UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERÍA
ESCUELA DE ELECTRÓNICA

SISTEMA RFID, SU EVOLUCIÓN, APLICACIONES ACTUALES E INTEROPERATIVIDAD. DESARROLLO DE UNA APLICACIÓN: SISTEMA AUTOMATIZADO DE ACCESO A REDES.

TRABAJO DE GRADUACIÓN

PRESENTADO POR

Gilberto Azcúnaga Vargas	AV-000300
Carlos Armando Cornejo Garcia	CG-001065

PARA OPTAR AL GRADO DE

Ingeniero en Automatización

Asesor:
Ing. Carlos Giovanni Vásquez

Marzo de 2008

Soyapango – El Salvador – Centro América

UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERIA
ESCUELA DE ELECTRONICA

AUTORIDADES:

RECTOR
ING. FEDERICO HUGUET RIVERA

VICERRECTOR ACADEMICO
PBRO. VICTOR BERMÚDEZ, sdb

SECRETARIO GENERAL
LIC. MARIO RAFAEL OLMOS

DECANO DE FACULTAD DE INGENIERIA
ING. GODOFREDO GIRÓN

DIRECTOR DE ESCUELA DE ELECTRONICA
ING. OSCAR DURAN VIZCARRA

ASESOR DEL TRABAJO DE GRADUACION
ING. CARLOS GIOVANNI VÁSQUEZ

JURADO EVALUADOR
ING. JUAN CARLOS CASTRO CHÁVEZ

ING. MARCO TULIO PORTILLO GUEVARA
ING. RAFAEL COBOS MELENDEZ
UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERIA
ESCUELA DE ELECTRONICA

JURADO EVALUADOR DEL TRABAJO DE GRADUACION

Ing. Juan Carlos Castro Chávez
JURADO

Ing. Marco Tulio Portillo Guevara
JURADO

Ing. Rafael Cobos Meléndez
JURADO

Ing. Carlos Giovanni Vásquez
ASESOR

AGRADECIMIENTOS

Este logro es dedicado primeramente a Dios por darme la oportunidad de alcanzar una meta más en mi vida, por brindarme a las personas más indicadas y que me han sabído guiar a lo largo del camino, principalmente mis Padres, y en especial por permitirme compartir mi vida a lado de la mujer más luchadora e incansable, mi Madre, la cual sé que desde el cielo está orgullosa de mí, tengo la certeza que ésta meta cumplida es el reflejo por lo que tanto se sacrifico y le estoy agradecido.

A mis parientes y todas las personas que de una u otra forma me apoyaron incondicionalmente con su paciencia, amistad y comprensión a lo largo de la evolución de este proyecto y de mi carrera universitaria.

GILBERTO AZCÚNAGA VARGAS

AGRADECIMIENTOS

Los unicos que han hecho posible que haya llevado acabo este trabajo de graduación asi como mi carrera universitaria han sido mis padres, a los cuales les dedico este logro.

Les agradesco también a todos los que estuvieron pendientes del progreso de mi trabajo y me alentaron para seguir adelante pese a las adversidades, me aconsejaron y me apoyaron incondicionalmente.

Y le gradesco a Dios por permitirme lograr otra meta más en mi vida.

CARLOS ARMANDO CORNEJO GARCIA

Índice General de contenidos

INTRODUCCION

En la actualidad, RFID[1] es una tecnología que facilita el reconocimiento de objetos, animales y/o personas[2]. Esta usa señales de radio frecuencia de baja potencia para intercambiar datos de manera inalámbrica entre el dispositivo a identificar, conocido como *tag* y el dispositivo de lectura, conocido como *reader*. Una de las ventajas de esta tecnología es que no se requiere que haya línea vista entre el *tag* (usualmente compuesto por un chip con memoria EPROM) y el dispositivo de lectura.

Los lectores RFID pueden reconocer y procesar simultáneamente cientos de *tags* dentro de sus campos de lectura. Dicha tecnología ofrece un sistema único de localización en tiempo real que permite además monitorear cualquier parámetro referente al objeto que la contenga.

Los *tags* son realmente pequeños y tal como van los avances, en poco tiempo podrían ser considerados virtualmente invisibles. Se pueden colocar desde en botones de ropa o relojes, hasta implantados en animales y humanos. Su composición habitual es un chip de silicio que generalmente integra una antena y una pequeña memoria. Pero todo esto lo estudiaremos con más detalle posteriormente.

[1] **R**adio **F**recuency **ID**entification por sus siglas en inglés o identificación por radio frecuencia.
[2] Articulo: *federales aprueban implantes RFID en humanos,* autor: *Thomas C Greene*, publicación: *14/10/2004* (http://www.theregister.co.uk/2004/10/14/human_rfid_implants)

DEFINICION DEL TEMA

Se hará un estudio amplio y un análisis acerca de la tecnología RFID en procesos automatizados y en los campos de aplicaciones actuales, tales como la industria, medicina, etc. Además, en el documento se analizará la posibilidad de la coexistencia e interoperatividad entre las tecnologías de redes WLAN con RFID. También se analizará la migración de los sistemas actuales de identificación hacia los basados en radio frecuencia. Dicho análisis permitirá desarrollar una aplicación práctica en un sistema automatizado de acceso a una red LAN. Dicho acceso se hará en base a un sistema de identificación por radio frecuencia, mediante la lectura de los *tags* y un servidor de autenticación.

El funcionamiento será de la siguiente manera: el *reader* al detectar un *tag* valido, mandará información por el puerto RS-232 hacia el servidor de autenticación. Luego en éste, por medio de una interfaz de software que se desarrollará, se procesaran los datos recibidos del *reader* para validar la autenticación del usuario y así activar o no el puerto del switch. Si el usuario ha sido validado tendrá acceso a una terminal de la red LAN, pero no a la configuración del servidor.

JUSTIFICACION

A nivel mundial, la tecnología RFID está teniendo importancia en aplicaciones de seguridad y monitoreo a varios niveles. Y se está convirtiendo en la tecnología del futuro para la identificación, a tal punto de reemplazar el sistema actual de códigos de barras. Motivo por el cual se vuelve importante su utilización en la identificación.

El RFID ha penetrado fuertemente en el mercado. Actualmente grandes empresas[3], han optado por utilizar la tecnología RFID para reemplazar el sistema tradicional de códigos de barra para la identificación de productos.

OBJETIVOS GENERALES

En el presente trabajo de graduación se pretende dar a conocer los objetivos a cubrir en el desarrollo del documento final, los cuales se enuncian a continuación:

- Elaborar una documentación amplia de la tecnología de identificación por radio frecuencia.

- Llevar acabo un estudio de investigación de las tecnologías de redes inalámbricas existentes y su compatibilidad con RFID.

- Realizar un estudio comercial de la tecnología de identificación por radio frecuencia.

- Diseño e implementación de un sistema de que permita utilizar dispositivos de RFID, para poder tener acceso a un ambiente de redes.

[3]Articulo: *Wal-Mart Begins RFID Process Changes*, autor: *Mark Roberti* , fecha de consulta: *12/12/2006* (http://www.rfidjournal.com/article/articleview/1385/1/20/)
Articulo: *Honda UK to Track Components Through the Supply Chain*, autor: *Beth Bacheldor*, publicación: *Oct. 5, 2006* (http://www.rfidjournal.com/article/articleview/2703/1/1/)

OBJETIVOS ESPECIFICOS

- Realizar un documento profesional en el cual se haga un análisis amplio y una investigación extensa sobre el tema de RFID, desde el funcionamiento básico hasta sus aplicaciones.

- Dar una orientación técnica, basada en los puntos más relevantes del diseño y la arquitectura, que contribuyan en gran medida a la implementación de sistemas basados en identificación por radio frecuencia.

- Investigar la interoperatividad entre sistemas de identificación de radio frecuencia y sistemas de redes inalámbricas.

- Investigar la posibilidad de utilizar un *access-point* de redes inalámbricas como sistema lector de identificación por radio frecuencia.

- Establecer una base que sirva de referencia económica para la adquisición de equipos con RFID. La cual permitirá encontrar precios, proveedores, estándares y compatibilidades.

- Generar un estudio de factibilidad de inversión para la migración de sistemas de reconocimiento e identificación actuales en El Salvador, hacia los sistemas basados en RFID.

- Estandarizar el sistema de administración de privilegios de red con identificación de radio frecuencia. En el cual se puedan asociar diferentes niveles de privilegio mediante los *tags* o *transponders* de RFID.

- Realizar una interfaz que permita compartir información entre dispositivos RFID y un servidor de autenticación.

ALCANCES

- Poder realizar una base teórica sólida, sustentable y factible, sobre la implementación de sistemas RFID en El Salvador.

- Los protocolos de comunicación de redes inalámbricas que se abordarán en la investigación de interoperabilidad con RFID, serán únicamente Wi-Fi y Wi-Max.

- Los equipos de acceso a redes con los que se pretende desarrollar la aplicación serán dispositivos genéricos y se utilizarán en redes LAN. El protocolo de autenticación será administrado por un servidor.

- Todo el software que se utilizará e implementará en la aplicación, será de licencia publica preferiblemente.

- Los *tags* que se utilizaran para el reconocimiento basado en radio frecuencia serán de tipo pasivo, con una frecuencia de operación de 13.56Mhz, bajo un estándar ISO/IEC 14443A.

LIMITACIONES

- No se profundizará la investigación de temas básicos de redes por la basta información ya existente. Aunque sí se detallarán con especial cuidado los protocolos WLAN mas utilizados en la actualidad.

- No se detallarán los costos en los que se incurre para la fabricación de dispositivos RFID, sino más bien los precios de adquisición en el mercado en la última década, para la implementación de diversas aplicaciones.

- En el desarrollo de la aplicación el alcance máximo que se utilizará para la identificación entre el *reader* y el *tag* es de 5cm, debido al equipo con el que se hará la demostración y su frecuencia de operación.

- La aplicación a implementar se desarrollará con una red de 2 computadoras con sistema operativo Windows y un servidor, para cinco diferentes usuarios (asociados cada uno a un *tag*) que serán identificados por un *reader*. Además no se implementarán circuitos de control eléctrico debido al costo económico que esto implica.

- También en dicha aplicación se implementará una interfaz (basada en software) que permitirá procesar: los datos de RFID leídos por el *reader*, con el sistema de autenticación (vía puerto RS-232).

- Debido a la robustez que se requiere para la funcionalidad del servidor de autenticación actual, no se trabajará con las versiones mas completas de software para servidores.

VALIDACIONES

Debido a que el sistema propuesto esta pensado diseñarse bajo un estándar de autenticación funcional en el país, las configuraciones y protocolos de acceso a redes deben de ser compatibles con el estándar utilizado.

Debido a esto la funcionalidad de dicho sistema se comprobará en una red real, la cual contará de computadoras con sus respectivos sistemas operativos, observándose una completa interacción entre los dispositivos y los usuarios de la red.

Como el sistema poseerá adaptabilidad al entorno red, cualquier computadora que soporte el estándar Ethernet se podrá incorporar como otra estación de trabajo más.

CAPITULO 1: Marco teórico de RFID

1.1 Métodos de identificación

A lo largo de la historia se han utilizado diferentes mecanismos para identificar objetos, personas, animales y/o procesos. Entre los más comunes en los últimos años y de los más aceptados a nivel mundial es el de los códigos de barras.

1.1.1 Código de barras

El código de barras es un método de identificación el cual consiste en representar determinada información mediante líneas paralelas de diferente grosor y separación. La información es codificada en una secuencia de símbolos alfanuméricos basados en el código ASCII. Las barras verticales son la representación grafica de estas secuencias.

1.1.1.1 Características

El código de barras almacena datos que pueden ser reunidos de manera rápida y con precisión, al mismo tiempo que ofrecen un método simple y fácil para la codificación de información de texto que puede ser leída por lectores ópticos.

El lector decodifica el código de barras a través de la digitalización proveniente de una fuente de luz que cruza el código y mide la intensidad de la luz reflejada por los espacios blancos. El patrón de la luz reflejada se detecta a través de un fotodiodo, el cual produce una señal eléctrica que coincide exactamente con el patrón impreso del código de barras. Luego esta señal es decodificada de regreso de acuerdo con la información original por los circuitos electrónicos del dispositivo. Debido a que el diseño de muchas simbologías de código de barras no marca diferencia alguna, se puede digitalizar el código de barras de derecha a izquierda o viceversa.

Los Código de barras han sido creados para identificar objetos y facilitar el ingreso de información eliminando la posibilidad de error en la captura.

Su estructura básica consiste de zona de inicio y término en la que se incluye: un patrón de inicio, uno o más caracteres de datos, opcionalmente unos o dos caracteres de verificación y patrón de término. Esta ampliamente difundido en el comercio y en la industria, siendo que una computadora se conecta a través de la interfaz puerto de serie. Posibilita la recolección de datos con rapidez, muy baja tasa de errores, facilidad y bajo

costo, en comparación con la lectura visual de códigos numéricos seguida de entrada manual por teclado.

1.1.1.2 Historia y evolución de los códigos de barras

La primera patente para un código de barras, que tenía forma circular, fue solicitada en 1949 en Estados Unidos por N. J. Woodland; los códigos de barras se emplearon por primera vez a principios de la década de 1960 para identificar material rodante ferroviario. De ahí en adelante ha venido avanzando su aplicación y desarrollo.

Es así como en los 60's se dieron los siguientes eventos relacionados con los códigos de barras. En 1961, aparece el primer escáner fijo de códigos de barras instalado por Sylvania General Telephone. Este aparato leía barras de colores rojo, azul, blanco y negro identificando vagones de ferrocarriles. Para 1967 la Asociación de Ferrocarriles de Norteamérica (EEUU) aplica códigos de barras para control de tránsito de embarques. El proyecto no duró mucho por falta de adecuado mantenimiento de las etiquetas conteniendo los códigos.

Figura 1.1.a. Modelo de los primeros códigos de barras utilizados

A fines de los años 60 y comienzos de los 70 aparecieron las primeras aplicaciones industriales pero solo para manejo de información. En 1969, Rust-Oleum fue el primero en interactuar un lector de códigos con un computador (ordenador). El programa ejecutaba funciones de mantenimiento de inventarios e impresión de reportes de embarque.

En 1970 aparece el primer dispositivo portátil de datos fabricado por Norand. Este utilizaba un "*wand*" o lápiz de contacto.

El código Plessey hace su aparición en Inglaterra (The Plessey Company, Dorset, Inglaterra), para control de archivos en organismos militares en 1971. Su aplicación se difundió para control de documentos en bibliotecas.

Codabar aparece en 1971 y encuentra su mayor aplicación en los bancos de sangre, donde un medio de identificación y verificación automática era indispensable. En el mismo año la fábrica de carros Buick utilizó identificación automática en las operaciones de

ensamble de transmisiones. El sistema era utilizado para conteo de los diferentes tipos de transmisión ensamblados diariamente.

En 1973 aparece un estándar que regularía la información concerniente a los productos de consumo masivo, denominado UPC (*Universal Product Code*). De esta forma la actualización automática de inventarios permitiría una mejor y más oportuna compra y reabastecimiento de bienes. Europa se hace presente con su propia versión de UPC en 1976, con el denominado código EAN (*European Article Number* por sus siglas en ingles).

Figura 1.1.b. Ejemplo de los códigos de barra basados
En los estándares UPC y EAN

En 1974, el Dr. Allais conjuntamente con Ray Stevens de Intermec inventan el código 39, el primero de tipo alfanumérico. El primer sistema patentado de verificación de códigos de barras por medio de láser aparece en el mercado en 1978.

Figura 1.1.c. Código 39

En 1980 aparece el código denominado PostNet, siendo usado por el Servicio Postal de los EEUU.

Figura 1.1.d. Codigo PostNet

La tecnología de CCD (*Charge Coupled Device*) es aplicada en un escáner en 1981. En la actualidad este tipo de tecnología tiene bastante difusión en el mercado asiático, mientras que el láser domina en el mundo occidental. En ese año también aparece el código 128, de tipo alfanumérico.

Figura 1.1.e. Código 128

Aparece la norma ANSI MH10.8M que especifica las características técnicas de los códigos 39, Codabar, e ITF (*Interleaved Two of Five*).

El Dr. Allais en 1987 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 1.1.f. Código PDF417

1.1.1.3 Tipos de códigos de barras

Uno de los códigos de barras más comunes es el UPC. Emparentado con el UPC, existe el código ISBN, usado en la cubierta de libros y revistas, también de 12 dígitos, así como el código 39 codifica números y letras para usos generales, siendo muy popular. Este código se usa mucho en la industria y para inventarios.

Otro es el código entrelazado 2 de 5 (ITF), puede ser de cualquier longitud, pero con un número par de dígitos. Este es uno de los pocos códigos en que los espacios en blanco tienen significado.

También existen códigos de barra en 2 dimensiones, que se deben escanear mediante un escáner o una cámara fotográfica digital. Una de las más utilizadas es el símbolo internacional de número de artículo, llamado símbolo EAN.

Este símbolo se emplea en el comercio abierto para identificar los productos al pasar del fabricante a los mayoristas, distribuidores y minoristas, y de ahí al cliente final.

El código de barras EAN-13 representa el número de artículo indicado debajo del mismo, y no contiene ninguna información sobre el producto al que identifica. Toda la información sobre el producto figura en una base de datos, y se accede a ella indicando el número de artículo. Cada una de las empresas que utilizan el sistema EAN recibe un bloque de números de artículos que puede emplear para identificar todos sus productos. Estos bloques son asignados por una organización nacional de numeración, que a su vez recibe los números del organismo rector internacional, EAN Internacional.

Figura 1.1.g. Detalle de la información contenida en los códigos de barras EAN-13

Un símbolo de código de barras puede tener, a su vez, varias características, entre las cuales podemos nombrar:

Densidad:
Es la anchura del elemento (barra o espacio) más angosto dentro del símbolo de código de barras. Está dado en miles (milésimas de pulgada). Un código de barras no se mide por su longitud física sino por su densidad.

WNR: (Wide to Narrow Ratio)
Es la razón del grosor del elemento más angosto contra el más ancho. Usualmente es 1:3 o 1:2.

Quiet Zone:
Es el área blanca al principio y al final de un símbolo de código de barras. Esta área es necesaria para una lectura conveniente del símbolo.

1.1.2 Códigos magnéticos

1.1.2.1 Tarjetas en el ámbito financiero

1.1.2.1.1 Historia

La tarjeta magnética convencional se desarrolló a finales de los 60 para satisfacer varias necesidades. Una de ellas es permitir a los clientes de los bancos y entidades de ahorro activar y operar de forma rápida y efectiva con los cajeros automáticos. También, para

proporcionar un medio con el que operar en puntos de venta específicos. Aunque también se pueden ver estas tarjetas en los sistemas de transporte públicos en Europa, tanto en bus como en metro.

1.1.2.1.2 Características

El objetivo de esta tarjeta es identificar a un cliente para acceder a una base de datos remota con la que se establece una conexión. La información que posee la base de datos permite aceptar o rechazar esa transacción.

En la actualidad, la utilización de la tarjeta magnética se ha generalizado de tal forma que, al año, se producen y utilizan una media de 1400 millones de tarjetas[4] magnéticas en el mundo. Es por esto que su fabricación y diseño se ha debido de normar. Para tal fin se diseñaron los estándares ISO 7810, ISO 7811, ISO 7812, ISO 7813 y ISO 4909, los cuales regulan las propiedades físicas de las tarjetas, los tamaños, la ubicación de las cintas magnéticas, etc.

Las tarjetas magnéticas han producido importantes resultados en el mercado financiero pero no ofrecen soluciones para los nuevos mercados y servicios que aparecen: televisión interactiva, telefonía digital, etc.

El problema se debe a que las tarjetas magnéticas actuales se han utilizado para dar solución a problemas que aparecieron hace 25 años y están ligados a esas tecnologías: dependencias de ordenadores centrales y grandes redes dedicadas, a diferencia de los sistemas distribuidos actuales y de las nuevas soluciones. Además, la tarjeta magnética ofrece muy baja densidad de datos, baja fiabilidad y poca o ninguna seguridad en la información que lleva.

1.1.2.2 Tarjetas en el ámbito de telecomunicaciones

Sus usos fueron evolucionando, de tal forma que en 1975, se inventaron tarjetas telefónicas en Europa y no fue hasta 1986 que éstas aparecieron en EEUU. Estas tarjetas se pusieron en funcionamiento en Italia debido al vandalismo y al fraude que existía en esa época para la telefonía pública.

World Telecom Group introdujo las primeras tarjetas telefónicas con cinta magnética a gran escala en 1987. Luego en 1989, AT&T creó sus propias cartas las cuales fueron llamadas "*Remote Telecommunications Prepaid Calling Card*".

[4] Datos obtenidos para estadísticas del 2005 por IBM, principal fabricante e inventor de las cintas magnéticas.

1.1.2.3 Otros tipos de tarjetas magnéticas

La información en cintas magnéticas se utilizó o se sigue utilizando en varias aplicaciones, en diferentes ámbitos.

Tal como se mencionó con anterioridad, en el sistema de transporte público urbano actual europeo (Italia, Francia, España, etc.) se utilizan tiquetes impresos a los cuales se les adicionan cintas magnéticas. Estas permiten verificar el uso de los tiquetes y la validez de los mismos.

Pero también se pueden hallar estas cintas magnéticas en los boletos de las líneas aéreas actualmente. Por ejemplo los tiquetes de avión de KLM y Continental utilizan cintas magnéticas para guardar en sus registros la de sus clientes antes de abordar un avión. Esto se realiza automáticamente pasando el tiquete de vuelo por un lector magnético.

Pero también se utilizó para otros tipos de controles. Por ejemplo en los EEUU la Asociación Americana de Vehículos de Motores (AAMVA por sus siglas en ingles) regulo las normas para el uso de las licencias de conducir con cintas magnéticas. En la cual delimitó la información almacenada en cada una de las tres pistas de la cinta magnética.

1.1.2.4 Características de las tarjetas magnéticas

Las tarjetas magnéticas, son tarjetas a las cuales se les ha incorporado una banda magnética en el proceso de fabricación. Dicha banda sirve para poder colectar información de manera codificada con el fin de ser escrita y leída.

En la mayoría de estas tarjetas, la cinta magnética, contenida en una película de plástico, esta localizada en 5.66 mm al borde de la tarjeta y tiene un grosor de 9.52 mm. La cinta magnética contiene tres pistas, cada una de 2.79 mm de ancho.

Los estándares de las pistas magnéticas son los siguientes:

- ISO 1 (parte alta de la banda magnética): 79 caracteres alfanuméricos con densidad de encodaje 210bpi.
- ISO 2 (parte central de la banda): 40 caracteres numéricos con densidad de encodaje 75bpi.
- ISO 3 (parte baja de la banda) : 107 caracteres numéricos con densidad de encodaje 210bpi

El registro de los datos sobre una pista magnética, utiliza la propiedad que tienen algunos materiales de magnetizarse de manera duradera bajo la acción de un campo magnético.

Principio de funcionamiento:
El registro, o escritura, se efectúa por medio de un pequeño electroimán (la cabeza de escritura) que transforma una señal eléctrica emitida por el sistema electrónico de codificación en campo magnético variable Norte/Sur o Sur/Norte. El material magnético se magnetiza según el campo y conserva así el rastro de la señal. La lectura se efectúa según el mismo principio.

La codificación de los datos:
La norma ISO 7811 define precisamente las características de la banda magnética de una tarjeta de plástico. Una banda magnética tiene 3 pistas: en la pista 1 se pueden codificar caracteres alfanuméricos. En las pistas 2 y 3 solamente se pueden codificar caracteres numéricos.

El registro de los datos se efectúa en codificación binaria, la presencia o la ausencia de cambio del sentido de la magnetización sobre una zona elemental que se traduce en O ó 1. La frecuencia y el método de montaje de esta información constituyen la codificación de la pista magnética.

Características de las tarjetas con bandas magnéticas:
Las características físicas definen la posición y la forma de la banda magnética en la cual se trazarán las pistas. Para un buen funcionamiento, estos datos deben respetarse imperativamente. Además la resistencia a la abrasión de la superficie de la pista será un factor de confianza y de longevidad de la tarjeta, así como la manera en que la pista magnética se habrá depositado sobre la tarjeta. Se aconseja favorecer pistas integradas en el plástico (*Flush*) a las pistas pegadas a su superficie. Las características magnéticas esenciales de la banda son las 3 siguientes:
- El nivel de la magnetización remanente que se mide con relación a un juego de tarjetas de referencia normalizado. Es la capacidad de la pista magnética para devolver la señal registrada.
- La resolución define la aptitud del material magnético a soportar la densidad necesaria de transición de flujo sin error de interpretación de la codificación.
- La coercitividad medida en oersted o kiloamperio por metro es la medida de la resistencia al borrado de la codificación sobre una pista, por lo tanto un criterio de fiabilidad y perpetuidad de las tarjetas codificadas en explotación.

1.1.3 Métodos ópticos

El mas utilizado en la actualidad es el OCR (Reconocimiento Óptico de Caracteres por sus siglas en ingles). Básicamente se trata de un software el cual ha sido diseñado para convertir texto escrito a mano o en maquina a un archivo de texto editable por computadora.

1.1.3.1 Historia

En 1929, G. Tauschek obtuvo la patente de OCR en Alemania, seguido por Andel quien la obtuvo en 1933 en EEUU (U.S. Patent 1,915,993). Luego Tauscheck también obtuvo su patente en EEUU pero 2 años mas tarde (U.S. Patent 2,026,329).

El primer sistema comercial fue instalado en Readers Digest en 1955. Posteriormente *Standard Oil Company of California* empezó a utilizar dicho sistema para leer las impresiones de las tarjetas de crédito, con propósitos puramente de facturación.

El primer uso que se le dió a dicho sistema de identificación en Europa fue para *British General Post Office*, en 1965. Con este sistema se implementó un sistema tipo bancario de cobro.

1.1.3.2 Estado actual del OCR

La proporción de texto reconocido actualmente por ésta tecnología se encuentra entre el 80 y el 90, en el caso de caracteres escritos a mano con gran claridad y pulcritud, pero estos porcentajes disminuyen sensiblemente en el caso de los escaneos de texto y es muy frecuente encontrar docenas de errores por página escaneada. Este problema condiciona la tecnología OCR haciéndola una tecnología útil en un reducido número de contextos. Esta variedad de OCR se conoce comúnmente en la industria como ICR (*Intelligent Character Recognition*).
Los sistemas para el reconocimiento de los textos escritos a mano alzada en años recientes, han tenido algunos éxitos comerciales. Entre estos se encuentran los dispositivos conocidos como asistentes digitales personales tales como los que se encuentran instalados en el *Palm OS*. El *Newton* de *Apple* fue el pionero en este tipo de asistentes. Los algoritmos que usa el software de estos aparatos se aprovecha del hecho de que se conocen el orden, la velocidad y la dirección de los segmentos de línea como información de entrada. El usuario se puede entrenar y ayudar al dispositivo usando solamente formas específicas de letras. Estos mismos métodos no se pueden trasladar a los programas que se encargan de interpretar los caracteres de documentos escaneados y sigue siendo un problema de cierta forma.

1.1.4 Sistemas biométricos

La biométrica es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos de conducta o físicos intrínsecos. El término se deriva de las palabras griegas "bios" de vida y "metro" de medida.

En las tecnologías de la información (TI), la autentificación biométrica se refiere a las tecnologías para medir y analizar las características físicas y del comportamiento humanas con propósito de autentificación.

Las huellas dactilares, las retinas, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, representan ejemplos de características físicas (estáticas), mientras que entre los ejemplos de características del comportamiento se incluye la firma, el paso y el tecleo (dinámicas). La voz se considera una mezcla de características físicas y del comportamiento, pero todos los rasgos biométricos comparten aspectos físicos y del comportamiento.

1.1.4.1 Historia

La biométrica no se puso en práctica en las culturas occidentales hasta finales del siglo XIX, pero era utilizada en China desde al menos el siglo XIV. Un explorador y escritor que respondía al nombre de Joao de Barros escribió que los comerciantes chinos estampaban las impresiones y las huellas de la palma de las manos de los niños en papel con tinta. Los comerciantes hacían esto como método para distinguir entre los niños jóvenes.

En Occidente, la identificación se basaba simplemente en la "memoria fotográfica" hasta que Alphonse Bertillon, jefe del departamento fotográfico de la Policía de París, desarrolló el sistema antropométrico (también conocido más tarde como Bertillonage) en 1883. Este era el primer sistema preciso, ampliamente utilizado científicamente para identificar a criminales y convirtió a la biométrica en un campo de estudio. Funcionaba midiendo de forma precisa ciertas longitudes y anchuras de la cabeza y del cuerpo, así como registrando marcas individuales como tatuajes y cicatrices. El sistema de Bertillon fue adoptado extensamente en occidente hasta que aparecieron defectos en el sistema principalmente problemas con métodos distintos de medidas y cambios de medida. Después de esto, las fuerzas policiales occidentales comenzaron a usar la huella dactilar esencialmente el mismo sistema visto en China cientos de años antes.

En estos últimos años la biométrica ha crecido desde usar simplemente la huella dactilar, a emplear muchos métodos distintos teniendo en cuenta varias medidas físicas y de comportamiento. Las aplicaciones de la biometría también han aumentado - desde sólo identificación hasta sistemas de seguridad y más.

1.1.4.2 Los diferentes sistemas

2.1.4.2.1 Diferencias

Lo que sigue a continuación es una tabla en la que recogen las diferentes características de los sistemas biométricos:

	Ojo (Iris)	**Ojo (Retina)**	**Huellas dactilares**	**Geometría de la mano**	**Escritura y firma**	**Voz**	**Cara**
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Media	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Muy alta	Alta	Alta	Media	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta	Muy alta
Estabilidad	Alta	Alta	Alta	Media	Baja	Media	Media

Tabla 1.1.a Diferencias entre los diferentes tipos de sistemas biométricos

1.1.4.2.2 Reconocimiento ocular

Los patrones de reconocimiento oculares se dividen en 2 tecnologías diferentes: análisis de patrones retinales y análisis del iris. Estos métodos suelen ser los considerados mas confiables. La probabilidad, entre una población de 200,000,000 es de 0 coincidencias. Además una vez muerto el individuo, los tejidos oculares se degeneran rápidamente, lo que hace mas difícil poder intentar burlar un sistema de reconocimiento de este tipo.

A. Retina

En lo que respecta a los análisis de retina el proceso es el siguiente: el usuario a identificar ha de mirar a través de unos binoculares, ajustar la distancia ínter ocular y el movimiento de la cabeza, mirar a un punto determinado y por último pulsar un botón para

indicar al dispositivo que se encuentra listo para el análisis. En ese momento se escanea la retina con una radiación infrarroja de baja intensidad en forma de espiral, detectando los nodos y ramas del área retinal para compararlos con los almacenados en una base de datos.

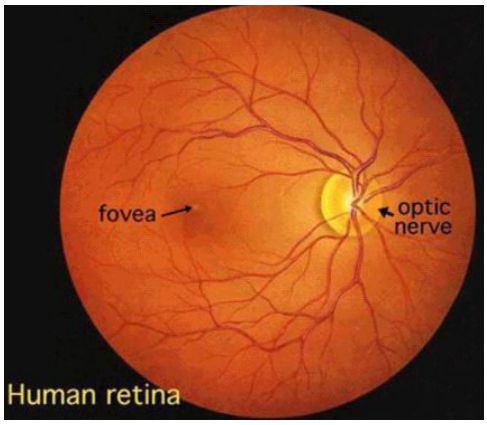


Figura 1.1.h. Retina humana

B. Iris

La identificación basada en el reconocimiento de iris es más moderna que la basada en patrones retinales; desde hace unos años el iris humano se viene utilizando para la autenticación de usuarios. El procedimiento que se sigue es el siguiente: se captura una imagen del iris en blanco y negro, en un entorno correctamente iluminado; esta imagen se somete a deformaciones pupilares (el tamaño de la pupila varía enormemente en función de factores externos, como la luz) y de ella se extraen patrones, que a su vez son sometidos a transformaciones matemáticas hasta obtener una cantidad de datos (típicamente 256 KBytes) suficiente para los propósitos de autenticación. Esa muestra, denominada *iriscode* (en la figura 2.1.i se muestra una imagen de un iris humano con su *iriscode* asociado) es comparada con otra tomada con anterioridad y almacenada en la base de datos del sistema, de forma que si ambas coinciden el usuario se considera autenticado con éxito; la probabilidad de una falsa aceptación es la menor de todos los modelos biométricos.

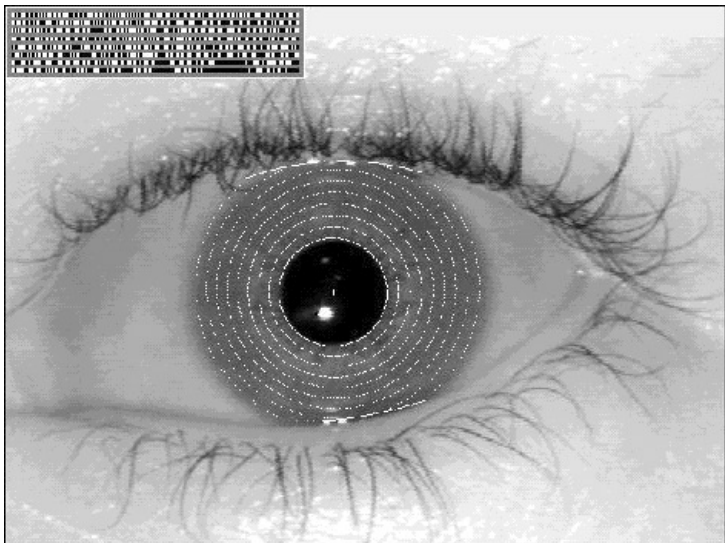


Figura 1.1.i. Iris del ojo humano.

1.2 RFID

1.2.1 Evolución del RFID

En años recientes los procedimientos de identificación automática (*Auto-ID*), han cobrado gran relevancia en muchas industrias de servicios, compra y logística de la distribución, compañías industriales y sistemas de flujo de material. La existencia de los procedimientos de identificación automática para proveer información acerca de personas, animales y transacciones de productos.

Las etiquetas omnipresentes de código de barras que revolucionaron los sistemas de identificación hace algún tiempo considerable, están empezando a considerarse inadecuadas en un aumentado numero de casos. El código de barras puede ser sumamente barato, pero su principal debilidad reside en su baja capacidad de almacenamiento y el hecho de no poder reprogramarse para contar con una base de datos dinámica. La solución técnica optima seria el almacenamiento de datos en un *chip* de silicón.
En la vida cotidiana la forma mas común de almacenamiento de datos en un dispositivo electrónico son las tarjetas inteligentes (*smart card*) implementadas en las tarjetas telefónicas y tarjetas bancarias, sin embargo el contacto mecánico usado en las tarjetas inteligentes es a menudo impractico. Un *contactless* transfiere datos entre dispositivos de acarreo de datos y su lector es mas flexible. En el caso ideal, la energía necesaria para poder operar el dispositivo electrónico de acarreo de datos puede ser transferida desde el lector utilizando tecnología *contactless*. Debido a los procedimientos utilizados para la

transferencia de alimentación y datos los sistemas de identificación *contactless* son llamados sistemas RFID (Identificación por Radio Frecuencia)

Además en años recientes la tecnología de identificación *contactless* se ha estado desarrollando en un campo interdisciplinario independiente, en el que ya no encaja en cualquiera de los sistemas convencionales, esta reúne varios elementos de campos sumamente variados, de tecnología HF y EMC, tecnología de semiconductor, protección de datos y criptografía, telecomunicaciones, tecnología manufacturera, y muchas otras áreas relacionadas.

Para ayudar a la comprensión del funcionamiento de la tecnología de identificación por radio frecuencia en la sección siguiente da una apreciación global breve de sistemas de ID automáticos diferentes que realizan funciones similares a RFID.

1.2.2 Sistemas RFID

Los sistemas de RFID se relacionan estrechamente a las tarjetas inteligentes descritas anteriormente. Como los sistemas de tarjetas inteligentes (*Smart Card),* los datos son almacenados en un dispositivo electrónico de acarreo de datos (*transponder*), sin embargo a diferencia e las tarjetas inteligentes, el suministro de poder al dispositivo transportador de datos (*data carrying*) y el intercambio de datos entre el dispositivo transportador de datos y el lector se logra sin el uso de contactos galvánicos, usando campos magnéticos o electromagnéticos en cambio. El procedimiento técnico subyacente es deducido de los campos de radio y radar.
La abreviación que RFID simboliza es identificación de frecuencia de radio, es decir información llevada por radio-ondas.
Debido a las numerosas ventajas de sistemas de RFID comparadas con otros sistemas de identificación, los sistemas de RFID están empezando a conquistar nuevos mercados de masas. Un ejemplo es el uso de *contactless* tarjetas inteligentes como boletos para transporte público de corta distancia.

1.2.3 Componentes de un sistema de RFID

Un sistema de RFID siempre se compone de dos componentes (Figura 1.2.a)

- el *transponder* que se localiza en el objeto a ser identificado
- el interrogador o lector (*Reader*) que dependiendo del diseño y la tecnología usada puede ser que sea un dispositivo de lectura o de lectura/escritura (para la familiarización de las nomenclaturas en este trabajo de graduación siempre llamaremos al lector como *reader* sin tomar en cuenta si solo puede leer los datos o si también puede ser capaz de realizar procedimientos de escritura

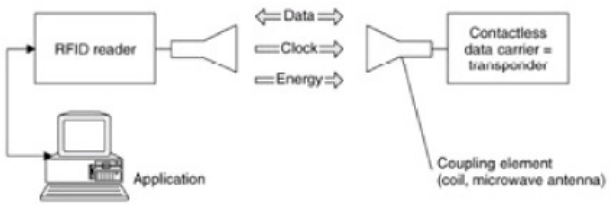


Figura 1.2.a El *reader* y el *transponder* son los componentes principales de cada sistema de RFID.

Típicamente un *reader* contiene un módulo de frecuencia de radio (transmisor y receptor), una unidad de mando y un elemento de acoplamiento al *transponder*.
Además, muchos *reader* se ajustan con un interface adicional (RS 232, RS 485, etc.) que les permite que remitan los datos recibidos a otro sistema (PC, sistema de mando de robot, etc.).

El *transponder* que representa el dispositivo de acarreo de datos real de un sistema de RFID normalmente consiste en un elemento de acoplamiento y un microchip electrónico (Figura 1.2.b).
Cuando el *transponder* que normalmente no posee su propio suministro de voltaje (batería), no está dentro de la zona de la interrogación de un lector es totalmente pasivo.
El *transponder* sólo se activa cuando está dentro de la zona de la interrogación de un *reader*. La energia requerida para la activacion del *transponder* es suministrada atraves de la unidad de acoplamiento (contactless), como el pulso cronometrando y datos.

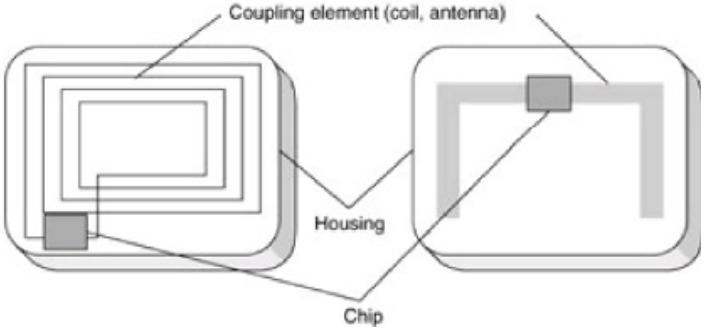


Figura 1.2.b esquema básico de dispositivo transportador de datos RFID. El *transponder* izquierdo acoplado inductivamente con enrollado de antena el *transponder* derecho con microondas por medio de una antena bipolar.

1.3 Principios físicos de RFID

Debido a que la gran mayoría de sistemas de RFID basan su funcionamiento en el accionar de campos magnéticos (sobre todo al acoplamiento inductivo), se estudiará en

este apartado los conceptos físicos de los campos magnéticos desde el punto de vista de RFID.

1.3.1 Campos magnéticos

Un campo magnético es un campo de fuerza creado por el movimiento de cargas eléctricas. La magnitud de un campo magnético esta definida por la fuerza del campo magnético, denotada por H. La intensidad de un campo se mide en Gauss (G) o en Tesla (T).

El campo magnético es producido por una corriente eléctrica, la cual da lugar a un campo magnético estático. También es producido por una corriente de desplazamiento la cual origina un campo magnético variante en el tiempo.

Un campo magnético puede ser producido por un campo eléctrico variable, y viceversa. Los campos eléctricos ejercen fuerzas sobre las partículas cargadas por el simple hecho de tener carga, independientemente de su velocidad; los campos magnéticos sólo ejercen fuerzas sobre partículas cargadas en movimiento.

Estos hallazgos cualitativos fueron expresados en una forma matemática precisa por el físico británico James Clerk Maxwell, que desarrolló las ecuaciones diferenciales en derivadas parciales que llevan su nombre. Las ecuaciones de Maxwell relacionan los cambios espaciales y temporales de los campos eléctrico y magnético en un punto con las densidades de carga y de corriente en dicho punto. En principio, permiten calcular los campos en cualquier momento y lugar a partir del conocimiento de las cargas y corrientes.

La integral de contorno de la fuerza del campo magnético a lo largo de una curva cerrada es igual a la suma de las fuerzas de las corrientes dentro de él.
De tal forma que para calcular H para diferentes tipos de conductores se tiene la siguiente formula:

$$\sum I = \oint \vec{H} \cdot \vec{d}s$$

En 1887, el físico alemán Heinrich Hertz consiguió generar físicamente esas ondas por medios eléctricos, con lo que sentó las bases para la radio, el radar, la televisión y otras formas de telecomunicaciones.

El comportamiento de los campos eléctrico y magnético en estas ondas es bastante similar al de una cuerda tensa muy larga cuyo extremo se hace oscilar rápidamente hacia arriba y hacia abajo.

Cualquier punto de la cuerda se mueve hacia arriba y hacia abajo con la misma frecuencia que la fuente de las ondas situada en el extremo de la cuerda. Los puntos de la cuerda situados a diferentes distancias de la fuente alcanzan su máximo desplazamiento vertical en momentos diferentes.

Cada punto de la cuerda hace lo mismo que su vecino, pero lo hace algo más tarde si está más lejos de la fuente de vibración (véase Oscilación). La velocidad con que se transmite la perturbación a lo largo de la cuerda, o la `orden' de oscilar, se denomina velocidad de onda. Esta velocidad es función de la densidad lineal de la cuerda (masa por unidad de longitud) y de la tensión a la que esté sometida.

Una fotografía instantánea de la cuerda después de llevar moviéndose cierto tiempo mostraría que los puntos que presentan el mismo desplazamiento están separados por una distancia conocida como longitud de onda, que es igual a la velocidad de onda dividida entre la frecuencia.

En 1819, el físico danés Hans Christian Oersted llevó a cabo un importante descubrimiento al observar que una aguja magnética podía ser desviada por una corriente eléctrica. Este descubrimiento, que mostraba una conexión entre la electricidad y el magnetismo, fue desarrollado por el científico francés André Marie Ampère, que estudió las fuerzas entre cables por los que circulan corrientes eléctricas, y por el físico francés Dominique François Arago, que magnetizó un pedazo de hierro colocándolo cerca de un cable recorrido por una corriente.

Así, Oersted demostró que una corriente eléctrica crea un campo magnético, mientras que Faraday demostró que puede emplearse un campo magnético para crear una corriente eléctrica. La unificación plena de las teorías de la electricidad y el magnetismo se debió al físico británico James Clerk Maxwell, que predijo la existencia de ondas electromagnéticas e identificó la luz como un fenómeno electromagnético. Los estudios posteriores sobre el magnetismo se centraron cada vez más en la comprensión del origen atómico y molecular de las propiedades magnéticas de la materia. En 1905, el físico francés Paul Langevin desarrolló una teoría sobre la variación con la temperatura de las propiedades magnéticas de las sustancias paramagnéticas (ver más adelante), basada en la estructura atómica de la materia.

Las llamadas bobinas cilíndricas cortas o conductores cerrados se utilizan como antenas magnéticas para generar el campo magnético alternante en los dispositivos de lectura y escritura de los sistemas inductivos de RFID. Tal como se muestra en la figura siguiente:

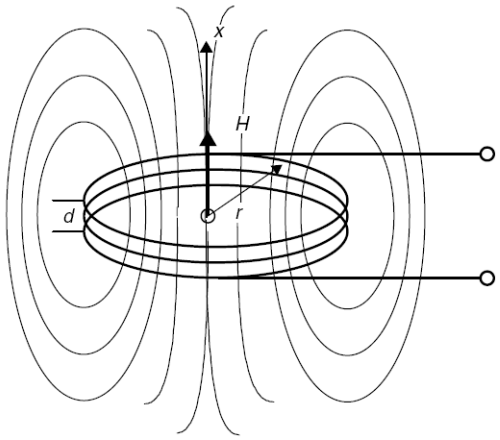


Figura 1.3.a. La trayectoria de las líneas del flujo magnético alrededor de la bobina cilíndrica corta o conductores cerrados, es similar a las antenas empleadas en los transmisores de los sistemas inductivos de RFID

Si el punto donde se mide H se aleja del centro de la bobina, a lo largo del eje x entonces el valor de H disminuirá a medida que el valor de x aumente. La fuerza del campo en relación con el área (radio) de la bobina se mantiene constante hasta cierta distancia, luego cae su valor rápidamente.

En el espacio libre, la caída de la fuerza del campo magnético es de aproximadamente 60dB por década, en las cercanías del campo de la bobina. Y es de aproximadamente 20 dB por década en un campo lejano de la onda electromagnética generada. Aunque estos datos son para bobinas cilíndricas, también se puede calcular H para bobinas rectangulares de dimensiones a x b, con la siguiente ecuación:

$$H = \frac{N \cdot I \cdot ab}{4\pi\sqrt{\left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2 + x^2}} \cdot \left(\frac{1}{\left(\frac{a}{2}\right)^2 + x^2} + \frac{1}{\left(\frac{b}{2}\right)^2 + x^2} \right)$$

Esta es la ecuación que se utiliza generalmente para una antena transmisora. Donde N representa el número de vueltas de la bobina. En base a esta formula se puede concluir que la fuerza del campo decae en distancias cortas de la bobina que actúa como antena. Sin embargo la antena más pequeña presenta una fuerza perceptiblemente más alta del campo en el centro de la antena, pero para distancias más grandes una antena mas grande genera una fuerza de campo significativamente mas grande. Es esencial que este efecto sea tomado en cuenta para el diseño de antenas de los sistemas inductivos de RFID.

1.3.2 Flujo magnético y densidad de flujo magnético

El flujo magnético esta representado por líneas de fuerza magnéticas. El número total de líneas de fuerza creadas por un campo magnético se denomina flujo magnético y esta

representado por Φ. Por lo tanto Φ = **B**. **S**, donde S es el área de la sección y B es la densidad de campo magnético (o líneas de fuerza magnética).

Si consideramos una tarjeta RFID, la cual contiene N numero de espiras, el flujo Φ del campo magnético, a través de las N espiras es: Φ = N**B**. **S**

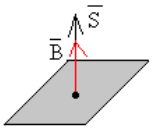


Figura 1.3.b Vectores de campo magnético

1.3.3 Inducción electromagnética

Es el fenómeno que da origen a la producción de una fuerza electromotriz (denominada comúnmente como f.e.m.) o voltaje, en un cuerpo expuesto a un campo magnético variable; o bien el caso opuesto, en un medio móvil respecto a un campo magnético estático.

Cuando el cuerpo es un conductor, se genera una corriente inducida, la cual se opone al cambio de flujo magnético.

1.3.4 Inductancia

Una bobina o inductor, tiene la propiedad de oponerse a cualquier cambio en la corriente que pasa a través de él. A esta propiedad se le denomina inductancia y se representa por la letra: L. Esta oposición genera un retardo en el paso de la corriente que circula por el inductor. Dicho retardo esta acompañado por absorción o liberación de energía y se asocia con el cambio en la magnitud del campo magnético que rodea los conductores.

La inductancia depende de las características físicas del conductor y de su tamaño.
Cuando una corriente I atraviesa un conductor, un campo magnético es creado. Las líneas de fuerza del campo magnético se expanden desde el centro del conductor hacia afuera.

La unidad de inductancia es el henrio. Los valores de inductancia utilizados en equipos dé radio varían en un margen amplio. En circuitos de radiofrecuencia, los valores de inductancia empleados se medirán en milihenrios (1 mH es una milésima de henrio) en frecuencias bajas, y en microhenrios (millonésima de henrio) en las frecuencias medias y altas. Aunque las bobinas para radiofrecuencia pueden bobinarse sobre núcleos de hierro especiales (el hierro común no es adecuado), muchas de las bobinas utilizadas por los

aficionados son del tipo de núcleo de aire, o sea, bobinadas en un material de soporte no magnético.

Cualquier conductor tiene inductancia, incluso cuando el conductor no forma una bobina. La inductancia de una pequeña longitud de hilo recto es pequeña, pero no despreciable si la corriente a través de él cambia rápidamente, la tensión inducida puede ser apreciable. Este puede ser el caso de incluso unas pocas pulgadas de hilo cuando circula una corriente de 100 MHz o más. Sin embargo, a frecuencias mucho mas bajas la inductancia del mismo hilo puede ser despreciable, ya que le tensión inducida será despreciablemente pequeña.

1.3.5 Inductancia en un conductor de lazo cerrado

Si se asume que el diámetro *d* del alambre utilizado es muy pequeño comparado con el diámetro *D* de la bobina del conductor (*d/D* < 0.0001), entonces se puede hacer la siguiente aproximación:

$$L = N^2 \mu_0 R \cdot \ln\left(\frac{2R}{d}\right)$$

Donde *R* es el radio del lazo del conductor.

1.3.6 Ley de Faraday

La ley de Faraday describe la inducción electromagnética sobre la cual se basa el funcionamiento de un generador eléctrico, el transformador y otros dispositivos.

Si el flujo de campo magnético a través de un circuito varía con el tiempo, mientras dura ésta variación, se da una corriente en el circuito. La variación del flujo magnético da lugar a una fuera electromotriz inducida denominada: fem inducida. Es debido a ésta fuerza que aparece una corriente en dicho circuito.

Si se coloca un conductor eléctrico en forma de bpbina en una región en la que hay un campo magnético. Si el flujo F a través de la bobina varía con el tiempo, se puede observar una corriente en la bobina (mientras el flujo está variando). Midiendo la fem inducida se encuentra que depende de la rapidez de variación del flujo del campo magnético con el tiempo:

$$\varepsilon_{ind} = -\frac{d\Phi}{dt}$$

El signo menos indica que la fem inducida (y por ende la corriente inducida) tiene un sentido que se opone al cambio que la provoca, resultado que se conoce con el nombre de

Ley de Lenz. De tal forma que que si el grupo magnético a través de la bobina aumenta, la corriente inducida toma un sentido que se opone a éste cambio, tratando de hacer disminuir el flujo magnético. Si por el contrario el flujo disminuye la corriente inducida se opone a éste cambio tomando un sentido que trata de hacer aumentar el flujo magnético a través de la bobina.

1.3.7 Resonancia

El voltaje inducido U2 en la antena del *transponder* es usado como fuente de energía necesaria para el chip en su proceso de almacenamiento de datos en memoria. Para mejorar la eficiencia un capacitor C2 se conecta en paralelo con la bobina del transponder L2, tal como se muestra en la siguiente figura:

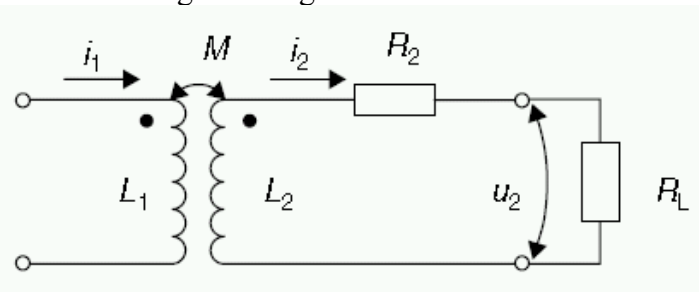


Figura 1.3.c. Circuito equivalente para un par de conductores

De manera que forma un circuito paralelo resonante con una frecuencia resonante que es la frecuencia de operación del sistema de RFID. La frecuencia resonante se puede calcular mediante la siguiente formula:

$$f = \frac{1}{2\pi\sqrt{L_2 \cdot C_2}}$$

En la práctica existe una capacitancia parásita, para la cual se utiliza un capcitor Cp. El cual se relaciona de la siguiente manera:

$$C_2' = \frac{1}{(2\pi f)^2 L_2} - C_p$$

Donde $C_2 = (C_2' + C_p)$

Por lo que el circuito equivalente real de un *transponder* sería:

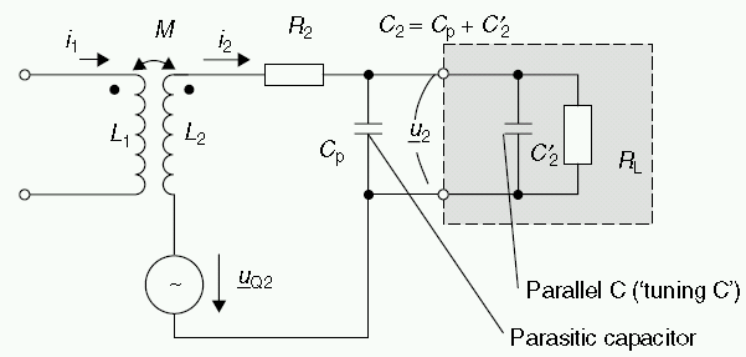


Figura 1.3.d circuito equivalente real de un transponder

Donde R2 es la resistencia natural de la bobina del tag L2 y la resistencia de carga Rl representan el consumo de corriente que se genera cuando se utiliza el chip para transmitir datos.

1.4 Arquitectura de RFID

Arquitectura de los portadores electrónicos de datos.

Antes de describir la funcionalidad de los portadores de datos utilizando RFID primero se debe establecer una diferencia entre dos principios de operación:

- Los portadores electrónicos de datos basados en circuitos integrados (microchips).
- Portadores de datos que se aprovechan de efectos físicos para el almacenamiento de los datos. *transponders* 1-bit y "componentes de superficie de onda pertenecen a la última categoría.

Los portadores electrónicos de datos se subdividen después en los portadores de datos con pura función de memoria incorporando un microprocesador programable.

1.4.1 Transponder con función de memoria.

Los *transponders* con función de memoria, van desde un simple *transponder* de solo lectura hasta el transponder de alta tecnología con funciones de criptografía inteligente.
Los *transponders* con una función de memoria contienen RAM, ROM, EEPROM o FRAM y una interfaz de HF para proporcionar el suministro de energía que permita la comunicación con el lector. La característica principal que distingue esta familia de *transponders* es la elaboración de direccionamiento y lógica de seguridad en el chip que usa la maquina de estado.

1.4.1.1 Interfaz de alta frecuencia, HF

La interfaz HF unifica formas de interfaz análogas entre el canal de alta frecuencia de transmisión desde la circuiteria digital del *reader* hasta la ROM del *transponder*.
La interfaz HF por consiguiente realiza la unión de las funciones de un módem clásico (modulador–demodulador) que realizaba la transmisión análoga de datos por la línea telefónica.
La señal modulada en HF desde el *reader* se reconstruye en la interfaz de HF por demodulación para crear cadenas de datos digitales seriales reprocesando el direccionamiento y lógica de seguridad.
Un circuito de reloj interno genera pulsos de sincronismo para el portador de datos desde la frecuencia portadora del campo de HF.

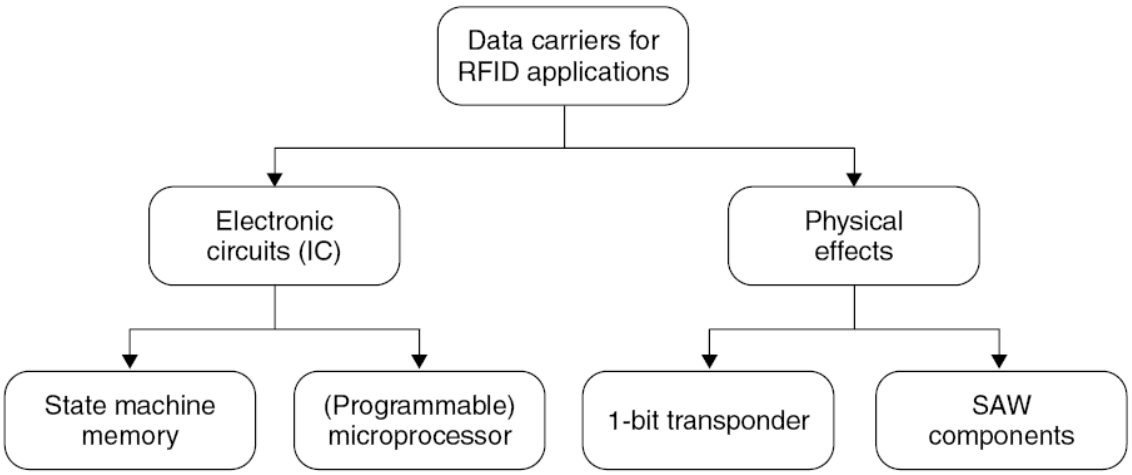


Figura 1.4.a La apreciación global de principios de operación de los diferentes portadores de datos usados en RFID.

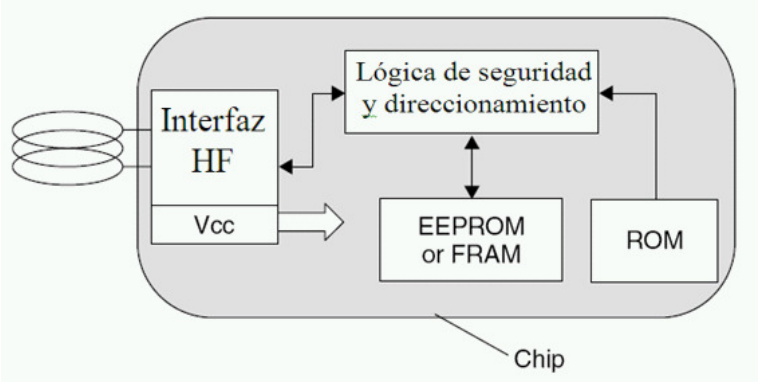


Figura 1.4.b diagrama en bloques de un portador de datos de RFID con funciones de memoria.

La interfaz de HF incorpora un modulador-demodulador de carga (o un procedimiento alternativo, por ejemplo divisor de frecuencia), controlado el trafico de datos digitales hacia el *reader*.
Por ejemplo los *transponders* pasivos, es decir *transponders* que no tiene su propio suministro de energía, se alimentan vía el campo de HF del lector. Para lograr esto, la interfase de HF, induce una corriente en la antena del *transponder* que se rectifica y se suministra al chip como una alimentación de voltaje regulado.

Circuito de modulación de carga con subportadora.

El circuito básico y principal de un modulador-demodulador de carga se muestra en la figura 2.4.4. Este genera una modulación de carga ohmica utilizando modulación de subportadora ASK o FSK.
La frecuencia de subportadora y de *baud rate* esta especificada de acuerdo a las especificaciones de la norma ISO 15693 (acople de tarjetas inteligentes aledañas).

La entrada de voltaje de alta frecuencia U2 del portador de datos (chip del *transponder*), sirve como base de tiempo de la interfaz de HF y se pasa a la entrada de un divisor binario.

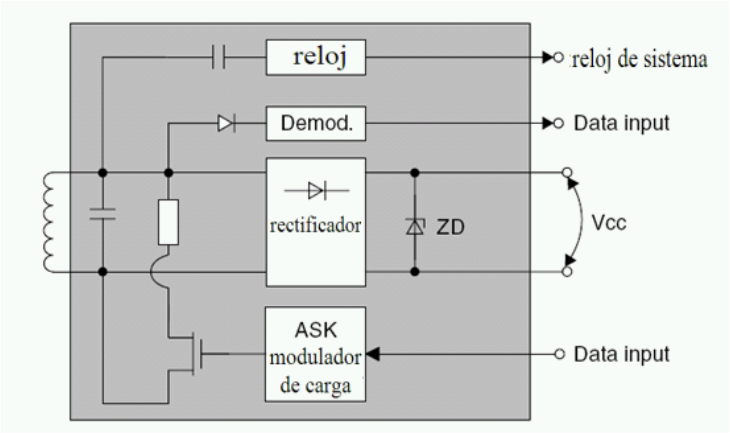


Figura 1.4.c diagrama en bloque de la interfaz de HF de un *transponder* acoplado inductivamente con modulación de carga.

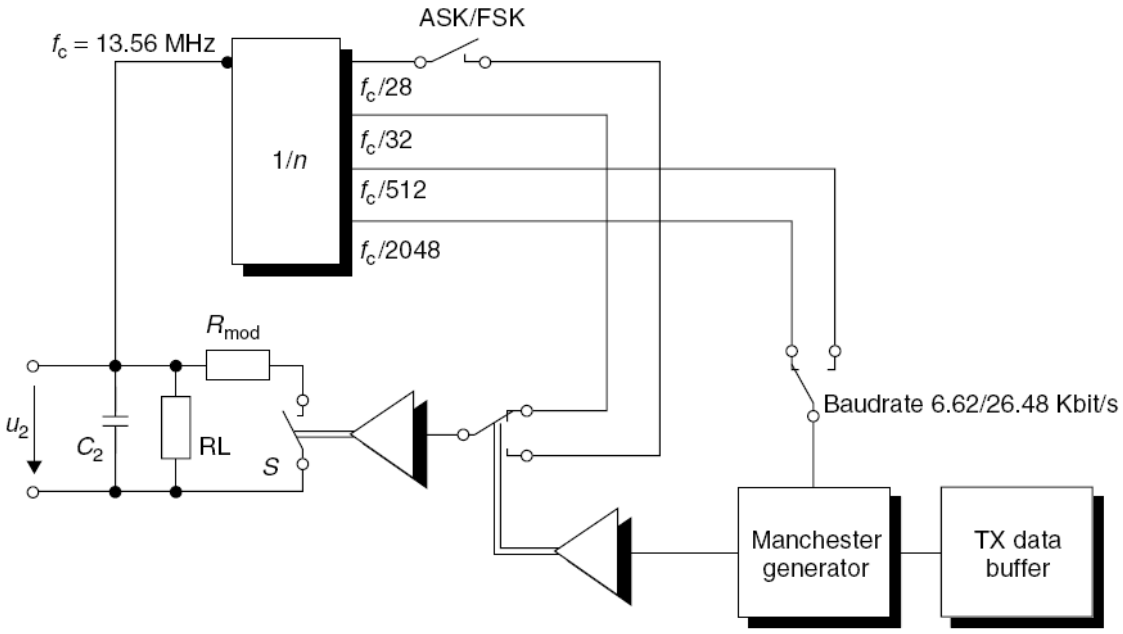


Figura 1.4.d Generación de una modulación de carga con subportadora modulada: la frecuencia de la subportadora es generada por una división binaria de la frecuencia portadora del sistema RFID.

La señal de subportadora se encuentran inicialmente con modulación ASK o FSK (según se encuentre la posición del interruptor ASK / FSK), para la codificación de cadenas de datos Manchester, mientras la resistencia de modulación en el *transponder* se enciende y se apaga en intervalos de tiempo por la señal de subportadora modulada.

Las frecuencias especificadas en el Standard para la *subportadora* y el *baud rate* pueden ser derivados de la sola división binaria de la señal de entrada de 13.56MHz (Tabla 1.4a)
Los datos seriales a ser transmitidos se transfieren primero a un generador de Manchester. Esto permite ajustar la proporción de baudio de la señal de banda base entre dos valores. La señal de banda base codificada en Manchester se usa para cambiar entre las dos frecuencias de subportadora f1 y f2 usando los niveles ‘1 ' y ‘0 ' de la señal, para generar una señal de subportadora modulada en FSK. Si la señal de reloj f2 es interrumpida, esto resultara en una señal de subportadora modulada en ASK. Lo que significa que su función es la de un simple interruptor entre la modulación ASK y FSK.
La señal subportadora es transmitida entonces al interruptor S, para que la resistencia de modulación del modulador de carga pueda activar conmutar en el tiempo con la frecuencia de subportadora.

Divisor N	Frecuencia	Implementación
1/28	485 kHz	ϕ2 de subportadora FSK
1/32	423 kHz	ϕ1 de Subportadora FSK mas Subportadora ASK
1/512	26.48 kHz	Bits de señal de reloj para un *baud rate* alto.
1/2048	6.62 kHz	Bits de señal de reloj para un *baud rate* bajo.

Tabla 1.4a Las frecuencias del reloj requeridas en la interfase de HF son generadas por la división binaria de láxenla de portadora de 13.56MHz.

1.4.1.2 Direcciones y seguridad lógica.

El direccionamiento y la seguridad lógica son la parte fundamental del portador de datos y controla todos los procesos en el chip. Ver fig. 1.4.e.
La lógica asegura que el portador de datos tome un estado definido cuando recibe el suministro de energía adecuado al entrar en el campo de HF de un *reader*. Los registros especiales de I/O realizan un intercambio de datos con el *reader* donde una unidad criptográfica optativa se requiere para la autenticación, la encriptación de los datos y administración es de suma importancia en todo este proceso.

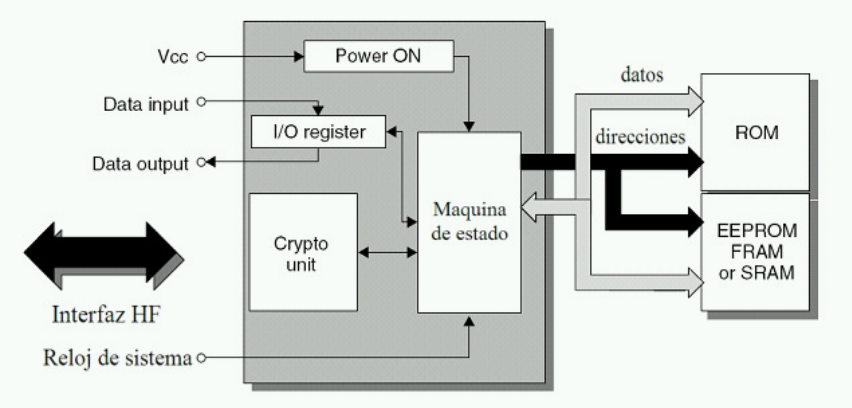


Figura 1.4.e. Diagrama en bloques de direccionamiento y seguridad lógica.

La memoria de los datos esta comprendida por una ROM para los datos permanentes como números de serie y EEPROM o FRAM son conectadas para el direccionamiento y lógica de seguridad por medio del direccionamiento y el bus de datos dentro del chip.

El reloj de sistema requerido para el sistema de control y la sincronización del sistema es derivado del campo de HF, por la interfaz de HF y proporciona la dirección y el modulo lógico de seguridad.

El control estado-dependiente de todos los procedimientos realizados por una maquina de estado en la cual la complejidad sus programas secuenciales simula los procedimientos ejecutados por un microprocesador.

1.4.1.3 Arquitectura de memoria

1.4.1.3.1 Transponder de solo lectura

Este tipo de *transponder* es el de menor capacidad y bajo costo del rango de los portadores de datos de RFID. Cuando un *transponder* de solo lectura entra en la zona de interrogación del *reader* este transmite su propio numero de identificación continuamente (fig. 1.4.f.), normalmente esta identificaron es un numero serial compuesto por unos bytes adjuntos en la trama de datos, usualmente el fabricante del chip incorpora el numero único de identificación lo cual garantiza que este numero serial es único para cada *transponder*, con lo cual imposibilita cualquier alteración de este numero serie o de cualquier dato, incorporado en el chip durante la fabricación. La comunicación es unidireccional, a través de la actualización del numero serie que el *transponder* le envía al *reader*.

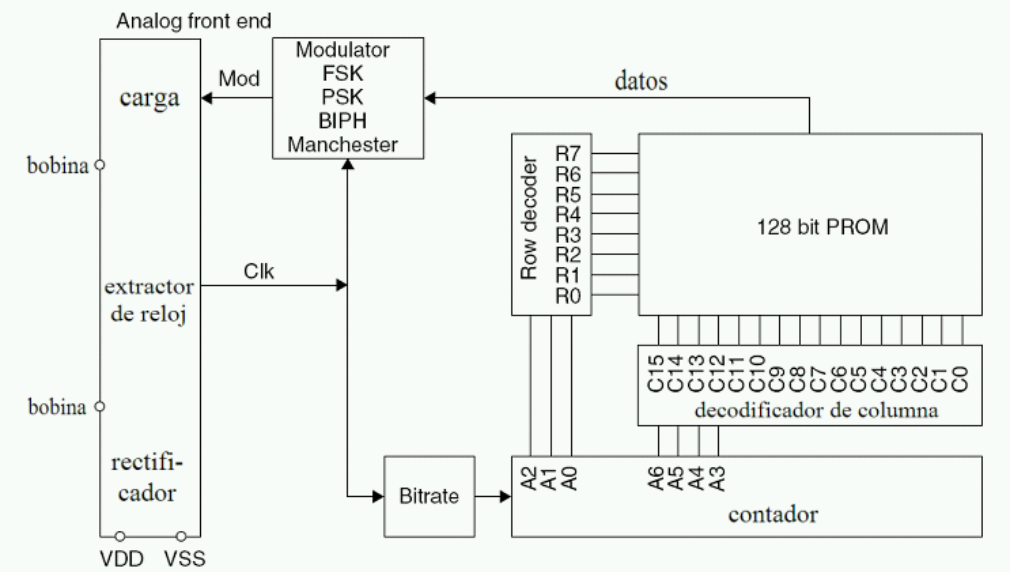


Figura 1.4.f diagrama en bloques de un *transponder* de solo lectura.

Cuando el *transponder* entra en la zona de interrogación del *reader* se habilita un contador que hace un barrido secuencial de la memoria interna (PROM), la salida de datos de la memoria se conecta a un modulador de carga que modula el código binario al código de banda base (modulador), de esta manera el contenido entero de la memoria (numero serial de 128 bits) puede ser emitido de manera cíclica como una cadena de datos seriales (imagen reproducida de Semiconductor de TEMIC GmbH, Heilbronn).

Los *transponder* de solo lectura se usan en aplicaciones donde no se requiere el almacenamiento de datos en el *transponder*. Por consiguiente los campo clásicos de aplicación son la identificación animal, mando de acceso y automatización industrial con administración de datos centralizados.

Un chip de solo lectura se muestra en la figura 1.4.g

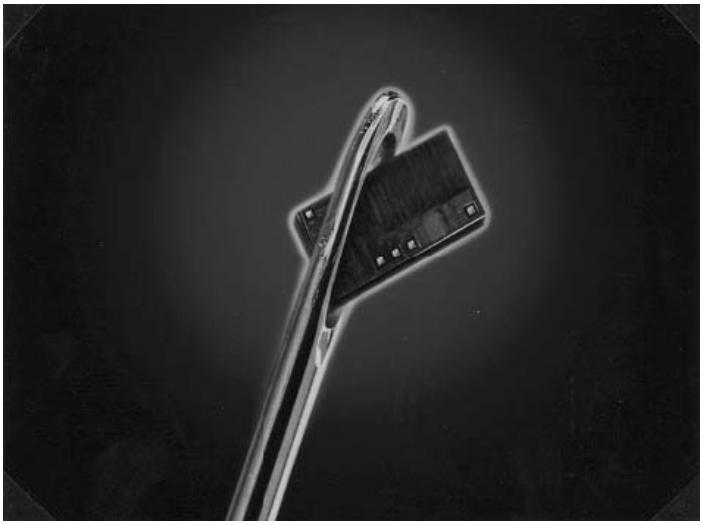


Figure 1.4.g Comparación de tamaño: los *transponder* económicos caben en el ojo de una aguja (imagen tomada de Electrónica de Philips N.V.).

1.4.1.3.2 Transponders de lectura y escritura

Los *transponder* con capacidad de escritura de datos por medio de un *reader* se encuentran disponibles con capacidades de memoria que van desde 1 byte (*transponder* pigeon), hasta 64 Kbytes (*transponder* de microondas con SRAM).

El acceso a la escritura y lectura de *transponder* se encuentra a menudo en bloques, un bloque es formado congregando un número predefinido de bytes que pueden leerse o escribirse como una sola unidad. Para cambiar el contenido de datos de un bloque individual, el bloque entero debe ser leído primero desde el *transponder*, después de que el mismo bloque, incluyendo los bytes modificados, pueden ser reescritos al *transponder.*
Los sistemas actuales usan bloques con tamaños de 16 bits, 4 bytes o 16 bytes. La estructura de bloque de la memoria facilita el direccionamiento en el chip y para el *reader*.

1.4.1.3.3 Transponder con función criptográfica

Si un *transponder regrabable* no es protegido de alguna manera, cualquier *reader* que forma parte del mismo sistema de RFID podrá leer o escribir en el, esto no siempre es deseable, porque en aplicaciones especiales lecturas o escrituras sin autorización podrían provocar daños o efectos inesperados en el mismo.

Dos ejemplos de tales aplicaciones son las tarjetas del *contactless* usadas como boletos en el sistema de transporte público y *transponders* en vehículos para codificación electrónica de sistemas de inmovilización.
Hay varios procedimientos por prevenir el acceso desautorizado a un *transponder*.
Uno de los mecanismos más simples es la protección de escritura y lectura por verificación de contraseña.
En este procedimiento, la tarjeta compara la contraseña transmitida con una contraseña de referencia guardada y permite el acceso a la memoria de datos si las contraseñas corresponden.
Sin embargo, si la autorización mutua es requerida o si es necesario verificar si ambos componentes pertenecen a la misma aplicación, entonces los procedimientos de la autenticación son usados. Fundamentalmente, el procedimiento de la autenticación siempre involucra una comparación de dos llaves confidenciales que no se transmiten vía la interfase. (Una descripción detallada de este procedimiento puede encontrarse en el Capítulo Autenticación). la autenticación de criptográfica es normalmente asociada con la transmisión de cadenas de datos encriptados (Figura 1.4.h).
Esto proporciona una protección eficaz contra la violación de integridad en la transmisión de los datos, supervisando el *transponder* inalámbrico usando un receptor de radio.
Además del área de memoria asignada a los datos de la aplicación, los *transponders* con funciones criptográficas siempre tienen un área de memoria adicional para el almacenamiento de contraseñas y un registro de configuración (registro de acceso, Acc) para la protección de escritura selectivamente en áreas de dirección seleccionadas. La contraseña se escribe a la *memoria de contraseñas* por el fabricante antes de proporcionar el *transponder* al usuario. Por las razones de seguridad, la memoria de contraseñas nunca puede leerse.

Concepto de *llave* jerárquica algunos sistemas proporcionan la opcion de almacenamiento dos *llave* separadas, -*llave* A y *llave* B- esto permite diferentes derechos de acceso. La autenticación entre el *trasnponder* y el *reader* se puede ejecutar usando la *llave* A o la *llave* B. La opción de asignar diferentes derechos de acceso (Acc) a las dos *llave* puede ser aprovechando para la definición de niveles de seguridad jerárquicos en una aplicación.
La figura 1.4.h l ilustra el principio para la clarificación. El *transponder* incorpora dos llave en memoria que son inicializadas por las dos *llaves* A y B. los derechos de acceso que se asignan a los *reader* después de una autenticación exitosa dependen de la *llave* que se ha utilizado que se ha seleccionado en el transponder (registro de acceso).
El *reader* 1, solo posee la key A. después de una autenticación exitosa, los parámetros seleccionados en el registro de acceso (Acc) solo permiten leer la memoria del *transponder*.
El *reader* 2, por otro lado, solo posee la *llave* B y después de una autenticación exitosa, los parámetros seleccionados en el registro permiten leer y escribir en la memoria del *transponder*.

Por ejemplo, una aplicación de un sistema de llave jerárquica se considera un sistema de boletos para una red de transporte publico, esto permite diferenciar entre dos grupos de readers el "devaluers" para pagos de tarifa, y el "revaluers" para el reevalúo de saldo de las tarjetas inteligentes, *contactless.*
Los derechos de acceso al *transponder* son configurados por dos registros de acceso A y B, esto permite que depuse de una autenticación exitosa utilizando la *llave* A el sistema solo permite la deducción de cantidades monetarias (decremento de un contador), mientras que la llave B permite reevaluar la cantidad de saldo restante, permitiendo leer para la determinación de la cantidad y escribir en el para asignarle el crédito monetario restante (reevaluación del mismo contador). De esta manera un *transponder* jamás podrá ser devaluado usando un reevaluador, tampoco el *transponder* podrá ser corrompido por software adhiriéndole cantidades al contador interno si no se autentifica por medio de la *llave* correspondiente.

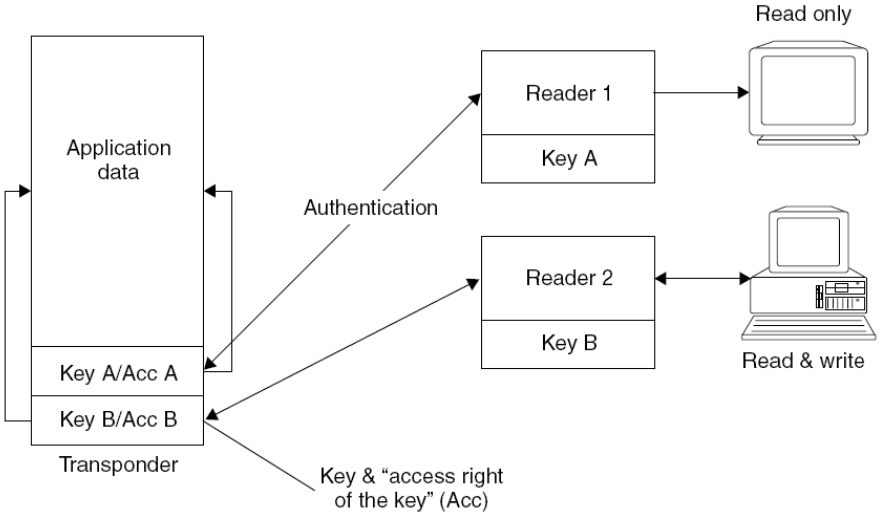


Figura 1.4.h *transponder* con dos llaves en memoria para facilitar el direccionamiento de memoria para aplicaciones jerárquicas.

1.4.1.3.4 Segmentación de memoria

Los *transponders* también pueden protegerse del acceso de *readers* que pertenezcan a otras aplicaciones usando procedimientos de autenticación. En *transponders* con grandes capacidades de memoria, es posible dividir toda la memoria en pequeñas unidades llamadas segmentos y proteger cada uno de estos segmentos con una *llave* diferente.
Un *transponder* con segmentación de memoria permite que datos de diferentes aplicaciones sean guardados completamente por separado y el acceso a cada segmento solo puede gestionarse mediante una autenticación exitosa con la llave especifica. Por consiguiente, un *reader* solo tendrá acceso a los segmentos de memoria solo si posee la contraseña de aplicación.

La mayoría de los sistemas de segmentación de memoria utilizan arreglos de memoria los cuales no pueden ser alterados por el usuario, un tamaño fijo de segmento ofrece la ventaja de ser baratos y simples de fabricar.
Sin embargo es muy raro que el espacio de almacenamiento requerido para una aplicación corresponda con el tamaño de segmento del *transponder*.

En aplicaciones pequeñas el valioso espacio de almacenamiento en el *transponder* se gasta porque los segmentos solo se usan parcialmente. Por otro lado en aplicaciones grandes, se necesita una mejor redistribución del espacio de almacenamiento y aminorar la cantidad de llaves específicas para cada segmento para evitar la partición de aplicaciones por insuficiente espacio en los segmentos.

Un mejor uso del espacio es logrado con segmentos de longitud constante (figura 1.4.i). En este caso la memoria asignada a un segmento puede igualarse a los requisitos de el área de memoria que usa la aplicación, debido a la dificultad en la realización de la segmentación variable, esta variante es rara en *transponders* que posean una lógica con maquina de estado.
La figura 1.4.j muestra la configuración de memoria de un *transponder* con segmentación fija, la memoria disponible es de 128 bytes y es dividida en cuatro segmentos, a esto se le conoce como compaginación, cada segmento puede protegerse contra la lectura o escritura por medio de contraseñas. El registro de acceso de este *transponder* (OTP, protección de escritura) consiste en un área de memoria adicional de 16 bits por segmento. Borrando un solo bit del registro de acceso se protegen 16 bits de la memoria de aplicación contra sobre escritura.

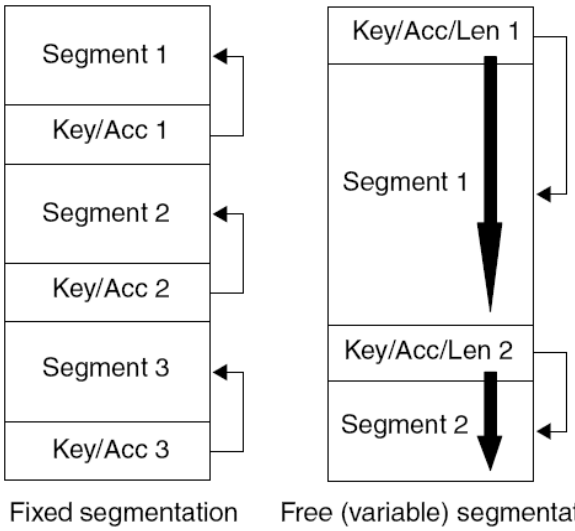


Figura 1.4.i diferenciación entre la segmentación fija y la segmentación variable.

Mapa de memoria de 1 Kbit (128 byte), de memoria RFID

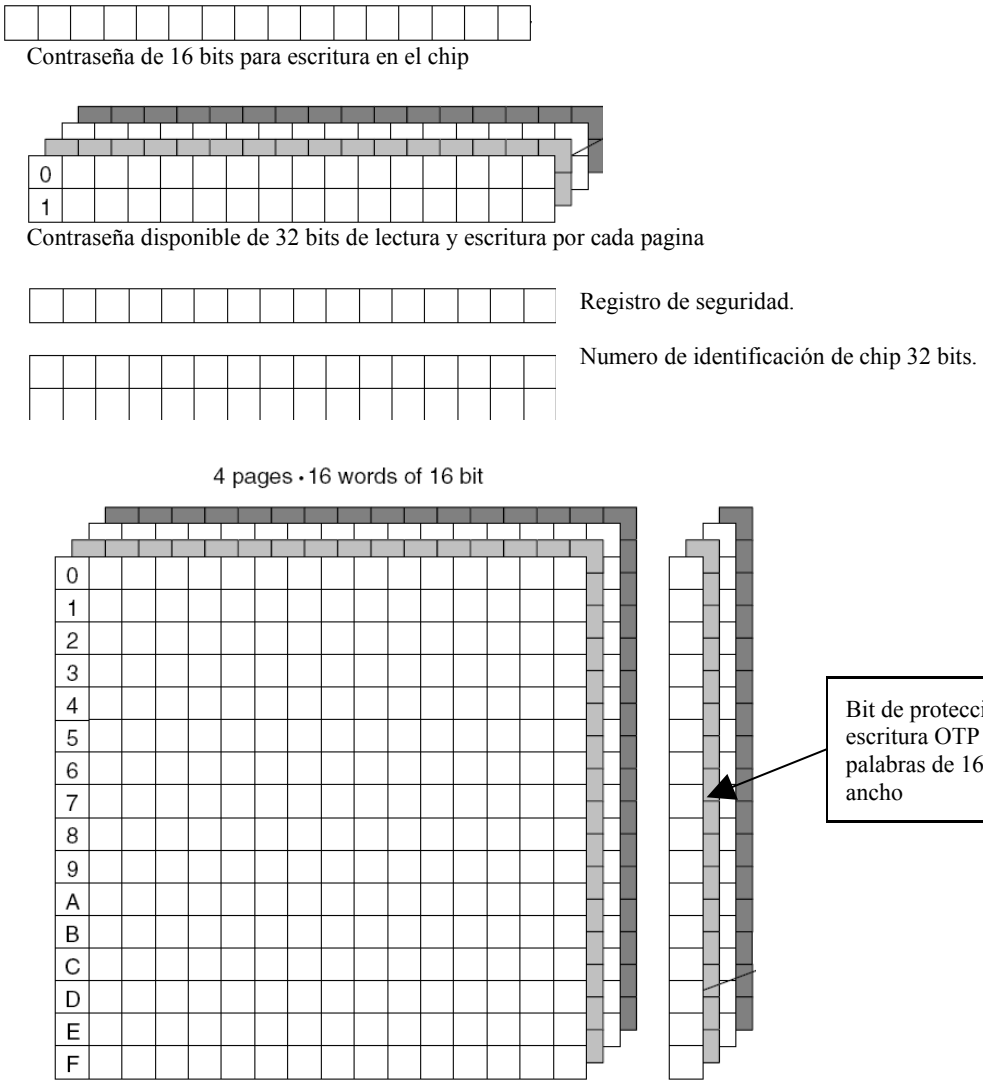


Figura 1.4.j ejemplo de segmentación e memoria de un chip de RFID

1.4.1.3.5 Directorio de aplicación MIFARE

La memoria de un *transponder* de MIFARE esta dividida en 16 segmentos independientes, conocidos como sectores, cada sector es protegido contra el acceso no autorizado a través de dos diferentes llaves (estructura jerárquica). Pueden asignarse derechos de acceso diferentes a cada uno de las dos llaves en su propio registro de acceso (config.). Así, 16 aplicaciones independientes son protegidas y cada una por llaves secretas que pueden ser cargadas hacia el *transponder* (Figura 2.4.k). Ninguna de las

aplicaciones puede leerse sin la llave confidencial, ni para verificación o identificación. Tampoco es posible identificar que aplicaciones han sido guardadas en el *transponder*.

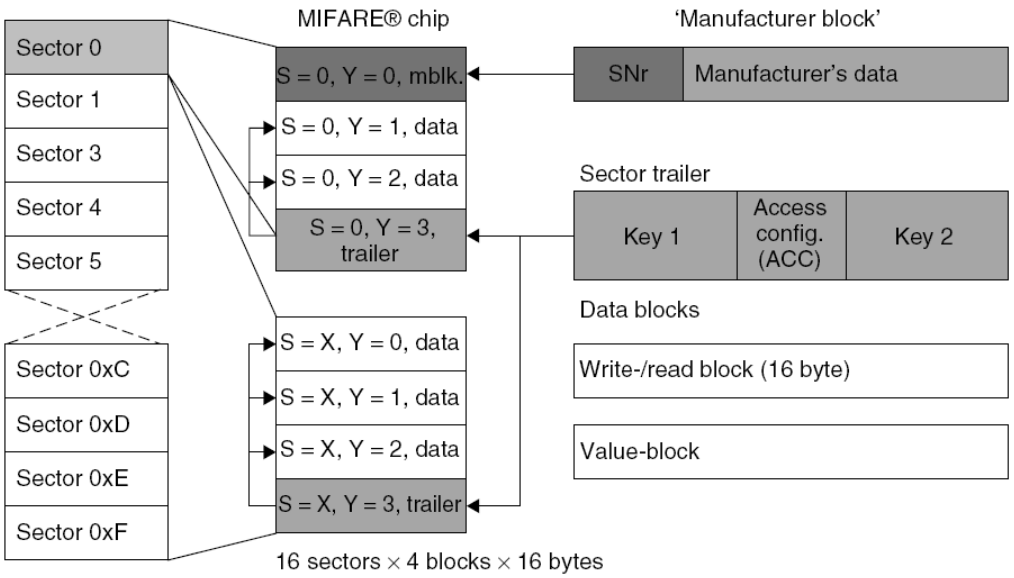


Figura 1.4.k Configuración de memoria de un portador de datos MIFARE. La memoria entera es dividida en 16 sectores independientes. Así un máximo de 16 aplicaciones separadas puede cargarse hacia una tarjeta de MIFARE

Se puede asumir que la ciudad de San Salvador decide implementar una tarjeta ciudadana *contactless*, con la cual cada ciudadano puede adquirir servicios de la ciudad, y que esta aplicación solo ocupa solo una pequeña parte de la memoria disponible de la tarjeta, así las unidades de memoria restantes podrían ser utilizadas para otras aplicaciones como por ejemplo: boletos de transporte local, arrendamiento de vehículos, pago de tarjetas bancarias, pago de escolaridad, pago de impuesto y vialidad, llenado de combustible en gasolineras, pago en supermercado, control medico, etc.

2.4.1.3.6 Puerto Dual EEPROM

El módulo de EEPROM con bus de interfaz serial I2C (IIC) se estableció hace años, el bus I2C es la abreviación para Inter IC, porque originalmente se desarrolló para la conexión de microprocesadores con otros ICs en una tarjeta de circuito impreso común. El bus I2C es un bus serie y sólo requiere dos líneas bidireccionales, SDA (Datos Serie) y SCL (Reloj Serie). Una EEPROM puede leerse o puede ser escrita por la transmisión de órdenes definidas a través de las dos líneas en el bus I2C.

Algunos de estos módulos serie de EEPROM también tienen una interfase de HF y puede leerse o escribirse en ellas por medio de las líneas SDA y SCL o por la interfaz *contactless*

El diagrama de bloque del puerto dual EEPROM (Atmel, 1998) se muestra en Figura 2.4.l.

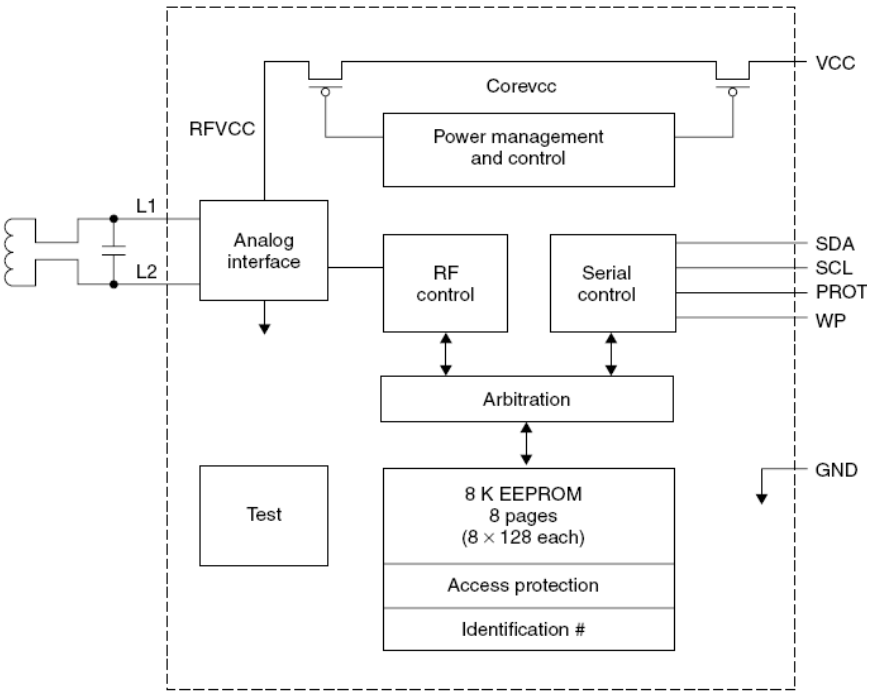


Figura 1.4.l Diagrama de Bloque de un puerto dual EEPROM.

La memoria puede direccionada por cualquier interfaz HF de *contactless* o un bus de interfase IIC (Imagen tomada de Atmel Corporación, San José, EE.UU.)

La memoria EEPROM se accede por medio de dos maquinas de estado (“Control RF” y “Control serie”) estos son muy independientes uno del otro. La lógica arbitraria adicional previene conflictos como resultado de accesos simultáneos a la EEPROM por medio de alta frecuencia (HF) e interfaces seriales, simplemente bloqueando a la otra interfase para prolongar el proceso de lectura o escritura.

La interfase de HF del modulo se diseña para el acoplamiento inductivo en un rango de frecuencia de 125 kHz. Si no hay voltaje de suministro en el pin Vcc del modulo, entonces el puerto dual EEPROM también puede ser alimentado por medio de la interfase de HF.

La fuente integral simplemente administra de una manera más eficiente la energía consumida apagando las partes del circuito con funciones que no son requeridos para el *contactless*.

La transferencia de datos del serial EEPROM al lector del *contactless*, se da por medio modulador de carga ohmica a través de la banda base.

Los comandos del *reader* se transfieren al puerto dual EEPROM por medio de modulación ASK (índice de modulación m > 10%) en la figura 2.4.m y 2.4.n se muestra la asignación de pines y la configuraron de memoria; el espacio total de memoria disponible de 1 Kbyte (8 Kbite) en el puerto dual EEPROM es dividido en ocho segmentos (bloques de 0 a 7) y cada uno de estos ocho bloques es subdividido en ocho subsegmentos de 16 bytes (paginas de 0 a 7), adicionalmente 16 bytes se encuentran disponibles como *paginas de protección de acceso.* La estructura de la página de protección de acceso se muestra en la figura 2.4.15.

La página de protección de acceso permite diferentes niveles de acceso a cada uno de los ocho bloques de la EEPROM aplicados independientemente por el bus I2C y la interfaz HF. Sin embargo, el acceso a la lectura y escritura en la página de la protección de acceso es solo posible a través del bus de interfaz I2C.

Los derechos de acceso de la interfase de HF en el bloque Y están definidos por los bits RFy de la pagina de protección de acceso (por ejemplo RF_7 contiene los derechos de acceso del bloque 7), de manera similar los derechos de acceso del bus de interfaz I2C están definidos en el bloque de memoria Y por el bit PBy de la pagina de proteccion de acceso (PB_5 contiene ls derechos de acceso del bloque 5).

Además el bloque 0 permite derechos de acceso a paginas individuales de 16 bytes por medio de los bits WP7-WP0; una peculiaridad de la pagina de protección de acceso es el bit Tamper, el proposito de este bit es seleccionar el tipo de interfaz con la cual se trabajara, si este tiene un valor de “1” la interfaz será HF o “0” para el bus de interfaz I2C, de esta manera con un acceso previo a lectura o escritura de la EEPROM, por medio la interfaz de HF se puede señalar al maestro que se haya conectado en el bus I2C.

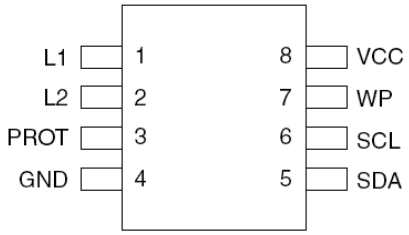


Figura 1.4.m Asignación de pines en el puerto dual EEPROM.

La bobina del *transponder* esta conectada a los pines L1 y L2, todos los demás pines del modulo están reservados para la conexión del bus I2C y la fuente de alimentación.

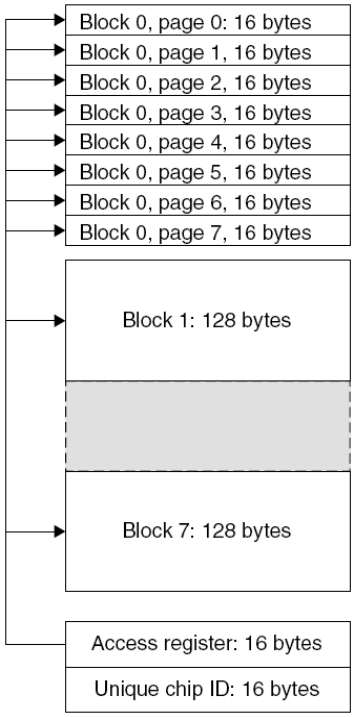


Figura 1.4.n Configuración de memoria del AT24RF08.

La memoria disponible de 1Kbyte es dividida en 16 segmentos (bloques de 0-7) con tamaño de 128 bytes. Memoria adicional de 32 bytes que contiene la pagina de protección de acceso y el único numero serial. La página de protección de acceso permite diferentes niveles de acceso los cuales pueden ser seteados a través de la interfaz de HF o por el bus de interfaz I2C.

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0	
SB0		RF0				PB0		Addr 0
SB1		RF1				PB1		Addr 1
SB2		RF2				PB2		Addr 2
SB3		RF3				PB3		Addr 3
SB4		RF4				PB4		Addr 4
SB5		RF5				PB5		Addr 5
SB6		RF6				PB6		Addr 6
SB7		RF7				PB7		Addr 7
SBAP						PBAP		Addr 8
WP7	WP6	WP5	WP4	WP3	WP2	WP1	WP0	Addr 9
DE	DC						Tamper	Addr A
Reserved								Addr B
Reserved								Addr C
Reserved								Addr D
Reserved								Addr E
Chip-revision								Addr F

Figura 1.4.o. Matriz de configuración de acceso de el modulo AT24RF08 facilita la configuración independiente de los derechos de acceso de los bloques 0 a 7.

1.4.2 Microprocesadores

Las tarjetas inteligentes *contactless* con microprocesador incorporan su propio sistema operativo, como en el caso de las tarjetas basadas en contacto.

La tarea del sistema operativo de una tarjeta inteligente *contactless*, es la transferencia de datos desde y para la tarjeta inteligente, control de secuencia de comandos, la administración de archivos y la ejecución de algoritmos criptográficos.

Los comandos típicos de la secuencia de procesamiento dentro del sistema operativo de una tarjeta inteligente se ejecutan de la siguiente manera: los comandos enviados del *reader* a la tarjeta inteligente son recibidos por medio de la interfase de HF. El reconocimiento de errores y los mecanismos de corrección son manejados por el administrador de entradas y salidas, indistintamente de los procedimientos de alto nivel. Un comando libre de errores recibido por el administrador de mensajería segura es desencriptado y chequeado para verificación de integridad.

Después de la desencriptación el intérprete de los comandos de alto nivel intenta decodificar los comandos.

Si esto no funciona, entonces es llamado el administrador de código de retorno, que genera el código de retorno apropiado y se reenvía por medio del administrador de entrada y salida. (Figura 1.4.p).

Si un comando válido se recibe, entonces es porque el actual código de programa se asoció con el comando de aplicación ejecutado. Si el acceso a los datos de la aplicación en la EEPROM es necesario, esto es realizado exclusivamente por el sistema de administración de archivos y el organizador de memoria que convierte todas las direcciones simbólicas en la correspondiente dirección física del área de memoria.
El administrador de archivos también verifica las condiciones de acceso (autorización), para los datos en cuestión.

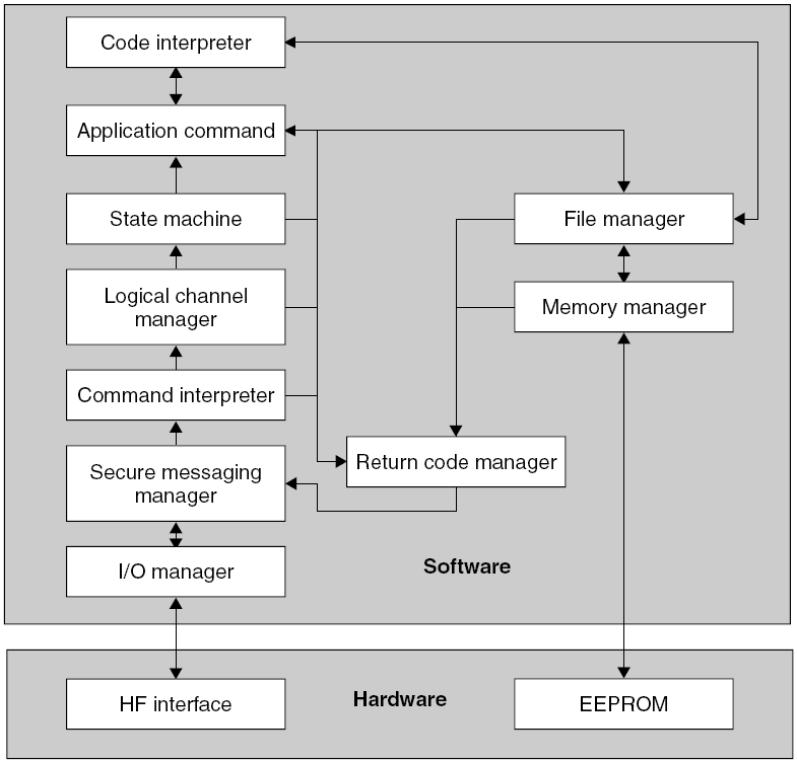


Figura 1.4.p. Secuencia de procesamiento de comandos por medio del sistema operativo de una tarjeta inteligente.

1.4.2.1 Tarjeta de interfaz dual

El mercado de tarjetas inteligentes es tradicionalmente utilizado en aplicaciones de pago (tarjetas de dinero en efectivo, ahorro electrónico), y para los teléfonos móviles (tarjetas SIM para teléfonos móviles con GSM), aplicaciones con alto grado de seguridad en el procesamiento y transmisión de datos. La necesidad resultante de ser capaz de calcular de manera rápida y simple complejos algoritmos criptográficos lleva a la necesidad de desarrollar coprocesadores en el chip de la tarjeta.

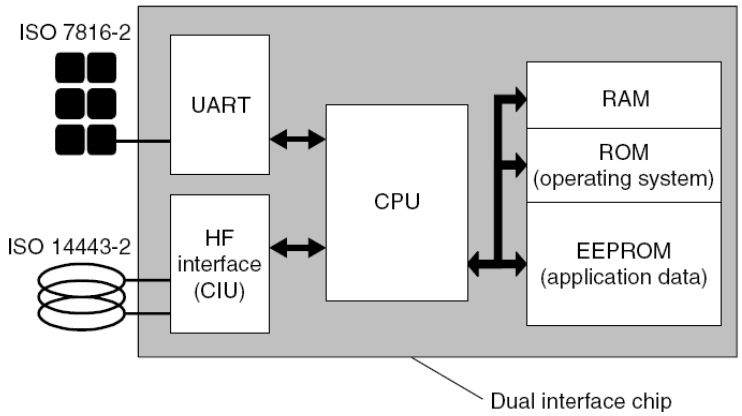


Diagrama en bloque de una tarjeta de interfaz dual, ambas interfaces de la tarjeta de interfaz dual pueden direccionar independiente una de la otra.

1.4.2.2 Mifare plus

El diagrama en bloque de la figura 2.4.17 muestra un esquema de la tarjeta de interfaz dual. Este es un chip que fue desarrollado por Semiconductores de Philips Gratkorn y Siemens HL cerca de 1997.
En el corazón de este chip es una memoria EEPROM de 8 Kbyte, la EEPROM común, en donde los datos de la aplicación son almacenados. De una manera similar a la RAM del puerto dual, esta EEPROM común puede accederse vía dos interfaces que están completamente separadas del punto de vista de circuitería. La interfase inactiva en cualquier momento está completamente separada del suministro de poder del chip, para que la energía disponible en funcionamiento del *contactless* se use óptimamente.
La interfase del *contactless* esta basada en una máquina de estados lógicos que forman una tarjeta de memoria *contactless* MIFARE. Del punto de vista de un *reader* de *contactless* esta tarjeta de interfaz dual se comporta así como una tarjeta de memoria, con una memoria EEPROM segmentada, en donde el arreglo de los segmentos individuales y bloques de memoria es idéntico al de una tarjeta de MIFARE convencional.
La interfase de contacto, por otro lado, esta basado en un microprocesador con su propio sistema operativo de tarjeta inteligente.
La segmentación de memoria antedicha es vista de nuevo cuando el microprocesador accede a la EEPROM común. El sistema operativo por consiguiente sólo y puede leer y escribirle a la EEPROM común en bloques dentro de los sectores correspondientes.
Además, los derechos de escritura y lectura para los bloques de memoria individuales de la EEPROM pueden configurarse separadamente para el contactless y interfase del contacto.
Éstos derechos de acceso son fijos y supervisados por la Matriz de Configuración de Acceso. Esto también facilita el realización de conceptos de seguridad jerárquicos.

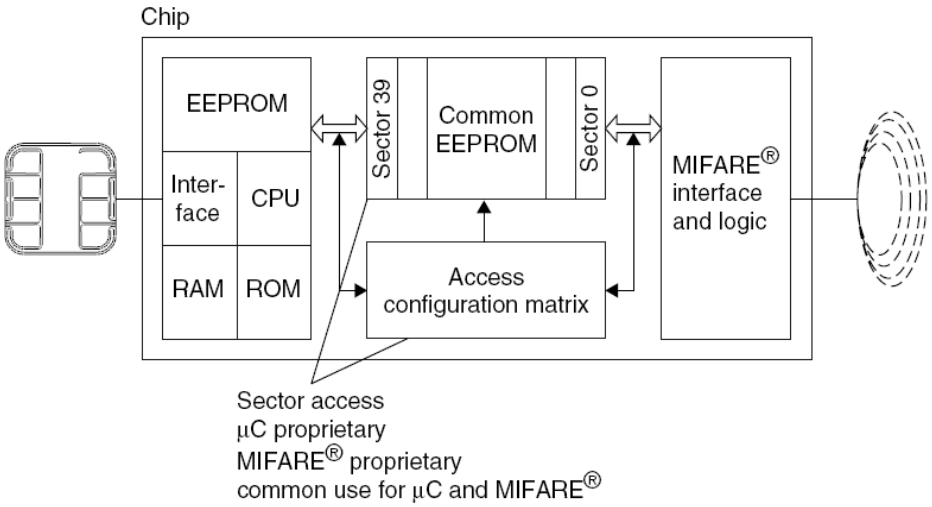


Figura 1.4.q Diagrama del bloque de la MIFARE-plus "tarjeta de inetrfaz dual", en modo de operación contactless la EEPROM común es accedida por medio del MIFARE

Al operar por medio de la interfase de contacto un microprocesador con sus propios sistema operativo de accede a la misma memoria.

1.4.2.3 Concepto moderno para la tarjeta de interfaz dual

La figura 1.4.18 muestra el diagrama de bloque de una tarjeta de la interfaz dual moderna. Esta tarjeta esta basada en un microprocesador 8051 con un sistema operativo de tarjeta inteligente. La interfaz de *contactless* es formada por un CIU (unidad de interfaz de contactless) que puede configurarse por medio de los registro de direccionamiento del CPU o también puede facilitar una interrogación del estado de la CIU.
Un CIU moderno realiza el traslado de un bloque del datos automáticamente desde y para un *reader* es por eso que automáticamente realiza el codificando necesario o decodificado de las cadenas de datos según las especificaciones en la norma ISO/IEC14443-2 y la ISO/IEC14443-3. A menudo también realiza el cálculo automático y comprobación del CRCs transmitido.

Para enviar un bloque de datos, el sistema operativo solo necesita guardar el bloque de datos a ser enviado en la memoria RAM del chip y cargar la dirección de memoria correspondiente y la longitud del bloque en el registro de configuración del CIU.
El CPU no se encuentra tan activamente involucrado en la transferencia de datos y puede cambiarse y puede cambiar a un modo de bajo consumo de energía para la duración del traslado de los datos. Cuando un bloque de datos se recibe, los datos del CIU se guardan automáticamente en el chip, se verifica la RAM y el CRC del bloque recibido.
Los tiempos de la transacción cortos representan un requisito particularmente importante para aplicaciones en *contactless*.

Para facilitar el cálculo de las funciones criptográficas durante cortos intervalos de tiempo muchos chips de interfaz dual tienen coprocesadores criptográficos.

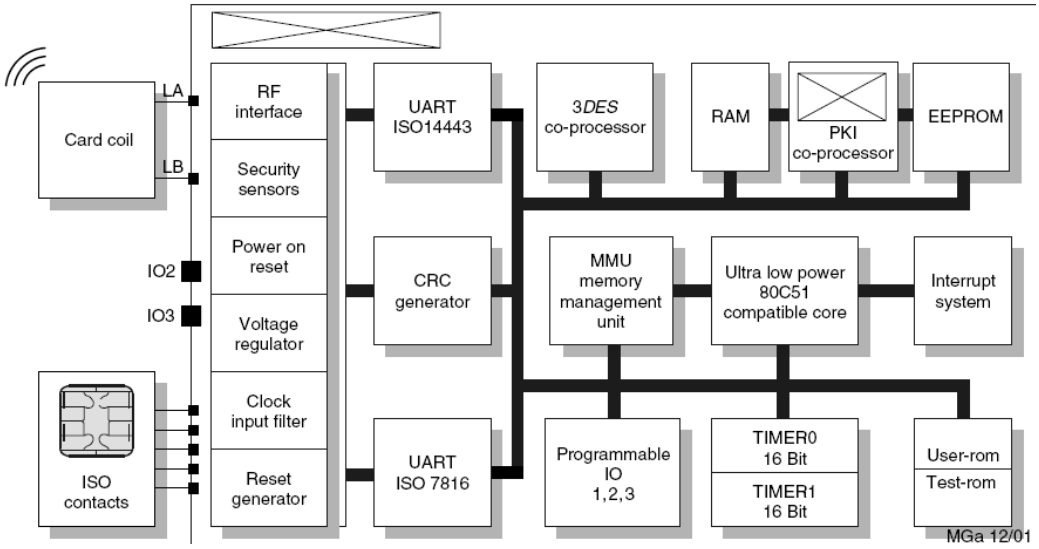


Figura 1.4.r. Diagrama en bloques de una tarjeta de interfaz dual MIFARE-ProX.

1.4.3 Medición de variable físicas

1.4.3.1 Transponders con funciones de sensor

Transmisores de telemetría operados con baterías que operan en rangos de frecuencias que van de 27.125Mhz a 433Mhz utilizan un sensor de datos para la detección.
El campo de aplicación de estos sistemas es muy limitado, tanto por su restringido tamaño como por el tiempo de vida de la batería.

Estos *transponders* de RFID especialmente desarrollados incorporan un convertidor A/D en el chip ASIC, facilitando la medida de variables físicas. En principio, cualquier el sensor puede usarse en lugar de la resistencia variable para medición de variables físicas.
Debido a la disponibilidad de sensores de temperatura miniaturizados (NTC), este tipo de sistema se desarrolló primero para la medida de temperatura (Figura 1.4.s).
La tecnología pasiva de RFID, sin necesidad de baterías garantiza una larga vida del *transponder* a la ves que es medioambientalmente funcional.

Los valores medidos por el convertidor A/D pueden ser leídos por comandos especiales del *reader,* en *transponders* de solo lectura el valor medido puede añadirse periódicamente al número de identificación emitido.

Hoy en día, el campo principal de aplicación para los *transponders* con funciones de sensor es para mediciones inalámbricas de temperatura en animales. En esta aplicación la temperatura del cuerpo de animales domésticos y trabajo son monitoreadas para la salud, supervisión de crías en gestación y control de nacimientos. La medida puede realizarse automáticamente durante la ingesta de agua y alimentos del animal o también puede hacerse usando un *reader* portátil.

En usos industriales, pueden usarse *transponders* con funciones de sensor en cualquier parte donde las variables físicas necesitan ser medidas.
Además de los sensores de temperatura clásicos un gran número de sensores pueden ser integrados.

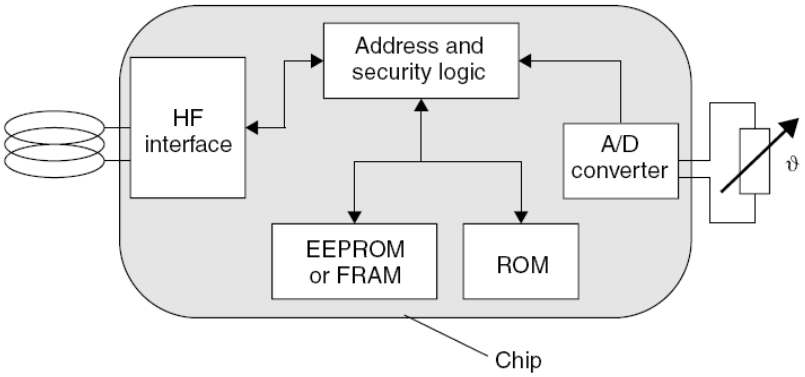


Figura 1.4.s *Transponder* inductivamente acoplado con sensor de temperatura adicional.

Arquitectura de los lectores de datos (readers).

1.4.4 Flujo de datos en una aplicación

Un software de aplicación que se diseña para leer o escribir datos en un portador de datos inalámbrico (*transponder*), necesita de una interfaz conocida como *reader contactless*. Desde el punto de vista del software de aplicación, acceder al *transponder* debe ser tan transparente como sea posible, en otras palabras las operaciones de lectura y escritura deben diferir lo menos posible comparados con los procedimientos de acceso a los portadores de datos con contacto (tarjeta inteligente con contacto)
Las operaciones de lectura y escritura llevadas a cavo en un portador de datos sin contacto se basan en el principio del maestro-esclavo (figura 1.4.t)
Esto significa que todas las actividades del *reader* y del *transponder* son comenzadas por el software de la aplicación. En un sistema de estructura jerárquica el software de la

aplicación es representado como el amo, mientras el *reader*, como el esclavo, este es activado solamente cuando se reciben las ordenes de lectura/escritura del software de aplicación.
Para que el *reader* pueda ejecutar los comandos del software de aplicación primero debe establecer comunicación con un *transponder*, una ves se establece la comunicación el *reader* toma el rol de maestro en relación al *transponer*

El *transponder* por consiguiente sólo responde a los órdenes del *reader* y nunca es independientemente activo (salvo el más simple *transponder* de solo lectura). Una orden de lectura del software de aplicación al *reader* puede comenzar con una serie de pasos entre el *reader* y el *transponder*.
Las funciones principales del *reader* son por consiguiente activar al portador de datos (*transponder*), estructurar la secuencia de comunicación con el *transponder*, y la transferencia de información entre el software de aplicación y el portador de datos sin contacto.

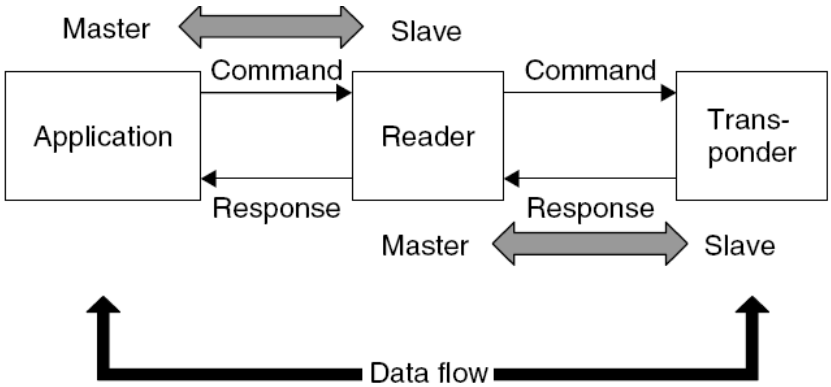


Figura 1.4.t principio de operación de maestro-esclavo entre el software de aplicación, el *reader* y el *transponder*.

1.4.5 Componentes de un Reader

A pesar de las diferencias fundamentales en el tipo de acoplamiento (inductivo-electromagnético), la secuencia de comunicación (FDX, HDX, SEQ), el procedimiento de transmisión de datos del *transponder* al lector (modulación de carga, backscatter, sub-armónicos) y el rango de frecuencia, todos los lectores son similares en su principio operando básico y en su diseño. Los lectores en todos los sistemas pueden reducirse a dos bloques funcionales fundamentales: el sistema de control y la interfaz de HF, estos consisten en un transmisor y receptor (figura 2.4.u).

La figura 1.4.v muestra un *reader* para un sistema de RFID inductivamente acoplado, al lado derecho podemos ver la interfaz de HF la cual se encuentra apantallada para protegerla de la frecuencias espurias. El sistema del lado derecho es el sistema de control, comprendido por un modulo ASIC, un microcontrolador así como su interfaz RS232.

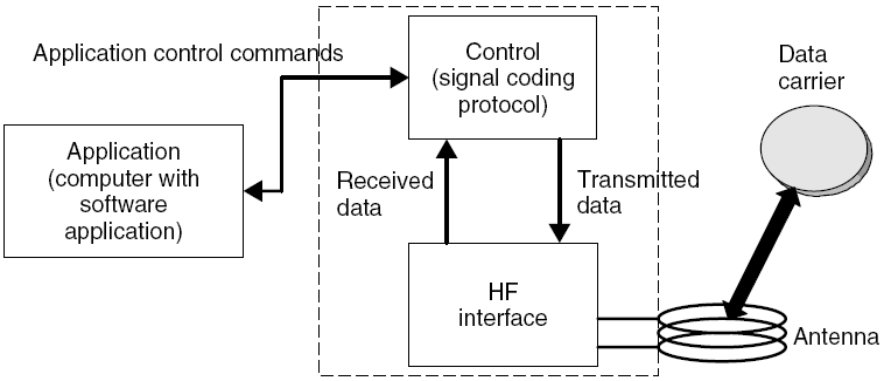


Figura 1.4.u. Diagrama en bloque de un *reader* constituido por el sistema de control y la interfaz de HF, todo el sistema es controlado a través de comandos provenientes de una aplicación externa.

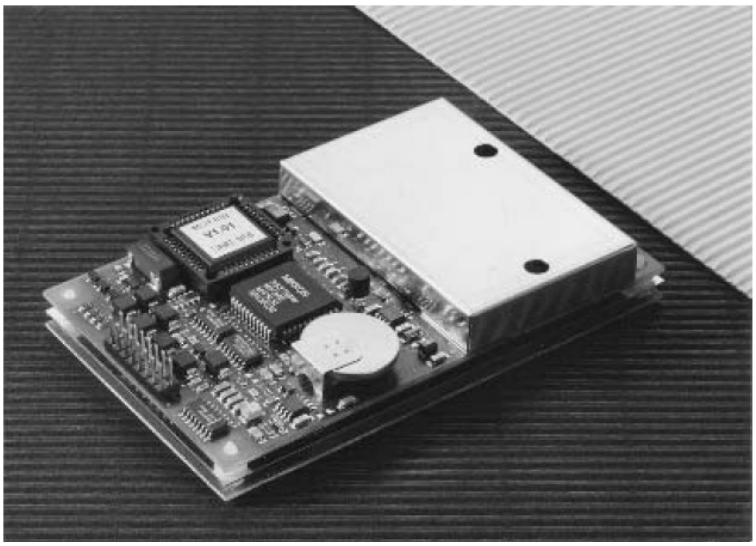


Figura 1.4.v. Ejemplo de un *reader*, con sus dos bloques funcionales formados por el sistema de control y la interfaz de HF.

1.4.5.1 Interfaz de HF

La interfase de HF del *reader* realiza las funciones siguientes:

- Generación de potencia en la transmisión de alta frecuencia para activar el *transponder* y proporcionarle alimentación.
- Modulación de la señal de transmisión para el envío de datos al *transponder*.
- Recepción y modulación de la señal de HF transmitida por el *transponder*.

La interfaz de HF contiene dos caminos separados por señales que corresponden con las dos direcciones de flujo de los datos de y para el *transponder* (Figura 1.4.y). Los Datos que se transmiten al *transponder* viajan a través del *transmiter arm*. Recíprocamente, los datos que se reciben de *transponder* son procesados en el *receiver arm*.

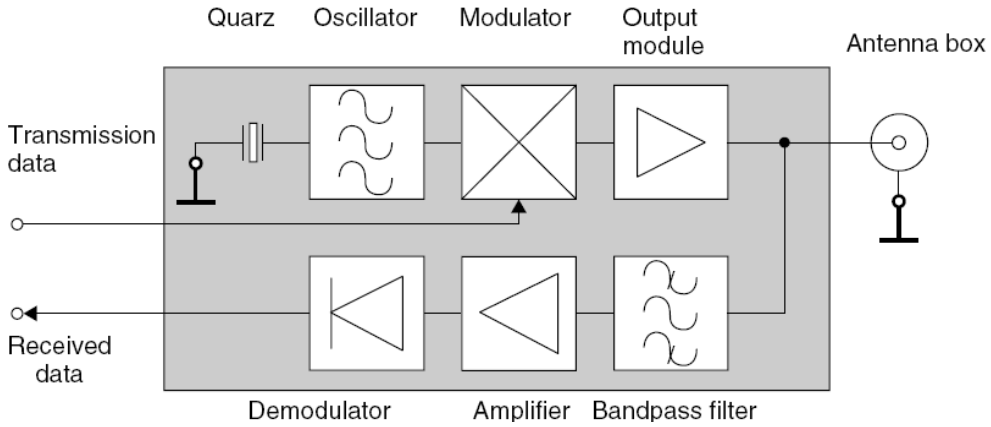


Figura 1.4.y. Diagrama en bloque de una interfaz de HF, para un sistema RFID acoplado inductivamente.

1.4.5.2 Unidades de control.

La unidad de control del *reader* (figura 1.4.w) realiza las siguientes funciones:

- Comunicación con el software de aplicación y la ejecución de las órdenes del software de aplicación.
- Control de la comunicaron con un *transponder*.
- Codificaron y decodificación de señales (figura 1.4.x).

En sistemas más complejos las funciones adicionales siguientes están disponibles:

- Ejecución de un algoritmo de anticolisión.
- Encriptación y desencriptación de los datos transferidos entre el *transponder* y el *reader*.
- Ejecución de autenticación entre el *transponder* y el *reader*.

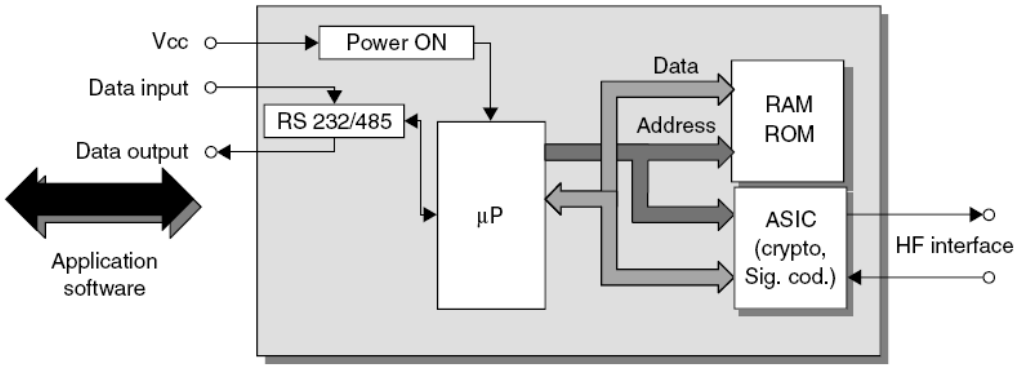


Figura 1.4.w. Diagrama en bloque de la unidad de control de un *reader*.

La unidad e control es basada normalmente en un microprocesador para realizar funciones complejas; procedimientos criptográficos como cifrado de tramas entre el *transponder* y el *reader,* así como la codificación de señales estas son realizadas a menudo en un modulo ASIC adicional para relevar al procesador de cálculos complejos.
Por razones de ejecución el ASIC es accedido a través del bus del microprocesador.
El intercambio de datos entre el software de aplicación y la unidad de control del *reader* es realizado por medio de un a interfase RS232 o RS485, se utiliza la codificación NRZ (8 bits asíncronos).

La proporción de baudio es normalmente un múltiplo de 1200Bd (4800Bd, 9600Bd, etc.)
El medio entre la interfaz de alta frecuencia (HF) y la unidad de control es representado por el estado de la interfaz de HF como un número binario, en un sistema con modulación ASK un 1 lógico representa la activación de la señal de alta frecuencia "HF *signal on*" mientras que un 0 lógico representa la desactivación de la señal de alta frecuencia "HF *signal off*".

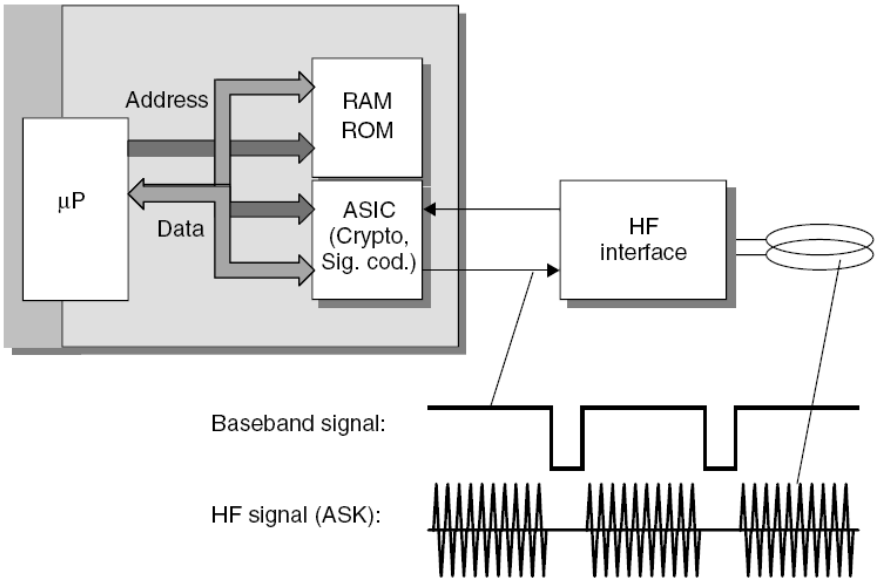


Figura 1.4.x Codificación y decodificación de señales realizada por medio de la unidad de control del *reader*.

1.4.6 Conexión de antenas para sistemas inductivos

Las antenas de los *readers* en sistemas de RFID acoplados inductivamente generan flujo magnético que se usa para el suministro de poder al *transponder* y para enviar mensajes entre el *reader* y el *transponder*. Esto da lugar a tres requisitos fundamentales para los requerimientos de diseño de una antena de *reader* (La profundización de estos temas no forma parte del objetivo de este documento por los cual solo se mencionaran):

- Una corriente máxima i1 en la bobina de la antena, para un flujo magnético máximo ϕ.
- Suministrar la energía necesaria para ser utilizada para la generación de flujo magnético.
- Suficiente ancho de banda para no distorsionar la señal portadora modulada con datos

Dependiendo en el rango de frecuencia, pueden usarse procedimientos diferentes para conectar la bobina de la antena a la salida de transmisor del *reader* uno de ellos es la conexión directa de la bobina de la antena al módulo de salida usando una energía equivalente o suministrando energía a la bobina de la antena por medio del cable coaxial.

1.5 Principios de operación

En este apartado se describe la interacción básica entre *tags* y *readers*; como es que se transfieren los datos entre estos dos dispositivos.

Las primeras aplicaciones comerciales de RFID datan de finales de la década de los 60, cuando varias compañías desarrollaron métodos para evitar el robo de artículos en las tiendas mediante *tags* que almacenaban un solo bit de información. Es decir hay un *tag* dentro de la "zona de lectura" o no lo hay. Es por esto que los sistemas básicos y elementales de RFID tenían un costo de producción realmente bajo y con resultados efectivos. A éstos sistemas se les conoce como "*1-bit transponder*".

1.5.1 1-bit transponder

Estos dispositivos básicamente se utilizan en sistemas electrónicos antirrobo (implementado principalmente en tiendas desde hace más de 4 décadas). A este sistema se le denomina EAS (*Electronic Article Surveillance* por sus siglas en ingles).

Un EAS esta compuesto básicamente por un *reader,* un *tag* y un dispositivo de desactivación el cual es opcional[5]. Este dispositivo de desactivación se utiliza para desactivar el *tag* luego de que el producto al cual está asociado haya sido comprado (Guía VDI 4470, *Anti-theft systems for goods*. Contiene las definiciones y procedimientos y pruebas para los cálculos de los rangos de detección y las falsas alarmas). Usualmente los dispositivos de desactivación se encuentran en las cajas de las tiendas y los dispositivos detección de robo se encuentran en todas las entradas y salidas de las tiendas. De tal modo que si un artículo no ha sido desactivado y sale de la tienda el sistema lo detecta y activa algún tipo de alarma sonora.

1.5.1.1 radio frecuencia

La radio frecuencia se genera a partir de circuitos LC de tipo resonantes, con una frecuencia de resonancia denominada f_R. Los sistemas modernos utilizan pistan delgadas que hacen las veces de bobinas debido a la ligera separación entre ellas, tal como se muestra en la figura siguiente:

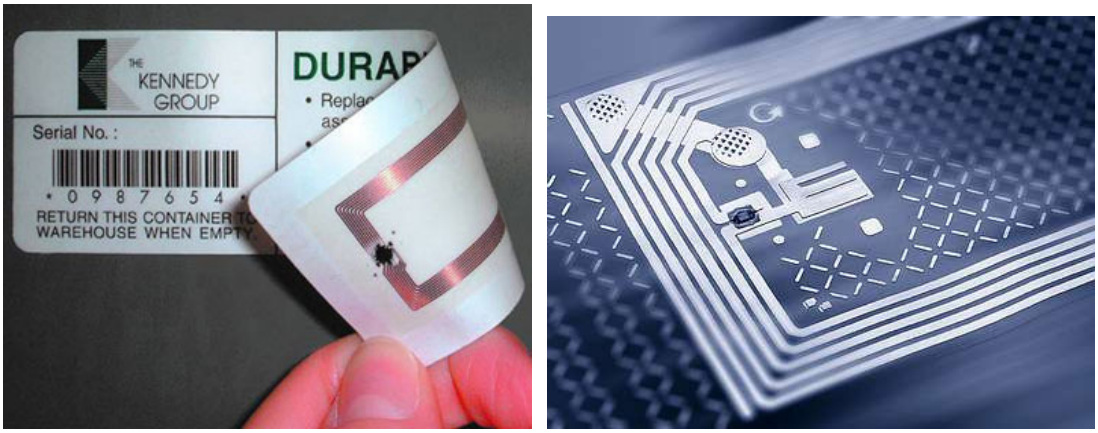


Figura 1.5.a Pistas de los tags RFID

Debido la los materiales con los que se pueden hacer estas pistas, resulta factible que estos circuitos sean bien delgados así como también flexibles.

[5] U.S. Patents Via Thomson Dialog NewsEdge) Pub. Number US7109867
Appl. Data 10 20040909, Applicant Avery Dennison Corporation, Inventor(s) Forster, Ian James

Figura 1.5.b Pistas de tags RFID

Para asegurarse que la resistencia de *damping* que presenta el circuito no sea muy alta y que no reduzca la calidad de la resonancia del circuito a niveles no aceptables, el espesor de las pistas (generalmente de aluminio) ubicadas sobre la capa delgada de polietileno debe de ser por lo menos de 25 μm (Jörn, 1994).

Por su parte el *reader* genera un campo magnético variable en el tiempo dentro del rango de las radio frecuencias. Si un circuito resonante LC se aproxima al campo magnético generado por el *reader*, entonces se induce energía del campo magnético sobre el circuito resonante debido a sus bobinas (ley de Faraday).

Sin embargo, los cambios de voltaje que se producen de éste acercamiento son bien débiles y por ende difíciles de detectar. Pese a esto la señal debe de ser lo mas clara posible para que el dispositivo de seguridad pueda ser detectado de una manera confiable. Es por esto que se usa una técnica particular: la frecuencia del campo magnético generado no es constante, sino variable. Esto da origen a que el generador de frecuencia cruce continuamente entre los valores máximos y mínimos. El rango de frecuencia para estos sistemas es generalmente 8.2MHz ±10% (Jörn, 1994).

Siempre que el barrido del generador de frecuencias corresponda exactamente con la frecuencia de resonancia del circuito del *tag*, el *transponder* comenzará a oscilar, produciendo así una clara caída de los voltajes del generador.

Usualmente los *tags* no se remueven de los artículos cuando estos son comprados, por lo que ésos tienen que ser alterados para que no activen el sistema antirrobo. Para lograr esto, en las cajas hay un dispositivo de desactivación. Este genera un campo magnético lo suficientemente fuerte que hace que el voltaje inducido destruya el capacitor del *tag*. Esto es posible porque los capacitores han sido diseñados intencionalmente con puntos de "cortocircuito". Luego de que se ha arruinado el capacitor, el *tag* ya no se puede energizar

de vuelta, aunque esté bajo el rango de acción del campo magnético y de ésta forma es que no activa ningún tipo de alarma a la hora de pasar por las antenas.

Las antenas de marco grande se utilizan para generar un campo magnético variable en el área donde se quieren detectar los *transponders*. Existen varios modelos para estas antenas sin embargo el principio de funcionamiento es el mismo.

Figura 1.5.c Se muestran algunos tipos de antenas de marco grande

Estas antenas son colocadas en las puertas de los almacenes y tienen un alcance promedio de 2m. Sin embargo existen ciertos materiales que pueden afectar la frecuencia de resonancia (como por ejemplo los metales o materiales que tengan su propia frecuencia de resonancia) y que pueden llegar a tener un efecto negativo en la detección del *tag*. Para este tipo de materiales se recomienda utilizar un *tag* más grande (generalmente de 50 mm x 50 mm como máximo).

1.5.1.2 microondas

En el caso de los sistemas EAS basados en microondas (frecuencias comprendidas entre 300 MHz y 300 GHz), estos explotan la generación de armónicos y los integran con componentes de características no lineales, tales como los diodos.

El armónico de un voltaje sinusoidal A con una frecuencia f_A es un voltaje sinusoidal B, cuya frecuencia f_B es un múltiplo entero de la frecuencia f_A. los subarmónicos de la frecuencia f_A son las frecuencias: $2f_A$, $3f_A$, $4f_A$, etc.

En principio, en una red con dos terminales de características de resistencias no lineales, la energía es consumida de tal forma que solo una parte de energía de la primera armónica es convertida en oscilación de armónicas. En condiciones favorables, la multiplicación de f por f x n ocurre con una eficiencia de $\eta = 1/n^2$. Si el almacenamiento de energía no linear es utilizado para la multiplicación entonces no se establecen perdidas idealmente (Fleckner, 1987).

Los diodos capacitivos son particularmente utilizados para almacenar energía no lineal para la multiplicación de frecuencias. El número asi como la intensidad de los armónicos generados dependen de la capacitancia del diodo básicamente. Es decir si por ejemplo un *tag* se coloca en el rango de operación de un transmisor de microondas que transmite a 2.45 Ghz. El segundo armónico, cuyo valor es de 4.90 GHz es generado por las características físicas del diodo del *transponder* y es a su vez retransmitido hacia un receptor el cual está compuesto por un filtro que permite detectar una señal de frecuencia especifica.

La disposición de *1-bit transponder* es simple: un diodo capacitivo se conecta a la base de un dipolo ajustado a la frecuencia de la portadora. La portadora generalmente tiene una de las siguientes frecuencias: 915 MHz, 2.45 GHz y 5.6 GHz. Si por ejemplo la portadora tiene una frecuencia de 2.45 GHz, el dipolo debe de tener una longitud de 6 cm.

Usualmente este tipo de dispositivos EAS por microondas se utilizan para proteger la mercadería textil en una tienda o almacén. Los *transponders* son hechos a base de una cubierta fuerte de plástico. Se remueven usualmente cuando el cliente ha comprado un a mercadería y generalmente son vueltos a utilizar posteriormente en otra prenda. Estos *tags* se muestran en las siguientes figuras:

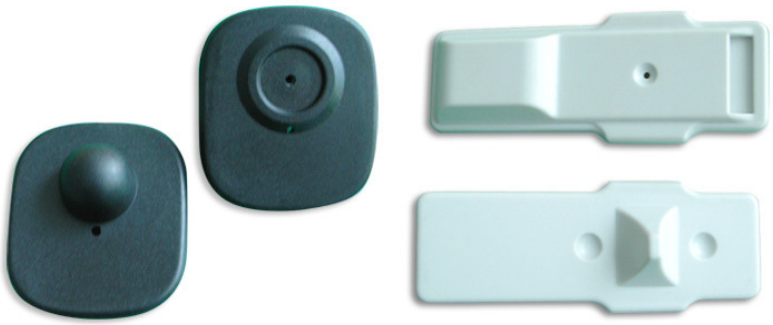


Figura 1.5.d: Tags de microondas

2.5.1.3 Electromagnéticas

Trabajan en el rango de 10 Hz a 20 KHz. Los elementos de seguridad tienen una franja magnética de metales suaves con una curva de histéresis muy inclinada. La magnetización de estas franjas es periódicamente revertida.

Este tipo de sistemas esta optimizado mediante la superposición de secciones de señales adicionales con altas frecuencias por encima de la señal principal. La no linealidad de la curva de histéresis genera no solo armónicos pero sino también segmentos de señales con

sumas y restas de frecuencias. Por ejemplo para una señal principal de frecuencia fS=20 Hz y las señales adicionales f1=3.5 y f2=5.3 KHz, se generan las siguientes señales para el primer orden:

f1 + f2 = f1+2 = 8.80 KHz
f1 − f2 = f1−2 = 1.80 KHz
fS + f1 = fS+1 = 3.52 KHz y así sucesivamente.

Para este tipo de sistemas los *tags* utilizados son en forma de franjas autoadhesivas de algún par de centímetros hasta una longitud máxima de 20 cm. Debido a que la frecuencia de operación de estos sistemas es demasiado baja, el sistema electromagnético se convierte en el sistema ideal para productos metálicos. Sin embargo la desventaja de este sistema es que la posición que tenga el *transponder* es esencial para una lectura correcta. Para una lectura correcta del *tag*, por la banda de metal deben de pasar verticalmente las líneas de campo magnético del emisor.

Para el proceso de desactivación, los *tags* están totalmente cubiertos con una capa de metal magnético dura o parcialmente cubiertos por la misma. Después de la compra se pasa el *tag* por un imán permanente fuerte a lo largo de la franja magnética (Plotzke et al., 1994).

Si se desea reactivar el *tag* para volver a ser utilizado, es necesario simplemente desmagnetizarlo. El proceso de desactivación y reactivación del *transponder* se puede realizar cualquier número de veces. En la siguiente imagen se presentan los *tags* electromagnéticos usados en productos de consumo personal.

Figura 1.5.e. Muestra un tag Escondido dentro de una etiqueta de loción

1.5.2 Full y Half duplex

Pese a la económico de estos sistemas descritos de 1 solo bit de información que básicamente aprovechan los principios físicos (oscilación, armónicos, etc.), hay otros sistemas que poseen mucha mas información. En los sistemas que de detallaran mas adelante los *tags* utilizan microchips electrónicos como dispositivos portadores de datos (usualmente en el rango de los kilobytes). Además de contar con una memoria para almacenar datos, estos sistemas cuentan también con la ventaja que pueden intercambiar datos con el dispositivo lector (que es el mismo emisor) y el *tag*. Esta transferencia de información se hace en dos vías, una en *half duplex* y la otra en *full duplex*.

En el sistema de Half Duplex (HDX) la transferencia de datos del *tag* hacia el *reader* se alterna con la del *reader* hacia el *tag*. Para frecuencias menores a 30 MHz lo mas usual es utilizar el procedimiento de modulación de carga, el cual se puede realizar con una circuiteria simple.

Para las frecuencias mayores a los 100 MHz se utiliza una técnica similar que consiste en ejercer una influencia en el campo electromagnético por medio de armónicos.

En un sistema *Full Duplex* (FDX) la transmisión de datos del *reader* hacia el *tag* o del *transponder* hacia el *reader* se hace de manera simultánea. Para esto se utilizan técnicas que permiten que los datos sean transmitidos del *tag* a una fracción de la frecuencia del *reader* (subarmónica) o en una completamente independiente (armónico).

Estos dos procedimientos tienen algo en común, la transferencia de energía del *reader* hacia el *transponder* y la del *tag* hacia el *reader* se hace de manera continua y además es independiente la dirección donde fluyen los datos. A diferencia de los sistemas secuenciales en los cuales la transferencia de energía del *tag* hacia el *reader* se da por un período de tiempo limitado.

Desafortunadamente la literatura relacionada con RFID no se ha podido estandarizar o por lo menos llegar a un acuerdo en cuanto a la nomenclatura a utilizar, dado que existen muchas variantes de los sistemas, tanto de full como de *half duplex*. También hay sistemas secuenciales (SEQ), en los cuales la transferencia de energía del *tag* hacia el *reader* se da por un periodo limitado de tiempo (por pulsos, por cual a estos sistemas se les llama pulsantes). A continuación se detalla de manera grafica el funcionamiento de los tres tipos de sistemas mas comunes, en función del tiempo.

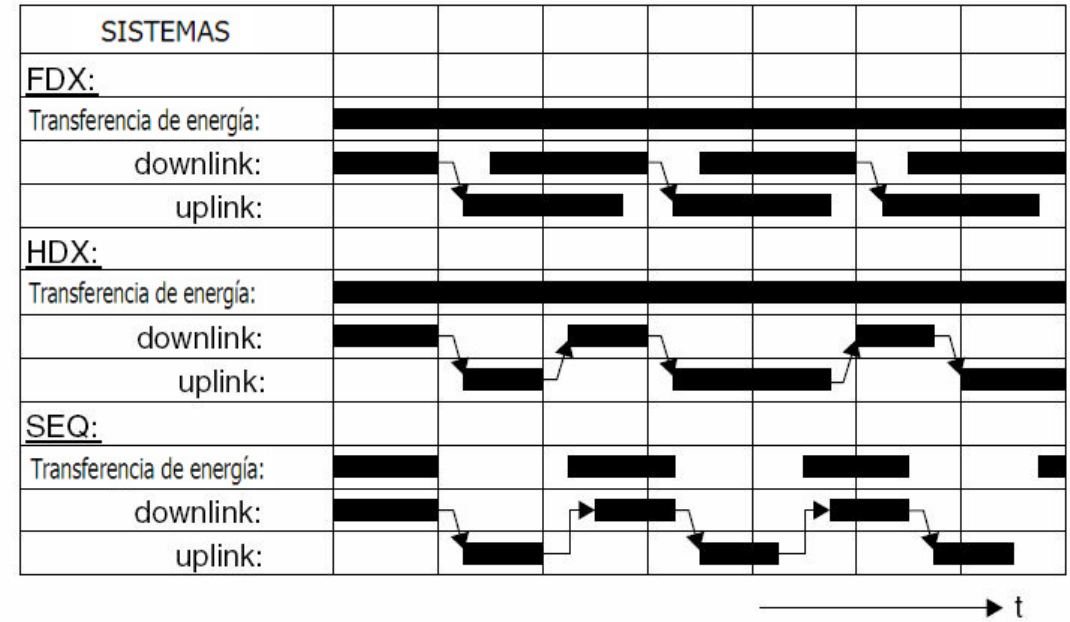


Figura 1.5.f Comparación de los sistemas HDX, FDX y secuenciales

1.5.2.1 acople inductivo

Un tag con acoplamiento inductivo esta compuesto por un dispositivo electrónico portador de datos, un tan solo microchip (en la mayor parte de los casos) y una bobina de área grande que funciona como antena.

Los *tags* de acople inductivo suelen ser utilizados de manera pasiva la mayor parte del tiempo. Es decir que la energía que necesitan para que opere el microchip tiene que proveerla el *reader*. Por tal motivo, el embobinado de la antena del *reader* genera un campo magnético fuerte de alta frecuencia, que penetra el área de corte transversal de la bobina y el área aledaña a este.

Como la longitud de onda de la frecuencia utilizada (para menores a 135 KHz: 2400 m y para 13.56 MHz: 221 m) es varias veces mayor que la distancia entre la antena del reader y el *tag*, campo electromagnético puede considerarse como alterno.

Una parte pequeña del campo emitido penetra el embobinado del *tag*, el cual está alejado a cierta distancia del embobinado del *reader*. Se genera un voltaje U_i en la bobina del *transponder* por inducción. Dicho voltaje se rectifica y sirve como fuente de energía para el dispositivo portador de datos (microchip). Un capacitor C_r se conecta en paralelo con el embobinado de la antena del *reader*; su valor de capacitancia debe de ser tal que con la inductancia del embobinado de la antena del *reader*, forme un circuito paralelo resonante, con una frecuencia de resonancia que corresponda con su frecuencia de transmisión.

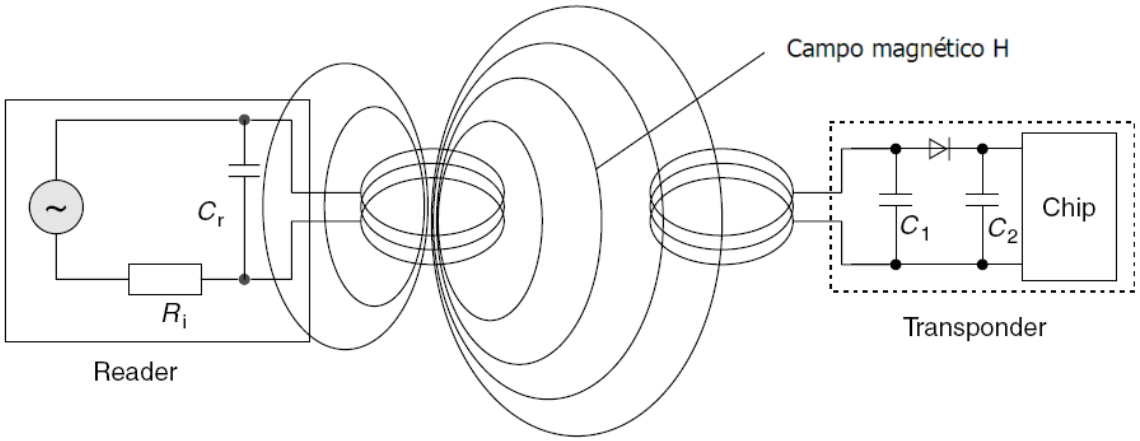


Figura 1.5.g Representación del campo magnético entre el reader y el tag

El embobinado de la antena del *tag* y el capacitor C_1 forman un circuito resonante sintonizado a la frecuencia de transmisión del *reader*. El voltaje U del embobinado del *tag* alcanza su valor máximo debido a la resonancia del circuito paralelo.

Por analogía, por la disposición de los dos embobinados se puede tratar como un transformador, donde el embobinado primario sería el del *reader* y el secundario el del *tag*. En este caso la eficiencia de la transferencia de energía entre los embobinados de la antena del *reader* y la del *tag*, es proporcional a la frecuencia de operación f, al número de vueltas n y la distancia entre las 2 bobinas.

Cuando la frecuencia f aumenta, la inductancia que se requiere en el embobinado del *tag*, así como su numero de vueltas n, se decrementan. Por ejemplo para una frecuencia de operación de 135 KHz se tiene un número aproximado de vueltas entre 100 y 1000. Mientras que para una frecuencia de 13.56 MHz entre 3 y 10 vueltas. Esto se da porque el voltaje en el *tag* sigue siendo proporcional a la frecuencia f.-

Si un *tag* con frecuencia de resonancia propia que corresponda con la frecuencia de transmisión de un *reader*, se encuentra dentro del campo magnético alterno de la antena del *reader*, el *tag* utiliza la energía del campo magnético. La retroalimentación resultante del *tag* en la antena del *reader* puede ser representada como una impedancia transformada Z_T en el embobinado del *transponde*r.

Alternar la resistencia de carga entre alimentada y no alimentada en la antena del *tag* conlleva a un cambio en la impedancia Z_T, y esos voltajes cambian en la antena del *reader*. Esto tiene el efecto de una modulación de amplitud del voltaje U_L en la bobina de la antena del *reader* producido por un *tag* remoto. Si el tiempo con el cambia la resistencia carga entre apagada y encendida es controlado por los datos, estos datos pueden ser transferidos del *tag* hacia el *reader*. A este tipo de transferencia de datos se le conoce como modulación de carga.

Para que el *reader* pueda leer los datos, el voltaje que llega a la antena del *reade*r debe de ser rectificado esto representa una desmodulación para una señal de amplitud modulada.

Debido al acople magnético débil entre la antena del *reader* y la del *tag*, las fluctuaciones del voltaje en la antena del *reader* que representa la señal útil, son más pequeñas por orden de magnitud que el voltaje de la salida del *reader*.

Por ejemplo para un sistema de 13. 56 MHz, con un voltaje de aproximadamente 100 V se podría esperar una señal útil de aproximadamente 10 mV (=80 dB relación señal/ruido). Debido a que la detección de éste cambio leve del voltaje requiere la elaboración de un circuito altamente complicado, se utilizan bandas laterales de modulación creadas por la modulación de amplitud.

Si una resistencia de carga adicional se coloca en el *tag* y ésta es alimentada y no alimentada a una frecuencia muy alta f_s se crean entonces dos líneas dentro del espectro a una distancia $\pm f_s$ alrededor de la frecuencia transmisión del *reader* f_{reader}. Éstas pueden ser detectadas mucho más fácilmente siempre y cuando f_s sea menor que f_{reader}.

A esta nueva frecuencia se le denomina subportadora. La transferencia de datos se da por las modulaciones ASK, FSK o PSK de la subportadora. Esto representa una modulación por amplitud de la subportadora.

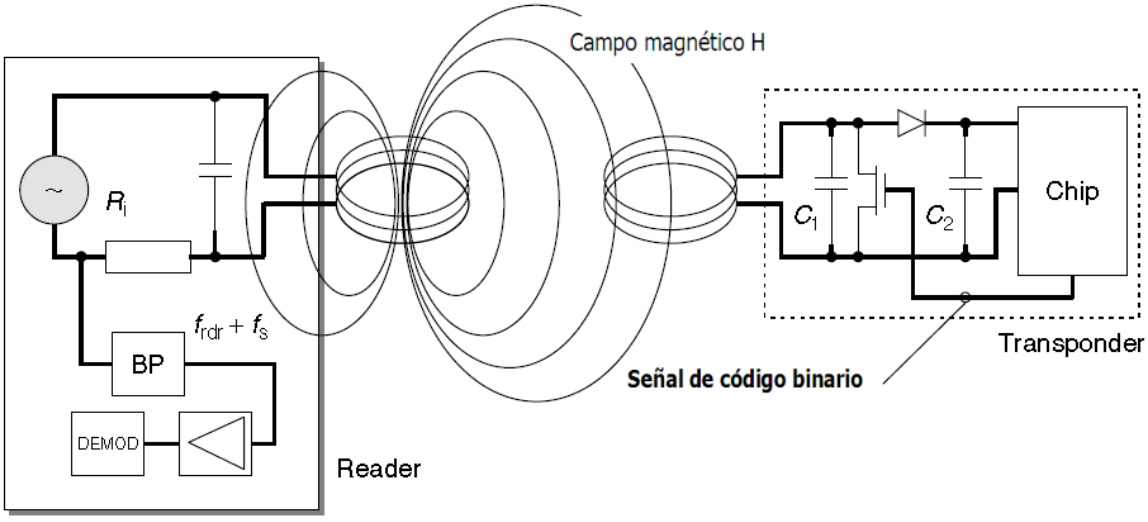


Figura 1.5.h Representación del campo magnético entre el reader y el tag

Esta modulación de bandas laterales puede ser separada de una señal fuerte del *reader* por medio de un filtro pasa banda en una de las dos frecuencias $f_{reader} \pm f_s$. Una vez ha sido amplificada la señal subportadora es más fácil de demodular.

Debido a que se requiere un ancho de banda demasiado grande para la transmisión de una subportadora, este procedimiento sólo puede ser usado en los rangos de frecuencias ISM: 6.78 MHz, 13. 56 MHz y 27. 125 MHz.

1.5.2.2 Sistemas de largo alcance

Para los sistemas de RFID en los cuales la distancia entre el reader y el tag es mayor que 1 m son llamados sistemas de largo alcance. Estos sistemas operan con frecuencias UHF, 868 MHz en Europa y 915 en EEUU. También con frecuencias de microondas de 2.5 GHz y 5.8 GHz. Debido a la corta longitud de onda de estos rangos de frecuencia las antenas pueden ser de dimensiones pequeñas y de una mayor eficiencia.

Para este tipo de sistemas es necesario calcular el camino de pérdidas en el espacio vacío a_F en relación con la distancia *r* entre el *tag* y la antena del *reader*, la ganancia G_T y G_R del *tag* y de la antena del *reader*, además de la frecuencia de transmisión f del *reader*:

$$a_F = -147.6 + 20\log(r) + 20\log(f) - 10\log(GT) - 10\log(GR)$$

El camino de pérdidas en el espacio vacío es una medida de la relación que existe entre la potencia de HF emitida por un *reader* en el espacio vacío y la potencia HF recibida por el tag.

Usando una tecnología de semiconductores de bajo consumo de potencia, los chips de los *tags* pueden ser producidos para consumir una potencia no mayor de 5 μW (Friedrich and Annala, 2001). La eficiencia de un integrado rectificador se puede asumir entre 5 y 25% en los rangos de UHF y microondas (Tanneberger, 1995). Para una eficiencia dada del 10%, se requiere una potencia recibida de P_e = 50 μW en la terminal de la antena de *transponder*.

Para poder alcanzar largas distancias, mayores a 15 m o incluso para poder controlar el consumo de potencia del *tag* en un rango aceptable. Para *tags* activos, estos tienen regularmente una materia de respaldo para proveer energía al chip. Para prevenir que esta batería se descargue innecesariamente, los microchips generalmente tienen un modo "apagado" y otro de "stand-by". Si el *tag* se mueve fuera del rango de alcance del *reader*, entonces el chip automáticamente cambia su estado al de "stand-by", modo en el cual su consumo de potencia es de solamente algunos μA. El chip no se reactiva al menos que reciba una señal lo suficientemente fuerte por parte del *reader*, la cual hace que vuelva a su funcionamiento normal. De todas formas la batería de un tag activo nunca provee potencia para la transmisión de los datos, sino más bien sirve únicamente para proveer voltaje al microchip, ya que la transmisión de datos es exclusiva del *reader* debido al campo magnético que éste genera.

1.5.2.3 Sistemas de corto alcance

Conocidos también como sistemas de acoplamiento magnético cercano, son diseñados para trabajar en los rangos de 0.1 cm hasta 1 cm. Usualmente para la lectura el *tag* se coloca dentro del *reader* o sobre una superficie (a lo que se le conoce como *''touch & go*").

De igual manera que para los sistemas anteriores, se puede hacer una analogía del funcionamiento este sistema con el funcionamiento de un transformador. En donde el embobinado primario sería el *reader* y e secundario el *transponder*. Una corriente alterna de alta frecuencia en las bobinas del primario genera un campo magnético de alta frecuencia en el núcleo paz aire de la red, permitiendo así que fluía también por la bobina del tag. Tal como se muestra en la siguiente figura:

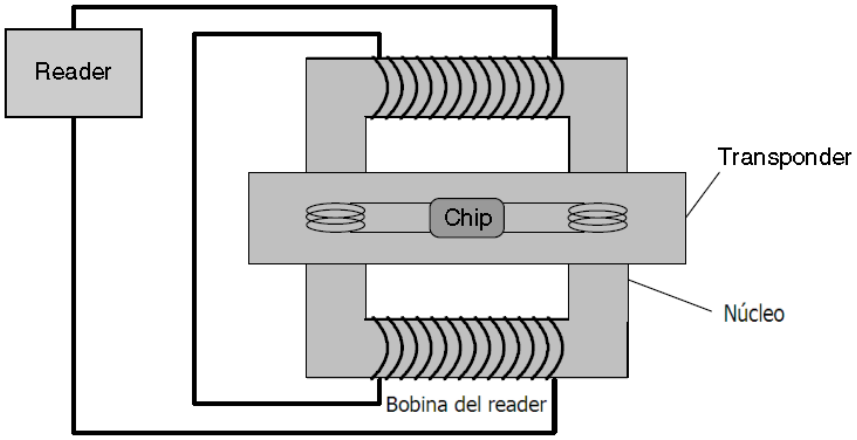


Figura 1.5.i Representación de la analogía del reader con el transformador

Como el voltaje U inducido en la bobina del *tag* es proporcional a la frecuencia f de la corriente, la frecuencia seleccionada para la transferencia de energía debe de ser lo más alta posible. En la práctica se utilizan frecuencias en un rango de 1 a 10 MHz, con el propósito de dejar bajas pérdidas en el núcleo del transformador, el cual debería de ser preferiblemente ferrita.

A diferencia de lo sistemas con acople inductivo o de microondas, la eficiencia de la transferencia de potencia desde el *reader* hacia el *tag* es muy buena. Los sistemas de acople cercano son ideales para operar con chips que consumen una alta potencia. Esto incluye microprocesadores (que requieren unos 10 mW por operación), es por esto que estos sistemas usan tarjetas que en su mayoría incorporan microprocesadores.

Los parámetros mecánicos y eléctricos para las tarjetas de acople cercano están definidos por su propio estándar, ISO 10536.

2.5.2.4 acople eléctrico

En estos sistemas el *reader* genera un campo magnético fuerte de alta frecuencia. La antena del *reader* consiste en un área conductiva grande (electrodo). De tal modo que si un voltaje de alta frecuencia es aplicado en el electrodo se forma un campo eléctrico de alta frecuencia entre el electrodo y tierra. Para esto se requiere que el voltaje varíe entre unos cuantos cientos de voltios a unos miles, este voltaje es generado en el *reader* debido a un aumento de voltaje en el circuito resonante la frecuencia de resonancia de dicho circuito corresponde con la frecuencia de transmisión del *reader*.

La antena del *transponder* esta hecha por 2 capas conductivas que actúan como electrodos. Si el *tag* se coloca entre el campo eléctrico del *reader*, entonces el voltaje se genera entre los 2 electrodos del *tag*, el cual sirve para proveer energía a los chips del *tag*. Las corrientes que circulan por las superficies de los electrodos del *transponder* son bien bajas.

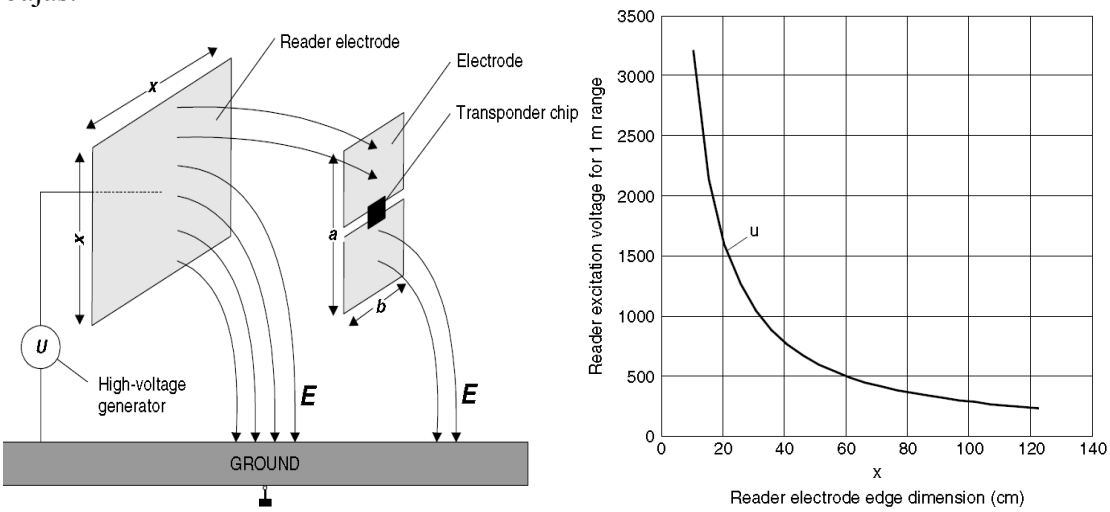


Figura 1.5.j Representación de las capas inductivas que actúan como electrodos

1.5.3 Sistemas secuenciales

Se habla de sistemas secuenciales cuando la transmisión de los datos desde el *reader*, por medio de la portadora alterna con la transferencia de datos del *tag* hacia el *reader*.
Estos sistemas se pueden dar también por diferentes formas de acoplamiento.

1.5.3.1 Acoplamiento inductivo

Estos sistemas de acople inductivo se utilizan para frecuencias que operan a frecuencias menores de 135 MHz. Nuevamente se puede hablar de un acople de transformador que se

crea entre el embobinado del *reader* y el del *tag*. El voltaje inducido que se genera en el embobinado del *tag*, el cual es alterno se rectifica y para ser utilizado como fuente de energía.

Para poder obtener una eficiencia elevada en la transferencia de datos, la frecuencia del *tag* debe de coincidir con la del *reader*. Para conseguir esta sincronización el transponder tiene un chip con un capacitor incorporado el cual tiene la función de compensar las tolerancias en las frecuencias resonantes.

A diferencia de los sistemas de *half* y *full duplex*, en los secuenciales el transmisor del *reader* no opera de manera continua. La energía que se transfiere hacia el transmisor para la transferencia de información, carga un "capacitor de carga" para poder almacenar energía. El chip del tag cambia en modo "*stand-by*' o en modo de ahorro de energía durante el proceso de carga. De tal forma que toda la energía recibida se utiliza para cargar el capacitor. Es así como después de un periodo de carga determinado, el transmisor del *reader* se apaga.
La energía que se almacena en el *transponder* es utilizada para mandar una respuesta al *reader*.

La capacitancía mínima que puede tener el capacitor de carga se debe de calcular en base al consumo de energía del chip y el voltaje necesario para su funcionamiento. De tal forma que mediante la siguiente formula se puede determinar dicho valor de capacitancía:

$$C = \frac{Q}{U} = \frac{It}{[V_{\max} - V_{\min}]}$$

Donde V_{max} y V_{min} son los valores extremos de voltaje que no deben de ser sobrepasados. I es el consumo de energía del chip mientras esta en funcionamiento y t es el tiempo que se necesita para la transmisión de datos del *tag* hacia el *reader*.

Como ya se menciono anteriormente los sistemas de *full duplex* la transferencia de energía del *reader* hacia el *tag* se da al mismo tiempo que la transferencia de datos en ambos sentidos, por lo cual el chip pasa siempre en modo de operación. Todo lo contrario a los sistemas secuenciales en los cuales durante el proceso de carga el chip se encuentra en estado de ahorro de energía o "stand-by". Al principio del proceso de carga el capacitor se encuentra completamente descargado por lo cual representa un valor ohmico muy bajo. Debido a esto una cantidad máxima de corriente fluye a través del capacitor de carga. Cuando dicho capacitor se empieza a cargar, la corriente de carga empieza a decrementarse de manera exponencial y llega a un valor de cero cuando el capacitor está completamente cargado.

En los sistemas secuenciales, un ciclo completo de lectura se realiza en 2 etapas: la de carga y la de lectura propiamente dicha. La primera etapa se termina cuando el detector de ruptura, en el embobinado del *tag*, detecta que el campo del *reader* ha sido apagado o

que ya no esta presente. Cuando esta etapa termina un chip integrado de oscilación, que usa el circuito resonante del *transponder* es activado. Un campo magnético alterno débil se genera en el embobinado del *transponder* y puede ser detectado por el *reader*.

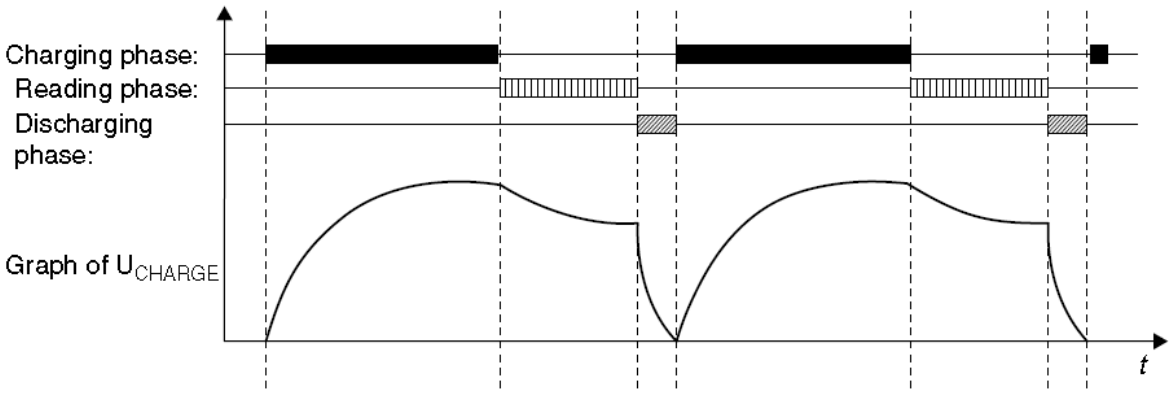


Figura 1.5.g Representación del ciclo de lectura

La frecuencia de transmisión del tag corresponde con la frecuencia de resonancia de su embobinado, el cual es ajustado a la frecuencia transmisión del *reader* desde que se generó.

Para poder modular la señal de HF generada en ausencia de una fuente de energía, un capacitor adicional para modulación se conecta en paralelo con el circuito resonante. Después que los datos han sido transmitidos, se activa la etapa de descarga, en la cual capacitor de carga se descargará completamente. Esto garantiza un *power-on-reset* al inicio del siguiente ciclo de carga

1.5.3.2 tags de onda acústica de superficie

A estos sistemas se les conoce como SAW (*Surfaces Acustic Wave* por sus siglas en ingles). Usualmente este tipo de sistemas se utilizan para medir variables físicas tales como la temperatura, presión, torque, aceleración, humedad, etc. Los dispositivos SAW no requieren de una fuente de alimentación (es decir que solo son de tipo pasivo). A diferencia de los *tags* basados en chips, no necesitan energía continua (DC) para alimentar su circuitería y poder hacer el envío de la información.

Un sistema completo de SAW consiste en un *tag* con antena dipolo y un *reader* con su respectiva antena. A diferencia de los sistemas tradicionales de RFID, los tags no son basados en chips o circuitos integrados, sino mas bien utilizan un transductor de acople de tipo interdigital, denominado IDT (*Inter Digital Transducer* por sus siglas en ingles). Los tags usan cristales o substratos piezoeléctricos (materiales que permiten que las ondas superficiales sean generadas mediante una excitación eléctrica) con “reflectores”

(pequeñas paredes que provocan que la onda acústica se refleje) e intervalos preestablecidos para representar los datos del *transponder*.

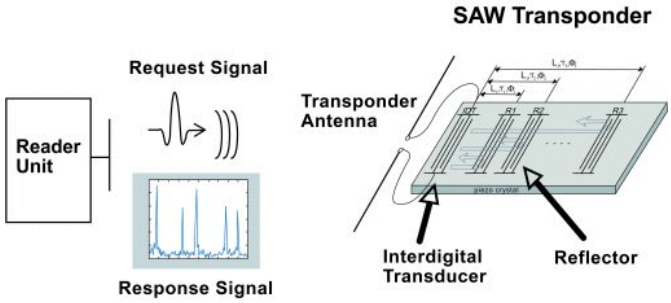


Figura 1.5.g modo de operación de los tags de onda acústica de superficie

Una señal de radio frecuencia de baja potencia y una frecuencia de 2.45 GHz es transmitida por el *reader* y la recibe la antena del *transponder* la cual aplica un impulso eléctrico al IDT. Este impulso genera ondas de superficie que viajan por el *tag*, algunas de estas ondas son absorbidas por el substrato y otras reflejadas de vuelta hacia el IDT, el cual responde con una señal de RF hacia el *reader*. La amplitud, frecuencia, fase y tiempo de llegada de ésta respuesta provee información acerca del *tag*. El espaciado de estas señales reflejadas (llamadas *echos* también) indica el lugar y la posición relativa de cada reflector, de tal forma que ésta posición puede ser calculada y representada en forma de datos. Los dispositivos de SAW

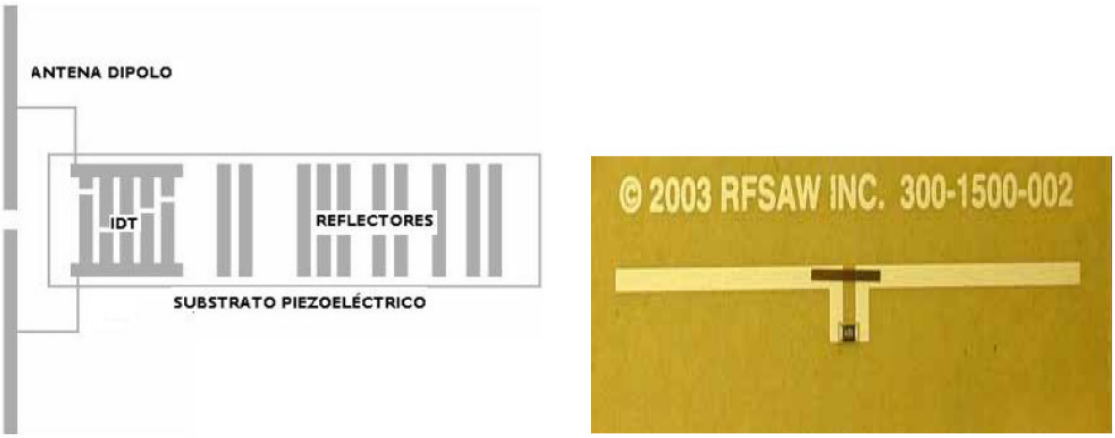


Figura 1.5.g Tags de onda acústica de superficie SAW

Referencias:
Guia VDI 4470, Anti-theft systems for goods. Contiene las definiciones y procedimientos de pruebas para los calculos de los rangos de detección y las falsas alarmas.

1.6 Codificación y modulación

En el diagrama de bloques de la Figura 1.6.a se describe un sistema de comunicación digital. Similarmente, la transferencia de datos entre el *reader* y el *tag* en un sistema RFID requiere 3 bloques básicos de funcionamiento.

- *Reader* (*Transmitter*): codificación de señal (*signal processing*) y el modulador (*carrier circuit*).
- El medio de transmisión (*channel*).
- *Transponder* (*Receiver*): el demodulador (*carrier circuit*) y el decodificador de canal (*signal processing*).

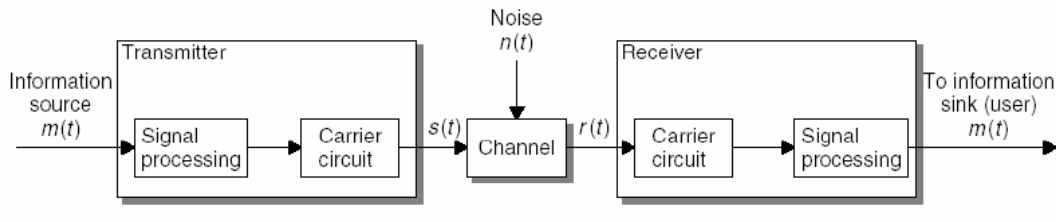


Figura 1.6.a. Esquema de funcionamiento de un sistema RFID.

Un sistema codificador de señal toma el mensaje a transmitir, su representación en forma de señal y la adecua óptimamente a las características del canal de transmisión.
Este proceso implica proveer al mensaje con un grado de protección contra interferencias o colisiones y contra modificaciones intencionadas de ciertas características de la señal.

1.6.1 Codificación en Banda Base.

Los signos binarios "1" y "0" pueden ser representados por varios códigos lineales. Los sistemas de RFID suelen usar una de las siguientes codificaciones: NRZ, Manchester, Unipolar RZ, DBP ("*diferential bi-phase*"), Miller o Codificación Pulso-Pausa (PPC).

Código NRZ (*No Return to Zero*):
Un '1' binario es representado por una señal 'alta' y un '0' binario es representado por una señal 'baja'. La codificación NRZ se usa, al menos, exclusivamente con una modulación FSK o PSK.

Código Manchester:

Un ‘1’ binario es representado por una transición negativa en la mitad del periodo de *bit* y un ‘0’ binario es representado por una transición positiva. El código Manchester es, por lo tanto, también conocido como codificación de ‘parte-fase’ (*splitphase coding*).

El código Manchester es frecuentemente usado para la transmisión de datos desde el *transponder* al *reader* basados en una modulación con sub-portadora.

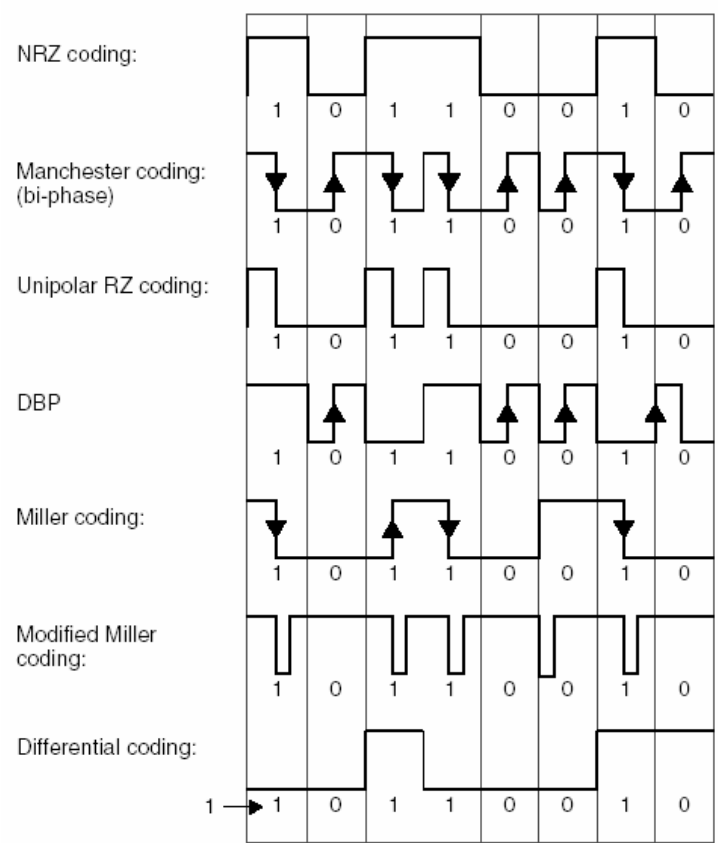


Figura 1.6.b. Representación grafica de las principales codificaciones.

Código Unipolar RZ:
Un ‘1’ binario es representado por una señal ‘alta’ durante la primera mitad del periodo de bit, mientras que un ‘0’ binario es representado por una señal ‘baja’ que dura todo el periodo de bit.

Código DBP:
Un ‘0’ binario es codificado por una transición, de cualquier tipo, en mitad del periodo de bit. Un ‘1’ es codificado con una ausencia de transición. Además, el nivel de señal es invertido a inicio de cada periodo de bit, de modo que el pulso pueda ser más sencillamente reconstruido en el receptor si es necesario.

Código Miller:
Un '1' es representado por una transición de cualquier tipo en la mitad del periodo de bit, mientras que el '0' binario es representado con la continuidad del nivel de la señal hasta el próximo periodo de bit. Una secuencia de ceros crea una transición al principio de cada periodo de bit, de modo que el pulso pueda ser más sencillamente reconstruido en el receptor si es necesario.

Código Miller Modificado:
En esta variante del código Miller, cada transición es reemplazada por un pulso 'negativo'. El código Miller Modificado es altamente recomendable para transmitir del *reader* al *tag* en sistemas RFID que usan acoplamiento inductivo.

Debido a la tan corta duración del pulso ($t_{pulso} << T_{bit}$) es posible asegurar una continua alimentación del *transponder* debido al campo magnético del *reader* mientras dura la transferencia de información.

Codificación Diferencial:
En la codificación Diferencial cada '1' binario que se tiene que transmitir causa un cambio en el nivel de la señal, así como para un '0' el nivel permanece invariante. El código diferencial puede ser generado muy simplemente a partir de una señal NRZ usando una puerta XOR y un Flip-Flor tipo D. En la siguiente figura vemos el circuito que logra este cambio en la señal.

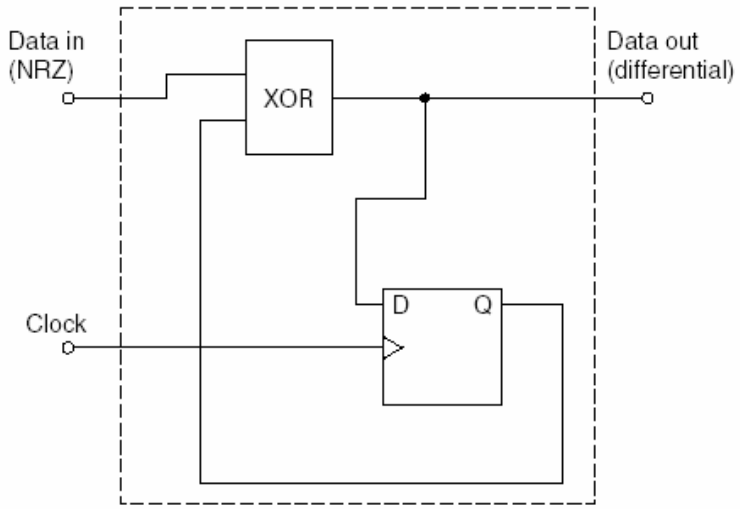


Figura 1.6.c. Generación de un código diferencial a partir de uno NRZ.

Codificación Pulso-Pausa:
En la codificación Pulso-Pausa (PPC – *Pulse Pause Coding*) un '1' binario es representado por una pausa de duración *t* antes del próximo pulso; un '0' binario es representado por una pausa de duración 2*t* antes del próximo pulso. Este método de

codificación es popular para la transmisión de datos del *reader* al *transponder* en los sistemas de RFID que usan acoplamiento inductivo.

Debido a la tan corta duración del pulso ($t_{pulso} << T_{bit}$) es posible asegurar una continua alimentación al *transponder* debido al campo magnético del *reader* mientras dura la transferencia de información.

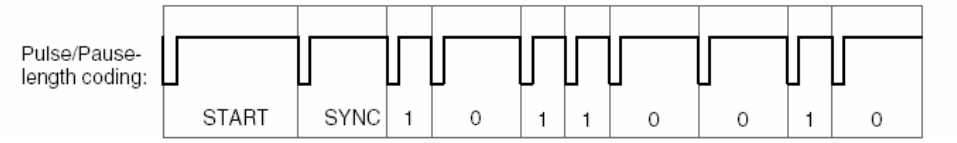


Figura 1.6.d. Transmisión de una señal usando PPC.

Debe tenerse en cuenta varias importantes consideraciones cuando se selecciona un posible sistema de codificación para un sistema RFID.
La consideración más importante es el espectro de la señal después de la modulación y lo susceptible que pueda ser a los posibles errores. Además, en el caso de *tags* pasivos (la alimentación de los *transponders* viene dada por el campo magnético que genera el *reader*), la fuente de alimentación (es decir, la señal que emite el *reader*) no debe ser interrumpida por una combinación inapropiada de los métodos de codificación de señal y modulación.

1.6.2 Modulación digital

La tecnología clásica de radiofrecuencia está fuertemente implicada con los métodos analógicos de modulación. Podemos diferenciar entre modulación de amplitud (AM), modulación de frecuencia (FM) y modulación de fase (PM), siendo éstas las tres principales variables de una onda electromagnética. Todos los demás métodos de modulación son derivados de cualquiera de uno de estos tres tipos.

Las modulaciones usadas en RFID son ASK (amplitude shift keying), FSK (frequency shift keying) y PSK (phase shift keying).

1.6.2.1 ASK (Amplitude shift keying)

En modulación ASK la amplitud de la oscilación de una portadora es variada entre dos estados u_0 y u_1 (*keying*) por un código de señal binario. U_1 puede tomar dos valores entre u_0 y 0. El intervalo entre u_0 y u_1 es conocido como el factor de trabajo (*duty* factor) *m*.

1.6.2.2 FSK 2 (Frequency shift keying)

En la modulación llamada '*2 frequency shift keying'* la frecuencia de la señal portadora se varía entre dos frecuencias f_1 y f_2.

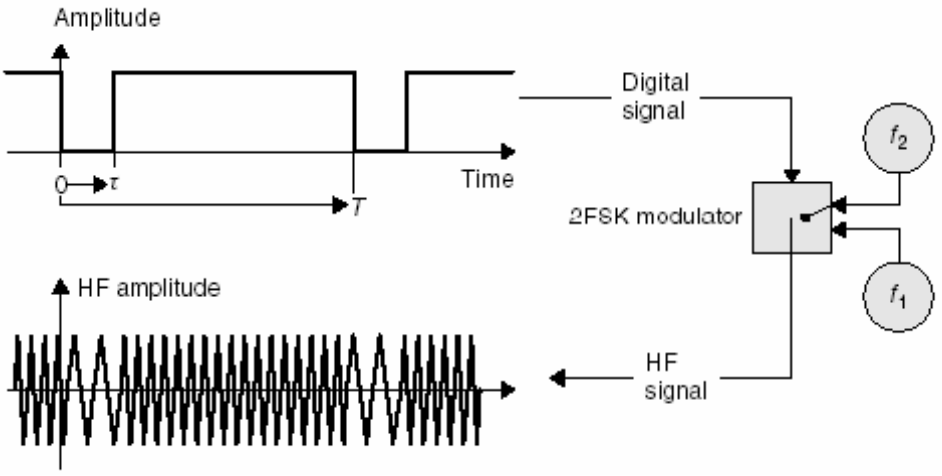


Figura 1.6.e. Generación de modulación 2FSK variando entre dos frecuencias *f1* y *f2* en el tiempo, con una señal binaria.

La frecuencia portadora es la media aritmética de las dos frecuencias características f_1 y f_2. La diferencia entre la frecuencia de la portadora y las frecuencias características es conocida como la desviación de frecuencia Δf_{CR}:

$$f_{CR} = \frac{f_1 + f_2}{2} \qquad \Delta f_{CR} = \frac{|f_1 + f_2|}{2}$$

1.6.2.3 PSK 2 (Phase shift keying)

En la modulación PSK los estados binarios '0' y '1' de una señal código se convierten en los respectivos "estados de fase" de la portadora, en relación a una fase de referencia. En este caso, la PSK 2, la fase de la señal varía entre los estados de fase de 0º y 180º.

1.6.2.4 Modulación con implementación de subportadora.

En los sistemas de RFID, las modulaciones que usan *subportadora* son básicamente usadas cuando se trabaja con acoplamiento inductivo, normalmente en las frecuencias

6.78MHz, 13.56MHz o 27.125MHz en transferencias de información desde el *transponder* al *reader*.

Para modular la *subportadora* se puede elegir entre ASK, FSK o PSK.

Cuando se obtiene la primera señal modulada (*subportadora* modulada), entonces se procede a una segunda modulación de la *subportadora* con la señal portadora (la que dará la frecuencia final a la que se transmitirá la señal).

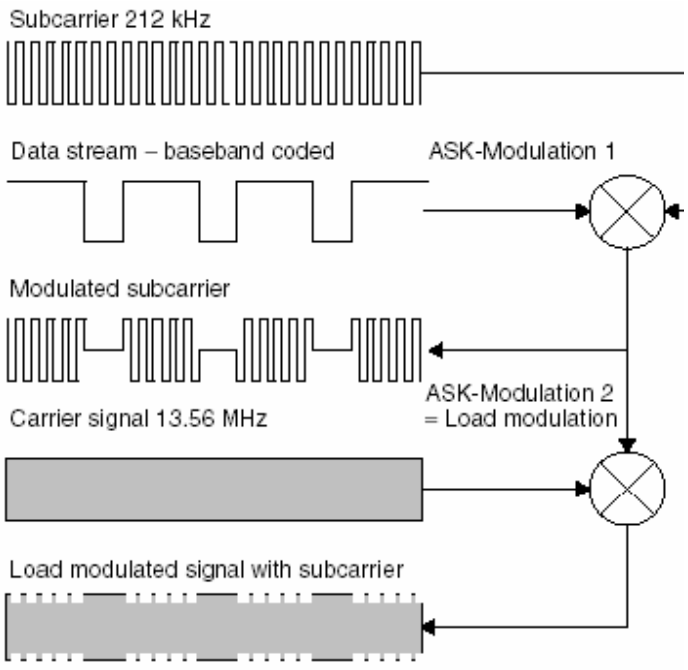


Figura 1.6.f. Proceso detallado de una modulación múltiple, con una *subportadora* modulada en ASK.

La ventaja de usar una modulación con *subportadora* sólo se aclara cuando se considera el espectro de la señal generada. Esta modulación inicialmente genera dos líneas espectrales a una distancia de ± la frecuencia de la *subportadora* f_H alrededor de la frecuencia central. La información se transmite, así, en las bandas laterales de las dos líneas *subportadoras*, dependiendo de la modulación de la *subportadora* generada a partir del código en banda base. Si la modulación usada es en banda base, las bandas laterales caerán justamente al lado de la señal portadora en la frecuencia central.

En los *transponders* que usan acoplamiento y que tienen unas pérdidas muy elevadas, la diferencia entre la señal portadora del *reader* f_T y las bandas laterales recibidas de la modulación varían en un rango de entre 80 y 90 dB.

Uno de los dos productos de la modulación con *subportadora* puede ser filtrado y remodulado usando la frecuencia de la modulación de las bandas laterales del flujo de

datos. Aquí es irrelevante si se usa la banda 'alta' $f_T + f_H$ o si se usa la banda 'baja' $f_T - f_H$ ya que la información está contenida en ambas.

1.7 Integridad de la información

Para la transmisión de datos por medio de tecnología inalámbrica es muy probable que se de un fenómeno de interferencia que pueda llegar a afectar o alterar el contenido de la información.
A continuación se detallaran los diferentes métodos utilizados en los sistemas RFID para mantener la integridad de la información y prevenir y corregir errores de transmisión en las tramas de datos. Si se desea información adicional con ejemplos y algoritmos se pueden consultar las siguientes fuentes:
- A. Tanenbaum. Computer Networks. Prentice-Hall International Editions (1989).
- W. Stallings. Local Networks. Macmillan Publishing Company (1990).
- J. Hammond, P. O'Reilly. Performance Analysis of Local Computer Networks. Addison Wesley (1988).

1.7.1 métodos de checksum

Por tal motivo se utiliza un *checksum*, el cual permite reconocer si ha habido un error en la transmisión así como también permite tomar medidas correctivas tales como la retransmisión de bloques de datos erróneos. Los procedimientos de *checksum* mas utilizados son la paridad de datos y el CRC.

1.7.1.1 Paridad de datos

Es una de las técnicas más comunes para revisar errores en la transmisión de datos. Este procedimiento consiste en adicionar a la trama de datos, compuesta de un byte, un bit adicional denominado "bit de paridad". Con dicho bit cada trama queda compuesta por 9 bits en total.

El bit de paridad indica si el número de bits con un valor de uno es par o impar.
Cuando se trata de una paridad par, se tiene que contar el número de bits con valor de uno que posee la trama de datos. Si el número de unos es par, se pone un 1 al final de la trama. En caso contrario se pone un cero.
Para el caso de una paridad impar, si el número de bits con valor de uno es impar, se pone un 1 al final de la trama. En caso contrario se pone un cero.

1.7.1.2 CRC

La revisión cíclica de redundancia (CRC por sus siglas en inglés) tiene un porcentaje muy elevado de confiabilidad en el reconocimiento de errores (superior al 99%), aunque al igual que el procedimiento de paridad de datos, no puede corregir errores.

Básicamente se trabaja con una trama de datos de *k* bits. El transmisor de los datos agrega *n* bits adicionales (usualmente ceros al lado derecho de la trama), a los cuales se les denomina secuencia de comprobación de trama FCS (Frame Check Sequence). La trama resultante de *k*+*n* bits es dividida por un numero predeterminado (basado en un polinomio generador) cuando llega al receptor. Si en la recepción, luego de dividir la trama no se da un resto en la división entonces significa que no ha habido errores en la transmisión.

Esta forma de detección de errores se basa en el cálculo de polinomios estandarizados:
CRC-12: $X^{12}+X^{11}+X^3+X^2+X+1$,
CRC-16: $X^{16}+X^{15}+X^2+1$,
CRC-CCIT: $X^{16}+X^{12}+X^5+1$
CRC-32: $X^{32} + X^{26} + X^{23} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$

Usualmente el número que acompaña a las siglas CRC es el número de bits que se deben de adicionar a la trama inicial. Por ejemplo el CRC-12 se utiliza en transmisiones de cadenas de caracteres de 6 bits y genera 12 bits de FCS.

En todos los polinomios utilizados aparece el factor: X+1. Este asegura la detección de todos los errores con un número impar de bits.

Por ejemplo si se transmite la cadena: 1010001101 (trama de 10 bits), su polinomio generador vendría dado por:

$$X^9+X^7+ X^3+X^2+X^0$$

Dicho polinomio generaría la trama siguiente: 110101 (6 bits). Al usar un FCS de 5 bits, a la trama inicial se le agregan cinco ceros al final:

101000110100000 (trama de 15 bits).

Al dividir esta trama de 15 bits por el polinomio generador (110101), el resultado es:

01110

Entonces la trama que se debe de transmitir es la trama original de 10 bits mas estos últimos bits obtenidos con la división. Por lo que la trama que debería de llegar hacia el receptor, sino hubiera errores en la transmisión sería:

101000110101110.

En el receptor esta trama recibida se divide entre 110101 (el polinomio generador) y si el resto es cero, entonces significa que efectivamente no hubo errores en la transmisión.

1.7.2 Anticolisión para múltiples accesos

Los sistemas que trabajan bajo RFID, usualmente llegan a involucrar numerosas cantidades de *tags* en la zona de interrogación de un tan solo *reader*. Sin embargo se pueden distinguir dos formas de comunicación cuando hay varios dispositivos presentes que pretenden comunicarse entre ellos.

Una se da cuando el *reader* transmite datos hacia los *transponders*. En esta situación, las cadenas de datos que transmite el *reader* las reciben todos los *transponders*, tal como se muestra en la figura 1.7.a.

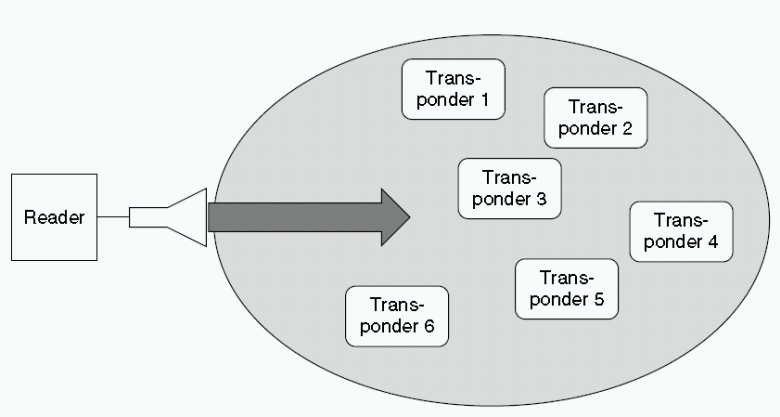


Figura 1.7.a

Se podría hablar entonces de una múltiple recepción, por parte de los *tags.* A éste tipo de comunicaciones se le denomina *broadcast*.
La segunda forma de comunicación se da cuando los diferentes *transponders* que están dentro de la zona de interrogación mandan sus cadenas de datos hacia el *reader*. A ésta forma de acceso se le conoce como acceso múltiple. Tal como se muestra en la figura 1.7.b

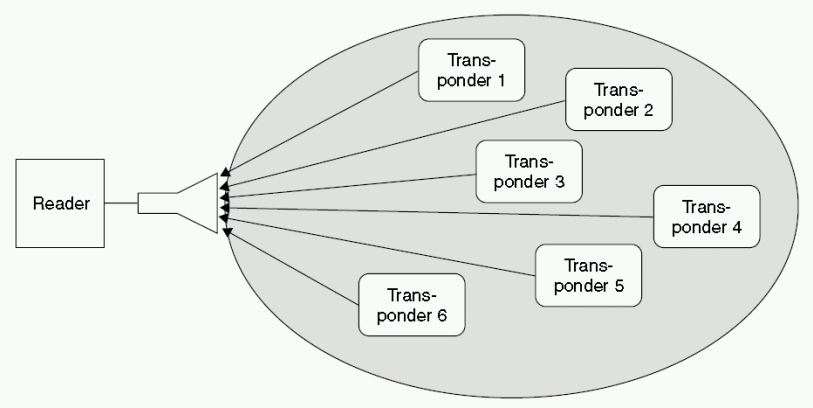


figura 1.7.b

Cada canal de comunicación tiene una capacidad definida, la cual esta determinada por la máxima taza de transferencia de datos del canal de comunicación y su tiempo de disponibilidad transcurrido.

La capacidad de disponibilidad del canal debe de ser dividida entre los tags que van a transferir información hacia el *reader* para que no se de una interferencia mutua en la transmisión, a lo que se le conoce como colisión.

El problema de colisiones de datos se ha dado siempre en los sistemas basados en radio. Por ejemplo las redes satelitales o las de telefonía móvil, en las cuales varios usuarios intentan acceder a un solo satélite o a una sola estación base. Para resolver ésta situación se han generado múltiples tecnologías cuyo propósito de separar de manera individual las señales de cada uno de los participantes de la red.

En este capitulo se estudiaran básicamente cuatro métodos diferentes para lograr separar dichas señales, las cuales basan su principio de funcionamiento en el hecho que sea una comunicación ininterrumpida de datos desde y hacia los participantes. Los cuatro metodos son los siguientes: acceso múltiple por división de espacio (SDMA, space division multiple access), acceso múltiple por división de frecuencia (FDMA, frequency domain multiple access), acceso múltiple en el dominio del tiempo (TDMA, time domain multiple access) y acceso múltiple por división de código (CDMA, code division multiple access)

1.7.2.1 Acceso Múltiple por división de Espacio (SDMA)

Esta técnica está relacionada con el rehúso de ciertos recursos tales como la capacidad del canal de comunicación en áreas espacialmente separadas.

Si se dispone de un tan solo *reader* con un rango de lectura particular. Al reducir significativamente su rango de lectura, pero compensando el área de cobertura mediante el aumento del numero de *readers* con sus respectivas antenas, como un arreglo. La capacidad del canal de los *readers* adyacentes aumenta. Por lo que se puede obtener el mismo rango de cobertura que el del *reader* original pero con una mayor capacidad de lectura para la misma zona de interrogación.

Otra opción que se tiene es la de usar una antena eléctricamente direccionable en el *reader*. Con esto lo que se logra es poder direccionar el campo de lectura directamente hacia el *tag* (SDMA adaptativo). Lo que se logra con este método de lectura es poder diferenciar cada uno de los *transponders* por su posición angular en la zona de interrogación del *reader*. Sin embargo éste tipo de técnica, solo puede utilizarse en sistemas RFID con frecuencias superiores a 850 MHz, debido a que se utilizan un grupo de dipolos, cada uno con fase independiente, para formar la antena. Si las frecuencias de trabajo fueran inferiores, se deberían de utilizar dipolos excesivamente grandes.

El SDMA presenta la desventaja de un elevado costo de implementación debido a la complejidad de la antena. Motivo por el cual no hay muchas aplicaciones que utilizan dicho sistema.

1.7.2.2 Acceso múltiple por división de frecuencias (FDMA)

Esta técnica se basa la disponibilidad de varios canales de transmisión, con sus respectivas frecuencias portadoras, para los participantes de la comunicación.

En los sistemas RFID se puede implementar por medio de *tags* con una frecuencia de transmisión no harmónica ajustable libremente. La fuente de alimentación de energía para el *tag* así como la transmisión de señales de control (*broadcast*) se realizan mediante una frecuencia óptima del *reader*. Y para los datos a transmitir, entre el *reader* y los *transponders*, se utilizan otro rango de frecuencias completamente diferente.

Precisamente este tipo de funcionamiento hace que los sistemas RFID que trabajen con FDMA se vuelvan relativamente caros, sobre todo el *reader*. Sobre todo porque el *reader* debe de contar con un receptor dedicado para cada canal de recepción, así como se ilustra en la figura 1.7.c.

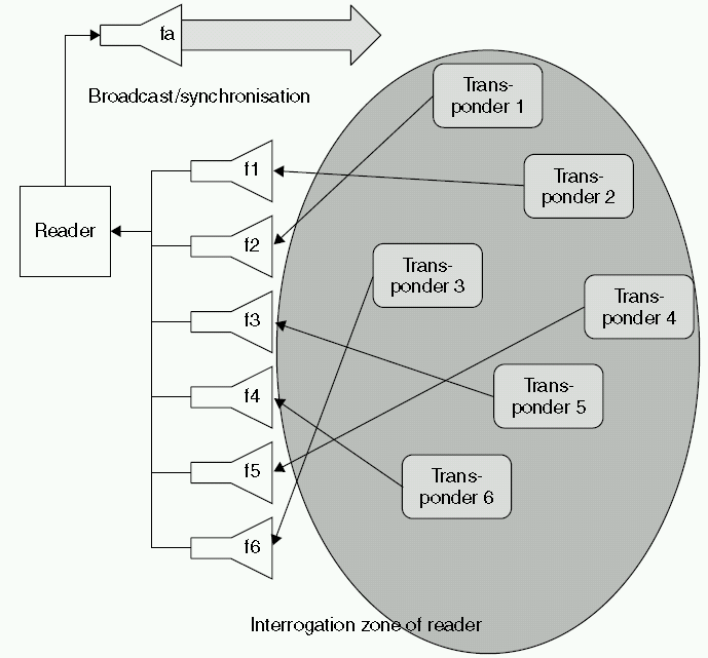


Figura 1.7.c

1.7.2.3 Acceso múltiple por división de tiempo (TDMA)

Esta técnica consiste en dividir la capacidad entera del canal, entre los participantes de la comunicación, entre intervalos de tiempo. Entre los sistemas de RFID, ésta es una de las mas utilizadas para evitar la colisión de datos.

Existen dos tipos de sistemas que trabajan bajo este esquema. Uno es asíncrono y el otro es sincrónico. En una comunicación asincrónica, no existe un control de los datos por parte del *reader*. En una transmisión sincrónica, todos los *tags* son controlados y revisados por *reader* de manera simultánea. El *reader* toma el papel de *master*, mientras que un *transponder* es seleccionado individualmente, de entre varios *tags*, dentro de la zona de interrogación utilizando un algoritmo determinado. Lo que permite que la comunicación se lleve a cabo entre el *tag* seleccionado y el *reader*. Únicamente cuando termina este intercambio de información en la comunicación el *reader* se pasa a comunicar con otro *transponder*, debido a que solo se puede iniciar un proceso de comunicación a la vez. Sin embargo esas comunicaciones entre esclavos y maestros se dan tan rápido que da la impresión que fuera de manera simultanea.

Uno de los ejemplos más comunes de aplicaciones anticolisión con TDMA sincrónico es el de ALOHA. Su nombre se deriva por una estación de radio en Hawai, Alohanet la cual utilizó dicho sistema luego de que éste fuera implementado en los 70's como una solución a la interconexión de computadoras mediante enlaces radioeléctricos. Es una de las

aplicaciones mas simples en cuanto a acceso múltiple se refiere. Su utilización es exclusiva para *transponders* de solo lectura, los cuales tienen que transferir únicamente una pequeña cantidad de datos, de manera cíclica hacia el *reader*.

Su modo de operación consiste en mandar información en cualquier momento en el que se necesiten mandar datos. Esto hace que la probabilidad de que colisionen los datos sea elevada. Sin embargo la forma de detectar colisión es fácil, por lo que se puede detectar cuando se produjo una collisión. Cuando esto pasa los datos que fallaron en llegar son reenviados nuevamente luego de esperar un cierto tiempo aleatorio para su reenvío. El algoritmo mas utilizado para la retransmisión de lso datos es: *random backoff*. Según este algoritmo, cuando un nodo transmite una trama y se detecta una colisión, elige, con probabilidad uniforme, un número entero en el intervalo [0;K - 1], espera una cantidad de ranuras igual al número escogido (tiempo de espera o *backoff*) y reintenta de nuevo. Si vuelve a producirse otra colisión repite el proceso una vez más, utilizando ahora un valor de K mayor, y así sucesivamente hasta que consigue transmitir la trama con éxito. En la práctica, es usual tomar K=2 para el primer reintento, y en cada nuevo reintento que colisione se duplica este valor hasta conseguir una transmisión exitosa.

El tiempo de transmisión de los datos es tan sólo una fracción del tiempo de repetición, ya que hay pausas relativamente largas entre las transmisiones. Sin embargo, los tiempos de repetición para cada etiqueta difieren levemente. Existe la probabilidad de que dos *transponders* puedan transmitir sus paquetes de datos en tiempos diferentes, logrando así que no colisionen el uno con el otro.

1.8 Seguridad e integridad de los datos

1.8.1 Encriptación de los datos

Los sistemas de RFID se están usando cada vez más en aplicaciones de alta seguridad como son los sistemas de acceso o para realizar pagos y *tickets* de caja. Por eso mismo el uso de los sistemas de identificación por radiofrecuencia necesita del uso de sistemas de seguridad para protegerse de ataques.

Los métodos de autenticación modernos funcionan como en la antigüedad: comprueban el conocimiento de un secreto para poder permitir una autenticación segura (por ejemplo conocer una clave criptográfica).

De todos modos se deben implementar algoritmos para prevenir que la clave secreta sea descubierta. Los sistemas de seguridad de los sistemas de RFID deben tener un modo de defensa contra los siguientes ataques individuales:

• La lectura no autorizada de la portadora de la información para poder conseguir una réplica y/o modificar los datos que lleva.

• Colocar una potadora de información extraña en la zona de influencia del interrogador con la intención de obtener un acceso no autorizado a un edificio o a una serie de servicios sin tener que pagarlos.

• Escuchar, sin ser advertido, en las comunicaciones radio y recolocar los datos imitando una portadora original (‘respuesta y fraude’).

Cuando se selecciona un sistema de RFID para su posterior implementación, debe tenerse en cuenta las medidas de seguridad que necesitan adoptarse dependiendo de su posterior funcionalidad. Así pues, un sistema que pretende una finalidad de automatización industrial o de reconocimiento de herramientas quizás no necesite añadir un coste adicional por medidas de seguridad que sí necesitarán sistemas de alta seguridad como pueden ser los sistemas de pago o de control de acceso a edificios. En el caso de los sistemas que necesitan seguridad, omitir un gasto en un proceso de criptología puede suponer un gasto posterior mucho más elevado si un intruso consigue acceso ilegal a servicios restringidos.

1.8.2 Criptografía de clave secreta o simétrica

Los criptosistemas de clave secreta se caracterizan porque la clave de cifrado y la de descifrado es la misma, por tanto la robustez del algoritmo recae en mantener el secreto de la misma.

Sus principales características son:

• Rápidos y fáciles de implementar
• Clave de cifrado y descifrado son la misma
• Cada par de usuarios tiene que tener una clave secreta compartida
• Una comunicación en la que intervengan múltiples usuarios requiere muchas claves secretas distintas

El cifrado de Verman verifica las condiciones de secreto perfecto definidas por Shanon, sin embargo presenta el inconveniente de que requiere un bit de clave por cada bit de texto. El hacer llegar tal cantidad de clave al emisor y receptor por un canal seguro desbordaría la propia capacidad del canal. Además requiere una clave aleatoria, y un ordenador genera claves pseudo aleatorias. La solución por tanto es la creación de claves de tamaño fijo y reducido.

Actualmente existen dos métodos de cifrado para criptografía de clave secreta, el *cifrado de flujo* y el *cifrado en bloques*.

Cifrado de flujo

El emisor A, con una clave secreta y un algoritmo determinístico (RKG), genera una secuencia binaria (*s*) cuyos elementos se suman módulo 2 con los correspondientes bits de texto claro *m*, dando lugar a los bits de texto cifrado *c*, Esta secuencia (*c*) es la que se envía a través del canal. En recepción, B, con la misma clave y el mismo algoritmo determinístico, genera la misma secuencia cifrante (*s*), que se suma modulo 2 con la secuencia cifrada (*c*), dando lugar a los bits de texto claro *m*.

Los tamaños de las claves oscilan entre 120 y 250 bits:

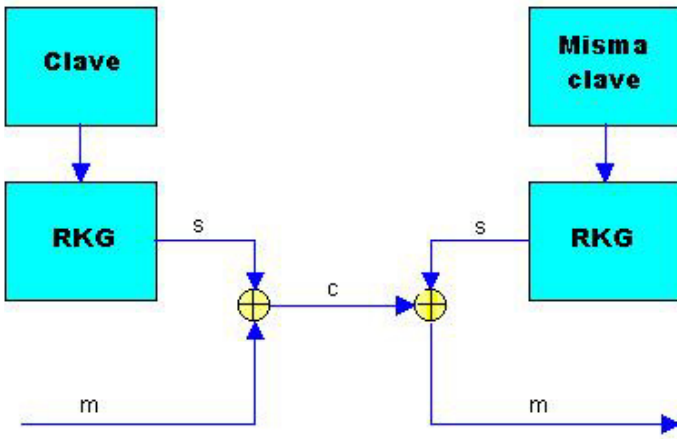


Figura 1.8.a. Ejemplo del diagrama de bloques del cifrado de flujo.

Cifrado en bloque

Los cifrados en bloque se componen de cuatro elementos:

- Transformación inicial por permutación.
- Una función criptográfica débil (no compleja) iterada r veces.
- Transformación final para que las operaciones de encriptación y desencriptación sean simétricas.
- Uso de un algoritmo de expansión de claves que tiene como objeto convertir la clave de usuario, normalmente de longitud limitada entre 32 y 256 bits, en un conjunto de subclaves que puedan estar constituidas por varios cientos de bits en total.

Cifrado de Feistel

Se denominan así los criptosistemas en los que el bloque de datos se divide en dos mitades y en cada vuelta de encriptación se trabaja, alternativamente, con una de las mitades. Pertenecen a este tipo los criptosistemas LUCIFER, DES, LOKI y FEAL.

1.8.3 Algoritmo DES

El algoritmo DES surge como consecuencia de un concurso organizado por NBS (National Bureau of Standards, USA) el cual solicitaba un "algoritmo de encriptación para la protección de datos de ordenador durante su transmisión y almacenaje". Este concurso lo ganó IBM con su algoritmo DES (modificado del LUCIFER).

DES es un algoritmo de cifrado en bloque; la longitud de bloque es de 64 bits (8 símbolos ASCII); la longitud de la clave es de 56 bits, lo que equivale a que existan:

$$2^{56} = 7.2x10^{16} \quad \textbf{Claves diferentes}$$

La norma del DES es FIPS (Federal Information Processing Standards). La norma exige que el DES se implemente mediante un circuito integrado electrónico. El chip de DES es un producto estratégico USA. No está permitida su exportación sin un permiso especial, y no se permite comercializar en USA chips fabricados en el exterior.

El ANSI (American National Standards Institute, USA) adopta el DES con el nombre de DEA (Data Encryption Algorithm) el cual no exige la implementación del algoritmo en un chip, pudiendo ser programado mediante software. Las librerías de implementación de DES y DEA son openSSL.

Estructura del DES

El DES trabaja alternativamente sobre las dos mitades del bloque a cifrar. En primer lugar se hace una permutación. Después se divide el bloque en dos mitades, a continuación se realiza una operación modular que se repite 16 veces; esta operación consiste en sumar módulo 2 la parte izquierda con la función $F(K_i)$ de la derecha, gobernada por una subclave K_i.

Después se intercambian las partes derecha e izquierda. En la vuelta 16 se remata el algoritmo con una permutación final que es la inversa de la inicial.
Para descifrar el DES basta con repetir la operación modular, es decir, su aplicación repetida dos veces conduce a los datos originales.

Función F(K_i)

Las operaciones realizadas por la función F son:

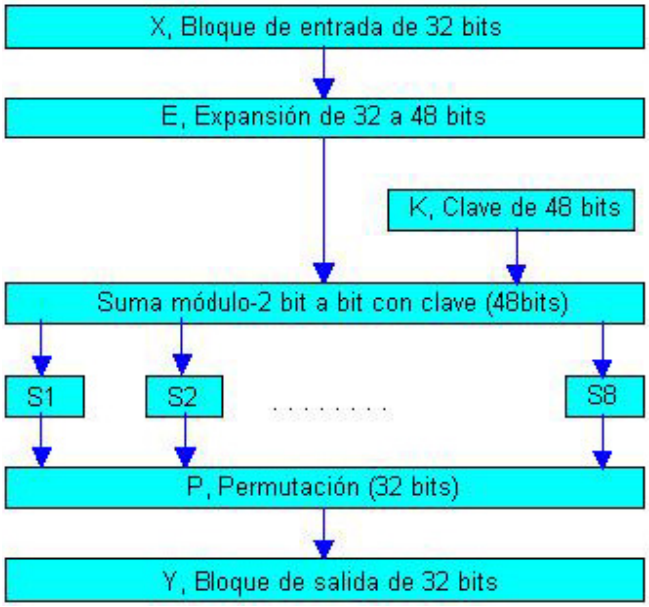


Figura 1.8.b. Operaciones realizadas por la función F.

Lo primero que se hace es fabricar un vector de 48 bits a partir de los 32 bits iniciales a través de una expansión lineal. Esta expansión es la que se describe a continuación :

Izquierda	32	1	2	3	4	5	4	5	6	7	8	9
Centro izda	8	9	10	11	12	13	12	13	14	15	16	17
Centro dcha	16	17	18	19	20	21	20	21	22	23	24	25
Derecha	24	25	26	27	28	29	28	29	30	31	32	1

Tabla 1.8.c. Ejemplo de la expansión lineal usada

Después se combina la clave local de 48 bits con la expansión por suma módulo 2 bit a bit, obteniéndose un vector de 48 bits que se divide en 8 grupos de 6 bits. Cada grupo entra en las llamadas "cajas S". Estas cajas son las responsables de la *no linealidad del DES*. En cada caja entran 6 bits, pero salen únicamente 4 bits. Además los bits centrales se sustituyen en función de los bits laterales. Los principios para la elección de las cajas S no han sido revelados y es información clasificada por el gobierno de los Estados Unidos.

La caja P realiza una permutación lineal fija, esta permutación es la siguiente:

El bloque	16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
Se cambia por	2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

Tabla 1.8.d Ejemplo de la permutación lineal fija usada

Expansión de claves K_i

En DES se manejan claves de 64 bits, pero se le realiza una operación de reducción a 56 bits, eliminando un bit de cada ocho. A continuación se reordenan los bits restantes mediante una permutación fijo que carece de significación criptográfica.
Después se generan las 16 subclaves necesarias en las 16 vueltas del algoritmo. Cada subclave estará compuesta por 48 bits.

La forma de generar las subclaves es la siguiente

- Se divide la clave de 56 bits en dos mitades de 28.
- Cada mitad se rota a la izquierda uno o dos bits dependiendo de la vuelta (de 1 a 16).
- Después de las rotaciones se vuelven a unir las mitades teniendo 16 grupos de 56 bits.
- A continuación se realiza una "permutación con compresión". Esta permutación elige 48 bits de cada grupo formando así las 16 subclaves.

Modos de uso

En la norma ISO 8372 se definen cuatro modos de uso de cualquier cifrado en bloque:

- ECB (Electronic Codebook): se caracteriza por el uso directo de un cifrador en bloque.
- CBC (Cipher Block Chaining): se carga inicialmente el registro (64 bits) con un vector inicial (VI) que no importe que sea secreto, pero si aleatorio. Sus principales características son que convierten el DES en un cifrador en flujo y puede hacer que cifre mensajes iguales de forma diferente con solo cambiar cada vez el VI.

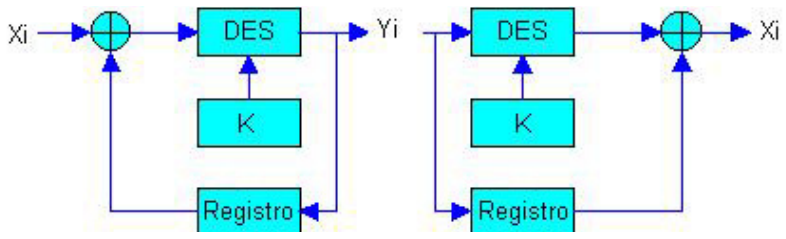


Figura 1.8.e. Diagrama de bloques del cifrado Cipher Block Chaining CBC

- CFB (Cipher Block Chaining): se carga inicialmente el registro de desplazamiento de 64 bits con un vector inicial (VI) que no importa que sea secreto, pero si

aleatorio. Se divide el mensaje en claro en bloques de n bits. La operación de suma módulo 2 se hace bit a bit sobre bloques de n bits que pueden variar de 1 y 64. El registro de desplazamiento de 64 bits se desplaza a la izquierda n bits después de cada operación de cifrado de cada bloque.

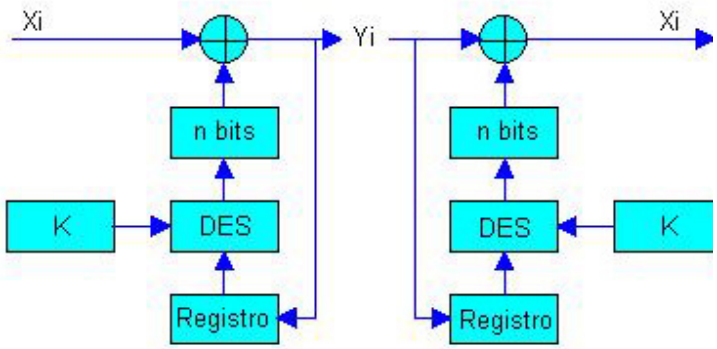


Figura 1.8.f. Diagrama de bloques del Cipher Block Chainig CFB

- OFB (Output Feedback): el funcionamiento es igual que en CFB, pero ahora el VI si tiene que ser secreto. Su principal característica es que convierte el DES como un generador de secuencia cifrante.

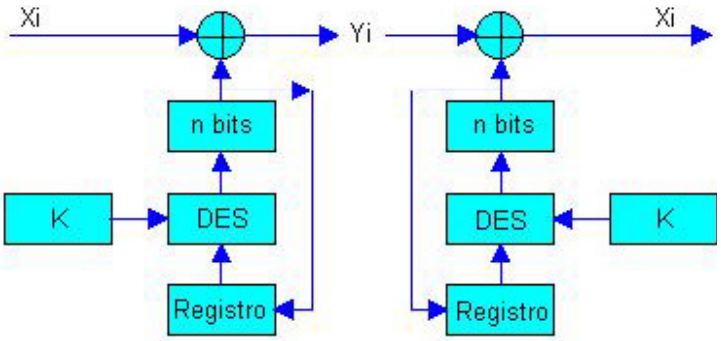


Figura 1.8.g. Diagrama de bloques del Output Feedback

Cifrado triple

Es un modo de cifrado para el DES o cualquier otro cifrador en bloque que no llega a ser un cifrado múltiple, porque no son independientes todas las subclaves. Es inmune a un ataque por encuentro a medio camino. Para el DES la longitud efectiva de clave es de 112 bits.

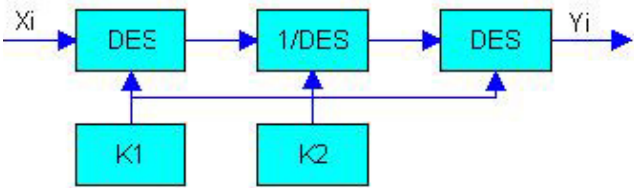


Figura 1.8.h. Diagrama de bloques del cifrado triple

1.8.4 IDEA (International Data Encription Algorithm)

En este algoritmo, tanto los datos en claro como los cifrados están compuestos por bloques de 64 bits, mientras que la clave consta de 128 bits. Se basa en el concepto de mezclar operaciones aritméticas de grupos algebraicos diferentes (introduce confusión y difusión en el mensaje). Se realizan ocho vueltas de encriptación idénticas seguidas de una transformación de salida. Es decir, como el DES, pero las vueltas son mas complejas. En cada vuelta de encriptación, el bloque de datos de entrada es dividido en cuatro sub-bloques de 16 bits. A su vez se utilizan para cada vuelta seis subclaves.

La seguridad de este algoritmo se basa en:

- Claves 2^{128} no se pueden computar actualmente.
- No se le puede aplicar criptoanálisis diferencial a partir de la cuarta vuelta, y este tiene ocho.
- Como inconveniente tiene que si se deducen varios sub-bloques de la clave, se puede deducir la clave.

1.8.5 Criptografía de clave pública o asimétrica

En la criptografía de clave secreta se presentan los siguientes problemas:

- **Distribución de claves**. Dos usuarios tienen que seleccionar una clave en secreto antes de empezar a comunicarse, lo que deberá hacer bien personalmente (cosa que no siempre es posible), bien por medio de un canal inseguro.

- **Manejo de claves**. En una red de n usuarios, cada pareja debe tener su clave secreta particular, lo que hace un total de n(n-1)/2 claves para esa red.

- **Sin firma digital**. En los criptosistemas de clave secreta no hay posibilidad, en general, de firmar digitalmente los mensajes, con lo que el receptor del mismo no puede estar seguro de que quien dice que le envía el mensaje sea realmente quien lo ha

hecho. De todos modos, este punto afecta poco a los sistemas RFID ya que no contienen firma digital.

Cambio de clave de Diffie-Hellman

Para evitar los problemas que se acaban de mencionar, Diffie y Hellman describieron un protocolo por medio del cual dos personas pueden intercambiarse pequeñas informaciones secretas por un canal inseguro.

Protocolo

1. Los dos usuarios *A* y *B*, seleccionan un grupo multiplicativo finito *G*, de orden *n* (Z_n^*) y un elemento $\alpha \in G$ (generador).
2. *A* genera un número aleatorio *a*, calcula $\alpha_a \pmod n$ en *G* y transmite este elemento a *B*.
3. *B* genera un número aleatorio *b*, calcula $\alpha_b \pmod n$ en *G* y transmite este elemento a *A*
4. *A* recibe α_b y calcula $(\alpha_b)_a$ en *G*
5. *B* recibe α_a y calcula $(\alpha_a)_b$ en *G*

Ejemplo: Sea *p* el número primo 53. Supongamos que $G=Z_{53}^* = \{1,2,...,52\}$ y sea $\alpha = 2$ un generador. El protocolo Diffie-Hellman es el siguiente:

1. *A* elige $a=29$, calcula $\alpha_a = 2^{29} \equiv 45 \pmod{53}$ y envía 45 a *B*.
2. *B* elige $b=19$, calcula $\alpha_b = 2^{19} \equiv 12 \pmod{53}$ y envía 12 a *A*.
3. *A* recibe 12 y calcula $12^{29} \equiv 21 \pmod{53}$.
4. *B* recibe 45 y calcula $45^{19} \equiv 21 \pmod{53}$

Ahora una escucha conocerá Z_{53}^*, 2, 45 y 12, pero no puede conocer la información secreta compartida por A y B que es 21.

Criptosistema RSA

El protocolo de desarrollo es el siguiente:

1. Cada usuario U elige dos números primos (actualmente se recomienda que tales números primos tengan más de 200 dígitos) *p* y *q* y calcula $n=p \cdot q$. El grupo a utilizar por el usuario U es, entonces, Z_n^*. El orden de este grupo es $\varphi(n)= \varphi(p \cdot q)=(p-1)(q-1)$.

2. Después, U selecciona un entero positivo e, $1 \leq e < \varphi(n)$, de modo que sea primo con el orden del grupo, es decir, de modo que mcd $(e, \varphi(n))=1$.

3. U calcula es inverso de e en $Z_{\varphi(n)}$, d; se tiene entonces $e \bullet d \equiv 1 (\text{mod } \varphi(n))$, con $1 \leq d < \varphi(n)$.

4. La clave pública del usuario U es la pareja (n,e), mientras que su clave privada es el número d. Por supuesto, también deben permanecer secretos los números p, q y $\varphi(n)$.

Si un usuario A desea enviar un mensaje m de Z_n a otro usuario B, utiliza la clave pública de B, (n_b,e_b), para calcular el valor de $m^{e_b} (\text{mod } n_b) = c$, que envía a B. Para recuperar el mensaje original, B calcula $c^{d_b} = (m^{e_b})^{d_b} = m^{e_b d_b} \equiv m (\text{mod } n_b)$

Ejemplo: Consideremos una codificación del alfabeto que transforme las letras de la A a la Z en los números del 0 al 25 (del alfabeto inglés), y enviamos un mensaje al usuario B.

- El usuario B elige dos primos $p_b=281$ y $q_b=167 \rightarrow n_b=281 \bullet 167=46927$ y considera el grupo Z^*_{46927}.

- Ahora $\varphi(46927)=280 \bullet 166=46480$ y B elige $e_b=39423$ y comprueba que mcd $(39423,46480)=1$.

- A continuación determina el inverso de 39423 módulo 46480 $d_b=26767$.

Clave privada= d_b =26767
Clave pública=(39424,46927)

Para enviar un mensaje de A a B, debemos determinar en la longitud del mismo. Como el mensaje ha de ser un elemento del grupo con el que estamos trabajando, su longitud no puede exceder del valor de n = 46927. Así pues como $26^3=17576 < n < 456976=26^4$, el mensaje ha de tener un máximo de tres letras. Si se quiere enviar un mensaje más largo, habrá que romperlo en grupos de tres letras. En la práctica, la longitud del mensaje es mucho mayor dado que n es un número con muchos dígitos.

$$\text{YES} = \text{Y} \bullet 26^2 + \text{E} \bullet 26 + \text{S} = 16346 = m$$

$$c = m^{e_b} (\text{mod } n_b) = 16346^{39423} (\text{mod } 46927) = 21166 \text{ [valor que A envía a B]}$$

- Ahora B recibe 21166 la decodificación sería así:

$$m = c^{d_b} (\text{mod } n_b) = 21166 \ (\text{mod } 46927_{39423}) = 16346$$

- Se decodifica m y se obtiene el texto original

$$m = 16346 = 24 \bullet 26^2 + 4 \bullet 26 + 18 = \text{YES}$$

Características de RSA

Existen algunos **mensajes no cifrables si $m^e = m \pmod n$**.

- El *e* suele ser el 3 o $2^{16}+1$ que son números primos.
- El algoritmo **DES implementado en software es 100 veces más rápido que RSA e implementado en chip es de 1000 a 10000 más rápido**. Por tanto para mensajes cortos se debe utilizar RSA y para los largos DES.
- Lo que se suele hacer es un *envoltorio digital*. El usuario A encripta el mensaje *m* con el criptosistema DES mediante una clave aleatoria, y a continuación la clave DES se encripta con RSA. Para recuperar el mensaje, el usuario B descripta la clave de DES mediante su clave privada del RSA y luego utiliza la clave obtenida para desencriptar el mensaje *m*.
- Para romper RSA se necesita conocer $\varphi(n)$ del cual puede deducir *d*. Conocido *n* no es fácil determinar $\varphi(n)$ ya que $n=p \bullet q$ y no se conoce ni *p* ni *q*.
- Para que un RSA sea fuerte *p* y *q* tienen que ser difíciles de adivinar, esto implica:
  - *p* y *q* sólo deben diferir en unos pocos dígitos, aunque no deben ser demasiado cercanos.
  - $(p-1)(q-1)$ deben contener factores primos grandes.
  - El mcd $(p-1, q-1)$ debe ser pequeño.
  - Una condición indispensable es que ***p* y *q* sean primos**.

1.8.6 Algoritmo asimétrico ELGAMAL

Suponiendo que los mensajes son elementos de G y que el usuario A desea enviar un mensaje m al usuario B. El protocolo utilizado es el siguiente:

1. Se selecciona un grupo finito G y un elemento α de G .
2. Cada usuario A elige un número aleatorio a, que será su clave privada, y calcular α^a en G, que será su clave pública.

Para que un usuario A envíe un mensaje, *m*, a otro usuario B, suponiendo que los mensajes son elementos de G, realiza las siguientes operaciones:

1. A genera un número aleatorio *v* y calcula α^v en G
2. A mira la clave pública de B, α^b, y calcula $(\alpha^b)^v$ y $m \bullet \alpha^{bv}$ en G
3. A envía la pareja $(\alpha^v, m \bullet \alpha^{bv})$ a B

Para recuperar el mensaje original:

1. B calcula $(\alpha^v)^b$ en G
2. B obtiene *m* sólo con calcular → $m \bullet \alpha^{bv} / \alpha^{vb}$

1.9 Estándares de RFID

Debido a la aceptación de la tecnología de RFID y a su constante crecimiento en las diferentes aplicaciones en la actualidad, se vio la necesidad de regular la tecnología RFID bajo ciertas normas internacionales, con el objetivo que dicha tecnología sea fácil de implementar en cualquier país sin necesidad de hacer cambios en los sistemas de funcionamiento.

En este apartado se darán a conocer los diferentes estándares utilizados en RFID, con el propósito de brindar un conocimiento de las diferentes normas que se utilizan en esta tecnología. Sin embargo si se quiere conocer más en detalles de cualquiera de los estándares que se describirán a continuación se puede consultar la base de datos de la ISO.

El ISO es una ONG constituida por una red de institutos nacionales de estándares en 146 países, cuya aportación es igualitaria (1 miembro por país). El organismo tiene una central de coordinación en Génova (Suiza).

Posee una lista de comités y concilios técnicos relacionados con el RFID:

- ISO JTC1 SC31
- ISO JTC1 SC17
- ISO TC 104 / SC 4
- ISO TC 23 / SC 19
- ISO TC 204
- ISO TC 122

De estos comités surgieron una cantidad importantísima de estándares relacionados con RFID, y utilizados en aplicaciones del mundo real. He aquí una lista completa de las normas relacionadas con el RFID:

- ISO 6346. Normas para containers, codificación, identificación y marcado.
- ISO 7810. Tarjetas de identificación. Características físicas, criterios de rendimiento, equipamiento para intercambios internacionales, y criterios sobre control hombre-máquina.
- ISO 7816. Tarjetas de identificación. Circuitos integrados, tarjetas con contactos. Está dividida en 12 partes.

- ISO 9798. Información tecnológica. Técnicas de seguridad y autentificación. Está dividida en 5 partes.
- ISO 9897. Normas para containers. Equipamiento, intercambio de información, códigos de comunicación.
- ISO 10373. Tarjetas de identificación. Métodos de test. Está dividido en 6 partes
- ISO 10374. Normas para containers. Identificación automática.
- ISO 10536. Tarjetas de identificación. Circuitos integrados para tarjetas sin contactos. Está dividido en 3 partes.
- ISO 11784. RFID para identificación de animales. Estructura del código.
- ISO 11785. RFID para identificación de animales. Conceptos técnicos. Especifica el proceso de transmisión entre tag y reader.
- ISO 14223. RFID para identificación de animales. Transponders avanzados. Contiene el protocolo de interfaz aire.
- ISO 14443. Tarjetas de identificación. Circuitos integrados para tarjetas sin contactos. Tarjetas de proximidad. Está dividida en 4 partes.
- ISO 14816. Normas para teletráfico. Equipamiento y automatización de vehículos. Numeración y estructuración de datos.
- ISO 15434. Información tecnológica. Sintaxis para transferencia de información ADC.
- ISO 15459. Información tecnológica. Identificación de unidades de transporte. Está dividida en 2 partes.
- ISO 15961. Información tecnológica. RFID para gestión de objetos. Protocolo de datos y interfaz de aplicación.
- ISO 15962. . Información tecnológica. RFID para gestión de objetos. Protocolo de codificación de datos y funcionalidades de la memoria.
- ISO 15963. Información tecnológica. RFID para gestión de objetos. Identificación única para tags RF
- ISO 17358. Aplicación para cadenas de suministro. Requerimientos de aplicación (En desarrollo)
- ISO 17363. Aplicación para cadenas de suministro. Contenedores (En desarrollo).
- ISO 17364. Aplicación para cadenas de suministro. Unidades de transporte (En desarrollo).
- ISO 17365. Aplicación para cadenas de suministro. Objetos reutilizables (En desarrollo)
- ISO 17366. Aplicación para cadenas de suministro. Empaquetamiento (En desarrollo).
- ISO 17367. Aplicación para cadenas de suministro. Etiquetado de productos (tagging) (En desarrollo).
- ISO 18000. Información tecnológica. RFID para gestión de objetos. (dividido en 6 partes):
    - 18000–1: Parámetros generales para las interfaces aire y correspondencia con las frecuencias mundialmente admitidas.
    - 18000–2: Interfaz aire para 135 KHz

  - 18000–3: Interfaz aire para 13.56 MHz
  - 18000–4: Interfaz aire para 2.45 GHz
  - 18000–5: Interfaz aire para 5.8 GHz
  - 18000–6: Interfaz aire desde 860 MHz hasta 930 MHz
  - 18000–7: Interfaz aire para 433.92 MHz
- ISO 18001. Información tecnológica. RFID para gestión de objetos. Perfiles de aplicaciones.
- ISO 18047. Información tecnológica. RFID para testeo. Similar al ISO 18000. Se divide en 3 partes.
- ISO 18185. Normas para contenedores. Protocolo de sellado eléctrico. (En desarrollo). Está dividido en 7 partes.
- ISO 19762. Información tecnológica. Técnicas AIDC. Dividida en 3 partes.
- ISO 23389. Normas para contenedores. Normas de lectura/escritura RFID.
- ISO 24710. Información tecnológica. Técnicas AIDC para gestión de objetos con interfaz ISO 18000. Funcionalidades elementales en interfaz aire.

En todas estas normas, las más utilizadas actualmente son la 18000-3 y 6.

Vale la pena mencionar también que pese a la existencia de dichos estándares, también hay empresas constructoras de estas tecnologías que utilizan como base dichos estándares para ellos hacer su propia versión del estándar como un código propietario. Tal es el caso de MIFARE, es un estándar adoptado por la Phillips que se basa en el ISO 14443-A.

1.9.1 tarjetas inteligentes contacless

Para estos dispositivos se han implementado tres diferentes tipos de estándares, los cuales se detallan en la siguiente tabla:

estándar	Tipo de tag	Rango de trabajo
ISO 10536	Acoplamiento cercano	0 – 1 cm
ISO 14443	Acoplamiento de proximidad	0 – 10 cm
ISO 15693	Acoplamiento de vecindad	0 – 1 m

Tabla 1.9.a Estándares para la tecnología RFID

1.9.1.1 tarjetas inteligentes de acoplamiento cercano (ISO 10536)

El estándar que describe la estructura y los parámetros de operación para este tipo de tags es el ISO 10536, el cual se titula: *Identification cards — contactless integrated circuit(s) cards*. Éste básicamente está compuesto en cuatro partes:

Parte 1: características físicas
Parte 2: dimensiones y localizaciones de las áreas de acople
Parte 3: partes electrónicas y procedimientos de reset
Parte 4: respuesta a los protocolos de transmisión y reset

a. Características físicas

Las especificaciones concernientes a los aspectos mecánicos son idénticas a las de las tarjetas inteligentes de contacto

b. Dimensiones y localizaciones de las áreas de acople

Los elementos inductivos (H1-4) y capacitivos (E1-4) son utilizados para este tipo de tarjetas. El arreglo para el acople de los elementos es diseñado de tal forma que una tarjeta de acoplamiento cercano pueda operar en un *reader* en cuatro distintas posiciones.

c. Partes electrónicas y procedimientos de reset

La fuente de alimentación para este tipo de tarjetas se deriva de los cuatro acoplamientos inventivos H1-H4. Además se establece que el campo inductivo alterno debe de tener una frecuencia de 4.9152 MHz. Los elementos de acople H1 y H2 son bovinas que tienen direcciones opuestas, por lo que si la energía es suministrada a los elementos de acople al mismo tiempo debe de haber una diferencia de fase de 180° entre los campos magnéticos asociados F1 y F2. Lo mismo se aplica para los elementos H3 y H4.

Los *readers* deben de ser diseñados de tal forma que provean una potencia de 150 mW hacia la tarjeta inteligente, es de cualquiera de los campos magnéticos F1-F4.

Para la transmisión entre el *reader* y el *tag* se pueden utilizar elementos de acople inductivo y capacitivo. Aunque durante la transmisión no sea posible pasar de un tipo de acople a otro.

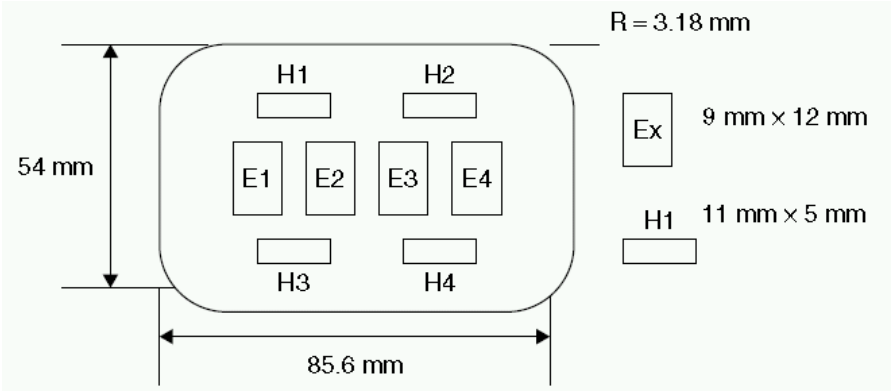


Figura 1.9.a: posición de los elementos capacitivos (E1-E4) e inductivos (H1-H4) en una tarjeta de acople cercano.

d. Respuesta a los protocolos de transmisión y reset

Esta parte del estándar está en desarrollo todavía por el comité encargado de la ISO, aunque en revisiones del estándar se pude encontrar información acerca del modo asíncrono de full duplex.

1.9.1.2 Tarjetas inteligentes de acoplamiento próximo (ISO 14443)

El estándar ISO 14443 describe los métodos y parámetros de operación para las tarjetas inteligentes de acoplamiento próximo. Se clasifican como *tags* del protocolo 14443 todas aquellas tarjetas inteligentes que no requieran contacto con el *reader* y que trabajen bajo un rango de 7 a 15 cm. Además utiliza dos tipos de protocolos de comunicación como principales, denominados A y B. Sin embargo han surgido mas tales como C (Sony/Japan), D (OTI/Israel), E (Cubic/USA), F (Legic/Switzerland) y G (China), aunque estos no son oficialmente reconocidos bajo el estándar. El estándar esta compuesto de las siguientes 4 partes:

Parte 1: características físicas
Parte 2: potencia de la radio frecuencia e interfaz de la señal
Parte 3: inicialización y anticolisión.
Parte 4: protocolos de transmisión.

a. características físicas

El ISO 14443-1 fue publicado el 15 de abril del 2000. En él se especifican las dimensiones de las tarjetas, las cuales coinciden con las del protocolo ISO 7810, el cual especifica valores de tolerancia de ± 85.72mm × 54.03mm × 0.76mm. Típicamente los *tags* que trabajan bajo este ISO, tienen una antena larga, la cual varía de 3 a 6 vueltas.

Además éste apartado trata sobre las irradiaciones de los rayos ultravioletas (UV), los rayos X y la sensibilidad a los campos electromagnéticos. Especifica también que la superficie de los *tags* debe de ser con calidad para impresión y resistencia mecánica.

b. Potencia de la radio frecuencia e interfaz de la señal

Denominado como ISO 14443-2, fue publicado el 1 de julio del 2001. Describe las características en cuanto a la transferencia de potencia y a la comunicación entre *reader*s y *tags*.

De acuerdo al estándar los *readers* se denominan PCD (*Proximity Coupling Device* por sus siglas en inglés). Mientras que los *tags* se denominan PICC (*Proximitty Integrated Circuits Cards*). Otras de las abreviaciones que se utilizan en éste estándar son: ASK (*Amplitude shift keying* por sus siglas en ingles), BPSK (*Binary phase shift keying*) y NRZ (*Non-return to zero*).

La fuente de energía de las tarjetas de acoplamiento inductivo, la provee el campo magnético alterno producido por el *reader*, con una frecuencia de transmisión de 13.56 MHz y con una tolerancia de +/- 7kHz. Esta frecuencia se ha escogido debido a varias razones técnicas (eficiencia en al acople inductivo, regulación EMC, etc.) y sobre todo por su poca absorción en los tejidos humanos entre otros.

En esta parte de estándar se especifican los 2 protocolos de comunicación, el tipo A y el B. asi como también los tiempos que dicho protocolo utiliza, por ejemplo se establece la velocidad de transmisión de datos en 106 Kbaudios. Ambos funcionan en modo *full duplex* con una transferencia de datos de 106 kbps en cada dirección. Además se establece que los datos transferidos de la tarjeta hacia el *reader* se logran mediante una subportadora de 847.5 KHz utilizando una modulación de carga.

Las diferencias entre los tipos A y B incluyen la modulación de los campos magnéticos utilizados para el acople con los campos magnéticos, la codificación de los bits y bytes y los métodos de anticolisión.

El tipo A utiliza un ASk de 100% del *reader* hacia la tarjeta, lo cual quiere decir que los datos son codificados con pequeñas pausas en la transmisión. Durante esas pausas no se transmite ningún tipo de potencia o energía hacia la tarjeta. Es por esto que el chip que se utiliza en el *tag* tiene que poseer ciertas especificaciones.

El campo magnético generado por el *reader* debe de estar dentro del rango de 1.5 A/m y 7.5 A/m.

c. inicialización y anticolisión

Publicado el 1 de febrero del 2001. Describe el poleo para los PICC cuando entra en el campo del PCD. El formato del byte de datos, comandos (petición o *request* y respuesta a la petición) y tiempos. Así como métodos de anticolisión para detectar y establecer una comunicación con una tarjeta en particular cuando hay varias más presentes en la zona de interrogación de un mismo *reader*.

Los métodos de anticolisión se fundamentan en una única identificación (denominada ID) por tag. Dependiendo del tipo de comunicación (sea del tipo A o B) el método de anticolisión es diferente. Para el tipo A utiliza un identificador único (UID por sus siglas en ingles) por un método de búsqueda binaria. Mientras que el tipo B utiliza el Aloha

rasurado (método mas sofisticado que el aloha puro) con ciertas ranuras marcadas especialmente.

d. protocolos de transmisión

Fue publicado el 1 de febrero del 2001. Especifica un protocolo de funcionamiento por bloques en *half duplex* (T=CL). Se incluyen varios escenarios de protocolos en el apéndice B de este estándar, con el propósito de demostrar el modo de funcionamiento de los protocolos de este estándar.

En esta parte se definen también los protocolos para la transmisión de datos de alto nivel, tanto para el tipo A como para el B. Además plantea la velocidad de la taza de transferencia de las comunicaciones con la tarjeta y la encapsulación de datos en bloques

1.9.2 2.8.2 VDI 4470: sistema antirrobo para mercancías

Este estándar provee lineamientos acerca de los sistemas de vigilancia de artículos electrónicos (EAS). Básicamente describe los procedimientos de prueba que hay que seguir para verificar y configurar los parámetros del sistema (porcentaje de falsas alarmas y de detección).

Los sistemas que basan su funcionamiento en éste estándar, tienen que tener un tiempo estimado de 3 semanas de prueba, según el estándar. En dichas pruebas se calibra el sistema en base a varias detecciones, en las cuales se establecen detecciones correctas y falsas alarmas. Las pruebas son variadas, desde artículos a simple vista hasta artículos escondidos en bolsas y en otros artículos.

También aparte de probar la correcta detección de artículos, el estándar regula el funcionamiento de los equipos que neutralizan o desactivan los tags. Todo con el propósito de evitar mas falsas alarmas.

1.9.3 ISO 14223/1

Es un estándar el cual especifica la estructura del código de radio frecuencia que se utiliza para el reconocimiento de *tags* avanzados para animales. Básicamente es una extensión de los estándares ISO 11784 y ISO 11785. en este estándar se describe la comunicación aérea entre los *transponders* avanzados y los *readers*.

Además de la transmisión acerca del código único de identificación de animales, se describen las aplicaciones de tecnología avanzada para facilitar el almacenamiento y

recuperación de la información adicional que se guarda en una base de datos integrada del *tag*.

Dicho estándar se divide en 3 partes, las cuales son: parte 1: *tags* avanzados e interfaz aérea, parte 2: *tags* avanzados: códigos y estructura de comandos, parte 3: aplicaciones de los *tags* avanzados.

1.9.4 EPCglobal

No se trata de un estándar, pero si de una organización sin fines de lucro fundada en octubre del 2003. Se encarga de la adopción y estandarización mundial de EPC (*Electronic Product Code*). El punto central de desarrollo de ésta organización es de crear un estándar mundial de RFID con el uso de Internet para transmitir datos mediante un red global denominada *EPCglobal Network*.

Esta organización ha tenido varios avances, el mas reciente, creado en 2006 es el estándar conocido por EPC Gen2 (de clase 1 y generación 2) al cual ahora se le denomina ISO 18000-6C. Este estándar se empezó en 2004 debido a los numerosos problemas que experimentaron los protocolos de generación 1 y 0 de ésta misma clase. Los sistemas que operan bajo éste estándar son bajo el rango de frecuencias 860 MHz - 960 MHz.

Esta organización ha desarrollado varios estándares, tales como:

- *Physical Markup Language* (PML): lenguaje basado en XML que define el formato de la información de intercambio entre componentes dentro de la red EPC.
- *Object Naming Service* (ONS): para la red global, que retiene la información sobre cualquier objeto etiquetado con un tag EPC en el mundo.
- *reader protocol* (RP)
- *Reader Management* (RM)
- *Low Level Reader Protocol* (LLRP)
- etc.

EPC o código de producto electrónico es un código numérico estandarizado de 96 bits que permite identificar a un objeto. Toda la información asociada a un código EPC se encuentra en la "*EPCGlobal Network*", accesible sólo a los usuarios autorizados. Estos datos son gestionados, filtrados y consolidados por el *Middleware* EPC, el cual los entrega a los sistemas corporativos y a los Sistemas de Información EPC. Para obtener información adicional sobre un EPC, el agente autorizado, a través de sus Sistemas de Información EPC ("EPCIS"), acudirá a los Servicios de Información centralizados ("*Discovery Services*"), entre los que destaca el Servicio de Nombres de Objeto ("*Object Naming Service*").

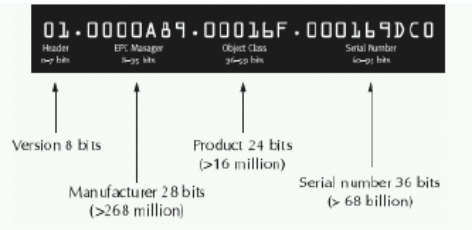


Figura 1.9.b Estructura del código EPC

El *Middleware* EPC es un componente crítico dentro de la red EPCGlobal ya que, por un lado, debe asegurar la integración de los equipos RFID de los distintos fabricantes, y por otro, facilita a los sistemas de la empresa los datos recogidos por los lectores. Dado que los lectores pueden estar recogiendo datos de cientos de *tags* por segundo, el *middleware* debe filtrar y consolidar adecuadamente los datos antes de enviarlos a los sistemas corporativos.

El *EPC Information Server* (EPCIS), ss la pasarela o intérprete para el intercambio de información entre aplicaciones remotas; especifica los servicios e interfaces que son necesarios para facilitar dicho intercambio a lo largo de la cadena de suministros completa. Una de sus principales características consiste en la existencia de un repositorio central de datos compartido, cuya información es actualizada por todos los partners que componen la red. El proceso de comunicación se realiza mediante servicios web (SOAP) utilizando el Lenguaje de Marcado Físico ("PML, Physical Markup Lenguaje"), de forma que cualquier aplicación local pueda comunicarse con sistemas remotos

1.10 Parámetros para diseño de una aplicación RFID

A continuación se detalla uno de los protocolos mas utilizados en el ambiente de RFID con el objetivo de brindar un conocimiento de todos los detalles técnicos que se pueden manejar para poder implementar un diseño apropiado implementando sistemas RFID en base a un estándar, como lo son la interacción entre el *tag* y el *reader*, tanto a un nivel físico como lógico y los tramas protocolarios. El estándar que se desarrollara en esta sección es el ISO 14443.

Este estándar describe los métodos y parámetros de operación de las tarjetas inteligentes (*smart cards*). Estas operan en un rango aproximado de 7 a 15 cm, el portador de datos de estos tarjetas es usualmente un microprocesador

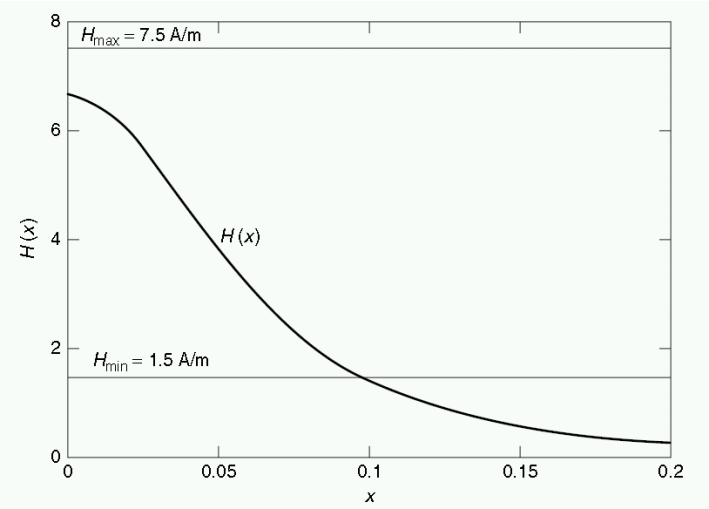
1.10.1 Parte 1: características físicas

En este apartado se definen los aspectos físicos externos de los *tags* que se fabrican bajo este estándar. Debido a que este tipo de información no es muy relevante en cuanto al diseño de implementación de sistemas basados en RFID, debido que el objetivo que se pretende no es fabricar los *tags*, ésta parte no se abordará en profundidad.

1.10.2 Parte 2: interferencia de la radio frecuencia

La fuente de energía del acoplamiento inductivo de las tarjetas de proximidad (PICC) es provisto por un campo magnético alterno desde el *reader* (PCD) a una frecuencia de 13.56 MHz. Para poder lograr esto la antena incorpora una larga antena de cobre de 3 a 6 vueltas alrededor de las tarjetas.

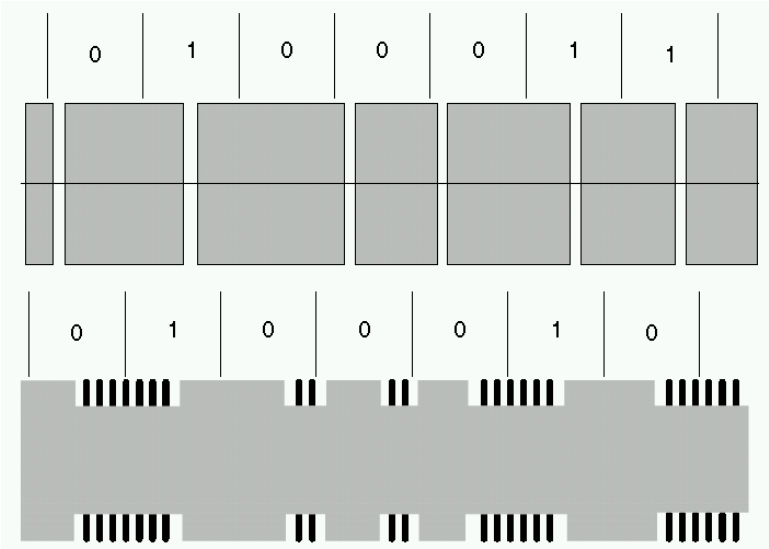
El campo magnético generado por el *reader* debe de estar entre un rango 1.5A/m ≤ H ≤ 7.5A/m. A continuación se muestra la curva típica del *reader* para dicho estándar.



En dicha grafica se puede apreciar que cuando el valor de la fuerza de interrogación del campo es de 1.5 A/m, el rango de lectura es de 10 cm. Sin embargo pese a tratarse de un tan solo estándar, se han creado dos diferentes métodos de transmisión de datos entre el *reader* y el *tag* (el tipo A y el tipo B), permitiendo así nada mas que una tarjeta se puede adaptar a un tan solo de estos métodos, pero no a los dos al mismo tiempo. Por el contrario, el *reader* si puede llegar a ser capaz de leer ambos métodos, con el propósito de poder leer todas los *tags* que operen bajo este estándar. Es por tal motivo que el *reader* debe de alternar entre dos modos de lectura periódicamente mientras se encuentra en el modo *idle* (modo de espera de una tarjeta inteligente).

1.10.2.1 Interfaz de comunicación (tipo A)

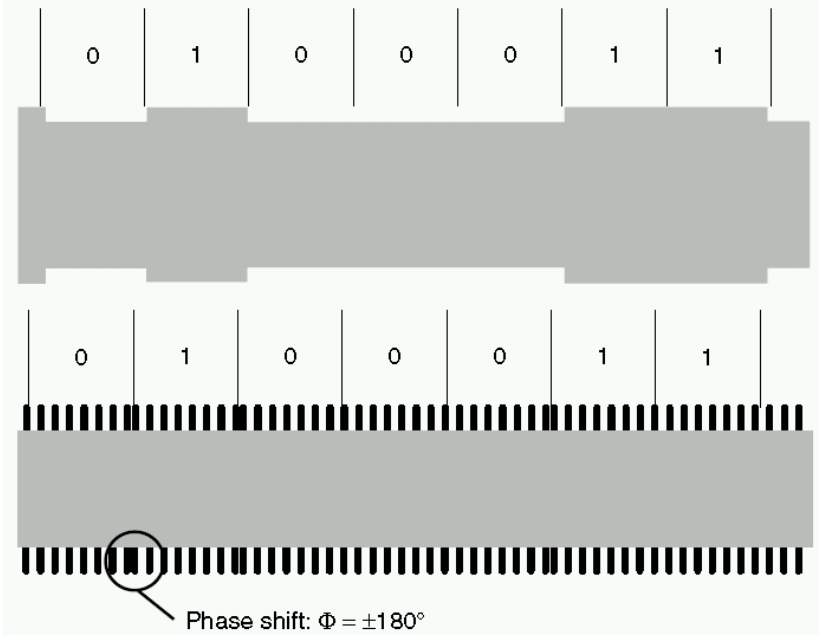
Para este tipo de tarjetas el 100% de las modulaciones ASK que utilizan las modificaciones de la codificación de Miller están definidas como el mecanismo de modulación utilizado para transferir datos desde el *reader* hacia el *tag*. En la siguiente figura se muestra en la parte superior, el *downlink* con el código de Miller modificado con un ASK del 100%. En la parte de abajo se muestra una modulación de carga con ASK, con una subportadora modulada a 847 KHz en codificación Manchester.



Para poder garantizar una fuente de alimentación hacia la tarjeta los intervalos en blanco deben de tener entre 2 y 3 µS. Posteriormente un procedimiento con modulación de carga y subportadora son utilizados para transferir datos desde la tarjeta hacia el *reader*. La frecuencia de la subportadora es de f_H = 847 kHz (13.56 MHz/16). En ambas direcciones de la transferencia el baud rate es de 106 kBit/s (13.56 MHz/128).

1.10.2.2 Interfaz de comunicación (tipo B)

Para este tipo de interfaz, se utilizan tarjetas con un 10% de modulación ASK para la transferencia de datos desde el *reader* hacia el *tag*. Una codificación simple de NRZ se utiliza para la codificación de bits. Este tipo de comunicación se detalla en la siguiente figura:



De igual manera para la transferencia de datos del tag hacia el reader se utiliza una modulación de carga con subportadora. La frecuencia de la subportadora es de f_H = 847 kHz (13.56 MHz/16). La subportadora se modula en fases de 180° (BPSK) de la subportadora utilizando la cadena de datos de NZR. En ambas direcciones de la transferencia el baud rate es de 106 kBit/s (13.56 MHz/128).

En la siguiente tabla se muestran las comparaciones en la transferencia de datos desde el *reader* hacia el *tag*.

PCD → PICC	**TIPO A**	**TIPO B**
Modulación	100% ASK	10% ASK
Codificación de bits	Código de Miller modificado	Código NZR
Sincronización	A nivel de bits (marcas a principio y al final de las tramas)	1 bit de inicio y 1 de stop por byte
Baud rate	106 KBd	106 KBd

En la siguiente tabla se muestran las comparaciones en la transferencia de datos desde el *tag* hacia el *reader*.

PCD → PICC	**TIPO A**	**TIPO B**
Modulación	Modulación de cargas con subportadora de 847 KHz,	Modulación de cargas con subportadora de 847 KHz,

	modulada con ASK	modulada con BPSK
Codificación de bits	Código Manchester	Código NZR
Sincronización	Sincronización de una trama de bits (marcas a principio y al final de las tramas)	1 bit de inicio y 1 de stop por byte
Baud rate	106 KBd	106 KBd

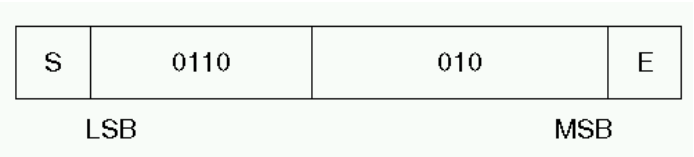
1.10.3 Parte 3: inicialización y anticolisión

Si una tarjeta inteligente de proximidad que entra en el campo de interrogación del *reader*, entonces se establece primero que nada una relación de comunicación entre el *reader* y el *tag*. Hay que tener en cuenta que puede haber más de un tag en la zona de lectura del *reader* por lo que no sería raro que el *reader* esté a media comunicación con un *tag*.

1.10.3.1 Tarjetas tipo A

Tan pronto como una tarjeta inteligente entra en el campo de interrogación del *reader* y una fuente proveedora de voltaje suficiente esté disponible, el microprocesador de la tarjeta comenzará a trabajar. Después de haber realizado ciertas rutinas de inicialización la tarjeta entra en un modo llamado *idle*. Éste modo permite que entre las cartas no se puedan intercambiar datos en la zona de interrogación, aunque el *reader* se encuentre en ese momento en comunicación con otra tarjeta (para no interrumpir la comunicación).

Cuando una tarjeta que se encuentra el modo *idle*, y recibe un comando de petición válido, denominado REQA (Request-A), entonces envía una respuesta a la petición, denominada ATQA (Answer to Request). Para asegurarse de que los datos destinados para otra tarjeta en el campo de interrogación del *reader* no sean mal interesados como un comando REQA, éste comando esta hecho de únicamente 7 bits de datos. Por el otro lado el bloque enviado de vuelta, ATQA consiste en 2 bytes y es devuelto en una trama estándar.



Representación de los 7 bits que componen el REQA, donde S=Stara de la trama y E=end

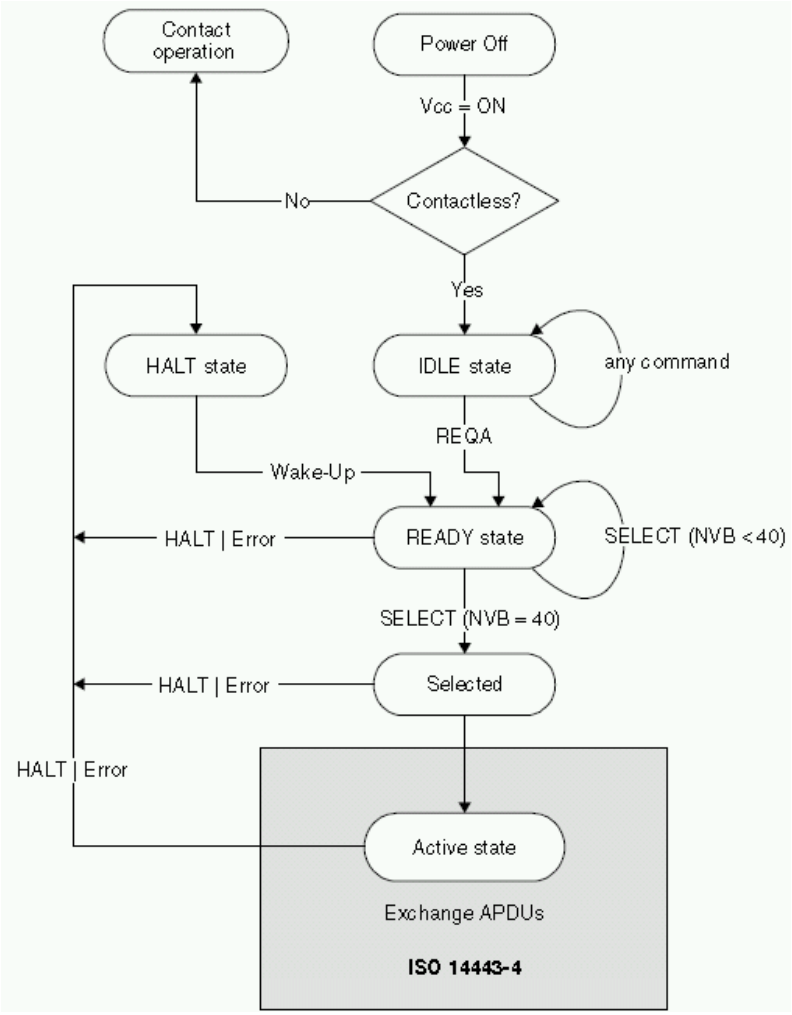
Después que el *tag* ha respondido al comando de REQA, éste pasa a un estado de *ready* (es decir listo para operar). Ahora el *reader* a reconocido que al menos una tarjeta se encuentra en el campo de interrogación y empieza a realizar algoritmos de anticolisión, lo cual se logra transmitiendo el comando *select*. El procedimiento de anticolisión utilizado

aquí es el de *binary search tree algorithm*. Una trama orientada a bits se utiliza para transferir los criterios de selección y respuesta de las tarjetas, de tal manera que la dirección de al transmisión pueda ser reservada después que un numero de bits han sido enviados. El numero de bits validos (NVB) que es un parámetro del comando *select*, especifica el largo del criterio de selección.

El largo de un número serie simple es de 4 bytes. Si algún numero serial es detectado por el algoritmo de anticolisión , el *reader* manda el numero serial completo (NVB=40_h) en el comando *select* para seleccionar la tarjeta en cuestión. La tarjeta que contiene el numero serial detectado confirma dicho comando mediante el envío de un reconocimiento (SAK :*select-acknowledge*) y esto hace que pase a un estado activo. Si embargo una peculiaridad se da debido a que no toda las tarjetas tiene un número serie de 4 bytes, porque el estándar también permite tarjetas con 7 bytes (tamaño doble) y de hasta 10 bytes (tamaño triple). Si el *tag* tiene un triple o un numero serial doble, éste debe de ser señalado en el *reader* por el SAK de la tarjeta por un bit de cascada (b3=1), permanecido la tarjeta e el estado de *ready*. Esto resulta en el reseteo del algoritmo de anticolisión en el *reader* para que se pueda detectar la segunda parte de numero de serie. Para u numero de serie triple, el algoritmo de anticolisión se debe de ejecutar una tercera vez. Para señalizar en la tarjeta que parte del numero de serie esta siendo detectado por el algoritmo que ha sido inicializado, el comando *select* diferencia entre los tres niveles de cascada (CL1, CL2, CL3), tal como se muestra en la siguiente figura:

El proceso de la detección del numero serial siempre empieza en el nivel de cascada 1. Para la respuesta de un comando REQA, WakeUp o select N=9. Para todas los otros comandos N tiene que ser mayor o igual que 9.

A continuación se muestra un diagrama de estado de las tarjetas inteligentes basadas en el estándar ISO 14443.



1.10.3.2 Tarjetas tipo B

Si una tarjeta inteligente tipo B se lleva cerca del campo de interrogación de un *reader*, después de haber realizado varias rutinas de inicialización, el *tag* se pone en estado de *idle* y espera recibir un comando de petición valida REQB.

La transmisión del comando REQB inicia inmediatamente el algoritmo de anticolisión en las tarjetas tipo B. El procedimiento que se utiliza para esto es el ALOHA, en el cual el numero de las divisiones puede cambiar dinámicamente por el reader. El numero de las divisiones disponibles es encodeado en el parámetro del comando REQB. Para facilitar alguna preselección de una tarjeta, el comando REQB tiene un parámetro, denominado

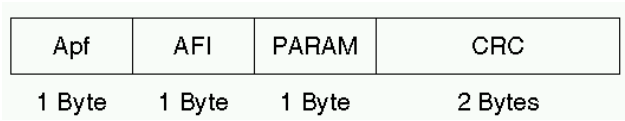
AFI (Application Family Identifier) el cual permite poder ingresar un grupo de aplicaciones como criterio de búsqueda. A continuación se muestra una tabla donde se especifican los códigos de preselección de un grupo de aplicaciones en el comando REQB>

AFI bit 7–bit 4 Application group	AFI bit 3–bit 0 Subgroup	Comment
0000	0000	All application groups and subgroups
—	0000	All subgroups of an application group
'X'	'Y'	Only subgroup Y of application group X
0001	—	Transport (local transport, airlines, ...)
0010	—	Payments (banks, tickets, ...)
0011	—	Identification (passport, driving licence)
0100	—	Telecommunication (telephone card, GSM, ...)
0101	—	Medicine (health insurance card, ...)
0110	—	Multimedia (internet service, Pay-TV)
0111	—	Games (casino card, lotto card)
1000	—	Data storage ('portable files', ...)
1001–1111	—	Reserved for future applications

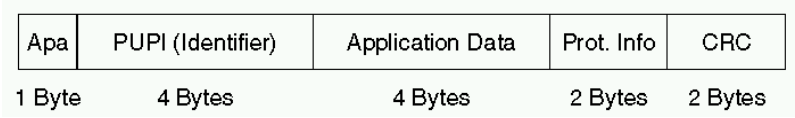
Después que una tarjeta ha recibido un comando valido de REQB revisa el grupo de aplicaciones preseleccionado en el parámetro AFI para ver si se encuentra presente en el *tag*. De encontrarse, revisa el parámetro M del REQB para detectar el numero de divisiones disponibles para la anticolisión. Si el número de las divisiones es mayor que uno, un generador de revisión aleatoria dentro de la tarjeta se utiliza para determinar el numero de divisiones en las cuales el *tag* desea transmitir su respuesta hacia el *reader*. A continuación se muestra una tabla con el numero de divisiones posibles que pueden ser configuradas por el parámetro M en el comando REQB.

Para *M* byte (bit 2–bit 0)	Number of slots *N*
000	1
001	2
010	4
011	8
100	16
101	Reserved for future applications
11x	Reserved for future applications

Para garantizar la sincronía de los *tags* con las divisiones de tiempo, el *reader* transmite su propio marcador de divisiones al inicio de cada división. El *tag* espera hasta que el marcador de división anteriormente determinado haya sido recibido y responde al comando REQB mediante el envío de un ATQB (*Answer to Request* B). Las estructuras de los comandos REQB y ATQB se muestran a continuación



Estructura del comando REQB

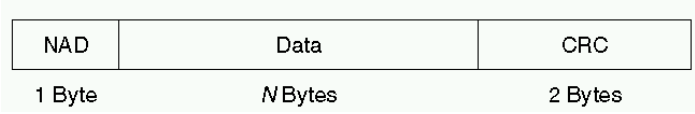


Estructura del comando ATQB

En un corto tiempo después de la transmisión de un marcador de división, el *reader* puede determinar si una tarjeta inteligente a comenzado a transmitir un ATQB dentro de la división actual. De no ser así, la división actual puede simplemente ser interrumpida por la transmisión del siguiente marcador de división para ahorrar tiempo.

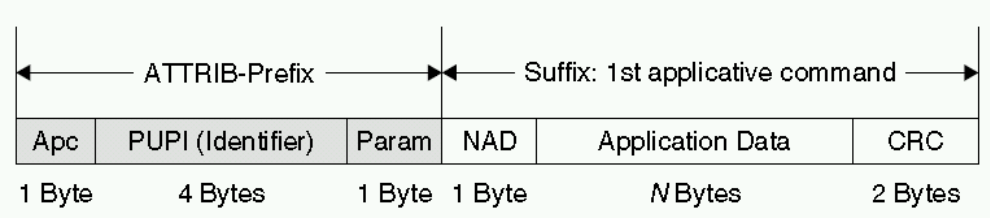
La respuesta solicitada ATQB enviada por el *tag* provee al *reader* con un rango de información acerca de ciertos parámetros del *tag*. Para hacer posible la selección del *tag*, el ATQB contiene al inicio un numero de serie de 4 bytes. A diferencia de las tarjetas del tipo A, las del tipo B no poseen un numero de serie que no es necesariamente ligado permanentemente al microchip, sino que mas bien puede consistir en un numero aleatorio, el cual es determinado cada vez que se da un *Power-On reset* (PUPI*, pseudo unique PICC identifier*).

Los parámetros de la interfaz de las tarjetas *contactless* son encodeados dentro del parametro *Protocol Info*, como por ejemplo el *baud rate* máximo posible de una *smart card*, el tamaño máximo de la trama o la información alterna en el protocolo. Los parámetros de los datos de aplicación pueden incluir mucha información de distintas aplicaciones disponibles en el *tag* (*tag* multi-aplicación).



Estructura de una trama estándar para la transmisión de datos de una aplicación bidireccional entre el *reader* y el *tag*.

Tan pronto como el *reader* recibe el ATQB de por lo menos un *tag* sin errores la tarjeta puede ser seleccionada. Esto pasa cuando el primer comando de la aplicación ha sido transmitido por el *reader*. La estructura de éste comando corresponde con la de una trama estándar, pero con una información adicional en un prefijo especial denominado prefijo-ATTRIB. Tal como se muestra en la siguiente figura.



Un tag es seleccionado enviando un comando de aplicación precedido por un prefijo ATTIB, si el identificador del tag corresponde con el identificador (PUPI) del prefijo

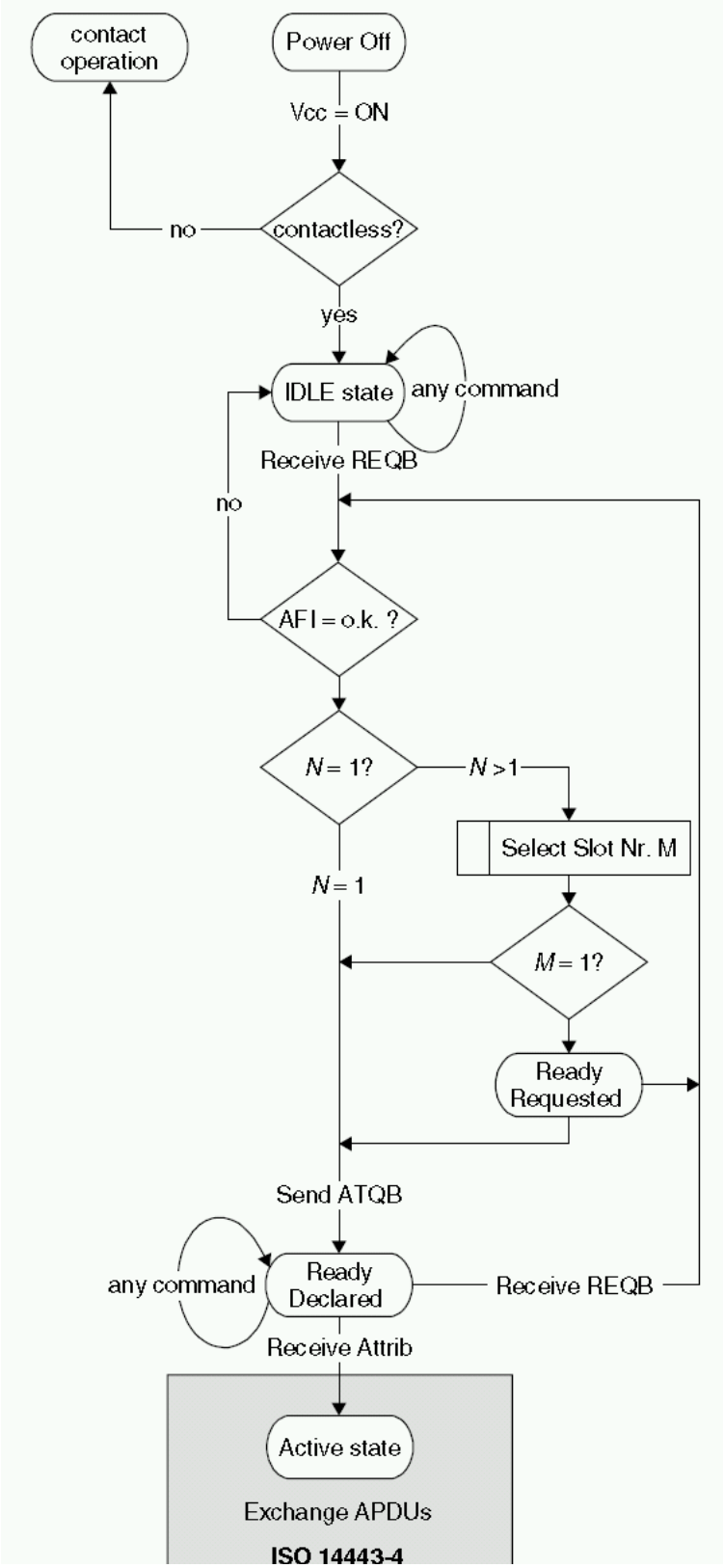

contact operation
Power Off
Vcc = ON
no
contactless?
yes
IDLE state
any command
Receive REQB
no
AFI = o.k. ?
N = 1?
N >1
Select Slot Nr. M
N = 1
M = 1?
Ready Requested
Send ATQB
any command
Ready Declared
Receive REQB
Receive Attrib
Active state
Exchange APDUs
ISO 14443-4

Diagrama de estado de una tarjeta inteligente tipo B de acuerdo al estándar ISO 14443

1.10.4 Parte 4: protocolos de transmisión

Después que se haya establecido una relación de comunicación entre el *reader* y el *tag*, los comandos de lectura, escritura y procesamientos de datos pueden ser enviados a la tarjeta. Esta parte del estándar describe la estructura del protocolo de datos y el procesamiento de los errores de transmisión, para que los datos puedan ser transferidos entre las comunicaciones entre los participantes sin errores.

En las tarjetas de tipo A, información adicional de la configuración del protocolo para diferentes propiedades de las tarjetas y *readers* pueden ser transferidas. En las tarjetas tipo B, esta información ya ha sido transferida durante el proceso de anticolisión (ATQB y ATTRIB), por lo que en esta caso el protocolo puede comenzar inmediatamente.

1.10.4.1 Protocolo de activación en las tarjetas tipo A

La selección de una tarjeta tipo A en el lazo de anticolisión es confirmado por la tarjeta mediante la transmisión de un SAK (*select acknowledge*). El SAK contiene la información del protocolo que contiene el *tag*, ya se que esté de acuerdo al ISO 14443-4 o que sea un protocolo propietario (ej.: MIFARE).

Si un protocolo de acuerdo con ISO 14443-4 está disponible en la tarjeta, el *reader* pregunta por el ATS (*answer to select*) de la tarjeta mediante la transmisión de un comando RATS (*Request for answer to select*). Dicho comando contiene dos parámetros que son importantes para la comunicación: FSDI y CID.

FSDI (*frame size device integer*) define el número máximo de bytes que pueden ser enviados de la tarjeta hacia el reader en un bloque. Algunos de los posibles valores para esto son 16, 24 32,…., 128 y 256 bytes. Además de esto en la tarjeta se encuentra almacenado un CID (*Card IDentifier*). Mediante su uso es posible para un *reader* mantener seleccionadas varias tarjetas tipo A al mismo tiempo y además poder direccionar individualmente cada una de ellas por su propio CID.

El ATS enviado por el tag en respuesta al comando RATS corresponde con la función del ATR (*answer to reset*) de una tarjeta y describe los parámetros importantes del protocolo para el sistema operativo de las tarjetas inteligentes. Permitiendo asi que la transmisión de datos entre el *reader* y el *tag* sea optimizada con respecto a las propiedades de la aplicación implementada.

Inmediatamente después de recibir un ATS, el *reader* puede todavía iniciar un cambio de la transmisión del baud rate enviando un comando especial PPS (*protocol parameter*

selection). Basado inicialmente en un baud rate de 106 Kbit/s, el cual se puede incrementar independientemente en ambas direcciones de la comunicación. Adicionalmente los valores altos de baud rate tienen parámetros opcionales: DS y DR dentro del ATS.

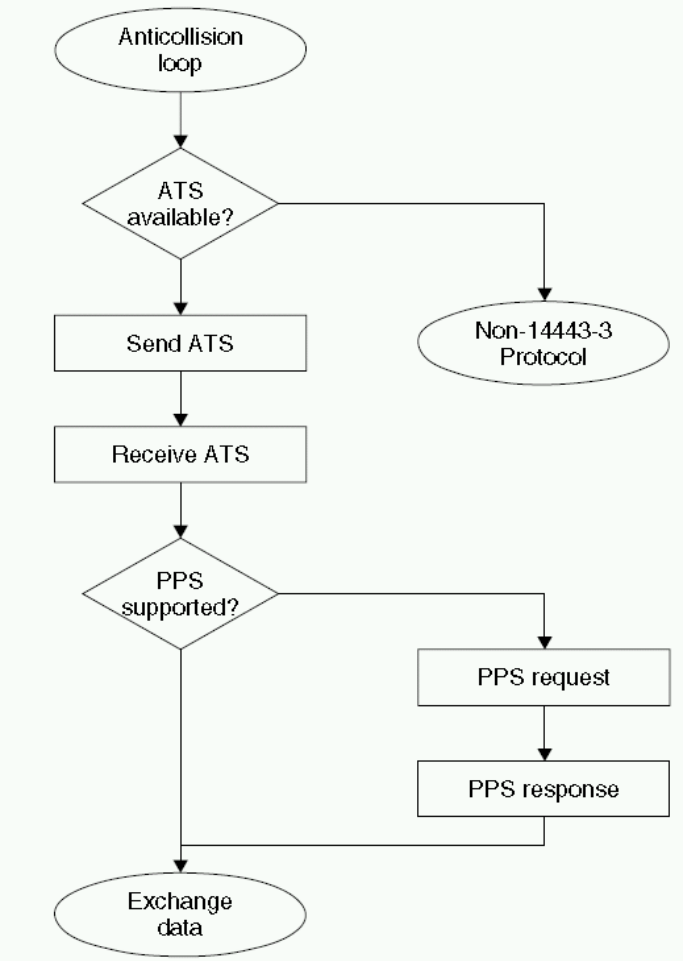


Diagrama que muestra la petición del ATS después del proceso de anticolisión

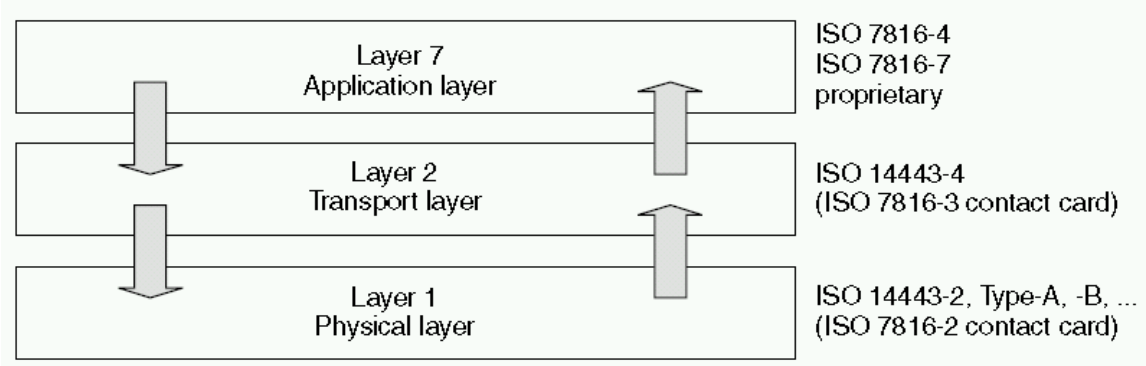
1.10.5 Protocolo

El protocolo descrito en el ISO 14443-4 soporta la transmisión de datos de aplicaciones (APDU= *aplication data unit*) entre el *reader* y el *tag*. El ADPU transmitido puede contener cualquier dato deseado, asi como tambien un comando o una respuesta. La estructura de este protocolo esta basada fuertemente en el protocolo ISO 7816-3, usualmente llamado T=1. El protocolo ISO 14443 es generalmente llamado T=CL

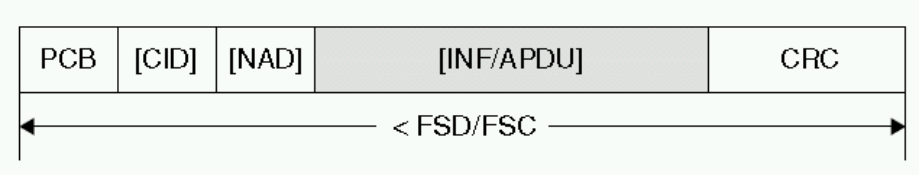
Toda la transmisión de datos para un *tag* ISO 14443 puede ser representada conforme con el modelo OSI. En este modelo cada nivel, de una manera independiente trabaja en su respectiva tarea de una manera transparenta para las demás capas superiores. La capa 1, capa fisica, describe el medio de transmisión y la codificación de los datos a nivel de byte. ISO 14443 provee dos procedimientos equivalentes, tipo Ay tipo B. capa dos, capa de transporte controlada transmisión de datos entre el *reader* y el *tag*. La capa dos automáticamente busca la dirección correcta del bloque de datos (CID), la transmisión secuencial de bloques de datos excesivos, el monitoreo del tiempo de proceso y el manejo de la transmisión de errores. La capa siete, la capa de aplicación, contiene los datos de la aplicación, el comando de la tarjeta o la respuesta a un comando. La capa 7, la capa de aplicación, contiene los datos de la aplicación, el comando del tag o la respuesta al comando. Las capas 3 y 6 se utilizan en redes complicadas en la parte de direccionamiento de los paquetes de datos, pero generalmente no se utilizan en las tarjetas contactless.

Después que un *tag* ha sido activado, éste espera el primer comando del *reader*. La secuencia que sigue después corresponde al principio de maestro-esclavo, con el *reader* como maestro y el *tag* como esclavo. El *reader* siempre manda un comando hacia el *tag* primero, el cual ejecuta el comando y manda una respuesta de vuelta hacia el *reader*. Por lo que un *tag* nunca puede iniciar una comunicación con el *reader*.

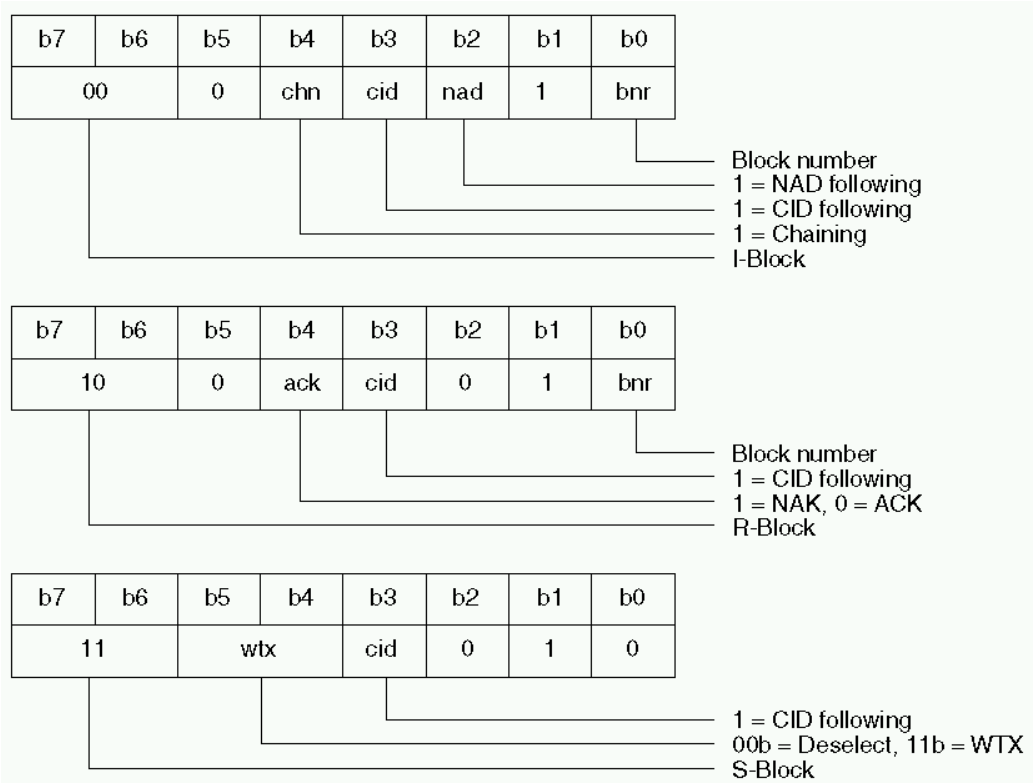
A continuación se muestra una figura que contiene el bloque de datos (frame). Donde hay tres tipos de bloques de acuerdo a la manea de funcionamiento. El bloque I: bloque de la información el cual se encarga de la transmisión de datos de la capa de aplicación (APDU). El bloque R, el bloque de recuperación el cual se encarga de la transmisión de errores y finalmente el bloque S o de supervisión, el cual es el mas alto del protocolo.



En la siguiente figura se detalla la estructura del bloque de datos en el ISO 14443. Los datos de la capa de aplicación, representada en gris, son puestos en paquetes en el paquete de datos del protocolo de la capa de transporte (representada en blanco).



En la siguiente figura se muestra la codificación del byte PCB (*protocol control byte* por sus siglas en ingles) en un *frame*. El comportamiento completo de transmisión es controlado por el PCB. Los bloques se diferencian por las distintas codificaciones del PCB.



1.11 Criterios de selección para sistemas RFID

En años recientes la tecnología de RFID ha tenido gran incremento. El mejor ejemplo de este fenómeno son las tarjetas inteligentes *contactless* usadas como boletos electrónicos para transporte público. Los campos de aplicación de los sistemas de identificación *contactless* han evolucionado y en esta medida los diseñadores de los sistemas de RFID han tomado muy en cuenta esta evolución, esto ha resultado en un incontable numero de sistemas existentes en el mercado.

Los parámetros técnicos de estos sistemas se han optimizado para varios campos de aplicación como en etiquetado, identificación animal, automatización industrial o control de acceso. Los requisitos técnicos de estos campos de aplicación se traslapan a menudo, lo que significa que una clasificación clara de los sistemas pertinentes de ninguna manera es algo simple, para no dificultar los procesos de selección, salvo en algunos casos especiales (identificación animal, *contactless* de acoplamiento cercano), no existe todavía un estándar obligatorio en lugar de los sistemas de RFID.

Es difícil incluso que un especialista conserve una descripción de la gama de los sistemas de RFID actualmente en oferta. Por lo tanto, no es siempre fácil que los usuarios seleccionen el sistema satisfactoriamente y más apegado a sus posibles necesidades. A continuación hay algunos puntos de consideración para la selección sistemas de RFID.

1.11.1 Frecuencia de operación

Los sistemas de RFID que utilizan frecuencias aproximadamente entre 100 kHz y 30MHz funcionan con acoplador inductivo. Por el contrario, los sistemas de la microonda en la gama de frecuencia 2.45-5.8 GHz son acoplados usando campos electromagnéticos. La tasa específica de la absorción (*damping*) para el agua o las sustancias non-conductivas es más baja por un factor de 100 000 en 100 kHz que está en 1 GHz. Por lo tanto, virtualmente ninguna absorción o el *damping* ocurren. Los sistemas de HF de una frecuencia más baja son mas usados debido a la penetración mejor de los objetos (Sch¨urmann, 1994). Un ejemplo de esto es el bolo, un transportador colocado en el tercer abdomen (panza) de los ganados, de los cuales puede ser leído en el exterior en una frecuencia de interrogación menor de 135kHz.

Los sistemas de microondas tienen una gama perceptiblemente más alta que los sistemas inductivos, típicamente 2-15m. Sin embargo, en contraste con los sistemas inductivos, los sistemas de microondas requieren una batería de reserva adicional. La energía de la transmisión del lector es generalmente escasa para proveer bastante energía para la operación del *transponder* . Otro factor importante es sensibilidad a los campos de interferencia electromágnetica, tales como los generados por soldadura con maquinas autógena por la robustez de los motores eléctricos, ante esto los *transponders* inductivos están en una desventaja significativa aquí. Los sistemas de la microonda por lo tanto se han establecido particularmente en las cadenas de producción y los sistemas de la pintura de la industria automovilística. Otros factores son la alta capacidad de memoria (hasta 32 kilobyte) y la resistencia de alta temperatura de los sistemas de microondas (Bachthaler, 1997).

1.11.2 Rango

El rango requerido de una aplicación es dependiente de varios factores (figura 2.18):

La exactitud de posición de *transponder* .
La distancia mínima entre varios *transponders* en la operación práctica.
La velocidad del *transponder* en la zona de interrogación.

Por ejemplo, en aplicaciones *contactless* para pago, por ejemplo boletos de transporte público, la velocidad de posicionamiento es muy baja, puesto que el *transponder* es dirigido al *reader* por la mano del portador. La distancia mínima entre varios *transponder s*, en este caso corresponde con la distancia entre dos pasajeros que entran en un vehículo. Para tales sistemas hay una gama óptima de 5-10 centímetros. Una mayor gama solamente daría lugar a problemas en este caso, puesto que los boletos de varios pasajeros se pudieron detectar por el lector simultáneamente. Esto haría imposible asignar confiablemente el boleto al pasajero correcto. Diversos modelos del vehículo de dimensiones que varían se construyen a menudo simultáneamente en las cadenas de producción de la industria automovilística. Estas variaciones de distancia entre el *transponder* en el vehículo y el lector se programan previamente (*Bachthaler*, 1997). La distancia de lectura y escritura del sistema de RFID usado se debe por lo tanto diseñar para la gama máxima requerida. La distancia entre los *transponders* debe ser tal que solamente un *transponder* esté siempre dentro de la zona de interrogación del lector a la vez. En esta situación, sistemas de microondas en los cuales el campo tiene la ventaja de radiar direccionalmente, ofreciendo claras ventajas totalmente sobre los sistemas de acople inductivo no direccionales.

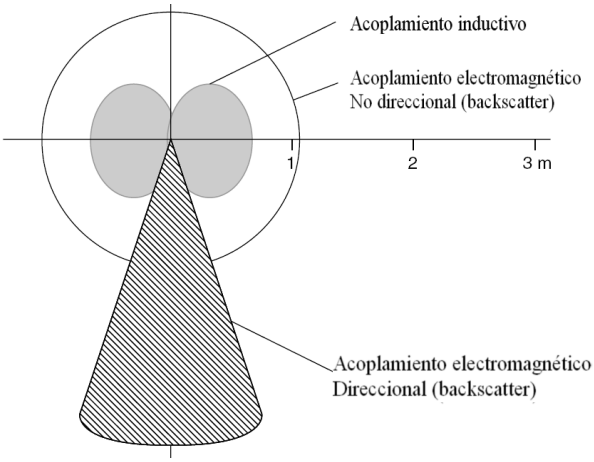


figura 1.11.a. Comparación de zonas de interrogación relativas a diferentes sistemas de RFID

La velocidad de los *transponders*, relativamente a readers, junto con la distancia máxima de lectura y escritura, determina la cantidad de tiempo que permanece en la zona de

interrogación del reader. Para la identificación de vehículos, la gama requerida de sistemas de RFID se diseña de tal manera que a la velocidad máxima del vehículo la longitud del tiempo pasada en la zona de interrogación es suficiente para la transmisión de los datos requeridos.

1.11.3 Requerimientos de seguridad

Los requerimientos de seguridad impuestos ante un uso previsto de RFID, por ejemplo: cifrado y autentificación, se deben determinar exactamente para no obtener ningún imprevisto o resultados indeseables durante la puesta en marcha. Para este propósito, el incentivo que el sistema representa a un atacante potencial es la manera de cómo manipular los bienes materiales o dinero esta iniciativa debe ser evaluada. Para poder determinar esta atracción, se dividen las aplicaciones en dos grupos:

Aplicaciones industriales o cerradas.
Aplicaciones públicas conectadas con dinero o bienes materiales.

Esto se puede ilustrar en base de dos ejemplos de aplicación en contraste.
Consideremos una planta de fabricación en la industria de automovilística como ejemplo típico de un uso industrial o cerrado. Solamente las personas autorizadas tienen el acceso a este sistema de RFID, así que el círculo de estos potenciales atacantes es razonablemente pequeño. Un ataque malicioso contra el sistema por la alteración o la falsificación de los datos sobre un *transponder* podría ocasionar un funcionamiento crítico no deseado en la secuencia de operación, pero el atacante no obtendría ningún beneficio. La probabilidad de un ataque así se puede fijar igual a cero, significando que incluso un sistema barato del bajo nivel sin lógica de seguridad puede ser utilizado.

El segundo ejemplo es un sistema de boletería para transporte público. Tal sistema, sobre todo portadores de datos de tarjetas inteligentes contactless, es accesible a cualquier persona. El círculo de atacantes potenciales es así enorme. Un ataque acertado contra tal sistema podía representar un daño financiero grande a dicha compañía del transporte público, por ejemplo en un acontecimiento de la venta organizada de pases de viaje falsificados, no dice nada del daño causado a la imagen de la compañía.

Para tales usos un *transponder* de alto desempeño y con procedimientos de la autentificación y del cifrado es imprescindible. Para tal aplicación el uso de *transponders* con requisitos máximos de seguridad es idóneo, por ejemplo aplicaciones de actividades bancarias con un monedero electrónico, solamente los *transponder* s con los microprocesadores deben ser utilizados.

1.11.4 Capacidad de memoria

El tamaño del chip portador de datos y la clase del precio, es determinado sobre todo por su capacidad de memoria. Por lo tanto, los portadores de datos permanentemente codificados de solo lectura se utilizan en aplicaciones masivas sensibles a las variaciones de precios y con un requisito de información local bajo. Sin embargo, solamente la identidad de un objeto se puede definir usando tal soporte.
Otros datos se almacenan en la base de datos central del controlador de la computadora. Si se requiere una reescritura de los datos continuamente, un *transponder* con tecnología de memoria RAM o EEPROM es requierida.

Las memorias EEPROM se encuentran sobre todo en sistemas acoplados inductivamente, las capacidades de memoria de 16 bytes a 8 kbytes están disponibles.
Los dispositivos de memoria SRAM con una batería de reserva, por otra parte, se utilizan predominantemente en sistemas de microondas. Las capacidades de memoria existentes se ofrecen en un rango de 256 bytes a 64 kbytes.

CAPITULO 2: Aplicaciones.

El gran número de aplicaciones que han sido implementadas, basadas en los sistemas de RFID, se debe a la versatilidad del manejo de la información que permite dicha tecnología. Se pueden apreciar aplicaciones de RFID básicamente en cualquier ámbito a nivel mundial, desde aplicaciones sencillas como identificación de productos hasta aplicaciones más complejas en ámbitos de logística y otros.

En este capitulo se abordaran cuatro aplicaciones en las cuales se puede evidenciar las diferentes aplicaciones que pueden implementarse, con sistemas basados en RFID y su impacto en cuanto a niveles de eficiencia y seguridad. Una de las aplicaciones es en el ambiente medico-farmacéutico, otra en la cadena de distribución y suministro, una mas de ventas al por menory finalmente una basada en el sistema de envío de cargas.

2.1 Venta al por menor

A continuación se detallará las medidas necesarias a tomar por parte de las compañías que se dedican a la venta al por menor y que estén interesadas en implementar tecnología RFID. Debido a la amplia gama de negocios de este tipo (supermercados, tiendas, librerías, ferreterías, etc.) es casi imposible diseñar una solución que se ajuste a cada negocio. Por lo que se han desarrollado las estrategias necesarias para implementar un sistema RFID y no parámetros de diseño de implementación.

Todos los almacenes, caracterizados por ventas al por menor, son especialmente cautelosos cuando se trata de adoptar una tecnología nueva o modernizar una ya existente. Debido a que esto puede cambiar por completo el modo de funcionamiento de los sistemas actuales y queda la incertidumbre, si para bien o para mal.

Los almacenes grandes tales como Wal-Mart no han tenido ningún problema en lograr que sus proveedores adopten el método identificación de RFID para reemplazar el sistema tradicional de códigos de barra. Éste no es el caso para los almacenes que manejan un menor volumen de productos, los cuales no tienen el mismo nivel de influencia con sus proveedores.

A continuación se detallará un método para implementar una aplicación basada en RFID, el cual pretende ser una guía para los distribuidores al por menor, de cómo implementar la tecnología de RFID para poder ser un punto de venta altamente competitivo.

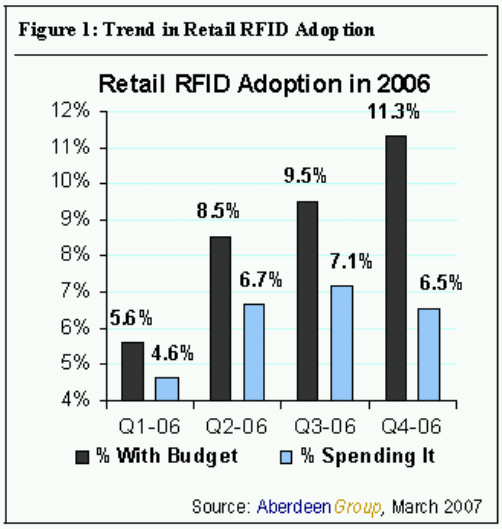
Generalmente se utilizan cuatro criterios de optimización para distinguir a las mejores compañías o a las mas competitivas. A estos indicadores se les conoce como KPIs (key

performance indicators) permiten reducir el tiempo de reabastecimiento de inventario, incidentes de robo, líneas mas cortas en las cajas de cobro, inventario menor de productos vencidos y problemas de precios establecidos.

Las compañías que utilizan estos indicadores pueden ver mejoras de hasta el 42% en incidentes de robo y 25% del tiempo de espera de los clientes en las cajas registradoras. Por lo que los beneficios del uso de identificación con RFID son altamente atractivos.

Sin embargo, en cuanto al mercado de venta al por menor, solo el 11% de las compañías, a nivel mundial, tienen destinado presupuesto para iniciativas de RFID. Sin embargo son muchas menos compañías las que esta usando ese presupuesto para implementar dichas soluciones. A continuación se muestran algunas estadísticas al respecto.

Figure 1: Trend in Retail RFID Adoption



El motivo de la poca inversión en este rubro del RFID se debe a tres factores:

1- no hay un camino ya establecido de cómo implementar un modelo RFID en el sector de venta al por menor, es decir que no se cuenta con nada estandarizado al respecto
2- sigue habiendo una confusión en cuanto a las tecnologías RFID y la mejor solución en cuanto a resolver el problema de de este tipo de negocios.
3- Sigue habiendo una cultura de esperar a que este tipo de tecnologías progresen en otros ambientes para ver su funcionamiento antes de tomar una decisión.

Los componentes para implementar una estrategia con sistemas de RFID son tecnologías que forman una solución y las cualidades de una organización que pueden brindar la habilidad de volver dichas tecnologías en una mejora competitiva.

Cuartos habitados con tecnología RFID en los probadores, estanterías inteligentes que permiten saber cuando el último artículo ha sido removido, permiten saber cuándo es que

ha sido removido el último producto. Así como un sistema de inventarios en tiempo real son algunas de las aplicaciones que ayudan que las ventas asistidas por RFID se incrementen.

Reabastecimientos inteligentes basados en "alerta y reacción" de RFID reducen las pérdidas debido a la descomposición o a rebajas. Con un control de inventario de "el primero en llegar, el primero en salir" los proveedores de productos, sobre todo alimenticios pueden estar más seguros de que los productos más viejos y por ende más propensos a que su vida útil caduquen más luego sean los primeros en venderse. Esto puede llegar a reducir las pérdidas por putrefacción o vencimiento en un 25%.

2.1.1 Estrategias para implementar un sistema de RFID con éxito

Lo primero es buscar el enfoque adecuado para incluirlo en el presupuesto. No siempre es competencia del departamento informático. También se puede incluir el sistema de RFID con la gerencia de operaciones o de logística. Por lo que se puede incluir incluso como una colaboración en conjunto de los departamentos de informática, logística y operaciones.

También se puede tomar la iniciativa en cuanto a la reducción perdidas debido al hurto o desaparición de productos y mercancías. Sin embargo esta puede ser una iniciativa difícil debido a que no es fácil cuantificar el valor en el que se puede llegar a reducir las pérdidas por robo. Sin embargo es otra posibilidad por la cual se puede afrontar la evaluación de utilizar un sistema basado en RFID.

Y finalmente para aquellos que tengan problemas en cuanto al presupuesto, se puede tratar de buscar un inventario manejado por un distribuidor y una infraestructura de RFID basada en el "pago por uso". Hay una nueva tendencia de servicio proveída por vendedores de tecnología, la cual consiste en hacer alianza con los proveedores para no solo proveer productos sino servicios de inventarios y sistemas de administración de inventarios de productos al mismo tiempo. Esta se puede ver como una opción para evaluar la tecnología RFID, sin el riesgo de la inversión inicial y de tener resultados favorables éste puede ser el camino correcto para llegar a implementar un sistema propio basado en RFID a mediano o largo plazo.

2.1.2 Acciones necesarias

La innovación es un factor fundamental para lograr sobresalir entre los demás. Por tal motivo, a una compañía se le hace indispensable buscar siempre las mejoras necesarias que le permitan mejorar sus procesos, aquí es donde aparecen los sistemas de RFID. Por lo que se hace casi indispensable designar personal en el área de la innovación.

Otra acción necesaria a tomar es la utilización de *tags* pasivos, por su bajo precio a comparación con los activos, además que utilizan menos espacio, motivo por el cual es más fácil tener cada uno de los productos etiquetados con *tags* de RFID.

Se vuelve necesario proveer de información del inventario al departamento de marketing, con el propósito que ellos puedan visualizar la demanda que tienen cada uno de los productos y así tomar medidas que permitan a la compañía incrementar sus ingresos o reducir perdidas mediante ofertas o promociones para los productos que estimen que convenientes. Lo interesante es que todo esto se puede hacer en tiempo real o "casi real", por lo que las medidas que tome dicho departamento pueden ser más efectivas y resolver el problema de manera casi inmediata. Por lo que aparte de disminuir perdidas se puede incrementar el nivel de productividad del área de marketing.

Además también vale la pena recalcar que en el caso de ver el movimiento de los productos por todo el almacén, mientras los clientes lo recorren, es un indicio fuerte de que áreas llaman más la atención de determinado cliente en base a los productos que éste consume). De tal forma que es una herramienta que hace posible también implementar, bajo el estudio y análisis de estadísticas de los consumidores, medidas de persuasión para el cliente o de reestructuración de productos entre otras acciones, para incrementar el nivel de ventas.

2.2 Contenedores de carga aérea

A continuación se presenta un aplicación que fue desarrollada pensando en el transporte aéreo de contenedores de cargas. Dicha aplicación ha sido denominada Cargo box y consiste en el diseño innovador de un contenedor de carga y un sistema de control de envío. Dicho contenedor además se integra con un sistema de seguridad llamado Cardisys. Lo que permite que los envíos de cargamentos sean completamente controlados, seguros, rápidos, eficientes y confiables.

2.2.1 Objetivo

El objetivo de esta aplicación es el de darle una solución sostenible y confiable con un nivel de seguridad adecuado que permita darle una solución completa en la cadena de suministros, incluyendo la industria de aerolíneas. Además dicha aplicación permite

demostrar una solución que opera a nivel mundial combinando envío de paquetes y logística en el control de transporte y seguridad para evitar perdidas en los envíos, optimizar tiempos de reacción y disminuir errores en los envíos.

2.2.2 Características

Todo el proceso de envío de cargamentos empieza desde que el pedido realizado por el cliente se empaca hasta que llega al destino del cliente. Sin embargo en medio de este proceso hay varias etapas en las cuales se necesita implementar medidas que disminuyan los costos de los procesos ineficientes intermedios. Aquí es donde Cargobox permite reducir sustancialmente el tiempo de entrega, volver mas eficiente el papeleo de los paquetes, sus contenidos, lugar de origen y destino, etc.

Lo mejor de dicha aplicación es que el contenedor de los cargamentos es reutilizable, altamente liviano y de fácil manejo, tanto para el transporte aéreo como terrestre. Con un peso de 35 kg (77 lbs) es capaz de soportar una carga de 750 kg (1650 lbs) con un volumen de alrededor de 64 cu.m. Dicho contenedor se puede apreciar en la figura 2.2.a

Figura 2.2.a: Contenedor Cargobox

2.2.3 Funcionamiento

La novedad de este concepto del Cargobox es el enfoque de un envío directo hasta la puerta y no como se hace tradicionalmente, que es de lugar de despacho o bodega al aeropuerto, del aeropuerto de origen al aeropuerto de destino, y del aeropuerto al destino final. Es obvio que entre mas etapas contenga la logística del envío son mas susceptibilidades a errores y mas tiempo de retraso posible en el envío.

Una vez el pedido se introduce en el Cargobox, el encargado de despachar el contenido, sella el contador mediante el Lockbar, lo cual se realiza mediante una computadora

portátil (PDA), asignando un código específico de seguridad y además secreto. Dicho código secreto es mandado vía e-mail, de manera encriptada, hacia el destinatario. Al mismo tiempo el sistema permite rastrear cada contenedor de carga y toda la información que éste posee se traslada hacia un base de datos centralizada al cual se puede tener acceso via web, en cualquier momento para poder verificar, tanto la ubicación del contenedor como su estado actual.

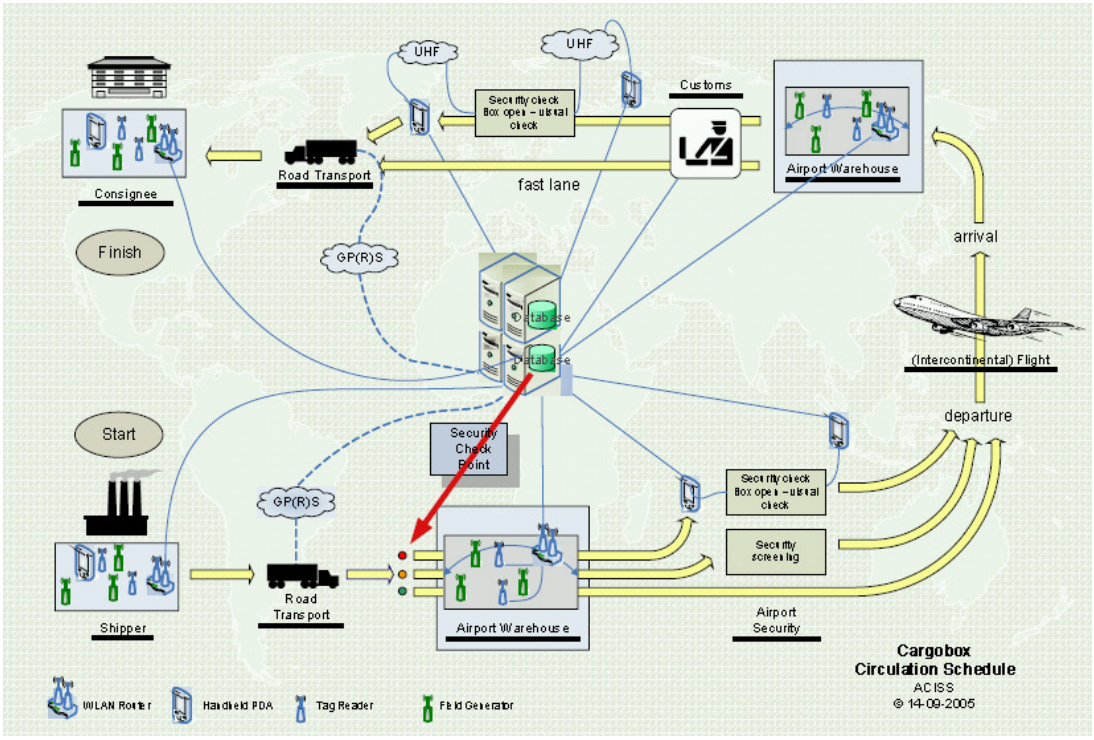


Figura 2.2.b: Diagrama de la logística en el envío de cargas aéreas mediante el sistema de Cargobox

2.2.3.1 El Lockbar

El Lockbar del Cargobox contiene una llave electromecánica que en combinación con un chip de memoria y un *tag* basado en RFID, puede ser activado utilizando el PDA. Esto quiere decir que tanto para abrir como para cerrar el Cargobox es necesario un código secreto generado de manera aleatoria.

Además también se puede almacenar en el *tag* toda la información concerniente al contenido de la carga, el origen y el destino. De manera que para poder tener acceso a toda esta información basta únicamente que el PDA se conecte de manera inalámbrica, mediante una red WLAN a un servidor donde esta alojado el programa que almacena toda la información de los Cargobox y en conjunto con el Cardisys. Asegurándole así al cliente

que toda su información permanece segura. Dicho sistema puede apreciarse en la figura 2.2.c.

El acceso a más o menos información detallada sobre el envío es administrado mediante la implementación de diferentes niveles de seguridad. Varios sensores se han instalado en el Cargobox por razones de seguridad, tales como sensores de temperatura, de detección de golpes fuertes y de cambio de peso.

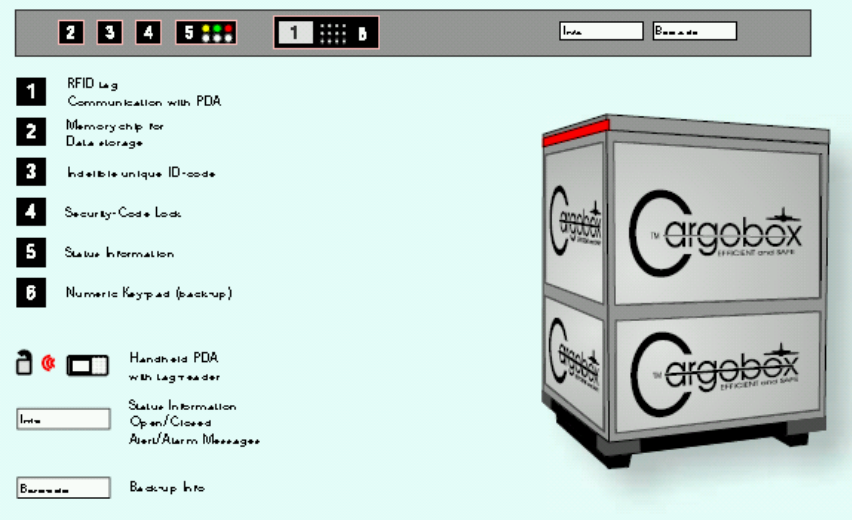


Figura 2.2.c Interfaz gráfica del programa computarizado para el control y manejo de los pedidos realizados en Cargobox

2.2.3.1 El Cardisys

El programa de base de datos, denominado Cardisys provee a los usuarios del Cargobox una total visibilidad de sus pedidos, a lo largo del día. Además dicho programa genera mensajes y los envía a las partes involucradas. De tal forma que cualquier contratiempo o atraso en la calendarización del envío se les notifica inmediatamente en forma de mensaje de alerta. Además mas servicios de envío de mensajes se pueden agregar al servicio de entrega del Cargobox, todo depende del nivel de información que el cliente este dispuesto a pagar en el servicio de transporte de carga. El objetivo de los mensajes es de asegurar y mejorar tanto la seguridad como la eficiencia de la entrega de las cargas aéreas.

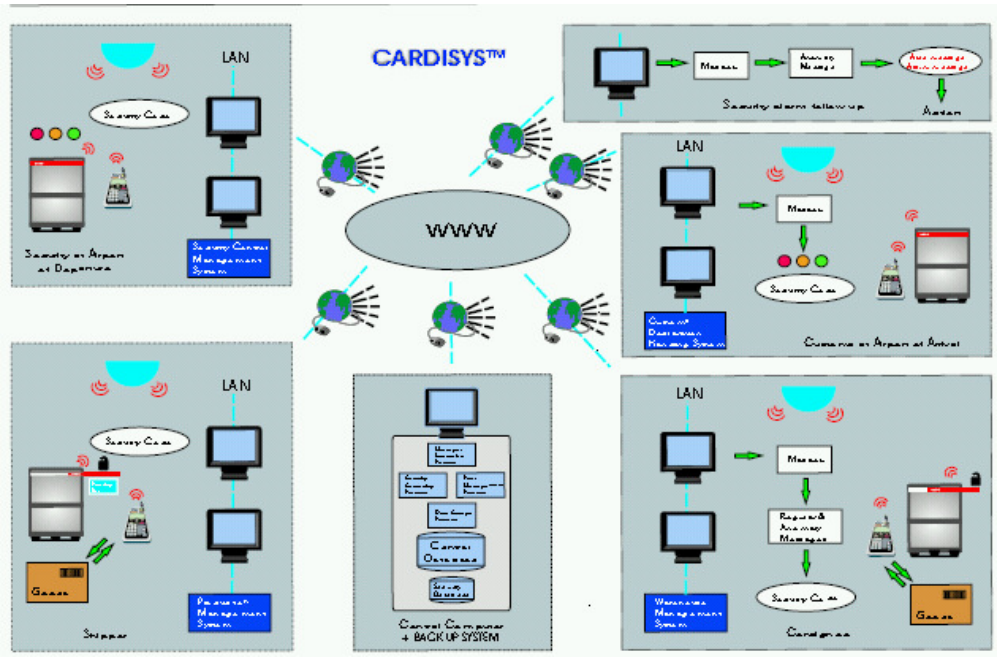


Figura 2.2.d Funcionamiento del sistema Cardisys

2.2.4 Dimensiones

Las dimensiones del Cargobox se han diseñado respetando el estándar actual de los contenedores utilizados para el transporte de carga. Es por tal motivo que se tienen 6 diferentes medidas. Una es de 125x96 pulgadas, una segunda de 125x88 pulgadas y cuatro unidades mas que entran en las dimensiones de las cargas de furgones. Además por basarse en dimensiones estándar, se pueden utilizar dichos contenedores en el transporte ferroviario de carga. Lo que facilita el transporte de los contendores en cualquier vía, de manera a que el tiempo de transporte sea reducido al máximo.

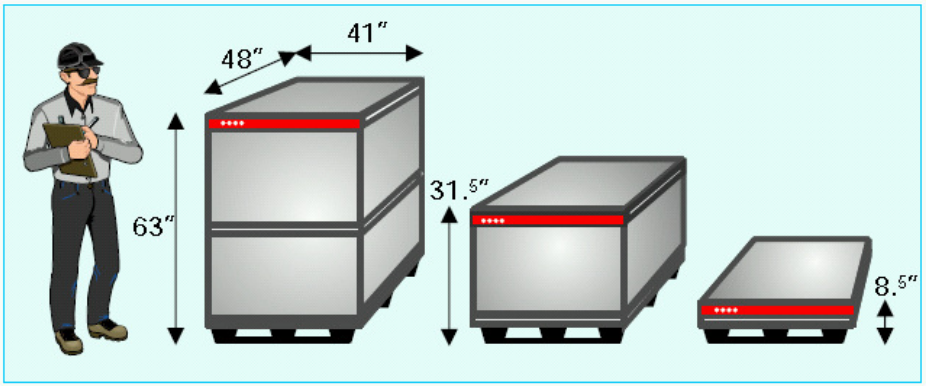


Figura 2.2.d: Dimensiones de los contenedores Cargobox

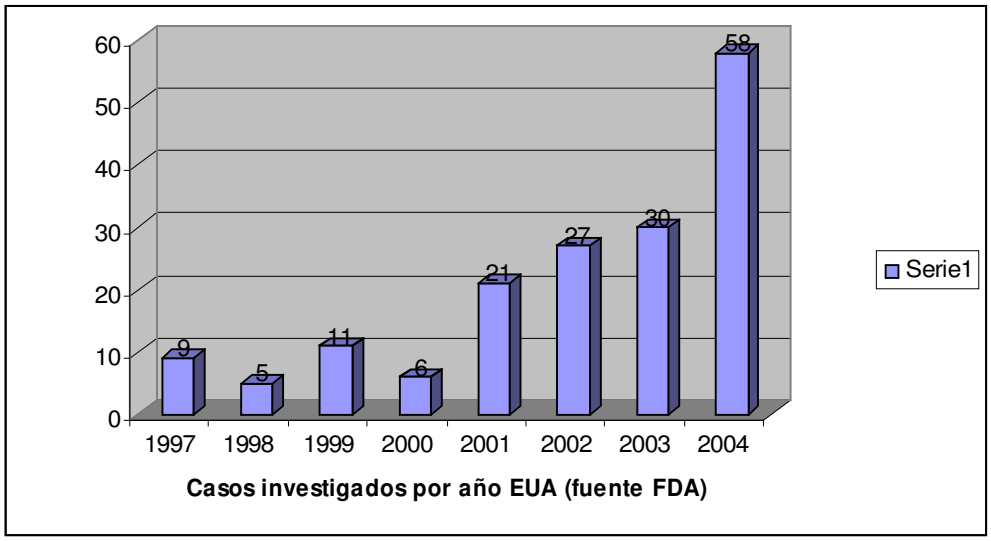
2.2.5 Pruebas de implementación

Actualmente se ha implementado dicho sistema en fase de prueba, con 1000 unidades de Cargobox, el cual durará de 18 a 24 meses. Dicho proyecto permitirá recolectar información práctica acerca de las mejoras en los tiempos de entrega y en la eficiencia del manejo de cargas aéreas.

El costo total de dicho sistema es de $3.17 millones. En el reporte final de la prueba se las conclusiones permitirán ver los pros y contras de dicho sistema versus el utilizado a nivel mundial actualemente. Sin embargo se anticipa una disminución de precios de operación entre 20% y 40%, entre costos indirectos y directos. Además se le apuesta a dicho sistema como el estándar de lso contendores de carga a nivel mundial en un par de años mas.

2.3 Implementación de RFID en la industria farmacéutica

La tecnología RFID/EPC permite obtener un control sobre el suministro, proporcionando la visibilidad total de los medicamentos desde su fabricación hasta el punto de venta. Además, tiene un impacto directo en la salud del consumidor, ya que es posible utilizar sus características para identificar medicamentos falsificados.
Como podemos observar en la gráfica, el número de casos investigados por falsificación de medicamentos en EEUU, según la FDA (Administración de Alimentos y Medicamentos), se ha disparado en los últimos años.



Algunos de los medicamentos que se falsificaron en EEUU fueron Lipitor, Viagra, Genapharm y Serostim.
Según la Organización Mundial de la Salud (OMS), la falsificación de medicamentos ronda entre el 6% y el 10% del mercado mundial. El estudio indica que afecta especialmente a los países en desarrollo que, entre 1999 y 2000, registraron el 60% de los casos denunciados, frente al 40% por ciento de los casos de los industrializados. En el 2005 creció un 40% a nivel mundial.
El comercio de medicamentos falsos es muy lucrativo y puede llegar a alcanzar los 75.000 millones de dólares en 2010, lo que supondría un incremento del 92% respecto a 2005. En Asia llegan hasta el 30% y en algunos países del continente suponen el 50 %. El año pasado se localizaron 781 casos de falsificación, en 89 países, frente a los 557 de 2004, con 67 países afectados. Entre los que tienen mayor riesgo de falsificación de medicamentos ocupa la primera posición Rusia, seguida de China, Corea del Sur, Perú, Colombia, Estados Unidos, Reino Unido, Ucrania y Alemania.
Respecto al canal de distribución, Internet es la principal vía en los países desarrollados, aunque también existe el mercado negro y los gimnasios. En las regiones más desfavorecidas, la falta de una regulación específica facilita su venta.

2.3.1 El riesgo de consumir medicamentos falsificados

La composición de los fármacos falsos puede poner en riesgo la salud, debido a la falta de calidad en su fabricación y a que contienen sustancias distintas a las del medicamento original, según los estudios de diversas entidades sanitarias.

Los medicamentos falsificados que se venden no contienen la misma sustancia que el original y su calidad es dudosa, según ha constatado el Colegio de Farmacéuticos de

Barcelona, mediante su Observatorio de Medicamentos de Abuso. Los análisis realizados por este organismo revelan que la red oferta fármacos como parches anticonceptivos u hormona del crecimiento, con ausencia total del principio activo del producto al que imitan.

Asimismo, analíticas de unidades de Viagra (para la disfunción eréctil), obtenidas mediante el mercado negro, mostraban una mayor concentración del principio activo. Estos resultados del Observatorio coinciden con los últimos datos de la Organización Mundial de la Salud (OMS) sobre medicamentos falsos, según los cuales, el 43% carece de principio activo, el 24% es de mala calidad, el 21% tiene menos principio activo del que debieran y el 7% contiene ingredientes inadecuados.

La OMS recuerda que la gente no puede morir por llevar un bolso o una camiseta falsos, pero si por tomar una medicina falsificada.
Por ejemplo, hace poco en España, se desarticuló la mayor producción y distribución de sustancias dopantes ilegales en el ámbito mundial. La Agencia Española de Medicametos y Productos Sanitarios (AEMPS) ya alertó sobre el grave riesgo para la salud que supone el consumo de anabolizantes falsificados como pueden ser alteraciones hormonales, diabetes, afectación cerebral y la posible producción de tumores, depresión, agresividad o infarto cerebral o de miocardio pueden ser algunos de los efectos de los productos dopantes falsificados, según advertía la AEMPS, debido a las sustancias tóxicas que contienen y a las malas condiciones higiénicas en las que son fabricados.

2.3.2 Beneficios para la cadena de suministro de la industria farmacéutica

Laboratorio
• Producción basada en la demanda
• Control de inventarios en tiempo real
• Combate a la piratería
    o Mayores ventas
    o Prestigio de marca
• Aumento en el nivel de servicio

Distribuidor
• Reabastecimiento oportuno
• Control de inventarios en tiempo real
• Eficiencia operativa
• Eficiencia en devoluciones
• Control de caducidades de los productos

Punto de venta (Minorista)

• Reabastecimiento oportuno
• Control de inventarios en tiempo real
• Reducción de pérdidas
• Eficiencia en devoluciones
• Control de caducidades de los productos

Consumidor
• Mayor surtido
• Combate a la piratería
    o Salud
    o Certeza que el medicamento es auténtico
• Producto siempre en existencia
• Venta de productos no caducados

Analizando en detalle cada una de las aplicaciones de RFID en la industria farmacéutica, obtenemos los siguientes modelos de valor.
• Combate a la piratería
• Logística de devoluciones
• Reabastecimiento
• Pérdidas
• Operaciones eficientes

2.3.2.1 Combate a la piratería

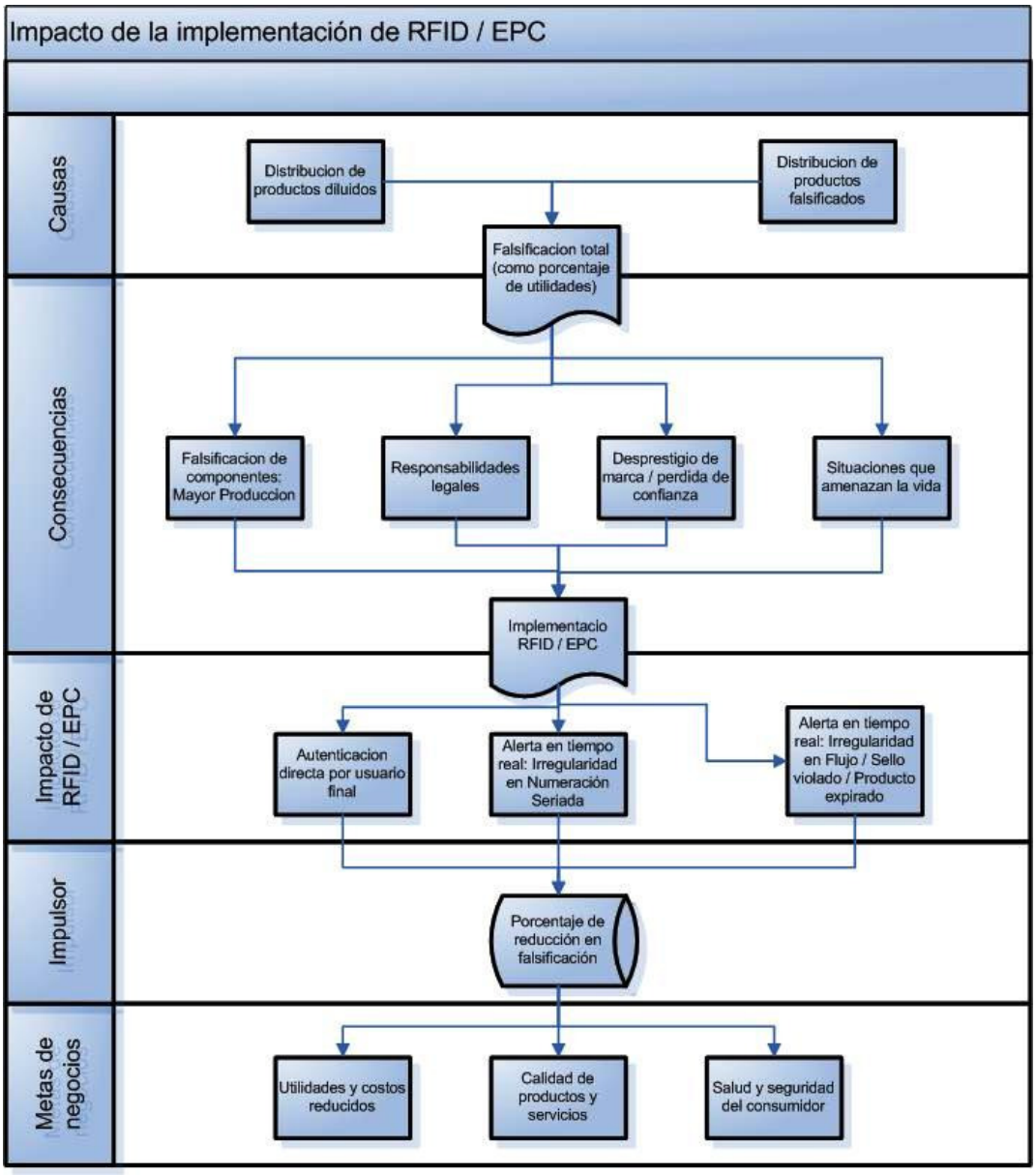
Las causas que provocan la piratería son:
• Distribución de productos diluidos
• Distribución de productos falsificados

Provocan que un determinado % de los medicamentos no sean los correctos con las siguientes consecuencias:
• Falsificación de componentes: mayor producción global
• Responsabilidades legales
• Desprestigio de marca y pérdida de confianza
• Situaciones que amenazan la vida

Impacto de la implementación de RFID/EPC
• Autenticación directa de usuario final
• Alerta en tiempo real de irregularidades en la numeración seriada de los productos
• Alertas en tiempo real de irregularidad en flujos, sellos extraídos, productos expirados.

Mediante RFID/EPC obtendremos un % de reducción de la falsificación, como objetivo principal. Además obtendremos otros beneficios gracias a la visibilidad en toda la cadena de suministro.

Los objetivos de negocio son:
• Reducción de costes
• Calidad de los productos y servicios
• Salud y seguridad del consumidor final



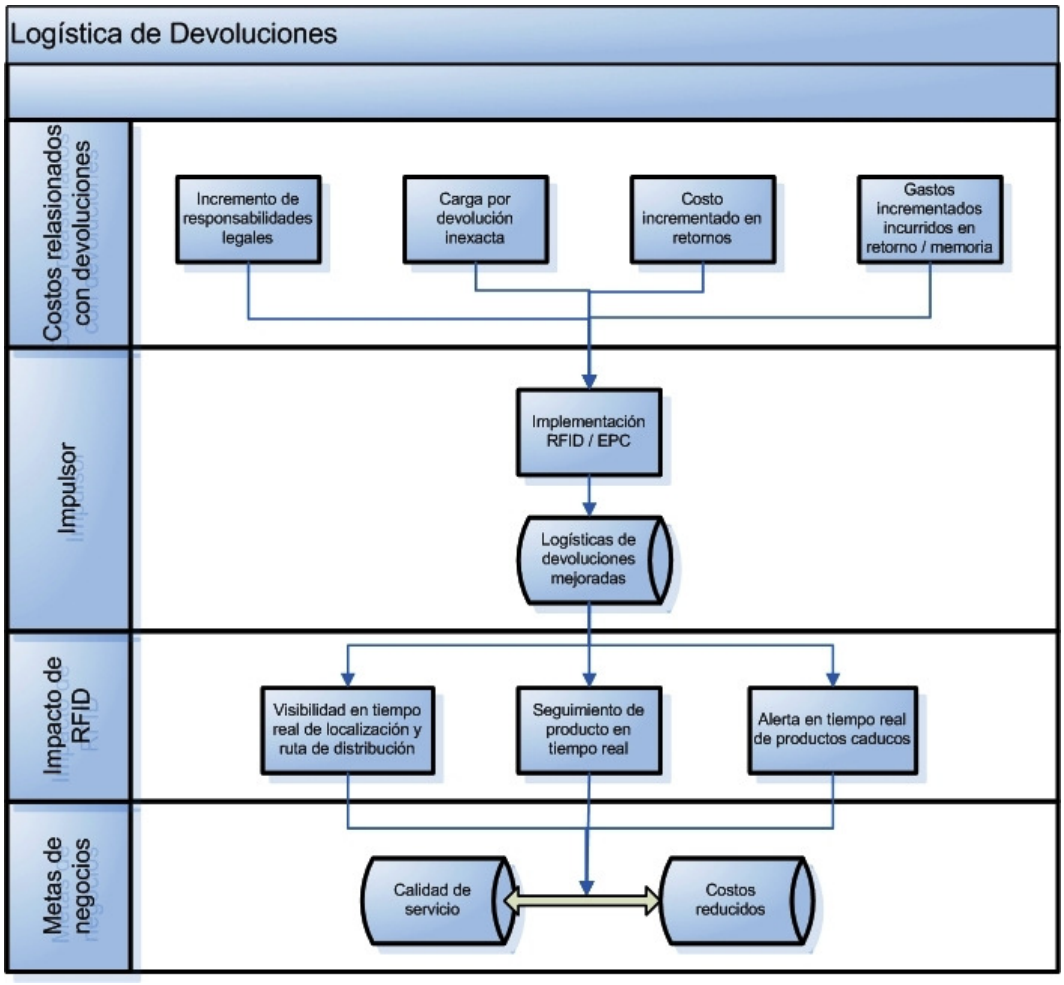
Fuente EPCglobal.

2.3.2.2 Logística de Devoluciones

Costes relacionados con las devoluciones
• Incremento de responsabilidades legales
• Carga por devolución inexacta
• Incremento de los costes por los retornos

Con RFID/EPC mejoramos la logística de devoluciones (Logística inversa)
• Visibilidad en tiempo real de la localización y ruta de distribución
• Seguimiento de producto en tiempo real
• Alerta en tiempo real de productos caducados

Obteniendo los siguientes objetivos:
• Reducción de costes
• Calidad de servicio



Fuente EPCglobal

2.3.2.3 Reabastecimiento

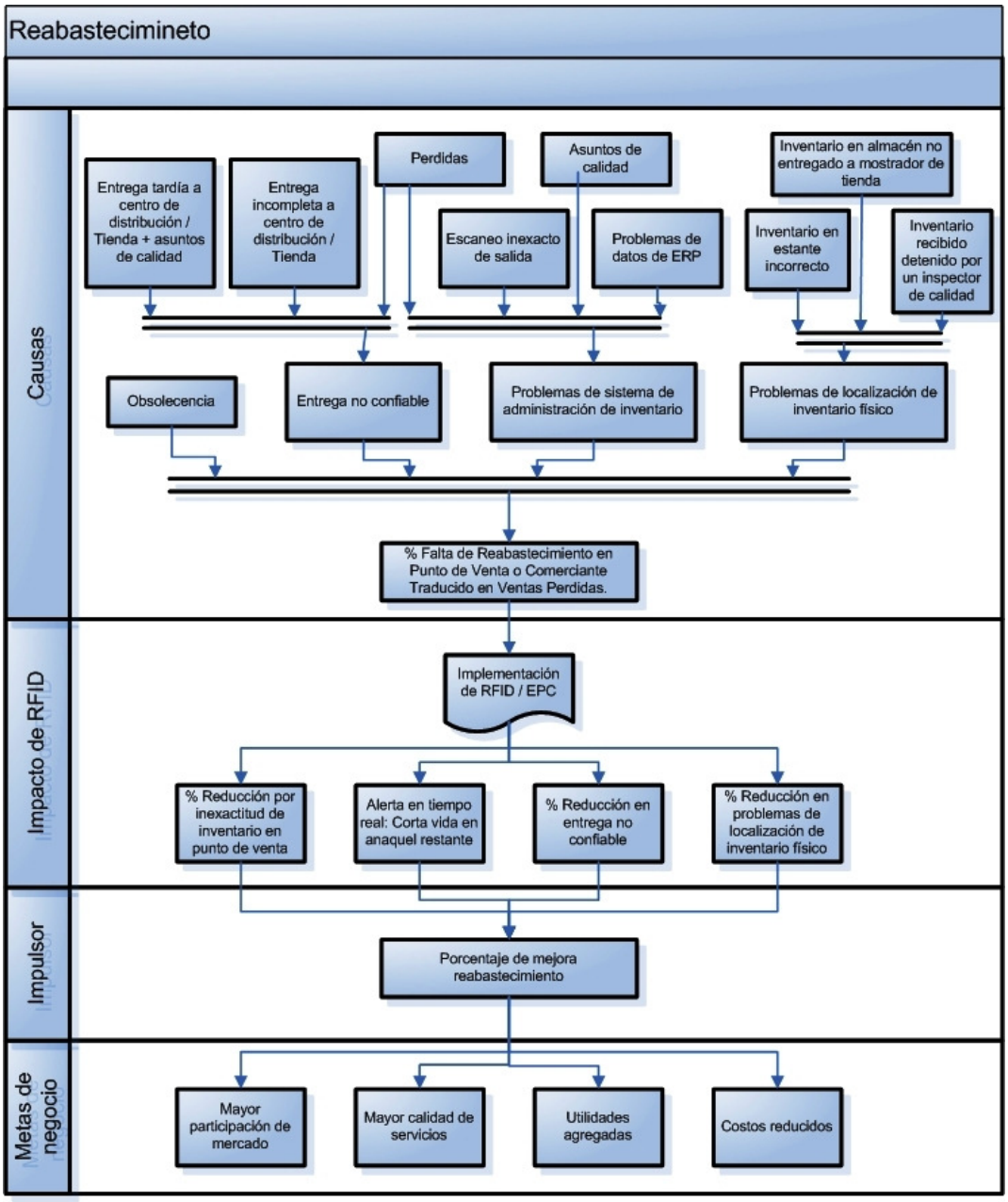
El porcentaje de falta de reabastecimiento en el punto de venta traducido en ventas perdidas es provocado:

• Obsolescencia
• Entrega no confiable
o Entrega tardía al centro de distribución o tienda.
o Factores de calidad
o Entrega incompleta al centro de distribución o tienda
o Pérdidas
• Problemas de sistema de administración de inventario
o Pérdidas
o Escaneo inexacto de la salida
o Factores de calidad

o Problemas de datos en el sistema ERP
• Problemas de localización del inventario físico
• Inventario en estante incorrecto
• Inventario en almacén no entregado a la tienda
• Inventario recibido pero detenido por cuestiones de calidad

Con la implementación de RFID/EPC podremos obtener un elevado impacto en:
• % reducción por inexactitud del inventario en el punto de venta
• Alerta en tiempo real
• % reducción en entrega no confiable
• % reducción en problemas de localización del inventario

Estos factores aportan una mejora en % del reabastecimiento con el objetivo de negocio:
• mayor participación en el mercado
• mayor calidad de servicio
• Reducción de costes



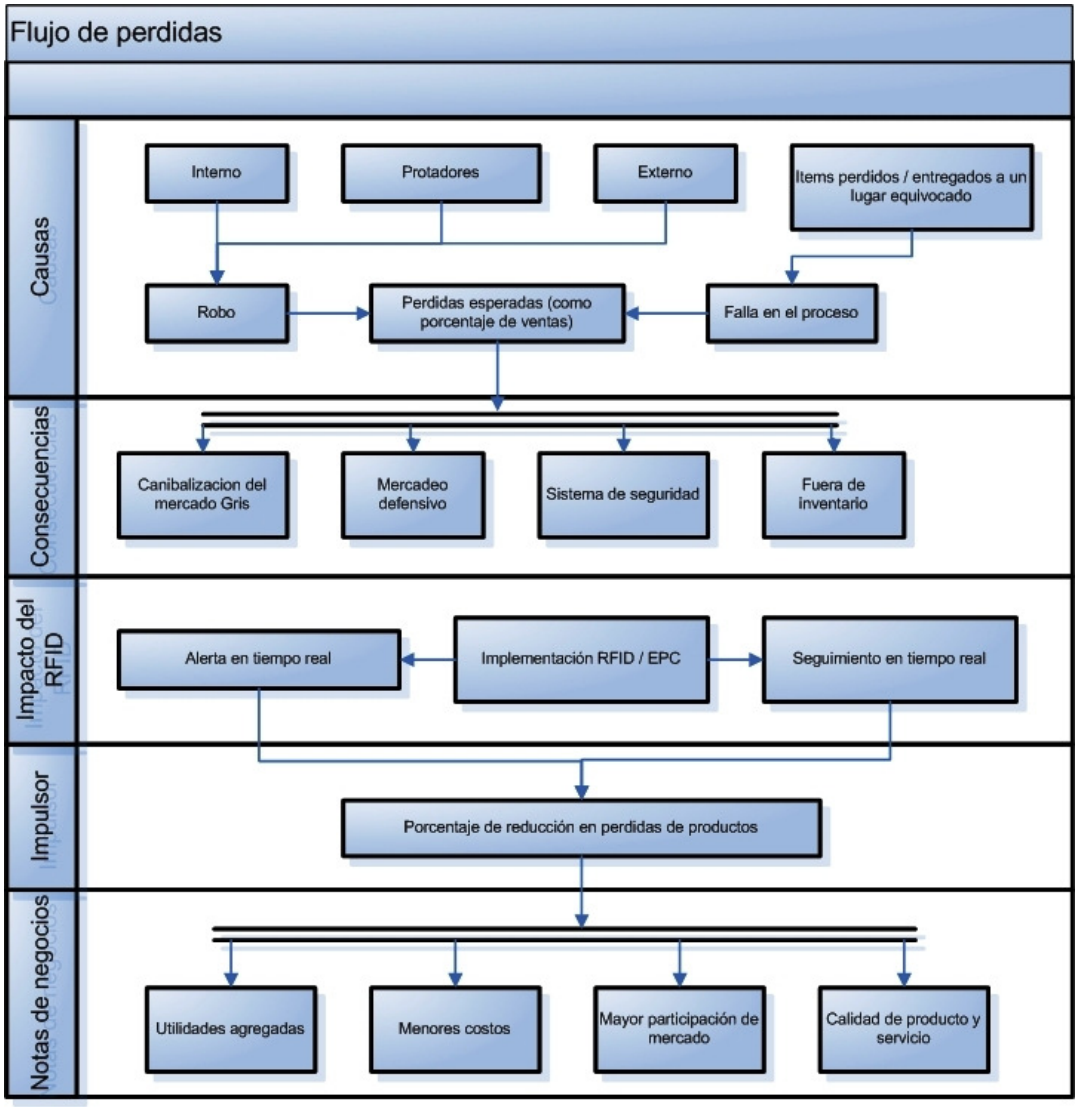
Fuente EPCglobal

2.3.2.4 Pérdidas

Las causas que provocan pérdidas son:
• Robo (Interno como externo)
• Pérdidas esperadas % de ventas (incluye los robos)

• Fallo en procesos (Unidades pérdidas o entregadas en lugares equivocados)

Con RFID/EPC tenemos alertas y seguimiento en tiempo real, obteniendo una reducción en % en pérdidas de productos. El objetivo es:
• Menores costes
• Mayor participación en el mercado
• Calidad de producto y servicio



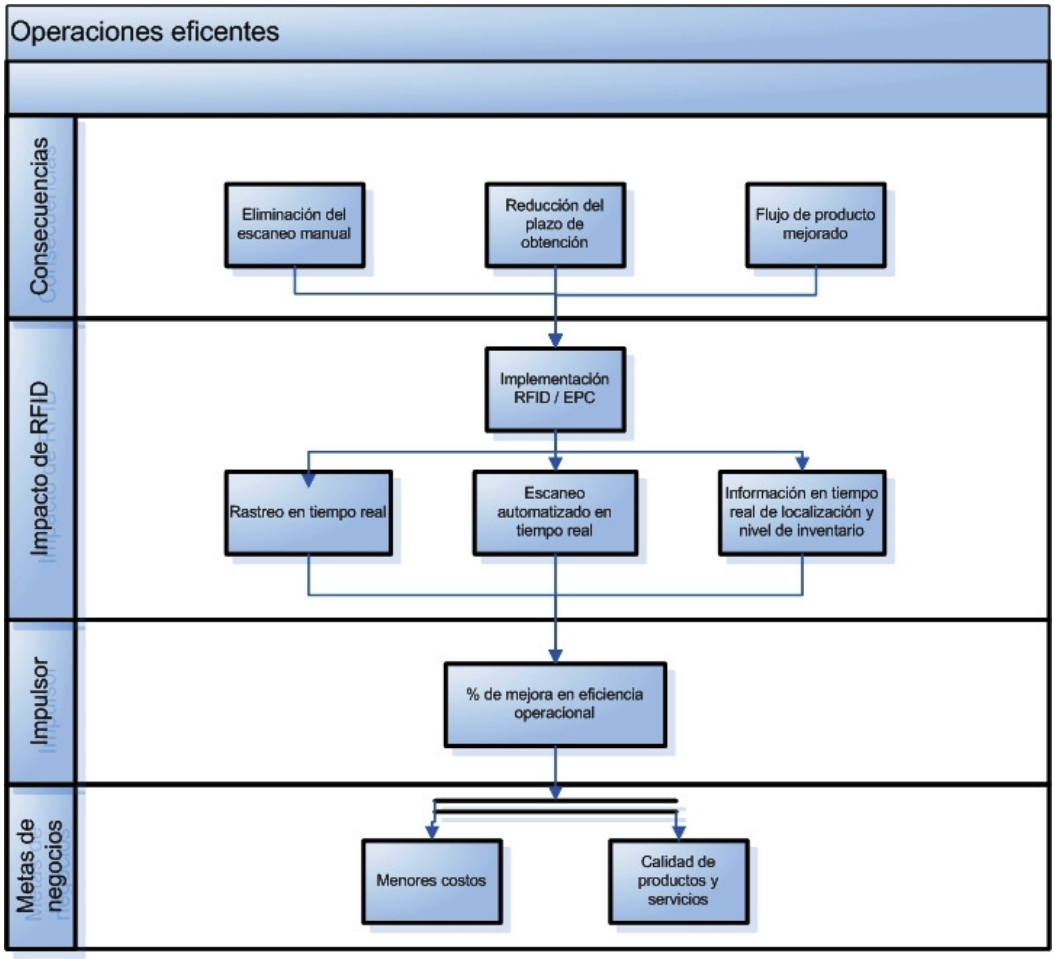
Fuente EPCglobal

2.3.2.5 Operaciones eficientes

La implementación de RFID/EPC persigue:
• La eliminación del escaneo manual
• Reducción del plazo de obtención
• Mejora del flujo del producto

Impactando en:
• Rastreo en tiempo real
• Escaneo automatizado
• Información en tiempo real de localización y nivel de inventario

Proporcionando una mejora en % en eficiencia operacional, con el objetivo de reducir costes e incrementar la calidad de servicio y producto.



Fuente EPCglobal

2.3.3 La frecuencia adecuada

La administración de alimentos y medicamentos de Estados Unidos (FDA) hizo públicos los planteamientos para la implementación de la tecnología RFID en la industria farmacéutica, y publicó un informe incluyendo todos estos planteamientos. Sin embargo, aunque existe el requerimiento de que los medicamentos incorporen tags a nivel de ítem, la FD no hizo ninguna recomendación concreta sobre la frecuencia a utilizar. Dos frecuencias fueron contempladas para llevar a cabo el proyecto, HF y UHF en sus respectivas frecuencias para uso de la tecnología RFID.
A pesar de que la cadena de suministro se ha volcado en UHF, algunos fabricantes de edicamentos han llevado a cabo pilotos con tags de HF para pruebas a nivel de unidad.

Sus principales argumentos son que la frecuencia HF esta regulada mundialmente, la tecnología es más madura, funciona mejor en líquidos y tiene mayores tasas de lectura a cortas distancias para la identificación a nivel de unidad.
Algunos de los fabricantes más reconocidos, como Phillips, Texas Instruments y Tagsys publicaron un documento en el 2004 comparando HF y UHF que proporcionan los argumentos suficientes para seleccionar HF. Pero hay que tener en cuenta que en esos momentos, ninguno de los fabricantes mencionados tenía productos en UHF, pero si se han dado prisa para desarrollar productos que cumplan con el estándar EPC, sobretodo de Gen2.
La opinión de algunas personas involucradas en los pilotos de la industria farmacéutica que han experimentado tanto con HF como en UHF, este es el caso de Rob Coyle, director de sistemas de GlaxoSmithKline, UHF es mejor frecuencia para trabajar a nivel de caja y palet, pero HF sigue siendo mejor para nivel unidad.

2.3.4 Análisis de riesgos

Al igual que cualquier reingeniería de procesos, la implementación de una nueva tecnología como RFID/EPC implica riesgos que deben ser identificados para poder mitigarlos. Algunos afectan directamente al consumidor, otros a los trabajadores implicados y como último a las decisiones relacionadas con el planteamiento inicial.

El siguiente listado desglosa alguno de los riesgos:

Incompatibilidad de frecuencias y estándares con otras industrias: provocaría que el proyecto no fuera sostenible a largo plazo por no trabajar con las frecuencias y estándares de las industrias relacionadas como podría ser el sector minorista. Por este motivo debe seleccionarse un estándar global considerando los avances de la industria.

Percepción en el consumidor de invasión a su privacidad: provoca un rechazo del consumidor a adquirir productos etiquetados con RFID. La solución esta en informar al consumidor sobre las características del proyecto y los alcances de la tecnología. También notificar en el embalaje la presencia del tag para que el consumidor tenga la opción de removerlo si así lo desea.

Resistencia al cambio de los trabajadores: el impacto negativo se encontraría en la falta de colaboración de todas las partes implicadas en la cadena de suministro debido a los costes de implementación y los cambios en las operaciones actuales.

Incremento de la temperatura en los medicamentos líquidos sujetos a exposición prolongada a las ondas radio: puede provocar el incremento de 1,1º a 1,7º C si un medicamento líquido se mantiene por más de 1 hora a menos de 40 cm. de la antena. La solución es evitar la exposición prolongada a corta distancia de medicamentos cuyas propiedades se afecten con los incrementos de temperatura descritos anteriormente. En el caso de encontrarnos con esta problemática habrá que diseñar procedimientos y recomendaciones para estos casos.

Productos o embalajes con materiales opacos a la radiofrecuencia: provocan dificultades de etiquetado y lectura de los productos con alto porcentaje de líquidos y metales.
Actualmente hay productos especiales para sobrepasar esta problemática, en los casos más extremos hay que rediseñar el embalaje.

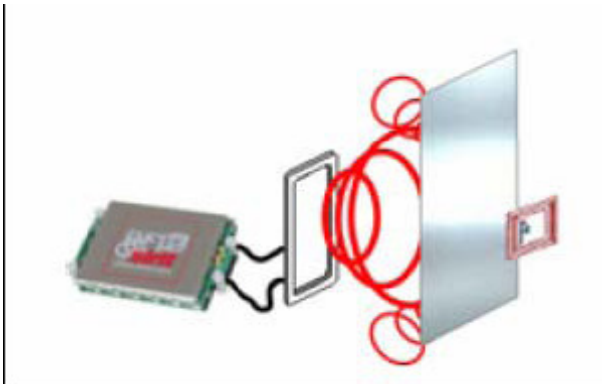
2.3.5 Recomendaciones de etiquetado y materiales de empaque

Las ondas radio se pueden clasificar según dos modalidades de acuerdo al efecto que tienen.

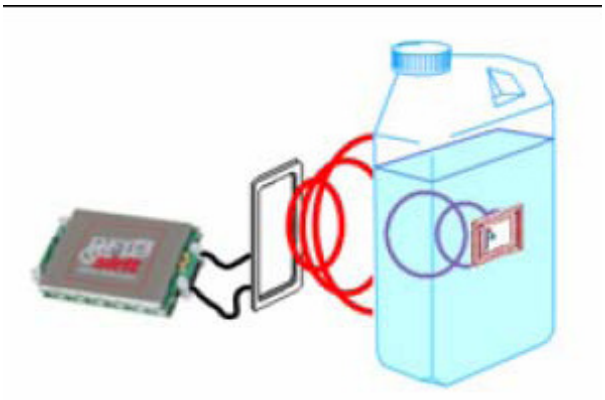
• **Luminosos:** materiales transparentes a las ondas radio como pueden ser por ejemplo plásticos en general, madera, cartón o papel seco.

• **Opacos:** materiales no transparentes a las ondas radio.

Reflejantes: impiden el paso de las ondas radio y las reflejan, por ejemplo los metales.



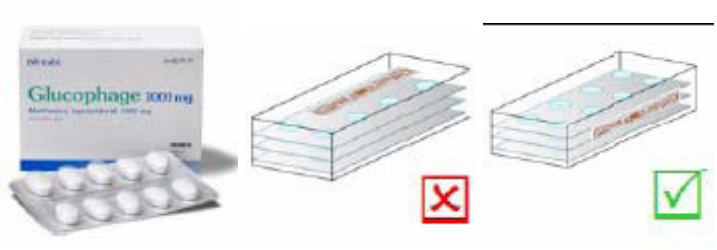
Absorbentes: como su nombre indica, absorben las ondas radio a su paso provocando atenuación de la señal. Esto sucede en materiales como por ejemplo los líquidos.



En el sector farmacéutico existen un gran porcentaje de medicamentos con materiales opacos a las ondas radio, tanto en su contenido como en su embalaje. Esto no quiere decir que no puedan ser etiquetados mediante RFID/EPC, sino que habrá que estudiar bien la ubicación de la etiqueta. Es más, seguro que es necesario la realización de pruebas o la asistencia de un experto en la materia.
A continuación mostramos varias recomendaciones de etiquetado para diferentes productos farmacéuticos.
En un medicamento líquido con envase de cristal y embalaje de cartón, si colocamos la etiqueta directamente sobre el envase plástico corremos el riesgo que el líquido que absorbe las ondas esta muy próximo, además si la señal de lectura le viene por el otro lado lo más seguro que no llegue o que lo haga de manera insuficiente. A esto hay que añadir que la señal del tag seguro que es absorbida totalmente.

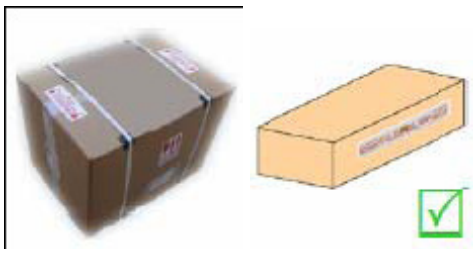
Por estos motivos la etiqueta RFID debe ser colocada sobre el cartón del embalaje, preferentemente en la parte que presenta mayor distancia al contenido líquido como pueden ser las esquinas.

En los medicamentos comprimidos, con embalaje de cartón y los blisteres de plástico y aluminio nos encontramos con la problemática del material reflejante del blister, que además acostumbra a ocupar casi la totalidad de la superficie de la caja. En este caso deberemos procurar que el tag no este situado en la misma posición del blister por los efectos que comportaría. La mejor situación en estos casos es colocar el tag o etiqueta sobre la caja de cartón en el lado perpendicular al foil del blister de aluminio.



En los medicamentos comprimidos almacenados en un bote o embalaje de plástico no existen demasiadas restricciones porque los materiales normalmente son luminosos para las ondas radio, sólo habrá que tener en cuenta un detalle en la posición del tag. Por todo ello, la etiqueta se debe situar en el propio envase plástico pero que el tag este situado perpendicularmente a su base, así evitamos que la etiqueta se doble lo que afectaría a su comportamiento. Debemos recordar que le tag debe estar en una base lo más uniforme posible.

Para etiquetar las cajas no hay ninguna restricción. El tag se coloca directamente e la superficie de cartón. Sólo habrá que tener en cuenta que el lado de la caja donde se sitúa el tag sea el lado donde se ubique el lector. Las posibles problemáticas podrían llegar en lecturas de palets donde hubieran múltiples cajas y que alguna de ellas estuviera entre más de una, según los medicamentos de su interior habrán problemáticas o no. Por ejemplo si pasamos 9 cajas que están en un palet, puede pasar que las situadas en el punto más interior no puedan llegar a leerse.



A nivel de palet sucede como a nivel de cajas, no existen restricciones de la ubicación. El tag se debe colocar en uno de los lados de los paquetes donde puede ser leído por una antena o lector.

2.3.6 Conclusiones de implementación en industria farmacéutica

Los agentes de la cadena de suministro pueden obtener beneficios de la tecnología RFID/ EPC en la medida en que exista colaboración y buenas prácticas entre todas las partes.

Su impacto no sólo debe medirse con el retorno de la inversión directo que proporcionan la eficiencia de las operaciones, sino también las ventajas y oportunidades que proporciona la visibilidad total que actualmente no tenemos.
La cadena de suministro de la industria farmacéutica tiene una gran oportunidad de tener control sobre el origen y transito de los medicamentos y ayudar a resolver el problema de salud pública que representa la falsificación.

La tecnología RFID/EPC es una poderosa herramienta para las operaciones logísticas y el control de inventarios en tiempo real, pero su implementación esta lejos de ser trivial.

Es muy importante asegurar la calidad y el cumplimiento de estándares internacionales, tanto de los dispositivos como de las empresas que nos proporcionan los servicios profesionales de asesoría, instalación, soporte y formación.

2.4 Sistemas RFID en la cadena de suministros *"Supply Chain Execution" (SCE)*

Los Sistemas "Supply Chain Execution" (SCE) administran el inventario, espacio, equipamiento, actividades, y recursos de transporte para asegurar el cumplimiento oportuno, libre de errores y visibilidad del estado del pedido a través de la cadena de suministro.

Ejecución y visibilidad de la cadena de suministro

Un sistema SCE puede ser visto como la integración de otras herramientas de ejecución y visibilidad de la cadena de suministro, tales como sistemas de administración de transporte (TMS) y sistemas de administración de trabajo (LMS) con un sistema de administración de almacén (WMS)

SCE = WMS + TMS + LMS + YMS

2.4.1 Componentes de los Sistemas SCE

"*Warehouse Management System*" (WMS) integra software, hardware y equipos periféricos para administrar en tiempo real los inventarios, espacio, equipamiento y actividades en almacenes y centros de distribución, con el objeto de maximizar la eficiencia de movilizar los productos al mercado. Además se ocupa de monitorear el desempeño de los procesos de recepción, almacenaje, picking y despacho.

"*Transportation Management System"* (TMS) optimiza el uso de los recursos de transporte para administrar la carga de entrada, de salida y despachos internos al más bajo costo, consistente con los estándares de servicio al cliente y los requerimientos de los socios de negocio. Un TMS provee mayor control sobre las operaciones e incrementa la eficiencia de transporte. Permite al usuario tomar decisiones apropiadas de transporte de carga basadas en reglas específicas del negocio.

"*Labor Management Systems*" (LMS) es un componente relativamente nuevo de los SCE. Permite medir la productividad, compararlo contra estándares, establecer programas de entrenamiento, determinar programas de pagos y de incentivos, y planificar las necesidades de trabajo para próximos proyectos. El desempeño puede ser monitoreado a nivel individual o grupal, utilizando estándares de ingeniería o datos históricos. El rastreo puede ser realizado con equipos RF o terminales PC. LMS permite que los costos de mano de obra se asocien directamente con pedidos de clientes, utilizando un enfoque de costeo basado en actividades.

"*Yard Management System*" (YMS) controla el flujo de tráfico y las actividades asociadas con las plataformas de recepción y despacho (muelles) y el patio de operaciones. El YMS planifica y coordina las operaciones de recepción y entrega para producir un tráfico fluido de vehículos y documentación evitando cuellos de botella en el patio.
No todos los SCE están necesariamente organizados tal como se ha descrito previamente. En ocasiones, la funcionalidad de un LMS puede ser incluida dentro de un WMS. Además, cabe la posibilidad que en ciertos casos un YMS pueda ser considerado un subsistema de un TMS.
Los WMS surgieron en la década de los 70's para permitir el rastreo en tiempo real de los materiales y la administración de los recursos en almacenes convencionales. Hoy en día, muchos WMS también brindan soporte al servicio de almacenamiento mecanizado mediante interfaces a equipos automatizados de manipuleo de materiales.
Como otros sistemas de ejecución, los WMS tienden a operar en un "silo" y enfocarse sólo en optimizar las actividades dentro de las cuatro paredes del almacén o centro de distribución. El actual enfoque estratégico de la gestión de las cadenas de suministro como herramienta competitiva, así como el potencial de Internet como facilitador de la colaboración entre los participantes de la cadena, dejan claro que la visión restrictiva de las cuatro paredes de una instalación debe ser expandida. El concepto de SCE fue

desarrollado para abarcar todos los componentes de sistemas de ejecución que soportan las funciones logísticas y de ejecución de la cadena de suministro.

Los sistemas SCE pueden ser un único producto integrado o varios productos de diferentes proveedores que interactúan entre sí.

2.4.2 Principales funcionalidades de los componentes de un SCE

Warehouse Management Systems (WMS)

- Comunicación de Datos por Radio Frecuencia
- Captura Automática de Datos RFID
- Control de calidad, bloqueo de inventario, asignación, liberación
- Cross Docking
- Monitoreo de caducidad de productos
- Procesamiento de devoluciones
- Punto de reposición / Consolidación
- Planeamiento y Programación de Órdenes
- Interpolación de tareas
- Conteo cíclico
- Rastreo de fechas, lotes y números de serie
- Monitoreo de desempeño en la recepción, almacenamiento, picking y despacho

Transport Management Systems (TMS)

- Administración de ruteos, incluyendo comparación de costos de los diferentes modos de transporte, tales como camión lleno, menos que camión lleno (LTL), intermodal, aéreo.
- Planeamiento y construcción de carga
- Selección de transportista
- Programación y consolidación de embarques
- Rastreo del estado de la carga (via web)
- Calculo de costos de transporte y selección de la mejor alternativa
- Auditoria de transporte y orden de pago.
- Evaluación de desempeño de transportistas

Yard Management Systems (YMS)

- Rastreo de camiones, trailers, sus contenidos y ubicaciones
- Administración de la puertas individuales de los muelles y ubicaciones del patio

- Visibiidad de los productos en cada puerta de los muelles.
- Manejo de entregas de urgencia
- Manejo de crossdocking de cargas parciales o totales de camiones
- Visibilidad a través de todos los patios.

2.4.3 Desafíos de la cadena de suministros

A Continuación se detallan algunos de los desafíos mas frecuentes de la cadena de suministros de una organización:

- Incorrecto envío de bienes.
- Entrega tardía de bienes.
- Dificultad en la localización de bienes.
- El extravío o robo de bienes
- El esfuerzo excesivo requerido para una precisa unificación entre los bienes físicos que el cliente pide y recibe.
- La previsión inexacta de bienes

Estos problemas ocurren debido a la combinación de muchos factores como procesos comerciales, datos de entrada múltiple, localización de activos con tecnologías pasiva, procesos comerciales iniciados por humanos, entre otras

Manejadores de mercado

Continuación se muestran algunos manejadores del mercado que surgen por la necesidad de un cambio en la cadena de suministro:

- Más del 20% de los productos alimenticios son descartados debido al vencimiento de los mismos ocasionados por una deficiente administración en la cadena de suministro.
- La inflación ocasionada por el empaquetado de los bienes entregados al consumidor en la cadena de suministro es anualmente de $60B, esta inflación se atribuye al robo, al vencimiento, perdidas y los daños ocacionados antes de localizar a los clientes.
- Los costos directos e indirectos de cargos por robos son de $20-60B anualmente.
- Arriba del 10% de los productos son falsificados, esto significa que el costo total de falsificación.
- La falta de productos en stock cuesta el 6% de ventas, etc.

2.4.4 Programas Alternativos.

Un número significativo de empresas líderes en el ámbito de la industria han optado por mejorar la eficiencia de sus procesos automatizando sus líneas de producción con tecnología de RFID, dando un cambio significativo a la industria de mercado de la siguiente manera:

- En Junio de 2003 Wal-Mart, el minorista más grande de mundo, anunció que sus 100 proveedores deben empezar a implementar RFID para lograr estandarizar sus procesos en enero de 2005. Luego de esto Wal-Mart solicita a finales del 2006 que sus siguientes 200 proveedores implementen RFID en sus líneas de producción.

- El departamento de Defensa de Estados Unidos (DoD) hizo un anuncio similar con respecto un sistema de rastreo con RFID con un costo por arriba de $5000 US en 2005 de enero. Los sistemas actuales empleados por DoD usan tecnología de RFID activa por el rastrear contenedores. Por otra parte sistemas de RFID pasivos, se implementaran para rastrear los volúmenes de recipientes, usando combinaciones de GPS y tecnologías de comunicación por satélite, entre otros.

- Hewlett-Packard (HP), que tiene la novena cadena de suministro no-militar más grande del mundo se encontrara dentro las directivas de Wal-mercado y El departamento de defensa de EEUU. HP empezó ensayos y pruebas piloto involucrando tecnología de RFID hace tres años con la finalidad de mejorar su cadena de suministros y competir con la demanda exigida por sus clientes.

- Marks & Spencer ha incorporado una cantidad significativa de *tags* de RFID en sus productos retornables involucrando el sistema a su cadena de suministros.

- Metro Group a finales del 2004 solicito que sus 100 proveedores contaran en su cadena de suministros con tecnología RFID.

- Telefonica Movistar desde Diciembre de 2005, trabaja en el desarrollo de una oferta sectorial que cubre las necesidades específicas en las áreas clave de la empresa como en la cadena de suministro y relacion a terceros con la implementacion de RFID.
  (ver *http://www.empresas.telefonica.es/publicaciones/tendencias_IDS/RFID.htm*)

2.4.5 Logros basados en la tecnología RFID.

La aplicación de tecnologías basadas en RFID estan siendo usadas para dar solucion a diferentes problemas específicos en aplicaciones comerciales, como por ejemplo:

- Mejoras en procesos de fabricación y reparación para la identificación de partes disponibles en inventario en tiempo real.
- Mejoras en la identificación de fallas en productos y el rastreo de los mismos.
- Incrementar en campo de cobertura de inventario sin modificar la ubicación y disposición de los bienes inventariados y todo con lecturas en tiempo real.
- Mejora de tiempos en el proceso de inventario de mercadería en lugares de despacho de carga.
- Mejor control de expiración y/o vencimiento de productos perecederos.
- Reubicación de mercadería con menor tiempo de vida con la finalidad evitar la perdida del mismo
- Alarmas en tiempo real de proximidad de vencimiento de productos alimenticios.
- Identification de tipo de productos que más se consumen.
- Identificación de la mejor ubicación de mercadería en base a la estadística de manoseo del producto.
- Aumentar las ventas a través de una mayor visibilidad del producto
- Reducir costos incrementando el rendimiento
- Proteger productos de manipulación y falsificación
- Ahorrar costes de mano de obra
- Reducir el fraude de los vendedores
- Recortar los descuentos en las facturas y los errores administrativos

CAPITULO 3: Interoperatividad

En este capitulo se aborda un tema de gran interés para todos aquellos que quieran implementar una red tipo WLAN, es decir basada en puntos de acceso inalámbricos (AP) bajo el protocolo 802.11, en combinación con sistemas de identificación basados en radio frecuencia RFID.

3.1 Impulsores de la interoperatividad

En la actualidad las redes inalámbricas han tenido una gran aceptación, ya sea por su comodidad al no tener que cablear ni utilizar canaletas, por estética al no querer cables visibles, por la ventaja de poder llegar con señal en áreas de difícil acceso o costosas de manera cableada, etc.

Tener que montar una infraestructura nueva, implica elevados costos debido a la capacitación de personal para instalación, configuración y mantenimiento. También el hecho de tener que cambiar de tecnología tiene como resultado tiempo no productivo para una empresa. Además el hecho de mezclar varias tecnologías que funcionen a la par en vez de una tan sola que haga todo, es mas complicado por el aumento del numero de hardware que se ve involucrado en el proceso.

Debido a esto nace la necesidad de poder crear sistemas que permitan integrar las nuevas tecnologías con las ya existentes. Es donde el tema de interoperatividad tiene una gran incidencia, debido que permitiría una reducción de costos en cuanto al montaje de una infraestructura nueva. Y además le dará mayor valor a los recursos de los que ya se disponen.

Para el caso de las redes informáticas de tipo WLAN, en donde toda una infraestructura de AP (A*ccess Point* o punto de acceso para conexiones inalámbricas) está funcionando bajo estándares IEEE 802.11. Poder integrar, sobre esa misma plataforma, una compatibilidad con la tecnología de RFID se vuelve un reto de interoperatividad. Donde el punto importante es el de utilizar el mismo AP que sirve de enlace de las redes inalámbricas como el *reader* de los *tags* de RFID. Significando esta integración en un ahorro considerable desde el punto de vista de adquisición de equipos. Además el hecho de proveer a una empresa con la capacidad de darle un nuevo uso a una tecnología ya instalada provee un valor agregado.

También la necesidad, cada vez mayor, para localizar al personal y los activos de una empresa, la reducción de pérdidas de activos, la necesidad de optimizar los tiempos de atención a los clientes, guardar información acerca de procesos y sus resultados, etc. (necesidades para las cuales la tecnología RFID es una solución muy optima). Han hecho

que aparezca la necesidad de crear una compatibilidad del RFID con el mundo WiFi e integrarlos en un mismo sistema de manera óptima.

3.2 Aproximaciones acerca de la localización

La principal aplicación que puede llegar a tener este tipo de unión de los dos mundos, es la localización orientada a servicios, vigilancia y/o seguridad. Es por tal motivo que en este capitulo se darán a conocer los factores esenciales para entender como funcionan los sistemas de localización

Los sistemas de localización o de rastreo de posición se clasifican por las técnicas de medición que emplean para determinar la ubicación de un dispositivo móvil. Usualmente los sistemas de localización en tiempo real (RTLS) se pueden agrupar en cuatro categorías basadas en las siguientes mediciones: celdas de origen, distancias, ángulos, modelos de localización.

Para diseñar un sistema RTLS se pueden escoger implementar una o mas de las técnicas mencionadas con anterioridad. El objetivo de adicionar más técnicas es la optimización de la aproximación del sistema.

3.2.1 Celdas de origen

Una de las técnicas más sencillas para estimar la localización, en cualquier sistema basado en RF son las celdas (punto de acceso más cercano para tecnologías de WiFi 802.11). Tal como se muestra en la siguiente figura.

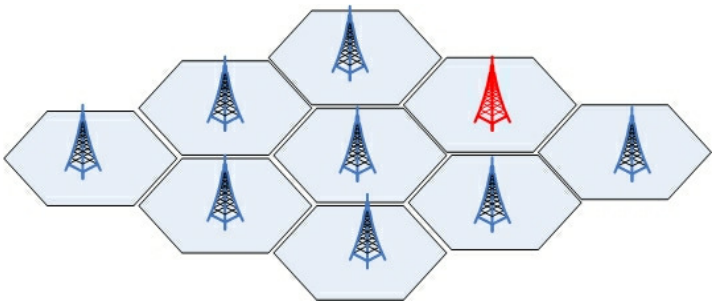


Figura 3.2.a División de zonas de cobertura por celdas

Desde el punto de vista más simple, ésta técnica no permite conocer el lugar exacto de ubicación, sino más bien únicamente la celda en donde se encuentra el dispositivo móvil. La ventaja de esta técnica es la facilidad de su implementación, debido a que no se requiere de un algoritmo complicado. Básicamente la gran mayoría de sistemas WLANs basados en celdas u otros sistemas de celulares basados en celdas de RF pueden ser

adaptados para determinar cual es la celda de origen de la señal del dispositivo móvil de una manera costo-efectiva.

Pese a la sencillez de esta solución, se pueden llegar a dar ciertos comportamientos errados, debido a que a veces, por diferentes razones, el dispositivo móvil se puede asociar a alguna celda que no este físicamente cerca (aunque las celdas mas cercanas sean mejores candidatas). A este fenómeno se le conoce con el nombre de granulosidad y puede ser especialmente frustrante cuando se necesita saber la localización exacta de de un dispositivo móvil en una estructura múltiple donde las celdas se pueden llegar a sobreponerse entre ellas.

Para determinar de una manera más certera que áreas de las celdas poseen la probabilidad más alta de contener el dispositivo móvil que se quiere localizar, se pueden tomar en cuenta ciertos métodos adicionales. Uno de ellos, es de forma manual (se busca dentro de cada celda a ver si ahí se encuentra el dispositivo móvil) y el otro es basado en computadora.

Las celdas reciben una información que se denomina: *received signal strength indication (RSSI)*. En base a esta información se puede utilizar la técnica de "la fuerza de señal más alta". De esta forma la localización del dispositivo móvil se realiza mediante la detección de la celda que detecte la señal más alta, eliminando así el efecto de la granulosidad. En la siguiente figura se muestra, se muestra un dispositivo móvil en color rojo, se encuentra ubicada cerca de la celda que lo ha identificado con la señal más alta.

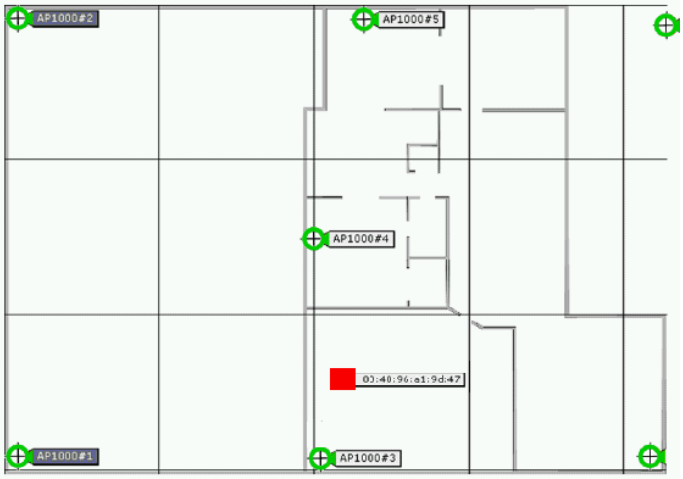


Figura 3.2.b Ejemplo de localización de dispositivos móviles en celdas. El dispositivo identificado con la MAC address 00:40:96:A1:9D:47 se encuentra señalizado en rojo.

El uso de esta técnica permite incrementar la probabilidad de seleccionar la verdadera "celda mas cercana". Si la necesidad que se tiene es de una localización no muy precisa, el uso de esta técnica es más que suficiente para proveer una localización certera del dispositivo móvil.

3.3 Técnicas basadas en distancias

3.3.1 Tiempo de llegada (ToA)

Los sistemas ToA están basados en la medida de tiempo exacta que tarda una señal transmitida desde un dispositivo móvil hacia varios sensores receptores. El principio de esta técnica radica en que las señales viajan a una velocidad conocida (usualmente a la velocidad de la luz o sino alrededor de 300 metros por microsegundo). Por lo que la distancia entre el dispositivo móvil y cada sensor receptor puede ser determinada por el tiempo que pasó entre la propagación de la señal entre ellos.

El uso de esta técnica requiere un conocimiento preciso de los tiempos de inicio de la transmisión así como también de la correcta sincronización de tiempos de los dispositivos móviles y los sensores receptores.

Conociendo tanto la velocidad de propagación como el tiempo medido, es posible calcular la distancia ρ entre el dispositivo móvil y el receptor:

$\rho = c\ (t)$

donde ρ: distancia (metros)
c: velocidad de la luz (metros/ microsegundos)
t: tiempo (microsegundos)

Si la distancia ρ se usa como radio, se puede representar un área circular alrededor del sensor receptor, en donde tiene que encontrarse el dispositivo móvil (con un alto grado de probabilidad).

Cuando la información del ToA, de 2 sensores pueden dar un resultado de la ubicación de un dispositivo móvil, con un grado de probabilidad igual para ambos. Se recomienda utilizar un tercer sensor para obtener una respuesta más exacta de la ubicación del dispositivo móvil, tal como se muestra en la siguiente figura

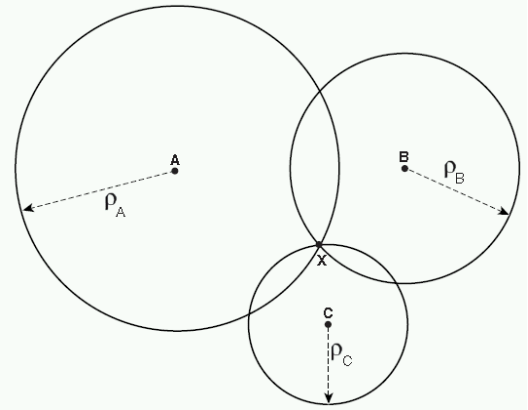


Figura 3.3.a Ubicación de un dispositivo móvil mediante la información de ToA

Para éste caso en particular de los tres sensores, la cantidad de tiempo que le toma al mensaje transmitido desde la estación móvil X para llegar a los sensores A, B y C es medida mediante t_A, t_B y t_C. Al tomar la velocidad c, como la velocidad de la luz, se pueden calcular las distancias ρ_A, ρ_B y ρ_C. Cada distancia permite hacer una circunferencia alrededor de cada uno de los sensores. Posteriormente al analizar cada una de las circunferencias se puede concluir que la intersección de todas ellas es el punto donde se sitúa el dispositivo móvil. Algunas veces puede haber mas de una posible solución al punto de ubicación, por lo que no es suficiente solo 3 sensores sino que se necesitan mas, en dicho caso se habla de un ToA múltiple.

Las técnicas del ToA se pueden emplear tanto para resolver locaciones bidimensionales como para resolver tridimensionales también, en donde ya no serian planos con circunferencias sino más bien esferas.

3.3.2 Diferencia en el tiempo de llegada (TDoA)

La técnica de TDoA utiliza un tiempo relativo para medir en cada sensor receptor y compararlo contra una medida de un tiempo absoluto. Debido a esto el TDoA no necesita de una sincronización entre los dispositivos móviles y los sensores.

TDoA es comúnmente implementado mediante un proceso de *hyperbolic lateration*. En esta técnica al menos tres sensores receptores de tiempo sincronizado A, B y C se necesitan. En la siguiente figura, se asume que un móvil X transmite un mensaje el cual llega a un sensor A con tiempo T_A y al sensor B con tiempo T_B. Al calcular la diferencia del tiempo de llegada del mensaje entre las locaciones de los sensores A y B, el resultado es un constante positva k:

$TDoA_{B\text{-}A} = | T_B - T_A | = k$

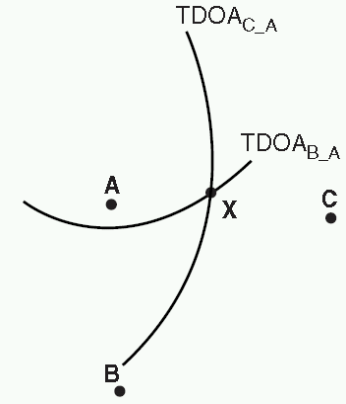


Figura 3.3.b técnica de Hyperbolic lateration

Se puede utilizar el valor de $TDoA_{B-A}$ para construir una hipérbola con las locaciones de los dos sensores de recepción A y B. En dicha hipérbola se representan todas las posibles locaciones del dispositivo móvil X:
$| D_{XB} - D_{XA} | = k(c)$
La localización mas probable del punto X se puede representar como un punto a lo largo de la hipérbola. Para lograr un dato mas preciso acerca de la localización del punto X, se utiliza un tercer sensor en la localidad C para calcular la diferencia de tiempo del mensaje de llegada entre los sensores A y C:
$TDoA_{C-A} = | T_C - T_A | = k_1$

Conociendo el valor de la constante k_1 se puede trazar una segunda hipérbola, la cual representaría la diferencia entre las dos distancias (sensores A y C)

Un cuarto sensor se puede crear y también una tercera hipérbola para implementar una *hyperbolic lateration.* Esto solo en el caso en el cual hayan mas de dos posibles soluciones a la hora de utilizar TDoA con tres sensores.

Las tecnologías tanto de TDoA como de ToA son altamente eficientes en cuanto a detección y posicionamiento en ambientes exteriores e interiores se refiere. A tal punto que son utilizados en aeropuertos, puertos marítimos, anfiteatros y estadios. A tal punto que ya se empiezan a fabricar tecnologías de WLAN que intengran TDoA, tales como los AP 802.11/TDoA (algunos de ellos ya bajo estándares normados tales como: ANSI INCITS 371.1/ISO24370)

3.4 Fuerza de la señal recibida (RSS)

Hasta el momento se han considerado las opciones en las que se usa el tiempo para medir distancias (TDoA y ToA). Sin embargo también es posible calcular la posición mediante la fuerza de la señal recibida (*Received Signal Strength* por sus siglas en ingles).

Mediante esta técnica la señal se puede medir ya sea en el dispositivo móvil o en el sensor receptor.

Conociendo la potencia de salida del transmisor, perdidas en cables y ganancia de antenas, asi como el modelo de perdidas del sistema se puede determinar cual es la distancia que separa los 2 dispositivos, mediante la siguiente ecuación:

$RX_{PWR} = TX_{PWR} - Loss_{TX} + Gain_{TX} - PL + Gain_{RX} - Loss_{RX}$

Al sustituir las pérdidas directamente resolver la distancia (D) mediante la formula:

$$D = \sqrt[n]{inv \log \frac{RX_{PWR} - TX_{PWR} + Loss_{TX} - S + Loss_{RX} - Gain_{RX}}{-10}}$$

Donde:
Rx_{PWR} representa la fuerza de la señal recibida en dB
Tx_{PWR} representa la potencia de salida del transmisor en dB
$Loss_{TX}$ representa la suma de las perdidas de todos los cables y conectores del lado del transmisor en dB
$Gain_{TX}$ representa la ganancia de la antena del transmisor en dB
$Loss_{RX}$ representa la suma de las perdidas de todos los cables y conectores del lado del receptor en dB
$Gain_{RX}$ representa la ganancia de la antena del receptor en dB

La información acerca de la fuerza de la señal utilizada para determinar la posición se puede obtener de dos formas. Una de ellas se da cuando la infraestructura de red reporta la fuerza de la señal recibida hacia el dispositivo móvil. La otra forma se da cuando el dispositivo móvil reporta la fuerza de su señal hacia la infraestructura de red.

3.5 Técnicas basadas en ángulos

La técnica del ángulo de llegada (AoA por sus siglas en ingles) o denominada también como dirección de llegada (DoA), localiza la estación móvil determinando cual es el ángulo de incidencia con el que la señal llega hacia el sensor receptor.

Debido al funcionar de esta técnica se pueden emplear relaciones geométricas para estimar la localización de la intersección de dos líneas de rodamiento (LoB) formadas por una línea radial hacia cada sensor receptor, tal como se ilustra en la siguiente figura.

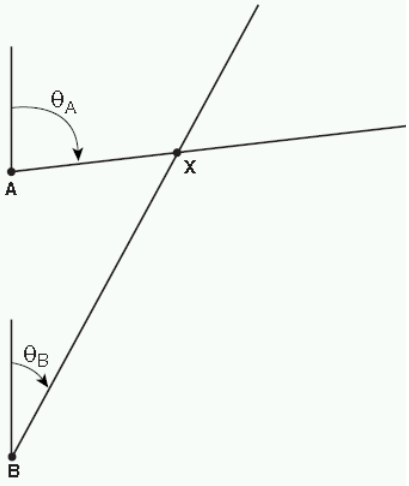


Figura 3.5.a localización mediante intersección de líneas

En un plano bidimensional, se requieren al menos dos sensores para poder determinar la ubicación con un grado de certeza apropiado, viniendo de al menos 3 o mas sensores receptores para poder hacer una triangulación.

Este tipo de técnica ha sido muy empleada en sistemas celulares para proveer servicios de localización, donde múltiples torres calculan el AoA de la señal del usuario móvil con el propósito de realizar inmediatamente después una triangulación. Tal como puede apreciarse en la siguiente figura.

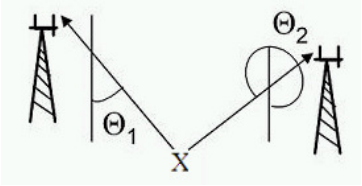


Figura 3.5.b Localización mediante AoA

Si un terminal que transmite una señal está en la línea de vista directa (LOS, Line Of Sight), la antena *multiarray* puede determinar de qué dirección viene la señal. Para conocer la posición del terminal es necesaria al menos una segunda estimación procedente de otra estación base con la misma tecnología que la primera. La segunda estación base localizará al terminal y comparará sus datos con los de la primera estación para después calcular la posición del usuario mediante trigonometría. En principio sólo son necesarias dos estaciones base para estimar la posición del terminal móvil

3.6 Consideraciones de los tags

Los *tags* que se utilizan para la interoparitividad entre ambas tecnologías tienen características especiales. La primera es que deben de ser activos. Además deben de cumplir con un estándar, el de las redes WiFi u 802.11 y por ende trabajar en las mismas frecuencias que las redes *wireless*.

3.6.1 Tecnología del Tag

Los *transponders* activos se pueden sub-categorizar en los que funcionan como *transponders* y los que funcionan como indicadores. Son de interés especial los *tags* activos que funcionan en bandas de ISM sin licencias y siguen los protocolos de IEEE 802.11. es por tal razón que a estos tags se les conoce como *RFID 802.11 tags* o *RFID WiFi tags*.

3.6.1.1 Tags activos de RFID 802.11

Los *tags* activos *802.11 (Wi-Fi) RFID* son diseñados para operar en las bandas ISM 2,450 – 2,483.5 GHz (según el espectro radioeléctrico de SIGET para la region dos para el reglamento de radiocomunicaciones de la UIT, el cual contempla su uso para radiolocalización entre otros, ver anexos). Estos *tags* conservan las características de los *tags* activos. Los *Wi-Fi RFID tags* pueden comunicarse directamente con una infraestructura estándar de Wi-Fi sin ningún hardware especial o modificaciones de *firmware* logrando así coexistir al lado de instrumentos Wi-Fi, tales como computadoras portátiles, teléfonos inalámbricos de voz sobre IP y otros equipos.

Figura 3.6.a Tags activos compatibles con WiFi (fuente: RFID Journal)

3.7 Distintas compañías que fabrican soluciones WiFi-RFID

Debido al gran potencial de la interoperatividad entre los sistemas de redes inalámbricos WiFi y al auge de los sistemas RFID para procesos de identificación, algunas compañías multinacionales de gran renombre, como Hitachi y Cisco, se han dado a la tarea de incorporar en sus equipos de redes compatibilidad para la detección de *tags* RFID y además de fabricar *tags* compatibles con el estándar IEEE 802.11 de las redes WiFi mas comunes.

3.7.1 Hitachi

Fue la primera compañía en sacar al mercado el localizador RFID WiFi[6]. Dicho localizador fue denominado *Airlocation II Tag-w*, el cual consistió en una etiqueta RFID para redes locales inalámbricas de detección de posición y gestión de la entrada y salida de personas en edificios. El dispositivo presentó también una función de mensajes de emergencia.

Las funciones combinadas del *tag* permiten la gestión precisa de personas que entran en el edifico e información sobre su localización exacta una vez esté dentro del edificio. En caso de emergencia, la función de mensajería de emergencia permite a los usuarios enviar un mensaje al centro de control e informar automáticamente al personal de emergencia acerca de su situación.

El costo inicial de estos *tags* fue de US $178[7] por unidad y salió a la venta en octubre del 2006. Este *tag* permite localizar con grado de precisión que va de 1 a 3 metros. Además su rango de lectura ha sido optimizado para trabajar hasta 50 metros en interiores y 200 metros en exteriores.

3.7.2 G2 Microsystems INC

Esta compañía se ha dado a la tarea fabricar *tags* que sean compatibles con la tecnología inalámbrica para redes WLAN. El enfoque que propone dicha compañía se basa en la reducción de costos (de hasta un 75%)[8], para la implementación de sistemas RFID en entornos don de se disponga de infraestructura WiFi.

El chip diseñado por dicha compañía es denominado G2C501, el cual aparte de ser leído por cualquier *access point*, puede también ser leído a través de Internet. Y ofrece la ventaja de un consumo bastante reducido de energía, el cual puede alargar su vida útil hasta cinco años, con reportes de lectura de hasta 40 segundos promedio con únicamente dos baterías AA. En la actualidad dicho chip tiene un valor cercano a los US $12 si es pedido en volúmenes grandes (según su sitio web en diciembre del 2007).

[6] Según www.rfid-spain.com, en su articulo titulado: Hitachi lanza el primer localizador RFID WiFi para el control de presencia y gestión de emergencias en edificios, en 03/10/2006
[7] Según http://www.engadget.com/2006/10/02/hitachis-employee-tracking-airlocation-ii-tag-w-wifi-enabled-rf/ y http://www.tmcnet.com/usubmit/2006/10/02/1945242.htm
[8] http://www.cbronline.com/article_news.asp?guid=936848EC-6412-4A6A-B71D-76F99C0C9E3F

3.7.3 Ekahau

Ekahau es una empresa que se ha dedicado a proveer soluciones de localización basadas en WiFi. Tal fin la ha llevado a diseñar etiquetas de RFID compatibles con WiFi. Dichos tags forman parte de las familias T201 y T301x.

Los tags T301-A, para activos, incorporan un sensor inteligente de movimiento, el cual es capaz de detectar cuando el *tag* se encuentra en movimiento o se ha colocado en una nueva locación y es mandar un alerta cuando eso sucede. Además dicha transmisión de datos consume un ancho de banda bajo. Además se puede ver el nivel de carga de las baterías y su configuración y datos internos remotamente a través de la WLAN.

Los *tags* T301-B son de baterías recargables, en forma de tarjeta de crédito, ideal para el rastreo de empleados. Además tiene un sensor y un botón que permite ser activado en casos de emergencia, incorpora una mini pantalla capaz de desplegar mensajes entrantes de texto.

Además de los *tags* esta compañía provee soluciones a nivel de software para la localización de los *tags* en las redes WLAN, así como *modems* y otros dispositivos relacionados con WiFi.

3.7.4 Pango

Otro fabricante de este tipo de *tags* es la empresa PanGo la cual paso a formar parte del grupo innerwireless. PanGO ofrece un *tag* denominado PanGO 802.11 V3. Dicho *transponder* forma parte de la solución de rastreo basada en WiFi de PanGO. Dicha solución esta compuesta de 4 componentes: una infraestructura de localización 802.11 Wi-Fi, PanGo Platform, PanGo Vision y los *tags* V3.

El diseño del *tag* ha sido pensado en la optimización del consumo de energía. El tiempo de vida estima de sus 2 baterías AA es de mas de 5 años. Posee además un botón de alerta y un sensor que detecta si el *tag* ha sido removido del activo al cual fue implantado y así poder enviar una alarma al sistema. Ofrece la ventaja que no necesita un protocolo particular para su funcionamiento, ya que la empresa asegura que su *tag* puede operar con cualquier AP que haya sido instalado anteriormente.[9]

3.7.5 Cisco

Cisco es otra de las compañías que mostró interés en la interoperatividad de redes WLAN con el mundo RFID. Sin embargo su incursión en el mundo de RFID fue mucho después,

[9] http://www.innerwireless.com/vision-tag.asp

en febrero del 2007. Su incursión fue de la mano en el aspecto de marketing con la empresa Aeroscout (empresa que se dedica exclusivamente al desarrollo de soluciones RFID combinadas con WiFi), para crear un sistema que utiliza *tags* activos de RFID bajo el estándar de IEE 802.11 de redes inalámbricas. El sistema que han desarrollado ambas compañías consiste en la localización en tiempo real.

La solución de localización fue formalmente anunciada en la feria RFID-ROI del 2007 en Londres. Dicho sistema utiliza los puntos de acceso bajo los estándares 802.11b y 802.11g. El sistema esta compuesto por los *tags* activos de RFID con código propietario de Aeroscout y por la serie 2700 *Wireless Location Appliance* de Cisco. Esta última permite calcular la posición del *tag* basada en la fuerza de la señal. Pero también se incorporan otros equipos de infraestructura inalámbricos de Cisco y un software de Aeroscout denominado *MobileView*.

El enfoque de ambas compañías se centra en resaltar las bondades de la interoperatividad, "a diferencia de la tecnología RFID típica, nuestro sistema utiliza un *access point* inalámbrico como *reader*", Josh Slobin director de marketing de Aeroscout.

El área en la cual han estas dos compañías han focalizado su accionar es en el sector industrial (aeroespacial, minería, automotriz y manufactura de semiconductores). Y mas recientemente el enfoque a sido orientado al sector salud donde utilizan equipos Philips para poder brindar una tecnología de solución en tiempo real (RTLS: *real time location system*).

3.8 Ejemplo de una aplicación especifica de interoperatividad: RFID & WiFi

Debido a que las aplicaciones inalámbricas tienen la ventaja de proveer flexibilidad y libertad de movilidad (conectarse a Internet al mismo tiempo que se toma un café fuera de su oficina hasta revisar el correo desde el celular), las redes *wireless* han tenido un gran auge en los últimos años. Sin embargo esto conlleva también a tomar medidas en cuanto a seguridad y administración de las redes. Este es uno de los motivos por los cuales se vuelve importante la localización de los activos dentro de la red de la empresa, ya que permite de manera visual poder tener el control de las redes WLANs. Bajo dicha premisa aparece el sistema *RF Fingerprinting* de Cisco.

Esta tecnología permite determinar la localización de un cliente *wireless*, con una precisión de un par de metros, mediante lo correlación de ciertas características propias de la radio frecuencia. Esto permite construir una aplicación de localización de usuarios en

tiempo real así como su información. De tal forma que "*RF Fingerprinting* puede permitir rastrear miles de clientes inalámbricos simultáneos"[10]

3.8.1 Arquitectura de servicios de CISCO basados en localización.

Tradicionalmente ha habido dos arquitecturas de sistemas para rastrear la localización en redes WiFi: el AP más cercano y la triangulación. Pero en la actualidad hay una tercera tecnología que permite, de una manera más precisa (escasos metros de distancia) poder descubrir la localización, el cual es el sistema *RF Fingerprinting* de Cisco.

El sistema que se basa en al AP mas cercano, funciona mediante el envió de una pregunta a la red para encontrar a un cliente de la red en base a su dirección MAC. Si se tiene en cuenta que los protocolos 802.11b/g tienen una cobertura de 100 metros, se puede deducir que el cliente que se pretenda localizar estará en un área cuadrada de 100 metros. Lo cual hace que dicho método no sea una técnica viable para la localización precisa de un cliente en una red inalámbrica.

El sistema basado en triangulación la pregunta de ubicación llega a todos los AP de la red y cada AP que encuentre la señal del cliente responderá hacia el sistema con que fuerza de señal lo ha encontrado. De tal forma que se puede hacer una aproximación mas certera que con el primer método.

Sin embargo, el sistema de rastreo para localización *RF Fingerprinting*, no solo toma en cuenta estos dos métodos. Sino que además incluye un método de reflexión, el cual se da cuando una onda de radio frecuencia se refleja en un objeto. Incluye también el método de atenuación, el cual mide el efecto físico que tiene un objeto sobre una señal de RF. Y como ultimo elemento, *RF Fingerprinting* incluye múltiples caminos, es decir que cuando se manda una señal de radio frecuencia, ésta puede tomar varios caminos antes de llegar a su destino final.

3.8.1.1 Bondades del sistema RF Fingerprinting

Cisco *RF Fingerprinting* es un acercamiento a un nuevo e innovador método que mejora significativamente la exactitud y precisión de las técnicas tradicionales de localización en base a la fuerza de señales. Además ofrece la simplicidad de una alteración del método de localización basado en RSSI, con un potencial de calibración personalizado para requisitos particulares y el funcionamiento interno previamente disponible para aplicaciones de localización.

[10] Allan Thompson, Technical Lead at Cisco for the Wireless networking business unit

Dicho sistema también ofrece la capacidad de calibrar un modelo de RF a un ambiente particular en una manera similar a (pero sin muchos procedimientos) los descritos para modelar de la localización.

Cisco *RF Fingerprinting* realza perceptiblemente la fuerza de señal recibida para la localización, usando los modelos de propagación de RF ya desarrollados de los datos de radio de propagación recopilados directamente del medio que la contiene o de medios similares a donde se encuentre la señal.

Sin embargo, a diferencia de los modelos de localización, no se requiere siempre una calibración única, especialmente en las situaciones donde hay pisos múltiples de similar construcción, contenido y disposición desplegada. En estos casos un modelo de RF común puede ser aplicado y esta es la razón por la que varios modelos conocidos de RF para ambientes de oficina (es decir, solamente oficinas con divisiones de tabla yeso o tabla roca (*Drywall*) y las oficinas *Drywall* combinadas) se prediseñan para una solución del Cisco LBS.

Estos modelos prediseñados permiten el despliegue con menos calibración en ambientes comunes de oficina, que es significativamente ventajoso sobre los modelados de localización existentes, especialmente en casos donde el despliegue rápido y sencillo es de fundamental.

Además del uso de los modelos pre-diseñados de propagación, Cisco *RF Fingerprinting* ofrece la capacidad de desarrollar un modelo modificado para requisitos particulares de propagación que mejore los modelos basados en fallas por perdida de trayectoria, en el sitio y en la fase de calibración.

Este proceso permite que las características totales de atenuación del ambiente real puedan ser tomadas en consideración durante el cálculo los exponentes de la pérdida de trayectoria de 2.4 GHz y de 5 GHz.

Para cada calibración de localización por cuadrante, la calibración de las coordenadas de la localización física del cliente (proporcionado por el operador de la calibración) se registra junto con la información de la fuerza de señal recibida del cliente a partir de tres o más puntos de acceso LWAPP[11]-*enabled*. Se realiza esto hasta que 150 medidas del punto de acceso para localización se registren por banda, a partir de 50 localizaciones distintas en el ambiente donde es desplegado el sistema.

Los datos acumulados durante la fase de la calibración se procesan y se preparan, después se utilizan estadísticas para construir un modelo de propagación de RF donde el

[11] Lightweight Access Point Protocol o Protocolo Ligero para Puntos de Acceso es un protocolo utilizado para la gestión centralizada de varios puntos de acceso en una red inalámbrica.

exponente de la pérdida de trayectoria y los valores del PL1meter se calculan de los datos de la calibración de la muestra para reflejar mejor las anomalías específicas de propagación (tales como atenuación) que están presentes en el ambiente. Este proceso consiste en varios ciclos de cómputo donde los parámetros mencionados previamente se calculan para cada banda. La técnica de estimación del error medio cuadrático (MMSE) se utiliza para obtener los valores iniciales para los parámetros, donde el exponente de la pérdida de trayectoria es representado por la pendiente de la línea aplicable del mejor ajuste de el MMSE (es decir, defecto o ajuste corregido). Sin embargo, se puede observar que en la aproximación del *RF fingerprinting* de Cisco, la selección del modelo de pérdida de trayectoria no se limita al MMSE. Mas bien, MMSE se utiliza solamente como el punto de partida para la selección de los parámetros concluidos para cada banda, siendo el objetivo la optimización del modelo de pérdida de trayectoria, como si perteneciese a la exactitud de localización en vez de simplemente obtener el mejor MMSE, para completar los datos de la calibración.

Para localizar a un cliente móvil durante la fase operacional del *RF Fingerprinting*, la localización de la RSS se realiza usando un modelo de RF por defecto o un modelo modificado para requisitos particulares creado durante la fase de la calibración. Este proceso proporciona localización donde existe la probabilidad más alta de la residencia del cliente. La información adicional recabada del análisis estadístico de la distribución de los datos de la calibración entonces se utiliza para mejorar la exactitud de la localización a mayores distancias.

El *RF Fingerprinting* ofrece varias ventajas de aproximación tradicionales:

- Las aplicaciones existentes de *LWAPP-enabled Cisco Unified Networking Components* difieren un poco con otras soluciones, Cisco LBS con *RF fingerprinting* es 100%, Wi-Fi RTLS sin la necesidad de los receptores especializados basados en tiempo o de otro hardware especializado. La aplicación de localización de Cisco se agrega a la localización de soporte, al historial de estadísticas y sirve como motor de colocación centralizada para seguir simultáneamente hasta 2500 dispositivos por la aplicación.

- Ningún hardware o software requiere un cliente propietario, la solución LBS de *Cisco RF Fingerprinting-based* se pone en ejecución como un modelo no del lado del cliente sino del lado de la red. Debido a esto, *RF Fingerprinting* puede proporcionar la localización para una gran variedad de estándares de distancias en la industria de clientes Wi-Fi (no precisamente para WinXP/2000/PPC) sin la necesidad de cargar a cada cliente con *software propietarios de rastreo de cliente* o *drivers wireless*. Esto incluye los populares teléfonos de VoIP tales como el Cisco 7920 entre otros.

- El soporte común de *tags* activos de RFID bajo una plataforma Wi-Fi, para rastreo de bienes de gran valor.

La solución de Cisco LBS implementa el *RF fingerprinting* como modelo del lado de Red, este no depende de un software propietario o no depende del fabricante de *tags* activos de RFID. Esto permite a la solución de Cisco LBS la interoperatividad con los *tags* activos de RFID de vendedores populares, incluyendo las redes de AeroScout y PanGo. Cisco también posibilita una especificación completa del *tag* de RFID para los socios de la tecnología de Cisco y anima al desarrollo del hardware activo para interoperatividad del *tag* de RFID. La solución de Cisco LBS es capaz de seguir otros *tags* activos de RFID a través de la red Wi-Fi para poder configurar, autenticar y asociar la infraestructura centralizada Cisco instalada subyacente de WLAN como un cliente de WLAN.

3.8.2 Funcionamiento de la solución de Cisco

Los AP utilizan la tecnología de *RF Fingerprinting* para recolectar información perteneciente a la topología RF, mediante la creación de celdas que permitan identificar cada uno de los distintos aspectos geográficos del lugar (ya sea un edificio, una bodega, una casa, etc.) y la ubicación de los AP. Un punto en la celda puede llegar a medir medio pie. Para determinar la radio frecuencia de cada punto de la celda, un sistema de administración de WLAN debe de primero predecir como las señales de RF van a interactuar con el lugar.

De tal forma que el sistema de administración crea un mapa detallado comparable al de una huella dactilar (de ahí el nombre de *fingerprinting*) donde se observa toda la información de la topología de RF y los datos de RF obtenidos mediante la traza de rayos de cada *access point* en la red para cada reflexión y caminos múltiples obtenidos para cada destino. Tal como se muestra en la figura 3.8.a. La predicción que involucra *RF fingerprinting* toma en cuenta la atenuación y reflexión, tanto de paredes como de cualquier otro objeto dentro del edificio. El sistema de administración de WLAN crea una base de datos de coordenadas, grabando como cada AP ve cada señal desde un punto de vista de fuerzas de señales.

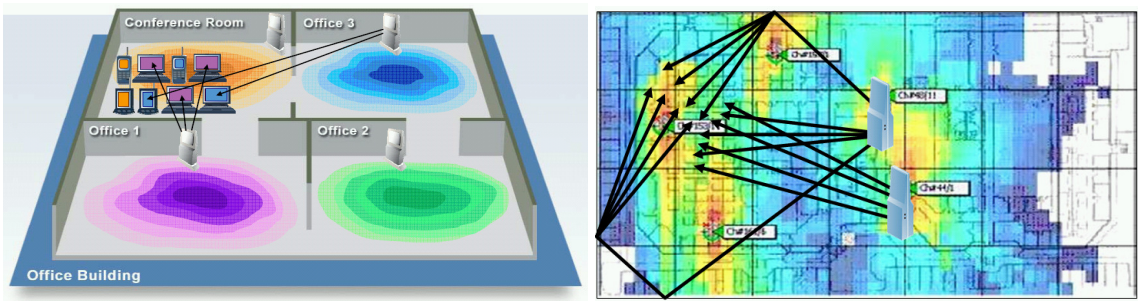


Figura 3.8.a Diagramas en los que se representa la fuerza de señal de cada AP en un edificio de oficinas asi como las trazas de rayos de cada AP (fuente imagen: Cisco).

Posteriormente el sistema de administración de WLAN cruza las referencias del cliente inalámbrico obtenidas, por medio de los APs, en tiempo real, con la topología de RF almacenada en el sistema para poder hacer un rastreo preciso y confiable.

La arquitectura total de la solución del Cisco LBS se puede considerar en el siguiente esquema. Los puntos de acceso transmiten a la información relacionada a la fuerza de señal detectada de cualquier cliente Wi-Fi a los controladores de la red WLAN, tag activo de RFID de 802.11, puntos de acceso, o a otros clientes. En operación normal, los puntos de acceso se centran en actividades de recolección de información en su canal primario de operación, cuando un canal es desactivado, la exploración de otros canales en los canales de regulación de un Access Point es llevada a cabo periódicamente. La información recogida se remite al controlador de la red WLAN en el cual el Acces Point se actualiza. Cada controlador maneja y agrega toda tal información de la fuerza de la señal que recibe de sus puntos de accesos. La aplicación de localización utiliza el SNMP para desactivar "dejar caer" cada regulador para la información más última para cada la categoría continua de dispositivos.

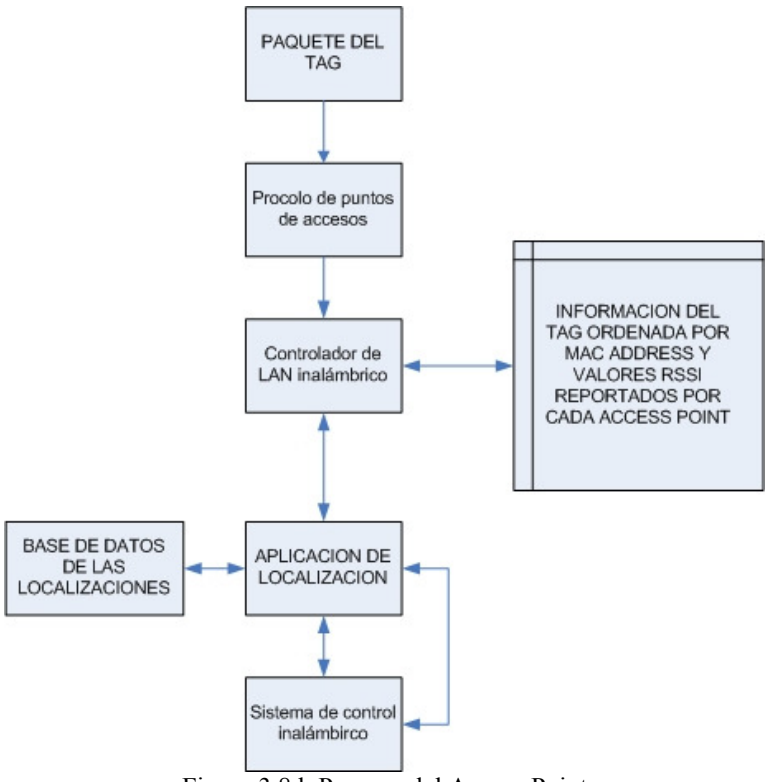


Figura 3.8.b Proceso del Access Point

En la figura anterior se pueden recapitular los siguientes acontecimientos:

1. Por lo menos 3 (y preferiblemente 4 o 5) *access point* detectan las transmisiones del *tag*. La transmisión es *multicast* y además reenviada hacia el controlador de

WLAN (WLC) en el cual el *access point* detector se encuentra conectado y registrado.

2. Para cada AP registrado el WLC también coloca la siguiente información del tag en una tabla interna:
- *tag* MAC *address*
- AP MAC *address*
- Interfaz AP
- Medidas RSSI

3. El WLC almacena la información referente al estado de la batería asociado con el *tag* en una tabla interna indexada mediante la MAC *address* del *tag*.

4. El servidor de localización periódicamente envía una serie de datos al WLC para ver los contenidos de las tablas del tag utilizando el protocolo SNMP.

5. El servidor de localización calcula la localización del tag usando la información RSSI contenida en las respuestas SNMP y almacena la información actualizada en la base de datos del servidor.

6. El servidor de localización despacha cualquier notificación de eventos basados en la actualización de la posición del *tag* hacia los destinatarios de las notificaciones.

La aplicación de localización y el WCS intercambian información acerca de la calibración de los mapas y diseños de redes durante un proceso conocido como sincronización. Durante una sincronización del diseño de red entre el WCS y la aplicación de localización, los *up-to-date* actualizan los datos acerca del diseño y la calibración de aquellos que están *out-to-date*. La aplicación de localización se sincroniza con cada controlador que contenga puntos de acceso participando en la localización durante la sincronización del controlador. La sincronización se da ya sea por una petición o porque fue planificada

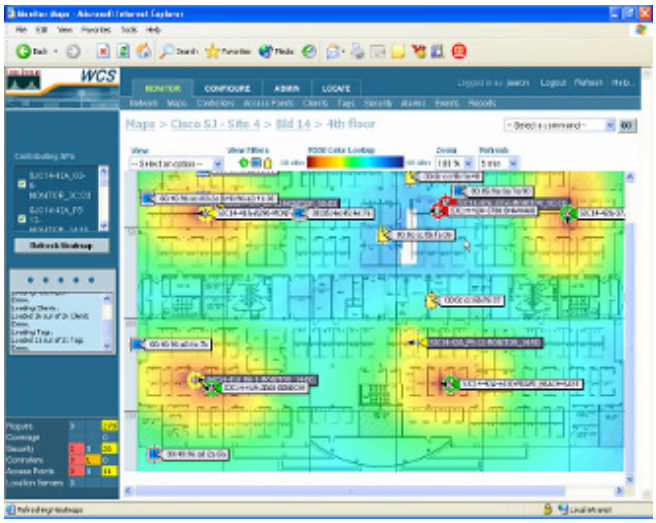


Figura 3.8.c Muestra en detalle la vista de las señales da cada AP y los dispositivos localizados por el sistema (fuente imagen: Cisco).

3.9 Comparación de las soluciones RFID WiFi

El siguiente cuadro resumen muestra la información necesaria para poder implementar una solución RFID que opere con la red WLAN nueva o ya instalada.

			protocolos de compatibilidad WLAN	
fabricante	**tipo de tag**	**compatible con culaquier AP**	**802.11g**	**802.11b**
Hitachi	activo	Si	si	no
Cisco	activo	No	si	No
G2	activo	Si	si	no
PanGO	activo	Si	si	no

La tabla anterior muestra que la mayoría de los fabricantes de *tags* WiFi-RFID apuntan a una tecnología estándar que permita una compatibilidad con cualquier marca hardware, en el protocolo 802.11g el cual es el mas utilizado en los dispositivos portátiles actuales (laptops, PDAs, etc.).

3.10 Redes WiFi implementadas en El Salvador

En la actualidad en El Salvador existen una gran variedad de empresas que implementan en sus sistemas de red la tecnología WiFi. Esto conlleva a una inversión considerable adicional a la red LAN instalada, por tal motivo la inversión en otro sistema tal como el

RFID incrementaría considerablemente el gasto en la infraestructura para manejo de información de datos en la red. Es por esto que la interoperatividad juega un factor importante en el desarrollo de una solución basada en RFID, porque permite utilizar los recursos de red WLAN ya instalados y evita así el costo de equipos adicionales, tales como los *readers* de RFID.

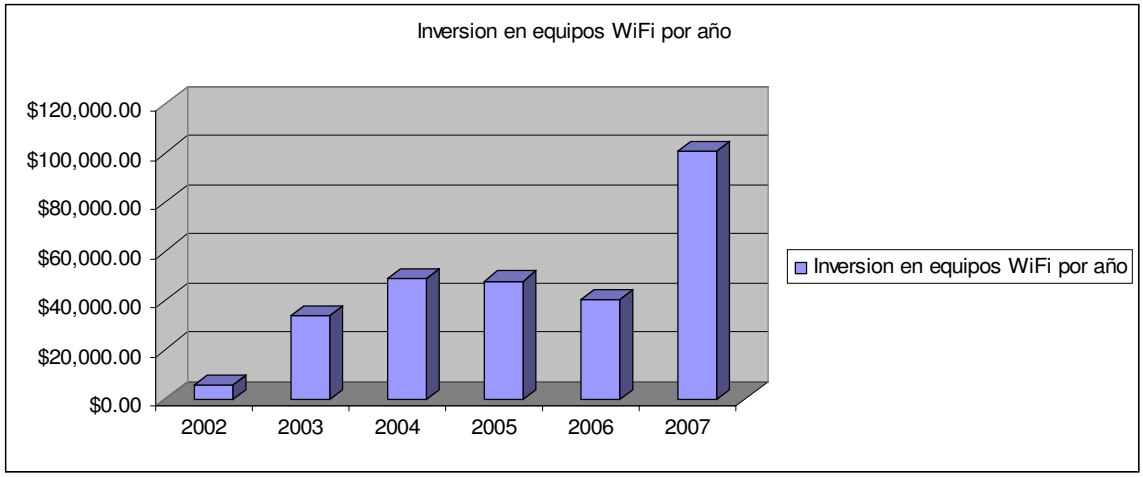
En el siguiente cuadro se muestran las compañías que han invertido en equipos de red inalámbricos (marca Cisco) en El país a través de un distribuidor autorizado, a manera de ejemplificar con cifras la tendencia en equipos de WiFi en nuestro país.

Años	Empresas		Inversión	
2002	Banco de Comercio			$4,731.00
	Textiles Lourdes (Fruit of the loom)			$1,099.37
	Total	**2**	**Total**	**$5,830.37**
2003	Banco de Comercio			$4,456.00
	IPSFA			$534.27
	Textiles Lourdes (Fruit of the loom)			$7,020.92
	Central Azucarera Izalco			$2,036.20
	Banco de Comercio			$15,583.20
	Credomatic (BAC)			$865.00
	Textiles Lourdes (FOTL)			$1,740.00
	Agrisal			$1,356.00
	Total	**8**	**Total**	**$33,591.59**
2004	Glaxo Smithkline			$550.00
	3M			$2,519.00
	SICA			$2,301.00
	Telecom			$36,681.57
	Banco de Comercio			$4,790.00
	General de Equipos			$2,024.00
	Total	**6**	**Total**	**$48,865.57**
2005	Banco de Comercio			$11,496.00
	BAC			$958.00
	Diszasa			$1,918.00
	Banco Agrícola			$2,800.98
	AIG			$2,371.20
	Iglesia Mormona			$13,472.06
	Banco Salvadoreño			$14,937.72
	Total	**7**	**Total**	**$47,953.96**
2006	Loteria Nacional			$8,952.21
	Duke Energy			$2,402.76
	Ministerio de Relaciones Exteriores			$4,268.56
	Walmart			$5,536.20
	Scotiabank			$5,138.50
	Banco Cuscatlan			$12,184.00

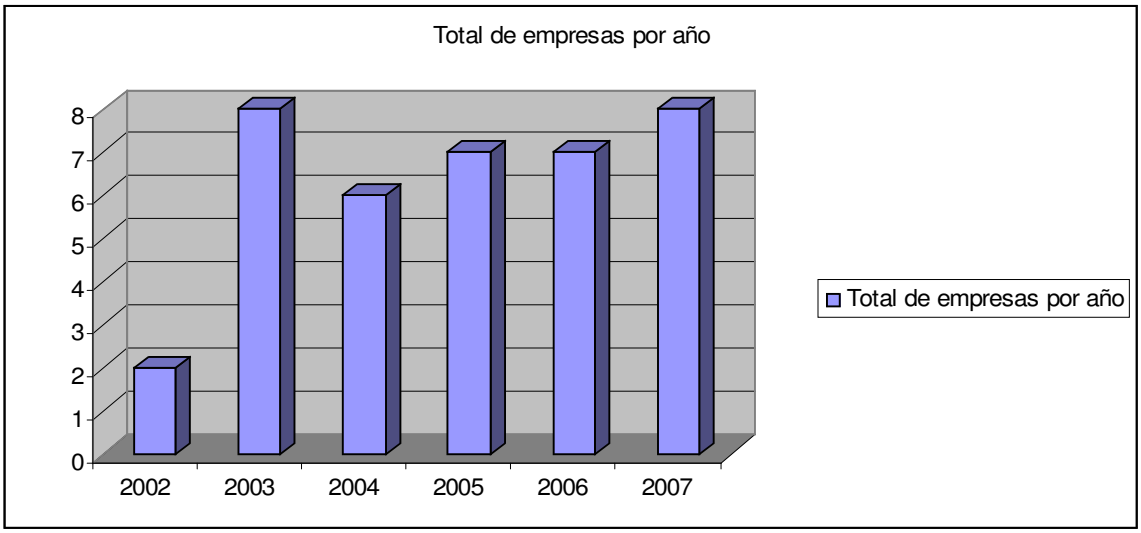
	Kimberly Clark			$1,745.34
	Total	**7**	**Total**	**$40,227.57**
2007	Phillips			$1,213.00
	Banco Salvadoreño			$2,887.12
	BMI			$2,973.94
	Walmart			$3,138.50
	Fruit of the loom			$5,693.00
	AES			$12,345.00
	Ministerio de Hacienda			$37,045.00
	TACA			$35,456.00
	Total	**8**	**Total**	**$100,751.56**

Tabla de montos de inversión en equipos WiFi en El Salvador (fuente: GBM, El Salvador)

De la tabla anterior se puede concluir que la inversión en equipos WiFi ha tenido un incremento a partir del año 2002 hasta la fecha, habiendo un despunte sobre todo en el año 2007 en cuanto al total invertido. Tal como se muestra en el grafico siguiente.



En la grafica siguiente se muestra la tendencia en cuanto al numero de empresas que invierten en tecnología WiFi por año.



Con el objetivo de disminuir los gastos de implementación en un sistema RFID, una empresa podría ver muy atractiva la posibilidad de poder trabajar con sus equipos WiFi ya instalados. Dado esto, se puede afirmar que la inserción de tecnología RFID-WiFi no es una idea lejana, ya que esta puede optimizar los recursos de la red WiFi.

CAPITULO 4: Estudio de mercado

En el siguiente capitulo se tratará sobre criterios económicos a tomar en consideración para la implementación de un sistema RFID-WiFi, en empresas que posean un alto valor de activos, enfocándose únicamente en inversión para implementación del mismo.

4.1 Análisis de la situación

Dentro del análisis cabe destacar que en reseña histórica se hace mención al capitulo 1.1 y 1.2 en el cual se trata extensamente la historia y evolución de los métodos de identificación, a la vez cabe aclarar que para el siguiente análisis no se tomaran en cuenta regulaciones legales al tema, ya que éstas como tales no son una documentación abierta al publico en nuestro país.

4.1.1 Premisas y perspectivas

Las soluciones basadas en RFID, se estiman que serán ampliamente aceptadas y asimiladas por y para el desarrollo de la empresa a la cual aplique.

Estas aplicaciones poseen claras características distintivas y únicas, que generarán un importante valor agregado a la empresa en la cual se implemente, incidiendo en los siguientes puntos:

- Optimización de procesos que influyen directamente en seguridad de los activos y de los productos circulantes en la empresa, en caso que hubieran.
- Fortalecimiento del principio de mejora continúa.
- Ayudar a cumplir eficientemente tareas de inventario y/o registro.
- Ágil trazabilidad de la información.
- Optimización de tiempos de operación y errores humanos.

4.1.2 Relevamiento del medio externo

4.1.2.1 Análisis del entorno

El crecimiento menguado de las tasas de productividad, así como otros indicadores de evolución de la economía de una empresa, podrían dar pronósticos desalentadores para proyectos de inversión en IT (micro y pequeña empresa principalmente), por otra parte si ocurre lo contrario como en el caso de un desarrollo continuo o sostenido (mediana y gran empresa), lo mencionado puede volcarse con pronósticos muy positivos y conservadores. Se debe considerar que el sistema puede ser implementado en empresas las cuales posean perdidas por no optimizar sus tiempos y procesos, a lo cual esta herramienta puede brindarle a la misma un futuro prometedor, no obstante existe la variante que una empresa no posea una evolución ascendente lo cual puede deberse a diversos factores económicos y financieros de la misma los cual no es el objetivo de este análisis sino la implementación del sistema y sus beneficios, en donde pudiese darse el caso de que aunque se invirtiese ampliamente en IT, la gerencia administrativa no pudiese sacar el mejor lucro de la herramienta que se propone implementar.

Las soluciones de RFID-WiFi, están orientada a la gestión de activos. A nivel internacional ya existen aplicaciones de este tipo.

4.1.2.2 Panorama general

El sistema de código de barras es usado por miles de empresas para identificar y controlar productos que se mueven diariamente. Sin embargo, la variabilidad de los negocios, ha impulsado a que esta tecnología evolucione, por la necesidad que tienen las empresas de poseer un mayor control de sus productos, en la medida en que se mueven a lo largo de la cadena de abastecimiento. Los códigos de barras, aunque sigan vigentes, no pueden seguir el ritmo de los cambios tecnológicos impulsados por las mismas empresas, en donde una empresa que se estanque en dichos sistemas de identificación paulatinamente quedaría relegada del medio.

Para el caso específico de la gestión de activos, no existen regulaciones en El Salvador según EPC Global en su informe del 4 de Septiembre de 2007, **Estado de Regulación para el Uso de RFID en el Espectro de UHF[12],** respecto de la identificación de productos. Por tanto la implementación de este sistema a nivel nacional se encuentra aún virgen respecto de las aplicaciones de gestión de activos, es de considerar esto a la hora de la implementación y búsqueda de soporte técnico para el sistema.

4.1.2.3 Insumos

Los insumos para un proyecto son principalmente un Kit RFID-WiFi, controladores, antenas, lectores y un servidor, si posee disponibilidad de alguno este puede ser el mismo con el que administran su red de datos. Estos elementos son todos importados y dependen de las políticas monetarias del estado y de comercio exterior. Por este motivo tienen un importante impacto en las aplicaciones de la gestión de activos que se están planteando y

[12] http://www.epcglobalinc.org/tech/freq_reg/RFID_at_UHF_Regulations_20070904.pdf

pueden ser considerados como críticos. Es importante destacar en este punto, que el éxito de la implementación de sistemas RFID-WiFi depende en gran parte de estos insumos.

4.1.2.4 Enfoque de empresas candidatas

La aplicación está orientada para ser empleada en cualquier empresa que posea un alto valor en su inventario y posibilidad de inversión en IT (Investigación de Tecnología), considerando no solo el alto costo que estos representan en los estados contables de las organizaciones, sino también por la información contenida en los mismos y que en algunos casos se considera vital.

4.1.2.7 Pronóstico de las tendencias claves / variables estratégicas

▪ Se aprecia que existe un mercado extranjero en materia de importaciones de interesantes perspectivas para la solución que se propone.

▪ La tecnología RFID seguirá siendo impulsada por GS1 EL SALVADOR lo cual brinda una excelente fuente de apoyo técnico local para el desarrollo de aplicaciones.

▪ Se poseerá una mayor visibilidad y control acerca de dónde se encuentran sus productos en la cadena de suministro en cualquier momento.

▪ Existe una economía que ciertamente muestra un crecimiento lento en el país pero la inversión extranjera podrá favorecer la incorporación de nuevas tecnologías en otras empresas, lo que podrían incrementar las importaciones de componentes de hardware en el país, los cuales podrían constituirse en insumos críticos que afecten el negocio sin embargo en la medida en este se implemente de manera masiva tal y como el código de barra el costo del hardware debería tender a la baja.

4.1.3 Relevamiento del medio interno

4.1.3.1 Aporte a la empresa

Una aplicación basada en tecnología RFID, está orientada a brindar una solución integral en una empresa con el control de inventarios. En adición a esto se puede implementar un nivel extra de seguridad en redes por medio de la unificación de dos mundos: el ambiente RFID y las redes WiFi, considerando que el sistema de código de barras ha llegado a un alto nivel de maduración y que la mayor parte de empresas que poseen un alto valor de inversión en desarrollo tecnológico que va a un ritmo mas acelerado que el antiguo código de barras. La aplicación se constituye dentro de la gestión de activos.

Las aplicaciones RFID-WiFi buscan incrementar el valor agregado de una empresa ofreciendo lo siguiente:

1

- Mejorar el stock.
- Reducción del trabajo administrativo.
- Análisis económico detallado de cada uno de sus activos.
- Gestión de alarmas para mantenimiento preventivo.
- Optimización de los recursos humanos para el mantenimiento y manipulación.
- Centralizar la organización y almacenamiento.
- Matricular sus activos con un identificador único.
- Mejorar la seguridad informática.
- Inventario y localización de activos.
- Disponibilidad de un histórico de actuaciones.
- Mejorar la imagen de su compañía.

4.1.3.2 Recursos

Los principales recursos que se requieren para llevar adelante el proyecto son los recursos financieros, humanos y tecnológicos.

Recursos Financieros: se deberá contar con una partida de la empresa para inversión específicamente en desarrollo de IT que brinde recursos para el diseño y desarrollo de la aplicación, así como también gran parte del capital inicial para la primera compra de elementos RFID-WiFi a ser instalados y equipamientos tecnológicos.

Recursos Humanos: En materia de desarrollo, se recurrirá a contratistas altamente conocedores de la materia, los cuales que realizará la codificación y prueba de la aplicación e interfases requeridas, proporcionando un entrenamiento y capacitación calificada de personal de la empresa para que estos trabajos de desarrollo puedan ser llevados a cabo por el personal de la empresa. El resto de las actividades administrativas (finanzas, legales, fiscales) serán desarrolladas por el personal de administrativo incorporando el monitoreo constante de progreso provocado por el proyecto.

Recursos Tecnológicos: Se considera la compra del equipamiento tecnológico necesario para llevar a cabo las primeras pruebas y la programación de la aplicación. Para ello se requiere de equipos PC, un Kit RFID-WiFi por ejemplo de la marca Cisco *AeroScout*, (que incluye controladores, antenas y lectoras de RFID para ser utilizados en el laboratorio, licencias de software de base) equipos de base de datos, equipos de backup, estabilizadores de tensión y un pequeño servidor central.

4.1.4 Atractivo del mercado y posición competitiva

De la evaluación de las 5 fuerzas de Porter, obtenemos:
1

Competencia: este caso no aplica por ser un proyecto de desarrollo interno.
2

Proveedores: en lo referente a documentación existen proveedores de consultarías sobre RFID como GS1 EL SALVADOR, para hardware no existen proveedores especializados en RFID en El Salvador, y los proveedores que pudiesen existir no brindan el esperado soporte técnico para los equipos que suministran, a pesar de esto existen muchas fuentes externas al país las cuales dada la experiencia que poseen y los canales de suministro que ya tienen, prevalece la necesidad de desarrollar alianzas estratégicas con estos proveedores; se estima que no existirán inconvenientes en la realización de dichas alianzas, por la necesidad de aumentar sus negocios basados en la tecnología propuesta.

Clientes: La implementación de la tecnología RFID-WiFi implica realizar en empresas clientes, la inserción paulatina de esta tecnología, haciendo que estas adopten una nueva postura hacia el desarrollo tecnológico de los productos que se les suministran. Podría existir una cierta sensibilidad en cuanto al precio total de la aplicación en la que incurrirían los clientes, aunque se puede demostrar la eficiencia de los procesos y la optimización de sus tiempos de operación en cuando al manejo de suministros.

Sustitutos: no existen sustitutos en el corto plazo de la aplicación que se ofrece.

Competidores potenciales: no aplica por tratarse de políticas de desarrollo tecnológico interno de la empresa.

4.1.5 ANALISIS FODA

AREAS CLAVE DE RESULTADO	
FORTALEZAS	**DEBILIDADES**
Rentabilidad: ▪ Reducción de costos: mejora del tiempo de operación, reducción de errores humanos, nuevas aplicaciones de marketing, rastreo permanente de activos, evita falsificaciones, incorruptibilidad de códigos, inventario automático, control de fechas de caducidad, etc. **Innovación:** ▪ Mejora continua de procesos: aplicación propuesta basada en RFID-WiFi.	**Recursos físicos:** ▪ Tecnología propia: no se cuenta con una estructura lógica y física de componentes, destinados a brindar el servicio, que sean de fabricación nacional. **Recursos humanos:** ▪ Capacitación del personal: no existe personal nacional capacitado, pero existe un auge

Recursos financieros: ▪ Inversión en IT: los socios de la empresa poseen suficientes solidez para inversiones que proporcionen tazas de retorno grandes a largo plazo.	notorio internacionalmente.
OPORTUNIDADES	**AMENAZAS**
Desarrollo comercial: ▪ Expansión de tecnología RFID y la existente WiFi: oportunidad en el país dado el apoyo por parte de entidades internaciones como EPC Global y nacionales como la Cámara de Comercio de La Republica en conjunto con Insaforp (Instituto Salvadoreño de Formación Profesional), que motivarían a los clientes de la empresa por la opción RFID-WiFi. ▪ Control de inventarios y seguridad informática: existiría en la empresa, una importante necesidad de control de inventarios de activos y seguridad informática, dado que en cuestión de seguridad de redes nunca esta demás algo extra de seguridad, tomando en cuenta las cantidades de dinero que una empresa pueden manejar en sus redes. ▪ Expansión económica: crecimiento de la economía de acuerdo a los indicadores económicos y correspondientemente los presupuestos de inversión de IT de la empresa. ▪ Presencia de GS1 EL SALVADOR: GS1 EL SALVADOR es el promotor de la mayoría de los proyectos relacionados con RFID y como fuente de asesoría para la implementación de sistemas con RFID. **Innovación:** ▪ Barrera de entrada: no existen barrera que impida el desarrollo del proyecto más que la inercia al cambio de sus procesos antiguos.	**Desarrollo comercial:** ▪ Insumos críticos: probabilidad de ser críticos los componentes de hardware por su condición de ser exclusivamente importados. ▪ Pruebas de la tecnología: experimentación con tecnología con la cual no se cuenta con una información técnica especializada en particular.

Tabla: Análisis FODA actual

4.1.6 Diagnóstico

- El mercado de aplicaciones de tecnología basada en RFID, se expandirá fuertemente a mediano plazo lo que nos indica que podría existir una fuerte tentativa por parte de los clientes y proveedores de materializar el lanzamiento de proyectos con RFID.

- Las cambiantes políticas comerciales y los componentes de hardware, que al ser importados podrían constituirse en insumos críticos, podrían afectar el desarrollo del proyecto.

- Existe una permanente necesidad de controlar los inventarios de activos y de un rango extra de seguridad en redes informáticas, por el importante valor que los mismos poseen.

- La aplicación basada en RFID que se propone es innovadora los cual colocaría a la empresa en un estatus de desarrollo tecnológico alto.

- La ventaja de poder manejar sus activos bajo una infraestructura de red WLAN es alentadora ya que se abarcan dos grandes campos con una aplicación RFID-WiFi: la administración de los activos por medio de una red WLAN, evitando el tedioso trabajo de mantenimiento e incomodidad que pudiese provocar el cableado de una red LAN y a la ves con un margen extra de seguridad.

- No se cuenta con la estructura tecnológica regional para sistemas de esta índole, razón por la cual, cobra especial importancia la concreción de alianzas con proveedores extranjeros.

- La aparición de productos sustitutos que pudiesen dejar la tecnología obsoleta no se visualiza en el corto plazo.

4.1.7 Propuesta de Valor

El valor agregado de la solución que se describirá en el capítulo siguiente es enorme para una organización. No sólo se concluye en un ordenamiento de los activos, sino que además permite mantener bajo control los movimientos de estos y evitar el robo de los mismos, así como la seguridad de su red y las implicaciones que esto tiene a nivel costo de reposición y resguardo de la información vital manipulada y almacenada en dichas redes.

Uno de los puntos en los cuáles se basa la propuesta es posibilitar la identificación de los activos mediante el grabado de número de serie en el Tag RFID. Esto permite generar una

base de datos en la cuál cada elemento es identificado inequívocamente para poder ser monitoreado constantemente, así como el nivel de seguridad de red por lectura de *Tag*.

Reducción de los tiempos de operación de inventarios ya que las mediciones se podrían ejecutar en tiempo real si la aplicación así lo necesitase.

Con la posibilidad de un inventario en línea, se amplía el rango de control de activos de una empresa dando como resultado un cien por ciento de fiabilidad en la integridad de activos monitoreados.

Los principales valores agregados de la tecnología de RFID son:

- Trazabilidad de activos en tiempo real.
- Recolección de datos sin contacto directo o visible de las etiquetas
- Verificar asistencia (ej universidad, charlas)
- Agregar seguridad informática
- Cantidad de información que puede guardar el chip
- Información almacenada en la etiqueta puede ser actualizada a demanda
- Alta velocidad de lectura
- Gran capacidad de almacenaje de información
- Mayor distancia de lectura
- Gran precisión en la recuperación de datos
- Nuevas aplicaciones de marketing en retail
- En el caso de las etiquetas pasivas, su fácil ocultamiento y colocación en productos.
- Seguridad de funcionamiento en condiciones de inclemencia (suciedad-polvo-humedad-temperatura)
- Capacidad de recoger información de muchas etiquetas al mismo tiempo
- Tracking permanente
- Reducción de errores humanos.
- Trazabilidad con gran información
- Control de robo en envío de mercancías
- Stocks en tiempo real
- Reducción de papeleo

CAPITULO 5: Evaluación económica-financiera

En este capitulo se hará un análisis de las principales variables que puede conllevar un proyecto de implementación de RFID. El objetivo es ver la rentabilidad y viabilidad del proyecto apoyado con el plan de comercialización del capitulo anterior.

5.1 Ejemplo de aplicación

Como se expuso en el capitulo 2, el RFID no es una aplicación exclusiva para sistemas de inventario. El que siga con esa mentalidad se cierra las puertas a nuevas alternativas tecnológicas de logística y seguridad. Sin embargo tanto en la industria como en el comercio RFID ha tenido un gran auge para la localización de activos y/ productos, lo que motiva a que en este capitulo se analice la implementación completa de un sistema de detección, pero con un enfoque nuevo: el de seguridad. Dicho enfoque plantea la coexistencia de la tecnología RFID con la de WiFi, así como el uso de un sistema mas complejo que el de un simple inventario local, dado que el inventario se puede llevar de una forma centralizada y automatizada.

El eje de este análisis gira en torno de la utilización de RFID para los procesos de la gestión de activos de una compañía, que cuente con una estructura de sucursales distribuidas geográficamente, de manera de abordar una alternativa para éste proceso permita la localización, el seguimiento, la administración de inventarios, el registro de activos y un sistema antirrobo en forma automatizada.

Uno de los grandes desafíos en las organizaciones hoy en día es el seguimiento y mantenimiento de los inventarios, especialmente los tecnológicos, considerando no solo el alto costo que representan en los estados contables de las organizaciones, sino también lo vital de la información contenida en los mismos. Esto es para afrontar uno de los mas grandes problemas de una empresa, el cual es mantener la información (uno de los activos mas vitales de cualquier empresa según la revista *The Economist*, agosto 2007) segura. Bajo esta premisa y considerando el crecimiento de la tecnología informática en las organizaciones, se plantea un escenario importante en cuanto a la inversión a nivel de seguridad de la información.

Básicamente el planteamiento que se abordará será desde el punto de vista de una empresa que quiera un control total de gestión de activos. Tomando en cuenta que dicha empresa cuenta ya con personal calificado en redes, no se incurre en los costos de capacitación de personal.

5.2 Consideraciones especificas de la aplicación

Para el análisis de la rentabilidad del proyecto se planteará el siguiente escenario. Se asumirá que la compañía que implementará el sistema de gestión de activos posee cinco departamentos: ingeniería, administrativo, contabilidad, recursos humanos y planificación. La amortización total del sistema comprenderá un periodo de 3 años aproximadamente.

5.3 Activos Fijos

Como primer paso, se ha definido la composición de los activos fijos a adquirir para la aplicación planteada. Estos bienes se adquieren por única vez y son amortizados en sus respectivos períodos.

En el primer cuadro se pueden observar los bienes de capital, los cuales se amortizarán en un período de 3 años. Se trata fundamentalmente de activos de tecnología que son utilizados para el desarrollo del proyecto. El cuadro muestra el precio unitario de cada ítem, la cantidad a adquirir, el precio total de los mismos y las observaciones en caso de corresponder. En la última fila se describe la inversión total en dólares.

Es de tener en cuenta que únicamente se aborda un estudio para la implementación del sistema de automatización basado en RFID y no para los equipos que puedan existir dentro de un sistema de cómputo.

Concepto	Cantidad	Precio unit. (US$)	Precio total (US$)	Observaciones	Amortización
Servidor	1	1500	1500		3 años
licencia	1	800	800	software de gestión	
rack	1	230	230	para el servidor	
kit RFID-WiFi	5	2900	14500	incluye tags	
		TOTAL	**17030**		

5.4 Costos operativos

Debido a que en cada compañía los activos de valor pueden llegar a ser variados, se necesita hacer un inventario sobre su existencia, para luego incorporarlos en las bases de datos y configurar el sistema. Para poder implementar dicha operación se necesita de personal que haga todas estas funciones.

Estimando un tiempo aproximado de 6 meses para poder desarrollar el sistema en su totalidad (incluyendo la etapa de pruebas de configuración), se ha elaborado el siguiente cuadro de los gastos mensuales en los cuales incurriría la empresa.

Durante los seis meses se instalaran y se harán pruebas de configuración y calibración gradualmente por departamento existente en la empresa aplicante. Las pruebas consisten en la medición de: potencia, diseño de celdas de cobertura, análisis de espectro, cantidad de atenuación, perdidas de señales por el fenómeno de reflexión, ajustes de ganancia de las antenas y orientación, muestreo de señales.

Esta actividad gradual inicia en departamento de ingeniería, administrativo, contabilidad, recursos humanos y por ultimo planificación, en algunos casos taller central y bodegas. La distribución de tiempo es de un mes por departamento para pruebas, finalizando en el último mes con pruebas de integración total del sistema. Con esto se persigue el poder afinar detalles y corregirlos durante el desarrollo de todo el proyecto, logrando así la depuración de imprevistos por medio de un análisis de seguimiento de fallas, en donde de acuerdo a la ruta tomada durante el mismo se podrá puntualizar errores o puntos débiles de la aplicación.

Se ha estimado un total de 2 empleados para la implementación del proyecto. De los cuales, uno se va a encargar de las configuraciones y todo lo referente a software y otro que se va a dedicar del hardware. Aunque para la primera etapa del proyecto, ambos deberán de recolectar toda la información acerca de los activos de la compañía.

Adicionalmente se deberá capacitar y reasignar a una persona de mantenimiento para dar soporte técnico del sistema. Dicha persona actualmente tiene un sueldo mensual de $300. Este costo mensual tendrá como periodo el tiempo total del proyecto. Sin embargo debido a que es un sistema automatizado el soporte técnico no será una tarea demandante, dejando así al técnico con tiempo para realizar otras labores, por lo que únicamente se tomará como un costo mensual de $100 para el proyecto.

Además, se requerirá de una persona que dé un mantenimiento a los equipos semestralmente, con un costo total de $400 por visita. De tal forma que si el periodo que comprende el servicio de gestión de activos es de 3 años, en concepto de mantenimiento se deberá de invertir $2,400 en total.

Costos Operativos (implementación del proyecto)			
	Costo Unitario Mensual	**Costo mensual**	**Costos Totales (3 primeros meses)**
Sueldos			6000
2 empleados	1000	2000	
Gastos varios	500	500	1500
Total	**1500**	**2500**	**7500**

Costos Operativos (mantenimiento del proyecto)		
	Costo anual	Costos Totales
Técnico de soporte y mantenimiento	1200	3600
Stock de repuestos RFID	490	1470
Gastos varios	200	400
Total	**1890**	**5470**

5.5 Financiamiento

Para poder sustentar el proyecto, se recurre a un préstamo pagadero en 3 años (mismo tiempo de vigencia del proyecto) por un total de $30,000. Con el cual se asume una tasa de 11% anual.

5.6 Presupuesto

A continuación se presentan tablas con flujo de fondos para poder realizar un cuadro de resultados. Permitiendo así generar un reporte que evidencie, en términos financieros la viabilidad o no del proyecto.

5.6.1 Cuadro de amortización de deuda

años	cuota mensual	intereses	amortización	amortizado	pendiente
0					30,000.00
1	982.16	3,300.00	8,976.39	8,976.39	21,023.61
2	982.16	2,312.60	9,963.80	18,940.19	11,059.81
3	982.16	1,216.58	11,059.81	30,000.00	0.00

5.6.2 Flujo de efectivo

Año	2008	2009	2010
Ingresos	**25,000.00**	**25,000.00**	**25,000.00**
Costos Operativos	**9,900.90**	**2,400.90**	**2,400.90**
Sueldos	7,200.00	1,200.00	1,200.00
Gastos varios	2,190.00	690.00	690.00
Depreciación	510.90	510.90	510.90

Utilidad antes de impuesto	**15,099.10**	**22,599.10**	**22,599.10**
Impuestos (25%)	3,774.78	5,649.78	5,649.78
Utilidad neta	**11,324.32**	**16,949.32**	**16,949.32**
Depreciación	510.90	510.90	510.90
Pago de capital	8,976.39	9,963.80	11,059.81
Flujo neto de Efectivo	**1,837.03**	**6,474.62**	**4,923.61**

5.7 análisis de resultados

De la evaluación del flujo de fondos se obtienen los siguientes valores:

$$\text{VAN} = (\text{Io}) + \frac{f1}{(1+i)^1} + \frac{f2}{(1+i)^2} + \ldots + \frac{fn}{(1+i)^n}$$

$$\text{VAN} = (17{,}030) + \frac{1837.03}{(1+0.1)^1} + \frac{6474.62}{(1+0.1)^2} + \frac{4923.61}{(1+0.1)^3} = 27750.13$$

$$\text{TIR} = \frac{(17030)+1837.03+6474.62+4923.61}{1837.03+2(6474.62)+3(4923.61)} = 2.04\%$$

Donde:
Io: Inversión inicial
fn : flujo de efectivo del n-esimo año
i: tasa de interés

El resultado del proyecto es aceptable, considerando que tanto la TIR como el VAN resultan con valores positivos superiores a 1.

Además una de las principales ventajas de este proyecto es la integración de las redes WiFi al sistema de detección de RFID lo cual reduce considerablemente el costo, sobre todo el de cableado. Además del costo de un equipo de acceso de red, ya sea un switch L3 o un router.

Para cualquier proyecto de mejora administrado adecuadamente se deben considerar dos áreas de importantes, y una de las formas más comunes para observar los beneficios de un proyecto es utilizando los términos “tangibles” e “intangibles”.

La mayoría de análisis de proyectos se concretan en beneficios tangibles (aquéllos que se pueden ver y tocar), sin embargo suelen pasar desapercibidos aquellos que son intangibles (que son difíciles de cuantificar pero que a menudo son importantes, como por ejemplo la perdida por robo o hurtó de activos, robo de información confidencial, etc.).

Las técnicas comunes de justificación de proyectos como retorno de la inversión (*Return of Investment: ROI*), entre otros, tienen su lugar en el proceso de aprobación de proyectos; sin embargo, ciertos planes tienen beneficios intangibles que pueden ser tan importantes como los beneficios tangibles.

Beneficios

Muy a menudo la tecnología a gran escala o el cambio de procesos en una compañía tales como la implementación de un sistema RFID o el establecimiento de un centro de servicios compartidos de red, crean la necesidad de un cambio cultural que genere los beneficios tangibles.

Sin las reestructuración de esquemas para planteamiento de los proyectos, los beneficios tangibles podrían no materializarse si fuesen los únicos en consideración, en este caso, sencillamente no se podría tener un tipo de beneficio sin el otro.

CAPITULO 6: Aplicación

En el presente capitulo se desarrollará un aplicación practica de un sistema RFID con fines didácticos. El objetivo de dicha aplicación es demostrar que los sistemas de RFID no se utilizan únicamente para control de inventarios. En ésta aplicación en particular, se utilizará la tecnología de identificación por RF para otorgar un grado adicional de seguridad de una red de área local, basado en autenticación.

6.1 Descripción de la aplicación

El sistema automatizado de control de red se divide en 3 partes. La primera es la parte de identificación del usuario, la cual se hace por Identificación basada en Radio Frecuencia. La segunda es la autenticación de los usuarios, la cual la realiza un servidor de autenticación RADIUS. Finalmente la última parte es la de gestión de permisos, la cual se realiza también por medio del servidor de autenticación con ayuda de un dispositivo de red con soporte RADIUS, permitiendo así dar acceso a solicitantes a la red local.

A continuación se detalla el diagrama de la aplicación:

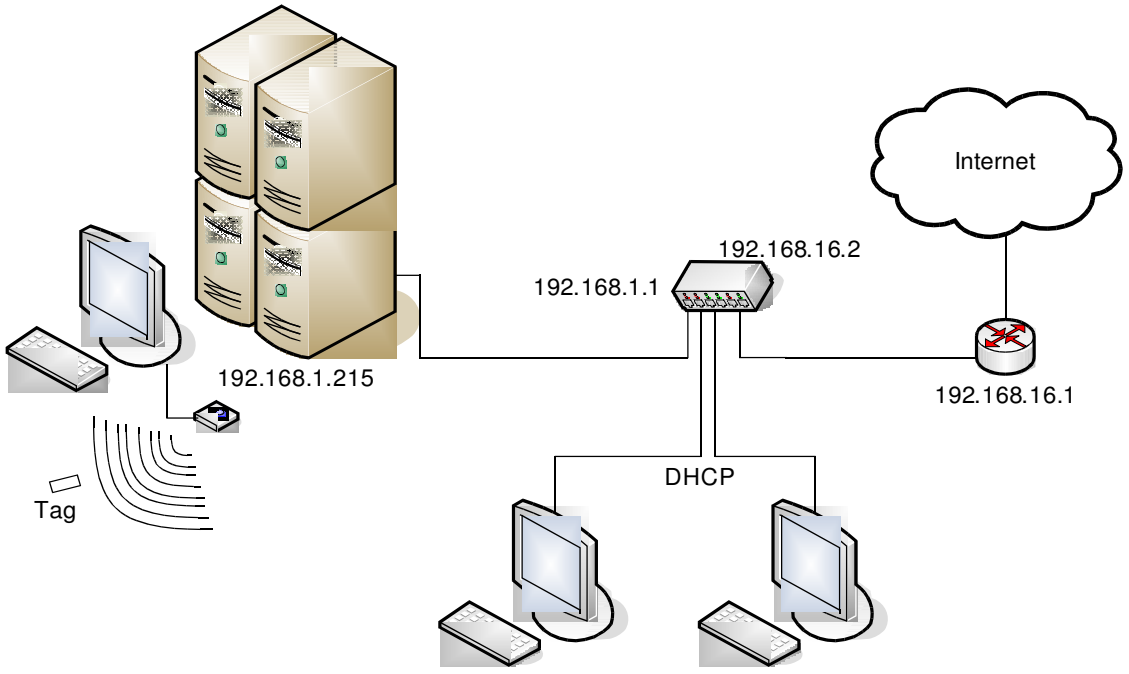


Figura 6.1: Esquema de la aplicación automatizada basada en RFID

6.2 Identificación de usuarios

En un ambiente de redes, se define por usuario a todo aquel que hace uso de la red. Para que los usuarios puedan acceder a ésta y al uso de sus recursos, administrarla, etc., dichos usuarios deben primero identificarse.

Para la aplicación del sistema automatizado de acceso a redes, cada usuario estará asociado a un solo *tag*. La información contenida en cada *tag* será la misma para todos los usuarios y consta de:

- Nombre. Se tomará en cuenta únicamente el primer nombre del usuario con un número máximo de ocho caracteres.
- Apellido. Se tomará en cuenta únicamente el primer apellido del usuario con un número máximo de ocho caracteres.
- Cargo. Se especificara el cargo desempeñado por el usuario igualmente limitado por un máximo de ocho caracteres.

Para la primera parte de la aplicación, se ha implementado una interfaz grafica la cual permite que un lector de tarjetas MIFARE MF1 (compatible con el estándar ISO 14443-A), realice lecturas sucesivas de los usuarios de red. Las lecturas realizadas se muestran en pantalla y además se almacena en un archivo, (de configuración para el servidor de autenticación) el nombre de usuario y una contraseña generada aleatoreamente.

La lectura del *tag* esta limitada al numero identificador del *tag* y a los bloques 0 (nombre de usuario),1 (apellido) y 2 (cargo desempeñado en la empresa) del sector 1 de la tarjeta. Debido a que dicha información es más que suficiente para poder desarrollar la aplicación que se ha planteado.

6.2.1 Interfaz de lectura de RFID

La lectura de los *tags* en la interfaz se realiza de la siguiente manera:

1. Para realizar la lectura de la información contenida en los *tags* se cuenta con un botón de selección (Leer Datos).
2. Al encontrar un *tag* valido, la interfaz muestra en pantalla la información acerca del *tag*.
3. Como mecanismo de seguridad para cada lectura de un mismo *tag*, se genera un código aleatorio distinto el cual es asociado a la contraseña de usuario en la base de datos del servidor de autenticación.

4. Al mismo tiempo que se realiza el procedimiento anterior se realiza también un proceso de escritura dentro del archivo de configuracion, con la información mostrada en pantalla. (dicha información esta contenida en el *tag* con números hexadecimales, sin embargo en la aplicación se a implementado la conversión de hexadecimal a ASCII para desplegar de forma comprensible la información guardada).

6.2.2 Restricciones de la interfaz

No es posible leer dos o más *tags* simultáneamente. Esto es debido a que en el tipo de aplicación que se implementa se necesita identificar un usuario a la vez, ya que cada usuario tiene diferentes tipos de permisos, contraseñas y accesos.

El *tag* leído cumple únicamente con el estándar MIFARE bajo ISO-14443-A, los protocolos y tramas de comunicación utilizados, han sido descritos en el capitulo 2.

6.2.3 Pasos para ejecutar la Interfaz

Para la interfaz se ha generado un archivo ejecutable, para sistemas operativos Windows, denominado *reader*. Luego de ejecutar dicha aplicación aparecerá la figura 6.2.a.

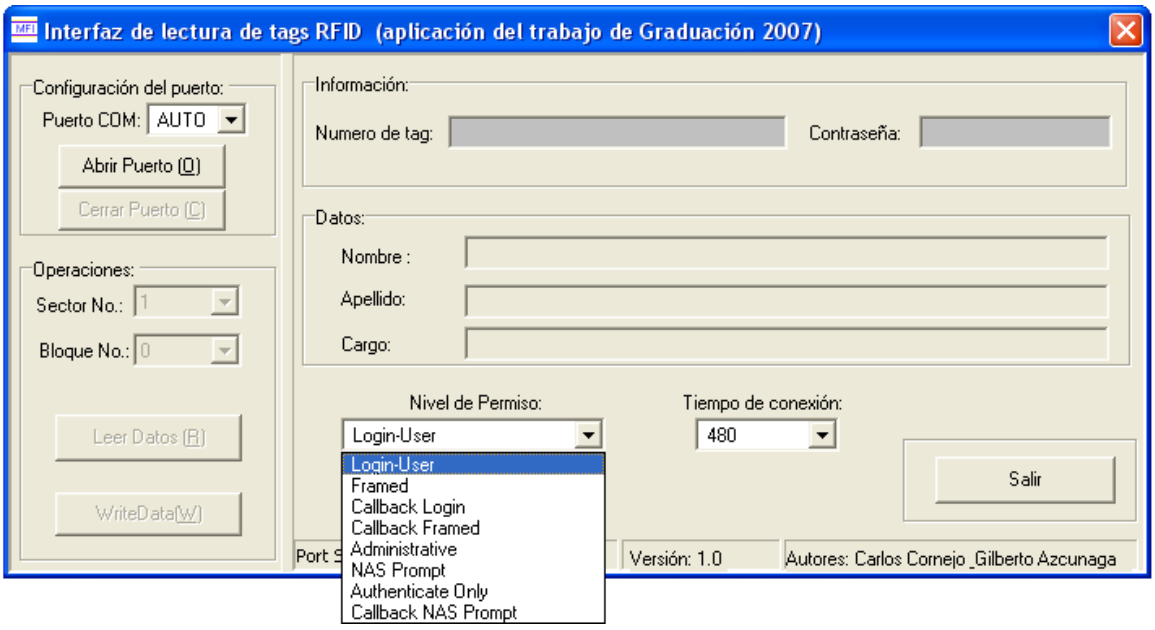


Figura 6.2.a: Interfaz de lectura para RFID

Como el puerto por el cual se comunica el *reader* con la computadora donde esta la interfaz es de tipo serial, se debe de "abrir" el puerto. Es decir se debe de establecer una comunicación entre el dispositivo de lectura y la computadora (para sincronizar los tiempos de operación entre ambos dispositivos). Para tal fin se debe de dar un clic en el botón: "Abrir Puerto". Al dejar la opción de Puerto COM en AUTO, el programa busca automáticamente en que puerto habilitado se encuentra el dispositivo de lectura.

Una vez inicializado el puerto de comunicación se procede a darle un clic al botón "Leer Datos". Automáticamente la interfaz despliega la información del *tag* en las casillas correspondientes y posteriormente genera un archivo de configuración para la asignación de permisos y contraseñas a usuarios (los cuales están relacionados a cada *Tags*).

6.2.4 Programación de la interfaz

La interfaz de comunicación se ha desarrollado en código Borland Delphi (orientado a objetos) utilizando como base para la comunicación con el hardware del *reader* la librería *RRMifare32.dll*, la cual es proporcionada por el fabricante con el *reader* en el momento de su compra. Dicha librería contiene todos los comandos necesarios para intercambiar datos y establecer la comunicación entre el *reader* y el *tag* y entre el *reader* y el ordenador de acuerdo a un estándar (en este caso de acuerdo al MIFARE). Por lo que la programación de la interfaz se enfoca básicamente en el manejo e interpretación de los datos que procesa dicha librería y en el desarrollo de una interfaz gráfica.

6.3 Autenticación de usuarios

La autenticación de un usuario se basa básicamente en la confirmación de su procedencia en base a su identificación. En términos de seguridad de redes de datos se puede considerar la autenticación como uno de los tres pasos fundamentales (AAA: Autenticación, Autorización y Auditoria).

La segunda parte del sistema consiste en la autenticación de usuarios, permitiendo así un acceso más restringido a la red. El proceso de autenticación se realiza por medio de RADIUS (Ver anexo de redes).

Para implementar RADIUS se tiene que instalar un software en una maquina con una dirección IP preestablecida 192.168.1.215. Para este caso se utilizará el software *Radl*, propietario de *Luteus*. Dicho software es de uso libre, por lo que no se requieren licencias. En la configuración del software se utilizan básicamente 2 archivos. Uno es de los clientes (*clients*) y el otro es de los usuarios (*Users*).

6.3.1 clientes

Los clientes son los dispositivos de red que permiten interconectar otras computadoras a la red mediante el servicio de RADIUS, pasando por el servidor de autenticación.
Para esta aplicación se utilizará únicamente un cliente. Para configurar el servidor es necesario poner la dirección IP del cliente y el *shared key* (ver definición en anexo de Redes) mediante el cual se comunican entre ellos, en un archivo de configuración llamado: *clients*

El cliente de la red es un equipo Fortinet, modelo Fortigate 50B, en el cual la configuración necesaria para establecer la comunicación con el Server, consiste en ingresar la dirección IP del Server y el *shared key* y habilitar permisos en el *firewall.*

6.3.2 usuarios

Los usuarios son todos aquellos autorizados para acceder a los servicios de red por medio del servidor de autenticación. Cada uno de estos usuarios esta asociado a un *tag*, mismos los cuales son almacenados en un archivo de configuración de manera automática por la interfaz descrita anteriormente

6.4 Gestión de permisos

La mayoria de los sistemas que tienen acceso a recursos compartidos permiten asignar permisos (a distintos niveles), para determinados usuarios.

En el caso particular del servidor Radius la gestion de permisos se realiza mediante parámetros denominados atributos. El atributo que se utiliza para poder diferenciar los privilegios de acceso de un usuario es: *Service-Type*. A continuación se detalla una lista de los distintos valores que puede tomar dicho atributo.

Login. El usuario se debe conectar mediante un Host.

Framed Se debe de inicializar un protocolo de *frame* para el usuario, tal como PPP o SLIP.

Callback Login El usuario debe estar desconectado y se le debe marcar para luego ser conectado a un *Host*

Callback Framed	El usuario debe estar desconectado y se le debe marcar mediante un protocolo basado en *Farme*.
Administrative	El usuario debe tener acceso de tipo administrativo a la interfaz de autenticación de la red de donde están ejecutando los comandos con privilegios.
NAS Prompt	El usuario debe de proveer los privilegios mediante una línea de comandos en el NAS (Dispositivo de almacenamiento de Red).
Authenticate Only	Solo se requiere de la autenticación y no se necesita regresar ningún tipo de parámetro de autorización
Callback NAS Prompt	El usuario debe ser desconectado y se le debe de marcar para luego proveerle los privilegios mediante una línea de comandos en el NAS (Dispositivo de almacenamiento de Red).

Otro atributo utilizado en el servidor de autenticación es: Sesion-Timeout, el cual permite establecer el tiempo de conexión a los recursos compartidos por parte de los usuarios. El valor de este atributo se especifica en segundos y su valor máximo es 9999.

Para llevar un histórico de la actividad del servidor Radius se ha instalado un sistema *Syslog* el cual permite almacenar en un archivo dicha información. El *syslog* utilizado es de código abierto.

CONCLUSIONES

Las conclusiones más relevantes que se pueden obtener del presente documento acerca de la tecnología RFID y su implementación descritas en son las siguientes:

- RFID es una tecnología de identificación que puede ser utilizada en una gran variedad de aplicaciones, el hecho de considerarla únicamente para la implementación de sistemas de inventario, cierra las posibilidades de cambiar otros tipos de procesos a una forma más efectiva en las áreas de logística, seguridad y control.

- Se puede trabajar dicha tecnología en base a estándares, dependiendo del tipo de aplicaciones para la que se destine su uso (por ejemplo para el uso en animales existe el ISO 14223).

- Aunque la tecnología de RFID abre caminos hacia el desarrollo optimo de procesos de automatización industrial, control de bienes, consumo y servicios, la mayoría de las aplicaciones son desarrolladas a manera de poder volver a emplear los recursos, permitiendo así la reutilización o reescritura de los *Tags*, lo cual hace que éstos no sean desechables compensando su costo actual.

- En aplicaciones donde los recursos no son reutilizables como el caso de etiquetas descartables, dichas aplicaciones favorecen casi en su totalidad a los clientes, quienes a su ves hacen uso de este recurso para optimizar sus procesos internos (por ejemplo: en el caso de un supermercado, él cual es un cliente de los distribuidores de sus productos controlados por RFID), mientras que los proveedores se conforman con aplicar Tags a los productos, en estos casos la implementación de RFID solo implica un costo adicional a los distribuidores de productos controlados por etiquetas de RFID.

- La tecnología RFID permite interoperatividad entre tags y dispositivos estándares de redes WiFi.

- La reestructuración de los esquemas seguidos actualmente para el planteamiento de negocios y la reingeniería de los procesos de organización interna son puntos claves para la adopción de sistemas de RFID en procesos de automatización industrial, control de bienes, consumo y servicios.

- Existen obstáculos de carácter tecnológico ya que los estándares aun no se encuentran totalmente definidos, el costo de los Tags es elevado, la infraestructura

es relativamente costosa y con tendencia a la pronta caducidad por estar en vías de evolución, aunado a ello no existen entidades especialistas en nuestro país.

- Existen impedimentos específicos en la industria de servicios públicos ya que inmersión de sistemas abarca temas delicados en donde para la implantación de este, tiene que pasar por procesos de licitación rigurosos en donde es filtrada por los múltiples niveles y tipos de decisión haciendo así que la aprobación del mismo sea un proceso extenso, complicado y sin un retorno de inversión a mediano plazo

- RFID permite una versatilidad de opciones en cuanto a *tags* basadas en tamaños, eléctricos, aspectos físicos, etc.

- Si se desea implementar sistemas RFID-WiFi se debe tener en mente el establecimiento de relaciones de negocios a largo plazo con proveedores de tecnología, formulando contratos donde las políticas de control de bienes, servicios y suministros sea bien definida, para asegurar la actualización de sistemas y la no obsolescencia de esquemas utilizados por medio de la actualización constante de los mismos, redefiniendo así estándares de la arquitectura implementada

Anexo 1: Redes

1.1 Conceptos básicos de redes

1.1.1 Concepto de red

Una red es un proceso que permite la conexión de equipo para la realización de operaciones centralizadas o distribuidas, con la finalidad de compartir recursos "hardware y software" la cual logra a través de la transmisión de datos el intercambio de información entre ordenadores la comunicación remota y la optimización del equipo.

Toda red esta formada por un Nodo o Terminal y un Medio de transmisión. Un nodo es un elemento de la red capaz de iniciar o terminar una comunicación. La comunicación entre ambas terminales es posible solo si existe un medio de transmisión capaz de llevar la información desde un nodo inicial hasta un nodo terminal.

Un **nodo** físicamente puede ser una PC, una súper computadora (*frame*), una impresora, un puente (*gate*) o un ruteador.
Por otra parte un **medio** puede ser un cable o una onda electromagnética que viaja a través del aire.

Un tercer elemento para un esquema de red se le conoce como **subred** y tiene significado cuando los nodos en conexión se encuentran bastante distantes entre sí, y no forman parte de la misma red; es en este caso donde pueden existir toda una serie de nodos intermedios que llevan a cabo la conexión física, a estos nodos intermedios se les denomina genéricamente como una **subred**. Una subred está formada por dos componentes:

Líneas de transmisión: quienes son las encargadas de llevar los bits entre los *hosts*.

Elementos interruptores (routers): son computadoras especializadas usadas por dos o más líneas de transmisión. Para que un paquete llegue de un router a otro, generalmente debe pasar por routers intermedios, cada uno de estos lo recibe por una línea de entrada, lo almacena y cuando una línea de salida está libre, lo retransmite.

1.1.2 Clasificación de redes

Desde el punto de vista de alcance, una red se clasifica según la distancia a la que se extiende y del alcance global con que se puede analizar.

Redes Punto a Punto.

Una red punto a punto es aquella para la que siempre dos terminales están unidas por una línea o cable no compartido tal que su uso es dedicado sólo a esas dos terminales.

Las topologías que soporta esta clasificación son: la topología anillo, topología estrella, topología de árbol y la topología de malla.

Redes Multipunto.

En una red multipunto sólo existe una línea de comunicación cuyo uso está compartido por todas las terminales en la red. La información fluye de forma en dos direcciones y es discernible para todas las terminales de la red.

Lo típico es que en una conexión multipunto las terminales compiten por el uso del medio (línea) de forma que el primero que lo encuentra disponible lo acapara, aunque también puede negociar su uso. La topología bus soporta este tipo de red.

Redes Basadas en servidor.

Las redes basadas en servidor son mejores para compartir gran cantidad de recursos y datos. Un administrador supervisa la operación de la red, y vela que la seguridad sea mantenida. Este tipo de red puede tener uno o más servidores, dependiendo del volumen de tráfico, número de periféricos etc. Por ejemplo, puede haber un servidor de impresión, un servidor de comunicaciones, y un servidor de base de datos, todos en una misma red.

1.1.2.1 Clasificación según alcance.

Las redes LAN (Local Area Network, redes de área local) son las redes que todos conocemos, es decir, aquellas que se utilizan en nuestra empresa. Son redes pequeñas, entendiendo como pequeñas las redes de una oficina, de un edificio. Debido a sus limitadas dimensiones, son redes muy rápidas en las cuales cada estación se puede comunicar con el resto. Están restringidas en tamaño, lo cual significa que el tiempo de transmisión, en el peor de los casos, se conoce. Además, simplifica la administración de la red.
Suelen emplear tecnología de difusión mediante un cable sencillo (coaxial o UTP) al que están conectadas todas las máquinas. Operan a velocidades entre 10 y 100 Mbps.
Características preponderantes:

- Los canales son propios de los usuarios o empresas.
- Los enlaces son líneas de alta velocidad.
- Las estaciones están cercas entre sí.

- Incrementan la eficiencia y productividad de los trabajos de oficinas al poder compartir información.
- Las tasas de error son menores que en las redes WAN.
- La arquitectura permite compartir recursos.

LANs muchas veces usa una tecnología de transmisión, dada por un simple cable, donde todas las computadoras están conectadas. Existen varias topologías posibles en la comunicación sobre LANs, las cuales se verán mas adelante.

Las redes WAN (Wide Area Network, redes de área extensa) son redes punto a punto que interconectan países y continentes. Al tener que recorrer una gran distancia sus velocidades son menores que en las LAN aunque son capaces de transportar una mayor cantidad de datos. El alcance es una gran área geográfica, como por ejemplo: una ciudad o un continente. Está formada por una vasta cantidad de computadoras interconectadas (llamadas *hosts*), por medio de subredes de comunicación o subredes pequeñas, con el fin de ejecutar aplicaciones, programas, etc.

Una red de área extensa WAN es un sistema de interconexión de equipos informáticos geográficamente dispersos, incluso en continentes distintos. Las líneas utilizadas para realizar esta interconexión suelen ser parte de las redes públicas de transmisión de datos.
Las redes LAN comúnmente, se conectan a redes WAN, con el objetivo de tener acceso a mejores servicios, como por ejemplo a Internet. Las redes WAN son mucho más complejas, porque deben enrutar correctamente toda la información proveniente de las redes conectadas a ésta.

INTERNET WORKS: Es una colección de redes interconectadas, cada una de ellas puede estar desarrollada sobre diferentes software y hardware. Una forma típica de Internet Works es un grupo de redes LANs conectadas con WANs. Si una subred le sumamos los host obtenemos una red.
El conjunto de redes mundiales es lo que conocemos como Internet.

Las redes MAN (Metropolitan Area Network, redes de área metropolitana), comprenden una ubicación geográfica determinada "ciudad, municipio", y su distancia de cobertura es mayor de 4 Kmts. Son redes con dos buses unidireccionales, cada uno de ellos es independiente del otro en cuanto a la transferencia de datos. Es básicamente una gran versión de LAN y usa una tecnología similar. Puede cubrir un grupo de oficinas de una misma corporación o ciudad, esta puede ser pública o privada. El mecanismo para la resolución de conflictos en la transmisión de datos que usan las MANs, es DQDB.
DQDB consiste en dos buses unidireccionales, en los cuales todas las estaciones están conectadas, cada bus tiene una cabecera y un fin. Cuando una computadora quiere transmitir a otra, si esta está ubicada a la izquierda usa el bus de arriba, caso contrario el de abajo.

Redes de area de almacenamiento (SAN), una red SAN es una red dedicada, de alto rendimiento que se utiliza para trasladar datos entre servidores y recursos de almacenamiento, esta al ser una red separada y dedicada evita el conflicto de tráfico entre clientes y servidores.
Esta tecnología permite conectividad de alta velocidad, de servidor a almacenamiento, almacenamiento a almacenamiento, o de servidor a servidor. Este método es una infraestructura de red por separado evitando así cualquier problema asociado con la conectividad de las redes existentes. Las SAN poseen alto rendimiento, disponibilidad y escalabilidad.

Red privada virtual (VPN), es una red privada que se constituye dentro de la infraestructura de una red pública, como la Internet global. Con una VPN un empleado a distancia puede acceder a la red de la sede de la empresa a través de Internet, en la cual el empleado posee un acceso seguro entre su PC y el router VPN de la sede.

1.1.2.2 Clasificación según su distribución lógica

Todos los ordenadores tienen un lado cliente y otro servidor: una máquina puede ser servidora de un determinado servicio pero cliente de otro servicio.

Servidor. Máquina que ofrece información o servicios al resto de los puestos de la red. La clase de información o servicios que ofrezca determina el tipo de servidor que es: servidor de impresión, de archivos, de páginas web, de correo, de usuarios, de IRC (charlas en Internet), de base de datos.

Cliente. Máquina que accede a la información de los servidores o utiliza sus servicios. Ejemplos: Cada vez que estamos viendo una página web (almacenada en un servidor remoto) nos estamos comportando como clientes. También seremos clientes si utilizamos el servicio de impresión de un ordenador remoto en la red (el servidor que tiene la impresora conectada).
Todas estas redes deben de cumplir con las siguientes características:

- Confiabilidad "transportar datos".
- Transportabilidad "dispositivos".
- Gran procesamiento de información.

y de acuerdo estas, tienen diferentes usos, dependiendo de la necesidad del usuario, como son:

- Compañías - centralizar datos.
- Compartir recursos "periféricos, archivos, etc".
- Confiabilidad "transporte de datos".
- aumentar la disponibilidad de la información.
- Comunicación entre personal de las mismas áreas.

- Ahorro de dinero.
- Home Banking.
- Aportes a la investigación "vídeo demanda, line T.V, Game Interactive".

1.1.3 Topologías de red

Una topología de red es la estructura de equipos, cables y demás componentes en una red. Es un mapa de la red física. El tipo de topología utilizada afecta al tipo y capacidades del hardware de red, su administración y las posibilidades de expansión futura.
La topología es tanto física como lógica:
1• La topología física describe cómo están conectados los componentes físicos de una red.
2• La topología lógica describe el modo en que los datos de la red fluyen a través de componentes físicos.
Existen cinco topologías básicas:
1• *Bus.* Los equipos están conectados a un cable común compartido.
2• *Estrella.* Los equipos están conectados a segmentos de cable que se extienden desde una ubicación central, o concentrador.
3• *Anillo*. Los equipos están conectados a un cable que forma un bucle alrededor de una ubicación central.
4• *Malla.* Los equipos de la red están conectados entre sí mediante un cable.
5• *Híbrida.* Dos o más topologías utilizadas juntas.

Topología de Bus.

Los buses lineales son quizás la topología más utilizadas para redes de área local, también son las más baratas y una de las más conflictivas. Consiste en conectar todas las terminales a una línea común, utilizando para ello un dispositivo llamado TAP, además de un segundo cable auxiliar (*drop line*) que conecta la terminal al TAP y éste a su vez a la línea compartida. También en los extremos del bus se requieren dos elementos terminadores.

Las desventajas en ésta topología es la longitud del cable, terminales, el no uso de Taps. Por otra parte los mensajes de desgastan cada vez que pasan por un Tap, y si no tuviese terminadores los mensajes se colapsarían y se perderán.

Topología en Estrella.

Ésta topología conecta a todas las terminales entre sí, aunque no en forma directa. Para ello utiliza un elemento que organiza el flujo de la información en la red mediante *switcheos* que conectan a la terminal destino con la terminal origen. A éste elemento se le

conoce cómo concentrador y su tarea debe ser invisible a las terminales que se comunican.

La ventaja de la topología de estrella, es que es más robusta que la topología de anillo, ya que si falla una terminal, el resto sigue funcionando. La desventaja es que si falla el concentrador entonces irremediablemente fallará toda la red.

Topología de Anillo.

La topología de anillo conecta a cualquier terminal, únicamente con sus dos destinos más próximos mediante una línea dedicada, de tal forma que la última de las terminales se conecta con la primera de ellas por uno de los extremos, formando así un ciclo o un anillo a través del cual fluye la información cuando las terminales se comunican. La comunicación en un anillo es unidireccional o *simplex,* y viaja de terminal a terminal hasta que encuentra su destino y regresa a su origen. Tiene la desventaja de que cualquier fallo entre alguna de las líneas dedicadas genera una falla letal en la red.

Topología en Malla.

Para ésta última se busca tener conexión física entre todas las terminales de la red. Utilizando conexiones punto a punto, esto permitirá que cualquier terminal se comunique con otras terminales de forma paralela si fuera necesario. La principal ventaja es que este tipo de redes difícilmente falla, pues inclusive, si alguna de estas líneas fallara aún así se podrían encontrar otras rutas para lograr la información.

La desventaja de la topología en malla, es que se requiere demasiado cableado específicamente si existen n terminales en la red entonces se requerirían: No. cables=n(n-1)/2 cables en total.

Además cada terminal requiere n-1puertos de comunicación. También el mantenimiento resulta costoso a largo plazo.

Topologías Hibridas.

En una topología híbrida, se combinan dos o más topologías para formar un diseño de red completo. Raras veces, se diseñan las redes utilizando un solo tipo de topología. Por ejemplo, es posible que desee combinar una topología en estrella con una topología de bus para beneficiarse de las ventajas de ambas.
En una topología híbrida, si un solo equipo falla, no afecta al resto de la red.
Normalmente, se utilizan dos tipos de topologías híbridas: topología en estrella-bus y topología en estrella-anillo.

En estrella-bus: En una topología en estrella-bus, varias redes de topología en estrella están conectadas a una conexión en bus. Cuando una configuración en estrella

está llena, podemos añadir una segunda en estrella y utilizar una conexión en bus para conectar las dos topologías en estrella.
En una topología en estrella-bus, si un equipo falla, no afectará al resto de la red. Sin embargo, si falla el componente central, o concentrador, que une todos los equipos en estrella, todos los equipos adjuntos al componente fallarán y serán incapaces de comunicarse.

En estrella-anillo: En la topología en estrella-anillo, los equipos están conectados a un componente central al igual que en una red en estrella. Sin embargo, estos componentes están enlazados para formar una red en anillo.
Al igual que la topología en estrella-bus, si un equipo falla, no afecta al resto de la red. Utilizando el paso de testigo, cada equipo de la topología en estrella-anillo tiene las mismas oportunidades de comunicación. Esto permite un mayor tráfico de red entre segmentos que en una topología en estrella-bus.

1.1.3.1 Mecanismos para la resolución de conflictos en la transmisión de datos

CSMA/CD: Son redes con escucha de colisiones. Todas las estaciones son consideradas igual, es por ello que compiten por el uso del canal, cada vez que una de ellas desea transmitir debe escuchar el canal, si alguien está transmitiendo espera a que termine, caso contrario transmite y se queda escuchando posibles colisiones, en este último espera un intervalo de tiempo y reintenta de nuevo.

Token Bus: Se usa un token (una trama de datos) que pasa de estación en estación en forma cíclica, es decir forma un anillo lógico. Cuando una estación tiene el token, tiene el derecho exclusivo del bus para transmitir o recibir datos por un tiempo determinado y luego pasa el token a otra estación, previamente designada. Las otras estaciones no pueden transmitir sin el token, sólo pueden escuchar y esperar su turno. Esto soluciona el problema de colisiones que tiene el mecanismo anterior.

Token Ring: La estación se conecta al anillo por una unidad de interfaz (RIU), cada RIU es responsable de controlar el paso de los datos por ella, así como de regenerar la transmisión y pasarla a la estación siguiente. Si la dirección de la cabecera de una determinada transmisión indica que los datos son para una estación en concreto, la unidad de interfaz los copia y pasa la información a la estación de trabajo conectada a la misma.

1.1.4 Componentes básicos de conectividad

Los componentes básicos de conectividad de una red incluyen los cables, los adaptadores de red y los dispositivos inalámbricos que conectan los equipos al resto de la red. Estos

componentes permiten enviar datos a cada equipo de la red, permitiendo que los equipos se comuniquen entre sí. Algunos de los componentes de conectividad más comunes de una red son:

- Adaptadores de red.
- Cables de red.
- Dispositivos de comunicación inalámbricos.

Con la aparicion de estos dispositivos se proporciona la conectividad a Internet a través de una conexión con cable, router, cablemódem o módem DSL y un punto de acceso inalámbrico que sirve de hub para los nodos inalámbricos.

1.1.4.1 Adaptadores de Red.

Cada adaptador de red tiene una dirección exclusiva, denominada dirección de control de acceso al medio (*media access control*, MAC), incorporada en chips de la tarjeta.
Los adaptadores de red convierten los datos en señales eléctricas que pueden transmitirse a través de un cable. Convierten las señales eléctricas en paquetes de datos que el sistema operativo del equipo puede entender.
Los adaptadores de red constituyen la interfaz física entre el equipo y el cable de red. Los adaptadores de red, son también denominados tarjetas de red o NICs (Network Interface Card), se instalan en una ranura de expansión de cada estación de trabajo y servidor de la red. Una vez instalado el adaptador de red, el cable de red se conecta al puerto del adaptador para conectar físicamente el equipo a la red.
Los datos que pasan a través del cable hasta el adaptador de red se formatean en *paquetes*. Un paquete es un grupo lógico de información que incluye una cabecera, la cual contiene la información de la ubicación y los datos del usuario.
La cabecera contiene campos de dirección que incluyen información sobre el origen de los datos y su destino. El adaptador de red lee la dirección de destino para determinar si el paquete debe entregarse en ese equipo.
Si es así, el adaptador de red pasa el paquete al sistema operativo para su procesamiento. En caso contrario, el adaptador de red rechaza el paquete.
Cada adaptador de red tiene una dirección exclusiva incorporada en los chips de la tarjeta. Esta dirección se denomina dirección física o dirección de control de acceso al medio (*media access control*, MAC).
El adaptador de red realiza las siguientes funciones:
1• Recibe datos desde el sistema operativo del equipo y los convierte en señales eléctricas que se transmiten por el cable
2• Recibe señales eléctricas del cable y las traduce en datos que el sistema operativo del equipo puede entender
3• Determina si los datos recibidos del cable son para el equipo
4• Controla el flujo de datos entre el equipo y el sistema de cable

Para garantizar la compatibilidad entre el equipo y la red, el adaptador de red debe cumplir los siguientes criterios:

1• Ser apropiado en función del tipo de ranura de expansión del equipo
2• Utilizar el tipo de conector de cable correcto para el cableado
3• Estar soportado por el sistema operativo del equipo.

1.1.4.2 Cables de red

Dentro de los medios utilizados para conectividad se encuentran los cables de cobre los cuales se utilizan en casi todas las LAN. Los cables tienen distintas especificaciones y generan distintas expectativas acerca de su rendimiento, un factor de importancia es la velocidad de transmisión de bits, por otra parte la transmisión puede ser transmisión digital o de banda base o transmisión analógica o de banda ancha.
Los tipos de cables mas utilizados son:

El cable de par trenzado es el tipo más habitual utilizado en redes.
El cable coaxial se utiliza cuando los datos viajan por largas distancias.
El cable de fibra óptica se utiliza cuando necesitamos que los datos viajen a la velocidad de la luz.

Al conectar equipos para formar una red utilizamos cables que actúan como medio de transmisión de la red para transportar las señales entre los equipos. Un cable que conecta dos equipos o componentes de red se denomina *segmento*. Los cables se diferencian por sus capacidades y están clasificados en función de su capacidad para transmitir datos a diferentes velocidades, con diferentes índices de error. Las tres clasificaciones principales de cables que conectan la mayoría de redes son: **de par trenzado, coaxial y fibra óptica**.

Algunos ejemplos de las especificaciones de Ethernet que están relacionadas con el tipo de cable son:

- 10BASE-T
- 10BASE5
- 10BASE2

10BASE-T se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base o digitalmente interpretada. T significa par trenzado.

10BASE5 se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base o digitalmente interpretada. El 5 representa la capacidad que tiene el cable para permitir que la señal recorra aproximadamente 500 metros antes de que la atenuación interfiera con la capacidad del receptor de interpretar correctamente la señal recibida. 10BASE5 a menudo se denomina "Thicknet". Thicknet es, en realidad, un tipo de red, mientras que 10BASE5 es el cableado que se utiliza en dicha red.

10BASE2 se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base o digitalmente interpretada. El 2, en 10BASE2, se refiere a la longitud máxima aproximada del segmento de 200 metros antes que la atenuación perjudique la habilidad del receptor para interpretar apropiadamente la señal que se recibe. La longitud máxima del segmeto es en reallidad 185 metros. 10BASE2 a menudo se denomina "Thinnet". Thinnet es, en realidad, un tipo de red, mientras que 10BASE2 es el cableado que se utiliza en dicha red.

- **Cable de par trenzado**

El cable de par trenzado (10baseT) está formado por dos hebras aisladas de hilo de cobre trenzado entre sí. Existen dos tipos de cables de par trenzado: par trenzado sin apantallar (*unshielded twisted pair*, **UTP**) y par trenzado apantallado (*shielded twisted pair*, **STP**). Éstos son los cables que más se utilizan en redes y pueden transportar señales en distancias de 100 metros.

- El cable UTP es el tipo de cable de par trenzado más popular y también es el cable en una LAN más popular.
- El cable STP utiliza un tejido de funda de cobre trenzado que es más protector y de mejor calidad que la funda utilizada por UTP. STP también utiliza un envoltorio plateado alrededor de cada par de cables. Con ello, STP dispone de una excelente protección que protege a los datos transmitidos de interferencias exteriores, permitiendo que STP soporte índices de transmisión más altos a través de mayores distancias que UTP.

El cableado de par trenzado utiliza conectores Registered Jack 45 (RJ-45) para conectarse a un equipo. Son similares a los conectores Registered Jack 11 (RJ-11).

- **Cable Coaxial**

El cable coaxial está formado por un núcleo de hilo de cobre rodeado de un aislamiento, una capa de metal trenzado, y una cubierta exterior. El núcleo de un cable coaxial transporta las señales eléctricas que forman los datos. Este hilo del núcleo puede ser sólido o hebrado. Existen dos tipos de cable coaxial: cable coaxial ThinNet (10Base2) y cable coaxial ThickNet (10Base5). El cableado coaxial es una buena elección cuando se transmiten datos a través de largas distancias y para ofrecer un soporte fiable a mayores velocidades de transferencia cuando se utiliza equipamiento menos sofisticado.

El cable coaxial debe tener terminaciones en cada extremo.

- El cable coaxial ThinNet puede transportar una señal en una distancia aproximada de 185 metros.
- El cable coaxial ThickNet puede transportar una señal en una distancia de 500 metros. Ambos cables, ThinNet y ThickNet, utilizan un componente de conexión (conector BNC) para realizar las conexiones entre el cable y los equipos.

- **Cable de fibra óptica**

La fibra óptica es el medio mas utilizado en los transmisores de punto a punto de mayor distancia y alto ancho de banda que requieren los backbones de LAN y WAN.

El cable de fibra óptica utiliza fibras ópticas para transportar señales de datos digitales en forma de pulsos modulados de luz. Como el cable de fibra óptica no transporta impulsos eléctricos, la señal no puede ser intervenida y sus datos no pueden ser robados. El cable de fibra óptica es adecuado para transmisiones de datos de gran velocidad y capacidad ya que la señal se transmite muy rápidamente y con muy poca interferencia. Un inconveniente del cable de fibra óptica es que se rompe fácilmente si la instalación no se hace cuidadosamente. Es más difícil de cortar que otros cables y requiere un equipo especial para cortarlo.

1.1.4.3 Dispositivos de comunicación inalámbricos

Los componentes inalámbricos se utilizan para la conexión a redes en distancias que hacen que el uso de adaptadores de red y opciones de cableado estándares sea técnica o económicamente imposible. Las redes inalámbricas están formadas por componentes inalámbricos que se comunican con LANs.
Excepto por el hecho de que no es un cable quién conecta los equipos, una red inalámbrica típica funciona casi igual que una red con cables: se instala en cada equipo un adaptador de red inalámbrico con un *transceptor* (un dispositivo que transmite y recibe señales analógicas y digitales). Los usuarios se comunican con la red igual que si estuvieran utilizando un equipo con cables.

Salvo por la tecnología que utiliza, una red inalámbrica típica funciona casi igual que una red de cables: se instala en cada equipo un adaptador de red inalámbrico con un *transceptor*, y los usuarios se comunican con la red como si estuvieran utilizando un equipo con cables.
Existen dos técnicas habituales para la transmisión inalámbrica en una LAN: transmisión por infrarrojos y transmisión de radio en banda estrecha.

• Transmisión por infrarrojos

Funciona utilizando un haz de luz infrarroja que transporta los datos entre dispositivos. Debe existir visibilidad directa entre los dispositivos que transmiten y los que reciben; si hay algo que bloquee la señal infrarroja, puede impedir la comunicación. Estos sistemas deben generar señales muy potentes, ya que las señales de transmisión débiles son susceptibles de recibir interferencias de fuentes de luz, como ventanas.

• Transmisión vía radio en banda estrecha

El usuario sintoniza el transmisor y el receptor a una determinada frecuencia. La radio en banda estrecha no requiere visibilidad directa porque utiliza ondas de radio. Sin embargo la transmisión vía radio en banda estrecha está sujeta a interferencias de paredes de acero

e influencias de carga. La radio en banda estrecha utiliza un servicio de suscripción. Los usuarios pagan una cuota por la transmisión de radio.

1.2 El Modelo de referencia OSI

Para evitar problemas de interoperabilidad entre redes de distintos fabricantes, la Organización Internacional de Estándares[13] (ISO, por sus siglas en inglés) creó un conjunto de normas que conforman un modelo de referencia. Dicho modelo se conoce como Modelo OSI (*Open System Interconection*).

El Modelo OSI es un lineamiento funcional para tareas de comunicaciones y, por consiguiente, no especifica un estándar de comunicación para dichas tareas. Sin embargo, muchos estándares y protocolos cumplen con los lineamientos del Modelo OSI.

Este modelo está compuesto por una estructura multinivel, con la idea de que cada nivel se dedique a resolver una parte de la comunicación.

El nivel superior utiliza los servicios de los niveles inferiores. Cada nivel se comunica con su similar en otras computadoras, pero debe hacerlo enviando un mensaje a través de los niveles inferiores en la misma computadora. La comunicación internivel está bien definida. El nivel N utiliza los servicios del nivel N-1 y proporciona servicios al nivel N+1. Sin embargo cada nivel es independiente de los demás niveles o capas, tanto inferiores como superiores.

En cada nivel, se incorpora al mensaje un formato de control. Este elemento de control permite que un nivel en la computadora receptora se entere de que su similar en la computadora emisora esta enviándole información. Cualquier nivel dado, puede incorporar un encabezado al mensaje.

[13] www.iso.ch

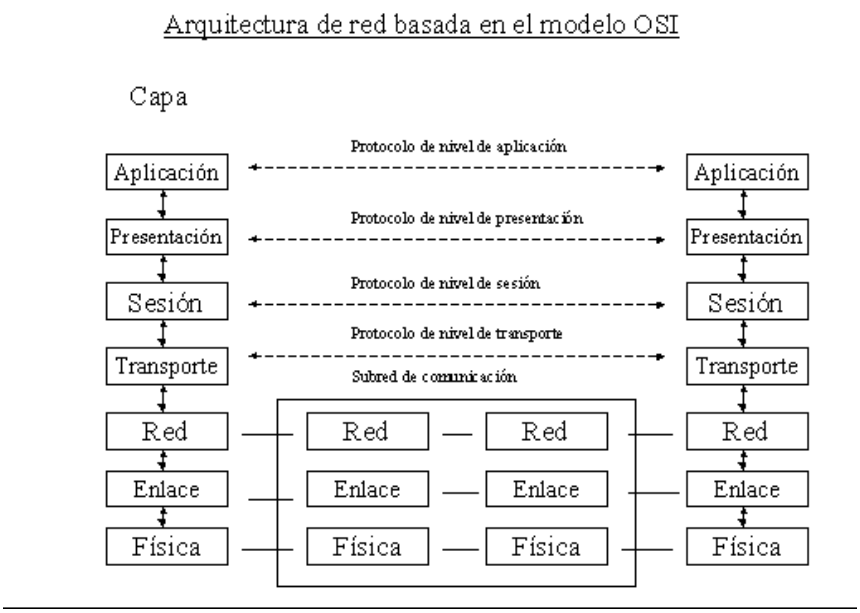


Figura 1.2a

1.2.1 Capas del Modelo OSI

Este modelo está compuesto por siete capas o niveles, las cuales son:

1. *Capa física (de acceso de red)*

Se ocupa de las propiedades físicas, características eléctricas y mecánicas de los diversos componentes de interconexión, asi como de la velocidad de transmisión y si ésta es unidireccional o bidireccional (*simplex, duplex* o *full-duplex*).

Se encarga de transformar un paquete de información binaria en una sucesión de impulsos adecuados al medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos (transmisión por cable), electromagnéticos (transmisión *Wireless*) o luminosos (transmisión óptica). Cuando actúa en modo recepción el trabajo es inverso, se encarga de transformar estos impulsos en paquetes de datos binarios que serán entregados a la capa de enlace.

2. *Capa de enlace de datos*

La capa de enlace de datos se ocupa del direccionamiento físico, de la topología de la red, del acceso a la misma, de la distribución ordenada de tramas y del control del flujo.

Además del direccionamiento fisico, se ocupa de la detección y control de errores ocurridos en la capa física, del control del acceso a dicha capa y de la integridad de los datos y fiabilidad de la transmisión. Para esto agrupa la información a transmitir en bloques, e incluye a cada uno una suma de control que permitirá al receptor comprobar su integridad. Las tramas recibidas son comprobadas por el receptor. Si alguna trama se ha corrompido se envía un mensaje de control al remitente solicitando su reenvío.

3. Capa de red

Encargada de enrutar los equipos, para llevar los datos desde un origen hacia un destino. Definiendo destino como un punto valido en la red donde los datos pueden llegar y ser enviados. En esta capa se proporciona conectividad y la selección de la ruta para la comunicación equipos de red.

Sus funciones principales son las dividir la información de la capa de transporte en unidades mas complejas, llamadas paquetes, a los cuales se les asignan las direcciones lógicas entre los equipos que se quieran comunicar.

Generalmente en esta capa se encuentran los routers (enrutadores de red), dispositivos que tienen las direcciones de una red y el enlace que conduce a ellas.

4. Capa de transporte

En esta capa se dividen los datos originados en el equipo de origen, en pedazos denominados segmentos los cuales se reensamblan en el equipo de destino. Esta división se hace para poder pasar la información por medio de la capa inferior.

Esta capa además, pretende aislar las capas superiores de los detalles de las tres capas inferiores del modelo OSI, con el objetivo de transferir los datos de una manera segura y confiable.

5. Capa de sesión

Proporciona el medio necesario para que los equipos que se están comunicando por red organicen, sincronicen su diálogo y procedan al intercambio de datos. Es decir que establece, mantiene y sincroniza la interacción entre los sistemas.

Entre sus funciones se encuentran las de hacer *checkpoints*, que son puntos de recuerdo en la transferencia de datos, necesarios para la correcta recuperación de sesiones perdidas. Si por algún motivo una sesión falla por cualquier causa ajena al usuario, restaurar la sesión a partir de un punto seguro y sin perdida de datos o, si esto no es posible, terminar la sesión de una manera ordenada, chequeando y recuperando todas sus funciones.

6. Capa de presentación

Se encarga de la sintaxis y la semántica de la información intercambiada entre dos sistemas. Garantiza que la información que envía la capa de aplicación de un sistema pueda ser entendida y utilizada por la capa de aplicación de otro, estableciendo el contexto sintáctico del diálogo.

Esta capa se ocupa de los aspectos semánticos de la comunicación, estableciendo los arreglos necesarios para que puedan comunicar máquinas que utilicen diversa representación interna para los datos. Describe como pueden transferirse números de coma flotante entre equipos que utilizan distintos formatos matemáticos.

7. *Capa de aplicación*

Proporciona a las aplicaciones servicios de red, asi como protocolos de transferencia. Algunos de los protocolos utilizados por los programas de esta capa son HTTP, SMTP, POP, IMAP.

Es frecuente encontrar el término interfaz de programa de aplicación (API) asociado a los servicios de la capa de aplicación. Un API es un conjunto de reglas que permiten que las aplicaciones escritas por los usuarios puedan acceder a los servicios de un sistema de software. Los diseñadores de programas y protocolos suelen proporcionar varias API para que los programadores puedan adaptar fácilmente sus aplicaciones y utilizar los servicios disponibles en sus productos.

1.2.2 TCP/IP vs Modelo OSI

El Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP) es un conjunto de protocolos aceptados por la industria que permiten la comunicación en un entorno heterogéneo (formado por elementos diferentes).

TCP/IP permite acceder a Internet y a sus recursos. Además se ha convertido en el protocolo estándar para la interoperabilidad entre distintos tipos de equipos.

Entre otros protocolos escritos específicamente para el conjunto TCP/IP se incluyen:

- SMTP: Protocolo básico de transferencia de correo electrónico.
- FTP: Protocolo de transferencia de archivos, es utilizado para la interconexión de archivos entre equipos que ejecutan TCP/IP.
- SNMP: Protocolo básico de gestión de red.

TCP/IP ha sido diseñado para ser enrutado, robusto y funcionalmente eficiente. Fue desarrollado por el Departamento de Defensa de Estados Unidos como un conjunto de protocolos para redes de área extensa (WAN). Su propósito era el de mantener enlaces de comunicación entre sitios en el caso de una guerra nuclear. Actualmente, la responsabilidad del desarrollo de TCP/IP reside en la propia comunidad de Internet. La utilización de TCP/IP ofrece varias ventajas:

- Es un estándar en la industria. Como un estándar de la industria, es un protocolo abierto. Esto quiere decir que no está controlado por una única compañía, y está menos sujeto a cuestiones de compatibilidad.

- Contiene un conjunto de utilidades para la conexión de sistemas operativos diferentes. La conectividad entre un equipo y otro no depende del sistema operativo de red que esté utilizando cada equipo.

- Utiliza una arquitectura escalable, cliente/servidor. TCP/IP puede ampliarse (o reducirse) para ajustarse a las necesidades y circunstancias futuras. Utiliza sockets para hacer que el sistema operativo sea algo transparente.

El protocolo TCP/IP no corresponde directamente con el modelo de referencia OSI. Este protocolo se fundamenta en 4 capas o niveles: interfaz de red, Internet, transporte y aplicación.

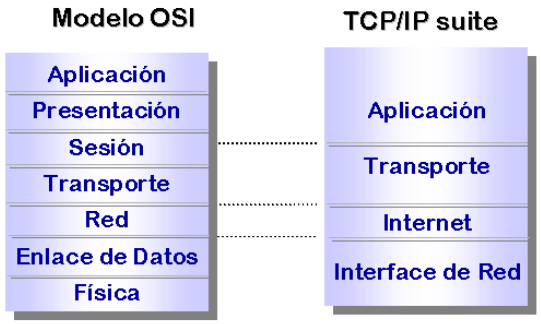


Figura 1.2b

1. *Nivel de interfaz de red*

Corresponde con los dos primeros niveles del modelo OSI. Se comunica directamente con la red. Proporciona la interfaz entre la arquitectura de red (como Token Ring, Ethernet) y el nivel Internet (siguiente nivel del protocolo).

2. *Nivel Internet*

Corresponde con la capa de red del modelo OSI. Provee la funcionalidad para las comunicaciones entre redes. Para realizar esto la capa de Internet depende del Protocolo de Internet (IP) principalmente, aunque hay mas protocolos que se utilizan en este nivel (ARP, RARP, etc.).

2.1 Protocolo Internet (IP)

El Protocolo Internet (IP) es un protocolo de conmutación de paquetes que realiza direccionamiento y enrutamiento. Cuando se transmite un paquete, este protocolo añade una cabecera al paquete, de forma que pueda enviarse a través de la red utilizando las tablas de encaminamiento dinámico. IP es un protocolo no orientado a la conexión y envía paquetes sin esperar la señal de confirmación por parte del receptor.

3. Nivel de transporte

Corresponde al nivel de transporte de modelo OSI. Nivel encargado de las comunicaciones de la red, establece y mantiene la comunicación entre dos equipos.

El nivel de transporte proporciona notificación de la recepción, control de flujo y secuenciación de paquetes.

Esta capa utiliza dos protocolos para realizar esta tarea: TCP (Transmission Control Protocol) y UDP (User Datagram Protocol).

3.1 TCP

Encargado de dividir el mensaje original en datagramas de menor tamaño, y por lo tanto, mucho más manejables. Los datagramas serán dirigidos a través del protocolo IP de forma individual. El protocolo TCP se encarga además de añadir cierta información necesaria a cada uno de los datagramas. Esta información se añade al inicio de los datos que componen el datagrama en forma de cabecera.

Es un protocolo orientado a la conexión y establece una conexión (también conocida como una sesión, circuito virtual o enlace) entre dos máquinas antes de transferir ningún dato. Para establecer una conexión fiable, TCP utiliza lo que se conoce como «acuerdo en tres pasos». Establece el número de puerto y los números de secuencia de inicio desde ambos lados de la transmisión. El acuerdo consta de tres pasos:

1. El solicitante envía al servidor un paquete especificando el número de puerto que él planea utilizar y el número de secuencia inicial (ISN).
2. El servidor responde con su ISN, que consiste en el ISN del solicitante más uno.
3. El solicitante responde a la respuesta del servidor con el ISN del servidor más uno.

3.2 UDP

A diferencia de TCP, UDP no establece una conexión, es decir es un protocolo no orientado a conexión. Cuando se utiliza UDP la garantía de que un paquete llegue a su destino es mucho menor que con TCP debido a que no se utilizan las señales de confirmación.

El protocolo de datagramas de usuario puede ser la alternativa al TCP en algunos casos en los que no sea necesario el gran nivel de complejidad proporcionado por el TCP. Puesto que UDP no admite numeración de los datagramas, éste protocolo se utiliza principalmente cuando el orden en que se reciben los mismos no es un factor fundamental, o también cuando se quiere enviar información de poco tamaño que cabe en un único datagrama.

4. *Nivel de aplicación*

El nivel de aplicación se corresponde con los niveles de sesión, presentación y aplicación del modelo OSI, y conecta las aplicaciones a la red.

Esta capa incluye todas las aplicaciones que hacen uso de la capa de transporte para enviar y recibir datos tales como RSH (remote Shell), REXEC (Remote Execute), TELNET, FTP, rlogin, DNS, NFS, etc.

1.3 Protocolos de red

1.3.1 Características

Un protocolo es el conjunto de normas para comunicarse dos o más entidades (objetos que se intercambian información) . Los elementos que definen un protocolo son:

- Sintaxis: formato, codificación y niveles de señal de datos.
- Semántica: información de control y gestión de errores.
- Temporización: coordinación entre la velocidad y orden secuencial de las señales.

Un protocolo es realmente un software que reside en la memoria de una computadora o en la memoria de un dispositivo de transmisión, como una tarjeta de red. Cuando los datos están listos para transmitirse, este software es ejecutado. EL software prepara los datos para la transmisión y configura la transmisión en movimiento. En la parte receptora, el software toma los datos y los prepara para la computadora, desechando toda la información agregada, y tomando sólo la información útil.

Las características más importantes de un protocolo son:

- Directo/indirecto: los enlaces punto a punto son directos pero los enlaces entre dos entidades en diferentes redes son indirectos ya que intervienen elementos intermedios.
- Monolítico/estructurado: monolítico es aquel en que el emisor tiene el control en una sola capa de todo el proceso de transferencia. En protocolos estructurados, hay varias capas que se coordinan y que dividen la tarea de comunicación.
- Simétrico/asimétrico: los simétricos son aquellos en que las dos entidades que se comunican son semejantes en cuanto a poder tanto emisores como consumidores de información. Un protocolo es asimétrico si una de las entidades tiene funciones diferentes de la otra (por ejemplo en clientes y servidores).

1.3.2 Funciones básicas

1. Segmentación y ensamblado: generalmente es necesario dividir los bloques de datos en unidades pequeñas e iguales en tamaño, y este proceso se le llama segmentación. El bloque básico de segmento en una cierta capa de un protocolo se le llama PDU (Unidad de datos de protocolo). La necesidad de la utilización de bloque es por:
La red sólo admite la transmisión de bloques de un cierto tamaño.
El control de errores es más eficiente para bloques pequeños.
Para evitar monopolización de la red para una entidad, se emplean bloques pequeños y así una compartición de la red.
Con bloques pequeños las necesidades de almacenamiento temporal son menores.
Hay ciertas desventajas en la utilización de segmentos:
La información de control necesaria en cada bloque disminuye la eficiencia en la transmisión.
Los receptores pueden necesitar interrupciones para recibir cada bloque, con lo que en bloques pequeños habrá más interrupciones.
Cuantas más PDU, más tiempo de procesamiento.

2. Encapsulado: se trata del proceso de adherir información de control al segmento de datos. Esta información de control es el direccionamiento del emisor/receptor, código de detección de errores y control de protocolo.

3. Control de conexión: hay bloques de datos sólo de control y otros de datos y control. Cuando se utilizan datagramas, todos los bloques incluyen control y datos ya que cada PDU se trata como independiente. En circuitos virtuales hay bloques de control que son los encargados de establecer la conexión del circuito virtual. Hay protocolos más sencillos y otros más complejos, por lo que los protocolos de los emisores y receptores deben de ser compatibles al menos .Además de la fase de establecimiento de conexión (en circuitos virtuales) está la fase de transferencia y la de corte de conexión . Si se utilizan circuitos virtuales habrá que numerar los PDU y llevar un control en el emisor y en el receptor de los números.

4. Entrega ordenada: el envío de PDU puede acarrear el problema de que si hay varios caminos posibles, lleguen al receptor PDU desordenados o repetidos, por lo que el receptor debe de tener un mecanismo para reordenar los PDU. Hay sistemas que tienen un mecanismo de numeración con módulo algún número; esto hace que el módulo sean lo suficientemente alto como para que sea imposible que haya dos segmentos en la red al mismo tiempo y con el mismo número.

5. Control de flujo: hay controles de flujo de parada y espera o de ventana deslizante. El control de flujo es necesario en varios protocolos o capas, ya que el problema de saturación del receptor se puede producir en cualquier capa del protocolo.

6. Control de errores: generalmente se utiliza un temporizador para retransmitir una trama una vez que no se ha recibido confirmación después de expirar el tiempo del temporizador. Cada capa de protocolo debe de tener su propio control de errores.

7. Direccionamiento: cada estación o dispositivo intermedio de almacenamiento debe tener una dirección única. A su vez, en cada terminal o sistema final puede haber varios agentes o programas que utilizan la red, por lo que cada uno de ellos tiene asociado un puerto.
   Además de estas direcciones globales, cada estación o terminal de una subred debe de tener una dirección de subred (generalmente en el nivel MAC).

   Hay ocasiones en las que se usa un identificador de conexión; esto se hace así cuando dos estaciones establecen un circuito virtual y a esa conexión la numeran (con un identificador de conexión conocido por ambas). La utilización de este identificador simplifica los mecanismos de envío de datos ya que por ejemplo es más sencillo que el direccionamiento global.

   Algunas veces se hace necesario que un emisor emita hacia varias entidades a la vez y para eso se les asigna un direccionamiento similar a todas.

8. Multiplexación: es posible multiplexar las conexiones de una capa hacia otra, es decir que de una única conexión de una capa superior, se pueden establecer varias conexiones en una capa inferior (y al revés).

9. Servicios de transmisión: los servicios que puede prestar un protocolo son:
   - Prioridad: hay mensajes (los de control) que deben tener prioridad respecto a otros.
   - Grado de servicio: hay datos que deben de retardarse y otros acelerarse (vídeo).
   - Seguridad.

1.3.3 Funcionamiento de un protocolo

Un protocolo sirve de medio de interacción entre dos o más unidades, por ejemplo si se posee dos unidades transmisor y receptor el protocolo posibilita una serie de pasos para hacer efectiva una comunicación.
Paso 1 el transmisor envía un bloque de datos x hacia el receptor, el receptor recibe el bloque de datos correctamente y envía un ACK (*Ackowledge* o reconocimiento), indicándole que se recibió con éxito el paquete de comunicación.

Paso 1: el transmisor recibe un ACK y envía el siguiente bloque de datos.

Paso 3: si el receptor recibe un bloque de dato y detecta un error el mismo envía un mensaje de NACK (*No Acknowledge* o No reconocimiento), indicándole al transmisor que existió un error y que debe enviar el dato nuevamente.

Paso 4: el transmisor retransmite el bloque de datos al receptor para el correcto procesamiento de este.

Paso 5: el receptor recibe el bloque de datos retransmitido y si no detecta un error nuevamente le envía al transmisor un ACK para indicarle que el bloque de datos fue recibido con éxito.

1.4 Equipos de interconexión

Los equipos que se conectan en forma directa a un segmento de red se denominan dispositivos, estos dispositivos se clasifican en dispositivos de usuario final y dispositivos de red.
Los dispositivos de usuario final incluyen ordenadores, impresoras, escáneres y demás dispositivos que brindan servicios directamente al usuario. Los dispositivos de red son todos aquellos que se conectan entre si para posibilitar la intercomunicación entre los dispositivos de usuario final.

Los dispositivos de usuario final que conectan a los usuarios con la red se conocen con el nombre de *hosts*. Estos dispositivos permiten a los usuarios compartir, crear y obtener información. Los dispositivos *host* pueden existir sin una red, pero sin la red las capacidades de los *hosts* se ven sumamente limitadas. Los dispositivos *host* están físicamente conectados con los medios de red mediante una tarjeta de interfaz de red (NIC). Utilizan esta conexión para realizar las tareas de envío de correo electrónico, impresión de documentos, escaneado de imágenes o acceso a bases de datos. Cada NIC individual tiene un código único, denominado dirección de control de acceso al medio

(MAC). Esta dirección se utiliza para controlar la comunicación de datos para el *host* de la red.

Los dispositivos de red son los que transportan los datos que deben transferirse entre dispositivos de usuario final. Los dispositivos de red proporcionan el tendido de las conexiones de cable, la concentración de conexiones, la conversión de los formatos de datos y la administración de transferencia de datos. Algunos ejemplos de dispositivos que ejecutan estas funciones son los repetidores, hubs, puentes, switches y routers.

Un repetidor es un dispositivo de red que se utiliza para regenerar una señal. Los repetidores regeneran señales analógicas o digitales que se distorsionan a causa de pérdidas en la transmisión producidas por la atenuación. Un repetidor no toma decisiones inteligentes acerca del envío de paquetes como lo hace un router o puente.

Los hubs concentran las conexiones. En otras palabras, permiten que la red trate un grupo de hosts como si fuera una sola unidad. Esto sucede de manera pasiva, sin interferir en la transmisión de datos. Los hubs activos no sólo concentran hosts, sino que además regeneran señales.

Los puentes convierten los formatos de transmisión de datos de la red, además de realizar la administración básica de la transmisión de datos. Los puentes, tal como su nombre lo indica, proporcionan las conexiones entre LAN. Los puentes no sólo conectan las LAN, sino que además verifican los datos para determinar si les corresponde o no cruzar el puente. Esto aumenta la eficiencia de cada parte de la red.

Los switches de grupos de trabajo agregan inteligencia a la administración de transferencia de datos. No sólo son capaces de determinar si los datos deben permanecer o no en una LAN, sino que pueden transferir los datos únicamente a la conexión que necesita esos datos. Otra diferencia entre un puente y un switch es que un switch no convierte formatos de transmisión de datos.

Los routers poseen todas las capacidades indicadas arriba. Los routers pueden regenerar señales, concentrar múltiples conexiones, convertir formatos de transmisión de datos, y manejar transferencias de datos. También pueden conectarse a una WAN, lo que les permite conectar LAN que se encuentran separadas por grandes distancias. Ninguno de los demás dispositivos puede proporcionar este tipo de conexión.

1.5 Direccionamiento IP

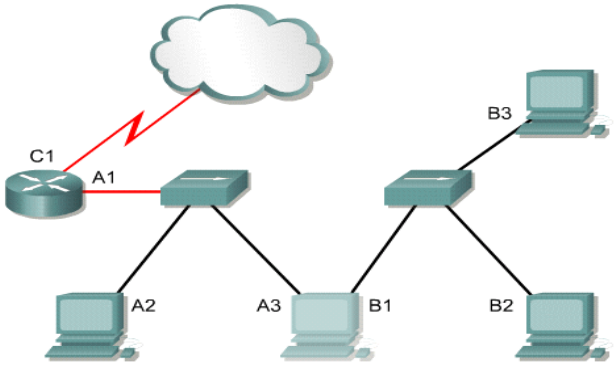


Figura 1.5a

Una dirección IP es una secuencia de unos y ceros de 32 bits. La Figura 1.5b muestra un número de 32 bits de muestra.

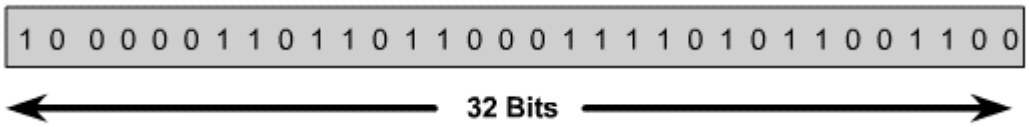


Figura 1.5b

Para que el uso de la dirección IP sea más sencillo, en general, la dirección aparece escrita en forma de cuatro números decimales separados por puntos. Por ejemplo, la dirección IP de un computador es 192.168.1.2. Otro computador podría tener la dirección 128.10.2.1. Esta forma de escribir una dirección se conoce como formato decimal punteado.
En esta notación, cada dirección IP se escribe en cuatro partes separadas por puntos. Cada parte de la dirección se conoce como octeto porque se compone de ocho dígitos binarios. Por ejemplo, la dirección IP 192.168.1.8 sería 11000000.10101000.00000001.00001000 en una notación binaria. La notación decimal punteada es un método más sencillo de comprender que el método binario de unos y ceros.
Esta notación decimal punteada también evita que se produzca una gran cantidad de errores por transposición, que sí se produciría si sólo se utilizaran números binarios. El uso de decimales separados por puntos permite una mejor comprensión de los patrones numéricos.
Tanto los números binarios como los decimales de la Figura 1.5c representan a los mismos valores, pero resulta más sencillo apreciar la notación decimal punteada.

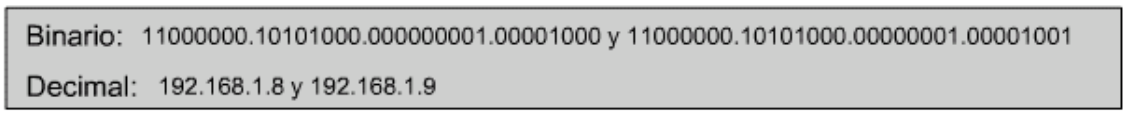


Figura 1.5c.

Los números binarios y decimales representan los mismos valores pero es mucho más fácil ver con los valores decimales punteados. Este es uno de los problemas mas comunes encontrados al trabajar directamente con loe números binarios. Las cadenas de unos y ceros repetidos aumentan la probabilidad de errores de transposición y omisión.

Este es uno de los problemas frecuentes que se encuentran al trabajar directamente con números binarios. Las largas cadenas de unos y ceros que se repiten hacen que sea más probable que se produzcan errores de transposición y omisión.
Resulta más sencillo observar la relación entre los números 192.168.1.8 y 192.168.1.9, mientras que 11000000.10101000.00000001.00001000 y 11000000.10101000.00000001.00001001 no son fáciles de reconocer. Al observar los binarios, resulta casi imposible apreciar que son números consecutivos.

DIRECCIONAMIENTO IPV4

Un Router envía los paquetes desde la red origen a la red destino utilizando el protocolo IP. Los paquetes deben incluir un identificador tanto para la red origen como para la red destino.

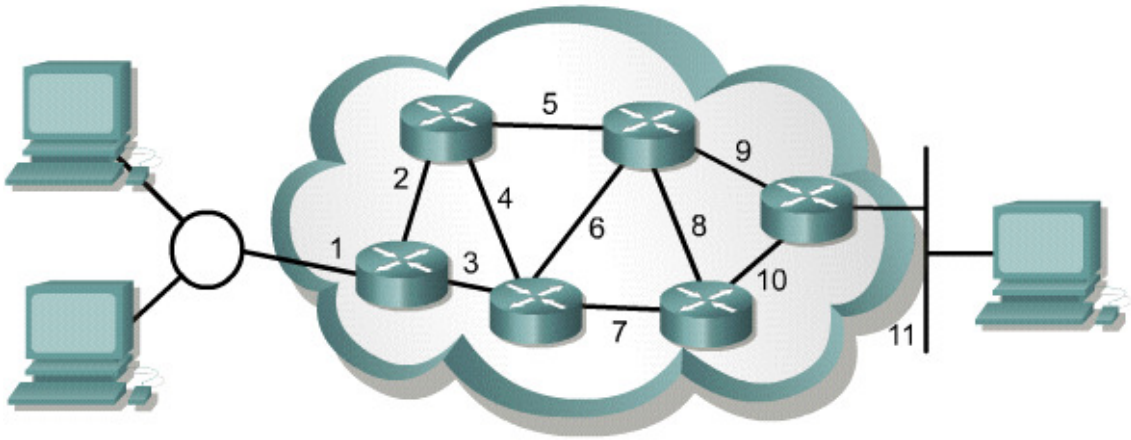
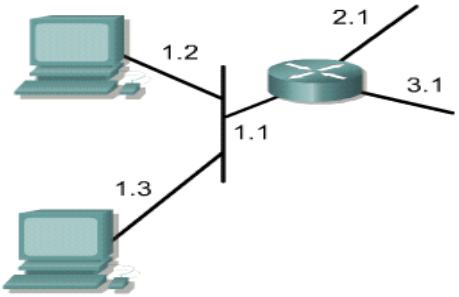


Figura 1.5d. Las direcciones representan la ruta de las conexiones entre medios.

Utilizando la dirección IP de una red destino, un Router puede enviar un paquete a la red correcta. Cuando un paquete llega a un Router conectado a la red destino, este utiliza la dirección IP para localizar el computador en particular conectado a la red.
Este sistema funciona de la misma forma que un sistema nacional de correo. Cuando se envía una carta, primero debe enviarse a la oficina de correos de la ciudad destino, utilizando el código postal. Dicha oficina debe entonces localizar el destino final en la misma ciudad utilizando el domicilio. Es un proceso de dos pasos.

De igual manera, cada dirección IP consta de dos partes. Una parte identifica la red donde se conecta el sistema y la segunda identifica el sistema en particular de esa red.

Figura 1.5e.



Red	Host
1	1 2 3
2	1
3	1

Como muestra la Figura, cada octeto varía de 0 a 255. Cada uno de los octetos se divide en 256 subgrupos y éstos, a su vez, se dividen en otros 256 subgrupos con 256 direcciones cada uno. Al referirse a una dirección de grupo inmediatamente arriba de un grupo en la jerarquía, se puede hacer referencia a todos los grupos que se ramifican a partir de dicha dirección como si fueran una sola unidad.

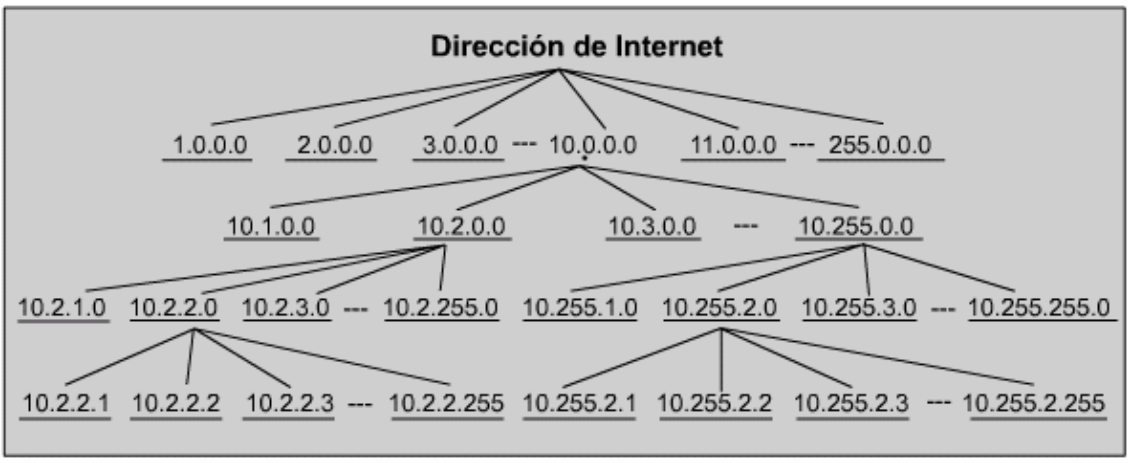


Figura 1.5f.

Este tipo de dirección recibe el nombre de dirección jerárquica porque contiene diferentes niveles. Una dirección IP combina estos dos identificadores en un solo número. Este número debe ser un número exclusivo, porque las direcciones repetidas harían imposible el enrutamiento.

La primera parte identifica la dirección de la red del sistema. La segunda parte, la parte del host, identifica qué máquina en particular de la red.

Las direcciones IP se dividen en clases para definir las redes de tamaño pequeño, mediano y grande. Las direcciones Clase A se asignan a las redes de mayor tamaño. Las

direcciones Clase B se utilizan para las redes de tamaño medio y las de Clase C para redes pequeñas.

Clase de dirección	Cantidad de redes	Cantidad de hosts por red
A	126 *	16,777,216
B	16, 384	65,535
C	2,097,152	254
D (Multicast)	No es aplicable	No es aplicable

Tabla 1.5a. *El intervalo de direcciones 127.x.x.x esta reservado como dirección de loopback, con propósitos de prueba y diagnostico.

Clase de dirección IP:	Bits de mayor peso	Primer intervalo de dirección de octeto	Número de bits en la dirección de red
Clase A	0	0 - 127 *	8
Clase B	10	128 - 191	16
Clase C	110	192 - 223	24
Clase D	1110	224 - 239	28

Tabla 1.5b.

El primer paso para determinar qué parte de la dirección identifica la red y qué parte identifica el host es identificar la clase de dirección IP.

Clase de dirección	Bits de mayor peso	Intervalo de dirección del primer octeto	Número de bits en la dirección de red	Número de redes	Número de hosts por red
Clase A	0	0-127	8	126	16,777,216
Clase B	10	128-191	16	16,384	65,536
Clase C	110	192-223	24	2,097,152	254
Clase D	1110	224-239	28	No es aplicable	No es aplicable

Tabla 1.5c.

DIRECCIONES IP CLASE A, B, C, D, Y E

Para adaptarse a redes de distintos tamaños y para ayudar a clasificarlas, las direcciones IP se dividen en grupos llamados clases.

Clase A	Red	Host		
Octet	1	2	3	4

Clase B	Red		Host	
Octet	1	2	3	4

Clase C	Red			Host
Octet	1	2	3	4

Clase D	Host			
Octet	1	2	3	4

Figura 1.5g. Las direcciones clase D se utilizan para grupos de multicast. No hay necesidad de asignar octetos o bits a las distintas direcciones de red o de host. Las direcciones clase E se reservan para fines de investigación solamente.

Esto se conoce como direccionamiento classful. Cada dirección IP completa de 32 bits se divide en la parte de la red y parte del host.

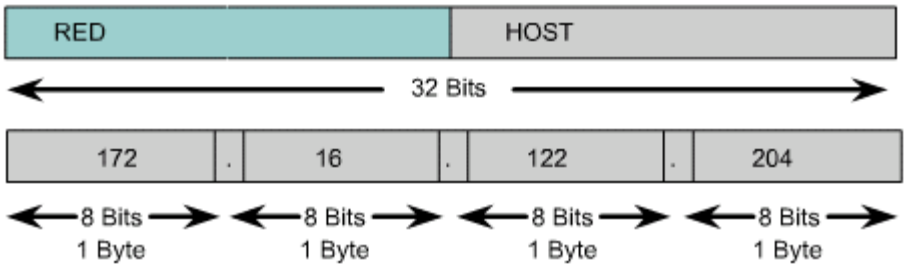


Figura 1.5h. Una dirección IP se divide en una parte de red y una parte de host. En n esquema de direccionamiento con clases, estas divisiones tienen lugar en los limites de los octetos.

Un bit o una secuencia de bits al inicio de cada dirección determinan su clase. Son cinco las clases de direcciones IP como muestra la tabla 1.5d.

Clase de dirección IP	Intervalo de dirección IP (Valor decimal d
Clase A	1-126 (00000001-01111110) *
Clase B	128-191 (10000000-10111111)
Clase C	192-223 (11000000-11011111)
Clase D	224-239 (11100000-11101111)
Clase E	240-255 (11110000-11111111)

Tabla 1.5d.

La dirección Clase A se diseñó para admitir redes de tamaño extremadamente grande, de más de 16 millones de direcciones de host disponibles.

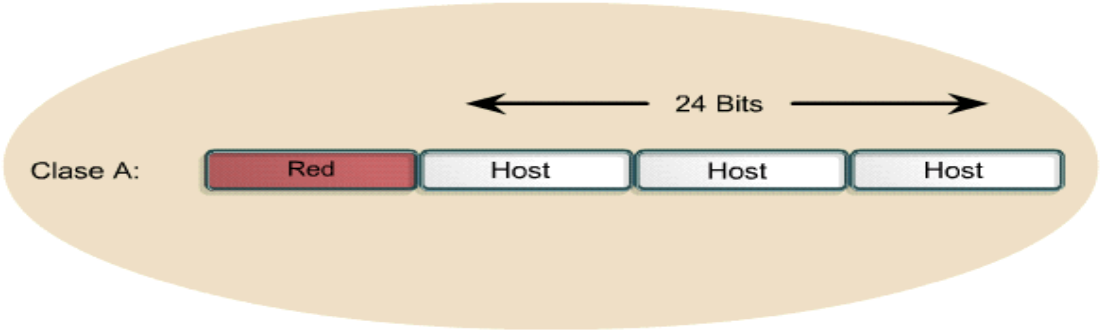


Figura 1.5i.

Las direcciones IP Clase A utilizan sólo el primer octeto para indicar la dirección de la red. Los tres octetos restantes son para las direcciones host.
El primer bit de la dirección Clase A siempre es 0. Con dicho primer bit, que es un 0, el menor número que se puede representar es 00000000, 0 decimal.
El valor más alto que se puede representar es 01111111, 127 decimal. Estos números 0 y 127 quedan reservados y no se pueden utilizar como direcciones de red. Cualquier dirección que comience con un valor entre 1 y 126 en el primer octeto es una dirección Clase A.
La red 127.0.0.0 se reserva para las pruebas de loopback. Los Routers o las máquinas locales pueden utilizar esta dirección para enviar paquetes nuevamente hacia ellos mismos. Por lo tanto, no se puede asignar este número a una red.
La dirección Clase B se diseñó para cumplir las necesidades de redes de tamaño moderado a grande. Una dirección IP Clase B utiliza los primeros dos de los cuatro octetos para indicar la dirección de la red. Los dos octetos restantes especifican las direcciones del host.

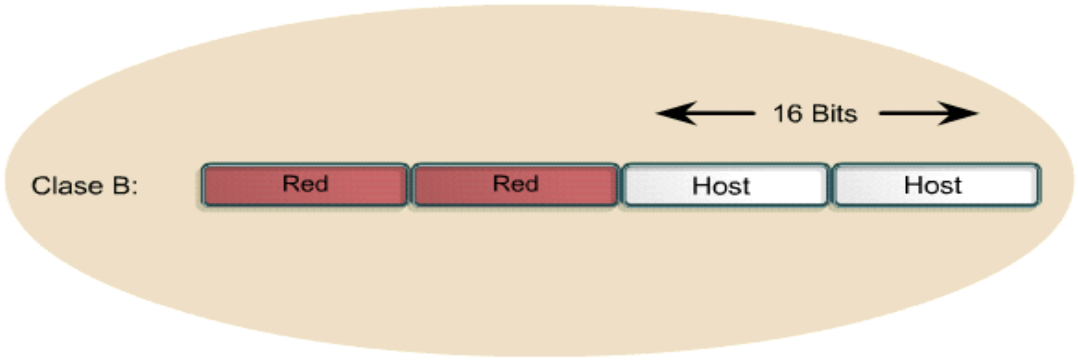


Figura 1.5j.

Los primeros dos bits del primer octeto de la dirección Clase B siempre son 10. Los seis bits restantes pueden poblarse con unos o ceros. Por lo tanto, el menor número que puede representarse en una dirección Clase B es 10000000, 128 decimal. El número más alto que puede representarse es 10111111, 191 decimal. Cualquier dirección que comience con un valor entre 128 y 191 en el primer octeto es una dirección Clase B.
El espacio de direccionamiento Clase C es el que se utiliza más frecuentemente en las clases de direcciones originales. Este espacio de direccionamiento tiene el propósito de admitir redes pequeñas con un máximo de 254 hosts.

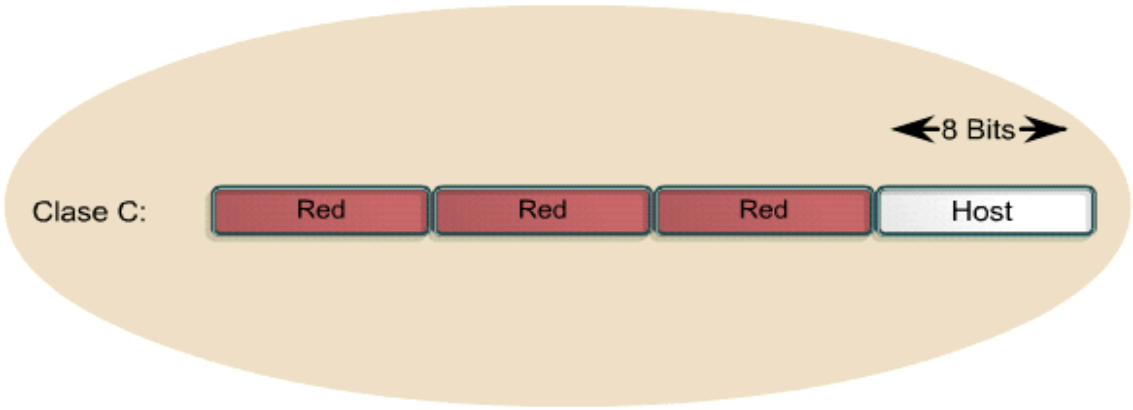


Figura 1.5k

Una dirección Clase C comienza con el binario 110. Por lo tanto, el menor número que puede representarse es 11000000, 192 decimal. El número más alto que puede representarse es 11011111, 223 decimal. Si una dirección contiene un número entre 192 y 223 en el primer octeto, es una dirección de Clase C.
La dirección Clase D se creó para permitir multicast en una dirección IP. Una dirección multicast es una dirección exclusiva de red que dirige los paquetes con esa dirección destino hacia grupos predefinidos de direcciones IP. Por lo tanto, una sola estación puede transmitir de forma simultánea una sola corriente de datos a múltiples receptores.

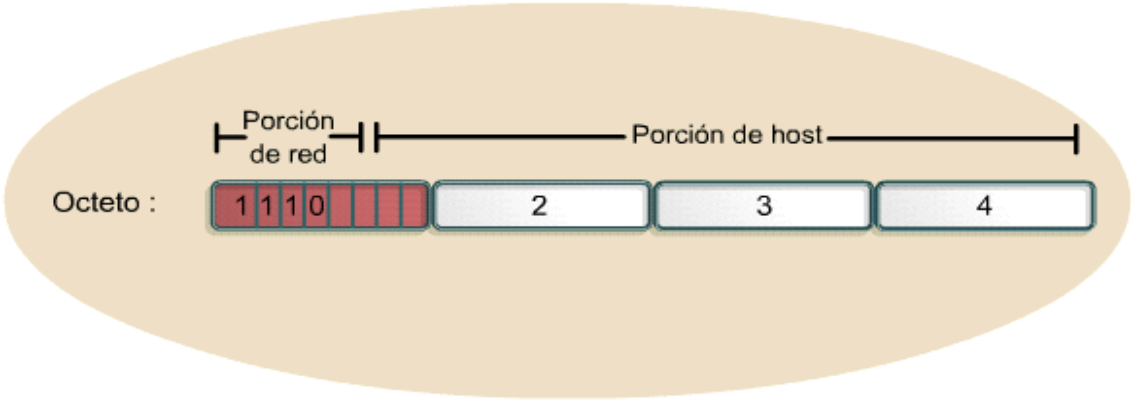


Figura 1.5l.

El espacio de direccionamiento Clase D, en forma similar a otros espacios de direccionamiento, se encuentra limitado matemáticamente. Los primeros cuatro bits de una dirección Clase D deben ser 1110. Por lo tanto, el primer rango de octeto para las direcciones Clase D es 11100000 a 11101111, o 224 a 239. Una dirección IP que comienza con un valor entre 224 y 239 en el primer octeto es una dirección Clase D.
Se ha definido una dirección Clase E. Sin embargo, la Fuerza de tareas de ingeniería de Internet (IETF) ha reservado estas direcciones para su propia investigación. Por lo tanto, no se han emitido direcciones Clase E para ser utilizadas en Internet. Los primeros cuatro bits de una dirección Clase E siempre son 1s. Por lo tanto, el rango del primer octeto para las direcciones Clase E es 11110000 a 11111111, o 240 a 255.

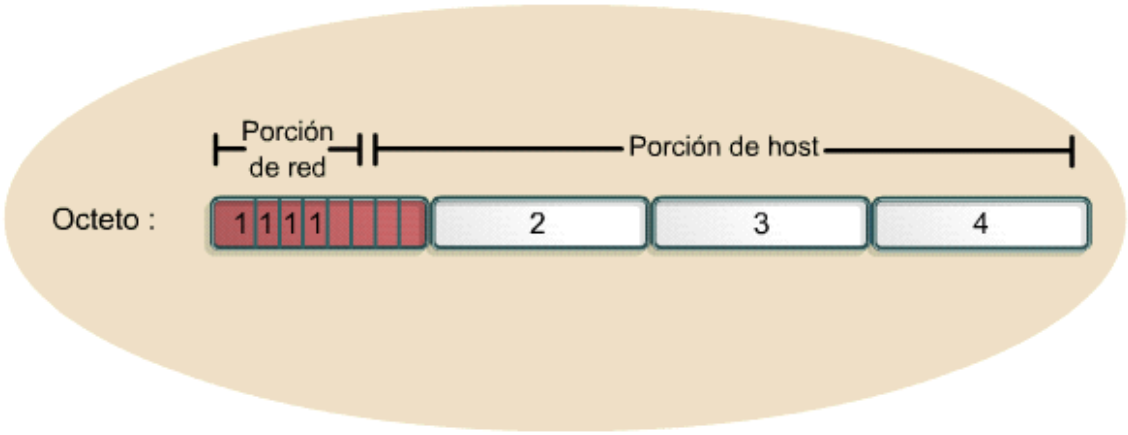


Figura 1.5m.

DIRECCIONAMIENTO IPV6

La característica principal de IPv6 es la utilización de direcciones de mucho mayor tamaño. El tamaño de una dirección en IPv6 es de 128 bits, que es cuatro veces mayor que el de una dirección de IPv4. Un espacio de direcciones de 32 bits permite 232 o 4.294.967.296 direcciones posibles. Un espacio de direcciones de 128 bits permite 2128 o 340.282.366.920.938.463.463.374.607.431.768.211.456 (3,4 x 1038) direcciones posibles.

A finales de la década de 1970, cuando se diseñó el espacio de direcciones IPv4, era inimaginable que se pudiera agotar. Sin embargo, debido a los cambios tecnológicos y una práctica de asignación que no anticipó la reciente aparición masiva de hosts en Internet, el espacio de direcciones IPv4 se fue agotando hasta el punto de que, en 1992, estaba claro que sería necesario reemplazarlo.
Con IPv6, es aún más difícil concebir el agotamiento del espacio de direcciones IPv6. Para ver el número con perspectiva, un espacio de direcciones de 128 bits proporciona 655.570.793.348.866.943.898.599 (6,5 x 1023) direcciones por cada metro cuadrado de la superficie terrestre.
Es importante destacar que la decisión de crear la dirección IPv6 con un tamaño de 128 bits no tenía como objetivo asignar 6,5 x 1023 direcciones a cada metro cuadrado de la Tierra. En su lugar, el tamaño relativamente grande de la dirección IPv6 está diseñado para subdividirse en dominios de enrutamiento jerárquicos que reflejen la topología de Internet en la actualidad. La utilización de 128 bits proporciona múltiples niveles de jerarquía y flexibilidad en el diseño del direccionamiento y enrutamiento jerárquicos, que son los elementos de los que carece actualmente la red Internet basada en IPv4.
Para mayor información sobre el protocolo de IPv6 refiérase al documento RFC 2460[1]

INTRODUCCIÓN A LA DIVISIÓN EN SUBREDES

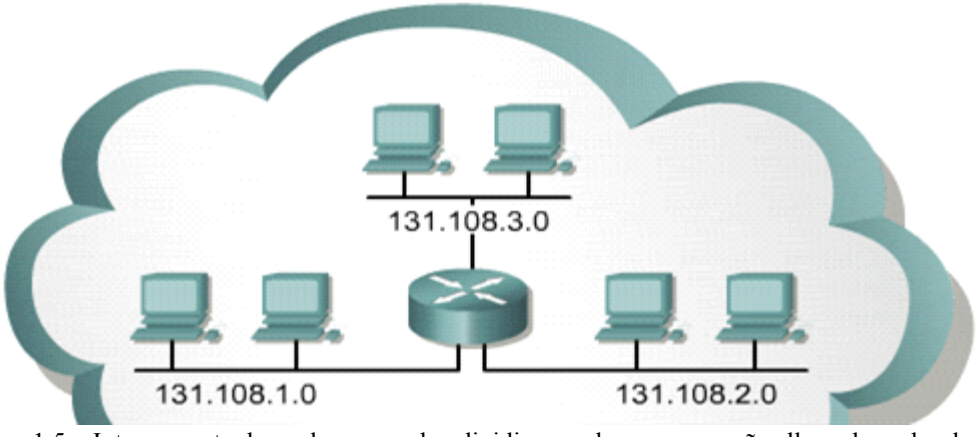


Figura 1.5n. Internamente, las redes se pueden dividir en redes mas pequeñas llamadas subredes. Al proporcionar un tercer nivel de direccionamiento, las subredes aportan flexibilidad adicional al administrar la red. Por ejemplo, una dirección de red clase B proporcionada por el registro americano de números de Internet (American Registry for Internet Numbers - ARIN), se puede dividir en varias subredes. En este

ejemplo, 131.108.1.0, 131.108.2.0 y 131.108.3.0 son subredes dentro de la red 131.108.0.0.

[1] http://www.merlinux.org/traductor/docs/resumenes/resumen_RFC2460.html

La división en subredes es otro método para administrar las direcciones IP. Este método, que consiste en dividir las clases de direcciones de red completas en partes de menor tamaño, ha evitado el completo agotamiento de las direcciones IP.
Resulta imposible hablar sobre el TCP/IP sin mencionar la división en subredes. Como administrador de sistemas, es importante comprender que la división en subredes constituye un medio para dividir e identificar las redes individuales en toda la LAN. No siempre es necesario subdividir una red pequeña. Sin embargo, en el caso de redes grandes a muy grandes, la división en subredes es necesario.

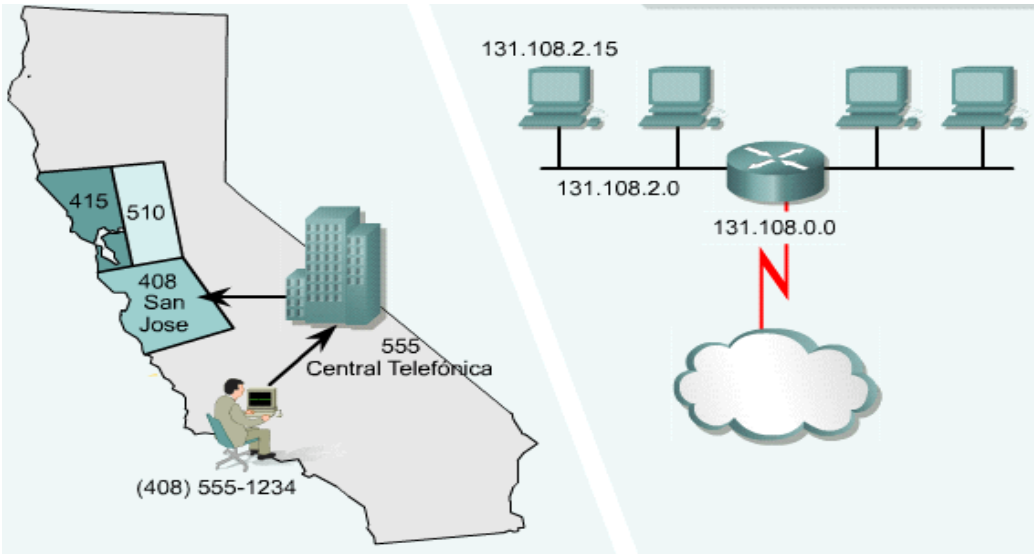


Figura 1.5º. Las subredes son similares al sistema de numeración telefónica de Estados Unidos. Este sistema de numeración se divide en códigos de área, que a su vez se dividen en intercambios, que a su vez se dividen en conexiones individuales. Las direcciones de subred incluyen un número de red, un número de subred dentro de la red y un número de host de la subred.

Dividir una red en subredes significa utilizar una máscara de subred para dividir la red y convertir una gran red en segmentos más pequeños, más eficientes y administrables o subredes. Un ejemplo sería el sistema telefónico de los EE.UU. que se divide en códigos de área, códigos de intercambio y números locales.
El administrador del sistema debe resolver estos problemas al agregar y expandir la red. Es importante saber cuántas subredes o redes son necesarias y cuántos hosts se requerirán en cada red. Con la división en subredes, la red no está limitada a las máscaras de red por defecto Clase A, B o C y se da una mayor flexibilidad en el diseño de la red.
Las direcciones de subredes incluyen la porción de red más el campo de subred y el campo de host. El campo de subred y el campo de host se crean a partir de la porción de host original de la red entera. La capacidad para decidir cómo se divide la porción de host

original en los nuevos campos de subred y de host ofrece flexibilidad en el direccionamiento al administrador de red.
Para crear una dirección de subred, un administrador de red pide prestados bits del campo de host y los designa como campo de subred.

Notación decimal para el primer octeto de host	Número de subredes	Número de Hosts de clase A por subred	Número de Hosts de clase B por subred	Número de Hosts de clase C por subred
.192	2	4,194,302	16,382	62
.224	6	2,097,150	8,190	30
.240	14	1,048,574	4,094	14
.248	30	524,286	2,046	6
.252	62	262,142	1,022	2
.254	126	131,070	510	-
.255	254	65,534	254	-

Tabla 1.5d.

El número mínimo de bits que se puede pedir es dos. Al crear una subred, donde se solicita un solo bit, el número de la red suele ser red .0. El número de broadcast entonces sería la red .255. El número máximo de bits que se puede pedir prestado puede ser cualquier número que deje por lo menos 2 bits restantes para el número de host.

CÓMO OBTENER UNA DIRECCIÓN IP?
Un host de red necesita obtener una dirección exclusiva a nivel global para poder funcionar en Internet. La dirección MAC o física que posee el host sólo tiene alcance local, para identificar el host dentro de la red del área local. Como es una dirección de Capa 2, el Router no la utiliza para realizar transmisiones fuera de la LAN.
Las direcciones IP son las direcciones que más frecuentemente se utilizan en las comunicaciones en la Internet. Este protocolo es un esquema de direccionamiento jerárquico que permite que las direcciones individuales se asocien en forma conjunta y sean tratadas como grupos. Estos grupos de direcciones posibilitan una eficiente transferencia de datos a través de la Internet.
Los administradores de redes utilizan dos métodos para asignar las direcciones IP. Estos métodos son el estático y el dinámico.
Más adelante, en esta lección, se tratará el direccionamiento estático y las tres variantes del direccionamiento dinámico. Independientemente del esquema de direccionamiento elegido, no es posible tener dos interfaces con la misma dirección IP. Dos hosts con la misma dirección IP pueden generar conflictos que hacen que ambos no puedan operar correctamente. Como muestra la Figura, los hosts tienen una dirección física ya que cuentan con una tarjeta de interfaz de red que les permite conectarse al medio físico.

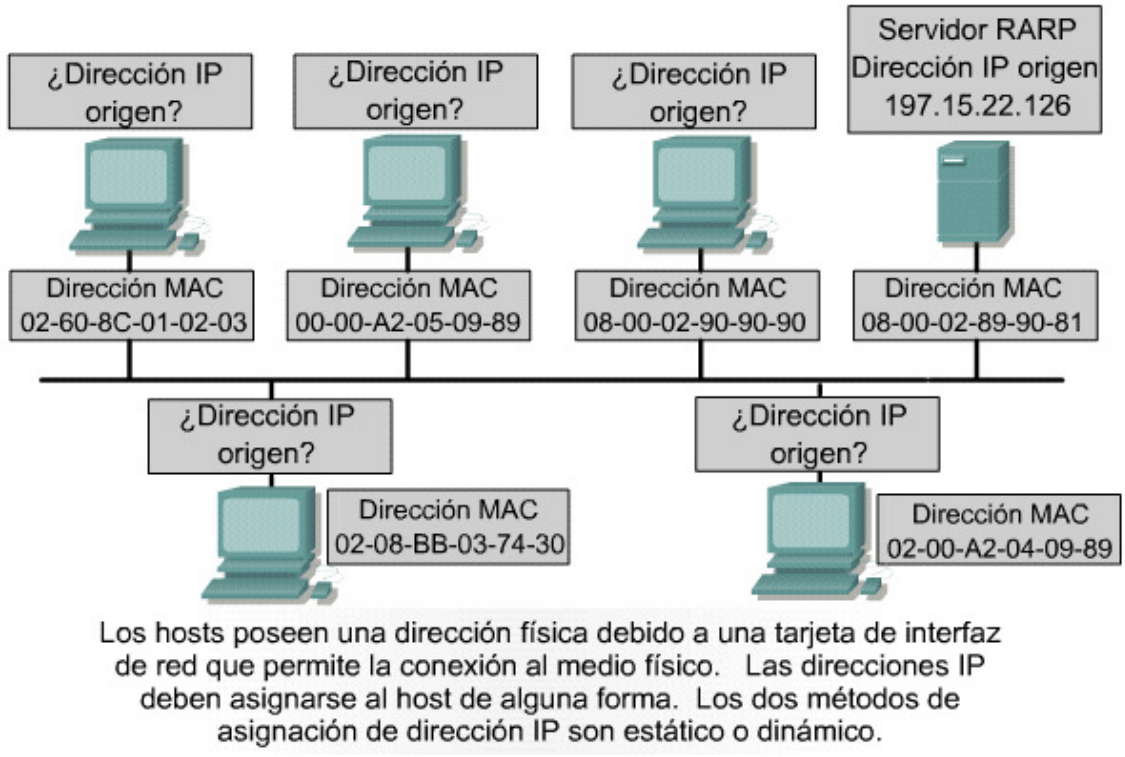


Figura 1.5p. los host poseen una dirección física debido a una tarjeta de interfaz de red que permite la conexión al medio físico. Las direcciones IP deben asignarse al host de alguna forma. Los dos métodos de asignación de dirección IP son estático y dinámico.

1.6 Redes inalámbricas

Son redes cuya comunicación se da por medio de ondas de radio o por luz infrarroja. Esta tecnología es muy útil en ambientes donde es difícil cablear las interconexiones de la red o cuando se necesita que un dispositivo móvil tenga conexión a la red de manera ininterrumpida, cuando pase de un lugar a otro, dentro del alcance de la red inalámbrica. Sin embargo esta comodidad de instalación tiene su contra, el cual es el reducido ancho de banda que soporta si se compara con las redes alambradas (por ejemplo la fibra óptica puede tener un ancho de banda de 10 Gbps mientras que el ancho de banda de una red inalámbrica alcanza comúnmente 54 Mbps).

Las redes inalámbricas están compuestas básicamente por dos elementos, los puntos de acceso y los dispositivos de cliente. Los puntos de acceso actúan como un hub, enviando y recibiendo información via radio a los dispositivos de cliente tales como computadoras, PDA, etc.

Las redes inalámbricas utilizan diversas tecnologías, las cuales se seleccionan dependiendo de la aplicación con la que se va a trabajar.

1.6.1 Tecnologías

1.6.1.1 Infrarrojos

Este medio de transmisión se utiliza en comunicaciones de corto alcance, pero tiene que ser direccionable y además no atraviesa objetos. Esto se convierte en una gran ventaja si se desea que una transmisión no interfiera o sea interceptada fuera de una habitación. La banda de frecuencia de trabajo va desde 300 GHz hasta los 200 THz, justo por debajo del espectro de la luz visible para transportar datos.

IrDA (Infrared Data Association por sus siglas en ingles), es un grupo de fabricantes de dispositivos que desarrollaron un estándar para la transmisión de datos vía ondas de luz infrarroja.

1.6.1.2 Banda angosta

Recibe éste nombre porque la transmisión y recepción se da en una banda especifica de frecuencia la cual es lo mas angosta posible. Generalmente se utiliza para interconectar redes LAN vecinas, por medio de microondas en ambos extremos de los enlaces y visibilidad entre las antenas.

Generalmente este tipo de tecnología utiliza frecuencias que tienen que ser autorizadas por el organismo regulador local, además de un uso amplio de frecuencias. Esto se debe a que cada cliente tiene una frecuencia distinta con el propósito de evitar interferencias.

1.6.1.3 Espectro extendido

Es actualmente las mas utilizada para en LANs inalámbricas. Esta tecnología consiste en repartir la potencia en una banda ancha de frecuencias, consiguiendo una mejor relación señal/ruido en detrimento del ancho de banda. Con esta técnica se consigue señales menos susceptibles al ruido eléctrico que con las modulaciones tradicionales de radio. Dado que las señales de radio comunes tienen un espectro estrecho solo interferirán en una pequeña porción de la señal “esparcida en el espectro”, obteniendo como resultado una menor interferencia y menores errores en la transmisión.

Existen dos tecnologías de espectro extendido empleadas en las transmisiones en banda ancha:

1. FHSS (Frequency Hopping Spread Spectrum) consiste en modular la señal de transmission con una señal portadora que 'salta" (hops) de frecuencia en frecuencia, dentro del ancho de la banda asignada, en función del timepo. El cambio periódico de frecuencia de la portadora, reduce la interferencia producida por otra señal originada por un sistema de banda estrecha, afectando solo si ambas señales se transmiten en la misma frecuencia y en el mismo momento. Un patrón de salto (hopping code), determina las frecuencias por las que se transmitirá y el orden de uso de estas.

La regulación impone a los fabricantes el uso de al menos 75 frecuencias distintas para la transmisión de un canal con un tiempo máximo de 400ms de uso por frecuencia (dwell time).

2. DSSS (Direct Sequence Spread Spectrum). Esta técnica consiste en la combinación de la señal a transmitir en una secuencia de bits a mayor velocidad de transmisión, a la cual se le denomina "codigo de troceado" (chipping code). Esta secuencia no es más que un patrón redundante de bits asignado a cada bit a enviar, que divide la información del usuario acorde a una relación de esparcimiento (Spread Ratio).

Aunque las redes inalámbricas necesitan cumplir con determinadas normas que se aplican de igual forma al mundo de las redes cableadas (IEEE 802.3 ó equivalentes), también se requiere del cumplimiento de una normativa específica que permita controlar su comportamiento con respecto al uso de los recursos radioeléctricos. Es por esto que en la gran mayoria de los paises, se hace uso de frecuencias no licenciadas, es decir de uso libre, como la de 2.4 GHz y de 5 GHz. La banda de 2.4 GHz es utilizada por la tecnología Wi-Fi, como por otros estándares de comunicaciones, como Bluetooth, Home RF para Home Networking, y por equipos para aplicaciones Industriales, Científicas y Médicas (ISM). La utilización de la banda de 5 GHz permite incrementar tanto el ancho de banda como la capacidad de tráfico disponible, dando lugar a nuevas dimensiones para esta tecnología.

1.6.2 Normalización IEEE

A mediados del año 1997, el IEEE (Institute of Electrical and Electronics Engineers) hizo público el estándar 802.11 que definía las especificaciones para las WLAN, y poco después, a finales de 1999, vio la luz el estándar 802.11 b que daría lugar posteriormente a la denominación Wi-Fi. La expresión Wi-Fi (abreviatura de Wireless Fidelity) se utiliza como denominación genérica para los productos que incorporan cualquier variante de la tecnología inalámbrica 802.11. Básicamente, esto significa que, vía radio, se mantienen las características de una conexión Ethernet cableada. El grupo de trabajo 802.11 es el responsable del desarrollo de los estándares de redes de área local inalámbricas bajo los

auspicios del Comité de Estándares del proyecto 802 de LAN/MAN del IEEE. A continuación se presentan algunos de los protocolos de las redes inalámbricas.

802.11 legacy
Es la versión original del estándar IEEE 802.11 publicado en 1997 que se basa en señales infrarrojas en la banda ISM a una frecuencia de 2.4 GHz, con velocidades de 1 y 2 Mbps. El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Tiene un alcance máximo de 75 m promedio, con un throughput de 0.7 Mbps.

802.11b
Ratificado en 1999, alcanza una velocidad máxima de 11 Mbps, en la frecuencia de 2.4 GHz y utiliza el mismo método de acceso CSMA/CA. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5.9 Mbps sobre TCP y 7.1 Mbps sobre UDP. El alcance máximo promedio es de 110 m con un throughput de 4 Mbps.

802.11a
Pese que este protocolo salió al mismo tiempo que el 802.11 b, no fue hasta el 2001 que empezaron a aparecer en el mercado equipos que soportaban dicho estándar.

El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 GHz y utiliza 52 subportadoras "orthogonal frequency-division multiplexing" (OFDM por sus siglas en ingles) con una velocidad máxima de 54 Mbps, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbps. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbps en caso necesario.

Este estándar presenta el inconveniente qque debido a la frecuencia de transmisión, las ondas de las señales de los puntos de acceso no pueden penetrar tan lejos como las del protocolo 802.11b, por lo que se hace casi necesario que los dispositivos estén en línea vista. El alcance máximo con el que puede operar es de un promedio de 100 m con un throughput de 23 Mbps.

802.11h
Se hizo público en octubre del 2003 para resolver problemas de coexistencia de los sistemas basados en IEEE 802.11a (básicamente) con sistemas de radares que trabajan también a 5 GHz, por recomendación de la International Telecommunication Union (ITU).

Es por tal motivo que 802.11h proporciona a las redes 802.11a la capacidad de gestionar dinámicamente tanto la frecuencia, como la potencia de transmisión.

DFS (Dynamic Frequency Selection) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz con el fin de evitar interferencias co-canal con sistemas de radar y para asegurar una utilización uniforme de los canales disponibles.

TPC (Transmitter Power Control) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz para asegurar que se respetan las limitaciones de potencia transmitida que puede haber para diferentes canales en una determinada región, de manera que se minimiza la interferencia con sistemas de satélite.

802.11g
Utiliza la frecuencia de 2.4 GHz, al igual que 802.11b pero opera a una velocidad teórica máxima de 54 Mbps, o cerca de 24.7 Mbps de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Tiene un alcance máximo promedio de 110 m, con un throughput de 19 Mbps. El tipo de modulacion que se utiliza es la division de frecuencia ortogonal multiplexada (OFDM).

802.11e
Soporta tráfico en tiempo real en todo tipo de entornos y situaciones debido a que incorpora las garantías de Calidad de Servicio (QoS). El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado Hybrid Coordination Function (HCF) con dos tipos de acceso:
(EDCA) Enhanced Distributed Channel Access
(HCCA) Controlled Access.

802.11n
Es un estándar que está supuesto a salir a en septiembre del 2008 de una manera ya oficial. Aunque a mitad del 2007 se planea que ya van a salir algunos hardwares que soportan la "pre-versión" de este protocolo. Se supone que va a tener un alcance máximo promedio de 70 m. Va a operar en ambas frecuencias, la de 2.4 GHz y la de 5 GHz. Va soportar una transmisión de datos de alrededor 248 Mbps, con un throughput de 74 Mbps. Esto es posible debido a la tecnología de transmisión que se utilizará, la cual es MIMO (multiples entradas multiples salidas por sus siglas en ingles).

1.7 AUTENTICACION

La autenticación forma parte fundamental de la seguridad de un sistema, la autenticación confirma la identidad de un usuario que intenta iniciar una sesión en un dominio o tener acceso a los recursos de una red, en términos de seguridad de redes de datos, se puede

considerar uno de los tres pasos fundamentales (AAA). Cada uno de ellos es, de forma ordenada:

1. **Autenticación** En la seguridad de ordenador, la autenticación es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente siendo autenticado puede ser una persona que usa un ordenador, un ordenador por sí mismo o un programa del ordenador. En un web de confianza, "autenticación" es un modo de asegurar que los usuarios son quién ellos dicen que ellos son - que el usuario que intenta realizar funciones en un sistema es de hecho el usuario que tiene la autorización para hacer así.
2. **Autorización** Proceso por el cual la red de datos autoriza al usuario identificado a acceder a determinados recursos de la misma.
3. **Auditoria** Mediante la cual la red o sistemas asociados registran todos y cada uno de los accesos a los recursos que realiza el usuario autorizados o no.

El problema de la autorización a menudo, es idéntico a la de autenticación; muchos protocolos de seguridad extensamente adoptados estándar, regulaciones obligatorias, y hasta estatutos están basados en esta asunción. Sin embargo, el uso más exacto describe la autenticación como el proceso de verificar la identidad de una persona, mientras la autorización es el proceso de verificación que una persona conocida tiene la autoridad para realizar una cierta operación. La autenticación, por lo tanto, debe preceder la autorización.

1.7.1 Mecanismo general de autenticación

La mayor parte de los sistemas informáticos y redes mantienen de uno u otro modo una relación de identidades personales (usuarios) asociadas normalmente con un perfil de seguridad, roles y permisos. La autenticación de usuarios permite a estos sistemas asumir con una seguridad razonable que quien se está conectando es quien dice ser para que luego las acciones que se ejecuten en el sistema puedan ser referidas luego a esa identidad y aplicar los mecanismos de autorización y/o auditoria oportunos.

El primer elemento necesario (y suficiente estrictamente hablando) por tanto para la autenticación es la existencia de identidades biunívocamente identificadas con un identificador único (valga la redundancia). Los identificadores de usuarios pueden tener muchas formas siendo la más común una sucesión de caracteres conocida comúnmente como **login**.

El proceso general de autenticación consta de los siguientes pasos:

1. El usuario solicita acceso a un sistema.

2. El sistema solicita al usuario que se autentique.
3. El usuario aporta las credenciales que le identifican y permiten verificar la autenticidad de la identificación.
4. El sistema valída según sus reglas si las credenciales aportadas son suficientes para dar acceso al usuario o no.

1.7.2 Métodos de autenticación

Cada regla define una lista de métodos de autenticación. Cada método de autenticación define los requisitos de comprobación de las identidades en las comunicaciones a las que se aplica la regla asociada. Los dos interlocutores deben tener, como mínimo, un método de autenticación común; de lo contrario, la comunicación no será posible. Si se crean varios métodos de autenticación, existirán más posibilidades de encontrar un método común para los dos equipos.

Sólo puede utilizarse un método de autenticación entre dos equipos, independientemente de cuántos se hayan configurado. Si se aplican varias reglas al mismo par de equipos, debe configurar la lista de métodos de autenticación de modo que los dos equipos puedan utilizar el mismo método. Por ejemplo, si una regla entre un par de equipos especifica únicamente un protocolo, por ejemplo Kerberos de Windows Server 2003, para la autenticación y sólo filtra datos de TCP, mientras que otra regla especifica únicamente certificados para la autenticación y sólo filtra datos de UDP, la autenticación no será posible. En el documento se tratara con especial énfasis el protocolo de autenticación RADIUS (IEEE 802.1x), mismo al cual se verificara la coexistencia e interoperatividad con los sistemas de RFID.

Los métodos de autenticación están en función de lo que utilizan para la verificación y estos se dividen en tres categorías:

- Sistemas basados en algo conocido.Ejemplo, un *password* (Unix) o *passphrase* (PGP).
- Sistemas basados en algo poseído.Ejemplo, una tarjeta de identidad ,una tarjeta inteligente(*smartcard*)
- Sistemas basados en una característica física del usuario o un acto involuntario del mismo: Ejemplo, verificación de voz, de escritura, de huellas, de patrones oculares.

Cualquier sistema de identificación ha de poseer unas determinadas características para ser viable:

- Ha de ser fiable con una probabilidad muy elevada (podemos hablar de tasas de fallo de en los sistemas menos seguros).
- Económicamente factible para la organización (si su precio es superior al valor de lo que se intenta proteger, tenemos un sistema incorrecto).
- Soportar con éxito cierto tipo de ataques.
- Ser aceptable para los usuarios, que serán al fin y al cabo quienes lo utilicen.

1.7.3 Protocolo de autenticación (IEEE 802.1x).

El protocolo IEEE 802.1x se basa en el control del puerto de conexión. Este será abierto una vez el cliente ha completado de manera satisfactoria el proceso de autenticación.

Protocolo EAP

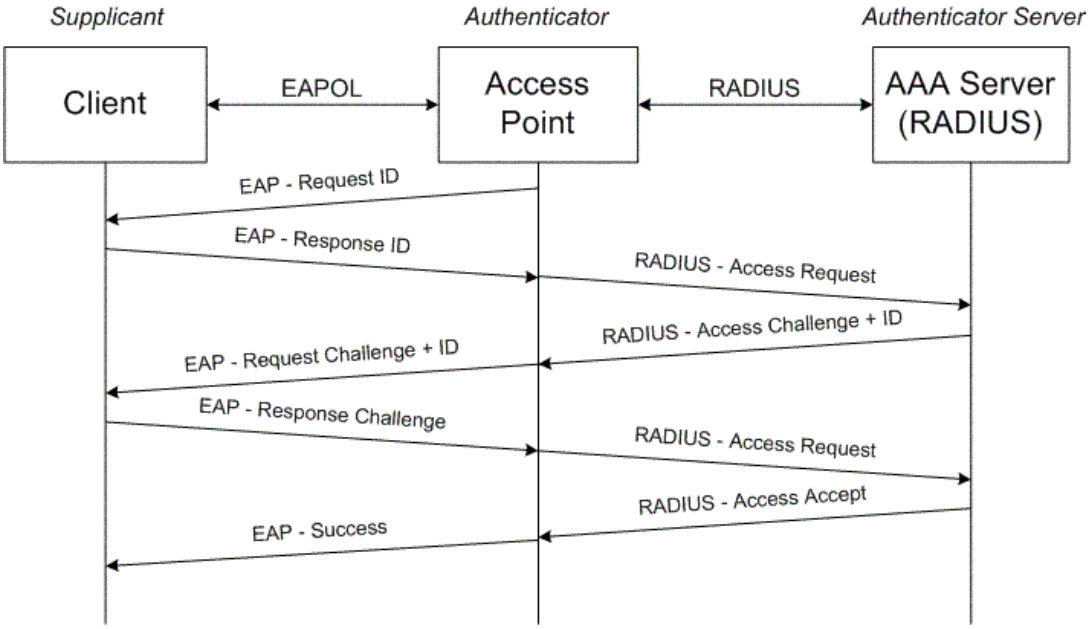
Extensible Authentication Protocol (EAP - RFC 2284). Uno de los elementos básicos del 802.1x y desarrollado como mejora del *Point to Point Protocol* (PPP - RFC 1661). PPP utiliza como método de autenticación "username" y "password". Actualmente existe la necesidad de ampliar dicho método a otros, que resulten más seguros o cómodos para el usuario. Así fue diseñado **EAP**, basado en el protocolo PPP y proporcionando un marco generalizado para diversos métodos de autenticación. EAP sirve como soporte a protocolos propietarios de autenticación, gestiona las contraseñas en mecanismos de desafío-respuesta y es capaz de trabajar con tecnología de clave pública.

Con un EAP estandarizado, la interoperabilidad y la compatibilidad de los métodos de la autenticación es más simple. Por ejemplo, si al intentar establecer una conexión se utiliza EAP como protocolo de control de acceso, el **RAS** (Servicio de Acceso Remoto) no necesitará conocer los detalles del método de autenticación a emplear, solamente el cliente y el servidor de la autenticación tienen que coordinarse. En EAP, un RAS reencamina los datos de autenticación hasta el servidor de autenticación local, el cual sabrá que método utilizar.

Esto nos lleva al estándar de IEEE 802.1x, que describe cómo encapsular mensajes de EAP en tramas Ethernet, es decir, funcionamiento del protocolo EAP en redes LAN (EAP over LANs -> EAPOL). 802.1x utiliza tres términos que es necesario concretar:

- **Supplicant**: Usuario o cliente que desea ser autenticado.
- **Autenticador**: Elemento intermedio que suministrará el servicio una vez el "supplicat" haya sido autenticado.
- **Servidor de Autenticación**: Servidor responsable de realizar una correcta autenticación del "supplicant".

Ejemplo del protocolo:



1. El authenticator envía un paquete de "**EAP-Request/Identity**" al supplicant tan pronto como detecte que el acoplamiento es activo.

2. El supplicant envía un paquete de "**EAP-Response/Identity**" al authenticator, que pasa directamente al servidor de la autenticación.

3. El servidor de la autenticación envía un desafío al authenticator. El authenticator desempaqueta el contenido del paquete IP, lo empaqueta de nuevo en EAPOL y lo envía al supplicant.

4. El supplicant responde al desafío vía el authenticator y pasa la respuesta al servidor de autenticación.

5. Si el supplicant proporciona identidad apropiada, el servidor de autenticación responde con un mensaje de éxito al authenticator, que es pasado así mismo al supplicant. El authenticator permite a partir de este momento el acceso al supplicant.

Protocolo EAP-TLS

Sus principales características son:

- Fue desarrollado por Microsoft.

- Ofrece una autenticación fuerte mútua, credenciales de seguridad y claves de encriptación dinámcias.
- Requiere la distribución de certificados digitales a todos los usuarios así como a los servidores RADIUS.
- Requiere una infraestructura de gestión de certificados (PKI).

Protocolo EAP-TTLS

Sus principales características son:

- Permite a los usuarios autenticarse mediante nombre de usuario y contraseña, u otro método de autenticación, sin pérdida de seguridad.
- Permite generación dinámica de claves de encriptación.
- Requiere sólo certificados de serividor, no de cliente.

El módulo EAP-TTLS tiene como objetivo permitir que los usuarios sean autenticados dentro de las WLANs con las credenciales existentes, y además, utilizando una criptografía fuerte de clave pública/privada, para proteger estas credenciales contra las "escuchas" a las que se exponen las comunicaciones sin cables.

El resultado es un protocolo que proporciona prácticamente el mismo nivel de seguridad que EAP-TLS, más sencillo de gestionar y económico, compatible con las bases de datos y la infraestructura existentes.

Anexo 2: Precios de sistemas RFID en el mercado internacional

En la actualidad hay una gran cantidad de sistemas implementados de RFID en varios ámbitos (industriales, hospitalarios, etc.). Esto se debe al gran auge que ha tenido la tecnología RFID, la cual ha pasado de ser una tecnología experimental a ser una de las mas novedosas y de mas rápido crecimiento en cuanto a los sistemas de identificación.

Es por tal motivo que en este capitulo, se detallaran los costos para implementar un sistema RFID completo, tanto en la actualidad, así como en el pasado y una proyección de lo que puede ser en el futuro próximo en base a un análisis del mercado y la tendencia de los precios.

2.1 Costos actuales.

En este apartado se detallan los precios de cada uno de los componentes de un sistema RFID en la actualidad. Para dar a conocer su precio en el mercado y poder sentar una base de información que a futuro sirva como referencia para hacer comparaciones de precios.

A continuación se detallan un buen número de dispositivos, con sus características principales y sus precios de mercado, con el propósito de cubrir aplicaciones y/o usos que se le puedan dar a un sistema de RFID.

2.1.1 Sistemas de baja frecuencia

a. Readers

En este apartado existe una amplia gama de dispositivos, por lo que se dividirá la sección de *reader* en 2 partes, *readers* móviles o portátiles y *readers* fijos.

Readers portátiles

Hay una amplia gama de sistemas portátiles de RFID, los precios varían dependiendo de la capacidad de cada uno. La mayor parte de sistemas portátiles están hechos para intercambiar información con un ordenador. Otros por el contrario ya tienen su propio

sistema operativo el cual se encarga de procesar los datos acerca de los *tags*, de manera independiente.

i. USB Pen Reader

Entre los dispositivos mas portátiles, por su tamaño es el *USB Pen Reader*. Este es un dispositivo que esta hecho para trabajar en 125 KHz y comunicarse con los protocolos EM4100/4102/UNIQUE. La ventaja que ofrece dicho dispositivo es que no necesita de ningún software en especial para funcionar. Los datos que recopila de los *tags* los puede mostrar en diferentes aplicaciones que este ejecutando el usuario (Excel, Word, Outlook, etc.) Una desventaja es que únicamente puede detectar *tags* si esta conectado a una computadora. En las siguientes figuras se muestran este *reader*.

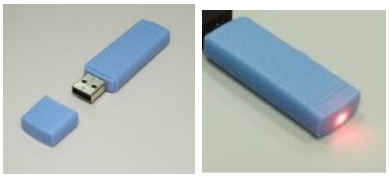


Figura 2.1.1.a: USB Pen Reader

Precio unitario: US $39.46
Tienda virtual: http://www.rfidshop.com/
Día de consulta: 1 de julio del 2007.

ii. CF RFID Card 125 kHz

Es un *reader* compacto con una tarjeta de interfaz CF, la cual viene para ser integrado en una PDA o en una *pocket PC*. Necesita de un software específico para poder hacer lecturas de *tags*. Esta diseñado para leer *tags* que vengan con el protocolo EM4102/UNIQUE. Al igual que el *reader* anterior presenta la desventaja que necesita de un dispositivo al cual conectarse para poder recolectar información. Es decir que no es un *reader* independiente. A continuación se muestra una figura donde se pude apreciar dicho dispositivo.

Figura 2.1.1.b: CF RFID Card

Precio unitario: US $132.19
Tienda virtual: http://www.rfidshop.com/
Día de consulta: 1 de julio del 2007

iii. DLP-RFID1

Es un *reader* portátil, alimentado por USB y de bajo costo. Este dispositivo a diferencia de los dos anteriores, aparte de leer *tags* permite escribir información en ellos. Soporta los sistemas operativos Windows/Windows CE/Linux/Mac PC.

Figura 2.1.1.c DLP-RFID1

Precio unitario: US $160.13
(Por compras mayores a 10 unidades: US $123.87)
Tienda virtual: http://apple.clickandbuild.com/cnb/shop/ftdichip?op=catalogue-product_info-null&prodCategoryID=50&productID=59
Día de consulta: 01 de julio del 2007

iv. LF Bluetooth scanner

Aparte de dispositivos portátiles que se conecten a través de de USB, hay dispositivos que se pueden interconectar mediante tecnologías inalámbricas tales como el bluetooth. Como es el caso del LF Bluetooth scanner, el cual opera en frecuencias de 125 KHz y no solo permite leer sino también escribir en los tags que trabajen en dicha frecuencia (tgasys, microchip, phillips, sokymat, infineon, texas instrument).

Figura 2.1.1.d: LF bluetooth scanner

Precio unitario: US $599.00
Tienda virtual: http://rfidusa.com/superstore/product_info.php?cPath=34&products_id=550
Día de consulta: 01 de julio del 2007

v. IPAQ RFID EM4102/UNIQUE

Es una HP IPAQ con una tarjeta incorporada de RFID para leer *tags* de 125 KHz EM4102/UNIQUE. La ventaja que ofrece esta IPAQ es la conectividad a Internet, es decir que los datos recolectados por el reader los puede mandar a través de correo electrónico o pueden ser ingresados a una base de datos mediante ftp.

Figura 2.1.1.e IPAQ HP con tarjeta de RFID incorporada

Precio unitario: US $670.80
Tienda virtual: http://www.rfidshop.com/index.asp?function=DISPLAYPRODUCT&productid=1189
Día de consulta: 01 de julio del 2007

Readers fijos

i. ID40

Este modelo ha sido diseñado para un rango de lectura medio (entre 40 y 45 cm de alcance máximo) con estándares Unique/EM4102 para *tags*. Esta diseñado con protección contra vibración e interferencias eléctricas, lo que hace que disminuya su efecto negativo en la transmisión de datos. Viene con una interfaz RS-232 para intercambiar datos con un ordenador. Trabaja a una frecuencia de 125 KHz.

Figura 2.1.1.f ID40

Precio unitario: US $147.98
Tienda virtual: http://www.rfidshop.com/index.asp?function=DISPLAYPRODUCT&productid=803
Día de consulta: 01 de julio del 2007

ii. ID70

Es básicamente el mismo *reader* que el anterior, con la diferencia que éste es capaz de leer *tags* ISO hasta en un rango de 70 cm de radio.

Figura 2.1.1.g ID70

Precio unitario: US $434.06
Tienda virtual: http://www.rfidshop.com/index.asp?function=DISPLAYPRODUCT&productid=39
Día de consulta: 01 de julio del 2007

iii. Series 2000 Reader S251B

Es un lector capaz de comunicarse con cualquier *tag* diseñado para frecuencias de 134.2 KHz. Se comunica a través del puerto serial (RS232, RS422/485). Como elemento adicional posee un sistema denominado DAT (*Dynamic Auto Tuning*) el cual automáticamente sintoniza la antena a cierta resonancia y mantiene dicha sintonización durante el proceso de comunicación. Su arquitectura permite comunicaciones punto a punto o punto a multipunto. Debido a sus 32 KB de RAM puede almacenar 909 códigos de identificación.

Figura 2.1.1.h: Series 2000 Reader S251B

Precio unitario: US $589.89
Tienda virtual: http://www.posglobal.com/RFID_READERS/RI-STU-251B-01/
Día de consulta: 01 de julio del 2007

iv. 25K-R-USB-KB-D1

Es un dispositivo compacto que se puede interconectar al puerto USB de un ordenador. Esto elimina la necesidad de una fuente de alimentación externa para el funcionamiento.. trabaja en una frecuencia de 125 KHz y es compatible con los protocolos EM4100 o similares. Tiene un rango de lectura maximo de 10 cm.

Figura 2.1.1.i:

Precio unitario: US $49
Tienda virtual: http://www.rfidshop.com.hk/
Día de consulta: 01 de julio del 2007

b. tags

El uso de los *tags* en RFID es extremadamente variado, esto da origen a que los *transponders* tengan varias formas o que vengan integrados en productos específicos dependiendo de su uso (botones de ropa, tarjetas de crédito, etiquetas de marca, etc.). Esta diversidad de aplicaciones hacen que el precio de los *tags* sea bastante variable (porque no solo depende del costo de fabricación del chip y su bobina sino que también del elemento al cual vaya adherido), sin embargo el enfoque de los fabricantes es el mismo, que el chip que conforma el *tag* y su antena, sean lo mas baratos posibles.

2.1.2 Sistemas de alta frecuencia

a. Readers

En este apartado existe una amplia gama de dispositivos, por lo que se dividirá la sección de *reader* en 2 partes, *readers* móviles o portátiles y *readers* fijos.

Readers portátiles

Al igual que para los de baja frecuencia se puede encontrar una amplia gama de dispositivos lectores. Las frecuencias más comunes para este tipo de *readers* son de 13.56 MHz.

i. SDiD™ 1010 MIFARE ISO14443A

No es un dispositivo lector únicamente, sino que además permite grabar información por lo que se le cataloga como *reader/writer* para PDA (Personal Digital Assistants) y teléfonos inteligentes. La ventaja que ofrece este dispositivo es que puede mandar información a través de WiFi , CDMA, GSM o Bluetooth. Esta hecho para trabajar con los readers ISO14443-A y con MIFARE. Posee grandes capacidades a nivel de seguridad y trae aplicaciones para su uso en cuidado medico, farmacéutico, logística y seguridad industrial.

Figura 2.1.2.a SDiD™ 1010

Precio unitario: US $147.98
Tienda virtual: http://www.rfidshop.com/
Día de consulta: 01 de julio del 2007

ii. Freedom HF Bluetooth Scanner

tien la capacidad de leer y escribir información en los tags. Trabaja en la frecuencia 13.56 MHz incluidos lso desarrollados por Tagsys, Microchip, Philips, Sokymat.

Figura 2.1.2b: Freedom HF Bluetooth Scanner

Precio unitario: US $599.00
Tienda virtual: http://rfidusa.com/superstore/product_info.php?cPath=34&products_id=552&osCsid=e24cc3095eefc77719929071191a639f
Día de consulta: 01 de julio del 2007

iii. Socket CF Rfid Reader Card HF

Tarjeta lectora de tags RFID compatible con computadoras portátiles

Figura 2.1.2.c: Socket CF Rfid Reader Card HF

Precio Unitario: US $219.00
Tienda virtual: http://www.nextag.com/511359120p/prices-html
Día de consulta: 01 de julio del 2007

Readers fijos

i. Symbol ,Rfid Fork Lift Reader, 802.11ABG,BT,WIN CE,EPC GEN 2

reader capaz de leer hasta tags EPC de segunda generacion, trabaje en alta frecuencia ademas de que es compatible con los estandares 802.11g y b. trae soporte para el sistema operativo Windows.

Figura 2.1.2.c: Socket CF Rfid Reader Card HF

Precio Unitario: US $4083.09
Tienda virtual: http://www.nextag.com/Symbol-RFID-FORK-LIFT-525435127/prices-html
Día de consulta: 01 de julio del 2007

b. Tags

i. Sokymat Disc Tag

Es un *transponder* en forma de disco con radio de 22 mm, compatible con el estándar MIFARE de Philips de 1Kbyte ISO/IEC 14443A. Este *tag* se pude implantar en brazaletes, monedas, tarjetas.

Precio unitario (paquete de 200): US $427 (precio por tag: $2.13)
Tienda virtual: http://www.therfidshop.com/product_info.php?cPath=25_67&products_id=296
Día de consulta: 01 de julio del 2007

ii. ACG Philips Mifare Card

Estos tags vienen en forma de tarjetas plásticas con superficie lisa para poder imprimir cualquier información (logo de empresa, identificación de empleados, publicidad, etc.). Trabajan bajo el estándar MIFARE de Philips de 1k.

Precio paquete 200 tarjetas: US $248 (precio unitario: $1.24)
Tienda virtual: http://www.therfidshop.com/product_info.php?cPath=25_67&products_id=260 Día de consulta: 01 de julio del 2007

2.2 Análisis de evolución de precio y demanda de sistemas RFID

IDTechEx, una empresa dedicada al rubro de identificación de productos, ha llevado a cabo y publicado una nueva investigación de mercado, titulada: "*RFID Forecasts, Players & Opportunities 2005-2015*". Dicha investigación analiza el estado actual y el futuro de la tecnología RFID hasta 2015. A continuación se detallan, unas cuantas reflexiones que surgen de dicho informe, en términos de previsiones y oportunidades para los actores implicados.

El punto de partida es que el mercado global de la RFID, incluyendo los tags, sistemas y servicios, alcanzó en el 2006 el valor de 1.940 millones de dólares; e impulsado por la demanda cada vez mayor y las nuevas normativas, conseguirá lograr los 26.900 millones de dólares en 2015.

Hasta 2005, se han vendido 1.800 millones de tags RFID. Las aplicaciones más significativas, en cuanto a volúmenes, atañen a las tarjetas de acceso en el sector financiero, así como los sectores de la seguridad de las redes o los edificios, los sectores del automóvil o del transporte de pasajeros, con resultados más reducidos en los sectores, ocio, bibliotecas, lavanderías y sanidad. La mayoría de dichos tags vienen con chip de silicio, resultando inteligentes, pero también delicados y costosos en la mayoría de los casos. Sin embargo, las ventas de *tags* sin chip han sido relativamente modestas respecto de las ventas de tags con chip.

Una vez resueltos los problemas técnicos relacionados con el UHF, en 2007 podrían utilizarse 3.100 millones de *tags* para identificar *pallets* y envases. El "*Item level tagging*" concretamente de productos farmacéuticos, así como de equipajes, animales, libros, billetes y otros objetos fuera del mercado de la distribución está creciendo significativamente en valor: en 2008 van a venderse 6.800 millones de *tags* por año para este tipo de aplicaciones y 15.300 millones de *tags* para pallets/envases, sin embargo éstos tendrán un valor muy inferior respecto de los de las aplicaciones mencionadas anteriormente.

El mercado de lectores RFID va a alcanzar los 1.140 millones de dólares en 2008 para los lectores en ámbito EPC, y 750 millones, el mismo año, para los lectores de otro tipo, entre otros, los que son para la tecnología *Near Field Communication*.

Desde un punto de vista territorial, según dichas previsiones, antes de 2010 un 48% de los tags, en números, se venderán en Asia oriental, seguido por un 32% en Norteamérica. Suministros y pedidos en 2004 han rebasado de mucho los del año anterior.
La consecuencia es que si, por error, aún se considerara el tag RFID nada más que una manera para sustituir el código de barras, dicha previsión resultaría ulteriormente confirmada, porque en el mundo se imprimen todos los años de cinco a diez billones de códigos de barras. Considerando que, para sustituir el código de barras, los tags tendrían por lo menos que imprimirse y costar menos que un centavo, el importe de diez billones de tags no podrá alcanzarse antes de 2020.

IDTechEx duda que el *tag* a un centavo, necesario para marcar cada producto en las estanterías del supermercado – la aplicación con mayores potencialidades para la RFID en cuanto a volúmenes – pueda alcanzarse con chips en silicio, ni siquiera para el 2015. La compañía considera que los gigantes como IBM, Xerox, Dai Nipón Printing y Samsung, que están desarrollando alternativas "sin chip", entre otras, circuitos transistores basados en polímeros y dispositivos SAW, van por el camino correcto, sobre todo a largo plazo.

Resumen de precios en cuadros comparativos:

sistemas de baja frecuencia			
dispositivo RFID	Tipo	modelo	precio
readers	Portátiles	usb pen readers	$39.46
		CF RFID Card 125 kHz	$132.19
		DLP-RFID1	$160.13
		LF Bluetooth scanner	$599.00
		IPAQ RFID EM4102/UNIQUE	$670.80
	fijos	ID40	$147.98
		ID70	$434.06
		Series 2000 Reader S251B	$589.89
		25K-R-USB-KB-D1	$49.00

sistemas de alta frecuencia			
dispositivo RFID	tipo	modelo	precio
readers	portatiles	SDiD™ 1010 MIFARE ISO14443A	$147.98
		Freedom HF Bluetooth Scanner	$599.00
		Socket CF Rfid Reader Card HF	$219.00
	fijos	Socket CF Rfid Reader Card HF	$4,083.09
tags		Sokymat Disc Tag	$2.13
		ACG Philips Mifare Card	$1.24

Anexo 3: Factibilidad técnico-comercial

El siguiente estudio de factibilidad técnica y económica esta dirigido a la cadena de suministros, la referencia de tiempo en el cual se deberán ubicar las interrogantes será tres y un año antes de la fecha actual y una proyección de un año en el futuro.
La introducción de la tecnología de RFID en el sector minorista apuntaría a la disminución de costos de implementación de *transponders*. Es de suponer que este estudio debería provocar cambios significativos en el desarrollo de la cadena de suministros de una empresa.
Este puede ser implementado en diferentes rubros de empresas en los cuales se asumen que poseen la capacidad de implementación de un sistema de etiquetado de RFID en sus procesos, este estudio se apoya de cuestionamientos planteados por analistas económicos de *EPC Global* en el cual se abordan puntos clave como son:

- Como poder resolver las cuestiones estratégicas que se les planteen.
- Como poder resolver los impedimentos que se verán a la luz, en el desarrollo del cuestionario
- Podrán evolucionar hacia mejores resultados en sus negocios y en los valores entregados al consumidor.

Ubic**a**ción de la empresa en la cadena de suministro:

- Fabricante
- Distribuidor
- Logístico
- Otro (especificar)

1 Situación Actual

1.1 Indicadores claves de rendimiento

1.1.1 indicadores claves de rendimiento financiero

- Ventas totales (en millones de $)
- Beneficio anual (en millones de $)
- Logística y costes de almacenaje (en millones de $)
- EBITDA[14] (en millones de $)
- Cuota de mercado (en %)

[14] Por sus siglas en ingles significa “Earnings Before Interests, Tax, Depreciation and Amortization” lo que significa margen o resultado bruto de explotación de la empresa antes de deducir los intereses (carga financiera), las amortizaciones o depreciaciones y el impuesto sobre sociedades.

1.1.2 indicadores claves del rendimiento operativo

- Número de roturas de stock en tiendas (en %)
- Rotación de inventario minorista % de entregas enviadas puntualmente por los fabricantes
- Rotación de inventario del fabricante
- Plazo de entrega medio del centro de distribución (CD) del minorista a las tiendas
- Plazo de entrega medio del CD central del fabricante al CD central del minorista
- Plazo de entrega medio de la planta de fabricación al CD central del fabricante

1.1.3 Información general

- Tamaño medio de las tiendas (en metros cuadrados)
- Número de unidades de almacenamiento (SKU)[15] por tienda
- Número de proveedores que constituyen el 80% de las ventas
- % de ventas conseguido mediante actividades promociónales
- Número de tiendas (sólo en el mercado nacional)
    - Mini mercado (<5.000 m², menos de 1.600 SKU)
    - Supermercado (<5.000 m², más de 1.600 SKU)
    - Hipermercado (>5.000 m², más de 1.600 SKU)

1.2 Estrategia

1.2.1 Intercambio de información

1.2.1.1 La empresa intercambia datos con otros miembros de su cadena de suministro (la respuesta puede estar dentro de los siguientes apartados)
a) Sí, con todos los miembros
b) Sí, pero sólo con jefes / asesores de categoría
c) No, en absoluto
d) Otros:
e) No sabe / no aplicable

1.2.1.2 Tipo de datos compartidos

a) Datos de los puntos de venta
b) Datos de las ventas de las categorías
c) Previsiones de demanda
d) Sincronización de actividades promociónales
e) Precio de promoción
f) Índice de la competencia

[15] Acrónimo de **Stock Keeping Unit**. Es un identificador usado en el Comercio con el objeto de permitir el seguimiento sistemático de los productos y servicios ofrecidos a los clientes.

g) Avisos de envíos con antelación
h) Otros:
i) No sabe / no aplicable

1.2.1.3 Frecuencia con que se intercambian los datos

- Menos de una vez por semana
- Una vez por semana
- Dos veces por semana
- Cada dos días
- Una vez al día
- Dos veces al día
- En tiempo real

1.3 Entorno competitivo

1.3.1 En la opinión de su empresa como es de interés la competencia en su sector valorada dentro de un rango del 1 al 10

1.3.2 A continuación se muestran atributos de importancia que puede poseer la competencia de su empresa, los cuales pueden ser calificados del 1 al 10, que atributos posee dicha competencia:

- Precios
- Promociones
- Servicios
- Localización
- Calidad
- Surtido
- Eficiencia operativa
- Índice de innovación
- Otros

1.4 Impedimentos

1.4.1 Detalle cual es la relación con sus minoristas y fabricantes

- De confrontación
- Neutral
- Comprometedora

1.4.2 Como se conceden los contratos de suministro

- Concursos de ofertas basadas en precios.
- Planificación colaborativa (con negociaciones)

1.4.3 Hasta que punto tienen en cuenta explícitamente las leyes de su región de ubicación en materia de competencia al determinar el nivel cooperación con los miembros de su cadena de suministro minorista en una escala del 1 al 10.

2 Cuestiones futuras

2.1 Efecto de RFID en las finanzas

2.1.1 En que áreas espera beneficiarse mas de RFID, calificando los siguientes parámetros en una escala del 1 al 10

- Ahorro de costes laborales
- Mayores ventas en tiendas
- Mayor trafico en tiendas
- Mayor servicio al cliente
- Mejores promociones minoristas
- Menos roturas de stock
- Mejores promociones de fabricantes
- Mejor introducción de nuevos productos
- Menor coste total
- Menos mermas
- Menor cantidad de robos
- Otras

2.1.2 Quien se beneficiara de RFID y cuanto, se calificaran los factores en una escala del 1 al 10

- Minoristas distribuidores
- Fabricantes
- Proveedores
- Clientes
- Proveedores de servicios logísticos
- Otros

2.1.3 que impacto sobre los costes se espera que tenga para el fabricante la introducción e implementación de RFID en los próximos 5 años (en porcentaje de ventas anuales), (<=1%, 2-3%, 3-5%, 5-10%, Más del 10%).

2.1.4 Que impacto se espera que tenga para el fabricante la introducción e implementación de RFID en los próximos 5 años (en porcentaje de ventas anuales), (Negativo, 1-2%, 3-5%, 5-10%, Más del 10%).

2.1.5 Qué impacto sobre el volumen de ventas se espera que tenga para el fabricante la introducción e implementación de RFID en los 5 próximos años (en porcentaje de ventas anuales), (Negativo, 1-2%, 3-5%, 5-10%, Más del 10%).

2.1.6 Qué impacto sobre los costes se espera que tenga para el minorista la introducción e implementación de RFID en los 5 próximos años (en porcentaje de ventas anuales), (<=1%, 2-3%, 3-5%, 5-10%, Más del 10%).

2.1.7 Qué impacto sobre el beneficio se espera que tenga para el minorista la introducción e implementación de RFID en los 5 próximos años (en porcentaje de ventas anuales), (Negativo, 1-2%, 3-5%, 5-10%, Más del 10%).

2.1.8 Qué impacto sobre el volumen de ventas se espera que tenga para el minorista la introducción e implementación de RFID a medio plazo (en porcentaje de ventas anuales), (Negativo, 1-2%, 3-5%, 5-10%, Más del 10%).

2.2 RFID y la tecnología de la información

2.2.1 Cómo usarán los minoristas/distribución los datos generados por RFID a corto plazo, evaluando los siguientes ítems en un rango del 1 al 10.

- Gestión de la demanda
- Seguimiento de clientes en la tienda
- Seguimiento de productos fuera de la tienda
- Gestión de promociones minoristas
- Gestión de categorías
- Programas de fidelidad de los clientes
- Marketing directo en la tienda
- Marketing directo fuera de la tienda
- Optimización del transporte / logística / cadena de suministro
- Introducción de nuevos productos
- Control de mermas
- Otros

2.2.2 Cómo usarán los fabricantes los datos generados por RFID a corto plazo, evaluando los siguientes ítems en un rango del 1 al 10.

- Gestión de inventario
- Trazabilidad de producción (recepción de materia prima, trazabilidad de l stock en curso, trazabilidad de los productos acabados)
- Gestión de promociones del fabricante
- Optimización del transporte / logística / cadena de suministro
- La cadena de suministro segura (logística inversa, gestión de caducidades)
- Planificación de la cadena de suministro (previsiones, coordinación)

- Control de mermas
- Otros

2.2.3 Dónde se guardarán los datos generados por los sistemas de RFID dentro de los socios de la cadena de suministros.

- Minorista
- Fabricante

2.2.4 Quién tendrá acceso a los datos.

- Fabricantes de artículos de marca
- Proveedores clave de los minoristas
- Minoristas
- Proveedores de servicios logísticos
- Otros

2.2.5 A qué nivel de resolución se implementará RFID (en los 3 próximos años).

- Ninguno
- Paleta
- Caja
- Artículo
- No sabe / no aplicable

2.2.6 Con qué amplitud se implementará RFID en su cadena de suministro.

- Tienda minorista
- Almacén central del minorista
- Almacén central del fabricante
- Proveedor de servicios logísticos
- Planta del fabricante
- Proveedores principales del fabricante
- No sabe / no aplicable

2.2.7 Hasta cuándo planean usar códigos de barras en su cadena de suministro.

- Próximos 1-3 años
- Próximos 3-5 años
- Más allá de los próximos 5 años
- No sabe / no aplicable

2.2.8 Quién soportará el coste de la infraestructura de RFID (lectores, redes, hardware y software), clasificándolos del 1 al 10.

- Minoristas
- Fabricantes
- Proveedores de servicios logísticos
- No sabe / no aplicable

2.2.9 Quién soportará los costes de los *transponders* de RFID, clasificándolos del 1 al 10.

- Minoristas
- Fabricantes
- Proveedores de servicios logísticos
- No sabe / no aplicable

2.2.10 Quién pagará la implementación organizativa de la tecnología RFID, clasificándolos del 1 al 10.

- Minoristas
- Fabricantes
- Proveedores de servicios logísticos
- No sabe / no aplicable

2.3 Estrategia

2.3.1 Quién gestionará el inventario a nivel minorista en el futuro.

- Minoristas
- Fabricantes
- Proveedores de servicios logísticos
- No sabe / no aplicable

2.3.2 Quién gestionará los precios minoristas en el futuro.

- Minoristas
- Fabricantes
- No sabe / no aplicable

2.3.3 Quién gestionará el surtido minorista en el futuro.

- Minoristas
- Fabricantes
- No sabe / no aplicable

2.3.4 Qué importancia tiene la implementación de RFID en su empresa desde un punto de vista estratégico, evaluándolo en un rango de 1 a 10.

2.3.5 en un rango del 1 al 10 que posición tomara de liderazgo o de seguimiento tomara su empresa en la implementación de RFID.

2.4 Entorno externo.

2.4.1 Cómo cambiarán sus estructuras de toma de decisiones con la implementación de RFID

- Serán menos centralizadas
- No cambiarán
- Serán más centralizadas

2.4.2 RFID tendrá un impacto sobre el grado de colaboración entre los miembros de su cadena de suministros.

- Menor
- La colaboración será la misma
- Mayor

2.4.3 RFID tendrá un impacto sobre el nivel de competencia entre fabricantes.

- Menor
- La competencia entre fabricantes será la misma
- Mayor

2.4.4 RFID tendrá un impacto sobre el nivel de competencia entre minoristas.

- Menor
- La competencia entre fabricantes será la misma
- Mayor

2.4.5 Influirá RFID e n la variedad de productos.

- Poco
- La variedad será la misma
- Mucho

2.4.6 Afectará RFID a la fidelidad de los consumidores a la tienda.

- Poco
- La fidelidad será la misma
- Mucho

2.4.7 Se verá afectado el gasto de los consumidores.

- Poco
- El gasto será el mismo
- Mucho

2.4.8 Se verá afectada la frecuencia de las compras.

- Poco
- La frecuencia será la misma
- Mucho

2.4.9 Será RFID un motivo para que sus clientes cambien de tienda.

- Poco
- Influirá en el ratio de cambio de tienda
- Mucho

2.4.10 La mayor eficiencia operativa debida a RFID afectará al tamaño de las tiendas.

- Poco
- El tamaño de las tiendas será el mismo
- Mucho

2.4.11 Afectará RFID a la frecuencia de las promociones minoristas.

- Poco
- La frecuencia de la promociones minoristas será la misma
- Mucho

2.4.12 Afectará RFID a la frecuencia de las promociones del fabricante.

- Poco
- La frecuencia de las promociones del fabricantes será la misma
- Mucho

2.5 Impedimentos

2.5.1 Se proponen abordar el reciclaje de los componentes electrónicos, por ejemplo, los *tags* de RFID

- No interesados
- Algo interesados
- Muy interesados

2.5.2 Se proponen abordar nuevos modos de reciclar materiales de empaquetado.

- No interesados
- Algo interesados
- Muy interesados

2.5.3 Se proponen abordar las preocupaciones sanitarias de los consumidores.

- No interesados
- Algo interesados
- Muy interesados

2.5.4 Se proponen abordar las preocupaciones sanitarias de los empleados.

- No interesados
- Algo interesados
- Muy interesados

2.5.5 Se proponen abordar temas de privacidad.

- No interesados
- Algo interesados
- Muy interesados

2.5.6 Se proponen abordar la manipulación de las etiquetas a nivel de artículo.

- No interesados
- Algo interesados
- Muy interesados

2.5.7 Se proponen abordar el acceso no autorizado a datos a nivel global.

- No interesados
- Algo interesados
- Muy interesados

2.5.8 Se proponen abordar las leyes de su región de ubicación en materia de competencia y las leyes antimonopolio de EEUU.

- No interesados
- Algo interesados
- Muy interesados

Anexo 4: Codigo fuente

```
unit mifare1;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, ComCtrls, ExtCtrls, Menus, ImgList, StdCtrls, ActnList;

type
  TForm1_Mlfare1 = class(TForm)
    PageControl1: TPageControl;
    Panel1: TPanel;
    Panel2: TPanel;
    ActionList1: TActionList;
    GroupBox1: TGroupBox;
    ComboBox_ComNum: TComboBox;
    Label1: TLabel;
    Button1: TButton;
    Button2: TButton;
    GroupBox2: TGroupBox;
    Button4: TButton;
    Button5: TButton;
    GroupBox3: TGroupBox;
    ComboBox_Sector: TComboBox;
    ComboBox_BlockNum: TComboBox;
    Label2: TLabel;
    Label3: TLabel;
    Edit_KeysANum: TEdit;
    RadioButton_keysA: TRadioButton;
    RadioButton_keysB: TRadioButton;
    Label4: TLabel;
    Button6: TButton;
    Button7: TButton;
    GroupBox9: TGroupBox;
    Action_OpenComPort: TAction;
    Action_CloseComPort: TAction;
    Action3: TAction;
    Action_close: TAction;
    Action_CloseRF: TAction;
    Action_OpenRF: TAction;
    Action_GetInfo: TAction;
```

Action_GetCarddata: TAction;
Action_changkeys: TAction;
Action_SingleWritedata: TAction;
Action_InitData: TAction;
Action_incdata: TAction;
Action_decdate: TAction;
Label9: TLabel;
Edit_keysBnum: TEdit;
Panel3: TPanel;
GroupBox4: TGroupBox;
Label5: TLabel;
Label6: TLabel;
Label7: TLabel;
Label8: TLabel;
Edit_Block0data: TEdit;
Edit_Block1data: TEdit;
Edit_Block2data: TEdit;
Edit_Block3data05: TEdit;
StatusBar1: TStatusBar;
GroupBox10: TGroupBox;
Label16: TLabel;
Label18: TLabel;
Edit_Readerinfo: TEdit;
Edit_CardNum: TEdit;
Edit_CardType: TEdit;
Edit_CardSize: TEdit;
GroupBox6: TGroupBox;
Label14: TLabel;
Button11: TButton;
Button12: TButton;
Button13: TButton;
Edit_getInitdata: TEdit;
Edit_UseData: TEdit;
Label11: TLabel;
Label12: TLabel;
GroupBox8: TGroupBox;
Button15: TButton;
Edit_Block3data69: TEdit;
Edit_Block3data1015: TEdit;
ComboBox_Sector_2: TComboBox;
ComboBox_BlockNum_2: TComboBox;
Label27: TLabel;
Label28: TLabel;
RadioButton_keysA2: TRadioButton;

```
  RadioButton_keysB2: TRadioButton;
  Edit_KeysatINCDEC: TEdit;
  Action_ReadCurrentdata: TAction;
  Label13: TLabel;
  GroupBox5: TGroupBox;
  Label19: TLabel;
  Label20: TLabel;
  Edit1_keya: TEdit;
  Edit1_Keyb: TEdit;
  Button9: TButton;
  StaticText1: TStaticText;
  StaticText2: TStaticText;
  GroupBox7: TGroupBox;
  Button8: TButton;
  Button3: TButton;
  procedure FormCreate(Sender: TObject);
  procedure Action_OpenComPortExecute(Sender: TObject);
  procedure Action_CloseComPortExecute(Sender: TObject);

  procedure FormClose(Sender: TObject; var Action: TCloseAction);

  procedure Action_closeExecute(Sender: TObject);
  procedure Action_OpenRFExecute(Sender: TObject);
  procedure Action_CloseRFExecute(Sender: TObject);
  procedure Action_GetInfoExecute(Sender: TObject);
  procedure Action_GetCarddataExecute(Sender: TObject);
 // procedure Action_GenDataExecute(Sender: TObject);
  procedure Action_OpenComPortUpdate(Sender: TObject);
  procedure Action_OpenRFUpdate(Sender: TObject);
  procedure Action_SingleWritedataExecute(Sender: TObject);
  procedure Action_changkeysExecute(Sender: TObject);
  procedure Action_InitDataExecute(Sender: TObject);
  procedure Action_incdataExecute(Sender: TObject);
 // procedure N17Click(Sender: TObject);
  //procedure MIfareI1Click(Sender: TObject);
  procedure Action_decdateExecute(Sender: TObject);
  procedure Action_ReadCurrentdataExecute(Sender: TObject);
  procedure N12Click(Sender: TObject);
  procedure Action_GetInfoUpdate(Sender: TObject);
  procedure Action_changkeysUpdate(Sender: TObject);
  procedure Action_SingleWritedataUpdate(Sender: TObject);
  procedure Action_InitDataUpdate(Sender: TObject);
private
fOpenComNum : integer;
```

```
  comisopen : boolean;
  RFisOpen : boolean;

    { Private declarations }

   procedure initcomlist;
   procedure initComboBox_Sectorlist;
  procedure initComboBox_BlockNumlist;

  procedure initComboBox_Sector_2list;
  procedure initComboBox_BlockNum_2list;

function checkHexStr(s: String): boolean;
function checkDNum(s:string ) :boolean;
////////////////////////////////
  public
    { Public declarations }
  end;

var
  Form1_MIfare1: TForm1_MIfare1;

implementation

uses MIfareIDDL_HEAD,   MIhelp;

{$R *.dfm}

procedure TForm1_MIfare1.FormCreate(Sender: TObject);

begin

   initcomlist;
   initComboBox_Sectorlist;
    initComboBox_BlockNumlist;
     Edit_KeysANum.Text:='FFFFFFFFFFFF';

     initComboBox_Sector_2list;
    initComboBox_BlockNum_2list;
    RFisOpen := false;

    //---------------------------------
     Edit_Block0data.Color := clBtnFace;
       Edit_Block1data.Color := clBtnFace;
```

```
      Edit_Block2data.Color := clBtnFace;
       Edit_Block3data05.Color := clBtnFace;
       Edit_Block3data69.Color  := clBtnFace;
       Edit_Block3data1015.Color  := clBtnFace;
       ComboBox_Sector.Color  := clBtnFace;
       ComboBox_BlockNum.Color := clBtnFace;
        Edit_KeysANum.Color :=  clBtnFace;
         Edit_KeysBNum.Color :=  clBtnFace;
 //-----------------------------------------------
  Edit1_keya.Color := clBtnFace;
     Edit1_Keyb.Color := clBtnFace;
 //-----------------------------------------------
  ComboBox_Sector_2.Color := clBtnFace;
     ComboBox_BlockNum_2.Color := clBtnFace;
    Edit_KeysatINCDEC.Color := clBtnFace;
    Edit_getInitdata.Color := clBtnFace;
    Edit_UseData.Color := clBtnFace;
 //-----------------------------------------------------

end;

  procedure TForm1_MIfare1.initcomlist;
 var
 i :integer;
 begin
     ComboBox_ComNum.Items.Clear;
     ComboBox_ComNum.Items.Add(' AUTO') ;
     for i:=1 to 12 do

       ComboBox_ComNum.Items.Add(' COM'+inttostr(i)) ;

      ComboBox_ComNum.ItemIndex:= 0;

  end ;

 procedure TForm1_MIfare1.initComboBox_Sectorlist;
 var
 i:integer;
 begin
    ComboBox_Sector.Items.Clear;

   for i:=0 to 15 do
    ComboBox_Sector.Items.Add("+inttostr(i));
```

```
 ComboBox_Sector.ItemIndex:=  ComboBox_Sector.Items.IndexOf('1');
end ;

procedure TForm1_MIfare1.initComboBox_BlockNumlist;
 var
 i:integer;
 begin
      ComboBox_BlockNum.Items.Clear;
      for i:= 0 to 3 do
      ComboBox_BlockNum.Items.Add("+inttostr(i)) ;
       ComboBox_BlockNum.ItemIndex:=ComboBox_BlockNum.Items.IndexOf('0')
;
 end ;

 procedure TForm1_MIfare1.initComboBox_Sector_2list;
 var
 i:integer;
 begin
    ComboBox_Sector_2.Items.Clear;

   for i:=0 to 15 do
    ComboBox_Sector_2.Items.Add("+inttostr(i));

 ComboBox_Sector_2.ItemIndex :=  ComboBox_Sector_2.Items.IndexOf('0');
 end ;
procedure TForm1_MIfare1.initComboBox_BlockNum_2list;
 var
 i:integer;
 begin
      ComboBox_BlockNum_2.Items.Clear;
       // for i:= 0 to 3 do
      for i:= 0 to 2 do   //====================================
      ComboBox_BlockNum_2.Items.Add("+inttostr(i)) ;
      ComboBox_BlockNum_2.ItemIndex:=ComboBox_BlockNum_2.Items.IndexO
f('0') ;
 end ;


 ////////////////////////////////////////////////////////////////////////////
 //  ´Función para abrir puerto serie
//////////////////////////////////////////////////////////////
 // AutoOpenComPort( Port: pchar)  :longint;stdcall;
procedure TForm1_MIfare1.Action_OpenComPortExecute(Sender: TObject);
var
```

```
 i:integer;
 t: string ;
 port : array[0..0] of char;
 portindex:integer;
begin
  if ComboBox_ComNum.ItemIndex= 0 then
    begin
       if  AutoOpenComPort(port)=0 then
       begin

      BUZZER(0,1,1,1);
       for i:=0 to 0do
     t:=t+ inttohex(ord(Port[i]),2);
     fOpenComNum:= strtoint(t);


                    StatusBar1.Panels.Items[0].Text  :=  'Port  state£ºOpen  COM' +
IntToStr(fOpenComNum+1);
        comisopen :=true ;
        RFisOpen :=true;
       end
       else
       begin
         MessageDlg('Serial  Communication Error', mtInformation, [mbOk], 0);
         exit;
       end;
    end
    else
    begin
    //   función   OpenComPort(Port:integer):longint; stdcall;
      portindex:= ComboBox_ComNum.ItemIndex-1;
       if  OpenComPort(portindex)=0 then
        begin
      BUZZER(0,1,1,1);

      comisopen :=true ;
      RFisOpen :=true;

                 StatusBar1.Panels.Items[0].Text  :=  'Port  state£ºOpen  COM' +
IntToStr(fOpenComNum+1);
       end
       else
       begin
```

```
        MessageDlg('Serial  Communication Error', mtInformation, [mbOk], 0);
         exit;
       end;
    end ;

 //--===-----------------------------------
      Edit_Block0data.Color := clWindow;
      Edit_Block1data.Color := clWindow;
      Edit_Block2data.Color := clWindow;
       Edit_Block3data05.Color := clWindow;
       Edit_Block3data69.Color  := clWindow;
       Edit_Block3data1015.Color  := clWindow;
       ComboBox_Sector.Color  := clWindow;
       ComboBox_BlockNum.Color := clWindow;
       Edit_KeysANum.Color:= clWindow;
       Edit_KeysBNum.Color:= clWindow;

 //--------------------------------------- -  --
     Edit1_keya.Color :=  clWindow;
     Edit1_Keyb.Color :=   clWindow;
 //-----------------------------------------------
   ComboBox_Sector_2.Color := clWindow;
     ComboBox_BlockNum_2.Color := clWindow;
    Edit_KeysatINCDEC.Color := clWindow;
    Edit_getInitdata.Color := clWindow;
    Edit_UseData.Color := clWindow;
 //-----------------------------------------------
end;

//////////////////////////////////////////////////////////////////////
// Cerrar el puerto serie
//////////////////////////////////////////////////////
procedure TForm1_MIfare1.Action_CloseComPortExecute(Sender: TObject);
begin
   //function  CloseComPort():longint; stdcall;
    BUZZER(0,1,1,1);
   if  CloseComPort()=0 then
   begin
    Edit_Readerinfo.Text:='';
    Edit_CardNum.Text :='';
    Edit_CardType.Text :='';
    Edit_CardSize.Text :='';
    Edit_Block0data.Text :'' ;
     Edit_Block1data.Text :'' ;
```

```
      Edit_Block2data.Text :=" ;
       Edit_Block3data05.Text :=" ;
     Edit_Block3data69.Text :=" ;
     Edit_Block3data1015.Text :=" ;
    //
     StatusBar1.Panels.Items[0].Text := 'Port state£ºClose ComPort' ;
     comisopen :=false;
   end ;
    //-------------------------------------
      Edit_Block0data.Color := clBtnFace;
      Edit_Block1data.Color := clBtnFace;
      Edit_Block2data.Color := clBtnFace;
      Edit_Block3data05.Color := clBtnFace;
      Edit_Block3data69.Color  := clBtnFace;
      Edit_Block3data1015.Color  := clBtnFace;
      ComboBox_Sector.Color  := clBtnFace;
      ComboBox_BlockNum.Color := clBtnFace;
      Edit_KeysANum.Color :=  clBtnFace;
      Edit_KeysBNum.Color :=  clBtnFace;
    //-------------------------------------
     Edit1_keya.Color := clBtnFace;
     Edit1_Keyb.Color := clBtnFace;
    //-------------------------------------
       ComboBox_Sector_2.Color := clBtnFace;
     ComboBox_BlockNum_2.Color := clBtnFace;
    Edit_KeysatINCDEC.Color := clBtnFace;
    Edit_getInitdata.Color := clBtnFace;
    Edit_UseData.Color := clBtnFace;
    //-------------------------------------

end;
////////////////////////////////////////////////
// Mensaje de salida
////////////////////////////////////////////////
procedure TForm1_MIfare1.FormClose(Sender: TObject;
  var Action: TCloseAction);
begin
              //if MessageDlg('ÊÇ·ñ¹Ø±Õµ±Ç°´°¿Ú?',mtconfirmation,
            //  [mbyes,mbno],0)=mrYes then
     if MessageDlg('Desear cerrar la aplicación?',mtconfirmation,
     [mbyes,mbno],0)=mrYes then

     Action :=caFree
     else
```

```
      Action :=caNone;
end;
////////////////////////////////////
///función SALIR
////////////////////////////////////
procedure TForm1_MIfare1.Action_closeExecute(Sender: TObject);
begin
 CloseComPort();
 comisopen :=false;
 close;
end;
//////////////////////////////////////////////////////////////////////////////
//function OpenRf():longint;stdcall;
// ´ò¿ªÉäÆµ
////////////////////////////////////////////////
procedure TForm1_MIfare1.Action_OpenRFExecute(Sender: TObject);
begin
//
   if OpenRf()= 0 then
   begin
     BUZZER(0,1,1,1);
     RFisOpen :=true;
     end;
end;
////////////////////////////////////////////////
// ¹Ø±ÕÉäÆµ
 //function CloseRf():longint;stdcall ;
procedure TForm1_MIfare1.Action_CloseRFExecute(Sender: TObject);
begin

   if CloseRf()= 0 then
   begin
     BUZZER(0,1,1,1);
     RFisOpen := false;
     end;
end;
//////////////////////////////////////////////////////////////////////////////
//funciónn GetInfo(info:pchar):longint;stdcall;
// obtiene la información de los datos de fabricación del tag
//////////////////////////////////////////////////////////////////////////////
procedure TForm1_MIfare1.Action_GetInfoExecute(Sender: TObject);
 var
    i:integer;
    t:string;
```

```
    info:array[0..12] of char ;
  ////
    Gdata11:array[0..3]of char;
    i1:integer;
    t1:string;
    Mode1:integer ;

   data22:array[0..3]of char;
   ii2:integer;
   tt2:string;
   xvar:integer;

 Rdatasize :array[0..12] of char;
   iii3:integer;
   ttt3 :string;
    SCardSn :longint;
//Para la genración del archivo ASCII
//  myFile : TextFile;
  text   : string;

begin

xvar:=1;
//while xvar <= 15 do
begin

 if GetInfo(info)=0  then
  begin

    for i:=0 to 12 do
      t:=t+ inttohex(ord(info[i]),2);

       Edit_Readerinfo.Text:= t;

   end
  else
  begin
   Edit_Readerinfo.Text:= 'NADA';
    end;
      Mode1:= 0;
    if  RRMifare_Request(Mode1, Gdata11)=0 then
      begin

      for i1:= 3 downto 0 do
```

```
        t1:=t1+ inttohex(ord(Gdata11[i1]),2);

        Edit_CardType.Text:= t1;
        end
         else
         begin
           Edit_CardNum.Text:='NADA';
           //WriteLn(myFile, 'NADA');
           //exit;
          end;

        if   RRMifare_AntiColl(data22)=0 then
       begin

         for ii2:= 3 downto 0 do
       tt2:=tt2+ inttohex(ord(data22[ii2]),2);
          Edit_CardNum.Text:= tt2;
      end ;
 //      AssignFile(myFile, 'usuarios.txt');
   //    Append(myFile);
     //  WriteLn(myFile, 'lectura'  );
//       WriteLn(myFile, Edit_CardNum.Text);
  //     CloseFile(myFile);
        if tt2 <> '' then
         SCardSn := strtoint64('$'+tt2);
     if RRMifare_Select(SCardSn,Rdatasize)=0 then
         begin
           BUZZER(0,1,1,1);
         for iii3:=0 to 3 do
         //ttt3:=ttt3+ inttohex(ord(Rdatasize[iii3]),2);
          //Edit_CardSize.Text:= ttt3;
    randomize();
         //ttt3:=ttt3+ inttohex(ord(retdatasize[iii3]),2);
         i := 1 + Random(100000);
         Edit_CardSize.Text := IntToStr(i);
 //        AssignFile(myFile, 'aleatorio.txt');
   //      Append(myFile);
     //    Write(myFile,Edit_CardSize.Text+'');
      //   WriteLn(myFile,'');
    //     CloseFile(myFile);

          end
          else
          begin
```

```
            Edit_CardSize.Text:='NADA';
            end ;

Edit_CardNum.Invalidate;
GroupBox10.Repaint;
GroupBox10.Refresh;
Sleep(1000);
xvar:=xvar+1;
tt2:= '';
ttt3:= '';
t1:= '';
t:= '';
end;

//Sleep(1000);
end; //end del while
////////////////////////////////////////////////////////////////////////////////
//función de leer los datos almacenados en el tag
////////////////////////////////////////////////////////////////////////
procedure TForm1_MIfare1.Action_GetCarddataExecute(Sender: TObject);
 var
  data11:array[0..3]of char;
   i1:integer;
   t1:string;
    Mode1:integer ;
 /////////
   data22:array[0..3]of char;
    ii2:integer;
    tt2:string;

  retdatasize :array[0..12] of char;
    iii3:integer;
    ttt3 :string;
     CardSn :longint;

    Mode:integer ;
    Sector:integer;

   data33:array[0..5]of char;
      iiii4:integer;
       tttt4 :string;
 i5 :integer;
 t5 :string;
  i15 :integer;
```

```
  t15 :string ;

  i25 :integer;
  t25 :string ;
   i35 :integer;
   t35 :string ;

    t35_69 : string ;
     t35_1015  : string ;

 BlockNo0 :integer;
  BlockNo1 :integer;
  BlockNo2 :integer;
  BlockNo3:integer;
  ReadBuff0 :array[0..15] of char ;
  ReadBuff1 :array[0..15] of char ;
  ReadBuff2 :array[0..15] of char ;
  ReadBuff3 :array[0..15] of char ;
  xvar:integer;
  palabra2 :string;
  palabra :string;
  longitud : integer;
  i :integer;
//  myFile : TextFile;
  text   : string;
  Archivo : TStringList;
  LineaPermiso, LineaBlanco,  LineaTarjeta, LineaBloque: string;
begin
                        //      function                        RRMifare_Request(Mode:integer;
CardTypeNo:pchar):longint;stdcall;
xvar:=1;
//while xvar <= 10 do  //numero d repeeticiones
begin
      Mode1:= 0;
      if  RRMifare_Request(Mode1, data11)=0 then
       begin
       //BUZZER(0,1,1,1);
      for i1:= 3 downto 0 do
        t1:=t1+ inttohex(ord(data11[i1]),2);
         end
          else
          begin
            Edit_Block0data.Text:='nada';
            Edit_Block1data.Text:='nada';
```

```
          Edit_Block2data.Text:='nada';
          Edit_CardNum.Text:='NADA';
          Edit_CardSize.Text:= 'NADA';
          //Edit_Block3data.Text:='nada';
          //exit;
         end;
       if   RRMifare_AntiColl(data22)=0 then
      begin
       // BUZZER(0,1,1,1);
     for ii2:=3 downto 0 do
       tt2:=tt2+ inttohex(ord(data22[ii2]),2);
        Edit_CardNum.Text:= tt2;
       end;
////////////////////////////////////////////////////////////////////////////////

      if tt2 <> '' then
      CardSn := strtoint64('$'+ tt2);
   //  if RRMifare_Select(373365118,retdatasize)=0 then
     if RRMifare_Select(CardSn,retdatasize)=0 then
      //if RRMifare_Select(CardSn,retdatasize)=0 then
        begin
          //BUZZER(0,1,1,1);
         for iii3:=0 to 3 do
        ttt3:=ttt3+ inttohex(ord(retdatasize[iii3]),2);
          // Edit5.Text:=Edit5.Text+ttt3;
          // Edit_CardSize.Text := Edit_CardSize.Text + ttt3;

    randomize();
        //ttt3:=ttt3+ inttohex(ord(retdatasize[iii3]),2);
         i := 1 + Random(100000);
        Edit_CardSize.Text := IntToStr(i);
//         AssignFile(myFile, 'aleatorio.txt');
 //        Append(myFile);
  //       Write(myFile,Edit_CardSize.Text+'');
   //      WriteLn(myFile,'');
    //     CloseFile(myFile);

      //    Edit_CardSize.Text := ttt3;
          //  application.MessageBox('Ñ¡Ôñ¿¨Ok','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
        end
        else
       begin
       // application.MessageBox('Ñ¡Ôñ¿¨´íÎó','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
       //--messagedlg('Select card error ',mtinformation,[mbOk],0) ;
```

```
          //--exit;
        end ;

  Mode:=0 ;
  // Mode:=1 ;        //=========================================
   Sector:= ComboBox_Sector.ItemIndex;  //+1

   if  RadioButton_keysA.Checked then
   begin
   tttt4 := Edit_KeysANum.Text;
    Mode:=0 ;

   end  ;
   if RadioButton_keysB.Checked then
   begin
     tttt4 := Edit_KeysBNum.Text;
      Mode:=1 ;
   end;
     //tttt4 := Edit_KeysBNum.Text;
     if Length( tttt4 )=12 then
     begin
        for iiii4:=0 to 5 do
          //keys[iiii4] := Char( StrToInt('$'+copy(tttt4,iiii4*2+1,2) ) );
          data33[iiii4]:=char( strtoint('$'+ copy(tttt4,iiii4*2+1,2)) );
         end
         else
         begin
                                        //    application.MessageBox('ÃÜÔ¿ÊäÈë´íÎó','ÐÅÏ
¢ÌáÊ¾',mb_iconinformation);
          //--messagedlg('Input key error ',mtinformation,[mbOk],0) ;
            //--exit;
         end ;
 //if  RRMifare_DirectAuthentication(mode,sector,keys)=0 then
  //if  RRMifare_DirectAuthentication(0,0,data33)=0 then
  if  RRMifare_DirectAuthentication(mode,sector,data33)=0 then
       begin
         //BUZZER(0,1,1,1);
       //application.MessageBox('ÃÜÔ¿ÑéÖ¤ok','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
         end
         else
         begin
                                       //    application.MessageBox('ÃÜÔ¿ÑéÖ¤´íÎó','ÐÅÏ
¢ÌáÊ¾',mb_iconinformation);
          //--messagedlg('key check error ',mtinformation,[mbOk],0) ;
```

```
            //--exit;
           end ;
   // Sleep(80);
//0-------------------------------------------------------------
  BlockNo0 :=  (ComboBox_Sector.ItemIndex )*4;
  BlockNo1 :=  (ComboBox_Sector.ItemIndex )*4+1;
  BlockNo2 :=  (ComboBox_Sector.ItemIndex )*4+2;
  BlockNo3 :=  (ComboBox_Sector.ItemIndex )*4+3;

  if   RRMifare_Read(BlockNo0,ReadBuff0)=0 then
  begin
     // BUZZER(0,1,1,1);
   for i5 := 0 to 15 do
     t5 := t5 + inttohex(ord(ReadBuff0[i5]),2) ;
     // Edit_Block0data.Text := Edit_Block0data.Text + t5;
       //CONVERSION A SCII

          longitud := length(t5);
  palabra2:='';
  i:=1;
  while i <= longitud do
  begin
       palabra := t5[i] + t5[i+1];
       if palabra = '65' then
             palabra2 := palabra2 + 'A';
       if palabra = '66' then
             palabra2 := palabra2 + 'B';
       if palabra = '67' then
            palabra2 := palabra2 + 'C';
       if palabra = '68' then
             palabra2 := palabra2 + 'D';
       if palabra = '69' then
             palabra2 := palabra2 + 'E';
       if palabra = '70' then
             palabra2 := palabra2 + 'F';
       if palabra = '71' then
            palabra2 := palabra2 + 'G';
       if palabra = '72' then
             palabra2 := palabra2 + 'H';
       if palabra = '73' then
             palabra2 := palabra2 + 'I';
       if palabra = '74' then
             palabra2 := palabra2 + 'J';
       if palabra = '75' then
```

```
            palabra2 := palabra2 + 'K';
        if palabra = '76' then
             palabra2 := palabra2 + 'L';
        if palabra = '77' then
             palabra2 := palabra2 + 'M';
        if palabra = '78' then
             palabra2 := palabra2 + 'N';
        if palabra = '79' then
            palabra2 := palabra2 + 'Ñ';
        if palabra = '80' then
             palabra2 := palabra2 + 'O';
        if palabra = '81' then
             palabra2 := palabra2 + 'P';
        if palabra = '82' then
             palabra2 := palabra2 + 'Q';
        if palabra = '83' then
             palabra2 := palabra2 + 'R';
        if palabra = '84' then
            palabra2 := palabra2 + 'S';
        if palabra = '85' then
             palabra2 := palabra2 + 'T';
        if palabra = '86' then
             palabra2 := palabra2 + 'U';
        if palabra = '87' then
             palabra2 := palabra2 + 'V';
        if palabra = '88' then
            palabra2 := palabra2 + 'W';
        if palabra = '89' then
             palabra2 := palabra2 + 'X';
        if palabra = '90' then
             palabra2 := palabra2 + 'Y';
        if palabra = '91' then
            palabra2 := palabra2 + 'Z';
        if palabra = '92' then
             palabra2 := palabra2 + ' ';

        i:=i+2;
end;
     if palabra2 = ''  then
       Edit_Block0data.Text:='nada';
 Edit_Block0data.Text:=palabra2;


      //Edit_Block0data.Text :=  t5;
```

```
  // application.MessageBox('¶ÁÈ¡0ok','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
  end
  else
  begin
     // application.MessageBox('¶ÁÈ¡0´íÎó','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
       //--messagedlg('Read Block0 error ',mtinformation,[mbOk],0) ;
       //--exit;
  end;
//1-----------------------------------------------------------
 if   RRMifare_Read(BlockNo1,ReadBuff1)=0 then
  begin
      //BUZZER(0,1,1,1);
   for i15 := 0 to 15 do
     t15 := t15 + inttohex(ord(ReadBuff1[i15]),2) ;
    // Edit_Block1data.Text := Edit_Block1data.Text + t15;

    longitud := length(t15);
  palabra2:='';
  i:=1;
  while i <= longitud do
  begin
       palabra := t15[i] + t15[i+1];
       if palabra = '65' then
             palabra2 := palabra2 + 'A';
       if palabra = '66' then
             palabra2 := palabra2 + 'B';
       if palabra = '67' then
            palabra2 := palabra2 + 'C';
       if palabra = '68' then
             palabra2 := palabra2 + 'D';
       if palabra = '69' then
             palabra2 := palabra2 + 'E';
       if palabra = '70' then
             palabra2 := palabra2 + 'F';
       if palabra = '71' then
            palabra2 := palabra2 + 'G';
       if palabra = '72' then
             palabra2 := palabra2 + 'H';
       if palabra = '73' then
             palabra2 := palabra2 + 'I';
       if palabra = '74' then
             palabra2 := palabra2 + 'J';
       if palabra = '75' then
            palabra2 := palabra2 + 'K';
```

```
        if palabra = '76' then
              palabra2 := palabra2 + 'L';
        if palabra = '77' then
              palabra2 := palabra2 + 'M';
        if palabra = '78' then
              palabra2 := palabra2 + 'N';
        if palabra = '79' then
             palabra2 := palabra2 + 'Ñ';
        if palabra = '80' then
              palabra2 := palabra2 + 'O';
        if palabra = '81' then
              palabra2 := palabra2 + 'P';
        if palabra = '82' then
              palabra2 := palabra2 + 'Q';
        if palabra = '83' then
              palabra2 := palabra2 + 'R';
        if palabra = '84' then
             palabra2 := palabra2 + 'S';
        if palabra = '85' then
              palabra2 := palabra2 + 'T';
        if palabra = '86' then
              palabra2 := palabra2 + 'U';
        if palabra = '87' then
              palabra2 := palabra2 + 'V';
        if palabra = '88' then
             palabra2 := palabra2 + 'W';
        if palabra = '89' then
              palabra2 := palabra2 + 'X';
        if palabra = '90' then
              palabra2 := palabra2 + 'Y';
        if palabra = '91' then
             palabra2 := palabra2 + 'Z';
        if palabra = '92' then
              palabra2 := palabra2 + ' ';

        i:=i+2;
end;
      if palabra2 = ''  then
         Edit_Block1data.Text:='nada';
 Edit_Block1data.Text:=palabra2;


//      Edit_Block1data.Text := t15;
   //application.MessageBox('¶ÁÈ¡1ok','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
```

```
end
else
begin
    //application.MessageBox('¶ÁÈ¡1´íÎó','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
     //--messagedlg('Read Block1 error ',mtinformation,[mbOk],0) ;
      //--exit;
end;
//2---------------------------------------------------------------
 if   RRMifare_Read(BlockNo2,ReadBuff2)=0 then
begin
    // BUZZER(0,1,1,1);
 for i25 := 0 to 15 do
   t25 := t25 + inttohex(ord(ReadBuff2[i25]),2) ;

   // Edit_Block2data.Text := Edit_Block2data.Text + t25;
     longitud := length(t25);
palabra2:='';
i:=1;
while i <= longitud do
begin
      palabra := t25[i] + t25[i+1];
      if palabra = '65' then
            palabra2 := palabra2 + 'A';
      if palabra = '66' then
            palabra2 := palabra2 + 'B';
      if palabra = '67' then
           palabra2 := palabra2 + 'C';
      if palabra = '68' then
            palabra2 := palabra2 + 'D';
      if palabra = '69' then
            palabra2 := palabra2 + 'E';
      if palabra = '70' then
            palabra2 := palabra2 + 'F';
      if palabra = '71' then
           palabra2 := palabra2 + 'G';
      if palabra = '72' then
            palabra2 := palabra2 + 'H';
      if palabra = '73' then
            palabra2 := palabra2 + 'I';
      if palabra = '74' then
            palabra2 := palabra2 + 'J';
      if palabra = '75' then
           palabra2 := palabra2 + 'K';
      if palabra = '76' then
```

```
            palabra2 := palabra2 + 'L';
        if palabra = '77' then
            palabra2 := palabra2 + 'M';
        if palabra = '78' then
            palabra2 := palabra2 + 'N';
        if palabra = '79' then
           palabra2 := palabra2 + 'Ñ';
        if palabra = '80' then
            palabra2 := palabra2 + 'O';
        if palabra = '81' then
            palabra2 := palabra2 + 'P';
        if palabra = '82' then
            palabra2 := palabra2 + 'Q';
        if palabra = '83' then
            palabra2 := palabra2 + 'R';
        if palabra = '84' then
           palabra2 := palabra2 + 'S';
        if palabra = '85' then
            palabra2 := palabra2 + 'T';
        if palabra = '86' then
            palabra2 := palabra2 + 'U';
        if palabra = '87' then
            palabra2 := palabra2 + 'V';
        if palabra = '88' then
           palabra2 := palabra2 + 'W';
        if palabra = '89' then
            palabra2 := palabra2 + 'X';
        if palabra = '90' then
            palabra2 := palabra2 + 'Y';
        if palabra = '91' then
           palabra2 := palabra2 + 'Z';
        if palabra = '92' then
            palabra2 := palabra2 + ' ';

        i:=i+2;
end;
     if palabra2 = ''  then
       Edit_Block2data.Text:='nada';
 Edit_Block2data.Text:=palabra2;
  end
  else
  begin
  end;
  //3-------------------------------------------------
```

```
 ControlLed(0);
 BUZZER(0,1,1,1);
        Sleep(80);
  ControlLed(1);

    // Creacion del TStringList
   Archivo := TStringList.Create;
   // se abre el alrchivo
   Archivo.LoadFromFile('users');
   // construccion de las lineas del archivo
   LineaTarjeta := '# Tarjeta numero:  '  +Edit_CardNum.Text;
         LineaBloque   :=   Edit_Block0data.Text+'      '   +   'Password   =   "'   +
Edit_CardSize.Text+'"';
   LineaPermiso := 'Permiso';
   LineaBlanco :='linea en blanco';
   // insertar las lineas en el StringList
   // siempre van desde el comienzo del archivo
   Archivo.Insert(0,LineaTarjeta);
   Archivo.Insert(1,LineaBloque);
   Archivo.Insert(2,LineaPermiso);
   Archivo.Insert(3,LineaBlanco);
   // limpiar los edits
 //  Edit_CardNum.Text := '';
 //  Edit_Block0data.Text := '';
 //  Edit_CardSize.Text := '';
   Archivo.SaveToFile('users');

   Archivo.Free;

//escribir resultados en archivo de texto
//AssignFile(myFile, 'users.txt');
//Append(myFile);
//WriteLn(myFile,'');
//WriteLn(myFile,'');
//Write(myFile,'# Tarjeta numero: '+Edit_CardNum.Text+'');
//WriteLn(myFile,'  ');
//Write(myFile,Edit_Block0data.Text+'          '     +     'Password     =     "'     +
Edit_CardSize.Text+'"','  ' );
//WriteLn(myFile,'  ');
//Write(myFile,'  '+ 'User-Service-Type = Login-User');
//Write(myFile,' ');
//WriteLn(myFile,'  ');
//CloseFile(myFile);
```

```
//refrescamiento de la pantalla

GroupBox10.Repaint;
GroupBox10.Refresh;

GroupBox4.Repaint;
GroupBox4.Refresh;

// para la las iteraciones
Sleep(1500);
xvar:=xvar+1;
tt2:= '';
ttt3:= '';
tttt4:= '';
t1:= '';
t5:= '';
t15:= '';
t25:= '';
t35:= '';
end; // end while
end; // end function
//////////////////////////////////////////////////////////////////////
//checkhexstr();
 ////////////////////////////////////////////////////
function TForm1_MIfare1.checkHexStr(s: String): boolean;
var
  i :Integer;
begin
  result := False;
  s:= trim(s);
  for i:=1 to Length(s) do
  begin
    case s[i] of
       '0'..'9','a'..'f','A'..'F' : Continue;
       else
          exit;
    end;
  end;
  result := true;
end;
function TForm1_MIfare1.checkDNum(s:string ) :boolean;
var
  i :Integer;
```

```
begin
  result := False;
  s:= trim(s);
  for i:=1 to Length(s) do
  begin
    case s[i] of
       '0'..'9': Continue;
       else
          exit;
    end;
  end;
  result := true;
end;

//============================================================
==========
////////////////////////////////////////////////////////////////////////////
// ´ò¿ª¶Ë¿ÚµÄ¸üÐÂ×´Ì¬
//============================================================
==================
procedure TForm1_MIfare1.Action_OpenComPortUpdate(Sender: TObject);

begin

  Action_OpenComPort.Enabled := not comisopen ;
  Action_CloseComPort.Enabled := comisopen ;

end;

procedure TForm1_MIfare1.Action_OpenRFUpdate(Sender: TObject);
begin
   Action_OpenRF.Enabled := comisopen and (not RFisOpen) ;
   Action_CloseRF.Enabled := comisopen and RFisOpen;

end;
////////////////////////////////////////////////////////////////////////////
// Ð´¿¨³ÌÐò
////////////////////////////////////////////////////////////////////////////
procedure TForm1_MIfare1.Action_SingleWritedataExecute(Sender: TObject);
var
  i :integer;

   data11:array[0..3]of char;
  i1:integer;
```

```
   t1:string;
    Mode1:integer ;
 /////////
   data22:array[0..3]of char;
    ii2:integer;
    tt2:string;

//CardSn:longint;// ¿¨µÄÐòÁÐºÅ
//retsize:pchar   // ·µ»ØµÄ¿¨ÈÝÁ¿´óÐ¡
// retsize : array[0..2] of char;
  retdatasize :array[0..12] of char;
    iii3:integer;
    ttt3 :string;
     CardSn :longint;
 //Mode:integer ;   Ö¤ÊµÄ£Ê½ 00 ÃÜÔ¿A 01 ÃÜÔ¿B
//Sector:integer;  ´ýÖ¤ÊµµÄ¿¨µÄÉÈÇøºÅ
//Keys:pchar   £» Ö¸Ïò6×Ö½ÚµÄÃÜÔ¿ µÍ×Ö½ÚÔÚÇ°
    Mode:integer ;
    Sector:integer;
   // keys:array[0..5] of char;
   data33:array[0..5]of char;
      iiii4:integer;
       tttt4 :string;

// //BlockNo:integer;  ¾ø¶Ô¿éºÅ0--63
//WriteBuff:pchar                  ´ýÐ´ÈëµÄÊý¾Ý»º³åÇø£¨16×Ö½Ú£©        Ò»´ÎÐ
´Èë16×Ö½ÚµÄÊý¾Ý

BlockNo0: longint;
writebuffer0: array[0..15]of char;
BlockNo1: longint;
writebuffer1: array[0..15]of char;
BlockNo2: longint;
palabra :string;
palabra2 :string;
cantidad_letras :integer;
ik :integer;
longitud :integer;
writebuffer2: array[0..15]of char;
//BlockNo3: longint;
//writebuffer3: array[0..15]of char;
 WriteBlockNo : longint ;
 writeDataStr : string ;
 writebufferDataStr : array[0..15] of char;
```

```
begin
                        //      function                    RRMifare_Request(Mode:integer;
CardTypeNo:pchar):longint;stdcall;
          //     Mode:integer;  ÇëÇóÃüÁîÄ£Ê½  01ËùÓÐµÄ¿¨¶¼ÏìÓ¦£¬00  Ö»ÓÐ
´¦ÓÚHALT×´Ì¬µÄ¿¨ÏìÓ¦
   //CardTypeNo:pchar  ·µ»ØµÄ¿¨ÀàÐÍ
     Mode1:= 0;
     if  RRMifare_Request(Mode1, data11)=0 then
      begin
      //BUZZER(0,1,1,1);

      for i1:= 3 downto 0 do
       t1:=t1+ inttohex(ord(data11[i1]),2);
       //Edit3.Text:= inttohex(ord(data11[0]),2)+';';
        // Edit3.Text:=Edit3.Text+t1;
      //application.MessageBox('ÓÐÊý¾Ý','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
        end
         else
         begin
          // application.MessageBox('ÎÞÊý¾Ý','ÐÅÏ¢ÌáÊ¾',mb_iconinformation)   ;
           messagedlg('Request Card Data Error ',mtinformation,[mbOk],0) ;
           exit;
          end;
           //  ControlLed(0);
             //BUZZER(0,1,1,1);
                   Sleep(80);
                        //ControlLed(1);
//  function   RRMifare_AntiColl( CardSn :pchar):longint;stdcall ;
// CardSn :pchar ·µ»ØµÄ¿¨ÐòÁÐºÅ
//CardSn:=data22
        if   RRMifare_AntiColl(data22)=0 then
       begin
        // BUZZER(0,1,1,1);
      for ii2:=3 downto 0 do
       //tt2:=tt2+ inttohex(ord(data22[ii2]),2);
      //Memo1.Text:= Memo1.Text+t;
        //  Edit4.Text:=Edit4.Text+tt2;
         // Edit_CardNum.Text:=tt2;
         tt2:=tt2+ inttohex(ord(data22[ii2]),2);
          //Edit4.Text:=Edit4.Text+tt2;
           //Edit_CardNum.Text:= Edit_CardNum.Text+tt2;
          Edit_CardNum.Text:= tt2;
        end;
            //ControlLed(0);
```

```
            // BUZZER(0,1,1,1);
            //       Sleep(80);
                      // ControlLed(1);

//function RRMifare_Select(CardSn:longint; retsize:pchar):longint;stdcall ;
//CardSn:longint;// ¿¨µÄÐòÁÐºÅ
//retsize:pchar   // ·µ»ØµÄ¿¨ÈÝÁ¿´óÐ¡
//retsize:=retdatasize :array[0..12] of char
//CardSn£º=data22  ti:=strtoint64('$'+t);
//CardSn :=      strtoint('$'+'1641197E') ;

 // CardSn := strtoint('$'+'7e194116') ;   ////////////////////////

 // if  RRMifare_Select(CardSn,retsize)=0 then
          // Edit_CardNum.Text
       //CardSn :=  strtoint('$'+tt2) ;
        if tt2 <> '' then
       CardSn := strtoint64('$'+ tt2);
    //  if RRMifare_Select(373365118,retdatasize)=0 then
       if RRMifare_Select(CardSn,retdatasize)=0 then
        //if RRMifare_Select(CardSn,retdatasize)=0 then
          begin
            //BUZZER(0,1,1,1);
           for iii3:=0 to 3 do
           ttt3:=ttt3+ inttohex(ord(retdatasize[iii3]),2);
             // Edit5.Text:=Edit5.Text+ttt3;
            // Edit_CardSize.Text := Edit_CardSize.Text + ttt3;

            Edit_CardSize.Text := ttt3;
             //  application.MessageBox('Ñ¡Ôñ¿¨Ok','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
          end
          else
         begin
         // application.MessageBox('Ñ¡Ôñ¿¨´íÎó','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
          messagedlg('Select card error ',mtinformation,[mbOk],0) ;
            exit;
          end ;
//      function      RRMifare_DirectAuthentication(Mode:integer      ;Sector:integer;
Keys:pchar):longint;stdcall;
//Mode:integer ;   Ö¤ÊµÄ£Ê½ 00 ÃÜÔ¿A 01 ÃÜÔ¿B
//Sector:integer;  ´ýÖ¤ÊµµÄ¿¨µÄÉÈÇøºÅ
//Keys:pchar   £» Ö¸Ïò6×Ö½ÚµÄÃÜÔ¿ µÍ×Ö½ÚÔÚÇ°
 // keys:array[0..5] of char;
 //  data33 :array[0..5] of char;
```

```
   Mode:=0 ;
   Sector:= ComboBox_Sector.ItemIndex;  //+1
 if  RadioButton_keysA.Checked then
   begin
   tttt4 := Edit_KeysANum.Text;
    Mode:=0 ;
   end  ;
   if RadioButton_keysB.Checked then
   begin
    tttt4 := Edit_KeysBNum.Text;
     Mode:=1 ;
   end;
   // tttt4 := Edit_KeysANum.Text;
     if Length( tttt4 )=12 then
     begin
        for iiii4:=0 to 5 do
          //keys[iiii4] := Char( StrToInt('$'+copy(tttt4,iiii4*2+1,2) ) );
          data33[iiii4]:=char( strtoint('$'+ copy(tttt4,iiii4*2+1,2)) );
         end
         else
         begin
                                          //application.MessageBox('ÃÜÔ¿ÊäÈë´íÎó','ÐÅÏ
¢ÌáÊ¾',mb_iconinformation);
           messagedlg('Input key error ',mtinformation,[mbOk],0) ;
            exit;
         end ;

 //if  RRMifare_DirectAuthentication(mode,sector,keys)=0 then
  //if  RRMifare_DirectAuthentication(0,0,data33)=0 then
  if  RRMifare_DirectAuthentication(mode,sector,data33)=0 then
       begin
         //BUZZER(0,1,1,1);
        //application.MessageBox('ÃÜÔ¿ÑéÖ¤ok','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
         end
         else
         begin
                                          //application.MessageBox('ÃÜÔ¿ÑéÖ¤´íÎó','ÐÅÏ
¢ÌáÊ¾',mb_iconinformation);
          messagedlg('key check error ',mtinformation,[mbOk],0) ;
           exit;
         end ;
//function  RRMifare_Write( BlockNo:integer; WriteBuff:pchar):longint;stdcall;
//BlockNo:integer;  ¾ø¶Ô¿éºÅ0--63
```

```
//WriteBuff:pchar                ´ýÐ´ÈëµÄÊý¾Ý»ª³åÇø£¨16×Ö½Ú£©      Ò»´ÎÐ
´Èë16×Ö½ÚµÄÊý¾Ý
  //BlockNo0: longint;
//writebuffer0: array[0..15]of char;
//BlockNo1: longint;
//writebuffer1: array[0..15]of char;
//BlockNo2: longint;
//writebuffer2: array[0..15]of char;
//BlockNo3: longint;
//writebuffer3: array[0..15]of char;
//---------------------------------------------------------------------------
//data33[iiii4]:=char( strtoint('$'+ copy(tttt4,iiii4*2+1,2)) );
 {    BlockNo0 := (ComboBox_Sector.ItemIndex)*4  ;
     BlockNo1 := (ComboBox_Sector.ItemIndex)*4+1  ;
     BlockNo2 := (ComboBox_Sector.ItemIndex)*4+2  ;
  //  BlockNo3 := (ComboBox_Sector.ItemIndex)*4+3  ;
                          if      not      (      checkHexStr(Edit_Block0data.Text)and
checkHexStr(Edit_Block1data.Text) and checkHexStr(Edit_Block2data.Text) )
        then exit;
     for i:= 0 to 15 do

     writebuffer0[i] := char(strtoint('$'+copy(Edit_Block0data.Text,i*2+1,2 )));

    for i:= 0 to 15 do

     writebuffer1[i] := char(strtoint('$'+copy(Edit_Block1data.Text,i*2+1,2 )));

      for i:= 0 to 15 do

     writebuffer2[i] := char(strtoint('$'+copy(Edit_Block2data.Text,i*2+1,2 )));


 if RRMifare_Write( BlockNo0, writebuffer0)=0 then
       begin
          BUZZER(0,1,1,1);
           sleep(80);
          //application.MessageBox('Ð´¿é0³É¹¦','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
       end
       else
       begin
       application.MessageBox('Ð´¿é0´íÎó','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
       end ;
   if RRMifare_Write( BlockNo1, writebuffer1)=0 then
       begin
```

```
        BUZZER(0,1,1,1);
        sleep(80);
        //application.MessageBox('Ð´¿é1³É¹¦','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
      end
      else
      begin
      application.MessageBox('Ð´¿é1´íÎó','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
      end ;
      if RRMifare_Write( BlockNo2, writebuffer2)=0 then
      begin
        BUZZER(0,1,1,1);
         sleep(80);
        //application.MessageBox('Ð´¿é2³É¹¦','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
      end
      else
      begin
      application.MessageBox('Ð´¿é2´íÎó','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
      end ;   }

{ //     if RRMifare_Write( BlockNo3, writebuffer3)=0 then
 //      begin
 // //       BUZZER(0,1,1,1);
 //        application.MessageBox('Ð´¿é3³É¹¦','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
 //      end
 //      else
   //    begin
    //    application.MessageBox('Ð´¿é3´íÎó','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
  //      end ;
            }
 //-------------------------------------------------------------------------------
 //¶ÔÊý¾Ý¿éÐ´ÈëÊý¾Ý

                    WriteBlockNo          :=          (ComboBox_Sector.ItemIndex)*4
+ComboBox_BlockNum.ItemIndex;

        palabra2:='';
       case WriteBlockNo of
       4: begin
       palabra := Edit_Block0data.Text;
         longitud := length(Edit_Block1data.Text);
         end;
       1: begin
       palabra := Edit_Block1data.Text;
         longitud := length(Edit_Block1data.Text);
```

```
  end;
2:begin
palabra := Edit_Block2data.Text;
  longitud := length(Edit_Block2data.Text);
  end;
5: begin
palabra := Edit_Block1data.Text;
  longitud := length(Edit_Block1data.Text);
  end;
6: begin
palabra := Edit_Block2data.Text;
  longitud := length(Edit_Block2data.Text);
  end;
end;

for ik:=1 to longitud do
begin
   case palabra[ik] of
      'a': palabra2:=palabra2 + '65';
      'b': palabra2:=palabra2 + '66';
      'c': palabra2:=palabra2 + '67';
      'd': palabra2:=palabra2 + '68';
      'e': palabra2:=palabra2 + '69';
      'f': palabra2:=palabra2 + '70';
      'g': palabra2:=palabra2 + '71';
      'h': palabra2:=palabra2 + '72';
      'i': palabra2:=palabra2 + '73';
      'j': palabra2:=palabra2 + '74';
      'k': palabra2:=palabra2 + '75';
      'l': palabra2:=palabra2 + '76';
      'm': palabra2:=palabra2 + '77';
      'n': palabra2:=palabra2 + '78';
      'ñ': palabra2:=palabra2 + '79';
      'o': palabra2:=palabra2 + '80';
      'p': palabra2:=palabra2 + '81';
      'q': palabra2:=palabra2 + '82';
      'r': palabra2:=palabra2 + '83';
      's': palabra2:=palabra2 + '84';
      't': palabra2:=palabra2 + '85';
      'u': palabra2:=palabra2 + '86';
      'v': palabra2:=palabra2 + '87';
      'w': palabra2:=palabra2 + '88';
      'x': palabra2:=palabra2 + '89';
      'y': palabra2:=palabra2 + '90';
```

```
            'z': palabra2:=palabra2 + '91';
            'A': palabra2:=palabra2 + '65';
            'B': palabra2:=palabra2 + '66';
            'C': palabra2:=palabra2 + '67';
            'D': palabra2:=palabra2 + '68';
            'E': palabra2:=palabra2 + '69';
            'F': palabra2:=palabra2 + '70';
            'G': palabra2:=palabra2 + '71';
            'H': palabra2:=palabra2 + '72';
            'I': palabra2:=palabra2 + '73';
            'J': palabra2:=palabra2 + '74';
            'K': palabra2:=palabra2 + '75';
            'L': palabra2:=palabra2 + '76';
            'M': palabra2:=palabra2 + '77';
            'N': palabra2:=palabra2 + '78';
            'Ñ': palabra2:=palabra2 + '79';
            'O': palabra2:=palabra2 + '80';
            'P': palabra2:=palabra2 + '81';
            'Q': palabra2:=palabra2 + '82';
            'R': palabra2:=palabra2 + '83';
            'S': palabra2:=palabra2 + '84';
            'T': palabra2:=palabra2 + '85';
            'U': palabra2:=palabra2 + '86';
            'V': palabra2:=palabra2 + '87';
            'W': palabra2:=palabra2 + '88';
            'X': palabra2:=palabra2 + '89';
            'Y': palabra2:=palabra2 + '90';
            'Z': palabra2:=palabra2 + '91';
            ' ': palabra2:=palabra2 + '92';
        else
           palabra2:=palabra2;
        end;
    end;

     if length(palabra2) <> 32 then
    begin
          longitud := length(palabra2);
          cantidad_letras := 32 - longitud;
          for ik:=1 to cantidad_letras do
          palabra2 := palabra2 + '0';
     end;


case ComboBox_BlockNum.ItemIndex  of
```

```
     0:    writeDataStr :=  palabra2  ;
     1:  writeDataStr :=  palabra2 ;
     2:  writeDataStr :=  palabra2 ;
    // 3:  writeDataStr :=  Edit_Blockd3ata.Text ;  //¶ÔÊý¾Ý¿é3µÄÐ´Èë
    //else
      //writeDataStr :=  Edit_Blockd0ata.Text ;
    end;
  if ComboBox_BlockNum.ItemIndex =3 then
     begin
      // if MessageDlg('ÊÇ·ñÐ´¿é3??',mtconfirmation,
     //[mbyes,mbno],0)=mrYes then
        if MessageDlg('Confirm to write Block3 ?',mtconfirmation,
     [mbyes,mbno],0)=mrYes then
        begin
         //application.MessageBox('Ð´¿é3','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
         messagedlg('Write Block3 ',mtinformation,[mbOk],0) ;
                writeDataStr  :=    Edit_Block3data05.Text+  Edit_Block3data69.Text+
Edit_Block3data1015.Text;
       end else
       begin
        //application.MessageBox(' ²»Ð´¿é3','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
         messagedlg(' Abandon ',mtinformation,[mbOk],0) ;
          exit;
         // application.MessageBox('Ð´¿é3?','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);

              //writeDataStr  :=    Edit_Block3data05.Text+  Edit_Block3data69.Text+
Edit_Block3data1015.Text;
      end;
      end ;
      if (writeDatastr = '')or(length(writeDatastr)<>32) then
      begin
       // application.MessageBox('Êý¾ÝÊäÈë´íÎó','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
        messagedlg('Input data error ',mtinformation,[mbOk],0) ;
         exit;
      end;

   for i:= 0 to 15 do

     writebufferDataStr[i] := char(strtoint('$'+copy(writeDatastr,i*2+1,2 )));


 if RRMifare_Write( WriteBlockNo, writebufferDataStr)=0 then
       begin
         BUZZER(0,1,1,1);
```

```
        sleep(80);
       //application.MessageBox('Ð´¿é³É¹¦','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
    end
    else
    begin

    //application.MessageBox('Ð´¿é´íÎó','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
    messagedlg('Write Block data error ',mtinformation,[mbOk],0) ;
    end ;

end;
////////////////////////////////////////////////////////////////////////////
// ÐÞ¸ÄÃÜÔ¿µÄ³ÌÐò  // ÏÈ¶Á³ö³ÌÐòÔÙ°ÑÕâ¸öÉÈÇøµÄÃÜÔ¿ÐÞ¸Ä
////////////////////////////////////////////////////////////////////////////
procedure TForm1_MIfare1.Action_changkeysExecute(Sender: TObject);

var
//I : integer;
//Sector:integer;    Òª¸ü¸ÄÃÜÂëµÄÉÈÇøºÅ
//Keya:pchar ;  Ö¸Ïò6×Ö½ÚµÄÃÜÔ¿A £¬µÍ×Ö½ÚÔÚÇ°
//Keyb:pchar  Ö¸Ïò6×Ö½ÚµÄÃÜÔ¿B £¬µÍ×Ö½ÚÔÚÇ°

Sectork:integer;
keya :array[0..5] of char ;
keyb :array[0..5] of char;
tkeya : string ;
tkeyb :string;
 ia ,ib :integer;

begin

  // Action_GetCarddata(Sender);

    Button5.Click;     // ¶ÁÈ¡ÉÈÇøµÄÊý¾ÝÄÚÈÝ

    sleep(80);
                //function           RRMifare_SetKey(Sector:integer;      Keya:pchar      ;
Keyb:pchar):longint;stdcall;
   //Sector:integer;    Òª¸ü¸ÄÃÜÂëµÄÉÈÇøºÅ
   //Keya:pchar ;  Ö¸Ïò6×Ö½ÚµÄÃÜÔ¿A £¬µÍ×Ö½ÚÔÚÇ°
   //Keyb:pchar  Ö¸Ïò6×Ö½ÚµÄÃÜÔ¿B £¬µÍ×Ö½ÚÔÚÇ°

      Sectork :=  ComboBox_Sector.ItemIndex ;
   //
```

```
     tkeya := Edit1_keya.Text;
                          if        (Edit1_keya.Text<>'')and    (Length(tkeya)=12)    and
checkHexStr(Edit1_keya.Text)  then
     begin
        for ia:=0 to 5 do

          Keya[ia]:=char( strtoint('$'+ copy(tkeya,ia*2+1,2)) );
         end
         else
         begin
                                        //application.MessageBox('ÃÜÔ¿AÊäÈë´íÎó','ÐÅÏ
¢ÌáÊ¾',mb_iconinformation);
           messagedlg('input key A error ',mtinformation,[mbOk],0) ;
            exit;
         end ;

     tkeyb :=  Edit1_Keyb.Text;
                              if        (Edit1_keyb.Text<>'')and    (Length(tkeyb)=12)and
checkHexStr(Edit1_keyb.Text) then
     begin
        for ib:=0 to 5 do
        Keyb[ib]:=char( strtoint('$'+ copy(tkeyb,ib*2+1,2)) );
         end
         else
         begin
                                      //    application.MessageBox('ÃÜÔ¿BÊäÈë´íÎó','ÐÅÏ
¢ÌáÊ¾',mb_iconinformation);
            messagedlg('input key B error ',mtinformation,[mbOk],0) ;
            exit;
         end ;

 if   RRMifare_SetKey(Sectork, Keya, Keyb)=0 then
 begin
      BUZZER(0,1,1,1);
                                       //application.MessageBox('ÐÂÃÜÔ¿Ð´Èë³É¹¦','ÐÅÏ
¢ÌáÊ¾',mb_iconinformation);
      messagedlg(' Key Modification successfully  ',mtinformation,[mbOk],0) ;
 end else
 begin
  // application.MessageBox('ÐÂÃÜÔ¿Ð´Èë´íÎó','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
    messagedlg('Key Modification error ',mtinformation,[mbOk],0) ;
     exit;
 end;
```

```
end;
//============================================================
======================
//////////////////////////////////////
//  ³õÊ¼»¯        ÔÚ¼ÓÖµ¼õÖµ    ²Ù×÷Ç°    ±ØÐëµÄ    ÊÇÊý¾Ý¿éÖÐ´æ
´¢Ò»¶¨¸ñÊ½µÄÊý¾Ý
//////////////////////////////////////
//============================================================
====================
procedure TForm1_MIfare1.Action_InitDataExecute(Sender: TObject);
var
   i :integer;
   n : longint;
     data11:array[0..3]of char;
   i1:integer;
  t22,t, t1:string;
    Mode1:integer ;
 /////////
   data22:array[0..3]of char;
    ii2:integer;
    tt2:string;

//CardSn:longint;// ¿¨µÄÐòÁÐºÅ
//retsize:pchar   // ·µ»ØµÄ¿¨ÈÝÁ¿´óÐ¡
// retsize : array[0..2] of char;
  retdatasize :array[0..12] of char;
    iii3:integer;
    ttt3 :string;
     CardSn :longint;
 //Mode:integer ;   Ö¤ÊµÄ£Ê½ 00 ÃÜÔ¿A 01 ÃÜÔ¿B
//Sector:integer;  ´ýÖ¤ÊµµÄ¿¨µÄÉÈÇøºÅ
//Keys:pchar   £» Ö¸Ïò6×Ö½ÚµÄÃÜÔ¿ µÍ×Ö½ÚÔÚÇ°
    Mode:integer ;
    Sector:integer;
   // keys:array[0..5] of char;
   data33:array[0..5]of char;
      iiii4:integer;
       tttt4 :string;

// //BlockNo:integer;  ¾ø¶Ô¿éºÅ0--63
//WriteBuff:pchar                  ´ýÐ´ÈëµÄÊý¾Ý»º³åÇø£¨16×Ö½Ú£©        Ò»´ÎÐ
´Èë16×Ö½ÚµÄÃÊý¾Ý

initBlockNo0: longint;
```

```
initwritebuffer0: array[0..15]of char;
//BlockNo1: longint;
//writebuffer1: array[0..15]of char;
//BlockNo2: longint;
//writebuffer2: array[0..15]of char;
//BlockNo3: longint;
//writebuffer3: array[0..15]of char;
 t11:string;
 // t112 :string ;
  // t113 :string ;
i11 :longint;
 //i11 :longword;
// i112 :integer;
 i113 :longint;
 adr:string;
 adrfei :string ;
i112,iif: longint;
  //i112,iif:  longword;

begin


                        //      function                    RRMifare_Request(Mode:integer;
CardTypeNo:pchar):longint;stdcall;
           //     Mode:integer;  ÇëÇóÃüÁîÄ£Ê½  01ËùÓÐµÄ¿¨¶¼ÏìÓ¦£¬00   Ö»ÓÐ
´¦ÓÚHALT×´Ì¬µÄ¿¨ÏìÓ¦
   //CardTypeNo:pchar  ·µ»ØµÄ¿¨ÀàÐÍ
     Mode1:= 0;
     if  RRMifare_Request(Mode1, data11)=0 then
      begin
      //BUZZER(0,1,1,1);

      for i1:= 3 downto 0 do
       t1:=t1+ inttohex(ord(data11[i1]),2);
       //Edit3.Text:= inttohex(ord(data11[0]),2)+';';
        // Edit3.Text:=Edit3.Text+t1;
      //application.MessageBox('ÓÐÊý¾Ý','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
        end
         else
         begin
                                  //    application.MessageBox('ÎÞRequestÊý¾Ý','ÐÅÏ
¢ÌáÊ¾',mb_iconinformation)   ;
          messagedlg('Request Card Data Error ',mtinformation,[mbOk],0) ;
          exit;
```

```
          end;
            //ControlLed(0);
            //BUZZER(0,1,1,1);
                  //Sleep(80);
                        //ControlLed(1);
//  function   RRMifare_AntiColl( CardSn :pchar):longint;stdcall ;
// CardSn :pchar ·µ»ØµÄ¿¨ÐòÁÐºÅ
//CardSn:=data22
        if   RRMifare_AntiColl(data22)=0 then
       begin
        // BUZZER(0,1,1,1);
      for ii2:=3 downto 0 do
       //tt2:=tt2+ inttohex(ord(data22[ii2]),2);
      //Memo1.Text:= Memo1.Text+t;
        //  Edit4.Text:=Edit4.Text+tt2;
         // Edit_CardNum.Text:=tt2;
         tt2:=tt2+ inttohex(ord(data22[ii2]),2);
          //Edit4.Text:=Edit4.Text+tt2;
           //Edit_CardNum.Text:= Edit_CardNum.Text+tt2;
          Edit_CardNum.Text:= tt2;
        end;
            //ControlLed(0);
           // BUZZER(0,1,1,1);
           //       Sleep(80);
                      // ControlLed(1);

//function RRMifare_Select(CardSn:longint; retsize:pchar):longint;stdcall ;
//CardSn:longint;// ¿¨µÄÐòÁÐºÅ
//retsize:pchar   // ·µ»ØµÄ¿¨ÈÝÁ¿´óÐ¡
//retsize:=retdatasize :array[0..12] of char
//CardSn£º=data22  ti:=strtoint64('$'+t);
//CardSn :=      strtoint('$'+'1641197E') ;
 // CardSn := strtoint('$'+'7e194116') ;   ////////////////////////
 // if  RRMifare_Select(CardSn,retsize)=0 then
          // Edit_CardNum.Text
      //CardSn :=  strtoint('$'+tt2) ;
       if tt2 <> '' then
       CardSn := strtoint64('$'+ tt2);
   //  if RRMifare_Select(373365118,retdatasize)=0 then
      if RRMifare_Select(CardSn,retdatasize)=0 then
       //if RRMifare_Select(CardSn,retdatasize)=0 then
          begin
            //BUZZER(0,1,1,1);
           for iii3:=0 to 3 do
```

```
          ttt3:=ttt3+ inttohex(ord(retdatasize[iii3]),2);
            // Edit5.Text:=Edit5.Text+ttt3;
            // Edit_CardSize.Text := Edit_CardSize.Text + ttt3;

           Edit_CardSize.Text := ttt3;
            //  application.MessageBox('Ñ¡Ôñ¿¨Ok','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
         end
         else
        begin
         //application.MessageBox('Ñ¡Ôñ¿¨´íÎó','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
           messagedlg('Select card error ',mtinformation,[mbOk],0) ;
           exit;
         end ;
//      function      RRMifare_DirectAuthentication(Mode:integer      ;Sector:integer;
Keys:pchar):longint;stdcall;
//Mode:integer ;   Ö¤ÊµÄ£Ê½ 00 ÃÜÔ¿A 01 ÃÜÔ¿B
//Sector:integer;  ´ýÖ¤ÊµµÄ¿¨µÄÉÈÇøºÅ
//Keys:pchar   £» Ö¸Ïò6×Ö½ÚµÄÃÜÔ¿ µÍ×Ö½ÚÔÚÇ°
 // keys:array[0..5] of char;
 //  data33 :array[0..5] of char;
    Mode:=0 ;  // Ä£Ê½00 ÃÜÔ¿A
    Sector:= ComboBox_Sector_2.ItemIndex;  //+1

      if  RadioButton_keysA2.Checked then
    begin
     tttt4   := Edit_KeysatINCDEC.Text  ;
     Mode:=0 ;
    end  ;
    if RadioButton_keysB2.Checked then
    begin
      tttt4   := Edit_KeysatINCDEC.Text  ;
      Mode:=1 ;
    end;
     //tttt4 := Edit_KeysANum.Text;
      // tttt4   := Edit_KeysatINCDEC.Text  ;
      if (Length( tttt4 )=12) and checkHexStr(Edit_KeysatINCDEC.Text) then
      begin
          for iiii4:=0 to 5 do
            //keys[iiii4] := Char( StrToInt('$'+copy(tttt4,iiii4*2+1,2) ) );
            data33[iiii4]:=char( strtoint('$'+ copy(tttt4,iiii4*2+1,2)) );
          end
          else
          begin
```

```
                                        //application.MessageBox('ÃÜÔ¿ÊäÈë´íÎó','ÐÅÏ
¢ÌáÊ¾',mb_iconinformation);
          messagedlg('Input key error ',mtinformation,[mbOk],0) ;
            exit;
          end ;

 //if  RRMifare_DirectAuthentication(mode,sector,keys)=0 then
  //if  RRMifare_DirectAuthentication(0,0,data33)=0 then
  if  RRMifare_DirectAuthentication(mode,sector,data33)=0 then
       begin
         //BUZZER(0,1,1,1);
        //application.MessageBox('ÃÜÔ¿ÑéÖ¤ok','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
         end
         else
         begin
                                        //application.MessageBox('ÃÜÔ¿ÑéÖ¤´íÎó','ÐÅÏ
¢ÌáÊ¾',mb_iconinformation);
           messagedlg('key check error ',mtinformation,[mbOk],0) ;
          exit;
          end ;
//function  RRMifare_Write( BlockNo:integer; WriteBuff:pchar):longint;stdcall;
//BlockNo:integer;  ¾ø¶Ô¿éºÅ0--63
//WriteBuff:pchar                 ´ýÐ´ÈëµÄÊý¾Ý»º³åÇø£¨16×Ö½Ú£©       Ò»´ÎÐ
´Èë16×Ö½ÚµÄÊý¾Ý
  //BlockNo0: longint;
//writebuffer0: array[0..15]of char;
//BlockNo1: longint;
//writebuffer1: array[0..15]of char;
//BlockNo2: longint;
//writebuffer2: array[0..15]of char;
//BlockNo3: longint;
//writebuffer3: array[0..15]of char;
//data33[iiii4]:=char( strtoint('$'+ copy(tttt4,iiii4*2+1,2)) );
      //BlockNo0 := 05;
     //BlockNo0 := (ComboBox_Sector.ItemIndex)*4  ;
                  initBlockNo0:=       (ComboBox_Sector_2.ItemIndex)       *4       +
ComboBox_BlockNum_2.ItemIndex;
  // ÅÐ¶Ï ÊäÈëµÄ³õÊ¼»¯ ÖµÊÇ²»ÊÇÊ®½øÖÆ
    if not ((Edit_UseData.Text<>'')and checkDNum(Edit_UseData.Text)) then
     begin
              //    application.MessageBox('³õÊ¼»¯ ÖµÎª¿Õ»ò²»ÊÇÊ®½øÖÆÊý','ÐÅÏ
¢ÌáÊ¾',mb_iconinformation);
      messagedlg('Initialization data error ',mtinformation,[mbOk],0) ;
     exit ;
```

```
      end  ;

     n := strtoint(Edit_UseData.Text);  // ×ª»¯³ÉÊ®Áù½øÖÆÊý¾Ý

      //   Edit_UseData.Text:=   inttohex(n,8);          //   ×ª»¯³ÉÊ®Áù½øÖÆÊý¾Ý×
¢ÒâÒªÊ¹Edit_UseData.TextµÄÊ®Áù½øÖÆÊý¾Ý±£³Ö8Î»
   Edit_getInitdata.Text  := inttohex(n,8);

   for i:=1 to 4 do                          // ×ª»»³ÉµÍ×Ö½ÚÔÚÇ°
   t:= t + copy(Edit_getInitdata.Text,9-i*2,2);
    Edit_getInitdata.Text := t;
   //
      for I :=0 to 3 do
      initwritebuffer0[I] := char(strtoint('$'+copy(Edit_getInitdata.Text,I*2+1,2 )));
       //t11:=   strtoint('$'+copy( Edit_initdata.Text,i*2+1,2 ))    ; // t1 4-7 ÖµÎªVALUE
µÄ·´

      i11 :=  strtoint('$'+ Edit_getInitdata.Text);
          iif := $ffffffff;
      //i112 := i11 xor $ffffffff ;
      i112 := i11 xor iif ;

      t11 := inttohex(i112,2);

      for i := 4 to 7 do
       initwritebuffer0[i] := char(strtoint('$'+copy( t11 ,(i-4)*2+1,2 )));
    for I :=8 to 11 do
      initwritebuffer0[i] := char(strtoint('$'+copy(Edit_getInitdata.Text,(i-8)*2+1,2 )));
 //////////////
 //i113 :longint;
 //adr:string;

     i112:= (ComboBox_Sector.ItemIndex) *4 + ComboBox_BlockNum.ItemIndex;
      adr := inttohex(i112,2);
      i113:= i112 xor  $ff ;
      adrfei :=  inttohex(i113,2);
// 12bit
    initwritebuffer0[12] := char(strtoint('$'+copy( adr,1,2 ))) ;
   // / 13bit
    initwritebuffer0[13] := char(strtoint('$'+copy( adrfei,1,2 ))) ;
   // / 14bit
    initwritebuffer0[14] := char(strtoint('$'+copy( adr,1,2 ))) ;
   // / 15bit
    initwritebuffer0[15] := char(strtoint('$'+copy( adrfei,1,2 ))) ;
```

```
 //Edit_getInitdata.Text  := Edit_UseData.Text;
    t22:= Edit_getInitdata.Text ;
  Edit_getInitdata.Text  :=  Edit_getInitdata.Text +   t11;
  Edit_getInitdata.Text  :=Edit_getInitdata.Text + t22;

  Edit_getInitdata.Text  :=Edit_getInitdata.Text + adr;
  Edit_getInitdata.Text  :=Edit_getInitdata.Text + adrfei;
  Edit_getInitdata.Text  :=Edit_getInitdata.Text + adr;
  Edit_getInitdata.Text  :=Edit_getInitdata.Text + adrfei;

//Edit_getInitdata.Text  := '01000000FEFFFFFF0100000005FA05FA';

//Edit_getInitdata.Text // °üÀ¨ 0-3 VALUE 4- 7VALUE µÄ·Ç £¬8-11 VALUE 12
ADR 13 ADR·Ç 14 ADR 15 ADR·Ç

   { for i:= 15 downto 0 do
   // begin
     initwritebuffer0[i] := char(strtoint('$'+copy(Edit_getInitdata.Text,i*2+1,2 )));
        }

     if RRMifare_Write( initBlockNo0, initwritebuffer0)=0 then
       begin
          BUZZER(0,1,1,1);
        //  application.MessageBox('³õÊ¼»¯ ¿é³É¹¦','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
       // messagedlg('initialization successfully',mtinformation,[mbOk],0);
       end
       else
       begin
       //application.MessageBox('³õÊ¼»¯ ¿é´íÎó','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
        messagedlg('initialization error',mtinformation,[mbOk],0);
       end ;
//                                                                          function
RRMifare_Increment(BlockNo:integer;Value:integer):longint;stdcall;external
'RRMifare32.dll';
//function                                    RRMifare_Decrment(BlockNo:integer;
Value:integer):longint;stdcall;external 'RRMifare32.dll';

end;
////////////////////////////////////////////////////////////////////////////////////////////
//=================================================================
==================================
////////////////////////////////////////////////////////////////////////////////////////////
```

```
//¼ÓÖµº¯ Êý ³ÌÐò ÊµÏÖ¶Ô¾ø¶ÔÊý¾Ý¿éµÄÖµµÄÂö¼ÓÒ»¸öÖµ
////////////////////////////////////////////////////////////////////////////////
//=============================================================
=====================================
procedure TForm1_MIfare1.Action_incdataExecute(Sender: TObject);
 var
   i :integer;
   n: longint ;
     data11:array[0..3]of char;
   i1:integer;
 tinc,t,t1:string;
    Mode1:integer ;
 /////////
   data22:array[0..3]of char;
    ii2:integer;
    tt2:string;

//CardSn:longint;// ¿¨µÄÐòÁÐºÅ
//retsize:pchar   // ·µ»ØµÄ¿¨ÈÝÁ¿´óÐ¡
// retsize : array[0..2] of char;
  retdatasize :array[0..12] of char;
    iii3:integer;
    ttt3 :string;
     CardSn :longint;
 //Mode:integer ;   Ö¤ÊµÄ£Ê½ 00 ÃÜÔ¿A 01 ÃÜÔ¿B
//Sector:integer;  ´ýÖ¤ÊµµÄ¿¨µÄÉÈÇøºÅ
//Keys:pchar   £» Ö¸Ïò6×Ö½ÚµÄÃÜÔ¿ µÍ×Ö½ÚÔÚÇ°
    Mode:integer ;
    Sector:integer;
   // keys:array[0..5] of char;
   data33:array[0..5]of char;
      iiii4:integer;
       tttt4 :string;
// BlockNo:integer;
 //Value:integer
  incBlockNo :integer;

   incValue  :integer;
begin
        //          function                                RRMifare_Request(Mode:integer;
CardTypeNo:pchar):longint;stdcall;
           //     Mode:integer;  ÇëÇóÃüÁîÄ£Ê½  01ËùÓÐµÄ¿¨¶¼ÌìÓ¦¬00   Ö»ÓÐ
´¦ÓÚHALT×´Ì¬µÄ¿¨ÌìÓ¦
   //CardTypeNo:pchar  ·µ»ØµÄ¿¨ÀàÐÍ
```

```
      Mode1:= 0;
      if  RRMifare_Request(Mode1, data11)=0 then
       begin
       //BUZZER(0,1,1,1);

       for i1:= 3 downto 0 do
        t1:=t1+ inttohex(ord(data11[i1]),2);
        //Edit3.Text:= inttohex(ord(data11[0]),2)+';';
         // Edit3.Text:=Edit3.Text+t1;
       //application.MessageBox('ÓÐÊý¾Ý','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
         end
          else
          begin
          //  application.MessageBox('ÎÞÊý¾Ý','ÐÅÏ¢ÌáÊ¾',mb_iconinformation)   ;
            messagedlg('Request Card Data Error ',mtinformation,[mbOk],0) ;
            exit;
           end;
             //ControlLed(0);
             //BUZZER(0,1,1,1);
                   //Sleep(80);
                        //ControlLed(1);
//  function   RRMifare_AntiColl( CardSn :pchar):longint;stdcall ;
// CardSn :pchar ·µ»ØµÄ¿¨ÐòÁÐºÅ
//CardSn:=data22
        if   RRMifare_AntiColl(data22)=0 then
       begin
        // BUZZER(0,1,1,1);
      for ii2:=3 downto 0 do
       //tt2:=tt2+ inttohex(ord(data22[ii2]),2);
      //Memo1.Text:= Memo1.Text+t;
        //  Edit4.Text:=Edit4.Text+tt2;
         // Edit_CardNum.Text:=tt2;
         tt2:=tt2+ inttohex(ord(data22[ii2]),2);
          //Edit4.Text:=Edit4.Text+tt2;
           //Edit_CardNum.Text:= Edit_CardNum.Text+tt2;
          Edit_CardNum.Text:= tt2;
        end;
            //ControlLed(0);
           // BUZZER(0,1,1,1);
           //       Sleep(80);
                      // ControlLed(1);

//function RRMifare_Select(CardSn:longint; retsize:pchar):longint;stdcall ;
//CardSn:longint;// ¿¨µÄÐòÁÐºÅ
```

```
//retsize:pchar   // ·µ»ØµÄ¿¨ÈÝÁ¿´óÐ¡
//retsize:=retdatasize :array[0..12] of char
//CardSn£º=data22  ti:=strtoint64('$'+t);
//CardSn :=      strtoint('$'+'1641197E') ;

 // CardSn := strtoint('$'+'7e194116') ;   ////////////////////////

 // if  RRMifare_Select(CardSn,retsize)=0 then
          // Edit_CardNum.Text
       //CardSn :=  strtoint('$'+tt2) ;
       if tt2 <> '' then
        CardSn := strtoint64('$'+ tt2);
    //  if RRMifare_Select(373365118,retdatasize)=0 then
       if RRMifare_Select(CardSn,retdatasize)=0 then
        //if RRMifare_Select(CardSn,retdatasize)=0 then
           begin
             //BUZZER(0,1,1,1);
            for iii3:=0 to 3 do
           ttt3:=ttt3+ inttohex(ord(retdatasize[iii3]),2);
             // Edit5.Text:=Edit5.Text+ttt3;
             // Edit_CardSize.Text := Edit_CardSize.Text + ttt3;

            Edit_CardSize.Text := ttt3;
             //  application.MessageBox('Ñ¡Ôñ¿¨Ok','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
          end
          else
         begin
          //application.MessageBox('Ñ¡Ôñ¿¨´íÎó','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
           messagedlg('Select card error ',mtinformation,[mbOk],0) ;
            exit;
          end ;
//      function      RRMifare_DirectAuthentication(Mode:integer      ;Sector:integer;
Keys:pchar):longint;stdcall;
//Mode:integer ;   Ö¤ÊµÄ£Ê½ 00 ÃÜÔ¿A 01 ÃÜÔ¿B
//Sector:integer;  ´ýÖ¤ÊµµÄ¿¨µÄÉÈÇøºÅ
//Keys:pchar   £» Ö¸Ïò6×Ö½ÚµÄÃÜÔ¿ µÍ×Ö½ÚÔÚÇ°
 // keys:array[0..5] of char;
 //  data33 :array[0..5] of char;
    Mode:=0 ;
    Sector:= ComboBox_Sector_2.ItemIndex;  //+1
     if  RadioButton_keysA2.Checked then
    begin
     tttt4   := Edit_KeysatINCDEC.Text  ;
     Mode:=0 ;
```

```
   end  ;
   if RadioButton_keysB2.Checked then
   begin
     tttt4   := Edit_KeysatINCDEC.Text  ;
     Mode:=1 ;
   end;

    //tttt4 := Edit_KeysatINCDEC.Text  ;
      if Length( tttt4 )=12 then
      begin
         for iiii4:=0 to 5 do
           //keys[iiii4] := Char( StrToInt('$'+copy(tttt4,iiii4*2+1,2) ) );
           data33[iiii4]:=char( strtoint('$'+ copy(tttt4,iiii4*2+1,2)) );
         end
         else
         begin
                                          //    application.MessageBox('ÃÜÔ¿ÊäÈë´íÎó','ÐÅÏ
¢ÌáÊ¾',mb_iconinformation);
          messagedlg('Input key error ',mtinformation,[mbOk],0) ;
            exit;
         end ;

 //if  RRMifare_DirectAuthentication(mode,sector,keys)=0 then
  //if  RRMifare_DirectAuthentication(0,0,data33)=0 then
  if  RRMifare_DirectAuthentication(mode,sector,data33)=0 then
       begin
         //BUZZER(0,10,1,1);
       //application.MessageBox('ÃÜÔ¿ÑéÖ¤ok','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
         end
         else
         begin
                                            //application.MessageBox('ÃÜÔ¿ÑéÖ¤´íÎó','ÐÅÏ
¢ÌáÊ¾',mb_iconinformation);
           messagedlg('key check error ',mtinformation,[mbOk],0) ;
          exit;
         end ;

 //function  RRMifare_Increment(BlockNo:integer;Value:integer):longint;stdcall;
 // BlockNo:integer;
 //Value:integer
  //  incBlockNo :integer;

  // incValue  :integer;
```

```
            incBlockNo      :=      (ComboBox_Sector_2.ItemIndex)      *4      +
ComboBox_BlockNum_2.ItemIndex;
  // ÅÐ¶ÏÊäÈëµÄ¼ÓÖµÊý¾ÝÊÇ²»ÊÇÎª¿Õ¼ºÊÇ²»ÊÇÊ®½øÖÆÊý¾Ý
   if not ((Edit_UseData.Text<>'')and checkDNum(Edit_UseData.Text))  then
     begin
                //    application.MessageBox('¼ÓÖµÊý¾ÝÎª¿Õ»ò²»ÊÇÊ®½øÖÆ','ÐÅÏ
¢ÌáÊ¾',mb_iconinformation);
      messagedlg('Add value error',mtinformation,[mbOk],0);
     exit ;
      end ;
    n := strtoint(Edit_UseData.Text);  // ×ª»¯³ÉÊ®Áù½øÖÆÊý¾Ý

        //Edit_UseData.Text:=   inttohex(n,8);          //   ×ª»¯³ÉÊ®Áù½øÖÆÊý¾Ý×
¢ÒâÒªÊ¹Edit_UseData.TextµÄÊ®Áù½øÖÆÊý¾Ý±£³Ö8Î»
    Edit_getInitdata.Text := inttohex(n,8);
          tinc:= Edit_getInitdata.Text ;
   for i:= 1 to 4 do
   t := t + copy(Edit_getInitdata.Text,9-i*2,2);
    Edit_getInitdata.Text := t  ;              // µ¹Ð´ ½«µÍ×Ö½Ú·ÅÔÚÇ°
    incValue := strtoint('$'+tinc);

 if RRMifare_Increment(incBlockNo,incValue )=0 then    // ¼ÓÖµÖ±½ÓÊÇÒª¼Ó
µÄÊýÖµ
 begin
     BUZZER(0,1,1,1);
     //application.MessageBox('¼ÓÖµok','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
     // messagedlg('Add value ok',mtinformation,[mbOk],0);
 end
 else
 begin
     //application.MessageBox('¼ÓÖµ´íÎó','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
      messagedlg('Add value Error',mtinformation,[mbOk],0);
      exit;
 end ;
end;
//////////////////////////////////////////////////////////////////////////////
// ÉèÖÃÏÔÊ¾ ÉèÖÃ¶Ô»°¿ò
{procedure TForm1_MIfare1.N17Click(Sender: TObject);
begin
  Form_SetControlBit.Show;
end; }
////////////////////////////////
// Èí¼þ°æ±¾ºïÖúÏÔÊ¾
////////////////////////////
```

```
//procedure TForm1_MIfare1.MIfareI1Click(Sender: TObject);
//begin
//Form_AboutThisSoft.Show;
//end;
//============================================================
=========================
////////////////////////////////////////////////////////////////////////////
// ¼õÖµº¯ Êý ÊµÏÖ¶Ô Êý¾Ý¿éµÄÖµ ¼õÉÙÖµ ²Ù×÷
//============================================================
=======================
 //function  RRMifare_Decrment(BlockNo:integer; Value:integer):longint;stdcall;
procedure TForm1_MIfare1.Action_decdateExecute(Sender: TObject);
var
   i :integer;
   n: longint ;
   data11:array[0..3]of char;
   i1:integer;
   tdec,t,t1:string;
    Mode1:integer ;
 /////////
   data22:array[0..3]of char;
    ii2:integer;
    tt2:string;

//CardSn:longint;// ¿¨µÄÐòÁÐºÅ
//retsize:pchar   // ·µ»ØµÄ¿¨ÈÝÁ¿´óÐ¡
// retsize : array[0..2] of char;
  retdatasize :array[0..12] of char;
    iii3:integer;
    ttt3 :string;
     CardSn :longint;
 //Mode:integer ;   Ö¤ÊµÄ£Ê½ 00 ÃÜÔ¿A 01 ÃÜÔ¿B
//Sector:integer;  ´ýÖ¤ÊµµÄ¿¨µÄÉÈÇøºÅ
//Keys:pchar   £» Ö¸Ïò6×Ö½ÚµÄÃÜÔ¿ µÍ×Ö½ÚÔÚÇ°
    Mode:integer ;
    Sector:integer;
   // keys:array[0..5] of char;
   data33:array[0..5]of char;
      iiii4:integer;
       tttt4 :string;
 BlockNo:integer;
  Value:longint;
  //incBlockNo :integer;
```

```
  //incValue  :integer;
begin
        //        function                                RRMifare_Request(Mode:integer;
CardTypeNo:pchar):longint;stdcall;
          //     Mode:integer;  ÇëÇóÃüÁîÄ£Ê½  01ËùÓÐµÄ¿¨¶¼ÏìÓ¦£¬00  Ö»ÓÐ
´¦ÓÚHALT×´Ì¬µÄ¿¨ÏìÓ¦
   //CardTypeNo:pchar  ·µ»ØµÄ¿¨ÀàÐÍ
     Mode1:= 0;
     if  RRMifare_Request(Mode1, data11)=0 then
      begin
      //BUZZER(0,1,1,1);

      for i1:= 3 downto 0 do
       t1:=t1+ inttohex(ord(data11[i1]),2);
       //Edit3.Text:= inttohex(ord(data11[0]),2)+';';
        // Edit3.Text:=Edit3.Text+t1;
      //application.MessageBox('ÓÐÊý¾Ý','ÐÅÏ¢ìáÊ¾',mb_iconinformation);
        end
         else
         begin
           //application.MessageBox('ÎÞÊý¾Ý','ÐÅÏ¢ìáÊ¾',mb_iconinformation)   ;
           messagedlg('Request Card Data Error ',mtinformation,[mbOk],0) ;
           exit;
          end;
            //ControlLed(0);
            //BUZZER(0,1,1,1);
                  //Sleep(80);
                      // ControlLed(1);
//  function   RRMifare_AntiColl( CardSn :pchar):longint;stdcall ;
// CardSn :pchar ·µ»ØµÄ¿¨ÐòÁÐºÅ
//CardSn:=data22
        if   RRMifare_AntiColl(data22)=0 then
       begin
        // BUZZER(0,1,1,1);
      for ii2:=3 downto 0 do
       //tt2:=tt2+ inttohex(ord(data22[ii2]),2);
      //Memo1.Text:= Memo1.Text+t;
        //  Edit4.Text:=Edit4.Text+tt2;
         // Edit_CardNum.Text:=tt2;
         tt2:=tt2+ inttohex(ord(data22[ii2]),2);
          //Edit4.Text:=Edit4.Text+tt2;
           //Edit_CardNum.Text:= Edit_CardNum.Text+tt2;
          Edit_CardNum.Text:= tt2;
        end;
```

```
            //ControlLed(0);
           // BUZZER(0,1,1,1);
           //      Sleep(80);
                    // ControlLed(1);

//function RRMifare_Select(CardSn:longint; retsize:pchar):longint;stdcall ;
//CardSn:longint;// ¿¨µÄÐòÁÐºÅ
//retsize:pchar   // ·µ»ØµÄ¿¨ÈÝÁ¿´óÐ¡
//retsize:=retdatasize :array[0..12] of char
//CardSn£º=data22  ti:=strtoint64('$'+t);
//CardSn :=      strtoint('$'+'1641197E') ;

 // CardSn := strtoint('$'+'7e194116') ;   ////////////////////////

 // if  RRMifare_Select(CardSn,retsize)=0 then
         // Edit_CardNum.Text
      //CardSn :=  strtoint('$'+tt2) ;

       CardSn := strtoint64('$'+ tt2);
   //  if RRMifare_Select(373365118,retdatasize)=0 then
      if RRMifare_Select(CardSn,retdatasize)=0 then
       //if RRMifare_Select(CardSn,retdatasize)=0 then
          begin
            //BUZZER(0,1,1,1);
           for iii3:=0 to 3 do
          ttt3:=ttt3+ inttohex(ord(retdatasize[iii3]),2);
            // Edit5.Text:=Edit5.Text+ttt3;
           // Edit_CardSize.Text := Edit_CardSize.Text + ttt3;

           Edit_CardSize.Text := ttt3;
            //  application.MessageBox('Ñ¡Ôñ¿¨Ok','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
         end
         else
        begin
         //application.MessageBox('Ñ¡Ôñ¿¨´íÎó','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
           messagedlg('Select card error ',mtinformation,[mbOk],0) ;
           exit;
         end ;
//      function      RRMifare_DirectAuthentication(Mode:integer      ;Sector:integer;
Keys:pchar):longint;stdcall;
//Mode:integer ;   Ö¤ÊµÄ£Ê½ 00 ÃÜÔ¿A 01 ÃÜÔ¿B
//Sector:integer;  ´ýÖ¤ÊµµÄ¿¨µÄÉÈÇøºÅ
//Keys:pchar   £» Ö¸Ïò6×Ö½ÚµÄÃÜÔ¿ µÍ×Ö½ÚÔÚÇ°
 // keys:array[0..5] of char;
```

```
//  data33 :array[0..5] of char;
   Mode:=0 ;
   Sector:= ComboBox_Sector_2.ItemIndex;  //+1
     if  RadioButton_keysA2.Checked then
   begin
    tttt4   := Edit_KeysatINCDEC.Text  ;
    Mode:=0 ;
   end  ;
   if RadioButton_keysB2.Checked then
   begin
     tttt4   := Edit_KeysatINCDEC.Text  ;
     Mode:=1 ;
   end;
   // tttt4 := Edit_KeysatINCDEC.Text;
     if Length( tttt4 )=12 then
     begin
        for iiii4:=0 to 5 do
          //keys[iiii4] := Char( StrToInt('$'+copy(tttt4,iiii4*2+1,2) ) );
          data33[iiii4]:=char( strtoint('$'+ copy(tttt4,iiii4*2+1,2)) );
         end
         else
         begin
                                          //    application.MessageBox('ÃÜÔ¿ÊäÈë´íÎó','ÐÅÏ
¢ÌáÊ¾',mb_iconinformation);
           messagedlg('Input key error ',mtinformation,[mbOk],0) ;
             exit;
         end ;

 //if  RRMifare_DirectAuthentication(mode,sector,keys)=0 then
  //if  RRMifare_DirectAuthentication(0,0,data33)=0 then
  if  RRMifare_DirectAuthentication(mode,sector,data33)=0 then
       begin
         //BUZZER(0,10,1,1);
       //application.MessageBox('ÃÜÔ¿ÑéÖ¤ok','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
         end
         else
         begin
                                          //    application.MessageBox('ÃÜÔ¿ÑéÖ¤´íÎó','ÐÅÏ
¢ÌáÊ¾',mb_iconinformation);
           messagedlg('key check error ',mtinformation,[mbOk],0) ;
           exit;
         end ;

 //function  RRMifare_Increment(BlockNo:integer;Value:integer):longint;stdcall;
```

```
// BlockNo:integer;
//Value:integer
 //  BlockNo :integer;
// Value  :integer;
              BlockNo        :=        (ComboBox_Sector_2.ItemIndex)        *4        +
ComboBox_BlockNum_2.ItemIndex;
 // ÅÐ¶ÏÊäÈëµÄ¼õÖµÊý¾ÝÊÇ²»ÊÇÎª¿Õ¼°ÊÇ²»ÊÇÊ®½øÖÆÊý¾Ý
  if not ((Edit_UseData.Text<>'')and checkDNum(Edit_UseData.Text)) then
    begin
                  //application.MessageBox('¼õÖµÊý¾ÝÎª¿Õ»ò²»ÊÇÊ®½øÖÆ','ÐÅÏ
¢ÌáÊ¾',mb_iconinformation);
   messagedlg('Decrease value error',mtinformation,[mbOk],0);
    exit ;
     end ;
   n := strtoint(Edit_UseData.Text);  // ×ª»¯³ÉÊ®Áù½øÖÆÊý¾Ý

     //   Edit_UseData.Text:=   inttohex(n,8);          //   ×ª»¯³ÉÊ®Áù½øÖÆÊý¾Ý×
¢ÒâÒªÊ¹Edit_UseData.TextµÄÊ®Áù½øÖÆÊý¾Ý±£³Ö8Î»
   Edit_getInitdata.Text := inttohex(n,8);
      tdec:= Edit_getInitdata.Text;
   for i := 1 to 4 do
  t:= t + copy(Edit_getInitdata.Text,9-i*2,2);

 Edit_getInitdata.Text := t;
   //Value := strtoint('$'+Edit_UseData.Text);
  Value := strtoint('$'+tdec);
if  RRMifare_Decrment(BlockNo,Value )=0 then
begin
    BUZZER(0,1,1,1);
    //application.MessageBox('¼õÖµok','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
    //messagedlg(' Decrease value Ok',mtinformation,[mbOk],0);
end
else
begin
    //application.MessageBox('¼õÖµ´íÎó','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
     messagedlg(' Decrease value Error',mtinformation,[mbOk],0);
    exit;
end ;
end;
//////////////////////////////////////////////////////////////////////
//==========================================================
=========
// ¶ÁÈ¡Óà¶î º¯ Êý
```

```
//=============================================================
=========
procedure TForm1_MIfare1.Action_ReadCurrentdataExecute(Sender: TObject);
 var
  data11:array[0..3]of char;
   i1:integer;
   t1:string;
    Mode1:integer ;
 /////////
   data22:array[0..3]of char;
    ii2:integer;
    tt2:string;

//CardSn:longint;// ¿¨µÄÐòÁÐºÅ
//retsize:pchar   // ·µ»ØµÄ¿¨ÈÝÁ¿´óÐ¡
// retsize : array[0..2] of char;
  retdatasize :array[0..12] of char;
    iii3:integer;
    ttt3 :string;
     CardSn :longint;
 //Mode:integer ;   Ö¤ÊµÄ£Ê½ 00 ÃÜÔ¿A 01 ÃÜÔ¿B
//Sector:integer;  ´ýÖ¤ÊµµÄ¿¨µÄÉÈÇøºÅ
//Keys:pchar   £» Ö¸Ïò6×Ö½ÚµÄÃÜÔ¿ µÍ×Ö½ÚÔÚÇ°
    Mode:integer ;
    Sector:integer;
   // keys:array[0..5] of char;
   data33:array[0..5]of char;
      iiii4:integer;
       tttt4 :string;

//BlockNo:integer;   ¾ø¶ÔµÄ¿éºÅ£¨0--63£©
 //ReadBuff:pchar    ¶ÁÈ¡Êý¾Ý»ºåÇø16×Ö½Ú Ò»´Î¶ÁÈ¡16 ×Ö½ÚµÄ¿éÊý¾Ý
// BlockNo1 : integer;
 //ReadBuff :array[0..15] of char ;
 i5 :integer;
 t5 :string;
 // i15 :integer;
  //t15 :string ;

  //i25 :integer;
  //t25 :string ;
  // i35 :integer;
  // t35 :string ;    // Êý¾Ý¿é3µÄÇ°0-5×Ö½ÚÊý¾Ý
```

```
  //  t35_69 : string ;  // Êý¾Ý¿é3µÄÇ°6-9×Ö½ÚÊý¾Ý
   //  t35_1015  : string ;  // Êý¾Ý¿é3µÄÇ°10-15×Ö½ÚÊý¾Ý

 BlockNo0 :integer;
//  BlockNo1 :integer;
 // BlockNo2 :integer;
 // BlockNo3:integer;
  ReadBuff0 :array[0..15] of char ;
  //ReadBuff1 :array[0..15] of char ;
 // ReadBuff2 :array[0..15] of char ;
 // ReadBuff3 :array[0..15] of char ;
  t :string;
  n: longint;

begin
                        //      function                        RRMifare_Request(Mode:integer;
CardTypeNo:pchar):longint;stdcall;
             //     Mode:integer;  ÇëÇóÃüÁîÄ£Ê½  01ËùÓÐµÄ¿¨¶¼ÌìÓ¦£¬00   Ö»ÓÐ
´¦ÓÚHALT×´Ì¬µÄ¿¨ÌìÓ¦
    //CardTypeNo:pchar  ·µ»ØµÄ¿¨ÀàÐÍ
      Mode1:= 0;
      if  RRMifare_Request(Mode1, data11)=0 then
       begin
       //BUZZER(0,1,1,1);
      for i1:= 3 downto 0 do
        t1:=t1+ inttohex(ord(data11[i1]),2);
       //Edit3.Text:= inttohex(ord(data11[0]),2)+';';
        // Edit3.Text:=Edit3.Text+t1;
      //application.MessageBox('ÓÐÊý¾Ý','ÐÅÏ¢ìáÊ¾',mb_iconinformation);
        end
         else
         begin
          // application.MessageBox('ÎÞÊý¾Ý','ÐÅÏ¢ìáÊ¾',mb_iconinformation)   ;
           messagedlg('Request Card Data Error ',mtinformation,[mbOk],0) ;
           exit;
          end;
            ControlLed(0);
            //BUZZER(0,1,1,1);
                  Sleep(80);
                       ControlLed(1);
//  function   RRMifare_AntiColl( CardSn :pchar):longint;stdcall ;
// CardSn :pchar ·µ»ØµÄ¿¨ÐòÁÐºÅ
//CardSn:=data22
        if   RRMifare_AntiColl(data22)=0 then
```

```
        begin
         // BUZZER(0,1,1,1);
       for ii2:=3 downto 0 do
        //tt2:=tt2+ inttohex(ord(data22[ii2]),2);
       //Memo1.Text:= Memo1.Text+t;
         //  Edit4.Text:=Edit4.Text+tt2;
          // Edit_CardNum.Text:=tt2;
          tt2:=tt2+ inttohex(ord(data22[ii2]),2);
           //Edit4.Text:=Edit4.Text+tt2;
            //Edit_CardNum.Text:= Edit_CardNum.Text+tt2;
           Edit_CardNum.Text:= tt2;
         end;
             ControlLed(0);
            // BUZZER(0,1,1,1);
                   Sleep(80);
                        ControlLed(1);

//function RRMifare_Select(CardSn:longint; retsize:pchar):longint;stdcall ;
//CardSn:longint;// ¿¨µÄÐòÁÐºÅ
//retsize:pchar   // ·µ»ØµÄ¿¨ÈÝÁ¿´óÐ¡
//retsize:=retdatasize :array[0..12] of char
//CardSn£º=data22  ti:=strtoint64('$'+t);
//CardSn :=      strtoint('$'+'1641197E') ;
 // CardSn := strtoint('$'+'7e194116') ;   ////////////////////////
// if  RRMifare_Select(CardSn,retsize)=0 then
          // Edit_CardNum.Text
       //CardSn :=  strtoint('$'+tt2) ;
        if tt2 <> '' then
       CardSn := strtoint64('$'+ tt2);
    //  if RRMifare_Select(373365118,retdatasize)=0 then
       if RRMifare_Select(CardSn,retdatasize)=0 then
        //if RRMifare_Select(CardSn,retdatasize)=0 then
          begin
            //BUZZER(0,1,1,1);
           for iii3:=0 to 3 do
          ttt3:=ttt3+ inttohex(ord(retdatasize[iii3]),2);
            // Edit5.Text:=Edit5.Text+ttt3;
           // Edit_CardSize.Text := Edit_CardSize.Text + ttt3;

           Edit_CardSize.Text := ttt3;
            //  application.MessageBox('Ñ¡Ôñ¿¨Ok','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
         end
         else
        begin
```

```
        // application.MessageBox('Ñ¡Ôñ¿¨´íÎó','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
          messagedlg('Select card error ',mtinformation,[mbOk],0) ;
           exit;
         end ;
//      function      RRMifare_DirectAuthentication(Mode:integer      ;Sector:integer;
Keys:pchar):longint;stdcall;
//Mode:integer ;   Ö¤ÊµÄ£Ê½ 00 ÃÜÔ¿A 01 ÃÜÔ¿B
//Sector:integer;  ´ýÖ¤ÊµµÄ¿¨µÄÉÈÇøºÅ
//Keys:pchar   £» Ö¸Ïò6×Ö½ÚµÄÃÜÔ¿ µÍ×Ö½ÚÔÚÇ°
 // keys:array[0..5] of char;
 //  data33 :array[0..5] of char;
    Mode:=0 ;
    Sector:= ComboBox_Sector_2.ItemIndex;  //+1
     if  RadioButton_keysA2.Checked then
    begin
     tttt4   := Edit_KeysatINCDEC.Text  ;
     Mode:=0 ;
    end  ;
    if RadioButton_keysB2.Checked then
    begin
      tttt4   := Edit_KeysatINCDEC.Text  ;
      Mode:=1 ;
    end;
   // tttt4 := Edit_KeysANum.Text;
      if Length( tttt4 )=12 then
      begin
         for iiii4:=0 to 5 do
           //keys[iiii4] := Char( StrToInt('$'+copy(tttt4,iiii4*2+1,2) ) );
           data33[iiii4]:=char( strtoint('$'+ copy(tttt4,iiii4*2+1,2)) );
         end
         else
         begin
                                          //    application.MessageBox('ÃÜÔ¿ÊäÈë´íÎó','ÐÅÏ
¢ÌáÊ¾',mb_iconinformation);
          messagedlg('Input key error ',mtinformation,[mbOk],0) ;
            exit;
         end ;
//if  RRMifare_DirectAuthentication(mode,sector,keys)=0 then
  //if  RRMifare_DirectAuthentication(0,0,data33)=0 then
  if  RRMifare_DirectAuthentication(mode,sector,data33)=0 then
       begin
         //BUZZER(0,1,1,1);
        //application.MessageBox('ÃÜÔ¿ÑéÖ¤ok','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
         end
```

```
          else
          begin
                                          //application.MessageBox('ÃÜÔ¿ÑéÖ¤´íÎó','ÐÅÏ
¢ÌáÊ¾',mb_iconinformation);
            messagedlg('key check error ',mtinformation,[mbOk],0) ;
           exit;
          end ;
           sleep(80);
//-------------------------------------------------------------
 //RRMifare_Read(BlockNo0, data0)
 //function RRMifare_Read(BlockNo:integer;  ReadBuff:pchar):longint;stdcall ;
 //BlockNo:integer;   ¾ø¶ÔµÄ¿éºÅ£¨0--63£©
 //ReadBuff:pchar    ¶ÁÈ¡Êý¾Ý»º³åÇø16×Ö½ÚÚ Ò»´Î¶ÁÈ¡16 ×Ö½ÚµÄ¿éÊý¾Ý
//BlockNo1 : integer;
// ReadBuff :array[0..12] of char ;
// i5 :integer;
// t5 :string;
              BlockNo0        :=              (ComboBox_Sector_2.ItemIndex        )
*4+ComboBox_BlockNum_2.ItemIndex;
 if RRMifare_Read(BlockNo0,ReadBuff0)=0 then
  begin
     BUZZER(0,1,1,1);
   for i5 := 0 to 3 do
    t5 := t5 + inttohex(ord(ReadBuff0[i5]),2) ;

     Edit_getInitdata.Text := t5;
    for i5:=1 to 4 do
     t:=t+ copy(Edit_getInitdata.Text,9-i5*2,2);

     n:= strtoint('$'+t);
     Edit_UseData.Text := inttostr(n);

  // application.MessageBox('¶ÁÈ¡Óà¶îok','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
  end
  else
  begin
     //application.MessageBox('¶ÁÈ¡Óà¶î´íÎó','ÐÅÏ¢ÌáÊ¾',mb_iconinformation);
     messagedlg(' Show value Error',mtinformation,[mbOk],0);
     exit;
  end;
  // BUZZER(0,1,1,1);
   //sleep(80);  //====================================
end;
```

```
//////////////////////////////////////////////////////////////
//============================================================
=
// ÏÔÊ¾ïÖúÎÄµµ
//////////////////////////////////////////
procedure TForm1_MIfare1.N12Click(Sender: TObject);
begin
Form_Help.Show;
end;

procedure TForm1_MIfare1.Action_GetInfoUpdate(Sender: TObject);
begin
   Action_GetInfo.Enabled := comisopen and RFisopen;
   //self.Enabled:=  comisopen;
   Action_GetCarddata.Enabled :=  comisopen and RFisopen;
   ComboBox_Sector.Enabled :=  comisopen and RFisopen;
   ComboBox_BlockNum.Enabled := comisopen and RFisopen;

   Edit_Block0data.Enabled :=  comisopen and RFisopen;
   Edit_Block1data.Enabled :=  comisopen and RFisopen;
   Edit_Block2data.Enabled :=  comisopen and RFisopen;
   Edit_Block3data05.Enabled :=  comisopen and RFisopen;
   Edit_Block3data69.Enabled :=  comisopen and RFisopen;
   Edit_Block3data1015.Enabled  :=  comisopen and RFisopen;
   Edit_KeysANum.Enabled :=   comisopen and RFisopen;
   Edit_KeysBNum.Enabled :=   comisopen and RFisopen;
  if not (comisopen and RFisopen) then
   begin
     Edit_Block0data.Color := clBtnFace;
     Edit_Block1data.Color := clBtnFace;
     Edit_Block2data.Color := clBtnFace;
      Edit_Block3data05.Color := clBtnFace;
      Edit_Block3data69.Color  := clBtnFace;
      Edit_Block3data1015.Color  := clBtnFace;
      ComboBox_Sector.Color  := clBtnFace;
      ComboBox_BlockNum.Color := clBtnFace;
       Edit_KeysANum.Color :=  clBtnFace;
        Edit_KeysBNum.Color :=  clBtnFace;
   end
   else
   begin
     Edit_Block0data.Color := clWindow;
     Edit_Block1data.Color := clWindow;
     Edit_Block2data.Color := clWindow;
```

```
      Edit_Block3data05.Color := clWindow;
      Edit_Block3data69.Color  := clWindow;
      Edit_Block3data1015.Color  := clWindow;
      ComboBox_Sector.Color  := clWindow;
      ComboBox_BlockNum.Color := clWindow;
      Edit_KeysANum.Color:= clWindow;
      Edit_KeysBNum.Color:= clWindow;
   end;
end;

procedure TForm1_MIfare1.Action_changkeysUpdate(Sender: TObject);
begin
   Action_changkeys.Enabled  :=  comisopen and RFisopen;
   Edit1_keya.Enabled := comisopen and RFisopen;
   Edit1_Keyb.Enabled := comisopen and RFisopen;
   if not(comisopen and RFisopen) then
   begin
     Edit1_keya.Color := clBtnFace;
     Edit1_Keyb.Color := clBtnFace;
   end
   else
   begin
     Edit1_keya.Color :=  clWindow;
     Edit1_Keyb.Color :=   clWindow;
   end;
end;

procedure TForm1_MIfare1.Action_SingleWritedataUpdate(Sender: TObject);
begin
  Action_SingleWritedata.Enabled :=  comisopen and RFisopen;
end;

procedure TForm1_MIfare1.Action_InitDataUpdate(Sender: TObject);
begin
    Action_InitData.Enabled :=  comisopen and RFisopen;
    Action_incdata.Enabled  :=  comisopen and RFisopen;
    Action_decdate.Enabled  :=  comisopen and RFisopen;
    Action_ReadCurrentdata.Enabled :=  comisopen and RFisopen;

   ComboBox_Sector_2.Enabled :=   comisopen and RFisopen;
   ComboBox_BlockNum_2.Enabled :=   comisopen and RFisopen;
   Edit_KeysatINCDEC.Enabled :=   comisopen and RFisopen;
   Edit_getInitdata.Enabled   :=   comisopen and RFisopen;
   Edit_UseData.Enabled :=   comisopen and RFisopen;
```

```
  if not  (comisopen and RFisopen ) then
   begin
      ComboBox_Sector_2.Color := clBtnFace;
     ComboBox_BlockNum_2.Color := clBtnFace;
    Edit_KeysatINCDEC.Color := clBtnFace;
    Edit_getInitdata.Color := clBtnFace;
    Edit_UseData.Color := clBtnFace;
   end
   else
   begin
   ComboBox_Sector_2.Color := clWindow;
   ComboBox_BlockNum_2.Color := clWindow;
    Edit_KeysatINCDEC.Color := clWindow;
    Edit_getInitdata.Color := clWindow;
    Edit_UseData.Color := clWindow;
   end;

end;

end.
```

BIBLIOGRAFIA

Libros:

[1] **RFID Sourcebook.** Sandip Lahiri. Prentice Hall PTR. 2005. (ISBN: 0-13-185137-3).

[2] **RFID Field Guide:** Deploying Radio Frequency Identification Systems. Bhuptani Manish, Moradpour Shahram Prentice Hall PTR 2005. (ISBN: 0-13-185355-4).

Sitios Web consultados:

[1] RFID Journal (http://www.rfidjournal.com).

[2] Philips Semiconductors (http://www.semiconductors.philips.com).

[3] Texas Instruments (http://www.ti.com/rfid/docs/datasheets.shtml).

[4] ATMEL (http://www.atmel.com).

[5] Impinj (http://www.impinj.com).

[6] EPCGlobal (http://www.epcglobalinc.org/home)

[7] http://www.swissdelphicenter.ch/en/showcode.php?id=1563

[8] http://www.delphibasics.co.uk/Article.asp?Name=Files

[9] http://mc-computing.com/Languages/Strings.htm

[10] http://www.delphibasics.co.uk/Article.asp?Name=Standard