarjetas Inteligentes sin Contacto**

Son similares a las de contacto con respecto a lo que pueden hacer y a sus funciones pero utilizan diferentes protocolos de transmisión en capa lógica y física, no utiliza contacto sino una interfase inductiva, puede ser de media distancia sin necesidad de ser introducida en una terminal de lector inteligente.

Una de las ventajas que esta tarjeta tiene es que como no existen contactos externos con la tarjeta, esta es más resistente a los elementos externos tales como la suciedad. Este tipo de tarjetas se relaciona de manera muy estrecha con la tecnología RFID (Identificación por Radio Frecuencia).

#### **I.4.3 Aplicaciones**

Las tarjetas inteligentes han sido desarrolladas como sistemas de almacenamiento de información interactivo. Por tanto su uso abarca desde sistemas de moneda electrónica, hasta sistemas de identificación asociados al almacenamiento de información de los elementos a identificar. Debido a su capacidad de modificar el contenido sin el requerimiento de un grabador excesivamente costoso y la capacidad de realizar múltiples grabaciones sin riesgo de pérdida de la información, están desbancando a las tradicionales tarjetas de banda magnética. Además, las tarjetas inteligentes con microprocesador permiten tener un control mucho más seguro sobre la identificación, de forma que tras acuerdos internacionales entre fabricantes, existen identificadores diferentes para todas las tarjetas que circulan por el mundo.

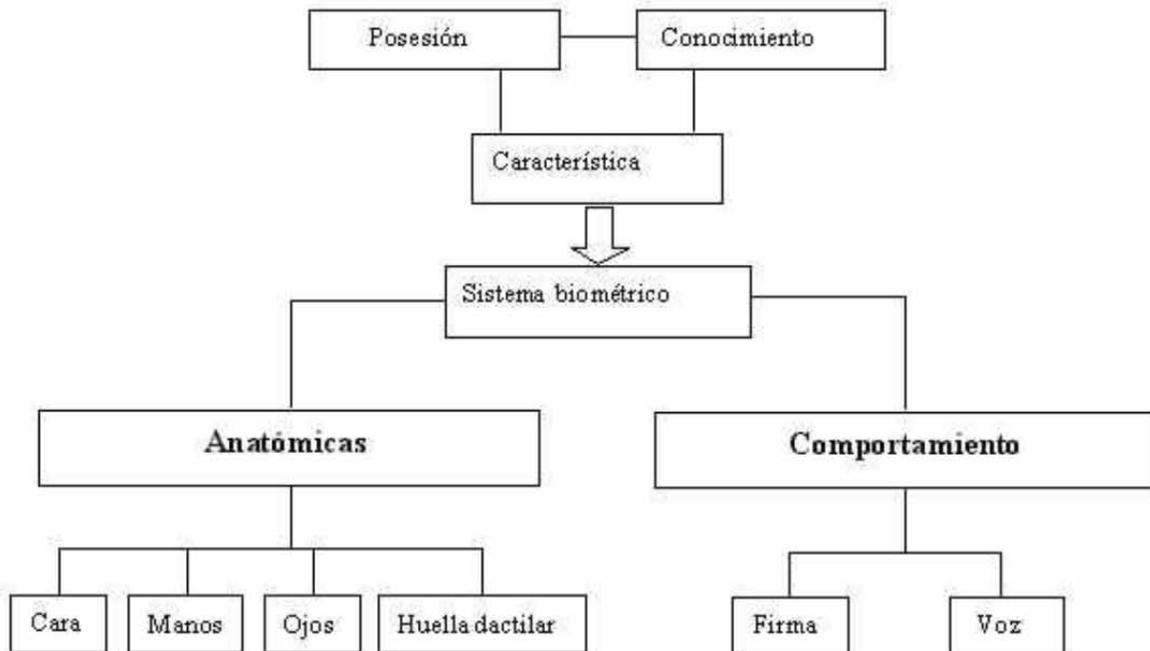
En la actualidad las tarjetas inteligentes están siendo utilizadas masivamente en la telefonía móvil, en tarjetas telefónicas de prepago y en tarjetas de crédito entre otras aplicaciones.

### **I.5 SISTEMAS BIOMÉTRICOS**

El contexto tecnológico de la palabra biometría se refiere a la aplicación automatizada de técnicas biométricas a la certificación, autenticación e identificación de personas en sistemas de seguridad. Las técnicas biométricas se utilizan para medir

características corporales o de comportamiento de las personas con el objeto de establecer una identidad. Para diferenciar estos conceptos, organizaciones y autores han dado un nombre compuesto al contexto tecnológico como biometría informática y autenticación biométrica.

La biometría es la ciencia que se dedica a la identificación de individuos a partir de una característica anatómica o un rasgo de su comportamiento. Una característica anatómica tiene la cualidad de ser relativamente estable en el tiempo, tal como una huella dactilar, la silueta de la mano, patrones de la retina o el iris. Un rasgo del comportamiento es menos estable, pues depende de la disposición psicológica de la persona, por ejemplo la firma. No cualquier característica anatómica puede ser utilizada con éxito por un sistema biométrico. Para que pueda ser así debe cumplir con las siguientes características: Universalidad, Unicidad, Permanencia y Cuantificación. La figura 1.11 muestra una división de las características biométricas para la identificación personal.



[16]

Figura 1.11 División de las características biométricas para la identificación personal.

Para realizar la autenticación biométrica primero se debe registrar a los individuos que van a hacer uso del sistema. Para el registro se utiliza un dispositivo biométrico para examinar el atributo físico o comportamiento elegido. Un software se encarga de cuantificar los datos examinados y transformarlos en datos matemáticos. El conjunto de estos datos matemáticos constituye la plantilla que identifica al individuo. La plantilla y un dato asociado al individuo (como por ejemplo un nombre o un número) son guardados electrónicamente. La lectura del atributo no se cuantifica en su totalidad de

esta manera no es posible reproducir a partir de la plantilla un miembro falso o un comportamiento artificial.

La autenticación posterior se realiza cuando el individuo presenta su rasgo corporal o muestra su comportamiento ante un dispositivo biométrico. Nuevamente se cuantifican los datos del rasgo en una nueva plantilla para compararlos contra la plantilla guardada. La búsqueda de la plantilla guardada puede realizarse de dos maneras. La primera es una búsqueda uno a muchos (1 – N). Solamente se presenta el rasgo y el sistema se encarga de buscar entre todas las plantillas guardadas, quién es el individuo. Esto es conocido como identificación. Este método requiere un mayor tiempo de búsqueda y es utilizado en bases de datos pequeñas o en aplicaciones criminalísticas.

El segundo método es una búsqueda uno a uno (1 – 1), donde el individuo presenta adicionalmente su nombre o número de identificación. El sistema se encarga de buscar la plantilla guardada que está bajo el nombre o el número de identificación solamente, y realiza la comparación. Esto es conocido como verificación y es utilizado en la mayoría de las aplicaciones biométricas.

Para que se certifique al individuo la comparación no necesariamente resulta en una igualdad entre ambas plantillas. En realidad pueden pasar años antes de que el individuo presente una plantilla igual a la guardada. Una serie de factores pueden influir en leves variaciones matemáticas, como por ejemplo el peinado en los dispositivos lectores faciales. Para realizar la certificación las plantillas deben ser similares entre sí en cierto grado. Esto no implica que los sistemas biométricos no sean seguros sino que son sistemas probabilísticos no absolutos. La exactitud de la medición varía de acuerdo a la tecnología y el fabricante en valores desde 1/1000 a 1/10E78.

### **1.5.1 Técnicas Biométricas**

A continuación se hará mención de las principales técnicas biométricas utilizadas en seguridad:

#### **Medición de huellas digitales**

Después del ADN, las huellas digitales constituyen la característica humana más singular. La probabilidad de que dos personas tengan la misma huella digital es 1/67 billones. La medición automatizada de la huella digital requiere un gran poder de procesamiento y alta capacidad de almacenamiento. Por esto, los productos biométricos basados en huella digital se basan en rasgos parciales, lo cual aumenta la posibilidad de que dos personas resulten con plantillas similares a valores entre 1/100,000 a 1/1,000,000, de los más seguros entre los dispositivos biométricos de seguridad.

Los dispositivos biométricos de huella digital son los más usados, a pesar de las aprensiones que tienen las personas en dar su huella digital. Son los productos con

mejor precio, mayor cantidad de fabricantes y mayores ventas. Son convenientes y fáciles de usar.

Algunos dispositivos utilizan lectores de silicón, los cuales se deterioran con el uso del tiempo. Otros lectores de cámara son susceptibles a la suciedad y humedad de los dedos.

Por estas razones, los biométricos de huella digital son recomendados para instalaciones de alta seguridad pero de acceso restringido (casas, cuartos de cómputo, oficinas de funcionarios de alto nivel, etc.), computadoras y redes de cómputo.

### **Geometría de mano**

Como su nombre lo indica, los biométricos basados en la geometría de la mano miden la forma de la mano por medio de una cámara infrarroja o visual. Ofrecen un buen balance entre la velocidad del análisis de las plantillas y facilidad de uso. Son ideales para uso masivo, como control de asistencia y acceso de entradas.

### **Retina**

Los lectores biométricos de retina analizan los capilares que están situados en el fondo del globo ocular. El usuario debe acercar el ojo al lector y fijar su mirada en un punto. Una luz de baja intensidad examina los patrones de los capilares en la retina. Este procedimiento es intimidante para algunos y hace de los lectores de retina los biométricos más impopulares, el usuario siente que su integridad física puede peligrar porque percibe un objeto extraño en su cuerpo, en ese caso la luz (esta característica no deseada de los lectores biométricos es conocida en inglés como *intrusive*). Para que el lector pueda realizar su trabajo, el usuario no debe tener lentes puestos.

### **Iris**

Los lectores de iris analizan las características del tejido coloreado que se encuentra alrededor de la pupila. Estos biométricos son los menos incómodos de usar de los lectores de ojo, porque no se realiza un contacto cercano con el lector. Además, es una de las tecnologías biométricas más exactas y el usuario puede usar los lentes al momento de la lectura. La facilidad de uso y la integración con otros sistemas no han sido puntos fuertes de los lectores de iris, pero se espera que mejoren con los avances técnicos.

### **Reconocimiento de cara**

Los biométricos de reconocimiento de cara analizan las características faciales. Una cámara digital captura una imagen de la cara, a partir de la cual se crea la plantilla. El uso de esta tecnología es muy extendido en Europa. Es utilizada principalmente en aplicaciones de identificación. Los casinos los utilizan para identificar estafadores.

Complejos comerciales y edificios los utilizan para identificar delincuentes y personas no gratas.

### **Lectura de firma**

La técnica de verificación de firma analiza la manera que el usuario realiza su firma personal. Factores diversos, como la rapidez y presión, son cuantificados, así como la forma de la firma. La verificación tiene uno de los niveles más bajos de exactitud entre los lectores biométricos. Sin embargo, su familiaridad con los actuales procesos de verificación manual la hace una de las técnicas más fáciles de introducir al usuario.

### **Reconocimiento de voz**

Los biométricos de reconocimiento de voz están basados en la verificación del patrón de voz. Su implementación puede ser económica si es realizada en computadoras, ya que la mayoría trae el hardware necesario: micrófonos y bocinas. Sin embargo, factores ambientales, como el ruido, pueden afectar la verificación. Además, el patrón del reconocimiento de voz es el que más espacio ocupa de todas las tecnologías biométricas. Por estas razones, los biométricos de voz son percibidos por los usuarios como dispositivos poco amigables. La tecnología está siendo mejorada y se espera que en el futuro gane popularidad.

### **I.5.2 Aplicaciones**

Los siguientes son los usos más comunes de los biométricos en los sistemas de seguridad.

#### **Acceso físico**

Por varias décadas, instalaciones de seguridad han utilizado la tecnología biométrica para los accesos de entrada. Actualmente es su uso principal: acceso a edificios y oficinas. Los biométricos permiten accesos seguros sin la presencia de un guardia de seguridad. Los biométricos de geometría de mano son los más usados en esta aplicación.

#### **Acceso virtual**

Actualmente, el método de seguridad más usado para el acceso a computadoras personales y redes es la introducción de la contraseña. Sin embargo, la contraseña brinda una seguridad mínima para la protección de la información. Los precios de los biométricos han caído a un nivel en que permite su utilización para el acceso a redes y PCs. Esto brinda una mayor seguridad a los datos, porque la seguridad no está basada en lo que la persona sabe, sino en quién es.

#### **Asistencia**

El control de asistencia es una de las aplicaciones en la cual los biométricos han tenido

una gran acogida. Los biométricos son utilizados para la verificación de la asistencia, reemplazando los relojes de tarjeta. Esta es una aplicación donde el retorno de la inversión se refleja más claramente, porque las compañías se ahorran mucho dinero evitando el robo de tiempo, que se da cuando los empleados marcan con las tarjetas de otros.

### **Aplicaciones de comercio electrónico**

Por muchos años, se ha aceptado la firma como el método para la verificación de la identidad de los dueños de tarjeta de crédito. Sin embargo, está emergiendo con fuerza la utilización de biométricos con tarjetas inteligentes en los puntos de venta para la verificación de la identidad, brindando una seguridad muy superior. El comercio por Internet es mucho más crítico aún, porque no existe posibilidad de verificación de firma, la verificación se realiza contra lo que el comprador sabe. Varias compañías de tecnología han creado divisiones para el desarrollo de productos de software que permiten la utilización de biométricos para verificar quién es el comprador.

### **Vigilancia**

Esta es una de las áreas de seguridad que presenta mayores retos para los biométricos. Utilizando reconocimiento de voz o de cuerpo, las compañías biométricas están desarrollando productos que permiten la identificación de sospechosos a edificios e instalaciones. Múltiples situaciones deben ser consideradas, como la identificación simultánea de varias personas y falta de consistencia en el ángulo, distancia y posición desde el lector.

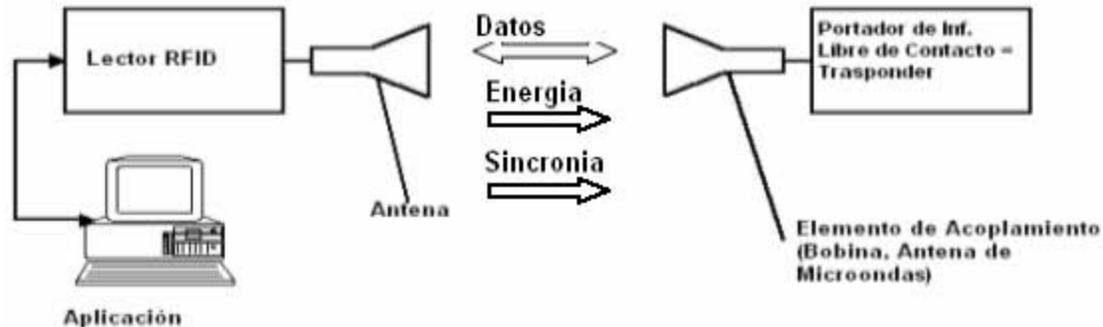
## **I.6 IDENTIFICACION POR RADIOFRECUENCIA**

En los últimos años, se ha utilizado ampliamente el código de barras para identificar tanto productos como gafetes de personal, sin embargo se ha encontrado que aunque éste método es muy económico presenta importantes limitaciones tales como el tamaño de la información almacenada y la imposibilidad de reprogramación.

Ante esto, la solución técnica óptima sería el almacenamiento de datos en un chip de silicón. La forma más común de dispositivo portador de datos en uso diario es la llamada "smart card" o tarjeta inteligente la cual está basada en un campo de contacto (Tarjetas telefónicas, tarjetas bancarias o de crédito). Sin embargo, el contacto mecánico utilizado en la tarjeta inteligente es con frecuencia impráctico. Es mucho más flexible la transferencia de datos inalámbrica o sin contacto entre el dispositivo portador de la información y el dispositivo lector. En el caso ideal, la energía requerida para operar la electrónica del dispositivo portador de información debería ser también transferida desde el dispositivo lector utilizando tecnología libre de contacto. Debido a los procedimientos utilizados en la transferencia de datos y energía, los sistemas de identificación libres de contacto son llamados sistemas RFID (Identificación por Radiofrecuencia). La figura I.12 muestra un sistema típico RFID.

Un sistema RFID está compuesto por hasta dos partes:

- El Transponder que está localizado en el objeto que será identificado y es el dispositivo que contiene la información que será leída en el sistema.
- El detector o lector que, dependiendo del diseño y la tecnología utilizada, puede ser un dispositivo lector o lector/escritor.



[1]

Figura 1.12 Esquema típico de un sistema RFID

Los transponder o etiquetas RFID existen en dos categorías principales: Activas y Pasivas. La diferencia primordial entre una etiqueta activa o pasiva es la fuente de energía, lo cual a su vez determina un número de atributos clave, incluyendo fuerza de la señal, capacidad de memoria, tamaño y costo.

Una etiqueta pasiva no contiene una fuente local de energía (por ejemplo una batería) para la transmisión de la señal, en cambio recibe la energía desde el lector mismo. Una antena proyecta energía desde el lector, lo cual proporciona suficiente potencia para la etiqueta pasiva (sin embargo, las etiquetas pasivas pueden utilizar una pequeña batería para mantener la información en la memoria). Dada ésta característica, las etiquetas pasivas operan sólo en rangos cortos. Además, algunas etiquetas a ciertas frecuencias tienen dificultad para funcionar en medio ambientes donde existe una gran cantidad de interferencia, incluyendo la presencia de metales, líquidos y otras fuentes de radiofrecuencia. Sin una batería interna, las etiquetas pasivas también están limitadas en la capacidad de memoria. Las etiquetas pasivas son mas baratas, mas pequeñas en tamaño, mas ligeras, tienen tiempos de vida más largos y están sujetas a menos regulaciones que las etiquetas pasivas.

Las etiquetas activas contienen una batería que actúa como fuente local de potencia para propósitos de transmisión. Esto permite una señal más fuerte lo cual le da a las etiquetas activas un número de ventajas sobre las etiquetas pasivas, incluyendo mayores rangos de lectura, menos susceptibilidad a interferencias y mayor capacidad

de memoria. Sin embargo, debido a la adición de la batería, son más caras y tienen menor tiempo de vida.

La tabla I.2 muestra un resumen de las principales características de las etiquetas o transponder pasivos o activos.

|                                   | <b>ETIQUETAS PASIVAS</b>         | <b>ETIQUETAS ACTIVAS</b> |
|-----------------------------------|----------------------------------|--------------------------|
| Fuente de poder de comunicaciones | Externa desde el lector          | Batería Interna          |
| Rango de lectura                  | Hasta 15 ft                      | Hasta 250 ft             |
| Rango de escritura                | 0.5x a 1.5x del rango de lectura | 1x del rango de lectura  |
| Capacidad de almacenamiento       | Relativamente menor              | Relativamente mayor      |
| Susceptibilidad a interferencia   | Mayor                            | Menor                    |
| Costo de la etiqueta              | 0.35 USD a varios dólares        | Mas de 20 dólares        |
| Vida de la etiqueta               | Hasta 20 años                    | Entre 5 y 10 años        |

*Tabla 1.2 Cuadro comparativo de etiquetas pasivas con etiquetas activas.*

Las etiquetas tienen diferentes tipos de memoria, incluyendo de solo lectura y lectura/escritura. Las etiquetas de sólo lectura, que son típicamente pasivas, son de relativamente baja capacidad (menor a 64 bits) y contienen datos que están permanentemente programados. En este aspecto son similares a un código de barras en el sentido de que la información almacenada es utilizada principalmente en su capacidad de “identificador”. Esta categoría de etiquetas ofrece un alto grado de seguridad dado que la información pre-especificada no puede ser alterada.

En contraste la etiquetas de lectura/escritura almacenan datos que pueden ser leídos y actualizados cuando es necesario. Estas etiquetas pueden tener una capacidad de memoria más grande y por lo tanto funcionar como bases de datos portátiles.

En la determinación de las características de un sistema RFID también es importante la frecuencia empleada. En general, entre más alta es la frecuencia, mas robusto es el sistema con respecto a los rangos de lectura y velocidad de captura de datos. Las frecuencias más altas tienden a ser mas caras también, aunque se espera que las aplicaciones serán cada vez mas en el rango de frecuencias altas, específicamente en la banda UHF (*Ultra High Frequency*), que se encuentra entre las frecuencias de 862MHz a 928MHz para los sistemas RFID. Con las frecuencias UHF se tiene un rango de lectura de 10 a 20 ft. En cambio, la mayoría de las aplicaciones de rastreo de productos opera en la banda de frecuencia intermedia a 13.56 MHz. Los productos a ésta frecuencia tiene un rango típico de lectura de hasta 8 ft. La tabla I.3 muestra un esquema de las bandas de frecuencia y algunas de sus aplicaciones.

| BANDA DE FRECUENCIA                           | CARACTERÍSTICAS RELATIVAS   | EJEMPLOS DE APLICACIÓN   |
|---|---|--|
| Baja<br>100-500 KHz                           | <ul style="list-style-type: none"> <li>• Rango de lectura corto</li> <li>• Velocidad de lectura baja</li> <li>• Relativamente barato</li> <li>• Puede leer a través de líquidos</li> </ul>  | <ul style="list-style-type: none"> <li>• Control de acceso</li> <li>• Identificación de animales</li> </ul>  |
| Alta<br>Típicamente 13.56 MHz                 | <ul style="list-style-type: none"> <li>• Rango de lectura de medio a corto</li> <li>• Velocidad de lectura media</li> <li>• Costo moderado</li> <li>• No puede leer a través de líquidos</li> </ul>   | <ul style="list-style-type: none"> <li>• Control de acceso</li> <li>• Rastreo de productos</li> <li>• Vigilancia electrónica de artículos</li> </ul>             |
| UHF<br>862 MHz a 928 MHz<br>2.5 GHZ a 5.8 GHz | <ul style="list-style-type: none"> <li>• Rango de lectura largo</li> <li>• Velocidad de lectura alta</li> <li>• Probabilidad de colisión reducida</li> <li>• Relativamente caro</li> <li>• Dificultad de leer a través de líquidos e interferencia con los metales</li> </ul> | <ul style="list-style-type: none"> <li>• Manejo de productos</li> <li>• Manejo de cadenas de producción</li> <li>• Cobro en cassetas a automovilistas</li> </ul> |

*Tabla 1.3 Frecuencias de los sistemas RFID y algunas de sus Aplicaciones.*

Recientemente con la creación de nuevos estándares y de EPC (Electronic Product Code), así como con la exigencia de grandes cadenas de supermercados y del Departamento de Defensa de los Estados Unidos a sus proveedores de que sea colocada una etiqueta RFID a todos sus productos, se le ha dado un gran impulso a la aplicación de ésta tecnología.

En el presente año se espera que la venta de etiquetas RFID supere la de la última década como consecuencia de nuevas exigencias de mercadeo. En el caso de las grandes cadenas de supermercados como Walmart, la intención primaria es utilizar la tecnología para el manejo y control de mercancías, sin embargo es de esperar que las aplicaciones sigan creciendo a medida que se vayan resolviendo las dificultades técnicas.

# **Fundamentos de la Tecnología RFID**

II.1. Diferencias Fundamentales en los Sistemas RFID

II.2. Tipos de Sistemas de RFID

II.3. Normalización.

## **Capítulo 2**

## FUNDAMENTOS DE LA TECNOLOGIA RFID

### II.1 DIFERENCIAS FUNDAMENTALES EN LOS SISTEMAS RFID

Los sistemas RFID existen en incontables variaciones, producidas por un casi igual número de fabricantes. En la figura II.1 se muestra un esquema de clasificación para diferenciar un sistema RFID de otro.

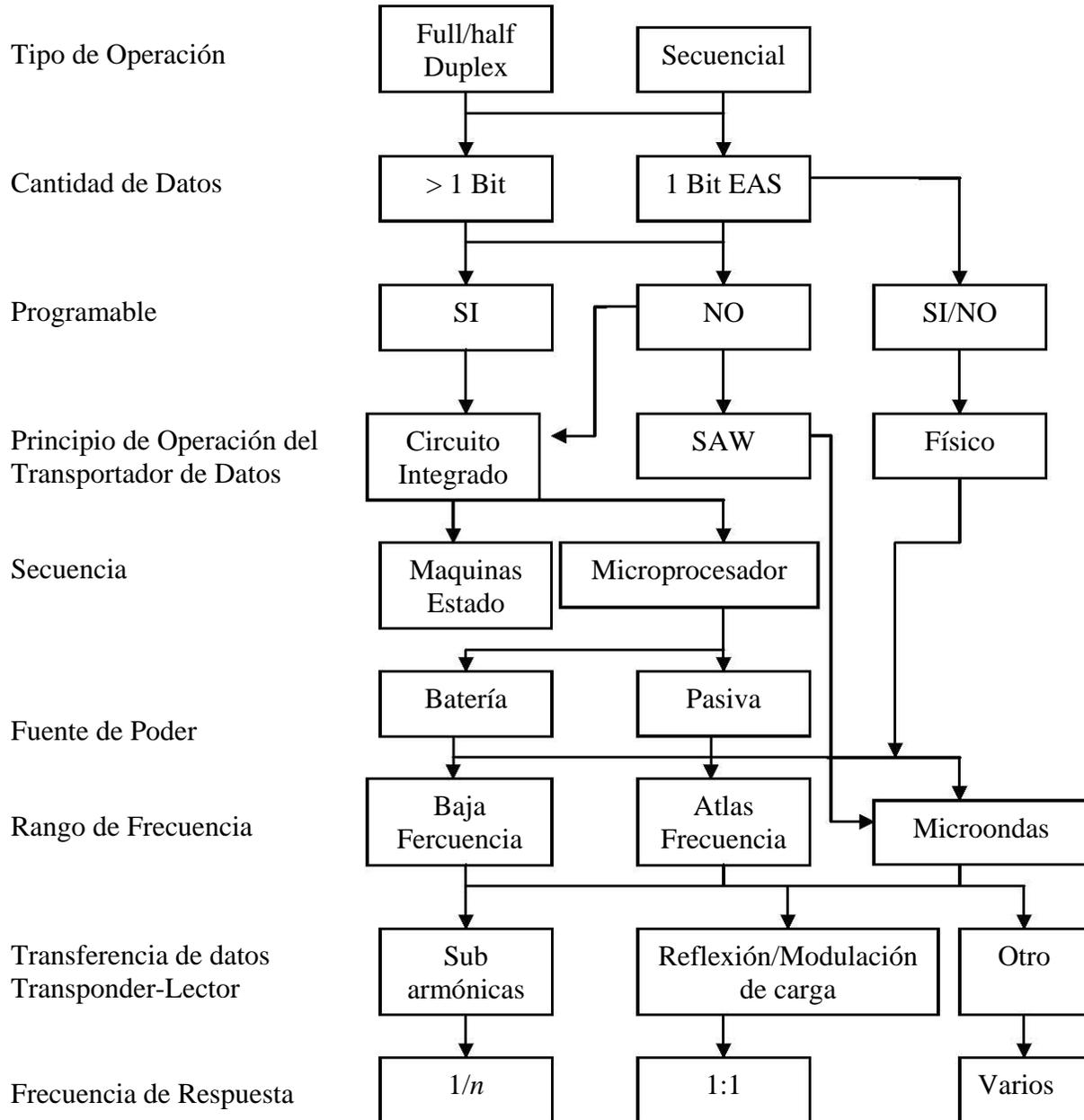


Figura II.1 Sistemas RFID y sus características (Integrated Silicon Design, 1996)

Los sistemas RFID pueden operar de acuerdo a uno de dos procedimientos básicos: sistemas *full duplex* (FDX) / *half duplex* (HDX) y sistemas secuenciales (SEQ).

En los sistemas *full* y *half duplex* la respuesta del transponder es emitida cuando es encendido el campo de radiofrecuencia (RF) del lector. Debido a que la señal del transponder a la antena del receptor puede ser extremadamente débil en comparación con la señal del lector mismo, deben ser empleados procedimientos de transmisión apropiados para diferenciar ambas señales. En la práctica, la transferencia de datos del transponder al lector tiene lugar utilizando modulación de carga, modulación de carga utilizando subportadora, pero también (sub)armónicas de la frecuencia de transmisión del lector.

En contraste, los procedimientos secuenciales emplean un sistema en el cual el campo del lector es apagado brevemente a intervalos regulares. Estos intervalos son reconocidos por el transponder y los utiliza para enviar los datos. La desventaja de este procedimiento secuencial es la pérdida de potencia en el transponder durante la interrupción de la transmisión, lo cual debe ser compensado con la provisión suficiente de capacitores auxiliares o baterías.

La capacidad de datos de los transponders RFID normalmente varía de unos cuantos bytes a varios kilobytes. Los así llamados transponders de 1-bit representan la excepción a esta regla. Una cantidad de datos de exactamente 1 bit es justamente para señalar dos estados al lector: “transponder en el campo” o “no transponder en el campo”. Sin embargo esto es perfectamente adecuado para cubrir funciones simples de monitoreo o señalización. Debido a que los transponders de 1-bit no necesitan un circuito electrónico, pueden ser fabricados a costos muy bajos. Por esta razón una gran cantidad de transponders de 1-bit son utilizado en la vigilancia electrónica de artículos (*Electronic Article Surveillance – EAS*) para proteger bienes en tiendas y negocios.

La posibilidad de escribir datos al transponder nos proporciona otra forma de clasificar los sistemas RFID. En sistemas muy simples la grabación de datos en el transponder, usualmente un número de serie, se incorpora cuando se fabrica el circuito integrado y no puede ser alterado después. Por otro lado, en los transponder programables el lector puede escribir datos en ellos. Existen tres procedimientos principales para almacenar los datos: Las EEPROMs (*electrically erasable programmable read only memory*) son dominantes en sistemas RFID acoplados inductivamente. Sin embargo tienen la desventaja de su alto consumo de energía durante la operación de grabación y un número limitado de ciclos de escritura (típicamente del orden de 100,000 a 1,000,000). Las FRAM (*ferromagnetic random access memory*) han sido utilizadas recientemente en casos aislados. El consumo de energía en la lectura de una FRAM es mas bajo que las EEPROMs por un factor de 100 y el tiempo de escritura es 1000 veces menor. Los problemas de fabricación han limitado su introducción en el mercado de una manera amplia hasta la fecha.

Las SRAM (*static random access memory*) son particularmente comunes en sistemas RFID en la frecuencia de microondas debido a su característica de tener ciclos de

escritura rápidos. Sin embargo, la retención de datos requiere de una fuente de poder ininterrumpible de una batería auxiliar.

En sistemas programables los acceso a la memoria para lectura y escritura deben ser controlados por la lógica interna del portador de datos. En el caso más simple, estas funciones pueden ser realizadas por una *máquina de estado*. Una máquina de estado es un arreglo utilizado para ejecutar operaciones lógicas y que también tiene la capacidad de almacenar estados variables. Se pueden realizar secuencias muy complejas con estos dispositivos pero su desventaja es su inflexibilidad respecto a cambios en las funciones programadas, ya que tales cambios necesitarían modificaciones a los circuitos. En la práctica, esto significa el rediseño del circuito con todos los costos asociados.

El uso del microprocesador mejora esta situación considerablemente. Al procesador se le incorpora un sistema operativo durante su fabricación, para el manejo de datos de la aplicación, utilizando una máscara. Por esto los cambios son más baratos de implantar y, en suma, el software puede ser adaptado específicamente para ejecutar diferentes aplicaciones.

En el contexto de tarjetas inteligentes libres de contacto, los portadores de datos programables con un maquina de estado son llamadas “tarjetas de memoria”, para distinguirlos de las “tarjetas de procesador”.

Otra característica importante de los sistemas RFID es la fuente de poder en el transponder. Los transponder pasivos no tienen su propia fuente de poder y por lo tanto toda la potencia requerida para su operación debe ser obtenida del campo electromagnético del lector. Por el contrario, los transponder activos incorporan una batería que proporciona todo o parte de la energía para la operación del circuito integrado.

Una de las características más importantes de los sistemas RFID es la frecuencia de operación y el rango resultante de lectura/escritura. La frecuencia de un sistema RFID es la frecuencia a la cual transmite el lector. En la mayoría de los casos la frecuencia del transponder es la misma (modulación de carga, reflexión). Sin embargo, la potencia de transmisión del transponder puede estar varias decenas de potencia mas bajo que el lector.

Las diferentes frecuencias de transmisión son clasificadas en tres rangos básicos, LF (baja frecuencia, 30 – 300 KHz), HF (alta frecuencia)/RF (radio frecuencia de 3 a 30 MHz) y UHF (Ultra alta frecuencia 300MHz a 3GHz)/microondas (> 3GHz). Otra división de los sistemas RFID de acuerdo al rango nos permite diferenciar entre acoplamiento cercano (0 – 1 cm), acoplamiento remoto (.01 a 1 m) y alcance largo (> 1m).

Los diferentes procedimientos para enviar datos del transponder al lector pueden ser clasificados en tres grupos:

- El uso de la reflexión (la frecuencia de la onda reflejada corresponde con la frecuencia de transmisión del lector).
- Modulación de carga (el campo del lector es influenciado por el transponder)
- El uso de subarmónicas y la generación de armónicas en el transponder.

## II.2 TIPOS DE SISTEMAS RFID

Existen varios tipos de sistemas RFID (figura II.2), determinados por la interacción básica del transponder y el lector, en particular la transferencia de energía y de datos entre ambos dispositivos.

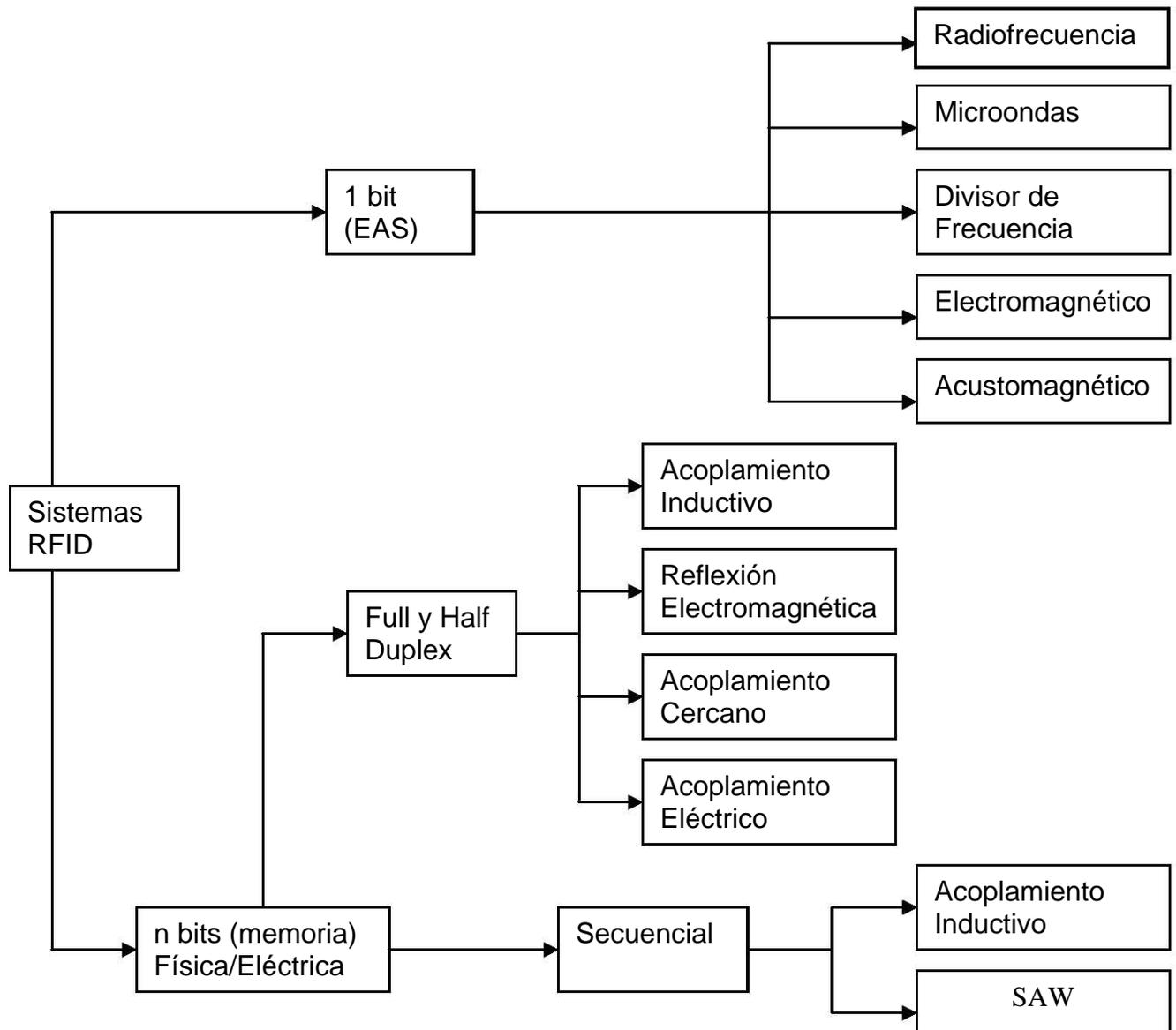


Figura II.2 Principios de Operación de los sistemas RFID (RFID Handbook, 2003)

## II.2.1 Sistemas de 1-bit

Un bit es la unidad de información más pequeña y tiene solamente dos estados: 1 y 0. Esto significa que solamente pueden ser representados dos estados en el sistema de transponder de 1-bit: “transponder en la zona de interrogación” y “no transponder en la zona de interrogación”. A pesar de ésta limitación, se han extendido su utilización principalmente en los sistemas antirrobo en tiendas (EAS).

Un sistema EAS está compuesto de hasta los siguientes elementos: la antena del lector, el elemento de seguridad o etiqueta y un equipo opcional de desactivación para desactivar la etiqueta después de pagar el artículo. Existen diferentes tipos de acoplamiento entre el transponder o etiqueta y el lector: Radiofrecuencia, microondas, Divisor de Frecuencia, Electromagnético y Acustomagnético.

### II.2.1.1 Radiofrecuencia

El procedimiento de acoplamiento por radiofrecuencia (RF) esta basado en circuitos resonantes LC ajustados a una determinada frecuencia. El lector (detector) genera un campo magnético variable en el rango de radiofrecuencia, como se puede apreciar en la figura II.3. Si el circuito resonante LC es movido a la vecindad del campo magnético variable, se puede inducir energía en el circuito resonante a través de sus bobinas. Si la frecuencia  $f_G$  del campo variable corresponde con la frecuencia de resonancia  $f_R$  del circuito resonante LC, este produce una oscilación similar. La corriente que fluye en el circuito resonante como resultado de esto actúa en contra de su causa, esto es actúa en contra del campo magnético variable. Este efecto se nota como un pequeño cambio en la caída de voltaje a lo largo de la bobina del generador del transmisor y en última instancia lleva a un debilitamiento en la fuerza del campo magnético. También puede ser detectado un cambio en el voltaje inducido en una bobina sensora opcional tan pronto como un circuito resonante sea llevado dentro del campo magnético de la bobina generadora.

La magnitud relativa de este “bajón” depende de la separación entre las dos bobinas (bobina del generador – elemento de seguridad, elemento de seguridad – bobina sensora) y la calidad Q del circuito resonante (en el elemento de seguridad).

La magnitud relativa de los cambios en el voltaje en las bobinas del generador y en el sensor son generalmente muy bajas y por lo tanto muy difíciles de detectar. Sin embargo, la señal debe ser lo mas clara posible de manera tal que pueda ser detectado el elemento de seguridad de manera confiable. Esto se logra mediante un pequeño truco: la frecuencia del campo magnético generado no es constante sino que es un barrido. Esto significa que la frecuencia del generador continuamente cruza el rango entre el mínimo y el máximo. El rango de frecuencias disponibles para los sistemas de barrido es de  $8.2 \text{ MHz} \pm 10\%$ .

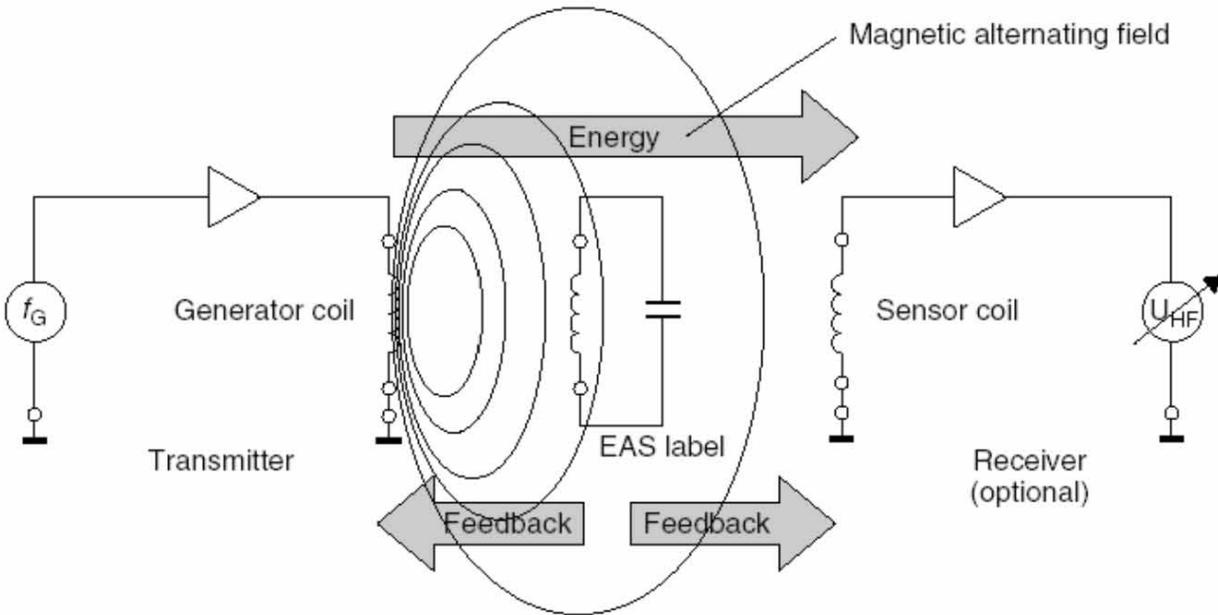


Figura II.3 Principio de operación del sistema EAS con el procedimiento de Radiofrecuencia [1]

Sin embargo, la frecuencia de barrido del generador corresponde exactamente con la frecuencia resonante del circuito LC (en el transponder), el transponder empieza a oscilar produciendo un escalón muy claro en los voltajes de las bobinas del generador y el sensor.

Debido a que las etiquetas no son removidas de los productos, estos deben ser desactivados de alguna forma. Para hacerlo, éstas son sometidas a campos magnéticos muy fuertes que usualmente destruyen los capacitores diseñados especialmente para corto-circuitarse ante ésta condición.

En este sistema usualmente se requieren antenas de gran tamaño llamadas *frame antennas*, para generar el campo magnético en el área de detección.

### II.2.1.2. Microondas

Los sistemas EAS en el rango de microondas aprovechan la generación de armónicos en los componentes con características no lineales (por ejemplo los diodos). El armónico de un voltaje senoidal  $A$  con una frecuencia definida  $f_A$  es un voltaje senoidal

$B$ , cuya frecuencia  $f_B$  es un múltiplo entero de la frecuencia  $f_A$ . Los subarmónicos de la frecuencia  $f_A$  son por lo tanto frecuencias  $2 f_A$ ,  $3 f_A$ ,  $4 f_A$ , etc. El múltiplo  $N$  de la frecuencia de salida es denominada  $n$ -armónica (onda  $n$ -armónica); la frecuencia misma de salida es denominada onda portadora o primer armónica.

En principio, cada red de dos terminales con características no lineales genera armónicos en la primera armónica. Sin embargo, en el caso de resistencias no lineales la energía se consume de manera tal que solo una pequeña parte de la potencia de la primer armónica es convertida en oscilación armónica. Bajo condiciones favorables, la multiplicación de  $f$  a  $f \times n$  ocurre con una eficiencia de  $\eta = 1 / n^2$ . En el caso ideal no habrá pérdidas si se utiliza el almacenamiento de energía no lineal para multiplicación.

Los diodos capacitivos son particularmente adecuados para almacenar energía para la multiplicación de frecuencia. El número e intensidad de los armónicos que son generados dependen del perfil de dopaje y de la línea de gradiente característico.

El esquema del transponder de 1-bit para la generación de armónicos es extremadamente simple: un diodo capacitivo se conecta a un dipolo ajustado ala onda portadora (figura II.4). Dada una frecuencia de 2.45 GHz el dipolo tiene una longitud total de 6 cm. Las frecuencias de la onda portadora utilizadas son de 915 MHz, 2.45 GHz o 5.6 GHz. Si el transponder está colocado dentro del rango del transmisor, entonces el flujo de corriente dentro del diodo genera y emite armónicos de la onda portadora. Se obtienen señales particularmente distintivas a dos o tres veces la onda portadora, dependiendo del tipo de diodo utilizado.

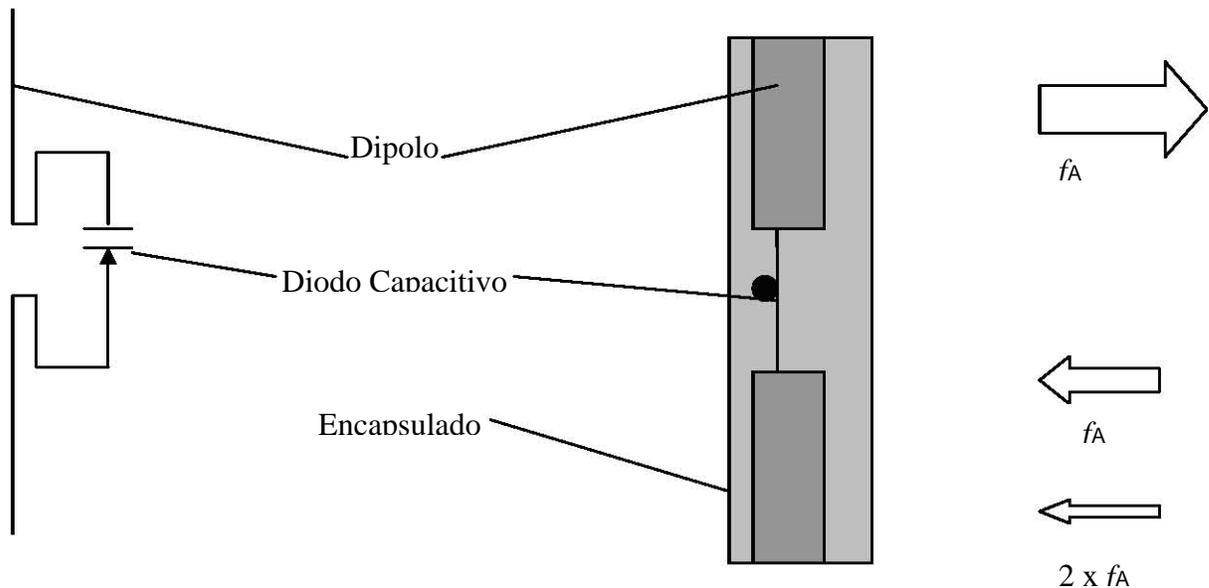


Figura II.4 Circuito básico y formato de construcción típico de una etiqueta de microondas

Si la amplitud o frecuencia de la onda portadora está modulada (ASK, FSK) entonces todas las armónicas incorporan la misma modulación. Esto puede ser utilizado para distinguir la interferencia de las señales del sistema, previniendo falsas alarmas debido a señales externas.

### II.2.1.3 Divisor de frecuencia

Este procedimiento opera en el rango de onda larga de 100 a 135.5 KHz. Las etiquetas de seguridad contienen un circuito semiconductor (microchip) y una bobina de circuito resonante. Este está diseñado para resonar a la frecuencia de operación del sistema EAS utilizando un capacitor.

El microchip en el transponder recibe su fuente de potencia desde el campo magnético del dispositivo de seguridad. La frecuencia a la bobina autoinductiva es dividida en dos en el microchip y enviada de regreso al dispositivo de seguridad. La señal a la mitad de la frecuencia original es alimentada a la bobina del circuito resonante (figura II.5)

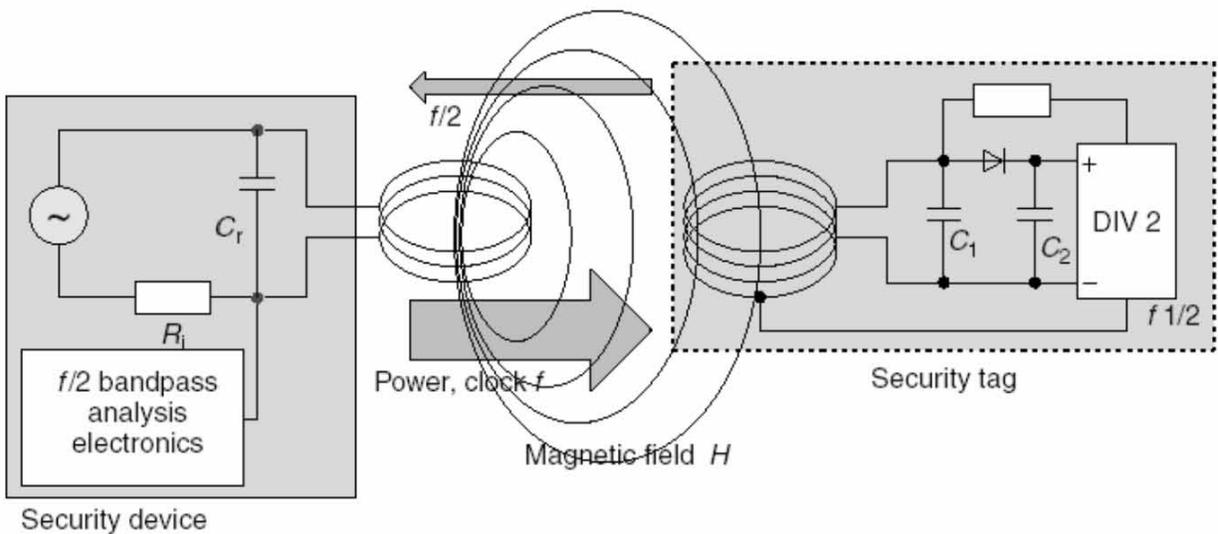


Figura II.5 Diagrama de circuito básico para el procedimiento de división de frecuencia en un sistema EAS. [1].

### II.2.1.4 Electromagnético

Los sistemas EAS de tipo electromagnético operan utilizando fuertes campos magnéticos en el rango de 10 KHz a 20 KHz. Los elementos de seguridad contienen una tira blanda de metal magnético amorfo con un pronunciado flanco en la curva de histéresis. La magnetización de estas tiras es revertida periódicamente y llevadas a la saturación magnética por un fuerte campo magnético alterno. La marcada relación no lineal entre la intensidad de campo aplicado H y la cercana saturación de la densidad

de flujo magnético  $B$ , genera armónicos a la frecuencia básica del dispositivo de seguridad.

Este tipo de sistemas son optimizados por la superposición de secciones de señal adicionales con mayores frecuencias de la señal principal. La no linealidad tan marcada de la curva de histéresis de la tiras generan no solamente armónicas sino también secciones de señal con adición y diferenciación de frecuencias de las señales proporcionadas. Por ejemplo, dada una señal principal de la frecuencia  $f_s = 20$  Hz y las señales adicionales  $f_1 = 3.5$  y  $f_2 = 5.3$  KHz, se generan las siguientes señales:

$$f_1 + f_2 = 8.80 \text{ KHz}$$

$$f_1 - f_2 = 1.80 \text{ KHz}$$

$$f_s + f_1 = 3.52 \text{ KHz}$$

En este caso el dispositivo de seguridad no reacciona a la armónica de la frecuencia básica, sino a la frecuencia de la adición o diferenciación de las señales extra.

Las etiquetas están disponibles en la formas de tiras auto adheribles con longitudes que van desde unos cuantos centímetros hasta 20 cm. Debido a la extremadamente baja frecuencia de operación, los sistemas electromagnéticos son los únicos adecuados para productos que contienen metal. Sin embargo, estos sistemas tienen la desventaja de que el funcionamiento de las etiquetas depende de la posición: para una detección confiable las líneas del campo magnético del dispositivo de seguridad deben correr verticalmente a través de las tiras de metal amorfo.

### II.2.1.5 Acustomagnético

Los sistemas acustomagnéticos para elementos de seguridad consisten en cajas de plástico extremadamente pequeñas de alrededor de 40 mm de largo, de 8 a 14 mm de ancho y de solo un milímetro de alto. Estas cajas contienen dos tiras de metal, una tira de metal magnético duro permanentemente conectada a la caja de plástico, más una tira hecha de metal amorfo, posicionado de tal manera que es libre de vibrar mecánicamente.

Los metales ferromagnéticos cambian ligeramente en longitud en un campo magnético bajo la influencia de la fuerza del campo  $H$ . Este efecto es llamado *magnetostricción* y resulta de un pequeño cambio en la distancia Interatómica como resultado de la magnetización. En un campo magnético alterno, las tiras de metal vibran en la dirección longitudinal de a la dirección de la frecuencia del campo. La amplitud de la vibración es especialmente alta si la frecuencia del campo magnético alterno corresponde con la de la frecuencia de resonancia (acústica) de la tira de metal. Este efecto es particularmente marcado en materiales amorfos.

El factor decisivo es el hecho de que el efecto magnetostrictivo es también reversible. Esto significa que una tira de metal oscilando emite un campo magnético alterno. Los sistemas de seguridad acustomagnéticos están diseñados de manera tal que la frecuencia del campo magnético generado coincide precisamente con las frecuencias de resonancia de las tiras de metal en el elemento de seguridad. Si el campo magnético alterno es apagado después de un tiempo, la tira excitada magnéticamente continúa oscilando por un momento y por lo tanto genera su propio campo magnético alterno que puede ser fácilmente detectado por el sistema de seguridad (Figura II.6).

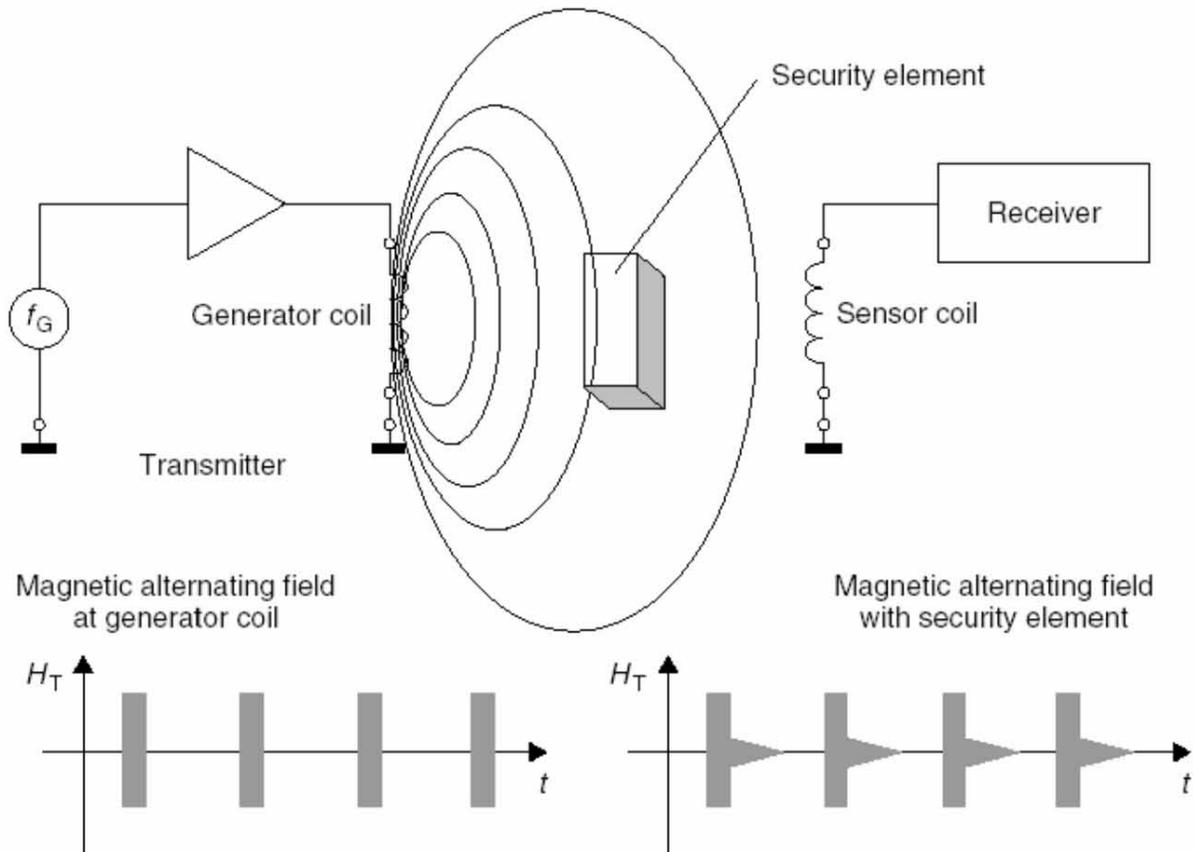


Figura II.6 Sistema Acustomagnético que comprende dispositivo de transmisión y detección. [1]

La gran ventaja de este procedimiento es que el sistema de seguridad no está transmitiendo mientras el elemento de seguridad está respondiendo y por esto el dispositivo receptor puede ser diseñado con un cierto grado de sensibilidad.

Las tiras de metal magnético duro solo pueden ser desmagnetizadas con un campo magnético alterno fuerte que tenga un declive lento en su fuerza de campo, por lo que es absolutamente imposible que los elementos de seguridad puedan ser manipulados por imanes muy fuertes.

### II.2.2 SISTEMAS DE n-BITS

Los sistemas de n bits toman su nombre de la capacidad de memoria del transponder, que en éste caso es mayor a 1 bit. Esto permite un tratamiento diferente del acoplamiento del transponder y el lector, ya que no solamente se va a detectar la presencia o ausencia del dispositivo, sino que se va a obtener información grabada en la etiqueta.

Como se mencionó anteriormente, existen dos formas genéricas diferentes para el flujo de información entre el lector y el transponder o etiqueta: procedimiento full y half duplex y procedimiento secuencial. Como se puede apreciar en la figura II.7, la diferencia básica entre ambas consiste en que la transferencia de energía del lector al transponder es constante en el procedimiento full y half duplex, no así en el procedimiento secuencial en el que existe un intervalo en el que sólo se recibe información del transponder al lector.

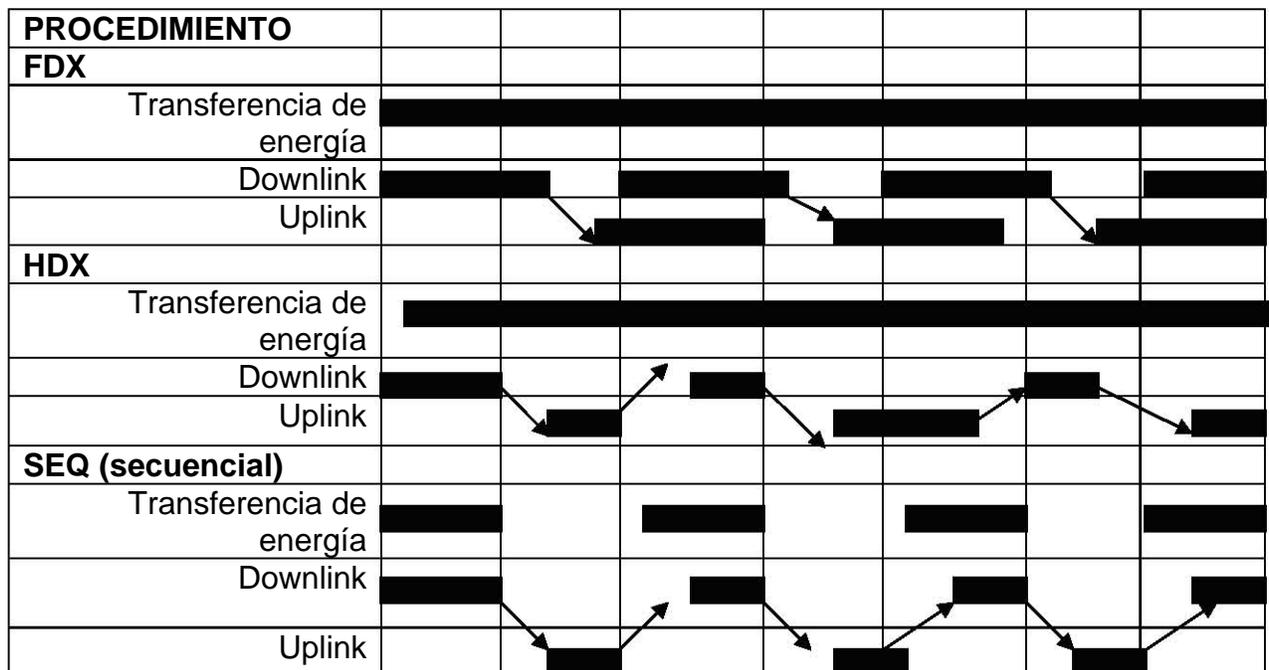


Figura II.7 Representación de los procedimientos full duplex, half duplex y secuencial en el tiempo.

### II.2.2.1 PROCEDIMIENTO FULL Y HALF DUPLEX

En el procedimiento half duplex (HDX) la transferencia del transponder al lector se alterna con la transferencia de datos del lector al transponder. A frecuencia por abajo de los 30 MHz esto se hace con mayor frecuencia con el procedimiento de modulación de carga, con o sin subportadora, lo que involucra circuitos simples. Muy cercano a esto es el procedimiento de modulación de sección cruzada reflejada y que se utiliza arriba de los 100 MHz. Estos procedimientos ejercen una influencia en los campos magnético o electromagnético del lector y por eso son llamados procedimientos armónicos.

En el procedimiento full duplex (FDX) la transferencia de datos del transponder al lector tiene lugar al mismo tiempo que la transferencia de datos del lector al transponder. Esto incluye procedimientos en el cual los datos son transmitidos del transponder a una fracción de la frecuencia del lector.

Sin embargo, ambos procedimientos tienen en común el hecho de que la transferencia de energía del lector al transponder es continua por lo que es independiente de la dirección de flujo de datos.

Existen varias formas diferentes de acoplamiento entre el lector y el transponder para los procedimientos full y half duplex:

#### **Acoplamiento Inductivo**

Un transponder acoplado inductivamente incluye un circuito integrado que es el que contiene los datos y una bobina de área grande que funciona como antena.

Los transponders de acoplamiento inductivo son casi siempre operados pasivamente, esto significa que el total de la energía requerida para la operación del microchip ha sido proporcionada por el lector. Para éste propósito, la antena del lector genera un fuerte campo electromagnético de alta frecuencia, el cual penetra el área de la bobina del transponder. Debido a que la longitud de onda en el rango de frecuencias utilizadas ( 135KHz: 2400 m, 13.56 MHz: 22.1 m) es varias veces mayor a la distancia entre la antena del lector y el transponder, el campo electromagnético puede ser tratado como un campo magnético simple y variable respecto a la distancia entre el transponder y la antena.

Como se puede apreciar en la figura II.8, una pequeña parte del campo emitido penetra la bobina de la antena en el transponder el cual está a cierta distancia de la bobina del Lector. Un voltaje  $U_i$  es generado en la antena del transponder por inductancia el cual es rectificado y sirve como fuente de poder para el dispositivo portador de información (microchip). Un capacitor  $C_r$  se conecta en paralelo con la bobina de la antena del Lector. Esta capacitancia se selecciona de manera tal que trabaja con la inductancia de la bobina de la antena para formar un circuito paralelo resonante que corresponde con

la frecuencia de transmisión del Lector. Debido a ésta resonancia, son generadas corrientes muy altas en la bobina de la antena, lo que es utilizado para generar la fuerza requerida del campo electromagnético para la operación del transponder remoto.

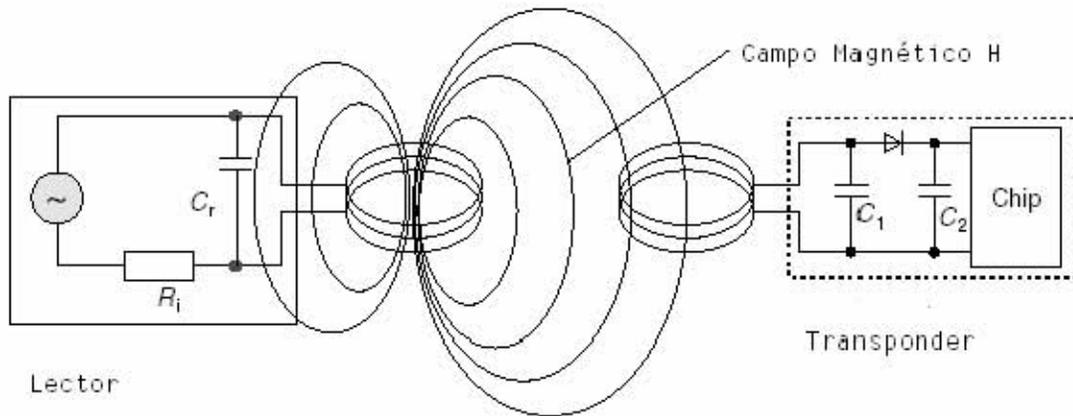


Figura II.8. Fuente de energía a un transponder acoplado inductivamente desde el campo magnético variable generado por el Lector. [1]

La bobina de la antena en el transponder y el capacitor  $C_1$  forman un circuito resonante sintonizado a la frecuencia de transmisión del Lector. El voltaje  $U$  en la bobina del transponder alcanza un máximo debido al escalamiento de resonancia en el circuito paralelo resonante.

El esquema de las dos bobinas puede ser interpretado también como un transformador en cuyo caso existe solo un acoplamiento débil entre los dos devanados.

Los sistemas acoplados inductivamente están basados en el acoplamiento tipo transformador, entre la bobina del primario en el Lector y la bobina del secundario en el transponder. Esto es cierto si la distancia entre las bobinas no excede  $0.16\lambda$ , de manera que el transponder esté localizado en el *campo cercano* de la antena transmisora.

Si un transponder resonante (un transponder con una frecuencia de autoresonancia correspondiente a la frecuencia de transmisión del lector) es colocado dentro del campo magnético variable de la antena del lector el transponder obtiene energía del campo magnético. La retroalimentación resultante del transponder en la antena del Lector puede ser representada como una *impedancia transformada*  $Z_T$  en la bobina de la antena del Lector. Conectando y desconectando una resistencia de carga en la antena del transponder provocará un cambio en la impedancia  $Z_T$  y por lo tanto cambio de voltajes en la antena del Lector. Esto tiene el efecto de una modulación en amplitud

del voltaje  $UL$  en la bobina de la antena del lector debido al transponder remoto. Si el resistor es conectado y desconectado de acuerdo a los datos almacenados en el transponder, entonces éstos datos pueden ser transferidos al Lector. Este tipo de transferencia de datos es llamada *Modulación de Carga*.

Para obtener los datos en el Lector, se rectifica el voltaje obtenido en la antena del Lector, lo que representa la demodulación de una señal de amplitud modulada.

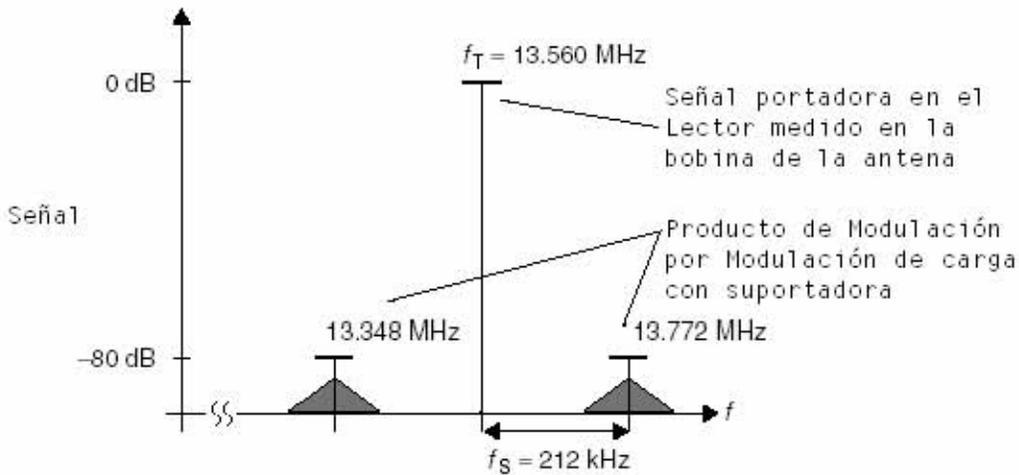
Debido al débil acoplamiento entre la antena del Lector y la antena del transponder, las fluctuaciones de voltaje en la antena del Lector que representan la señal útil son más pequeñas por fracciones de magnitud que la salida de voltaje del Lector.

En la práctica, para un sistema de 13.56 MHz, dado un voltaje de aproximadamente 100 V (Escalamiento de voltaje por resonancia) se puede esperar una señal útil de alrededor de 10mV (= 80dB señal/ruido). Debido a que la detección de este pequeño voltaje requiere de sistemas de circuitos altamente complicados, se utilizan las bandas de modulación laterales creadas por la modulación en amplitud del voltaje de la antena.

Si un resistor adicional en el transponder es conectado y desconectado a una frecuencia elemental muy alta  $f_s$ , entonces se crean dos líneas espectrales a una distancia  $\pm f_s$  alrededor de la frecuencia de transmisión del Lector *freader*, la cual puede ser fácilmente detectada (Sin embargo  $f_s$  debe ser menor que *freader*). En la terminología de la tecnología de radio la nueva frecuencia elemental es llamada *subportadora*. La transferencia de datos es por modulación ASK, FSK o PSK de la subportadora en sincronía con el flujo de datos. Esto representa una modulación en amplitud de la subportadora.

La modulación de la carga con una subportadora crea dos lóbulos de modulación en la antena del Lector a una distancia de la frecuencia de la subportadora alrededor de la frecuencia *freader* (Figura II.9) estos lóbulos de modulación laterales pueden ser separados de la señal significativamente más fuerte, utilizando un filtro pasa banda

En una de las dos frecuencias *freader*  $\pm f_s$ . Una vez que ha sido amplificada, la señal ahora es muy fácil de demodular.



[1]

Figura II.9. Lóbulos producidos por la modulación de carga con subportadora.

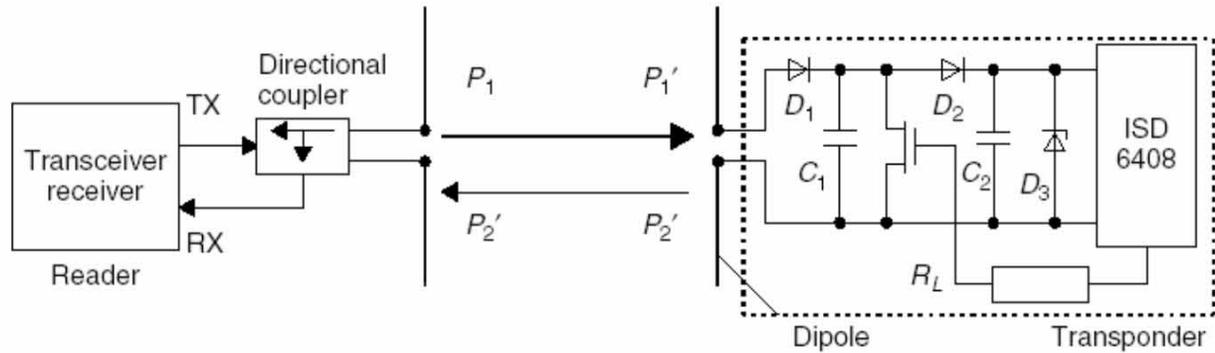
### Acoplamiento por reflexión electromagnética

Los sistemas RFID en los cuales el espacio entre el lector y el transponder es mayor a 1 m son llamados sistemas de alcance largo. Estos sistemas son operados en las frecuencias UHF de 868 MHz (Europa) y 915 MHz (Estados Unidos), y en las frecuencias de microondas de 2.5 GHz y 5.8 GHz. Las cortas longitudes de onda de estos rangos de frecuencias facilitan la construcción de antenas con dimensiones mucho menores y de mayor eficiencia de lo que sería posible utilizando rangos de frecuencia debajo de 30 MHz.

A partir de la tecnología del Radar que las ondas electromagnéticas son reflejadas por objetos cuyas dimensiones son mayores que aproximadamente la mitad de la longitud de onda. La eficiencia con la cual el objeto refleja las ondas electromagnéticas es llamada reflexión de sección transversal.

En la figura II.10 se puede apreciar el principio de funcionamiento de este acoplamiento. En estos sistemas juega un papel muy importante las pérdidas por la atenuación del espacio libre, sin embargo se utiliza tecnología en el transponder que requiere que en ocasiones sólo  $5\mu\text{W}$  en las terminales de la antena para operar los circuitos integrados. En algunas ocasiones se utiliza un sistema de baterías únicamente para hacer funcionar los circuitos del transponder pero no para la transmisión de datos.

Con ésta energía y partiendo de que parte de la potencia recibida se refleja al lector, se utiliza una resistencia  $R_L$  para lograr lo que se conoce como modulación de reflexión de sección transversal. Este proceso consiste en que la energía reflejada se puede alterar en sincronía con el flujo de datos del transponder, a través de conectar la resistencia  $R_L$  y cambiando por lo tanto la impedancia, obteniendo así una modulación de la señal reflejada.



[1]

Figura II.10 Principio de operación de un transponder de reflexión.

Una pequeña proporción de la señal reflejada es captada por la antena del lector, el cual a través de un acoplador direccional separa la señal transmitida de la reflejada.

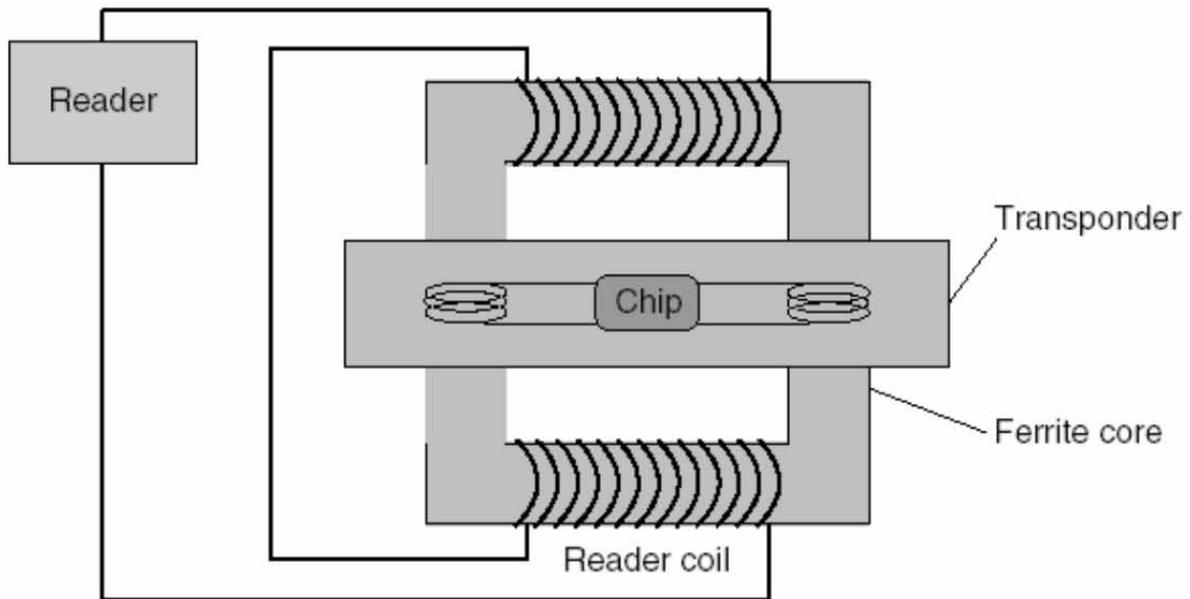
### Acoplamiento cercano

Los sistemas de acoplamiento cercano están diseñados para rangos entre 0.1 cm y 1 cm. Por lo tanto el transponder es insertado en el lector o colocado en el área marcada para la operación.

Al insertar el transponder al lector, o colocarlo sobre él, permite que la bobina del transponder sea posicionada precisamente en el espacio de aire de un núcleo en forma de anillo o de U. En la figura II.11 se muestra el esquema funcional de la bobina del transponder y la bobina del lector, lo cual corresponde a un transformador. El lector representa el devanado primario, en el cual debido a una corriente alterna de alta frecuencia se genera un campo magnético de alta frecuencia en el núcleo y en el espacio de aire del arreglo, mismo que fluye a través de la bobina del transponder. Esta potencia es rectificadora para proporcionar de energía al circuito integrado.

Debido a que el voltaje inducido en el transponder es proporcional a la frecuencia de la corriente de excitación, la frecuencia seleccionada para transferir energía debe ser tan alta como sea posible. En la práctica se utiliza un rango de frecuencias de 1 a 100 MHz. Para mantener bajas las pérdidas en el núcleo del transformador se debe seleccionar un material de ferrita adecuado para ésta frecuencia.

Debido a que la eficiencia en la transferencia de energía del lector al transponder es alta, los sistemas de acoplamiento cercano son muy adecuados para la operación de circuitos integrados con alto consumo de energía. Esto incluye microprocesadores, los cuales requieren de cerca de 10 mW de potencia para operar. Por ésta razón todos los sistemas de acoplamiento cercano que hay en el mercado incluyen microprocesadores en el transponder.



*Figura II.11 Transponder de acoplamiento cercano en un lector de inserción con bobinas de acoplamiento magnético.[1]*

Para la transferencia de datos del transponder al lector se utiliza también la modulación de carga con subportadora. Las frecuencias de la subportadora y la modulación están especificadas en la norma ISO 10536.

Debido a la corta distancia entre el lector y el transponder los sistemas de acoplamiento cercano también pueden emplear el acoplamiento capacitivo para la transmisión de datos. Para esto se construyen placas de capacitor en la superficie de acoplamiento aisladas una de la otra. Se colocan de manera tal que queden exactamente en paralelo cuando el transponder es insertado.

### **Acoplamiento eléctrico**

En los sistemas acoplados eléctricamente (o capacitivo), el lector genera un fuerte campo eléctrico de alta frecuencia. La antena del lector consiste en gran área eléctricamente conductiva (electrodo), generalmente una placa de metal. Si se aplica

un voltaje de alta frecuencia al electrodo se forma un campo eléctrico de alta frecuencia entre éste y la tierra potencial. El voltaje requerido para esto va desde unos cientos hasta unos pocos miles de volts, los cuales son generados en el lector por el incremento de voltaje en un circuito resonante (ver figura II.12) hecho de una bobina  $L_1$  y un capacitor en paralelo  $C_1$  además de la capacitancia activa entre el electrodo y la tierra potencial  $C_{R-GND}$ . La frecuencia resonante del circuito corresponde con la frecuencia de transmisión del lector.

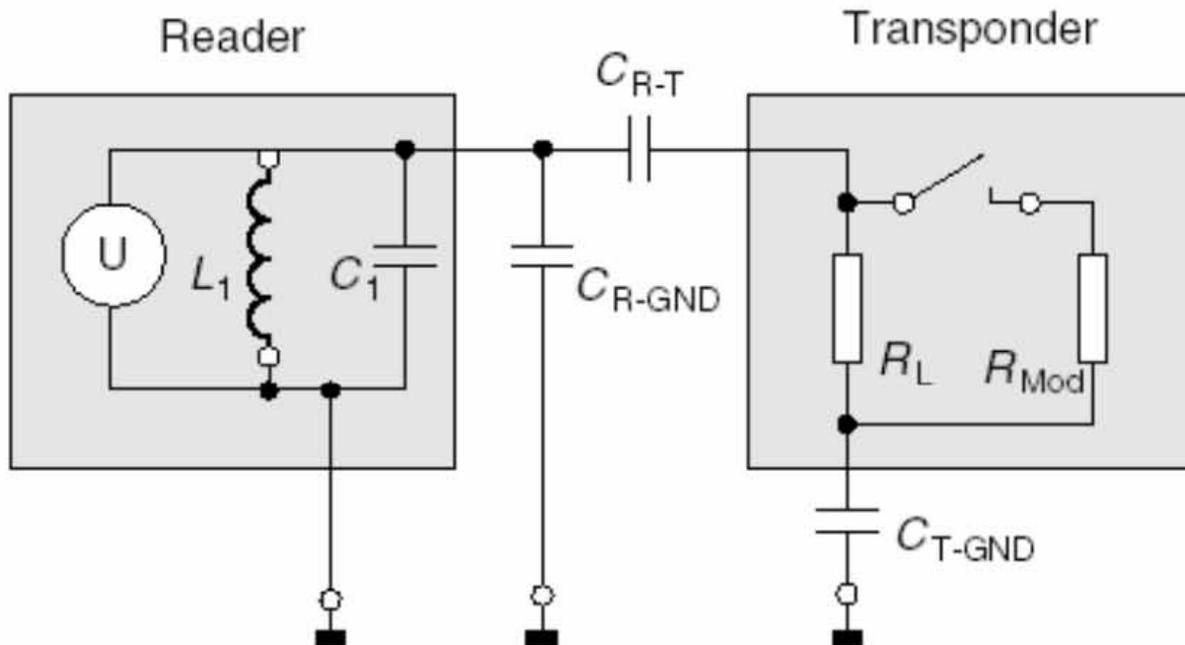


Figura II.12 Diagrama de un circuito equivalente para un sistema RFID acoplado eléctricamente. [1]

La antena del transponder está hecha de hasta dos superficies conductoras en un plano (electrodos). Si el transponder es colocado dentro del campo eléctrico del lector, entonces aparece una diferencia de potencial entre los dos electrodos del transponder, lo cual es utilizado para proporcionar energía a los circuitos (figura II.13).

Sin un transponder acoplado eléctricamente es colocado dentro de la zona de interrogación de un lector, la resistencia de entrada  $R_L$  actúa sobre el circuito resonante del lector a través del acoplamiento con la capacitancia activa  $C_{R-T}$  entre el lector y los electrodos del transponder, alterando ligeramente el circuito resonante. Esta alteración puede ser cambiada a dos valores conectando y desconectando el resistor  $R_{MOD}$ , de ésta manera al conectar y desconectar el resistor se obtendrá una fluctuación de voltaje presente en  $L_1$  y  $C_1$  ocasionada por el transponder. Si la conexión y desconexión se

realiza en sincronía con los datos almacenados, obtendremos que se transmiten estos datos al lector. Este proceso se denomina modulación de carga.

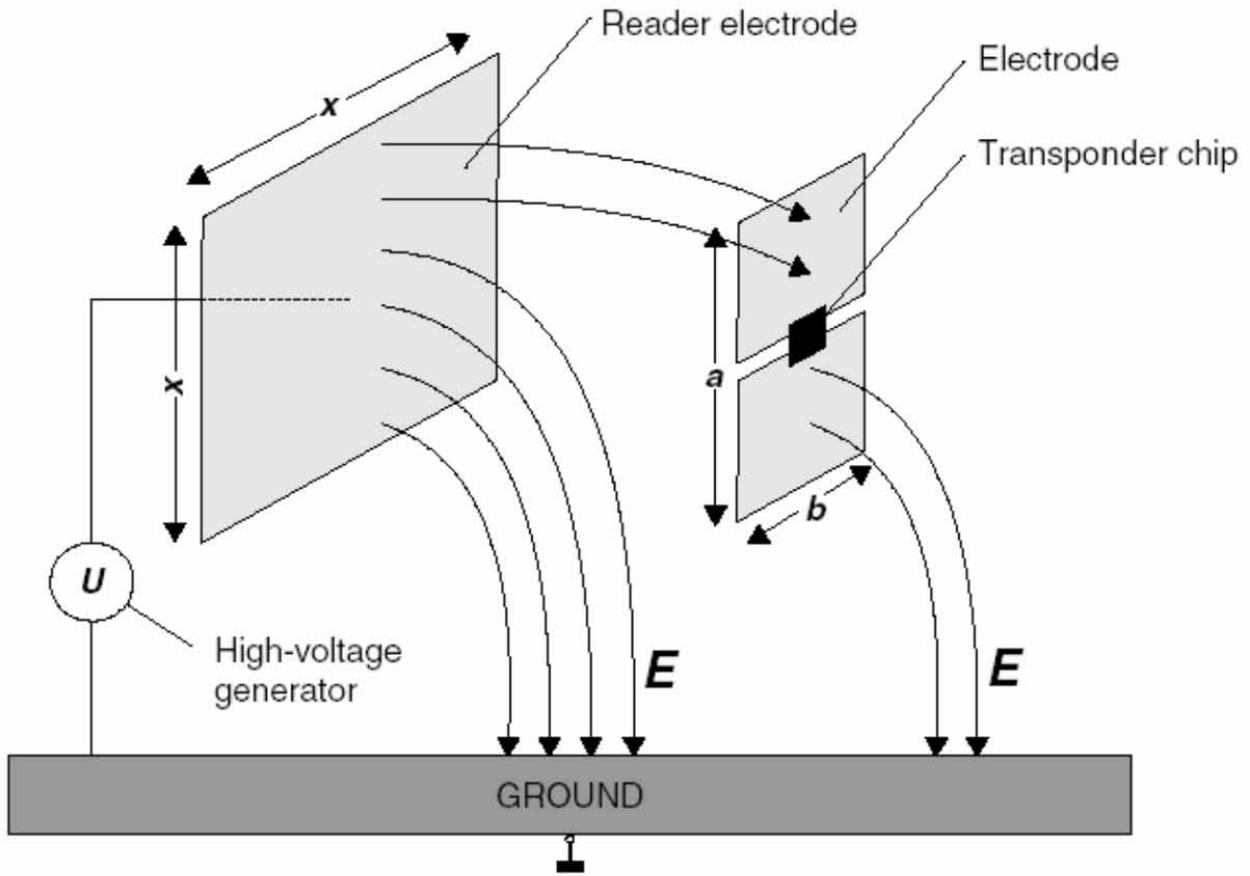


Figura II.13 En un sistema acoplado eléctricamente se utilizan los campos eléctricos para la transmisión de energía y datos.[1]

El envío de datos del lector al transponder en los sistemas full y half duplex utilizan básicamente tres procedimientos, independientemente de la frecuencia que se utilice: ASK (*amplitude shift keying*), FSK (*frequency shift keying*) y PSK (*phase shift keying*).

Debido a que la modulación ASK es más fácil de demodular, es utilizada por la mayoría de los sistemas.

### **II.2.2.2 Sistemas de procedimientos secuenciales**

La diferencia principal de los procedimientos secuenciales es que la transmisión de datos y de energía del lector al transponder se alterna con el envío de datos del transponder al lector.

Existen dos formas de acoplamiento básico para los sistemas secuenciales: el acoplamiento inductivo y el denominado SAW (surface acoustic wave- onda acústica de superficie).

#### **Acoplamiento inductivo**

Los sistemas secuenciales que utilizan el acoplamiento inductivo son operados exclusivamente a frecuencias menores a 135 kHz. Se crea un acoplamiento tipo transformador entre la bobina del lector y la bobina del transponder. El voltaje inducido en la bobina del transponder se rectifica y puede ser utilizado como fuente de energía.

Para obtener la máxima eficiencia en la transferencia de datos, la frecuencia del transponder debe ser precisamente la del lector, y la calidad de la bobina del transponder debe ser cuidadosamente especificada. Por ésta razón se utilizan capacitores para compensar las tolerancias de fabricación.

Sin embargo, a diferencia de los sistemas half y full duplex, en los sistemas secuenciales el transmisor del lector no opera en una base continua. La energía transferida carga un capacitor para proveer un almacenaje. El circuito integrado del transponder es apagado o colocado en ciclo de espera para que casi toda la energía recibida sea almacenada en el capacitor. Después de un período de carga fijo, el transmisor de lector es apagado nuevamente. A partir de esto la energía almacenada en el capacitor es utilizada para enviar una réplica al lector.

En los sistemas secuenciales el ciclo completo de lectura consiste en dos fases, la fase de carga y la fase de lectura. El fin de la fase de carga es detectado monitoreando la ruta del voltaje en la bobina del transponder y reconociendo de ésta manera el momento cuando el lector ha cesado su transmisión. Inmediatamente después se activa un oscilador que produce un campo magnético alterno débil que puede ser detectado por el lector.

Para poder modular la señal de HF generada en la ausencia de una fuente de energía, se conecta un capacitor de modulación adicional en paralelo con el circuito resonante, en sincronía con el flujo de datos, resultando una modulación 2 FSK.

Después de que todos los datos son transmitidos, se activa el modo de descarga para descargar por completo el capacitor. Esto garantiza un inicio seguro en el siguiente ciclo de carga.

### Onda acústica de superficie (SAW)

Los dispositivos SAW están basados en el efecto piezoeléctrico y en la dispersión de ondas elásticas (acústicas) a baja velocidad. Si un cristal (iónico) es deformado elásticamente en una cierta dirección aparecen cargas de superficie incrementando el voltaje en el cristal. Si por el contrario, se aplica un voltaje a un cristal ocurre una deformación elástica. Los dispositivos SAW son operados a frecuencias de microondas, normalmente en el orden de 2.45 GHz.

En la figura II.14 se puede apreciar un esquema básico de un transponder SAW. Una estructura de electrodos en forma de dedo, el transductor interdigital, es colocado al final del largo substrato piezoeléctrico., y una antena de dipolo adecuada para la frecuencia reoperación es colocada a su barra de bus. El transductor interdigital es utilizado para la conversión entre señales eléctricas y ondas acústicas de superficie.

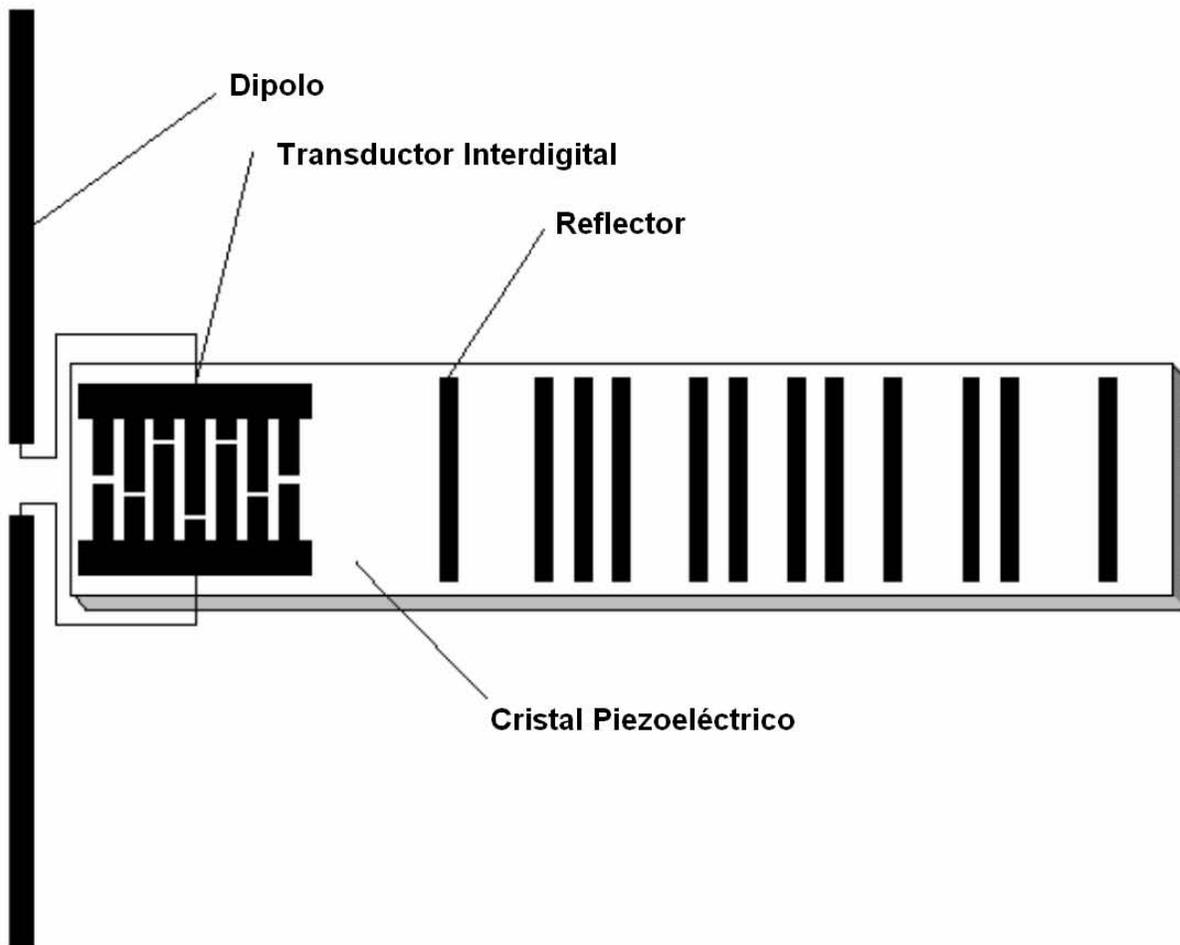


Figura II.14 Esquema básico de un transponder SAW

Un impulso eléctrico aplicado en la barra del bus causa una deformación mecánica a la superficie del sustrato debido al efecto piezoeléctrico entre los electrodos, el cual se dispersa en ambas direcciones en la forma de una onda de superficie. Similarmente, una onda de superficie entrando al convertidor crea un impulso eléctrico en la barra del bus en el transductor interdígital debido al efecto piezoeléctrico.

Se colocan electrodos a lo largo de la superficie del transponder, los cuales reflejan un aparte de las ondas acústicas de superficie al transductor interdígital. Debido a la diferente velocidad con la que viajan las ondas de superficie, comparadas con las ondas electromagnéticas, se puede hacer un arreglo de manera tal que el espaciamiento entre los electrodos corresponda a un bit, de manera similar al código de barras. Existen limitaciones físicas para el espaciamiento entre barras, pero se puede tener información de 16 a 32 bits transfiriéndose a una velocidad de 500 kbits/s.

El rango de un sistema de ondas de superficie depende principalmente de la potencia de la transmisión. A la potencia permisible de transmisión en la frecuencia de 2.45 GHz se puede esperar un rango de lectura de 1 a 2 m.

### **II.3 NORMALIZACIÓN**

Existen estándares relativos al rango de frecuencias, la forma en que se comunican el lector y el transponder, la sintaxis de transferencia de datos, la unicidad del número almacenado en la etiqueta o transponder, etc. Sin embargo debido a la gran cantidad de fabricantes y a la falta de regulación se han creado muy diferentes sistemas que hacen casi imposible la comunicación entre los diferentes componentes del mismo, cuando éstos provienen de diferentes fabricantes.

En los últimos años sin embargo la ISO (*Internacional Standard Organization*) ha realizado esfuerzos para la uniformidad y regulación de la fabricación de componentes, y su uso, en los sistemas RFID.

A continuación se hace una breve explicación de los estándares más importantes.

#### **II.3.1 Identificación de animales**

Los estándares ISO 11784, 11785 y 14223 tratan con la identificación de animales utilizando los sistemas RFID.

El ISO 11784 trata de la estructura del código. Entre sus características principales es que define un total de 64 bits (8 bytes) para el código de identificación de animales. El código de identificación nacional debe ser manejado por países individuales. Los bits del 27 al 64 pueden ser utilizados para definir entre diferentes tipos de animales, regiones dentro de los países, etc

El estándar ISO 11785 define el método de transmisión para los datos del transponder y las especificaciones del lector para activarlo. Un propósito central en el desarrollo de éste estándar era facilitar la interrogación de los transponders desde un rango extremadamente amplio de fabricantes utilizando un lector común. Un lector para identificación de animales que cumple con ésta norma, reconoce y hace la diferenciación entre transponders que utilizan sistemas full-half duplex y los que utilizan sistemas secuenciales.

El estándar ISO 14223 define la interfaz de alta frecuencia (HF) y la estructura de datos de los llamados transponder avanzados. ISO 14223 está basado en los estándares anteriores, ISO 11784 e ISO 11785, representando un desarrollo adicional a éstos. Mientras que los transponders que cumplen con la norma ISO 11785 solo transmiten un código de identificación permanentemente programado, en los transponder avanzados existe la posibilidad de manejar mayores áreas de memoria. Como resultado, los datos pueden ser leídos, escritos e inclusive protegidos contra sobre - escritura.

### **II.3.2 Tarjetas inteligentes libres de contacto**

Existen cuatro diferentes estándares para las tarjetas inteligentes libres de contacto: ISO 10536, ISO 14443, ISO 15693 e ISO 10373.

El estándar ISO 10536 titulada “Tarjetas de identificación - tarjetas de circuitos integrados libres de contacto”, describe la estructura y los parámetros de operación de las tarjetas inteligentes libres de contacto de acoplamiento cercano. La norma consiste de las siguientes cuatro secciones:

- Parte 1: Dimensiones físicas.
- Parte 2: Dimensiones y localización de las áreas de acoplamiento.
- Parte 3: Señales electrónicas y procedimientos de inicialización.
- Parte 4: Respuesta a la inicialización y protocolos de transmisión.

El ISO 14443 describe el método y los parámetros de operación de las tarjetas inteligentes de proximidad libres de contacto. Esto significa tarjetas inteligentes libre de contacto con un rango aproximado de 7 a 15 cm. La norma comprende las siguientes partes:

- Parte 1: Características físicas.
- Parte 2: Potencia de Radiofrecuencia e interfaz de señal.
- Parte 3: Inicialización y anticolisión.
- Parte 4: protocolos de transmisión.

El estándar ISO 15693 titulada “Tarjetas de Identificación – tarjetas de circuito integrado libres de contacto – tarjetas de vecindad” define el método y los parámetros de operación y funcionamiento de las tarjetas con un rango de hasta 1 m. El estándar está hecho de las siguientes partes:

- Parte 1: Características físicas.
- Parte 2: Potencia de Radiofrecuencia e interfaz y marcos de señal.
- Parte 3: Protocolos.
- Parte 4: Registro de aplicaciones/emisores.

El estándar ISO 10373 proporciona la norma relativa a las pruebas de las tarjetas con o sin circuito integrado. Además de las pruebas para las características de calidad, tales como resistencia al doblaje, resistencia a químicos, flamabilidad, etc, también describe los diferentes métodos de prueba desarrollados para verificar las características.

### **II.3.3 ISO 69873 - Portadores de datos para herramientas**

Esta norma especifica las dimensiones para tarjetas libres de contacto y su espacio de montaje en herramientas y cortadores. Normalmente los portadores de datos son colocados en un eje de rápida liberación de acuerdo a la norma ISO 69871 o en una perilla de retención de acuerdo a la norma ISO 69872. El estándar proporciona ejemplos para esto.

### **II.3.4. Identificación de contenedores**

Este estándar describe el sistema de identificación automática para contenedores basado en transponders de microondas. La identificación óptica de los contenedores está descrita en el ISO 6346 y está reflejado en el registro de datos de identificación de contenedores basados en transponders.

### **II.3.5 VDI 4470 - Sistemas antirrobo de bienes**

La VDI 4470 comprende los lineamientos para los sistemas antirrobo en tiendas, basados principalmente en los sistemas de 1 bit (EAS). Estos lineamientos incluyen desde las dimensiones de los sistemas detectores hasta las pruebas de operación y funcionamiento.

# **Componentes de Hardware de un sistema RFID**

III.1. Dispositivo Lector

III.2. Transponder

**Capítulo 3**

## COMPONENTES DE HARDWARE DE UN SISTEMA RFID

En su núcleo, los sistemas RFID utilizan tecnología de semiconductores e inalámbrica como un medio para identificar y rastrear productos. Como se ha mencionado anteriormente, el sistema típico de RFID requiere de un transponder o etiqueta la cual está compuesta por un semiconductor y una pequeña antena, y de un lector de etiquetas.

Estas etiquetas, dependiendo de su tipo, son capaces de almacenar cantidades significativas de información (hasta varios kilobytes), y puede ser montada en una gran variedad de productos con el propósito de identificarlos y rastrearlos. Cada etiqueta tiene un código de identificación instalado por el fabricante así como memoria disponible adicional. Cuando una etiqueta RFID pasa dentro del rango de un lector, la etiqueta es detectada e interrogada por su contenido de información. Este proceso es conducido por una señal de radiofrecuencia inalámbrica a través de la antena.

El lector es capaz de almacenar y transferir la información del producto, lo cual puede incluir el número de lote del producto, su localización y estado, así como una amplia variedad de otra información potencial, a un sistema de cómputo.

### III.1 Dispositivo Lector

Una aplicación de software que está diseñada para leer datos de un transponder o escribir datos en él, requiere de un lector libre de contacto como interfaz. Desde el punto de vista de la aplicación de software, el acceso al portador de datos (transponder) debe ser lo más transparente posible. En otras palabras, las operaciones de lectura y escritura deberían diferir lo menos posible del proceso de acceder a otros portadores de datos comparables.

Las operaciones de lectura y escritura son realizadas en el principio de maestro-esclavo. Esto significa que todas las actividades del lector y del transponder son iniciadas por la aplicación de software, en donde ésta representa al maestro y el lector al esclavo.

Un comando simple de la aplicación de software al lector puede iniciar una serie de pasos de comunicación entre el lector y el transponder. Por lo tanto, las funciones principales del lector son activar al transponder, estructurar la secuencia de comunicación con él y transferir datos entre el lector y el dispositivo portador de datos. Todas las características de la comunicación libre de contacto, por ejemplo hacer la conexión y ejecutar los procedimientos de anticollisión y autenticación, son realizadas por el lector.

### III.1.1 Componentes de un lector

A pesar de las diferencias fundamentales en el tipo de acoplamiento, como por ejemplo la secuencia de comunicación, el procedimiento de transmisión del transponder al lector y el rango de frecuencia, todos los lectores son similares en su principio básico de operación y por lo tanto en su diseño.

Los lectores de todos los sistemas pueden ser reducidos a dos bloques de funcionamiento principales: el sistema de control y la interfaz de alta frecuencia, la cual consiste de un transmisor y un receptor (figura III.1).

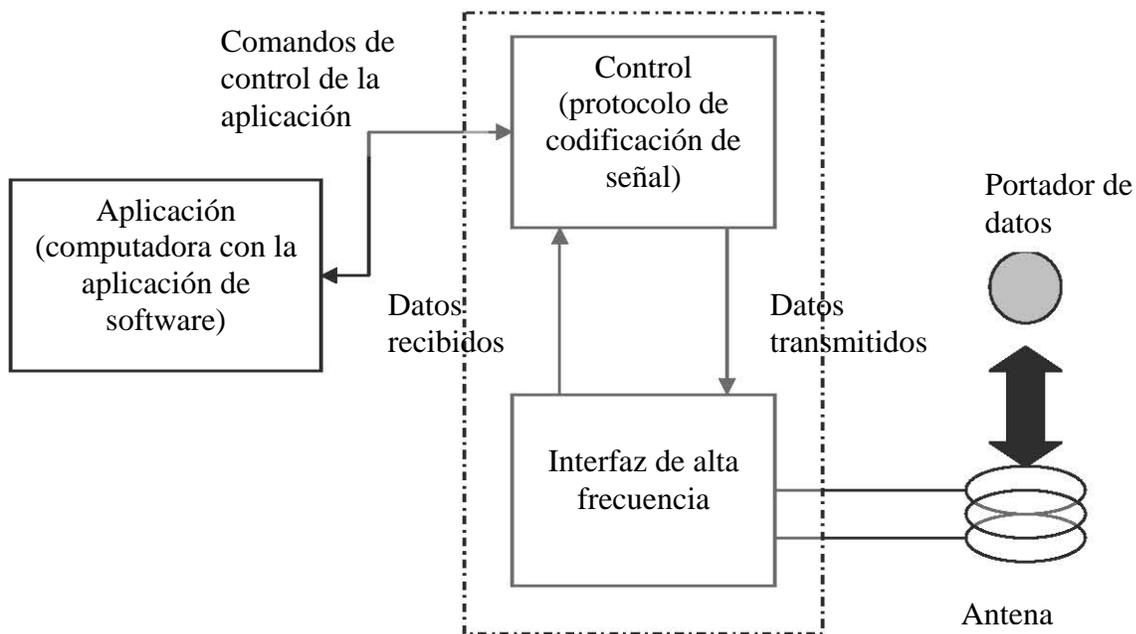


Figura III.1 Diagrama de bloques de un lector.

#### III.1.1.1 Interfaz de alta frecuencia

La interfaz de alta frecuencia del lector tiene las siguientes funciones:

- Generación de la potencia de transmisión de alta frecuencia para activar el transponder y proporcionarle energía.
- Modulación de la señal de transmisión para enviar datos al transponder.
- Recepción y demodulación de las señales de alta frecuencia transmitidas por el transponder.

La interfaz de alta frecuencia contiene dos rutas de señal separadas para corresponder con las dos direcciones de flujo de datos desde y hacia el transponder (figura III.2). Los datos transmitidos al transponder viajan por el *brazo transmisor*. Por el contrario, los datos recibidos del transponder son procesados en el *brazo receptor*.

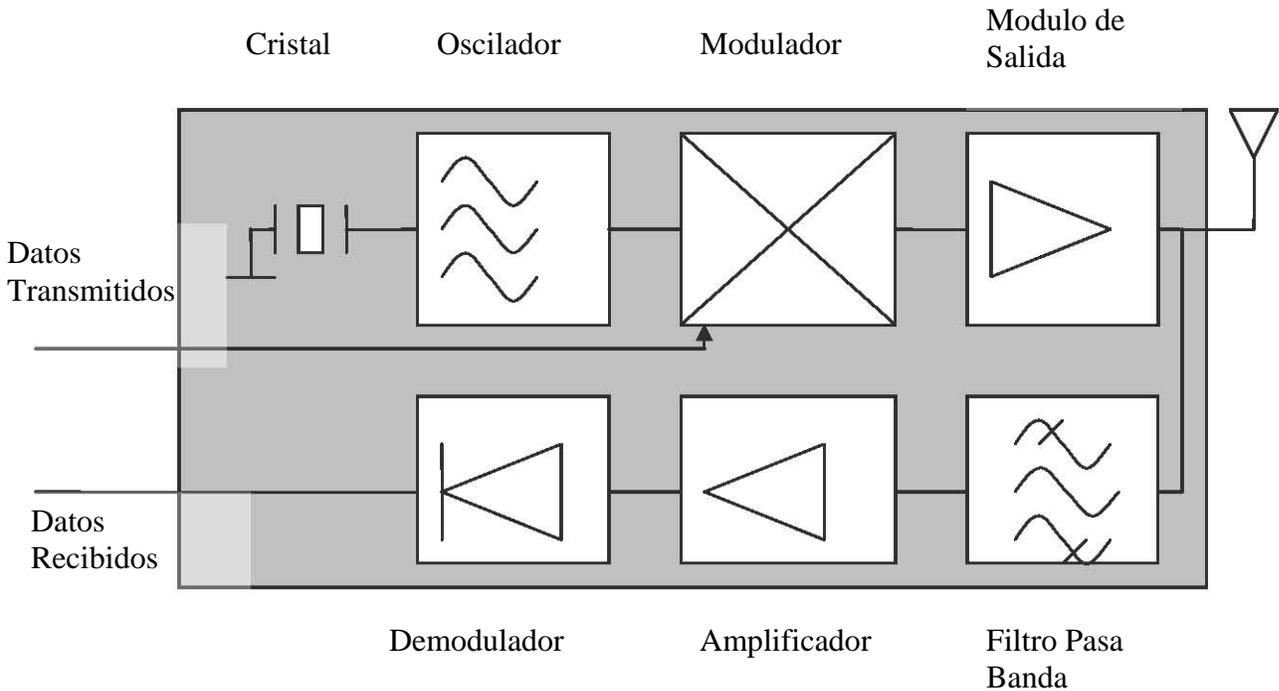


Figura III.2 Diagrama de bloques de una Interfaz de alta frecuencia para un sistema RFID

En los sistemas Full y Half Duplex acoplados inductivamente, primero se obtiene una señal a la frecuencia requerida utilizando para ello un oscilador. Esta señal es alimentada a un modulador que a su vez está controlado por otra señal que contiene los datos transmitidos. En ésta última, la información se encuentra en los diferentes niveles TTL, lo que quiere decir que es una señal binaria, y viene codificada con algunos métodos diferentes (Manchester, Millar, NRZ). Dependiendo del tipo de modulador, se puede realizar una modulación ASK o PSK a la señal proveniente del oscilador. También se puede realizar una modulación FSK para lo cual la señal de datos es alimentada directamente en el sintetizador de frecuencia.

Después de la etapa de modulación, la señal es llevada a un módulo de salida el cual proporciona la potencia necesaria para ser transmitida por la antena.

El *brazo receptor* de la interfaz de alta frecuencia consiste en su primera etapa en un filtro que se encuentra acoplado directamente a la antena. Este filtro tiene una importancia particular, ya que dependiendo del tipo de acoplamiento debe ser capaz de

bloquear la señal de transmisión, generalmente con mucho mas potencia que la señal recibida desde el transponder.

Como se puede apreciar en la figura III.3, en los sistemas RFID que operan a frecuencia de microondas la obtención de ésta no puede ser a través de la generación por un oscilador de cuarzo. En cambio, lo que se hace es un proceso de multiplicación de frecuencia (o excitación de armónicas) hasta obtener la frecuencia deseada. Debido a que la modulación es retenida durante éste proceso de multiplicación, el modulador se encuentra en una etapa anterior a la excitación de armónicas.

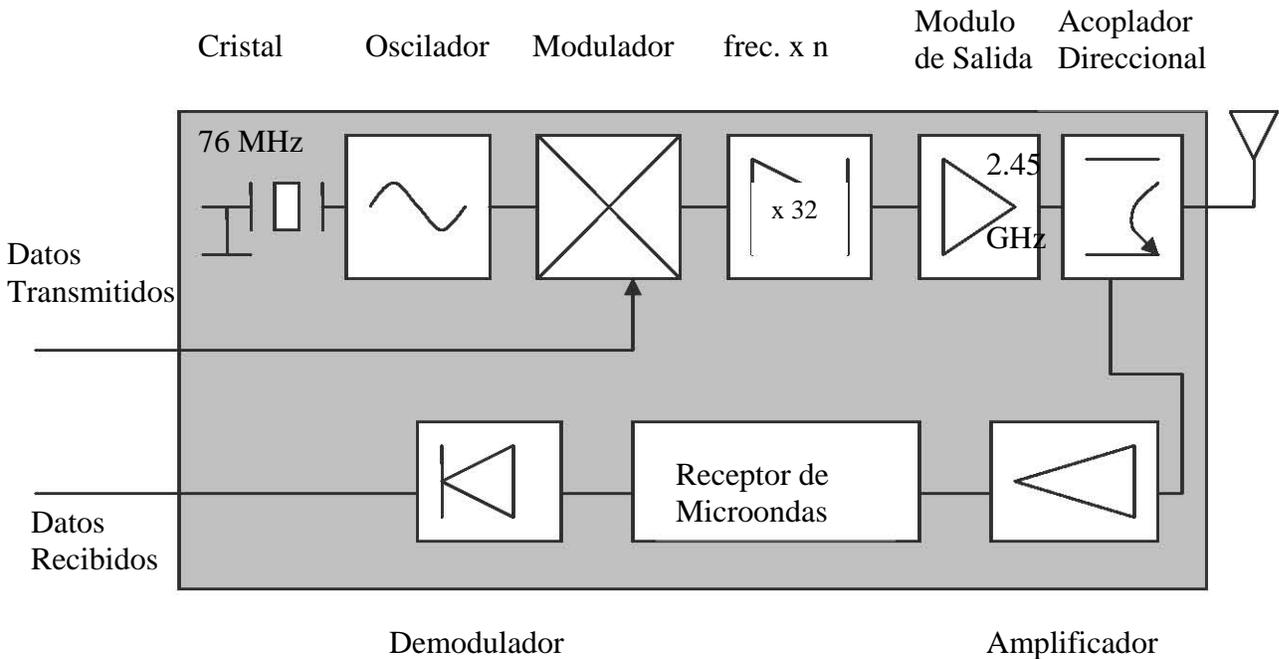


Figura III.3 Diagrama de bloques de una interfaz de HF para sistemas de microondas

Algunos lectores de microondas emplean un acoplador direccional para separar la señal propia de la reflejada por el transponder.

En los sistemas secuenciales de RFID el campo de alta frecuencia del lector sólo transmite brevemente para proporcionarle potencia y comandos al transponder. El transponder transmite sus datos al lector mientras éste no está transmitiendo, por lo que tanto el lector como el transponder se activan secuencialmente. En la figura III.4 se puede apreciar el diagrama de bloques de la interfaz de alta frecuencia para un sistema secuencial.

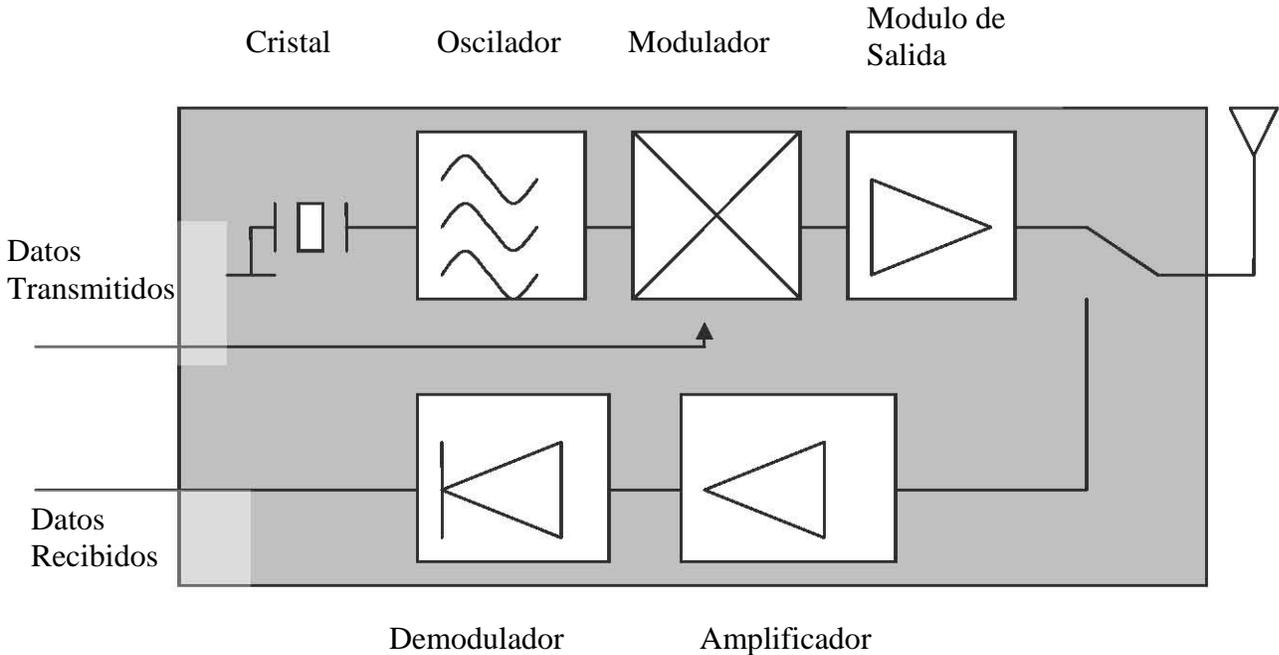


Figura III.4 Diagrama de bloques de una interfaz de HF para un sistema secuencial.

En los sistemas de microondas de onda acústica de superficie (SAW) la antena del lector transmite un pulso electromagnético corto el cual es recibido por la antena del transponder y convertido en una onda de superficie en un cristal piezoeléctrico. Un arreglo característico de estructuras parcialmente reflectoras da lugar a numerosos pulsos que son transmitidos de vuelta a la antena del transponder como una señal de respuesta.

Debido a los tiempos de retardo en el cristal piezoeléctrico, la señal reflejada por el transponder puede ser fácilmente separada por el lector de otras señales electromagnéticas reflejadas.

Como se puede apreciar en la figura III.5, se utilizan un estabilizador de frecuencia y un oscilador de fase con un resonante de onda de superficie para la generación de la alta frecuencia. Utilizando una conmutación rápida, se obtienen pulsos cortos de alta frecuencia de alrededor de 80 ns de duración, los cuales son amplificados a alrededor de 36 dBm (4 W pico) por la etapa de salida de potencia, que son transmitidos por la antena del lector.

Si un transponder SAW se encuentra en la vecindad del lector reflejará una secuencia de pulsos individuales después de un tiempo de retardo de propagación de unos pocos microsegundos. Estos pulsos son recibidos por la antena del lector a través de un

amplificador de bajo ruido y luego son demodulados en un demodulador de cuadratura. Esto conduce a dos componentes ortogonales (I y Q) que facilitan la determinación del ángulo de fase entre los pulsos individuales y entre los pulsos y el oscilador. La información obtenida puede ser utilizada para determinar la distancia entre el transponder SAW y el lector y para la medición de cantidades físicas.

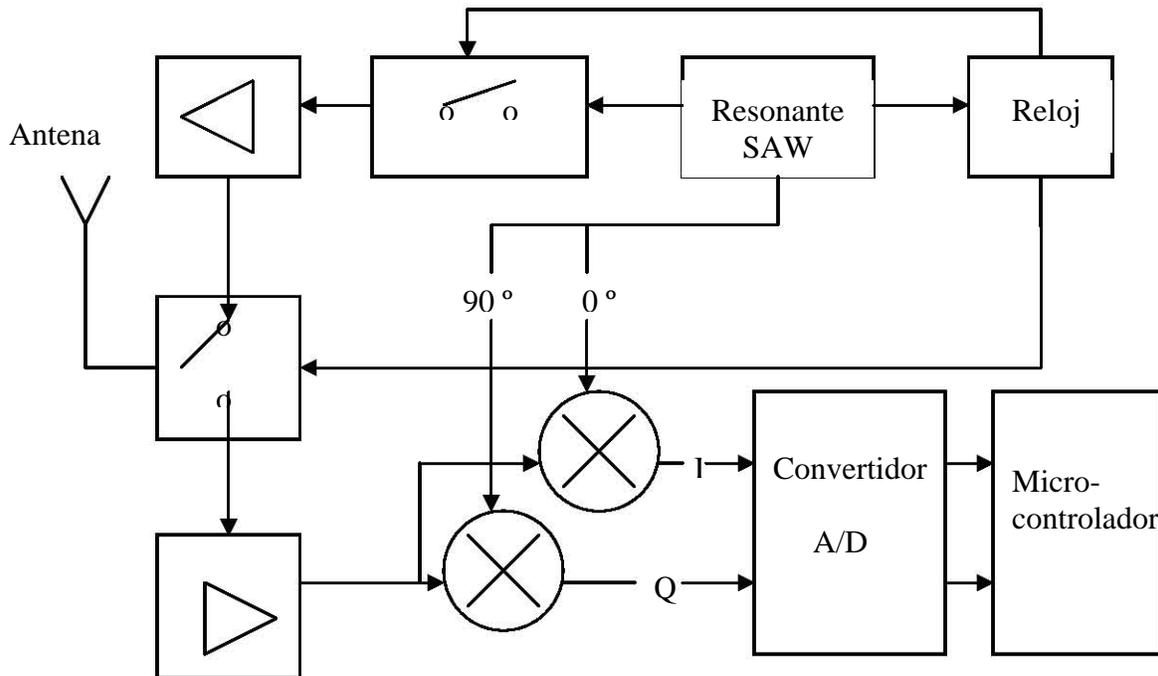


Figura III.5 Diagrama de bloques para un lector SAW

### III.1.1.2 Unidad de Control

La unidad de control del lector ejecuta las tiene funciones:

- Comunicación con el software de la aplicación y la ejecución de comandos recibidos.
- Control de la comunicación con en transponder (principio maestro-esclavo).
- Codificación y decodificación de la señal.

En sistemas más complejos se encuentran disponibles las siguientes funciones:

- Ejecución del algoritmo de anticolidión.
- Encriptado y decriptado de los datos transferidos entre el transponder y el lector.
- Realizar la autenticación entre el transponer el lector.

La unidad de control usualmente está basada en un microprocesador para ejecutar las funciones complejas. Los procedimientos de encriptado y también la codificación de señal con frecuencia son realizados por un módulo adicional ASIC (*Application Specific Integrated Circuit*) para liberar al procesador de procesos intensos de cálculo. En la figura III.6 se muestra el diagrama de bloques de una unidad de control de un lector.

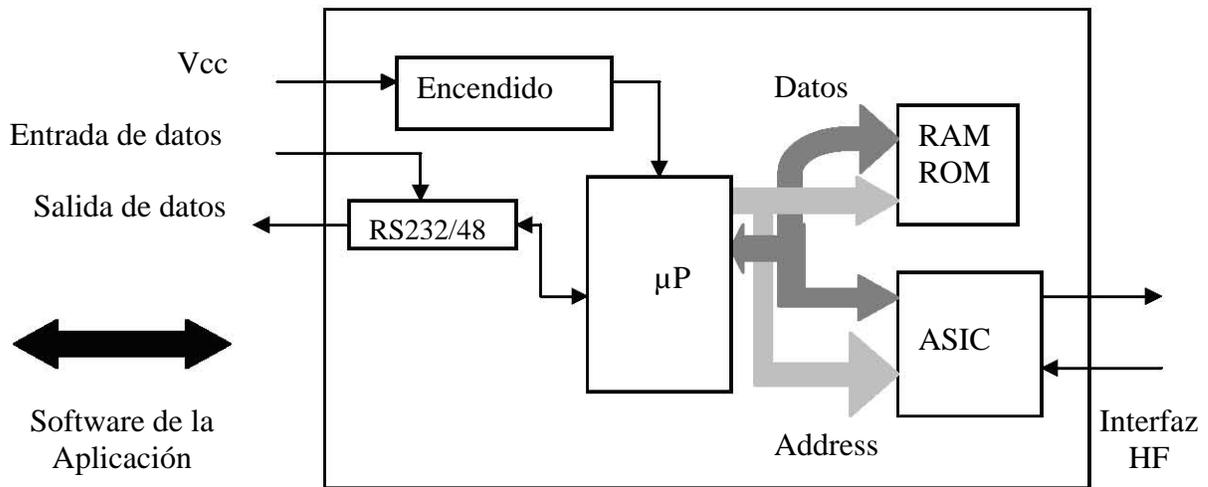


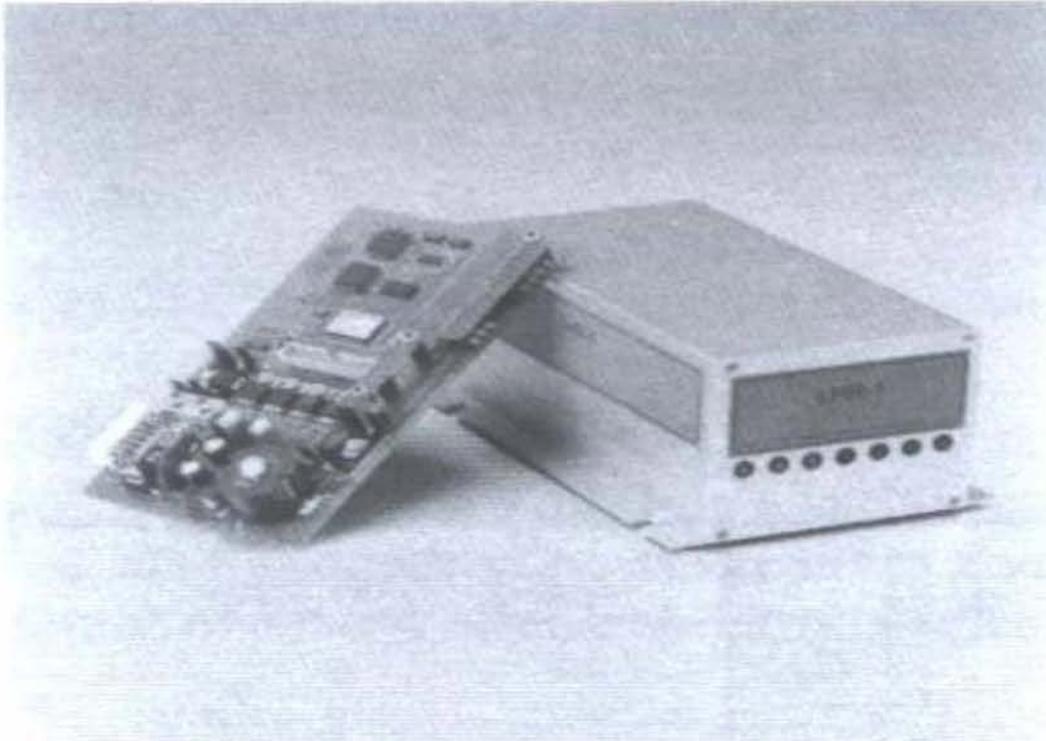
Figura III.6 Diagrama de bloques de la unidad de control del lector.

### III.1.2 Tipos de Lector

#### III.1.2.1 Lectores OEM

Los lectores OEM (Original Equipment Manufacturer) son aquellos disponibles para integrarse en los sistemas de captura de datos del cliente. Esto es, el cliente puede colocar su propia marca en el lector para tener un producto final del que éste forme parte. Estos lectores generalmente vienen en presentaciones con encapsulado sellado o en tarjetas electrónicas. En la figura III.7 se puede observar un ejemplo de éstos lectores.

Algunos de los datos técnicos típicos de los lectores son: Voltaje, Antena (interna o externa), tipo de conexión de la antena, interfaz de comunicación, protocolo de comunicación y temperatura ambiental.



[1]  
*Figura III.7 Ejemplo de un lector OEM*

### III.1.2.2 Lectores para uso industrial

Los lectores industriales son diseñados para su uso en plantas de fabricación y ensamblaje. Estos usualmente tienen un bus de interfaz estandarizado para tener una integración simple a los sistemas ya existentes. Además, éstos lectores tienen varios tipos de protección incluyendo los que soportan cierto tipo de explosiones.

### III.1.2.3. Lectores portátiles

Los lectores portátiles son utilizados en la identificación de animales, como dispositivo de control en el transporte público, como terminal para pagos, como ayuda en mantenimiento y en pruebas y en sistemas especiales (inventarios, etc). Estos lectores generalmente tienen una pantalla de LCD (*Liquid Cristal Display*) y un teclado para la introducción de datos. En ocasiones tienen una interfaz RS-232 para intercambiar datos con una computadora.

Algunos de estos dispositivos tienen protección contra agua o para protegerlo de condiciones ambientales difíciles.

[1] Finkenzerler, K. *RFID Handbook*. Segunda Edición. 2004. John Wiley & Sons, Ltd. West Sussex. UK. 327.

En la figura III.8 se muestra un ejemplo de un lector portátil.



*Figura III.8 Lector RFID portátil*

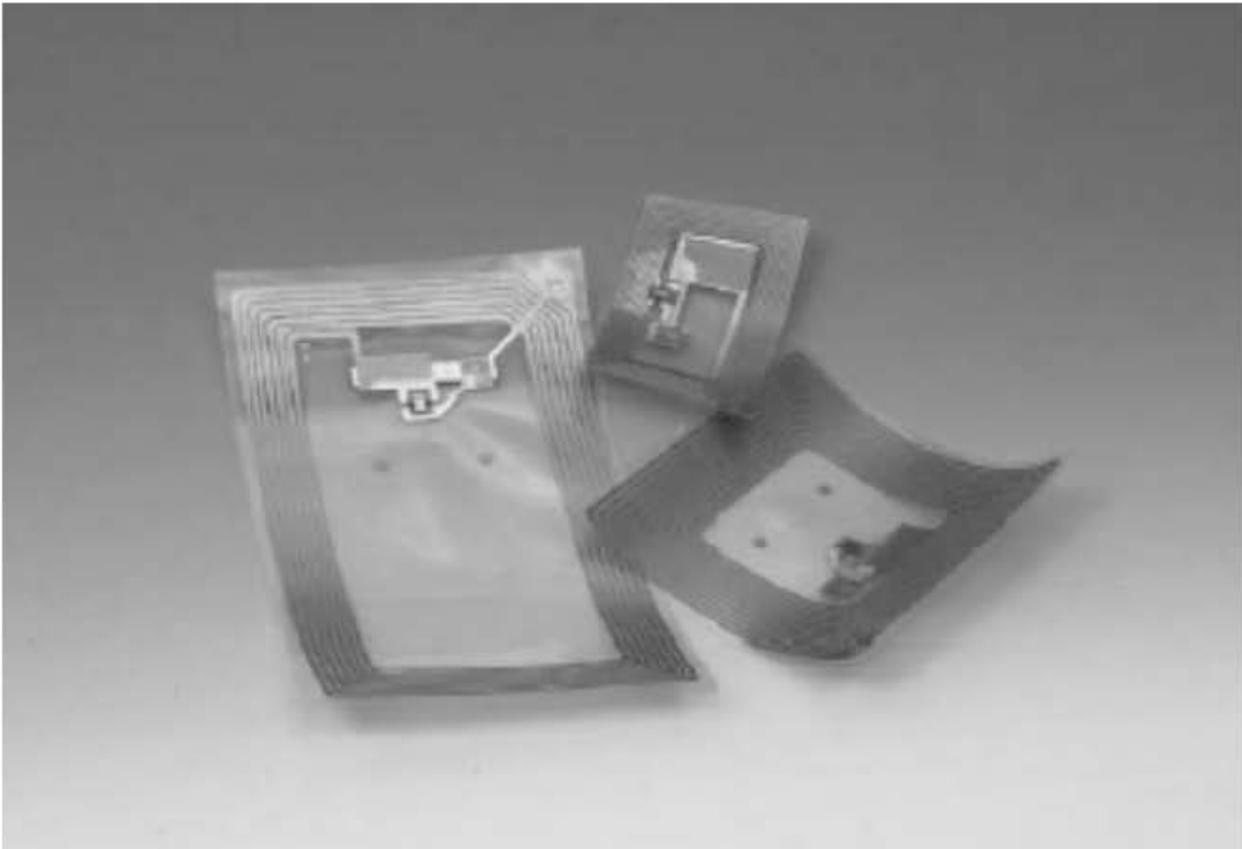
### **III.2 TRANSPONDER**

Existen una gran variedad de transponder o etiquetas RFID. Por lo mismo es imperativo seleccionar los más adecuados para que el sistema funcione correctamente. Los transponders o etiquetas pueden colocarse en superficies de madera, plástico, metal, en etiquetas con código de barras, en animales y dependiendo de la aplicación en una gran variedad de dispositivos.

Un transponder está compuesto por:

- Circuito Integrado de silicón: dispositivo que contiene los datos.
- Antena: Esta se encuentra unida al circuito integrado (chip) para transmitir o recibir datos.
- Substrato: Papel o plástico donde se montan la antena y el circuito integrado.

La figura III.9 muestra varios transponders de Texas Instruments de la serie Tag-it™ en forma rectangular y que operan en la frecuencia de 13.56 MHz.



[20]

*Figura III.9 Transponders de la serie Tag-it™ de Texas Instruments.*

Las etiquetas RFID pueden ser de muchas formas y niveles de potencia. El identificador único es codificado en un circuito integrado que se convierte en el portador de datos. Los datos son transmitidos al lector a través de una antena incorporada dentro de la etiqueta. Las etiquetas pueden ser tan pequeñas como la cabeza de una hormiga o mas grande que la palma de un humano adulto, o cualquier tamaño entre ellas. El factor forma que toma la etiqueta RFID es dictado por factores que incluyen potencia, durabilidad y requerimientos de tiempo de vida. Las características de la etiqueta están definidas por la aplicación y pueden variar en sus requerimientos de potencia, capacidad de lectura/escritura y frecuencia. Esta frecuencia se fija de acuerdo a las necesidades del sistema incluyendo el rango de lectura y el medio ambiente en el cual será leída.

Existen tres tipos básicos de etiquetas:

- Etiquetas pasivas.
- Etiquetas Activas

[20] Texas Instruments. 03 de Julio de 2005. <http://www.ti-rfid.com>

- Etiquetas semiactivas.

### **Etiquetas Pasivas**

Las etiquetas “pasivas” son etiquetas RFID que no contienen una fuente de energía independiente y obtienen su potencia directamente del Lector. Consecuentemente las etiquetas pasivas son más ligeras que las etiquetas pasivas, menos caras y ofrecen un tiempo de operación virtualmente ilimitado. A cambio, tienen rangos de lectura más cortos que las etiquetas activas y requieren un lector de más alta potencia. Las etiquetas pasivas son las más comunes asociadas con el rastreo de mercancías.

Las etiquetas de solo lecturas son típicamente pasivas y están programadas con un juego único de datos (usualmente de 32 a 128 bits) que no pueden ser modificados. La mayoría de las etiquetas de solo lectura operan como un enlace a la base de datos de la misma manera en que los códigos de barras hacen referencia a una base de datos que contiene información específica del producto.

### **Etiquetas Activas**

Las etiquetas activas son energizadas por una batería interna y son típicamente de lectura/escritura en donde los datos pueden grabados o modificados. En éste caso el tamaño de memoria varía dependiendo de los requerimientos del sistema. El uso de una batería interna proporciona un mayor rango de lectura. A cambio, estas etiquetas son más robustas, más caras y tienen un tiempo de vida mas corto, dependiendo de las condiciones de temperatura ambiental y tipo de batería.

### **Etiquetas Semiactivas**

Las etiquetas semiactivas incorporan baterías, pero éstas solo son utilizadas para energizar la circuitería y no para mejorar la comunicación con el lector. En este caso la energía para transmitir la información sigue siendo tomada del campo generado por el Lector. Estas etiquetas son menos comunes pero están emergiendo como una solución que combina el mayor rango de lectura de las etiquetas activas, con el menor costo de las etiquetas pasivas.

Las etiquetas RFID pueden ser de lectura/escritura (R/W) o de sólo lectura (R/O), o alguna combinación de éstas. Las etiquetas de lectura/escritura permiten que los datos sean actualizados o escritos en la etiqueta. Las etiquetas de solo lectura se utilizan cuando es necesario que los datos contenidos no cambien ya que no permiten la escritura en ellas.

### **Solo Lectura**

Las etiquetas de solo lectura contienen un identificador, tales como un número de producto o un número de serie que es programado en el chip cuando es fabricado. Este identificador permanece constante a lo largo de la vida del circuito integrado, en

donde no es posible la adición de datos o la sobre escritura de los mismos. Los chips de solo lectura son generalmente más baratos pero tiene la limitante de que actúan como un número en una placa, casi como un código de barras.

### Una escritura/Muchas Lecturas (WORM – *Write Once Read Many*)

Un chip WORM permite a los usuarios agregar datos al chip más allá del identificador único, pero éstos sólo pueden ser agregados una vez. No hay límite en la cantidad de lecturas.

### Lectura/Escritura

Los chips de Lectura/Escritura están abiertos a la manipulación de datos sin restricciones para el usuario del sistema. Estos chips aún contienen un identificador único del fabricante, pero también portan una base de datos actualizable donde los datos pueden ser agregados al chip. Estos transponder son generalmente más caros que los de Sólo Lectura y los WORM debido a su versatilidad.

Adicionalmente las clasificaciones anteriores, los transponders pueden también ser diferenciados entre dos principios fundamentales de operación: portadores electrónicos de datos basados en circuitos integrados (microchips) y portadores de datos que aprovechan efectos físicos para el almacenamiento de de los datos. Tanto los transponders de 1 bit como los de onda de superficie corresponden a ésta última categoría. La figura III.10 muestra un esquema de los tipos de transponder dependiendo de su principio de operación.

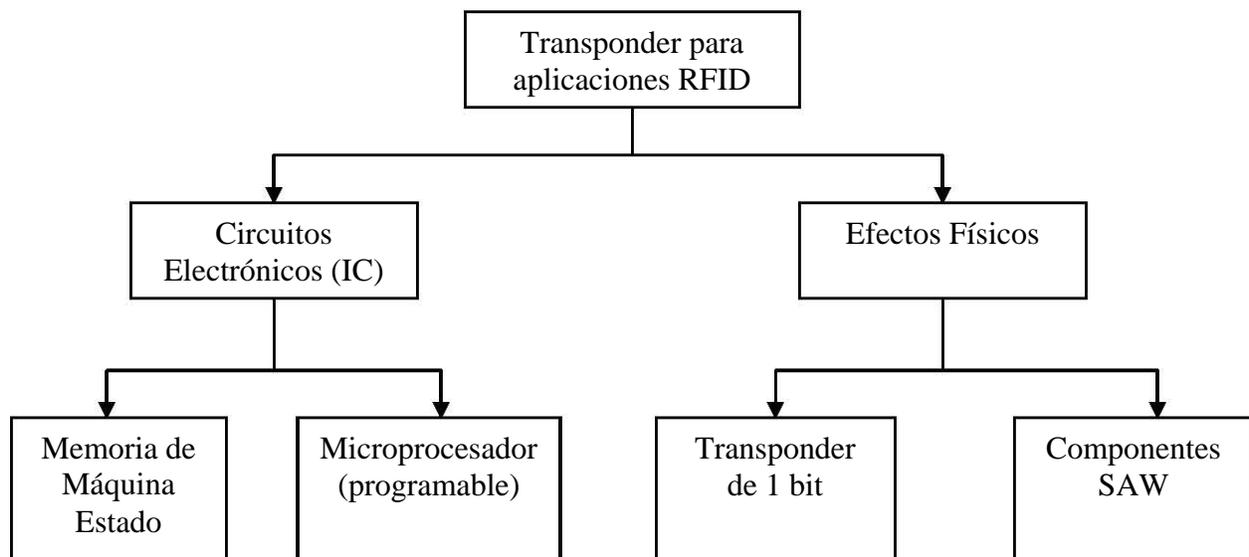


Figura III.10 Tipos de Transponder de acuerdo a su principio de operación.

### III.2.1 Transponder con Función de Memoria

Los transponder con función de memoria (de Sólo lectura, lectura/escritura o WORM) contienen una interfaz de alta frecuencia (HF) para proporcionar la fuente de poder y permitir la comunicación con el lector. La figura III.11 muestra un diagrama de bloques de un transponder RFID con función de memoria.

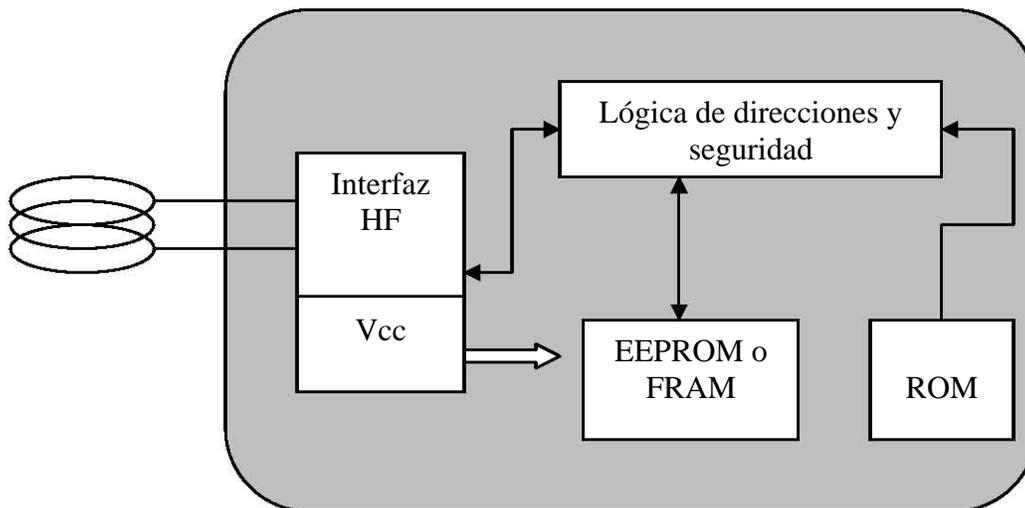


Figura III.11 Diagrama de bloques de un transponder con función de memoria

#### III.2.1.1 Interfaz HF

La interfaz HF forma el puente entre canal analógico de transmisión de alta frecuencia del lector y los circuitos digitales del transponder. Por lo tanto, el módulo HF ejecuta las funciones de un modem clásico (modulador – demodulador) utilizado para la transmisión de datos por vías telefónicas.

La señal modulada HF proveniente del lector es reconstruida en la interfaz HF por *demodulación* para crear un flujo de datos seriales que son procesados en la lógica de direcciones y seguridad. El reloj del sistema es generado por un circuito de generación de pulsos desde la frecuencia portadora del campo de HF y es utilizado por el portador de datos.

Para regresar información al lector, la interfaz de HF incorpora un modulador de carga o un modulador por reflexión (o un procedimiento alternativo, como por ejemplo un divisor de frecuencia), controlado por los datos digitales que son transmitidos. En la figura III.12 se muestra un diagrama de bloques con una interfaz HF para un transponder acoplado inductivamente con modulador de carga.

En este caso, siendo un transponder pasivo, la energía se obtiene desde el campo de HF del lector. Para lograr esto la interfaz HF obtiene una corriente de la antena del transponder que luego es rectificadora y proporcionada al chip como una fuente regulada de voltaje.

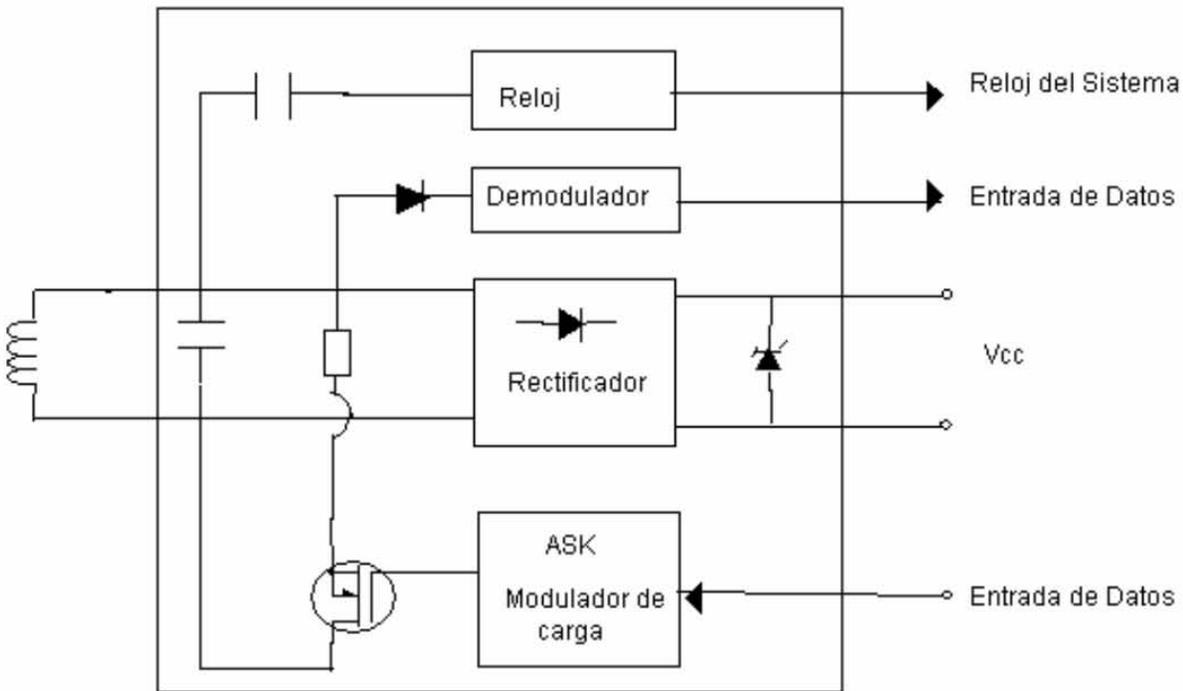


Figura III.12 Diagrama de bloques de una interfaz HF de un transponder acoplado inductivamente con modulación de carga.

### III.2.1.2 Lógica de Direcciones y Seguridad

La lógica de direcciones y seguridad forma el corazón del portador de datos y controla todos los procesos en el chip. En la figura III.13 se muestra un diagrama de bloques del módulo de direcciones y seguridad.

La lógica de encendido o *power on* se asegura que el transponder tome un estado definido tan pronto como recibe una fuente de poder adecuada a través del campo de HF de un lector. Registros especiales de entrada y salida (I/O) ejecutan el intercambio de datos con el lector. Opcionalmente, se puede insertar una unidad de encriptado si se requiere autenticar encriptar datos y administrar claves.

La memoria de datos, que comprende de una ROM para los datos permanentes como el número de serie, la EEPROM o FRAM, se conecta a la lógica de direcciones y seguridad a través del bus de datos y *address* dentro del chip.

El reloj del sistema requerido para control de secuencias y sincronización del sistema es obtenido del campo de alta frecuencia del lector a través de la interfaz de HF y proporcionado al módulo de la lógica de direcciones y seguridad.

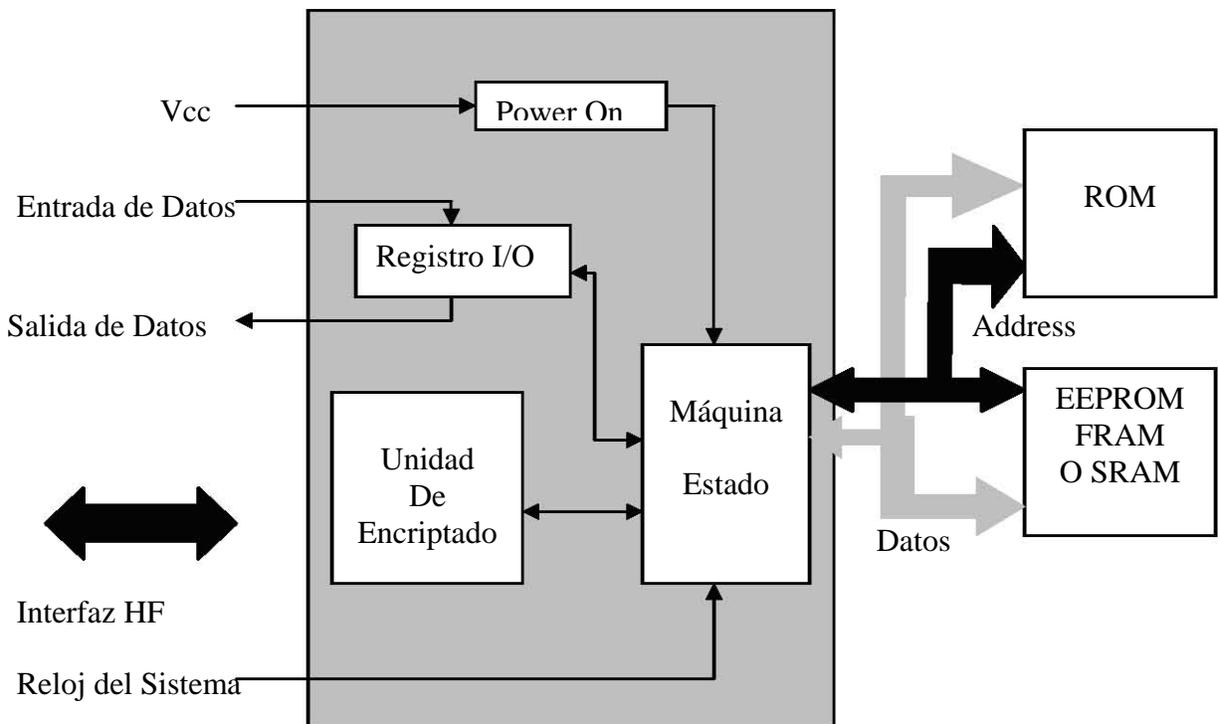


Figura III.13 Diagrama de bloques del modulo de seguridad y address.

### III.2.2. Transponder con Microprocesador

Los transponder con microprocesador se están haciendo cada vez más comunes en aplicaciones que utilizan las tarjetas inteligentes libre de contacto. En vez de una máquina estado inflexible, estas tarjetas incorporan un microprocesador.

Los microprocesadores estándar en la industria, tales como el 8051 o el 6805 son utilizados como el corazón del chip. Además algunos fabricantes ofrecen simples coprocesadores matemáticos (unidades de encriptado) en el mismo chip, lo cual permite una ejecución rápida de los cálculos requeridos para el proceso de encriptado (figura III.14).

Las tarjetas inteligentes libres de contacto con microprocesadores incorporan su propio sistema operativo, como ha sido el caso en las tarjetas de contacto. Las tareas del sistema operativo consisten en la transferencia de datos desde y hacia la tarjeta inteligente, controlar la secuencia de comandos, manejo de archivos y la ejecución de los algoritmos de encriptado.

Los módulos de programa están escritos en la ROM y son incorporados en el chip en el momento de su fabricación.

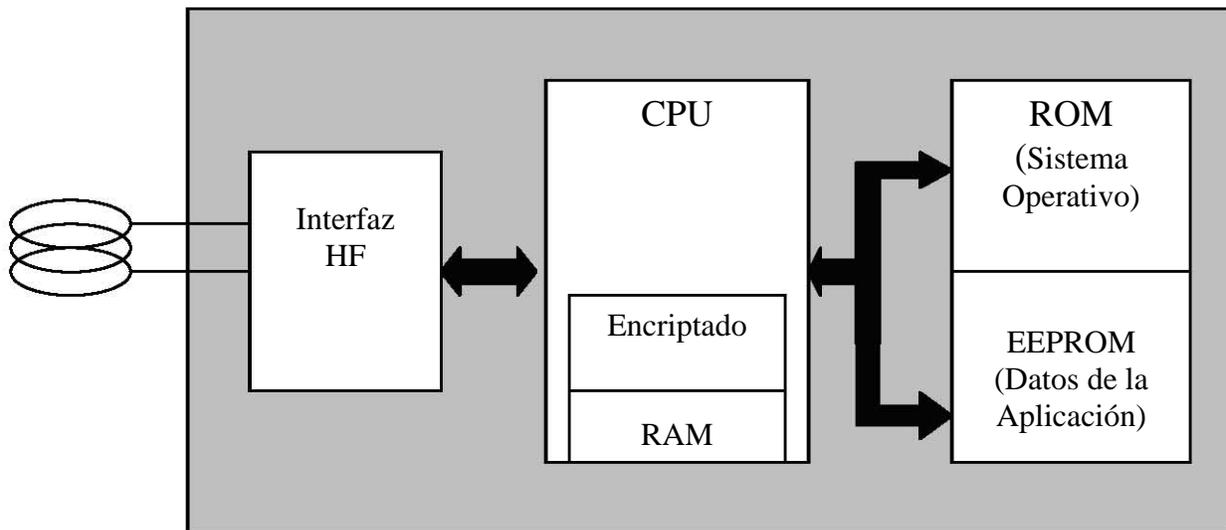


Figura III.14 Diagrama de bloques de un transponder con un microprocesador.

La secuencia de procesamiento de comandos típica de un sistema operativo de una tarjeta inteligente es como sigue: los comandos enviados desde el lector a la tarjeta libre de contacto son recibidos a través de la interfaz HF. Independientemente de los procedimientos de más alto nivel, el manejador de entradas/salidas (I/O) ejecuta mecanismos de reconocimiento y corrección de errores. Los comandos libres de error recibidos por el manejador son descifrados o verificada su integridad. Después de la descifración el interpretador de comandos de más alto nivel intenta decodificar el comando. Si esto no es posible, entonces se llama al manejador de regreso de códigos, el cual genera el código apropiado y lo envía de regreso al lector a través del manejador I/O.

Si se recibe un comando válido entonces se ejecuta el código de programa real asociado con este comando de la aplicación. Si es necesario el acceso a los datos de la aplicación en la EEPROM, esto se realiza exclusivamente por el sistema de manejo de archivos y el manejador de memoria, que convierte todas las direcciones simbólicas en las correspondientes direcciones físicas del área de memoria. El manejador de archivos también verifica las condiciones de acceso (autorización) para los datos en cuestión.

### **III.2.3. Tecnología de Memoria**

Después de la máquina estado y del microprocesador, el componente más importante del transponder es la memoria en la que se leen o se escriben los datos del usuario.

En el caso de los transponder de solo lectura, los datos se encuentran grabados desde el proceso de fabricación, ya sea a través de una máscara de exposición o a través de Laser.

En el caso de que sea necesario escribir datos en el transponder, entonces se incorporan celdas RAM, EEPROM o FRAM en el chip. Sin embargo, solamente las celdas EEPROM y FRAM pueden almacenar los datos escritos por períodos largos (típicamente períodos de retención mayores a 10 años) sin una fuente de poder.

#### **III.2.3.1 RAM**

La RAM es una memoria que puede ser utilizada para el almacenamiento temporal de datos ya que cuando se le quita la fuente de poder se pierden los datos almacenados. En los transponders, la RAM es usada principalmente para almacenar temporalmente datos que existen brevemente durante la operación en la zona de interrogación del lector. Los transponder activos tienen su propia batería, lo que se usa en ocasiones para almacenar datos en la RAM por un mayor período de tiempo.

### III.2.3.2.EEPROM

El principio de operación de una celda EEPROM está basado en la habilidad de los capacitores de almacenar cargas por períodos de tiempo largos. Una EEPROM por lo tanto representa a un pequeño capacitor que puede ser cargado o descargado. Un capacitor cargado representa un “1” lógico y un capacitor descargado representa un “0” lógico.

En su forma más simple, una celda EEPROM consiste básicamente de un transistor de efecto de campo (FET) modificado en un substrato hecho de silicón. La celda EEPROM contiene una compuerta adicional entre la compuerta de control del FET y el substrato, que no está conectada a una fuente de energía externa y que está posicionada a una muy corta distancia (~ 10 nm) del substrato. Esta *compuerta flotante* puede ser cargada o descargada a través del substrato utilizando el efecto túnel, representado por lo tanto un capacitor.

Para escribir un “0” o un “1” en una celda EEPROM se aplica un alto voltaje negativo o positivo a la compuerta de control, lo que activa el efecto túnel. El voltaje requerido para cargar la celda es de aproximadamente 17 V en la compuerta de control el cual cae a 12 V en la compuerta flotante. Dado que a los transponder RFID se les proporciona un voltaje entre 3 V y 5 V de una interfaz de HF ( o una batería), se genera un voltaje de 25 V del bajo voltaje utilizando una bomba de carga en cascada integrada al chip, quedando en los 17 V después de la estabilización.

### III.2.3.3. FRAM

El principio subyacente de las celdas FRAM es el efecto ferroeléctrico, que consiste en la capacidad de un material de retener la polarización eléctrica aún en la ausencia de un campo eléctrico. Esta polarización está basada en el alineamiento de dipolo elemental dentro de un cristal en el material ferroeléctrico debido al efecto de un campo eléctrico que es mayor que la fuerza coercitiva del material. Un campo eléctrico opuesto causa el alineamiento opuesto del dipolo interno. El alineamiento de los dipolos por lo tanto cae en uno de dos posibles estados que son retenidos después de que es quitada la influencia del campo eléctrico.

A diferencia de las celdas EEPROM, la operación de escritura en las celdas FRAM ocurre a una muy alta velocidad. Los tiempo típicos de escritura caen en el orden de 0.1  $\mu$ s. Por lo que las memoras FRAM pueden ser grabadas en tiempo real en el tiempo del ciclo de escritura de un microprocesador.

Las FRAM son también superiores a las EEPROM en términos de su consumo de energía, por lo que son ideales para los sistemas RFID. Sin embargo los problemas de combinar procesadores CMOS y circuitos analógicos (Interfaz HF) con las celdas FRAM en un chip único, hacen que la difusión de ésta tecnología de memoria avance lentamente.

Actualmente, derivado de la necesidad de que las etiquetas puedan ser leídas por diferentes lectores independientemente del fabricante, se ha creado los diferentes tipos de etiquetas de acuerdo a la organización EPC Global, (*EPC – Electronic Product Code*). El estándar EPC incluye también la distribución de la información en el transponder con el propósito de identificar un código universal de producto para su aplicación en sistemas de punto de venta en supermercados y tiendas al menudeo.

Las principales características de las clasificaciones EPC para los transponders son:

- EPC Clase 0 : Etiqueta de sólo lectura.
- EPC Clase 1: Etiqueta de una Escritura / Muchas Lecturas.
- EPC Clase 2: Etiqueta de múltiples Lecturas y Escrituras.

El estándar EPC para los transponder maneja diferentes frecuencias que son:

- EPC clase 0 a 900 MHz.
- EPC clase 1 a 13.56 MHz.
- EPC clase 1 de 860 a 930 MHz.

Los requerimientos a los proveedores de las cadena de distribución más grandes en Estados Unidos (por ejemplo Walmart o el Departamento de Defensa), incluyen transponder que cumplen con las normas de EPC Global.

# **Análisis de los Componentes de Hardware Utilizados en el Sistema**

IV.1 Requerimientos y Definición del Sistema

IV.2 Transponder

IV.3 Lector

IV.4 Dispositivo Handheld

IV.5 Fuente de Poder

## **Capítulo 4**

## ANÁLISIS DE LOS COMPONENTES DE HARDWARE UTILIZADOS EN EL SISTEMA

### IV.1 Requerimientos y definición del sistema

El objetivo del presente proyecto es desarrollar un dispositivo que utilice la tecnología de RFID (Identificación por Radiofrecuencia) para realizar inventarios en el Laboratorio de Microsoft de la Facultad de Ingeniería. Este dispositivo debe ser capaz de:

- Realizar el inventario de manera rápida sin que exista necesariamente línea de vista entre el dispositivo y los bienes.
- Leer y escribir en las tarjetas de RFID utilizadas para identificar los bienes.
- Portátil.
- Localizar un bien en particular, indicándolo mediante una alarma audible y/o visual.

La característica principal del dispositivo es la de su portabilidad, ya que esto nos permitirá realizar el inventario simplemente con colocarlo cerca del bien a inventariar. Por lo tanto, la distancia para la realización de la actividad debe estar comprendida entre 0.5 y 1.5 m. Los sistemas que cumplen con ésta característica de lectura son de alcance medio y de alcance largo.

En la realidad, el rango de lectura se ve afectado por múltiples variables, incluyendo el nivel de potencia del lector, la eficiencia de la antena, la frecuencia del transponder, el tamaño y la orientación relativa de los dispositivos, el ambiente eléctrico y el ruido magnético presente así como la proximidad de varios materiales (tales como el metal), sólo por nombrar algunos.

Las hojas de especificaciones de los fabricantes tienden a ser optimistas al predecir la funcionalidad de sus dispositivos. Sin embargo, ante la imposibilidad de probar todos los dispositivos para determinar el rango de lectura ideal, se han obtenido algunas pruebas realizadas por algunos distribuidores que nos indican el comportamiento general para algunas frecuencias.

En la tabla IV.1 se muestran los resultados de pruebas realizadas en laboratorio para de rangos de lectura de un sistemas de LF.

En este caso, podemos observar que los resultados son de un mayor alcance, tanto de lectura como de escritura, cuando el tamaño de la antena es mayor. Aquí entre las condiciones de lectura y escritura para realizar las pruebas se encuentran que se contaba con línea de vista y sin materiales que pudieran cancelar o disminuir la señal del lector.

Es claro que en las consideraciones del presente proyecto se deben considerar que las condiciones ideales de funcionamiento no estarán presentes nunca, ya que dentro del

Laboratorio de Microsoft existen bienes y componentes de múltiples materiales, tales como el metal, por lo que es de esperar que la señal tenga disminuciones y cancelaciones dependiendo de los factores mencionados.

| Transponder                                     | Antenna Type           |                        |                        |                        |
|---|------------------------|------------------------|------------------------|------------------------|
|   | Stick<br>(In Kit)      | Sm. Gate               | Med. Gate              | Lg. Gate               |
| <u>12mm Wedge R/O</u>                           | Read: 6"               | Read: 11"              | Read: 9"               | Read: 5"               |
| <u>23mm Glass R/W</u>                           | Read: 9"<br>Write 8"   | Read: 15"<br>Write 13" | Read: 12"<br>Write 11" | Read: 12"<br>Write 11" |
| <u>32mm Glass R/W</u>                           | Read: 11"<br>Write 10" | Read: 12"<br>Write 11" | Read: 20"<br>Write 17" | Read: 21"<br>Write 18" |
| <u>30mm Disk R/O</u>                            | Read: 18"              | Read: 23"              | Read: 17"              | Read: 17"              |
| <u>Keyring R/O</u>                              | Read: 11"              | Read: 16"              | Read: 17"              | Read: 16"              |
| <u>Credit Card R/O</u>                          | Read: 21"              | Read: 21"              | Read: 30"              | Read: 27"              |
| <u>85mm Large Disk R/W</u>                      | Read: 32"<br>Write 23" | Read: 27"<br>Write 26" | Read: 40"<br>Write 37" | Read: 45"<br>Write 44" |
| <u>120mm Cylinder R/W-MPT</u>                   | Read: 28"<br>Write 18" | Read: 40"<br>Write 30" | Read: 42"<br>Write 38" | Read: 47"<br>Write 44" |
| <u>Mount on Metal R/W</u><br><u>NOT MOUNTED</u> | Read: 19"<br>Write 18" | Read: 19"<br>Write 18" | Read: 25"<br>Write 22" | Read: 26"<br>Write 23" |

Tabla IV.1 Rangos de Lectura para el Lector S-2000 de Texas Instruments operando a una frecuencia de 134 kHz. (Fuente: Dynasys Technologies, Inc)

Las dimensiones de las 3 antenas mas grandes utilizadas para las pruebas son de 40" x 20.5" x 1" para la antena larga (Lg. Gate), de 28" x 11" x 1" para la antena mediana (Med. Gate) y de 8" x 8" x 1" para la antena pequeña (Sm. Gate).

Como es evidente, las dimensiones de las tres antenas son muy grandes para cubrir la característica de portabilidad, por lo que se descartan como posible solución para el presente proyecto.

En el caso de la antena tipo Stick, sus dimensiones si son adecuadas pero el alcance logrado en ningún caso llega a 1.5 m. A esto se le suma el hecho de que es de esperar una disminución en la señal en su utilización en campo, hacen que la utilización de lectores de baja frecuencia no sea adecuada para el presente proyecto.

En la tabla IV.2 se muestra los resultados realizados con un lector que opera a 13.56 MHz.

| Transponder                                       | Antenna Type                     |                                  |   |
|---|----------------------------------|----------------------------------|---|
|   | <u>Dynasys</u><br><u>20"x63"</u> | <u>Dynasys</u><br><u>20"x20"</u> | <u>TI Small Gate</u> 13.25"<br>x 12.67" |
| <u>Large Rectangle</u><br><u>(45x76mm) Inlay</u>  | Read: 23"                        | Read: 20"                        | Read: 12"                               |
| <u>Square (45x45mm) Inlay</u>                     | Read: 20"                        | Read: 16"                        | Read: 12"                               |
| <u>Mini Rectangle</u><br><u>(22.5x38mm) Inlay</u> | Read: 19"                        | Read: 15"                        | Read: 12"                               |

Tabla IV.2 Rangos de Lectura para el Lector S-6520 de Texas Instruments operando a una frecuencia de 13.56 MHz. ( Dynasys Technologies, Inc)

Las dimensiones de las antenas son también muy grandes para su propósito de uso. Además podemos observar que los rangos de lectura alcanzados son muy cortos y no cumplen con los requerimientos del rango de lectura.

La mayoría de los fabricantes de sistemas RFID concuerdan en asignar un mayor rango de lectura a sus dispositivos que operan en la frecuencia UHF en comparación con los de HF y LF<sup>1</sup>, de hasta varios metros de alcance. Es por esto que se considera para el presente proyecto que la frecuencia de operación adecuada deberá estar en el rango UHF.

Los dispositivos UHF que están disponibles en el Mercado hasta hoy operan en la banda de 860 – 960 MHz. En los Estados Unidos se especifica una frecuencia de 915 MHz mientras que en la Unión Europea se ha especificado una frecuencia de 868 MHz. Algunos de los fabricantes más importantes se localizan en Estados Unidos, por lo que han enfocado su producción en el rango de frecuencia de 915 MHz, por lo que resultan mejor, tanto en precio como en disponibilidad el basar el presente proyecto en ésta frecuencia.

Por otro lado y siguiendo con los requerimientos de portabilidad del sistema es necesario el tener un dispositivo de interfaz con el usuario que sea amigable y con las dimensiones adecuadas para permitir un manejo sencillo de las diferentes funcionalidades del sistema. De igual forma se requiere que dicha interfaz sea capaz de comunicarse con otros tipos de sistemas ya sea a través de *bluetooth*, comunicación infrarroja y/o a través de un cable de comunicación.

Los dispositivos que cumplen con todas éstas características son los llamados PDA, ya que la mayoría incluyen todas las formas de comunicación mencionadas además de que por su tamaño son ideales para formar parte de un sistema portátil.

<sup>1</sup> [http://www.tagsys.net/eng/rfid/tagsys/rfid\\_tag-3-2.html](http://www.tagsys.net/eng/rfid/tagsys/rfid_tag-3-2.html)

El uso de PDA o su variante de Pocket PC permite también el desarrollo de diferentes aplicaciones en entornos ya conocidos, tales como Java en su versión J2ME o .Net Compact Framework para dispositivos de recursos limitados. Estas aplicaciones podrían agregar mayor funcionalidad al dispositivo, dependiendo de las necesidades que surjan en el futuro.

## IV.2 Transponder

Como se ha mencionado anteriormente, la clasificación más importante de los transponders es la que los divide en pasivos y en activos. Los transponder activos, al incorporar una batería reducen considerablemente su tiempo de vida, llegando a ser típicamente de 5 años, lo cual representa un serio inconveniente en aplicaciones donde se requiere un tiempo de vida muy largo, tales como el control de inventarios de activo fijo, como es el caso nuestro, en donde los bienes pueden permanecer en el área 10 años o más.

Un inconveniente adicional de las etiquetas activas es su costo. La incorporación de la batería agrega costos adicionales, en la mayoría de los casos mayores al 100 % en comparación con los transponder pasivos.

Los transponder pasivos en teoría tiene un tiempo de vida infinito. Pero el proceso de oxidación de los componentes limita su tiempo de vida útil, aunque frecuentemente es superior a los 10 años.

El costo menor de éstos transponders los hace mucho mejores, especialmente cuando se manejan una gran cantidad de productos a identificar. Por ésta razón se eligió un transponder pasivo como el portador de información en el sistema.

Los formatos de construcción de los transponder varían desde discos o monedas hasta encapsulados de vidrio o plástico, pasando por formatos tipo llave, reloj, encapsulado de metal y etiquetas adhesivas.

Este último formato es el más adecuado debido a que presenta la flexibilidad de adherirse a las diferentes superficies de los productos a identificar, además en la mayoría de los casos el costo es mucho menor.

Actualmente existen una gran cantidad de fabricantes transponders en todo el mundo Alien Technology, Symbol Technologies y Texas Instruments.

La figura IV.1 muestra la etiqueta UHF modelo ALL-9238 del fabricante Alien Technology. Entre sus características principales se encuentran que es tipo EPC clase 1 y su tamaño es de 10 x 95 mm. La capacidad de memoria es de 96 bits, 64 de los cuales son programables por el usuario. Su Frecuencia de operación es de 915 MHz

y cuenta con fuerte adhesivo que la hace ideal para colocarlo diferentes superficies y además es de bajo costo.



*Figura IV.1 Etiqueta Alien Technology modelo ALL-9238*

La figura IV.2 muestra la etiqueta de Alien Technology modelo ALL-9250, que opera a la frecuencia de 915 MHz. Es EPC clase 1 y su tipo de memoria es WORM (Write Once Read Many) con una capacidad de 96 bits, de los cuales solo 64 son programables por el usuario. Las dimensiones son de 13 x 134 mm y es muy sensible a la orientación por lo que se su lectura mejora notablemente cuando está alineada de la manera adecuada.



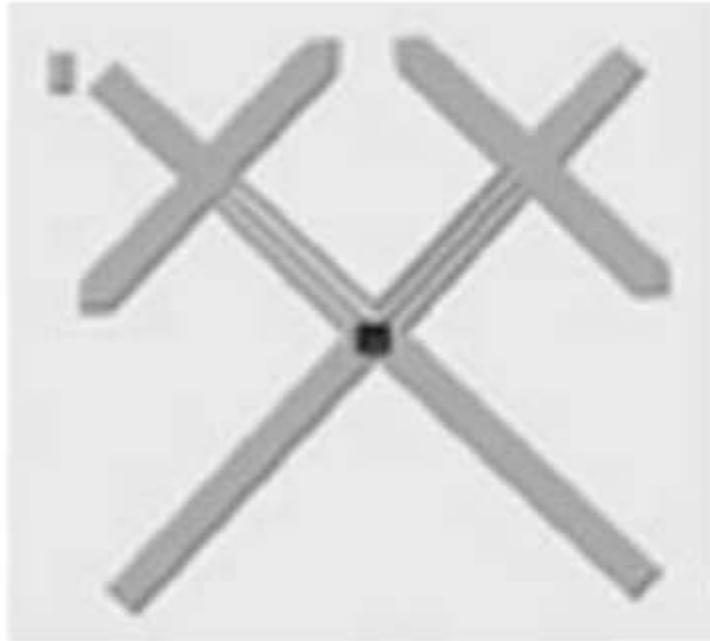
*Figura IV.2 Etiqueta Alien Technology modelo ALL-9250*

La figura IV.3 muestra la etiqueta UHF de Alien Technology modelo ALL-9254 es de un tamaño aproximado de 95 x 30 mm. Es de tipo EPC clase 1 y opera a una frecuencia de 915 MHz. La capacidad de memoria (de tipo WORM) es de 96 bits, de los cuales 64 son programables por el usuario. Tiene un factor de ganancia mejorado que permite una mayor distancia de lectura.



*Figura IV.3 Etiqueta de Alien Technology modelo ALL-9254*

La figura IV.4 muestra la etiqueta modelo MAT-4X4 de Symbol Technologies, a través de su división MATRICS, que opera a 915 MHz y sus dimensiones son de 101 x 101 mm. Su memoria es de solo lectura y tiene una capacidad de 80 bits. Es muy rápida pero trabaja solamente con el lector de Symbol.



*Figura IV.4 Etiqueta de Symbol Technologies modelo MAT-4X4*

Texas Instruments liberará próximamente dos transponders UHF EPC generación II. Actualmente su enfoque ha estado en el rango de LF y HF principalmente.

Basado en la información mostrada de las etiquetas, podemos observar que la mejor opción para el proyecto es la etiqueta de Alien Technology modelo ALL-9238 por sus características de tamaño y bajo costo.

### IV.3 Lector

Los requerimientos de portabilidad del dispositivo restringen el tamaño de todos los componentes, entre ellos el del lector. Éste deberá operar en la frecuencia de UHF a 915 MHz y sus dimensiones y requerimientos de energía deberán ser lo mas pequeños posibles.

Entre los fabricantes principales de lectores se encuentra Sirit Inc, Intermec, Skyetec Inc , Alien Technology y Symbol Technologies.

En las opciones investigadas se encontró que los lectores de Sirit, Alien Technology y de Skyetek son de dimensiones más pequeñas que los hace adecuados para dispositivos portátiles.

La figura IV. 5 muestra el lector de Alien Technology modelo ALR-9640 tipo EPC Clase 1 con antena integrada, para aplicaciones que involucran hasta 20 transponders al mismo tiempo. Este dispositivo está diseñado para integrarse fácilmente con dispositivos externos, sensores o indicadores y opera autónomamente sin la necesidad de realizar un *polling* continuo. El lector opera en la banda de 915 MHz.

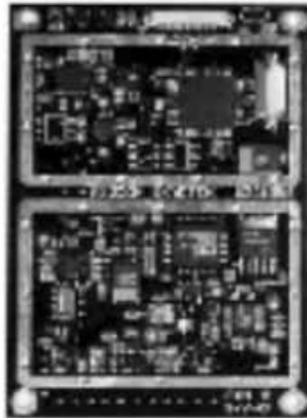
El costo de éste lector es relativamente alto en comparación con otros lectores de características similares. En contraste, es uno de los más pequeños en el mercado y de los más fácil integración.

La figura IV.6 muestra el lector SkyeModule M8, que consiste básicamente de las tarjetas electrónicas sin cubiertas protectoras o de blindaje. El módulo permite operar con transponder EPC clase 0 y 1 y además mediante la actualización del firmware con transponder EPC generación II. La antena es externa y se maneja de manera separada dependiendo de la frecuencia final de operación (865-875 MHz en Europa) 50-956 MHz en Japón y 902-928 MHz en Estado Unidos).

El alcance es de hasta 3 m con la antena externa y tiene un sistema de comunicaciones multiprotocolo para adaptarse al tipo de transponder con el que opera.



*Figura IV.5 Lector de Alien Technology modelo ALR-9640*



*Figura IV.6 Lector de Skyetek Inc modelo Skyemodule M8*

La figura IV.7 muestra el lector de Sirit Inc, modelo Sirit ST200 que opera en la banda de 902 a 928 MHz. Este lector soporta operaciones con transponder EPC clase 0, clase1 y con una actualización del firmware EPC Generación II.

Cuenta con una antena integrada de polarización horizontal o se puede conectar a una antena externa que tenga una impedancia de 50 ohm. Además, el firmware se puede actualizar por medio de una interfaz serial en caso de que se requieran aplicaciones diferentes el futuro.



*Figura IV.7 Lector de Sirit Inc, modelo ST200*

El lector tiene la facilidad de que su potencia de salida es ajustable vía software, lo que es ideal para operaciones de escritura en donde puede haber otros transponder cercanos, ya que de ésta manera se puede bajar la potencia de salida en el momento de la escritura para que sea necesario que el transponder a grabar esté lo más cercano posible.

La tabla IV.3 muestra las especificaciones del Lector Sirit ST200.

| <b>CARACTERÍSTICAS DE FUNCIONAMIENTO</b>   |  |
|--|--|
| Frecuencia   | Banda UHF 902 -928 MHz   |
| Transponder Soportados   | EPC Global Clase 0, EPCGlobal Clase 1<br>Opcional EPCGlobal Generación II    |
| Protocolo de Comunicaciones  | Serial con CCITT CRC-16 bit detección de error                               |
| Parámetros de Comunicación   | 115,200 bps, 8 bits de datos, sin paridad, 1 bit de paro.                    |
| Nivel de comunicaciones de la Señal  | Nivel TTL  |
| Conector de la Interfaz  | 10 pines   |
| Tipo de Antena   | Antena Interna de parche Integrada<br>Opcionalmente Antena externa de 50 ohm |
| Firmware actualizable  | Si   |
| <b>CARACTERÍSTICAS FISICAS</b>   |  |
| Dimensiones (Largo x Ancho x Profundidad)  | 97.8 x 67.3 x 26.9 mm  |
| Peso   | Con Antena Integrada 147 g<br>Sin Antena Integrada 77 g                      |
| <b>MEDIO AMBIENTE</b>  |  |
| Temperatura de Operación   | -20 °C a +70 °C  |
| Temperatura de Almacenamiento  | -40 °C a +100 °C   |
| Humedad Relativa   | 80 % Sin condensar   |
| Energía<br>Voltaje de Entrada<br>Corriente Activa<br>Corriente en Standby<br>Variación | +5VDC ±5%<br>1.5 A pico<br>160 mA, nominal<br><1 mA                          |
| Potencia de Salida RF  | 1 W (30 dBm)   |
| Regulaciones   | Cumplimiento de FCC parte 15   |

Tabla IV.3 Especificaciones del SIRIT ST200

La combinación de bajo costo, dimensiones pequeñas y flexibilidad hacen a éste lector al más apropiado para la realización del proyecto.

#### **IV.4 Dispositivo Handheld**

La interfaz con el usuario exige un entorno amigable y un dispositivo que además pueda comunicarse con otros sistemas de cómputo para analizar la información obtenida por la realización del inventario. Los dispositivos que cumplen con éstas características son los llamados PDA (*Personal Digital Assistant* – Asistente Digital Personal), que en realidad son equipos multifuncionales que cuentan con varias formas de enlace al exterior, entre los que se encuentran puertos infrarrojos, bluetooth o el estándar IEEE 802.11b.

Existen una gran variedad de PDA's en el mercado, entre los que destacan las Pocket PC que es muy similar a un equipo de cómputo de escritorio pero con recursos muy limitados (dimensiones, memoria, procesador, etc). Las siguientes son algunos PDA disponibles actualmente con sus características principales:

##### **HP iPaq H4350.**

La figura IV.8 muestra la iPaq H4350. Esta Pocket PC viene con 64 MB de RAM y tiene un procesador de INTEL de 400 MHz Xscale. Está habilitado con conexión WiFi que le permite conectarse a internet. LA vida de la batería es de 6 a 5 horas reproduciendo videos con una simple carga. El sistema operativo es Microsoft Pocket PC 2003. Una desventaja es su costo que es relativamente alto.



*Figura IV.8 Pocket PC iPAq modelo H4350.*

##### **Garmin iQue 3600**

La figura IV.9 muestra el PDA Garmin iQue 3600. Su principal característica es que cuenta con un sistema GPS incorporado. Tiene un procesador de 200 MHz y su

sistema operativo es Palm OS 5.2.1. Su batería es de baja duración, de aproximadamente 3 horas y 45 minutos.



*Figura IV.9 PDA Garmin iQue 3600*

### **Toshiba Pocket PC e750**

La figura IV.10 muestra la Toshiba Pocket PC e750. Este PDA tiene un procesador de 400 MHz y 64 MB de RAM así como 32 MB de ROM. Cuenta con el sistema operativo Microsoft Pocket PC. Está equipada con una tarjeta WiFi y su batería tiene una duración aproximada de 3 horas y 55 minutos, tocando archivos de MP3 constantemente. También cuenta con puerto IrDA y Bluetooth.

Una de las características notables es su bajo peso de aproximadamente 6.9 oz.



*Figura IV.10 Toshiba Pocket PC e750*

### **Palm Tungsten E**

La figura IV.11 muestra el PDA Palm Tungsten E. Este cuenta con un procesador de Texas Instruments de 126 MHz OMAP 311 ARM y 32 MB de memoria interna. Tiene el sistema operativo Palm OS 5.2 y su batería tiene una duración de aproximadamente 3 horas y 30 minutos.

### **Sony Clie PEG-TJ25**

La figura IV.12 muestra la Sony Clie PEG-TJ25. Este PDA cuenta con procesador de 200 MHz y tiene un sistema operativo de Palm OS 5.2. La pantalla tiene una resolución de 320 x 320 pixeles y cuenta con el sistema de almacenamiento de Sony llamado Memory Stick.



Figura IV.11 PDA Palm Tungsten E



Figura IV.12 Sony Clie PEG-TJ25

Dado que existen una gran variedad de PDA la tabla IV.4 muestra un resumen de algunos dispositivos con sus características principales.

| <b>Modelo</b>          | <b>Sistema Operativo</b>                 | <b>RAM Instalada</b> | <b>Procesador</b>                 | <b>Ranura de Expansión</b>                   | <b>Vida de la Batería</b> |
|------------------------|--|----------------------|-----------------------------------|--|---------------------------|
| HP iPaq H5550          | Microsoft Windows Mobile 2003            | 128MB SDRAM          | Intel 400MHz                      | 1 SD Tarjeta de memoria                      | 6 Horas, 5 minutos        |
| HP iPaq rx3100         | Microsoft Windows Mobile 2003            | 56 MB                | Samsung 400 MHz                   | 1 SD Tarjeta de memoria                      | 4 horas 30 minutos        |
| Garmin iQue 3600       | Palm OS 5.0                              | 32MB                 | Motorola 150MHZ                   | 1 SD Tarjeta de memoria                      | 3 Horas, 45 minutos       |
| Toshiba Pocket PC e335 | Microsoft Pocket PC 2002                 | 64MB SDRAM           | Intel PXA250 300MHz               | 1 SD Tarjeta de memoria                      | 4 Horas, 16 minutos       |
| Toshiba Pocket PC e750 | Microsoft Windows Mobile 2003            | 64MB SDRAM           | Intel PXA255 400MHz               | 1 SD Tarjeta de memoria, 1 CompactFlash card | 3 Horas, 55 minutos       |
| Palm Tungsten E        | Palm OS 5.2                              | 32MB                 | 126MHz Texas Instruments OMAP 311 | 1 SD Tarjeta de memoria                      | 3 Horas, 30 minutos       |
| Dell Axim X5           | Microsoft Pocket PC 2002 Premium Edition | 64MB SDRAM           | Intel PXA250 400MHz               | 1 SD Tarjeta de memoria, 1 CompactFlash card | 6 Horas, 22 minutos       |
| Toshiba Pocket PC e350 | Microsoft Windows Mobile 2003            | 64MB SDRAM           | Intel PXA255 300 MHz              | 1 SD Tarjeta de memoria                      | 3 Horas, 51 minutos       |
| Sharp Zaurus SL-5600   | Trolltech Qtopia                         | 32MB SDRAM           | Intel PXA250 400MHz               | 1 SD Tarjeta de memoria, 1 CompactFlash card | 4 Horas, 10 minutos       |
| Sony Clie PEG-TJ25     | Palm OS 5.2                              | 32MB                 | 200MHz                            | Memory Stick                                 | No disponible             |
| Palm m125              | Palm OS 4.0.1                            | 8MB                  | Motorola MC68VZ328 33MHz          | ninguno                                      | No disponible             |

*Tabla IV.4 Resumen de las características principales de algunos PDA.*

El software del presente proyecto debe trabajar en cualquier PDA para permitir actualizaciones de hardware en el futuro. Nuestra mejor opción basados en el precio y en la plataforma del dispositivo es el Pocket PC iPaq 3100, que cuenta con puertos

IrDA, bluetooth, WiFi y un puerto USB que en conjunto nos proporciona una conectividad adecuada para los requerimientos.

#### **IV.5 Fuente de Poder**

La característica principal de los requerimientos de energía nos la proporciona el Lector debido a su alto consumo (1.5 A pico de acuerdo a las especificaciones del SIRIT ST200). Dado que el dispositivo es portátil es necesario que éste puede trabajar en ocasiones sin estar conectado a fuentes de energía eléctrica externas, de aquí la necesidad también de encontrar una batería con las características suficientes.

Entre las baterías recargables investigadas se encuentran las siguientes:

##### **Alcalinas**

Estas no son muy comunes en el mercado y requieren un cargador también poco común. Su voltaje puede llegar a ser de 1.5 Volts.

##### **Níquel-Cadmio (Ni-Cd)**

Este tipo de baterías son muy habituales. Contienen cadmio, un metal pesado que representa un peligro ecológico. Interiormente tienen dos electrodos, el de cadmio (negativo) y el de hidróxido de níquel (positivo), separados entre sí por un electrolito de hidróxido de potasa. Llevan también un separador situado entre el electrodo positivo y la envoltura exterior y un aislante que las cierra herméticamente. Su aspecto más positivo es el precio.

Lo peor es el llamado “efecto memoria”. Significa que antes de recargarlas es necesario haberlas agotado completamente ya que en caso contrario su vida se va acortando. Además son contaminantes.

##### **Níquel-Metalhidruro (Ni-MH)**

Además de ser menos contaminantes proporcionan voltajes de 1.3 volts y tienen una capacidad mucho mayor (1.000, 1.200, 1.300 mAh, las del tipo AA o R6, y hasta 700 mAh las del tipo AAA, que son las más pequeñas), por lo tanto duran más que las de Níquel-Cadmio y dan más energía. No tienen efecto memoria, de modo que se pueden recargar aunque no se hayan agotado al completo. Las mejores llegan a soportar hasta 1.000 procesos de carga.

En contra tienen que su costo es elevado, pero si se va a hacer un uso muy frecuente del equipo, por ejemplo en utilidades profesionales o en circunstancias en que se precisa una mayor duración, son las más indicadas y terminan por amortizarse pronto.

##### **Iones de litio (Li-ión)**

Utilizan un electrodo de óxido de níquel y otro de cobalto, intercalándose entre ellos el litio. Surgieron para paliar los problemas que causaba la reactividad del litio en los acumuladores de litio-dióxido de manganeso.

Este tipo de baterías, a pesar de ser costosas presentan la mejor opción en cuanto a capacidad y duración, por lo que es la más apropiada para los fines del presente proyecto.

Las baterías se caracterizan por perfiles que incluyen seguridad y eficiencia en el tiempo de carga. El método óptimo de carga depende de la química (Li-Ion, NIMH, NiCD, etc.), sin embargo la mayoría de las estrategias de carga implantan un esquema de tres etapas.

1. Etapa de acondicionamiento de baja corriente.
2. Etapa de corriente constante.
3. Etapa de voltaje constante y terminación de carga.

Durante la etapa final de la carga de la batería, lo cual generalmente toma el mayor tiempo del proceso de carga, se deben verificar ya sea la corriente o el voltaje o una combinación de ambas para determinar cuando se ha completado la carga.

Durante el proceso de carga, parte de la energía eléctrica es convertida en energía térmica hasta que la batería alcanza la carga completa. A partir de entonces toda la energía eléctrica es convertida en energía térmica. Si no se termina el proceso de carga, se puede dañar o destruir la batería. Los cargadores rápidos ( aquellos que pueden cargar la batería en menos de 2 horas) incluyen éste problema ya que utilizan una corriente de carga alta para minimizar el tiempo de carga. Por lo tanto verificar constantemente la temperatura es crítico ya que especialmente las baterías de Iones de Litio pueden explotar si se sobrecargan. En estos casos la temperatura es verificada durante todas las fases y el proceso de carga se termina inmediatamente si la temperatura excede un límite máximo establecido.

La figura IV.13 muestra un esquema de la fuente de poder que incluye un dispositivo que nos proporcionará un voltaje de 5V y un circuito cargador de la batería. En este caso se utiliza un eliminador de baterías con la capacidad de corriente adecuada para proporcionar la energía para el cargador de baterías y el funcionamiento del sistema. Esto nos proporciona la ventaja de que el dispositivo pueda funcionar conectado tanto a la corriente eléctrica externa como con baterías para situaciones o lugares donde no esté disponible.

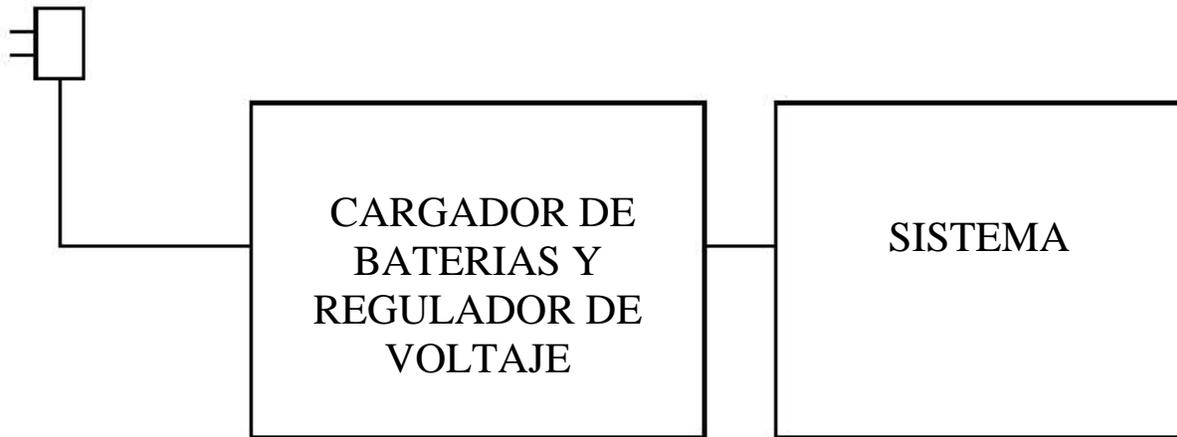


Figura IV.13 Esquema de la fuente de poder del sistema

La figura IV.14 muestra el circuito regulador de voltaje donde se utiliza el diodo zener de 6.2 V en conjunto con un par de transistores que proporcionan alta corriente al dispositivo Lector. Este circuito se conecta a la batería cuya energía proviene de un cargador de baterías externo que además contiene un sensor de temperatura.

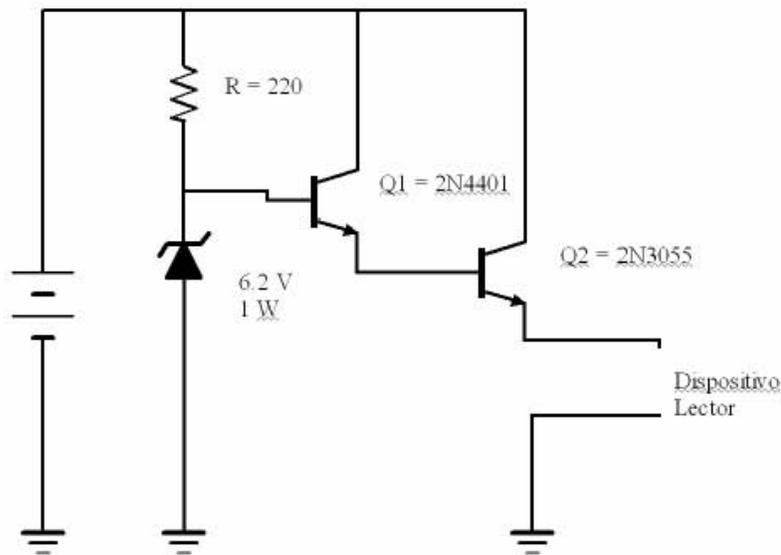


Figura IV.14 Circuito regulador de voltaje..

El dispositivo contará con un interruptor por medio del cual se activará o desactivará el Lector, por medio de la conexión y desconexión de la fuente de poder. Este interruptor no desconectará la energía de la Pocket PC, ya que ésta contará con su propia batería. Sin embargo, cuando el dispositivo lector esté desconectado, el software del sistema en la Pocket PC emitirá una alarma visual y audible notificándolo.

# **Análisis y Diseño del Software del Sistema**

V.1. Requerimientos del sistema.

V.2. Protocolo de Comunicación con el Lector.

V.3. Plataforma de Desarrollo.

V.4. Módulo de captura de datos.

V.5. Módulo de Almacenamiento de Datos.

## **Capítulo 5**

## ANÁLISIS Y DISEÑO DEL SOFTWARE DEL SISTEMA

### V.1 Requerimientos del Sistema

El proyecto ha sido definido con tres funciones principales:

- Realizar el inventario de bienes.
- Localizar un bien específico y emitir una alarma visible y/o audible cuando sea localizado.
- Realizar operaciones con etiquetas como son grabar, leer o borrar una etiqueta específica.

La figura V.1 muestra los menús con las opciones que estarán disponibles para el usuario.

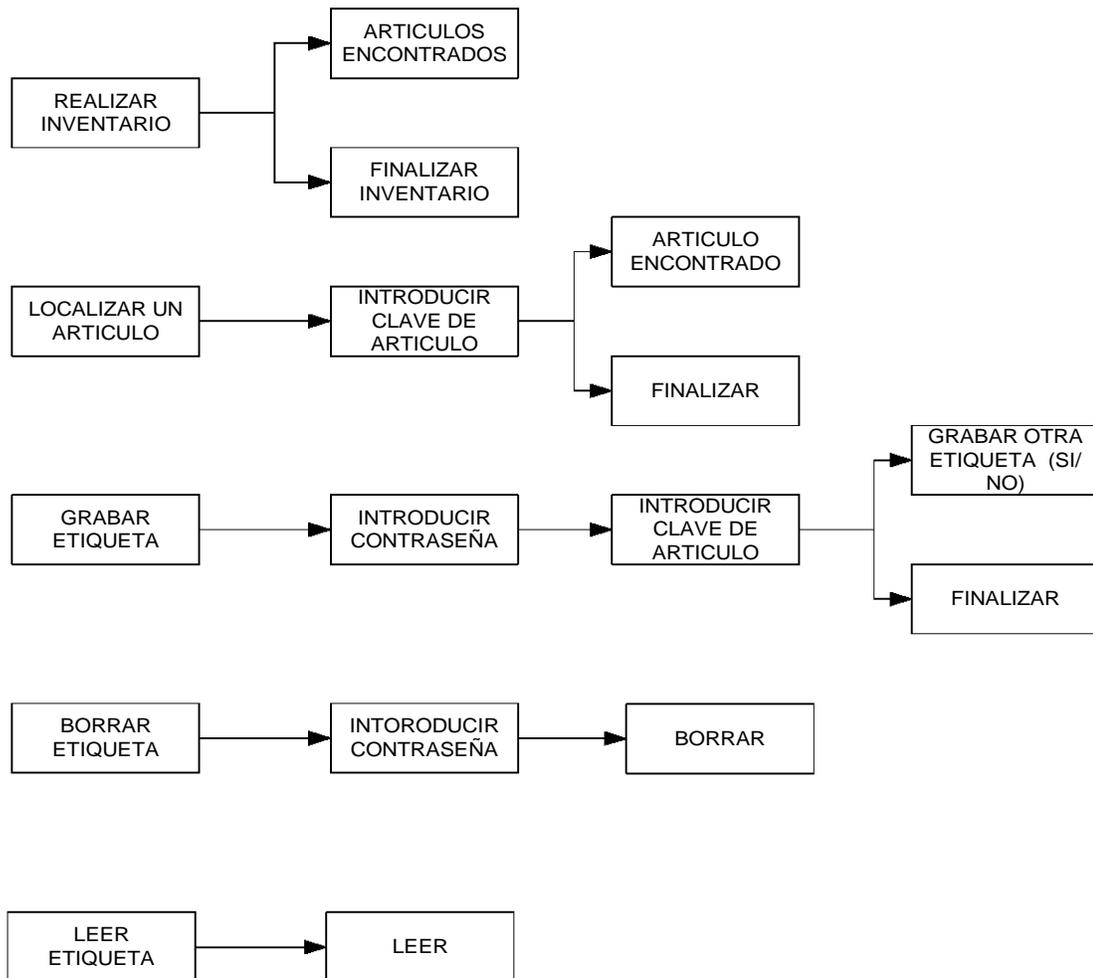


Figura V.1 Funciones del Sistema RFID

La primera pantalla que mostrará el programa se muestra en la figura V.2, en la cual se pueden apreciar que consiste en una serie de botones que se activarán al ser presionados en la pantalla:



*Figura V.2 Menú principal del sistema RFID*

La primera opción se encargará únicamente de realizar el inventario y de grabar la información en un archivo que se encontrará disponible posteriormente para su transmisión a otro sistema o para consulta. El nombre del archivo será dado por el usuario.

Al ingresar el nombre el archivo aparecerá la pantalla y que contendrá el número de bienes encontrados, la descripción del último bien localizado y las opciones de suspender, continuar y finalizar. Cuando el botón “Finalizar” sea presionado, la pantalla desplegará el total de los artículos encontrados y a través de un botón de control podrá desplegar los bienes que no se encontraron en el inventario.

La segunda opción del menú se encargará de localizar un bien específico. En la figura V.3 podemos observar las características de ésta pantalla.



Figura V.3 Pantalla de la función “Localizar” del Sistema RFID

Accediendo a ésta opción el sistema desplegará la base de datos en un Datagrid en el cual se podrá buscar el artículo por medio de una palabra de identificación y del campo al que corresponde. Cuando se seleccione la opción “Buscar Artículo”, se borrarán todos los registros en el Datagrid que no correspondan a las palabras buscadas. Una vez hecho esto se seleccionará directamente en el Datagrid el artículo y se presionará el botón “Localizar Artículo” que iniciará una rutina de conexión con el dispositivo lector para emitir las instrucciones de lectura de etiquetas hasta que sea localizado el bien o que se presione el botón “Detener”.

La tercera opción nos da acceso a la funcionalidad de grabar etiquetas. Esta opción, previa introducción de la contraseña, nos despliega una pantalla en la que se debe introducir el número a grabar en la etiqueta. Para esto se requerirá una cercanía mayor del transponder (aproximadamente 10 cm) que la de lectura, evitando realizar grabaciones no deseadas en otros transponder.

Al terminar la grabación estará disponible la opción de grabar otra etiqueta o de finalizar el proceso para regresar al menú principal.

La cuarta opción consistirá en borrar etiquetas lo cual dependerá de las necesidades del usuario y sólo será posible cuando el tipo de etiqueta lo permita y cuando esta no haya sido programada de manera definitiva. Al inicio se solicitará una contraseña para evita que sea utilizada esta funcionalidad de manera no permitida.

La quinta opción será la de leer etiqueta que nos permitirá conocer el número grabado en la etiqueta deseada.

Como parte de la seguridad del sistema se deberán introducir códigos de acceso de 4 caracteres alfanuméricos que permitirán la ejecución algunas funciones particulares del menú, tal como la opción de borrar etiquetas. Esta función requiere de una contraseña adicional ya que es muy importante que no sea accesible a cualquier usuario.

## **V.2 Protocolo de Comunicación con el Lector**

Los parámetros de comunicación del Lector con el puerto serial son de 115200 bps, 8 bits de datos, sin paridad y 1 bit de paro. El protocolo del Sirit ST200 es “orientado a bytes”, lo que significa que los paquetes y mensajes son una secuencia de bytes. Todos los parámetros y respuestas compuestos de varios bytes son codificados con el Byte más significativo (MSB), así como todos los bits son codificados iniciando con el bit más significativo (el MSBit en primer orden del MSByte).

La tabla V.1 muestra la estructura de un paquete, el cual puede contener comandos, instrucciones e información para el Lector. En esta estructura el SOF (Start of Frame – Inicio de Marco), se encuentra en el Byte más significativo, seguido por el campo LENGTH que es la longitud en Bytes del paquete, excluyendo el SOF. A continuación

se tiene el campo MESSAGE que contiene los comandos o respuestas seguido por el campo CRC. Este campo contiene el resultado de aplicar a los campos LENGTH y MESSAGE la secuencia de chequeo de marco (FCS) CRC-16 del CCITT con el fin de detectar posibles modificaciones de los valores de estos campos durante la transmisión del paquete.

| MSB                       |               |                    | LSB            |
|---------------------------|---------------|--------------------|----------------|
| <b>SOF</b><br><b>0x01</b> | <b>LENGTH</b> | <b>MESSAGE</b>     | <b>CRC</b>     |
| <b>1 Byte</b>             | <b>1 Byte</b> | <b>1-128 Bytes</b> | <b>2 Bytes</b> |

Tabla V.1 Estructura de un paquete del protocolo del Sirit ST200

La porción MESSAGE de un paquete es utilizada para transportar tanto comandos del host al módulo Lector, como respuestas del módulo lector al host, aunque el módulo lector no enviará respuestas autónomas (no solicitadas).

La Tabla V.2 muestra la estructura del formato del "MESSAGE" con la estructura de los campos de comando y respuesta. Aquí los mensajes de comandos contienen un campo de un byte denominado "Comando", seguido por un campo llamado "Parámetro" que puede contener desde cero hasta muchos parámetros asociados con el campo comando.

Los mensajes de respuesta contienen un campo de un byte llamado "Estado", al que le sigue un campo "Respuesta" que puede tener desde cero hasta muchas respuestas asociadas con el campo "Estado".

| MSB            |                   | LSB |
|----------------|-------------------|-----|
| <b>MESSAGE</b> |                   |     |
| <b>COMANDO</b> | <b>PARAMETROS</b> |     |
| <b>1 BYTE</b>  | <b>127 BYTES</b>  |     |

| MSB            |                  | LSB |
|----------------|------------------|-----|
| <b>MESSAGE</b> |                  |     |
| <b>ESTADO</b>  | <b>RESPUESTA</b> |     |
| <b>1 BYTE</b>  | <b>127 BYTES</b> |     |

Tabla V.2 Estructura del formato de los campos de Comando y Respuesta.

Los códigos del campo Estado posibles son 0xFF, que significa que el procesamiento del comando se ha completado con errores o fallas, 0x00 que significa que el comando se ha completado sin errores o fallas y 0x01 que significa que el comando aún se está procesando y que se deben esperar más datos de respuesta. El apéndice A muestra la lista de errores posibles y su explicación, así como la tabla de comandos disponibles en el módulo lector.

La tabla V.3 muestra el formato del mensaje de comando para las etiquetas o transponder clase 1. Cabe señalar que el código de comando para definir que la etiqueta es clase 1 es el 0x03.

| <b>MSB</b>               |                             | <b>LSB</b>         |
|--------------------------|-----------------------------|--------------------|
| <b>CODIGO DE COMANDO</b> | <b>PARAMETROS</b>           |                    |
| <b>0X03</b>              | <b>CODIGO DE SUBCOMANDO</b> | <b>PARAMETROS</b>  |
| <b>1 BYTE</b>            | <b>1 BYTE</b>               | <b>1-126 BYTES</b> |

*Tabla V.3 Formato del Comando para Etiquetas Clase 1*

La tabla V.4 muestra los subcomandos disponibles para las etiquetas clase 1. En este caso, los más importantes son los subcomandos READ, el cual es el subcomando de lectura de etiquetas y el subcomando WRITE que es utilizado para escribir en las etiquetas.

| SUBCOMANDO | CODIGO | DESCRIPCION   | MENSAJE DE RETORNO DE CODIGO |
|------------|--------|---|------------------------------|
| KILL       | 0xFF   | Se utiliza para deshabilitar por completo la etiqueta clase 1   | Si                           |
| SET        | 0x00   | Se utiliza para ajustar la potencia de radiofrecuencia y la profundidad de modulación                     | Si                           |
| READ       | 0x01   | Lee la etiqueta utilizando los parámetros subsiguientes. Este subcomando utiliza el comando SCROLL_ALL_ID | Si                           |
| PROGRAM_ID | 0x02   | Todas Las etiquetas clase 1 que reciban este comando programarán la ID de la etiqueta                     | Si                           |

|           |      | especificada   |    |
|-----------|------|--|----|
| VERIFY_ID | 0x03 | Todas las etiquetas clase 1 que reciban este comando replicarán con su CRC, seguid con el código ID completo y luego la contraseña. Si una etiqueta ha ejecutado exitosamente el comando LOCK_ID ignorará este subcomando. | Si |
| LOCK_ID   | 0x04 | Este comando previene cualquier modificación posterior de la ID de la etiqueta, el CRC y la contraseña   | Si |
| ERASE_ID  | 0x05 | Este comando coloca todos los bits del CRC, ID y contraseña en 0   | Si |
| PING_READ | 0x06 | Lee las etiquetas clase 1 con los parámetros especificados. Esta lectura utiliza el comando PING   | Si |

Tabla V.4 Subcomandos para etiquetas EPC Clase 1

### V.3 Plataforma de Desarrollo

Existen una gran cantidad de lenguajes de programación, y de éstos varios que se pueden utilizar en las Pocket PC.

Por un lado, Palm, nos brinda una plataforma de desarrollo basada en su propio lenguaje, el cual tiene fundamentos en C y C++. En la actualidad, el software para desarrollar para estos dispositivos es totalmente gratis, pero, para poder compilar una aplicación desarrollada para este, es necesario desembolsar una gran suma, ya que, los compiladores se venden por separado y son vendidos por terceros, y por último, si uno no posee un equipo Palm, es necesario obtener el BIOS del equipo para el cual queremos desarrollar, pero para ello, se deben llevar a cabo una serie de trámites entre Palm y la empresa a desarrollar, para poder obtener una copia de dicho BIOS. Está claro que habiendo seleccionado un dispositivo Pocket PC con sistema operativo Windows, esta opción queda descartada.

En contraste con Pocket PC, con Windows incluido. Podemos programar con la plataforma de desarrollo .Net, que nos permite programar en lenguajes como Visual Basic o Visual C.

En el caso de que queramos otras tecnologías, también podemos desarrollar con .Net,

el cual acepta, no solo los lenguajes tradicionales de Microsoft, si no, lenguajes alternativos como Java, Borland C, entre otros, y por supuesto, podemos acceder a toda la potencia de .Net, pero desde nuestro Pocket PC. Vale aclarar que .Net, por parte de terceros, también puede desarrollar para Palm.

El lenguaje de programación Java se ha creado con el propósito de ejecutar programas independientemente del hardware. En el caso de .Net, los alcances son mayores ya que incluyen la ejecución de varios lenguajes de programación y que pueden ser ejecutados inclusive desde Internet, por lo que su portabilidad, al igual que Java, constituye un punto importante.

### V.3.1 JAVA Micro Edition (J2ME)

Cuando una persona desarrolla una aplicación en un lenguaje como C o C++, el archivo binario que genera el compilador y que contiene el código que implementa dicha aplicación, se puede ejecutar únicamente sobre la plataforma sobre la cual fue desarrollada, debido a que dicho código es específico a esa plataforma.

La plataforma Java se encuentra por encima de otras plataformas. El código que generan sus compiladores no es específico de una máquina física en particular, sino de una máquina virtual. Aún cuando existen múltiples implantaciones de la Máquina Virtual Java, cada una específica de la plataforma sobre la cual subyace, existe una única especificación de la máquina virtual, que proporciona una vista independiente del hardware y del sistema operativo sobre el que se esté trabajando. De esta manera un programador en Java "escribe su programa una vez, y lo ejecuta donde sea"<sup>2</sup>.-

Es precisamente la máquina virtual Java la clave de la independencia de los programas Java, sobre el sistema operativo y el hardware en que se ejecutan, ya que es la encargada de proporcionar la vista de un nivel de abstracción superior, donde además de la independencia de la plataforma antes mencionada, presenta un lenguaje de programación simple, orientado a objetos, con verificación estricta de tipos de datos, múltiples hilos, con ligado dinámico y con recolección automática de basura.

Java es un lenguaje de programación de Sun Microsystems originalmente llamado "Oak", que fue concebido bajo la dirección de James Gosling y Bill Joy, quienes pertenecían a una subsidiaria de Sun, conocida como "*FirstPerson Inc*". Oak nació para programar pequeños dispositivos electrodomésticos, como los asistentes personales digitales PDAs (*Personal Digital Assistants*) y un poco más adelante se utilizó para ejecutar aplicaciones para televisores. Ninguno de estos productos tuvo éxito comercial. Gosling y Joy se quedaron con una tecnología robusta, eficiente, orientada a objetos, independiente de la arquitectura, pero hasta ese momento, sin ninguna utilidad práctica.

---

<sup>2</sup> Sun Microsystems: Write Once, Run Anywhere

No pasó mucho tiempo, cuando en Sun se dieron cuenta de que todas estas características cubrían a la perfección las necesidades de las aplicaciones de Internet. De esta manera, con unos cuantos retoques, Oak se convirtió en Java.

Aunado a todas las características que posee Java (modelo de objetos dinámico, sistema estricto de tipos, paquetes, hilos, excepciones, etcétera), cuando Nestcape Inc. anunció su incorporación dentro de su navegador (*Netscape Navigator*), el nivel de interés sobre el lenguaje creció dramáticamente, debido al número importante de personas que utilizan el Internet diariamente. Todo lo anterior se ha conjugado para lograr el éxito actual de Java, siendo el actor principal su máquina virtual.

El concepto de máquina virtual es antiguo. Fue usado por IBM en 1959 para describir uno de los primeros sistemas operativos que existieron en la historia de la computación, el *VM*. En 1970, el ambiente de programación de *SmallTalk* llevó la idea a un nuevo nivel y construyó una máquina virtual para soportar abstracciones orientadas a objetos de alto nivel, sobre las máquinas subyacentes.

Las máquinas virtuales tienen varias ventajas importantes. La primera es que presentan un medio excelente para alcanzar la portabilidad. Otra de las ventajas importantes, es que introduce otro nivel de abstracción y de protección, entre la computadora y el software que ejecuta sobre ella. Esto cobra particular importancia en un ambiente donde el código que ejecutamos proviene de algún lugar del mundo y es escrito por personas desconocidas.

Es posible decir que los lenguajes totalmente interpretados, como *Tcl* y *JavaScript*, también poseen las cualidades de ser altamente portables y seguros, pero existe una diferencia importante entre este tipo de lenguajes y los basados en una máquina virtual: la eficiencia.

Para ejecutar un programa escrito en un lenguaje completamente interpretado, el intérprete debe realizar el análisis léxico y sintáctico en el momento de estar ejecutando el programa, lo que provoca una sobrecarga muy considerable en la ejecución del mismo. De hecho, en algunas pruebas informales *Tcl* puede ser hasta 200 veces más lento que C.

Los lenguajes basados en una máquina virtual, comúnmente son más rápidos que los totalmente interpretados, debido a que utilizan una arquitectura de código intermedio. La idea es dividir la tarea de ejecutar un programa en dos partes. En la primera, se realiza el análisis léxico y sintáctico del programa fuente, para generar el programa en instrucciones del procesador virtual (código intermedio) y en el segundo paso, se itera sobre el código intermedio para obtener la ejecución final del programa.

Los lenguajes compilados de código intermedio, pueden llegar a ser un orden de magnitud más rápido que los lenguajes completamente interpretados, pero, por consiguiente, un orden de magnitud más lentos que lenguajes optimizados como C o C++.

Se dice que el código Java es portable debido a que es posible ejecutar el mismo archivo de clase (.class), sobre una amplia variedad de arquitecturas de hardware y de software, sin ninguna modificación.

Java es un lenguaje dinámico, debido a que las clases son cargadas en el momento en que son necesitadas (dinámicamente), ya sea del sistema de archivos local o desde algún sitio de la red mediante algún protocolo *URL*.

Java tiene la capacidad de aumentar su sistema de tipos de datos dinámicamente o en tiempo de ejecución. Este "enlace tardío" (*late-binding*) significa que los programas sólo crecen al tamaño estrictamente necesario, aumentando así la eficiencia del uso de los recursos. Java hace menos suposiciones sobre las implantaciones de las estructuras de datos, que los lenguajes estáticos de "enlace temprano" o en tiempo de compilación (*early-binding*) como C o C++.

Debido a que Java nació en la era post-Internet, fue diseñado con la idea de la seguridad y la fiabilidad, por lo que se le integraron varias capas de seguridad para evitar que programas maliciosos pudiesen causar daños en los sistemas, sobre los que ejecuta la implantación de la Máquina Virtual Java.

La Máquina Virtual Java es el núcleo del lenguaje de programación Java. De hecho, es imposible ejecutar un programa Java sin ejecutar alguna implantación de la MVJ. En la MVJ se encuentra el motor que en realidad ejecuta el programa Java y es la clave de muchas de las características principales de Java, como la portabilidad, la eficiencia y la seguridad.

Siempre que se corre un programa Java, las instrucciones que lo componen no son ejecutadas directamente por el hardware sobre el que subyace, sino que son pasadas a un elemento de software intermedio, que es el encargado de que las instrucciones sean ejecutadas por el hardware. Es decir, el código Java no se ejecuta directamente sobre un procesador físico, sino sobre un procesador virtual Java, precisamente el software intermedio que se había mencionado.

Como se muestra en la figura V.4<sup>3</sup>, Java se divide en tres grupos principales:

Java Standard Edition (J2SE) - Desarrollado para estaciones de trabajo y computadoras de escritorio.

Java Enterprise Edition (J2EE) – Desarrollado especialmente para aplicaciones basadas en servidor.

---

<sup>3</sup> <http://java.sun.com/j2me/docs/j2me-ds.pdf>

Java Micro Edition (J2ME) - Desarrollado para dispositivos con capacidades limitadas de procesamiento, memoria y despliegue.

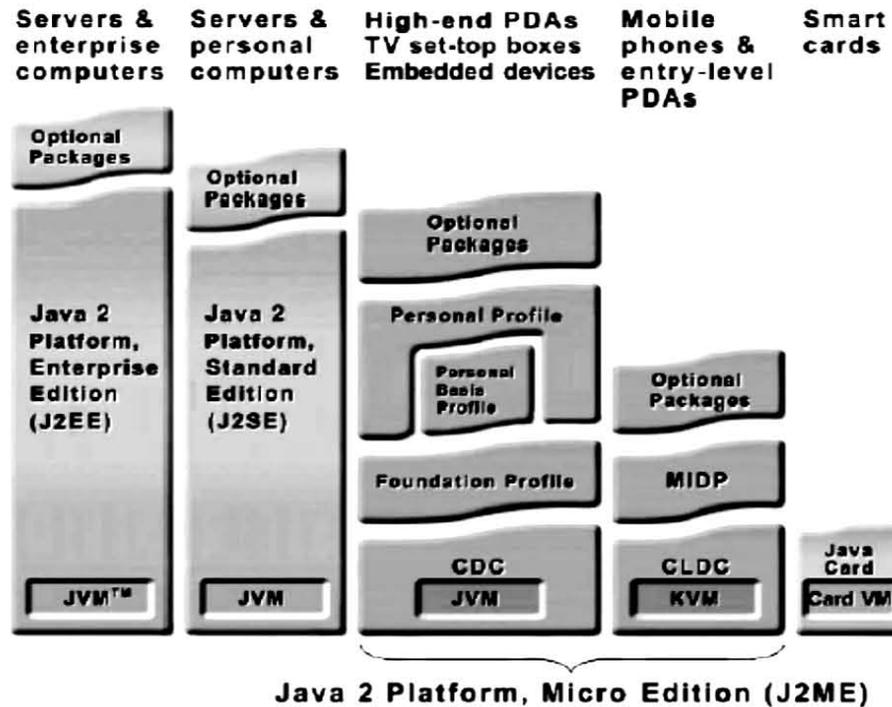


Figura V.4 Ediciones de Java [30]

La edición J2ME de Java hace que los dispositivos que soportan esta plataforma no sean estáticos. Los dispositivos modernos como teléfonos celulares y PDA permiten a los usuarios crear y descargar nuevas aplicaciones, diferentes a las proporcionadas durante el proceso de fabricación.

Micro Edition de Java fue desarrollado tomando en consideración las limitaciones técnicas de éstos dispositivos. Evidentemente no todas las funciones de J2SE y J2EE pueden ser aplicadas a un teléfono celular o a un PDA, como por ejemplo la interfaz gráfica, que está limitada por el tamaño de la pantalla del dispositivo.

Para encajar en las diferentes características de los dispositivos, Sun introdujo el concepto de configuración y perfil. La división por configuraciones está basada en las características del dispositivo. Tales como memoria, eficiencia del procesador o de despliegue y está conectado de manera muy cercana con la Máquina Virtual de Java, que define las características del lenguaje y las librerías núcleo.

### V.3.2 Net Compact Framework

El día de hoy, los usuarios se encuentran con aplicaciones que son amigables pero no son independientes de la plataforma. Por ejemplo, cuando se visita una página de Internet, podemos registrarnos y esta información puede ser utilizada por el administrador de la página para ofrecer productos específicos de nuestro interés. Lo mismo es pertinente para aplicaciones como Microsoft Word, en el cual podemos almacenar nuestras preferencias. Comparativamente, si tenemos dos aplicaciones ejecutándose en dos plataformas diferentes (tales como Linux y Windows juntos), puede ser que no se ofrezca una completa interoperabilidad, lo que significa que no se pueden ejecutar aplicaciones de Windows en la plataforma Linux.

Podemos concluir entonces que personalizar una aplicación es fácil para un usuario, pero tenemos opciones limitadas cuando se trata de personalizar una aplicación por otra. La iniciativa .NET apunta a extender un puente entre este espacio de personalización entre aplicaciones.

La interoperabilidad de aplicaciones permite acceder datos existentes y funcionalidades desde aplicaciones diferentes que pueden correr en plataformas también diferentes. Si estas aplicaciones exponen su funcionalidad sobre el Internet, pueden ser accedidas desde cualquier parte. Por lo tanto tendríamos que se comunican una con la otra a través de Internet y esto es exactamente lo que .NET trata de lograr.

Para entender como .NET habilita que las aplicaciones se comuniquen entre sí, tomemos como ejemplo dos aplicaciones que necesitan interactuar y que por lo tanto tienen que sobrepasar las siguientes barreras:

**Geográfica:** Las aplicaciones que necesitan interactuar pueden estar localizadas en diferentes partes del mundo.

**Plataforma:** Las aplicaciones pueden correr en diferentes plataformas.

**Lenguaje:** Estas aplicaciones pueden haber sido desarrolladas en diferentes lenguajes de programación sin el mínimo grado de similitud.

Considerando las posibles soluciones a estos obstáculos, encontramos que lo más simple para resolver la barrera geográfica, es que las aplicaciones se ejecuten sobre Internet, ya que éste es la forma más rápida y fácil para romper barreras geográficas.

Para el problema del tipo de plataforma, se puede necesitar un lenguaje común que puede hacer que las aplicaciones se comuniquen entre sí. El XML (eXtensible Markup Language) ha surgido como éste lenguaje común y es también el estándar en la industria para la descripción y transporte de datos. Por lo tanto, el XML es utilizado para intercambiar información entre las aplicaciones .NET y también resuelve el problema de la diferencia de lenguajes, ya que se pueden comunicar en tanto estén basadas en XML.

Por lo tanto, se pueden crear aplicaciones que no requieran la interacción del usuario pero que se comunican entre sí para servir a un propósito común. A estas aplicaciones se les llama *servicios* para distinguirlas de las aplicaciones que utilizamos normalmente. Los XML Web Services (servicios) es el resultado más significativo de la iniciativa .NET.

Con los servicios XML Web se pueden proporcionar productos de software como servicios. En este caso, los usuarios no necesitarían comprar el software sino suscribirse a un servicio y utilizarlo por el tiempo necesario.

La iniciativa .NET incluye una gama de productos que van desde .Net Enterprise servers, hasta la plataforma de desarrollo Visual Studio.NET, que están centrados en Servicios XML Web.

Los dos beneficios principales de la iniciativa.NET son la Interoperabilidad de los dispositivos cliente y una mejor experiencia del usuario. El software de Microsoft, tales como Windows CE.NET y Windows XP pueden ser utilizados para operar computadoras de mano, portátiles y PC de escritorio. Windows XP utiliza de manera extensiva el XML para implantar funciones como la asistencia remota y la publicación de páginas Web. Por otro lado, Windows CE.NET soporta XML 3.0 habilitando el acceso a los servicios Web sobre dispositivos móviles.

.NET Framework es la plataforma utilizada para crear Servicios XML Web. Esta proporciona las clases necesarias, espacios de nombres y ensamblajes para crear tales aplicaciones. .Net Framework consiste de tres componentes:

Lenguaje Común en Tiempo de Ejecución - *Common Language Runtime* (CLR): el CLR maneja la ejecución del código en tiempo de ejecución. El CLR asegura memoria eficiente, manejo de hilos y seguridad al ejecutar el código. EL CLR se denomina de esta manera ya que asegura la interoperabilidad entre códigos de programación que están escritos en diferentes aplicaciones de Visual Studio.NET. Como resultado, se puede correr una aplicación codificada en otro lenguaje.

Biblioteca de Clases (Class Library). El .NET Framework incluye una biblioteca de clases que es una colección completa de clases orientadas a objetos que pueden ser utilizadas para desarrollar aplicaciones Windows y Web.

ASP.NET: Es un componente importante de .NET Framework ya que proporciona capacidades avanzadas, tales como acceso eficiente a bases de datos y capacidades fáciles de utilizar de estado de Aplicación y Sesión. Las aplicaciones ASP.NET pueden ser creadas utilizando cualquier lenguaje .NET, tales como Visual Basic.NET o Visual C#.NET.

## **.NET Compact Framework<sup>4</sup>**

.NET Compact Framework es un subconjunto de .NET Framework, en donde se han excluido algunos componentes debido a que está dirigido para el desarrollo de aplicaciones en dispositivos móviles, los cuales tienen características limitadas de memoria y capacidad de procesamiento.

.NET Compact Framework simplifica el desarrollo de aplicaciones para dispositivos inteligentes. Actualmente, esto incluye a los dispositivos Pocket PC, Pocket PC Phone Edition y otros dispositivos que ejecuten Windows CE.NET 4.1 o posterior.

Se necesita Visual Studio .NET para crear aplicaciones destinadas a .NET Compact Framework y solo se pueden crear aplicaciones utilizando Visual C# .NET, Visual Basic .NET y Visual J#.

.NET Compact Framework tiene dos componentes principales: el tiempo de ejecución en lenguaje común (CLR) y la biblioteca de clases de .NET Compact Framework.

El tiempo de ejecución es la base de .NET Compact Framework, ya que, al igual que en el .NET Framework, se encarga de administrar el código en el momento de la ejecución, proporcionando servicios esenciales como la administración de la memoria y de los subprocesos, al mismo tiempo que garantiza la seguridad y la precisión. Si el código está destinado al tiempo de ejecución se denomina código administrado, si no lo está, como ocurre con eMbedded Visual C++, se denomina código no administrado o nativo.

La biblioteca de clases de .NET Compact Framework es una colección de clases reutilizables que se pueden utilizar para desarrollar aplicaciones de manera fácil y rápida. Este marco se ha diseñado pensando en la portabilidad, tanto para plataformas Microsoft como de otros fabricantes. Esto significa que las técnicas de codificación y las aplicaciones creadas hoy en un Pocket PC se pueden ejecutar en otras plataformas, como un teléfono móvil o un PDA de otro fabricante, si se ha creado una versión de .NET Compact Framework para dicha plataforma.

El tiempo de ejecución en lenguaje común proporciona un entorno de ejecución de código que administra el código destinado a .NET Compact Framework. La administración de código se refiere a la administración de la memoria, de los subprocesos y de la seguridad, así como a la verificación y compilación del código en otros servicios del sistema.

El tiempo de ejecución se ha diseñado para mejorar el rendimiento. Utiliza compilación directa (JIT), que permite que el código administrado se ejecute en el lenguaje del equipo nativo de la plataforma en el que se está ejecutando la aplicación. De esta manera es posible crear aplicaciones destinadas a una gran variedad de plataformas,

---

<sup>4</sup> [www.microsoft.com](http://www.microsoft.com)

sin que haya que preocuparse de volver a compilar o generar ejecutables destinados a cada plataforma concreta.

Aunque la aplicación móvil esté escrita en Visual Basic .NET o C# .NET, al tratarse de código administrado, seguirá siendo posible incorporar funciones y subrutinas almacenadas externamente en bibliotecas de vínculos dinámicos (DLL), incluidas las API de Windows CE. .NET Compact Framework proporciona los tipos de datos y la compatibilidad con las estructuras necesaria para incorporar con facilidad funciones de las API de Windows CE en su aplicación.

La biblioteca de clases de .NET Compact Framework es una colección de clases reutilizables que se integra estrechamente con el tiempo de ejecución en lenguaje común. Las aplicaciones aprovechan estas bibliotecas para obtener ciertas funcionalidades.

Como es de esperar en una biblioteca de clases orientada a objetos, los tipos de .NET Compact Framework permiten llevar a cabo una serie de tareas de programación habituales, entre las que se incluye el diseño de interfaces, el uso de XML, el acceso a bases de datos, la administración de subprocesos y la E/S de archivos.

A continuación, se incluye una lista de funcionalidades habituales disponibles en .NET Compact Framework. Clases relacionadas con formularios .NET Compact Framework que implementa un subconjunto de las clases System.Windows.Forms y System.Drawing, que permite crear una cómoda interfaz de usuario basada en Windows CE para la aplicación del dispositivo.

El diseñador de formularios de Visual Studio.NET se ocupa automáticamente de gran parte de la interacción utilizando estas clases. La implementación de Windows Forms con .NET Compact Framework incluye la posibilidad de utilizar formularios, la mayoría de los controles de .NET Framework, el alojamiento de controles de otros fabricantes, mapas de bits y menús.

Al ser .NET Compact Framework un subconjunto de .NET Framework, los controles incluidos ofrecen un subconjunto de las funcionalidades de sus equivalentes para equipos de escritorio. Debido a consideraciones de tamaño y de rendimiento, los controles de .NET Compact Framework no incluyen algunas propiedades, métodos y eventos de los controles. Con un poco de codificación, se pueden implementar estas funcionalidades en caso de que sean necesarias, ya que .NET Compact Framework permite crear controles mediante herencia de la clase base del control. A partir de esta base, se pueden agregar métodos, propiedades y eventos para crear exactamente el control que necesita.

### **Clases de XML y de datos**

.NET Compact Framework incluye un conjunto de clases que permiten incorporar con facilidad datos (ya sea de un origen de datos relacional o no), entre los que se incluye

el contenido XML, en las aplicaciones móviles. Estas clases se definen para los espacios de nombres **System.Data** y **System.Xml**. La implementación de clases de XML y de datos en .NET Compact Framework es un subconjunto de la que se encuentra en .NET Framework.

### Servicios Web

.NET Framework presta una atención especial a los servicios Web. En el espacio de nombres **System.Web** de .NET Compact Framework, hay una versión a escala reducida de las posibilidades y funcionalidades que ofrece el correspondiente espacio de nombres de .NET Framework. La característica más destacable es que se pueden crear clientes de servicios Web pero no se pueden alojar servicios Web en .NET

### Compact Framework.

Estos clientes de servicios Web XML pueden ser sincrónicos o asincrónicos. Se pueden crear fácilmente clientes de servicios Web XML destinados a .NET Compact Framework. El IDE de Visual Studio .NET hace automáticamente la mayor parte del trabajo.

### Compatibilidad con GDI

.NET Compact Framework proporciona compatibilidad con los elementos básicos de dibujo de GDI incluidos mapas de bits, pinceles, fuentes, iconos y plumas mediante el espacio de nombres **System.Drawing**.

### Clases base

.NET Compact Framework proporciona un conjunto robusto de clases base que expone una amplia variedad de funcionalidades que los desarrolladores pueden aprovechar. Esta infraestructura subyacente le permite escribir cómodas aplicaciones .NET que incluyen la posibilidad de crear aplicaciones con varios subprocesos (**System.Threading**), aprovechar recursos de red (**System.Net**) y trabajar con archivos (**System.IO**).

### Compatibilidad con IrDA

Algunos dispositivos incluyen la posibilidad de comunicarse mediante infrarrojos (IR). Para poder aprovechar esta posibilidad, .NET Compact Framework incluye clases que permiten aprovechar la comunicación mediante infrarrojos desde la aplicación. Estas clases son parte del espacio de nombres **System.Net.IrDA**. Se puede utilizar infrarrojos para comunicarse con equipos Pocket PC, impresoras y otros dispositivos compatibles con infrarrojos.

## **Compatibilidad con Bluetooth**

.NET Compact Framework no incorpora compatibilidad nativa con Bluetooth. Se puede obtener acceso a la mayoría de implementaciones de Bluetooth en equipos Pocket PC de otros fabricantes mediante las comunicaciones del puerto serie o mediante una API del proveedor.

## **Compatibilidad con Visual Basic**

Visual Basic .NET utiliza bastante las funciones auxiliares de la biblioteca auxiliar de Visual Basic. .NET Compact Framework incluye también un subconjunto de estas funciones, consideradas por los desarrolladores de Visual Basic como una parte esencial del lenguaje, por lo que se ha decidido incluirlas.

Para los desarrolladores de Visual Basic o eMbedded Visual Basic que están comenzando a trabajar con .NET Compact Framework, esto significa que la mayoría de las funciones del lenguaje Visual Basic con las que está acostumbrado a trabajar también estarán disponibles en Visual Basic .NET.

## **Características a la carta**

Para ahorrar recursos en el dispositivo de destino, Microsoft ha dividido .NET Compact Framework en componentes lógicos. Al suministrar los componentes como DLL independientes (o ensamblados, según se les denomina en .NET Compact Framework) Microsoft ofrece la oportunidad de decidir y seleccionar las características que necesita y sólo aquéllas para las que el dispositivo de destino tiene espacio.

Un ejemplo de esto es el ensamblado System.SR, que contiene las cadenas de los mensajes de error. Si incluye este ensamblado en la aplicación se pueden ver descripciones detalladas de todos los errores detectados, lo cual es ciertamente útil durante una sesión de depuración, pero normalmente no es necesario una vez que se ha lanzado a producción. Si no se incluye este ensamblado, no se verán afectados ni el rendimiento ni la funcionalidad de la aplicación, pero no podrá ver mensajes de error detallados.

Otro ejemplo del enfoque a la carta de .NET Compact Framework son los componentes SQL Server CE, que se entregan en un conjunto de DLL cuyo tamaño total apenas supera 1 MB. A menos que se agregue explícitamente una referencia a los ensamblados System.Data.SqlServerCe, estas DLL no se incluirán en la aplicación.

## **Características no incluidas en .NET Compact Framework**

Ha sido necesario realizar importantes recortes en .NET Framework para adaptarlo a las limitaciones de funcionamiento de Windows CE. Las características más destacables de .NET Framework que no se han incluido en .NET Compact Framework son las siguientes:

## Sobrecargas de métodos

La sobrecarga de un método ofrece maneras alternativas de llamar a dicho método. También aumenta el tamaño de Framework. Por este motivo, .NET Compact Framework ha eliminado las sobrecargas de prácticamente todos los métodos.

Hay dos consecuencias básicas de esto. Es bastante probable que una determinada sobrecarga de un método que solía utilizarse con una aplicación de escritorio no esté disponible a la hora de desarrollar aplicaciones basadas en .NET Compact Framework.

## Controles no incluidos

Hay una serie de controles de .NET Framework que no se han incluido en .NET Compact Framework. La ausencia de la mayoría de estos controles carece de importancia para los desarrolladores de aplicaciones móviles. Teniendo en cuenta que las aplicaciones móviles apenas imprimen, no es ningún problema eliminar la familia completa de controles relacionados con la impresión. Por tanto, se han eliminado los controles `CrystalReportViewer`, `PageSetupDialog`, `PrintDialog`, `PrintDocument`, `PrintPreviewControl` y `PrintPreviewDialog`. Se puede sustituir la mayoría de los cuadros de diálogo que faltan por sus propios cuadros de diálogo o bien utilizar directamente los cuadros de diálogo del sistema mediante la API de Windows CE.

También están empezando a aparecer controles de otros fabricantes que sustituyen a los controles que no se han incluido en .NET Compact Framework.

## Funcionalidad XML

Aunque se ha incluido buena parte de la funcionalidad de XML de .NET Compact Framework, ha sido necesario recortarla. El componente clave relacionado con el XML que no se ha incluido es el espacio de nombres **System.Xml.XPath**. El espacio de nombres XPath hacía la interpretación del XML mucho más fácil que los métodos que incorpora .NET Compact Framework. Para compensar esto, se puede utilizar una combinación de las búsquedas recursivas e iterativas con el modelo de objetos de documento (DOM, Document Object Model).

Hay otro componente clave XML que no se ha incluido en .NET Compact Framework: XSLT (Extensible Stylesheet Language Transformation). Mediante XSLT, es posible convertir un documento XML en diferentes formatos.

En relación con el XML, .NET Compact Framework no ofrece actualmente compatibilidad para el desarrollo de servicios Web XML basados en dispositivos.  
Compatibilidad con bases de datos

.NET Compact Framework ofrece un conjunto robusto de herramientas relacionadas con los datos. La compatibilidad con la base de datos local la proporciona SQL Server CE. En el servidor, .NET Compact Framework ofrece compatibilidad con SQL Server.

### **Serialización binaria**

Debido a consideraciones de tamaño y de rendimiento, no se han incluido las clases BinaryFormatter y SoapFormatter en .NET Compact Framework.

### **Acceso al registro de Windows**

.NET Framework incorpora el espacio de nombres Microsoft.Win32.Registry, que facilita el trabajo con el registro de Windows desde una aplicación. Obviamente, este espacio de nombres no se ha incluido en .NET Compact Framework, ya que hace referencia a Win32 y no a Windows CE. Se puede tener acceso al registro de Windows CE llamando a las correspondientes API de Windows.

### **Aprovechamiento de los componentes COM**

El proceso de incorporación de objetos COM en una aplicación basada en .NET Compact Framework consta de dos pasos. Primero, se debe escribir un empaquetador DLL no administrado (es decir, en eMbedded Visual C++) que exponga el objeto COM. Dependiendo de la complejidad del objeto COM, hacer esto puede ser muy sencillo o extremadamente complicado. Segundo, se debe utilizar PInvoke para tener acceso al empaquetador DLL.

### **Seguridad**

.NET Compact Framework no impide el acceso al código no administrado. Cualquier aplicación puede llamar a una API, ya sea del sistema o no.

Actualmente, no hay ningún tipo de seguridad basada en funciones en .NET Compact Framework. El objeto principal no entiende de identidad conocida o de función conocida.

### **Servicios Web XML**

La exclusión más notable de las posibilidades de los servicios Web XML de .NET Compact Framework es la posibilidad de utilizar cookies. Las cookies se utilizan con frecuencia para almacenar el estado en el servidor entre diferentes llamadas desde un cliente. Aunque el uso de las cookies en los servicios Web no es tan frecuente como su uso en sitios Web, también se utilizan.

.NET Compact Framework ofrece posibilidades de cifrado limitadas respecto a los servicios Web.

## **Impresión**

.NET Compact Framework no ofrece ninguna función para imprimir. No hay ninguna manera fácil de interactuar con impresoras de red ni con impresoras externas mediante infrarrojos.

La solución para tener acceso a las impresoras de red es crear una aplicación basada en el servidor, que acepte e imprima las tareas enviadas por la aplicación móvil.

Se puede enviar una salida mediante el puerto de infrarrojos directamente a impresoras compatibles con infrarrojos. Se puede utilizar el espacio de nombres **System.Net.IrDA** para tener acceso al puerto de infrarrojos del dispositivo.

## **GDI+**

Windows CE no es compatible de manera nativa con GDI+, por lo que las funcionalidades relacionadas con GDI+ se han eliminado de .NET Compact Framework.

## **Entorno remoto**

La primera versión de .NET Compact Framework no es compatible con el entorno remoto.

## **Lenguajes admitidos**

.NET Compact Framework admite dos lenguajes de desarrollo, C# .NET y Visual Basic .NET. Mientras que las versiones anteriores de las herramientas de desarrollo de Windows CE favorecían el uso de lenguajes basados en C (concretamente, eMbedded Visual C++) con .NET Compact Framework apenas importa el lenguaje que se utilice, ya que todos son igualmente eficaces y funcionales.

Hay otra limitación de lenguaje en .NET Compact Framework que no existe en .NET Framework. Con .NET Framework se pueden utilizar componentes en diferentes lenguajes en un único proyecto. En comparación, los proyectos de .NET Compact Framework están restringidos a un único lenguaje, ya sea C# .NET o Visual Basic .NET. La solución que permite superar esta limitación de utilizar un único lenguaje en cada proyecto impuesto por .NET Compact Framework es crear proyectos adicionales utilizando la plantilla Class. Se Agrega el código del lenguaje alternativo a la plantilla y, a continuación, sólo se tiene que agregar referencias a estas clases en el proyecto de la aplicación.

Dado que nuestro proyecto está estrechamente relacionado con la tecnología .NET de Microsoft, ya que los bienes a inventariar son precisamente del Laboratorio de Microsoft, se tiene más fácil acceso a información relacionada al desarrollo de software

utilizando la plataforma .NET Compact Framework, de ahí que es la plataforma seleccionada para el desarrollo del proyecto con el lenguaje Visual Basic.NET

#### V.4 MODULO DE CAPTURA DE DATOS

En este módulo se incluye la comunicación entre la Pocket PC y el dispositivo lector. En Visual Studio 2003, no se incluyen librerías de comunicación con el puerto serial, sin embargo es posible descargarlas a través de algunos sitios de Internet.

Para el presente proyecto se descargó el archivo SerialNet.dll el cual incluye una clase denominada Port con las propiedades Enabled, Comport y Baudrate que fueron utilizadas para la configuración del puerto a 115,200 bauds del puerto 1.

Los métodos de ésta clase incluyen a Purge, Dispose, Read, Write, Stringtobytearray y Bytearraytostring.

Para utilizar el método Write y enviar el comando al dispositivo lector fue necesario calcular primero los dos bytes menos significativos, a través del cálculo del CRC (*Cíclic Redundancy Code* –Código de Redundancia Cíclica) y luego convertir la variable a transmitir al tipo Byte.

Para el cálculo del CRC se utiliza el generador polinomial especificado por CRC-CCITT para un valor de 16, que es el polinomio

$$X^{16} + X^{12} + X^5 + 1$$

El código que calcula el CRC es el siguiente:

```

Private Sub CRC16(ByVal inicio As Integer, ByVal conteo As Integer, ByRef
datosrcrc() As Byte)
    Dim resultemporal As Integer
    Dim indicebit As Integer
    Dim indicebyte As Integer
    Dim contenedor As Byte
    For indicebyte = inicio To inicio + conteo - 1
        contenedor = datosrcrc(indicebyte)
        For indicebit = 0 To 7
            resultemporal = (Fix(CRC / 32768) Xor Fix(contenedor / 128))
And 65535
            CRC = (CRC * 2) And 65535
            If resultemporal And 1 = 1 Then
                CRC = (CRC Xor 4129) And 65535
            End If
            contenedor = (contenedor * 2) And 255
        Next indicebit
    Next indicebyte
End Sub

```

En donde inicio es el byte inicial y conteo es el número de bytes que serán utilizados para el cálculo del CRC. DatoCRC es el arreglo que contiene el valor para cada byte. Los bytes menos significativos se forman con las siguientes instrucciones:

```
txarr(6) = Fix((CRC And 65280) / 256) And 255      ' CRC MSB
txarr(7) = CRC And 255                             ' CRC LSB
```

El arreglo es luego convertido a una variable tipo Byte y enviado al dispositivo lector utilizando el método Write. La respuesta se solicita de manera inmediata ejecutando el método Read, tal como se describe a continuación.

```
comando = SerialNET.Port.ByteArrayToString(txarr)
objPort.Write(comando)

str = objPort.Read(0, 500)
```

En donde el valor 500 representa el tiempo de espera de respuesta en milisegundos.

Todos los comandos enviados al dispositivo lector, ya sea de escritura, lectura o borrado de etiqueta, incluyen el cálculo del CRC aquí descrito.

#### **V.4 MODULO DE ALMACENAMIENTO DE DATOS**

Para el almacenamiento de los datos que se obtienen al realizar el inventario se escogió SQL CE ya que es una base de datos fácil de programar y además se encuentra incluida en las herramientas disponibles en el Compact Framework de Visual Studio 2003.

Se realizó primero una base de datos conteniendo toda la información de la totalidad de los bienes, junto con el número de etiqueta asociada a cada bien. Al momento de iniciar la realización del inventario, el sistema solicita el nombre de la nueva base de datos en donde se va a guardar la relación de los bienes encontrados. Este nombre constituye un archivo con una copia exacta de la base de datos original, el cual además incluye un campo adicional que sirve como indicación de que el bien ha sido localizado en este nuevo inventario.

El resumen de instrucciones que ejecutan estas tareas son las siguientes:

```
base_nueva = TextBox1.Text
ruta = "\My Documents\Inventario\" & base_nueva & ".sdf"
origen = "\My Documents\basnueva.sdf"
File.Copy(origen, ruta)
```

En este caso el valor de la variable `base_nueva`, que es el nombre de la nueva base, es introducido por el usuario en el `TextBox1`.

Al estar realizando el inventario, el sistema obtiene un número único de identificación localizado en la etiqueta, el cual es proporcionado por el dispositivo lector a través del módulo de comunicaciones. Con este número, se realiza la verificación del inventario y en caso de ser un número válido para un bien, se despliegan los datos del dispositivo encontrado.

El resumen de instrucciones que ejecutan estas tareas son las siguientes:

```
Dim insertar As SqlCeCommand = coneccion.CreateCommand()
Dim Seleccion As String = "SELECT Tipo, Equipo, Componente, Serie, Found
FROM Productos WHERE etiqueta_id =" & tag_id
Dim accesa As New SqlCeCommand(Seleccion, coneccion)

insertar.CommandText = "UPDATE Productos SET Found ='1' WHERE etiqueta_id ="
& tag_id
bien_encont = False
coneccion.Open()
lect = accesa.ExecuteReader()
While lect.Read()
    resultado = lect.GetString(4)
    tipod = lect.GetString(0)
    equipod = lect.GetString(1)
    componented = lect.GetString(2)
    seried = lect.GetString(3)
End While
If resultado = "" Then
    TextBox2.Text = "Etiqueta Sin Asociacion al Inventario"
Else
    If resultado = 0 Then
        bien_encont = True
        insertar.ExecuteNonQuery()
        etiqueta = etiqueta + 1
        TextBox1.Text = etiqueta
        TextBox2.Text = ("Tipo:" & tipod & vbCrLf &
"Equipo: " &
equipod & vbCrLf & "Componente: " & componented & vbCrLf &
"Serie:" & seried)
    End If
End If
```

Una vez que es encontrado cualquier bien, se le cambia el campo que indica bien encontrado para que posteriormente sean borrados de la base de datos los bienes que no contengan este cambio y de esta manera el archivo sólo contenga los bienes encontrados durante la realización del inventario.

# **Construcción y Resultados**

VI.1. Construcción del Dispositivo

VI.2. Pruebas y Resultados.

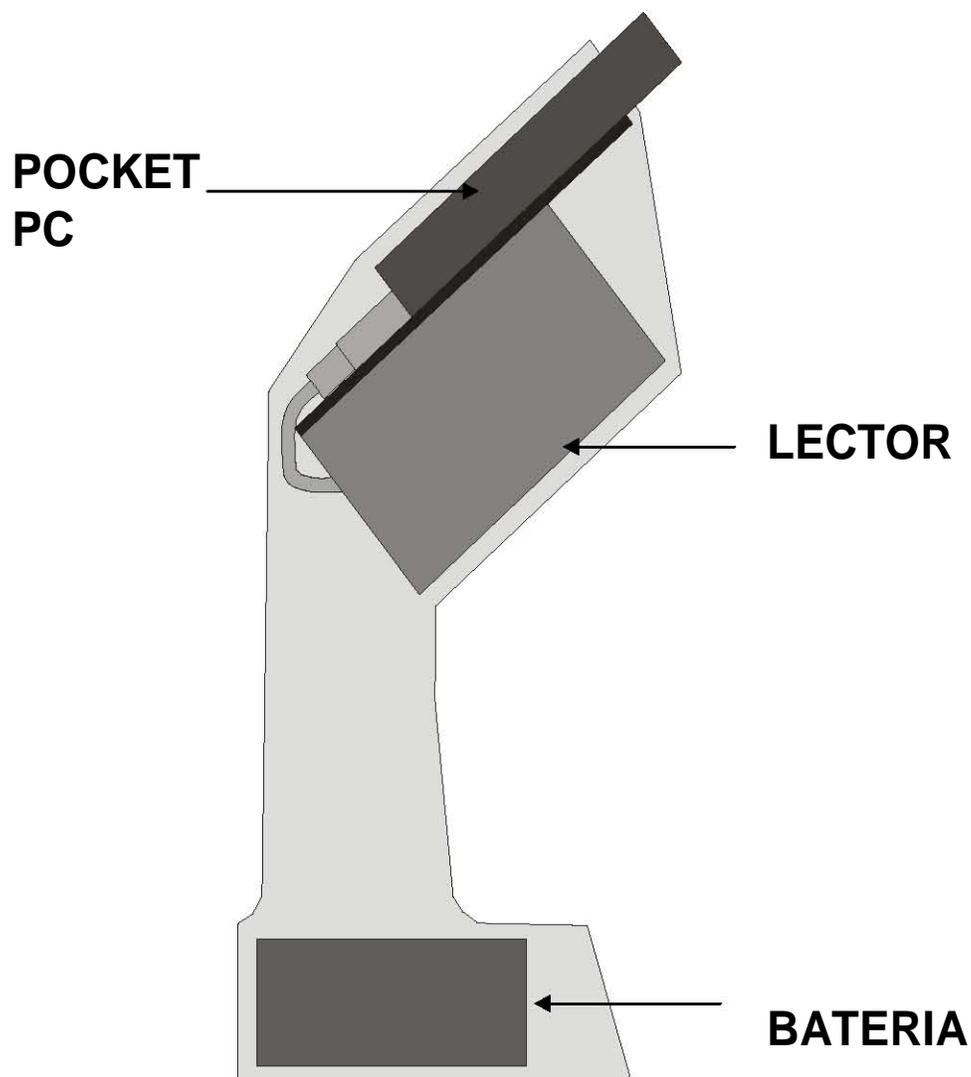
## **Capítulo 6**

## CONSTRUCCIÓN Y RESULTADOS

### VI.1 Construcción del Dispositivo

El dispositivo se diseñó para cumplir con las características de autonomía y ergonomía que facilitarían su manejo y que fuera fácilmente utilizable en áreas en donde pudieran faltar abastecimientos de energía eléctrica o con condiciones de uso rudo y sujetos a características ambientales similares a aulas o laboratorios de instituciones académicas.

El diseño final es el siguiente:



*Figura VI.1 Dispositivo para la Realización de Inventarios*

Como se puede observar en la figura VI.1, el dispositivo es fácilmente manejable con una mano y su forma se adaptó para que en su interior se colocaran de manera estratégica el dispositivo Lector, la Pocket PC y la Batería.

El dispositivo lector es una de las partes cuya ubicación es determinante para el funcionamiento del dispositivo, ya que dependiendo de ésta pudieran atenuarse las señales electromagnéticas, lo que pudiera impedir que se establezca el enlace con el Transponder.

Se escogió por lo tanto la posición mas externa posible y con mayor facilidad para el acercamiento a la etiquetas.

La batería se colocó en la base del dispositivo para que además facilitara su colocación en posición vertical y que además permitiera acoplar en el interior el circuito regulador de voltaje que proporciona la energía al Lector.

La Pocket PC se colocó en una posición de fácil visibilidad para el usuario y además con la característica de ser removible, lo que permite su utilización de manera rápida en aplicaciones y usos diferentes al levantamiento de inventarios. Este requerimiento obedece a la poca frecuencia en la que se realizan inventarios y a la rapidez con la que el dispositivo permite realizarlo. Además, en caso de falla de la Pocket PC, es muy fácil reemplazarla sin necesidad de cambios mayores ni en el diseño ni en el estado del dispositivo de inventarios.

Este punto resultó de gran importancia, ya que los usos que se le dan a las Pocket PC en el Laboratorio de Microsoft consisten principalmente en la experimentación y desarrollo de programas de software, lo que necesariamente requiere de la extracción y desacoplamiento de la Pocket PC.

Por otro lado, para la determinar el tipo de material que contendrá el dispositivo lector y por lo tanto la antena que emitirá las ondas electromagnéticas, es necesario considerar la propagación de éstas en distintos medios.

La transferencia de energía en un medio depende de ciertas propiedades electromagnéticas de éste, así como de propiedades similares del medio circundante. De esta forma, la transferencia de ondas electromagnéticas dependerá en diversos grados de las propiedades sobre el cual tiene lugar la transmisión.

Estas propiedades están definidas por los siguientes parámetros:

- Constante Dieléctrica  $\epsilon$ , (permitividad), es la capacidad de un medio para almacenar energía electrostática. Un dieléctrico es un material no conductor, esto es, un aislante. Buenos dieléctricos son el aire, hule, vidrio y mica por ejemplo.

- Permeabilidad  $\mu$  , es la medida de la superioridad de un material comparado con el vacío, para servir como trayectoria para líneas de fuerza magnética. Los materiales ferromagnéticos como el hierro, acero, níquel y cobalto poseen altas permeabilidades. Por otro lado sustancias diamagnéticas como el cobre, latón y bismuto tienen permeabilidades comparables a la del espacio libre.
- Conductividad  $\sigma$  , es la medida de la habilidad de un medio para conducir corriente eléctrica. Todos los metales puros son conductores, teniendo algunos mejor conductividad que otros. La conductividad es el recíproco de la resistividad y se mide en siemens (mhos).

Considerando la ecuación de una onda plana que viaja en la dirección  $+x$  y considerando sólo la componente en  $y$ , tenemos que:

$$E_y(x,t) = e^{-\alpha x} \operatorname{Re} \{ E_m e^{j(\omega t - \beta x)} \}$$

En donde  $E_m$  es la magnitud del campo,  $\omega$  es la frecuencia angular,  $\beta$  es la constante de fase y  $e^{-\alpha x}$  es la constante de atenuación.

En los buenos dieléctricos, se considera que:

$$\frac{\sigma}{\omega \epsilon} \ll 1$$

Por lo que:

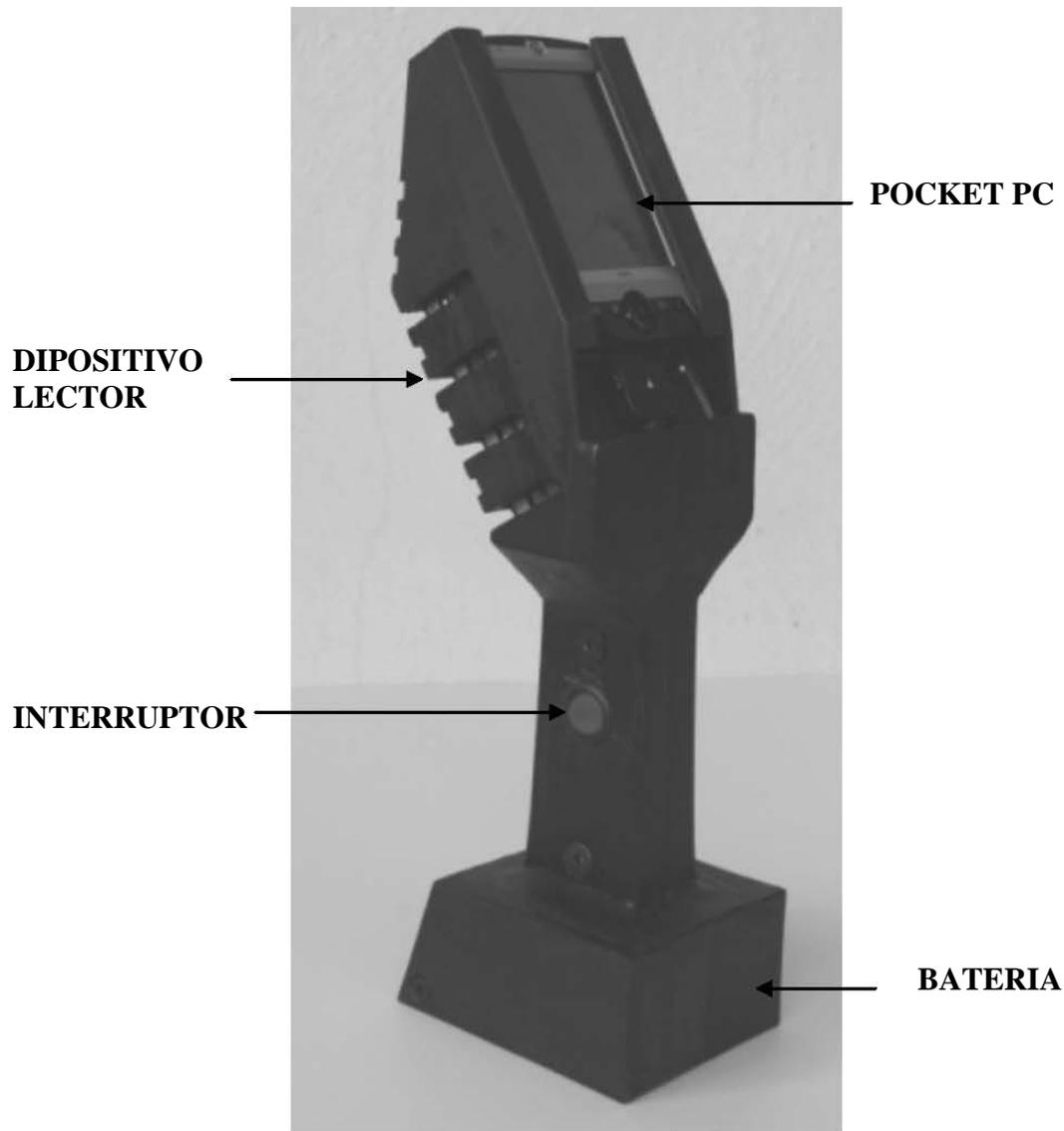
$$\alpha = (\sigma/2) \sqrt{\mu \epsilon}$$

Podemos concluir entonces que un buen dieléctrico tendrá un factor de atenuación bajo, permitiendo la transmisión máxima de las ondas electromagnéticas y un mayor rango de lectura de las etiquetas.

El Nylamid es un plástico a base de Nylon que posee mejores características comparado con otros materiales. Es muy fácil de maquinar, por lo que resulta muy económico y además posee características dieléctricas excelentes para los propósitos del presente proyecto. Además, es ligero y muy resistente por lo que cumple con las requisitos del presente proyecto de portabilidad y resistencia para el uso rudo.

Las características eléctricas del Nylamid incluyen una constante Dieléctrica de 4 a 4.4 y una resistividad de  $2.6 \times 10^{13}$  a  $5.5 \times 10^{13}$  ohm m, por lo que es un excelente dieléctrico muy adecuado para el material del prototipo a construir.

La figura VI.2 muestra el prototipo construido:



*Figura V.I Prototipo del Dispositivo RFID*

En la Figura V.I se puede apreciar que se hicieron ranuras en la parte que contiene al dispositivo Lector. Esto se realizó con los propósitos de facilitar la disipación de energía

térmica y al mismo tiempo de aumentar el rango de lectura ya que durante la fabricación fue difícil hacer una capa delgada del material sin comprometer la resistencia de la estructura.

## V.2 Pruebas y Resultados

Al tener el prototipo terminado, se grabaron 187 etiquetas con un número consecutivo al que se asoció con cada uno de los bienes existentes en el Laboratorio de Microsoft de la Facultad de Ingeniería incluyendo libros y manuales. Esta asociación se da a través de la base de datos que se mantiene fija y que sirve como base para la realización de diferentes inventarios y actividades que se encuentran disponibles en el sistema desarrollado. Se excluyeron de la base los bienes que por sus dimensiones no permitían la colocación de la etiqueta tales como los *Mouse* y las *Pocket PC*.

Se encontró que la posición de la etiqueta o transponder era un aspecto crítico ya que en los equipos de cómputo las partes de metal o de materiales conductores, tales como el chasis o las tarjetas electrónicas hacían difícil o imposible la lectura de los datos almacenados en la etiqueta.

En el caso de la Tablet PC disponibles en el Laboratorio, se encontró que el único lugar en donde es factible la lectura es la pantalla, aunque no es el lugar ideal ya que la pantalla es utilizada como área de contacto para introducir datos a la PC.

En algunos monitores se observó también que las áreas conductoras o metálicas abarcan prácticamente todo el aparato por lo que se requirió colocar las etiquetas en lugares que no son fácilmente accesibles por el lector, haciendo más lento también el proceso de lectura.

En los teclados de las PC disponibles se pudo colocar la etiqueta prácticamente en cualquier lugar, sin embargo la cercanía con la tarjeta conductora que contiene las pistas que transmiten la información de las teclas presionadas hizo que la lectura fuera lenta y que en ocasiones el dispositivo lector estuviera prácticamente pegado a la etiqueta.

En los libros o manuales se observó en uno de los casos que la cubierta contenía un tipo de pintura laminada o metalizada que imposibilitó de manera definitiva la lectura de la etiqueta. Las pruebas realizadas en este caso en particular incluyeron la colocación en diferentes partes del interior del libro y aún sobre la cubierta de libro sin resultados positivos.

En general, se observó que el alcance o rango de lectura del prototipo fue mucho menor a lo esperado debiéndose esto principalmente a las siguientes causas:

- El material seleccionado para la fabricación del prototipo presentó limitaciones para el grosor de la pared fuera muy delgado, por lo que el factor de atenuación aumentó y por lo tanto el rango de lectura o alcance disminuyó.

- La colocación de las etiquetas en el área donde el material permitía la lectura dio lugar a que la posición de éstas respecto al plano XY no fuera el mismo en todos los bienes. Dado que la polarización de las ondas electromagnéticas del dispositivo lector no es circular, fue necesario mover el dispositivo de posición hasta que el enlace se hacía posible.
- El medio en donde se encuentran los bienes contiene numerosas partes metálicas o conductoras que reflejan las ondas electromagnéticas cancelando en ocasiones la señal emitida debido a que la suma de las amplitudes de la onda reflejada y la onda emitida daba un resultado neto de cero o un valor muy bajo.

Por otro lado se observó en la mayoría de los casos que la lectura se pudo efectuar de una manera rápida y fácil, aún cuando no existía línea de vista entre el dispositivo lector y la etiqueta o transponder, resultando también en una disminución considerable de tiempo y disminuyendo los errores comparativamente con formas alternas de realizar inventarios.

Fue posible observar también que la parte del sistema encargada de localizar algún bien específico resultó de gran utilidad, ya que el software desarrollado permite buscar en la base únicamente los bienes que cumplan con una característica dada y a partir de esto seleccionar en la pantalla el bien. Los resultados obtenidos en las diferentes pruebas realizadas resultaron satisfactorios y no hubo confusiones o localizaciones falsas en ninguna de ellas.

En cuanto a las opciones disponibles en el software del sistema, tales como grabar, borrar o leer etiquetas, estas funcionaron sin problemas de consideración lo que permitió generar todas las etiquetas con los datos requeridos por el presente proyecto y hacer los cambios de acuerdo a las necesidades que se presentaron.

## CONCLUSIONES

Se logró plenamente el objetivo de la presente Tesis el cual se especificó como: " Al término de esta Tesis se dispondrá de un dispositivo que utilice la tecnología de RFID (Identificación por Radiofrecuencia) para realizar inventarios en el Laboratorio de Microsoft de la Facultad de Ingeniería. Este dispositivo será capaz de:

- Realizar el inventario de manera rápida sin que exista necesariamente línea de vista entre el dispositivo y los bienes.
- Leer y escribir en las tarjetas de RFID utilizadas para identificar los bienes.
- Será utilizado fácilmente en cualquier área de la Facultad de Ingeniería para la realización de Inventarios.
- Portátil.
- Localizar un bien en particular, indicándolo mediante una alarma audible y/o visual."

Los resultados obtenidos muestran claramente que el dispositivo cumple con todas las características planteadas al inicio del presente trabajo.

Queda sin embargo abierta la posibilidad de mejorarse el funcionamiento ya sea través del acoplamiento de antenas conjuntamente con amplificadores de la señal que permitan un alcance mayor .

El prototipo resultante puede modificarse en sus dimensiones a través de fuentes de poder alternativas o lectores de menores dimensiones que con seguridad saldrán al mercado o se podrán diseñar directamente en la Facultad de Ingeniería en proyectos futuros.

En su estado actual, el proyecto se puede escalar a un uso más generalizado extendiéndose su aplicación a la totalidad de los laboratorios e instalaciones de la Facultad así como a otras instalaciones tales como oficinas administrativas, bibliotecas, etc.

Quedan en poder de la Facultad de Ingeniería y específicamente al Laboratorio de Microsoft Research todos los componentes utilizados, que seguramente servirán como punto de partida a nuevas investigaciones y aplicaciones en la tecnología RFID cuyo uso se encuentra en crecimiento en estos días.

## COMANDOS DISPONIBLES EN EL SIRIT ST-200

| COMANDO  | CODIGO | DESCRIPCION   |
|----------|--------|---|
| DOWNLOAD | 0x00   | Descarga un nuevo software de aplicación al Módulo                    |
| SYSTEM   | 0x01   | Fija el modo del sistema operacional y obtiene versiones del software |
| TAG_0    | 0x02   | Comandos de etiqueta clase 0  |
| TAG_1    | 0x01   | Comandos de etiquetas clase 1   |

### Subcomandos Download

| COMANDO | CODIGO | DESCRIPCION  |
|---------|--------|--|
| NOTIFY  | 0x00   | Si la aplicación recibe este comando responderá y se reiniciará en el cargador. Si el cargador recibe este comando simplemente responderá. |
| START   | 0x01   | Notifica al cargador de borrar el área de aplicación de la memoria flash   |
| PROGRAM | 0x02   | Programa un mensaje de longitud variable en la memoria flash   |
| END     | 0x03   | Notifica al cargador que no hay mas mensajes de programación   |
| REBOOT  | 0x04   | Después de responder a este mensaje, el sistema se reiniciará.   |

### Subcomandos System

| COMANDO | CODIGO | TIPO DE COMANDO | DESCRIPCION  |
|---------|--------|-----------------|--|
| NO_CHG  | 0x00   | Modo            | El sistema no cambia (Solo sirve para verificar versiones) |
| STANDBY | 0x01   | Modo            | Procesador ON, Circuitos RF OFF                            |
| ENABLED | 0x02   | Modo            | Procesador, Circuitos Receptores y PLL ON. TX OFF          |
| RF_ON   | 0x80   | Prueba          | Enciende el transmisor de RF                               |

### Definiciones de Campos del Subcomando RF\_ON

| CAMPO             | VALOR        | DEFINICION                                    |
|-------------------|--------------|---|
| Nivel RF          | 0x00 -- 0x10 | 16 pasos de 1dBm cada uno de +15 dBm a 30 dBm |
| Freq Index        | 0 -- 50      | Tabla de índice de frecuencias                |
| Período de Espera | 0x00 -- 0xFF | Espera cada (n * 10) ms                       |

### Subcomandos Clase 0

| COMANDO | CODIGO | DESCRIPCION   |
|---------|--------|---|
| KILL    | 0xFF   | Destruye la etiqueta clase 0                                      |
| SET     | 0x00   | Se fija el nivel de potencia de RF y la profundidad de modulación |
| READ    | 0x01   | Lee el ID de la etiqueta utilizando los parámetros que le siguen  |

### Subcomandos Clase 1

| COMANDO    | CODIGO | DESCRIPCION   |
|------------|--------|---|
| KILL       | 0xFF   | Destruye la etiqueta clase 0  |
| SET        | 0x00   | Se fija el nivel de potencia de RF y la profundidad de modulación                                 |
| READ       | 0x01   | Lee el ID de la etiqueta utilizando los parámetros que le siguen                                  |
| PROGRAM_ID | 0X02   | Todas las etiquetas clase 1 que reciben este comando programarán el ID especificado en su memoria |
| VERIFY_ID  | 0X03   | Al recibir este comando, la etiqueta responde con el CRC, el ID de la etiqueta y la contraseña    |

**CODIGOS DE ERROR DEL SIRIT ST-200**

| <b>ERROR</b>          | <b>CODIGO DE ERROR</b> | <b>DESCRIPCIÓN</b>                                  |
|-----------------------|------------------------|---|
| ERR_NONE              | 0x00                   | No se encontraron errores o fallas                  |
| ERR_UNDEFINED         | 0xFF                   | Se encontró falla/error desconocido                 |
| ERR_INVALID_CMD       | 0xFE                   | Comando no reconocido                               |
| ERR_INVALID_PARAM     | 0xFD                   | Parámetro(s) del comando fuera de rango             |
| ERR_INSUFFICIENT_DATA | 0xFC                   | Datos insuficientes proporcionados con el comando   |
| ERR_ANT_FAULT         | 0xFB                   | Se detectó una falla en la antena                   |
| ERR_PLL_LOCK_FAIL     | 0xFA                   | Falla en el PLL                                     |
| ERR_DC_FAIL           | 0xF9                   | Voltaje de entrada fuera de rango (5%)              |
| ERR_RF_FAIL           | 0xF8                   | Baja potencia de RF                                 |
| ERR_OVR_TEMP          | 0xF7                   | Aislante del TX sobrecalentado                      |
| ERR_DNL_BAD_CRC       | 0xF6                   | Datos inválidos del CRC durante el comando Download |

**Bibliografía:**

- [1] Finkenzeller, K. *RFID Handbook*. Segunda Edición. 2004. John Wiley & Sons, Ltd. West Sussex. UK. 2-392.
- [2] Shepard, S. *RFID Radio frequency Identification*. Primera Edición. 2005. McGraw-Hill. New York, NY. 2-88.
- [3] Halvorson, M. *Microsoft Visual Basic.Net Step by Step*. Primera Edición. 2003. Microsoft Press. Redmond, WA. 3-335. 361-453.487-525.
- [4] Firtman, M. *Desarrollos Móviles Con .Net*. Primera Edición. 2005. MP Ediciones. Buenos Aires, Argentina. 242-298.
- [5] Wigley, A. Wheelwright, S. *Microsoft .Net Compact Framework*. Primera Edición. 2003. Microsoft Press. Redmond, WA.
- [6] Johnk, C.T.A. *Teoría Electromagnética*. Primera Edición. 1990. Limusa. México, D.F. 417-448.
- [7] Escobar Salguero, L. H. Cortés Soto, F. O. *Fundamentos de Teoría Electromagnética*. Primera Edición. 2000. Facultad de Ingeniería, UNAM. 81-95.
- [8] Krauss, J. D. *Antennas*. Segunda Edición. 1988. McGraw-Hill International Editions. Singapur. 17-82, 545.
- [9] Edminister, J.A. *Electromagnetismo*. Primera Edición. 1995. McGraw-Hill. Mexico, D.F. 181-188.

**Referencias Electrónicas:**

- [10] Adams, R. 03 de Junio de 2005. <http://www.adams1.com/pub/russadam/history.html>.
- [11] Amable, E. E.03 de Junio de 2005. <http://www.ent.ohiou.edu/~amable/autoid/history.htm>.
- [12] Taltech, I.S.S. 04 de Junio de 2005. [http://www.taltech.com/resources/intro\\_to\\_bc/bcbascs.htm](http://www.taltech.com/resources/intro_to_bc/bcbascs.htm).
- [13] A.I.M. 06 de Junio de 2005. <http://www.aimglobal.org/technologies/othertechnologies/ocr.pdf>.

- [14] S/A. 06 de Junio de 2005. <http://www.fombella.org/astic2005/Volumen%20III%20PDF/096.pdf#search='reconocimiento%20optico%20de%20caracteres'>.
- [15] Cardtech. 7 de Junio de 2005. <http://www.cardtech.com.mx/credenciales.php?opc= BMagnetica>
- [16] Neotec. 08 de Junio de 2005. <http://www.neotec.com.pa/pdf/introduccionalosbiometricos.pdf>.
- [17] Morales, D. Ruiz del Solar, J. 08 de Junio de 2005. [http://www2.ing.puc.cl/~iing/ed429/sistemas\\_biometricos.htm](http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm)
- [18] EPC Global. 17 de Junio de 2005. <http://www.epc.org.mx/contenido/EPCTagData Specification 11rev124.pdf>
- [19] Tagsys. 14 de Junio de 2005. [http://www.tagsys.net/eng/rfid/tagsys/rfid\\_tag-3-2.html](http://www.tagsys.net/eng/rfid/tagsys/rfid_tag-3-2.html)
- [20] Texas Instruments. 03 de Julio de 2005. <http://www.ti-rfid.com>
- [21] Philips. 04 de Julio de 2005. [http://www.semiconductors.philips.com/applications/smart\\_cards/index.html](http://www.semiconductors.philips.com/applications/smart_cards/index.html).
- [22] EPC Global. 06 de Julio de 2005. <http://www.epcglobalinc.org/>
- [23] Alien Technology. 06 de Julio de 1005. <http://www.alientechnology.com/webresources/datasheets/96bitDatasheet.pdf>
- [24] Marsh, M. 07 de Julio de 1005. <http://transpondernews.com/>
- [25] Skyetek. 13 de Julio de 2005. [http://www.skyetek.com/readers\\_M8.html](http://www.skyetek.com/readers_M8.html)
- [26] IEEE. 23 de Julio de 2005. <http://grouper.ieee.org/groups/802/11/>
- [27] CNet. 28 de Julio de 2005. <http://www.cnet.com>
- [28] Sun Microsystems. 20 de Agosto de 2005. <http://java.sun.com/products/jdk/1.3/docs/guide/jni>.
- [29] Menchaca Méndez, R. García Carballeira, F. 23 de Agosto de 2005. <http://www.revista.unam.mx/vol.1/num2/art4/>
- [30] Sun Microsystems. 24 de Agosto de 2005. <http://java.sun.com/j2me/docs/j2me-ds.pdf>

- [31] Microsoft. 02 de Septiembre de  
2005. <http://www.microsoft.com/net/Basics.aspx>