ESCUELA POLITECNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE UN SISTEMA DE CONTROL DE ACCESO UTILIZANDO LA TECNOLOGÍA DE IDENTIFICACIÓN RFID PARA LA EMPRESA SOLUCIONES G CUATRO DEL ECUADOR CIA. LTDA.

PROYECTO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN ELECTRONICA Y REDES DE INFORMACIÓN

PABLO WALTER PUPIALES ANGAMARCA
ppupiales@arenapremier.com

DIRECTOR: Ing. NELSON AVILA
navila@tallard.com

Quito, julio 2009

DECLARACIÓN

Yo, Pablo Walter Pupiales Angamarca, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Pablo Pupiales A.

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Pablo Walter Pupiales Angamarca, bajo mi supervisión.

Ing. Nelson Avila
DIRECTOR DE PROYECTO

DEDICATORIA

A mis adorados padres Teodoro y Rosa quienes incondicionalmente me han apoyado en todo y siempre han estado pendientes de mis éxitos y fracasos de mis alegrías y tristezas a ellos que siempre me han dado el buen ejemplo de superación les dedico con todo mi amor este triunfo tan importante. A ti Consuelo que eres mi hermana y segunda madre y siempre has estado cuidando de mí, te quiero mucho. A mis demás hermanos Alberto, Serafín, Segundo, Edwin quienes han sido para mí un ejemplo de superación y guía. A mis hermanos que terrenalmente no están acá pero también han sido un ánimo para seguir adelante, a ellos también va dedicado este triunfo. A mi adorada novia Paty quien ha sido muy comprensiva en estos momentos y juntos hemos podido superar muchas cosas, te amo mucho. A mis amigos Carlos, Joe, Hermes quienes han aportado de una u otra manera con sus conocimientos para culminar este proyecto, A mi profesor y amigo Nelson Avila quien ha sido mi principal guía para la elaboración y culminación de este proyecto.

Finalmente a Dios por darme salud y vida y lo más principal, la dicha de tener a mis padres con vida para darles una felicidad mas, porque después de tanto sufrimiento por darnos una educación digna a mí y a todos mis hermanos, se merecen eso y mucho mas. Gracias a todos.

Pablo Pupiales.

CONTENIDO

CAPITULO 1

CAPITULO 2

RESUMEN

El presente proyecto está estructurado en tres capítulos, cada uno los cuales tiene su enfoque definido con el objetivo de dar una clara idea del funcionamiento de la tecnología RFID.

En el primer capítulo se realiza una descripción de los sistemas de control de acceso más comunes en nuestro medio como lo son los sistemas basados en tarjetas inteligentes, sistemas biométricos, sistemas basados en tarjetas magnéticas y código de barras. En cada una de estas tecnologías se detalla su funcionamiento y sus aplicaciones más comunes para luego en el capítulo dos hacer una comparación de estas tecnologías especialmente del código de barras frente a la tecnología de identificación por Radio Frecuencia (RFID)

En el segundo capítulo se realiza un estudio de la tecnología RFID partiendo de sus fundamentos, infraestructura de operación, estándares a los cuales está sometida, comparación frente a otras tecnologías de identificación y finalmente revisar sus aplicaciones en los diferentes ámbitos del mercado actual.

En el tercer capítulo se presenta una solución para control de accesos utilizando esta tecnología para la empresa SOLUCIONES G4 DEL ECUADOR S.A. Para lo cual se inicia presentando una descripción acerca de la situación actual del control de accesos a espectáculos públicos, en base a esto se plantea los requerimientos para control de accesos y seguidamente se procede con el desarrollo e implementación del prototipo para control de accesos utilizando la tecnología de identificación RFID, finalmente se realiza un análisis costo beneficio de la solución y una comparación con la situación actual.

PRESENTACIÓN

El presente proyecto tiene como objetivo principal solventar las brechas de seguridad que se tienen en el ámbito de control de accesos a espectáculos públicos, especialmente en el ámbito del control de acceso de pases especiales para un determinado evento, dichos pases son entregados al personal que está involucrado directamente en la organización de un evento por lo que es vital llevar un control minucioso de este tipo de asistentes.

Actualmente los pases especiales se los elabora de manera manual y sin ninguna seguridad electrónica que permita autenticar al usuario portador de dicho pase, esto deja abierta una amplia posibilidad de falsificación de dichos pases lo que ocasiona que cualquier individuo que no tiene ninguna relación con la organización del evento se involucre en el mismo, generando una total inseguridad a las áreas que acceda este individuo no autorizado.

Con la solución propuesta en el presente proyecto se busca solventar estos inconvenientes y tener un mayor control tanto en seguridad como en administración del personal involucrado en la organización del evento ya que el sistema permitirá tener un control desde la generación de la credencial RFID hasta la finalización de su uso que viene a ser el fin del control de acceso a un evento.

CAPITULO 1

SISTEMAS DE CONTROL DE ACCESO

Este capítulo presenta una breve descripción de algunas de las tecnologías de control de acceso utilizadas actualmente. Entre ellas se describe a los sistemas basados en tarjetas inteligentes, sistemas biométricos, sistemas basados en tarjetas magnéticas y códigos de barras, a fin de proveer un contexto global dentro del cual se pueda evaluar la contribución del presente trabajo.

1.1 SISTEMAS BASADOS EN TARJETAS INTELIGENTES

1.1.1 DEFINICIÓN DE TARJETAS INTELIGENTES

En la vida diaria es muy común el uso de tarjetas que sirven para identificar a una persona, acceder a edificios, áreas restringidas, realizar transacciones bancarias, etc. Estas tarjetas han ido evolucionando de una manera rápida hasta el punto de añadir un chip con un microprocesador interno que permita almacenar una mayor cantidad de información, pero el objetivo de esto no sólo es almacenar una mayor cantidad de información de manera segura sino también el poder tener la posibilidad de almacenar dicha información en otros sistemas, a este conjunto de características se las denomina un sistema basado en tarjetas inteligentes.

Las tarjetas inteligentes nacieron en la década de los 70, básicamente una tarjeta inteligente es un chip con un microprocesador el cual está encapsulado en una tarjeta PVC con determinadas dimensiones, dicho chip dispone de contactos exteriores o campos electromagnéticos que permiten tener una comunicación con él para poder almacenar y procesar información de una manera segura, ésta puede ser información personal, bancaria, historiales clínicos, claves privadas de acceso, etc.

La seguridad en este tipo de tarjetas es mayor ya que el chip contiene una tecnología interna sofisticada que hace que las posibilidades de manipulación física se reduzcan, esta tecnología además permite soportar procesos

criptográficos complejos que permiten tener un sistema de seguridad mucho más sólido.

1.1.2 ARQUITECTURA

El chip de una tarjeta inteligente generalmente consta de un CPU o microprocesador, memoria, control de encendido y circuitos especiales para la seguridad y comunicación con el mundo exterior. Como se puede observar en la figura 1.1 el acceso a las áreas de memoria sólo es posible a través de la unidad de entrada/salida y de la CPU lo que permite aumentar la seguridad del sistema. Algunas tarjetas también cuentan con un generador de números aleatorios, que se usa cuando se requiere una autenticación *two-ways* que consiste en que ambas partes envíen un número aleatorio, para que se realice un tipo de procesamiento y este resultado sea devuelto a su emisor, y así poder comprobar la autenticidad de la identidad de su interlocutor.

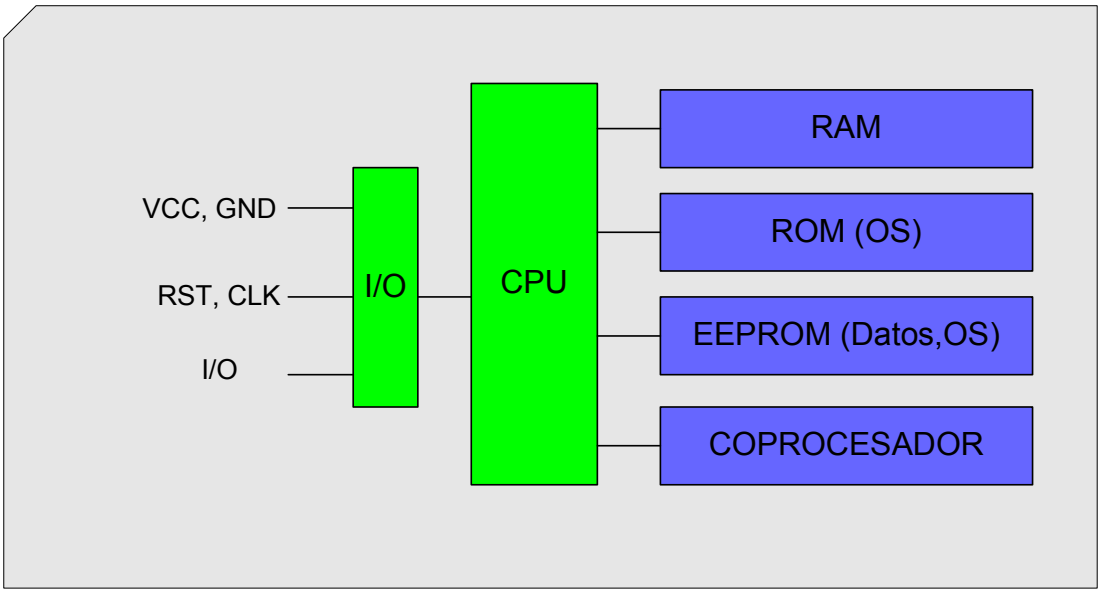


Figura 1.1 Estructura de una tarjeta Inteligente.

- RAM (Random Access Memory).-

  Esta es la memoria de trabajo del microprocesador aquí se almacena los datos de sesión, al ser volátil ésta pierde toda su información al momento de ser desconectada de su alimentación de energía.

- La ROM:

  (Read Only Memory).- Aquí es donde se encuentra el sistema operativo (OS) el cual se encarga de manejar la asignación de almacenamiento de la memoria, la protección de accesos y las comunicaciones descartando así la posibilidad de poder introducir externamente comandos falsos que puedan comprometer la seguridad del sistema.

- EEPROM:

  (Electrical Erasable Programable Read Only Memory).- Memoria no volátil que contiene todos los datos que deben permanecer en la tarjeta a lo largo de múltiples sesiones, así como también el código de las instrucciones que están bajo el control del sistema operativo. También puede contener información como el nombre del usuario, número de identificación personal o PIN (Personal Identification Number)

- COPROCESADOR:

  Este elemento se utiliza básicamente para propósitos de criptografía.

- CPU:

  Controla el funcionamiento del resto de componentes y además realiza operaciones de cálculo.

- I/O:

  El puerto de entrada/salida normalmente consiste en un simple registro, a través del cual la información es transferida bit a bit.

Funcionamiento

Las tarjetas se activan al introducirlas en un lector de tarjetas que son el dispositivo que actúa como la interface entre el usuario y el sistema, existe una gran diversidad de lectores y sus capacidades varían de acuerdo a las necesidades de los usuarios. Los lectores pueden ser alámbricos, inalámbricos, con teclado, sin teclado, con pantalla o sin ella. Un contacto metálico, un campo magnético o incluso una lectura láser, permite la transferencia de información entre el lector y la tarjeta.

"Las comunicaciones de las tarjetas inteligentes se rigen por el estándar ISO 7816/3, en donde se define las señales eléctricas, los protocolos de transmisión, niveles de tensión y los procedimientos para iniciar la comunicación". [1]

1.1.3 CLASES DE TARJETAS INTELIGENTES

Las tarjetas inteligentes se clasifican en dos grandes grupos que son:

- De contacto.
- Sin contacto.

Tarjetas inteligentes de contacto

Este tipo de tarjetas tienen la estructura mencionada en el apartado 1.1.2 y necesitan ser insertadas físicamente en una terminal con lector inteligente para que por medio de contactos pueda ser leída. El chip de este tipo de tarjetas tiene 8 contactos (Figura 1.2) de los cuales se utilizan sólo 6 los mismos que son el único interfaz electrónico existente entre la tarjeta y el terminal lector. Todas las señales eléctricas circulan a través de estos contactos.

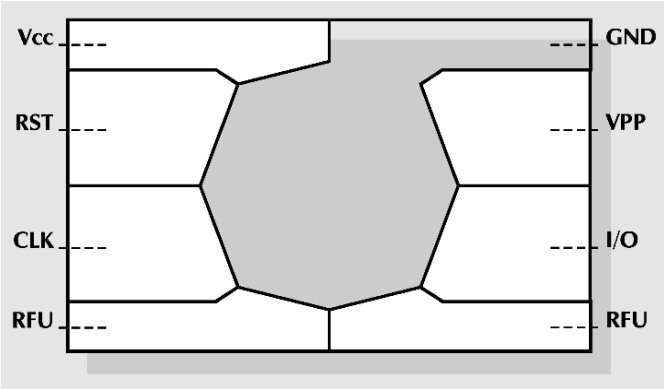


Figura 1.2 Contactos de una tarjeta inteligente.[2]

[1] http://www.latinoseguridad.com/LatinoSeguridad/Reps/TI.shtml

[2] Sandoval Juan D., Brito Ricardo, Mayor Juan C., 1999. "Tarjetas Inteligentes". España: Thomson Publishing Company.

- VCC.- Fuente de alimentación del chip.
- RST.- Reset del chip
- CLK.- Reloj.
- RFU.- Contacto reservado para usos futuros.
- I/O.- Punto de entrada y salida de la información.
- VPP.- Voltaje externo que permite programar la memoria de la tarjeta.
- GND.- Tierra.

Tarjetas inteligentes sin contacto

Tienen una estructura y funcionalidad similar a las tarjetas inteligentes de contacto con la diferencia que éstas ya no utilizan contacto físico sino una interface inductiva (Figura 1.3) es decir la comunicación se la realiza por medio de antenas por donde se transfiere toda la información entre el lector y la tarjeta, el tipo de interface utilizado implica que se utilicen otros protocolos de comunicación los mismos que se encuentran especificados en el estándar ISO 14443.

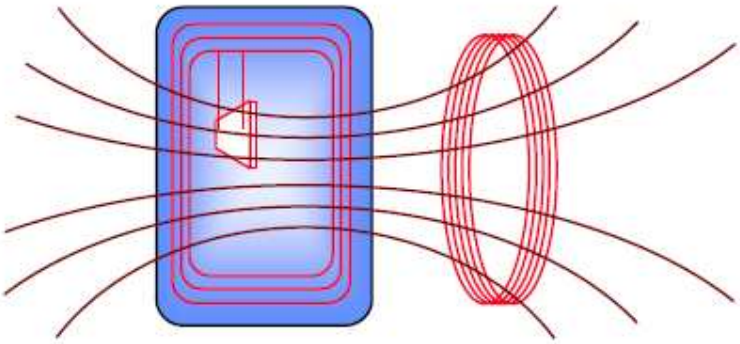


Figura 1.3 Tarjeta inteligente sin contacto[3]

.

Este tipo de tarjetas permiten tener una lectura mucho más rápida que una tarjeta de contacto ya que no es necesario hacer una inserción en el lector y además se evitan los problemas de fallos en la lectura por el deterioro en la superficie de los contactos o por residuos que impiden realizar una lectura correcta.

[3] http://www.idensis.com/tecnologias_elementos.html

Estas tarjetas reciben su alimentación de energía ya sea por medio de una batería insertada junto al chip o por medio de un hilo metálico sobre el cual se induce una corriente eléctrica que es capaz de alimentar al resto de elementos del circuito.

1.1.4 ESTÁNDARES

Cada tipo de tarjeta se rige a los estándares de la ISO en donde se especifican las características que deben cumplir las tarjetas inteligentes.

Tarjetas inteligentes de contacto

Este tipo de tarjetas cumplen con los estándares de la serie ISO 7816 partes del 1 al 10:

ISO 7816-1:

Define las características físicas de la tarjeta dentro de estas tenemos:

- Dimensiones de la tarjeta
- Tolerancia frente a la radiación electromagnética
- Tolerancia frente a la tensión electromecánica
- Tolerancia a los Rayos-X y luz ultravioleta
- Resistencia a la electricidad estática
- Localización del chip en la tarjeta

ISO 7816-2:

Define las dimensiones, ubicación número y función de cada uno de los contactos. Para el caso se tienen 8 contactos de los cuales se utilizan únicamente 6.

ISO 7816-3:

Define las señales electrónicas, niveles de tensión procedimientos, protocolos de transmisión así como también el procedimiento para iniciar una comunicación.

ISO 7816-4:

Define los comandos y respuestas entre la tarjeta y los dispositivos de acceso. Estructura de los ficheros y métodos de acceso.

ISO 7816-5:

Define el sistema de numeración y proceso de registro para identificadores de aplicaciones (AIDs).

ISO 7816-6:

Define las reglas a seguir para codificar la información necesaria en la tarjeta.

ISO 7816-7:

Define el lenguaje de consulta estructurado de tarjeta (SCQL) para la interoperabilidad de los comandos.

ISO 7816-8:

Incluye los comandos para el control interno de la seguridad de la tarjeta y puede incluir técnicas de cifrado y otros métodos para el control de la seguridad.

ISO 7816-9:

Define comandos adicionales así como también atributos de seguridad

ISO 7816-10:

Define las señales electrónicas y respuesta al reset para una tarjeta síncrona.

Tarjetas inteligentes sin contacto

Este tipo de tarjetas está estandarizado por la norma ISO 14443 partes de 1 al 4.

ISO 14443-1:

Define las características físicas de la tarjeta.

ISO 14443-2:

Frecuencia de operación y potencia de la señal de transmisión.

ISO 14443-3:

Inicialización de la comunicación entre la tarjeta y el lector y métodos de anticolisión.

ISO 14443-4:

Define los protocolos de transmisión.

Tipos de lectores

El lector es un dispositivo que permite tener acceso a la información contenida en las tarjetas inteligentes, normalmente son dispositivos adaptadores que se incorporan al sistema de comunicaciones del ordenador generalmente por un puerto específico, se los puede dividir de la siguiente manera.

- Lectores conectados a un ordenador: Estos lectores son fabricados para ser usados conectándolos a un ordenador, esta conexión puede ser a través de un puerto serial, USB, PCMCIA, etc.
- Lectores conectados a un equipo específico: Son lectores que se pueden instalar en un aparato determinado para cumplir con una cierta función. Estos lectores se pueden instalar en cajeros automáticos, máquinas expendedoras, peajes, accesos a escenarios masivos, etc.
- Lectores Portátiles: Son equipos que no necesitan de otro aparato para cumplir su función. Estos lectores poseen los recursos integrados como baterías, memoria, etc.

1.1.5 VENTAJAS Y DESVENTAJAS

Entre las principales ventajas tenemos:

- Capacidad de almacenamiento y procesamiento seguro que otorga el microprocesador.
- Está sujeta a estándares internacionales lo que garantiza su uso universal.
- Tiempo de vida largo
- Los sistemas operativos de estas tarjetas soportan múltiples aplicaciones y políticas de seguridad independientes para almacenamiento de datos en una misma tarjeta.

Como desventajas tenemos las siguientes:

- El costo unitario y de gestión alto.

- La ausencia de infraestructura implica que se tenga que instalar lectores en los ordenadores implicados y en otros dispositivos que sean necesarios.
- Compatibilidad de los dispositivos y el software a pesar de la existencia de los estándares.
- Ambigüedades legales relacionadas con la privacidad y confidencialidad del usuario.

1.1.6 SEGURIDAD EN TARJETAS INTELIGENTES

Se deben tener algunos criterios en la protección de la información expuesta en la seguridad de información, las tarjetas inteligentes las afrontan de la siguiente manera:

Confidencialidad. No se debe aplicar sólo a los datos almacenados en la tarjeta sino también a los datos almacenados en otros sistemas que pueden ser accedidos usando la tarjeta. Los controles de acceso y cifrado son las herramientas más usadas para proteger la confidencialidad y la privacidad.

Integridad. Los datos almacenados en la tarjeta o en otro sistema deberían estar protegidos contra alteraciones. Para ello las tareas de memoria pueden ser protegidas contra accesos no autorizados, o con memoria WORM (write once, read many times), que sólo puede ser escrita una vez.

No repudio. Ni el dueño de la tarjeta ni la entidad puedan repudiar la transacción o reclamar que nunca tuvo lugar.

"Los requerimientos del almacenamiento dependerían de si los datos deben ser portables o accedidos sin conexión, por lo que podrían ser almacenados en una tarjeta; o si no sería preferible almacenar los datos en el computador y usar la tarjeta para permitir el acceso a los datos". [4] Según el nivel de confidencialidad requerido se tiene lo siguiente:

- Almacenar los datos en claro en una tarjeta con memoria o en un fichero del ordenador.

[4] http://www.tec-mex.com.mx/promos/bit/bit0703-msr.htm

- Almacenar los datos en una tarjeta con memoria protegida o en un ordenador con control de acceso controlado por una contraseña o un sistema de tarjeta.
- Cifrar los datos o almacenarlos en una tarjeta con memoria y circuitos de protección

Los datos se hacen confusos a personas no autorizadas a través de cifrado con clave secreta. También se debe comprobar que los datos almacenados no son alterados, y que no se pueden perder como resultado de un mal funcionamiento o fallo eléctrico.

Cuando los datos son transmitidos desde un sistema a otro, se debe asegurar que la información no es alterada, accidental o deliberadamente, en el camino. Si es confidencial, entonces se debe proteger el interfaz físicamente o con cifrado. Para comprobar la integridad de los mensajes se usan códigos de redundancia cíclica (CRCs, Cyclic Redundancy Checks), contadores de transacción y códigos de autenticación de mensajes (MACs,Message Authentication Code).

1.2 SISTEMAS BIOMÉTRICOS

1.2.1 DEFINICIÓN

El término biometría proviene de los términos bio (vida) y metría (medida), estudia la identificación o verificación de individuos a partir de una característica física o del comportamiento de la persona. Esta tecnología se basa que cada persona es única y posee rasgos distintivos que pueden ser utilizados para identificarla.

1.2.2 CARACTERÍSTICAS

Las principales características que debe cumplir un sistema biométrico para la identificación de personal son:

- El desempeño: El sistema de debe ser rápido, exacto y robusto al momento de identificar a un individuo.
- La aceptabilidad: El grado hasta el cual los usuarios están dispuestos a aceptar el sistema biométrico, el sistema debe proteger la integridad física de las personas y debe inspirar confianza ya que a veces en lugar de

obtener información para validar un parámetro de acceso se puede estar profanando rasgos importantes del usuario.

- La fiabilidad: Esta característica refleja cuán seguro es el sistema al momento de validar la información de acceso ya que en ocasiones se puede tratar de suplantar la identidad de una persona por medio de diferentes técnicas como por ejemplo crear dedos de látex, prótesis de ojos, grabaciones de voz, etc.

1.2.3 TIPOS DE SISTEMAS BIOMÉTRICOS

Entre los diferentes tipos de Sistemas Biométricos tenemos:

Rostro

Este sistema de reconocimiento es el más dable ya que el rostro es la manera directa para identificar familiares, amigos o conocidos. Los métodos utilizados en el reconocimiento de rostros van desde la correlación estadística de la geometría y forma de la cara, hasta el uso de redes neuronales que funcionan en el cerebro humano.

Iris

El método del iris del ojo es el método más raro para las personas ya que el humano no se reconoce por la apariencia del iris y también no es un método utilizado por la ley.

El método es como sigue: la imagen del iris se captura con una cámara de alta resolución y el sistema analiza dobleces y patrones, que son manejados para identificar a la persona, por lo general esto se hace acercando una cámara al ojo o mirando a través del lente de una cámara fija.

Este identificador es uno de los más precisos entre los sistemas biométricos.

Huellas digitales

Gracias a que los patrones de las huella digitales son únicos y se mantienen durante la vida de la persona, ésta es la primera técnica que se viene a la mente y de hecho es un método utilizado en diversos proyectos de muchos países para la construcción de bases de datos de huellas digitales para control y por otro lado la incorporación de la tecnología en diminutos aparatos tales como teléfonos móviles, ordenadores portátiles, teclados, tarjetas bancarias, armas de fuego, entre otros.

Firma

"La firma es un método de verificación de identidad de uso habitual, a diario las personas utilizan su firma para validar cheques o documentos importantes". [5]
Dependiendo del sistema ya sea la superficie donde se firma como el bolígrafo utilizado pueden contener varios sensores, que miden características mucho más allá que la forma o apariencia de la firma.

Voz

La voz es una característica que las personas utilizan para identificar a los demás y al igual que los sistemas basados en el rostro, goza de mucha aceptación entre sus usuarios.

Los sistemas de verificación mediante la voz "escuchan" mucho más allá del modo de hablar y el tono de voz. Mediante el análisis de los sonidos que emitimos, estos sistemas también crean modelos de la anatomía de la tráquea, cuerdas vocales y cavidades.

---

[5] http://www.microsoft.com/latam/technet/articulos/articulos_seguridad/NewsAbril06/abr06-01.mspx

En la siguiente tabla se pueden resumir 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 Tabla comparativa de sistemas biométricos

1.2.4 ARQUITECTURA

La arquitectura de un sistema biométrico está compuesta de dos módulos:

- Módulo de inscripción.
- Módulo de identificación.

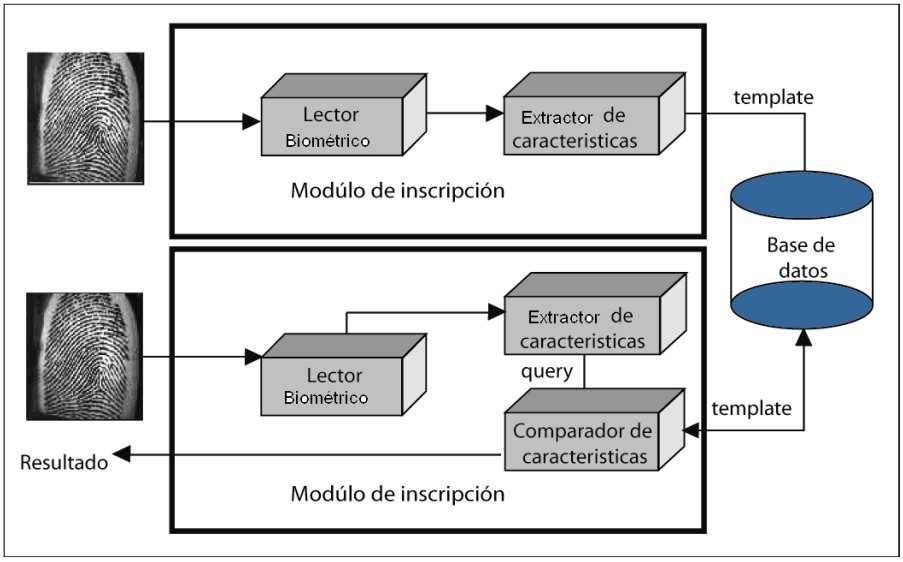


Figura 1.4 Arquitectura de un sistema biométrico para identificación personal, aquí ejemplificado con huellas dactilares[6]

En el módulo de inscripción se obtiene la información proveniente de un indicador biométrico elegido luego se convierte esta información a formato digital para que luego el extractor de características produzca una representación compacta que será almacenada en la Base de Datos.

El módulo de identificación es el responsable del reconocimiento del individuo. Este proceso inicia cuando el lector biométrico captura la característica del individuo a ser identificado y la convierte a formato digital, para que a continuación el extractor de características produzca una representación compacta con el mismo formato de la información almacenada en la Base de Datos, esta representación es enviada al comparador de características el cual confronta con los respectivos registros almacenados en la Base de Datos para establecer la identidad.

1.2.5 FASE OPERACIONAL DE UN SISTEMA DE IDENTIFICACIÓN PERSONAL

La fase operacional en un sistema biométrico opera en 2 modos:

[6] http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm

- Modo de Verificación
- Modo de Identificación

En el modo de verificación un sistema biométrico acredita la identidad de un individuo comparando su característica con el template, así si una persona ingresa su nombre de usuario entonces no es necesario revisar toda la base de datos buscando el template que más se asemeje al de él, sino basta con comparar la información de entrada que esté asociada al usuario.

"Un sistema que esté operando en modo de identificación revela a un individuo mediante una búsqueda exhaustiva en la base de datos con los templates lo que conduce a una comparación de tipo uno a muchos para constituir la identidad del individuo". [7]

1.2.6 EXACTITUD EN LA IDENTIFICACIÓN: MEDIDAS DE DESEMPEÑO

Toda la información provista por los templates permiten particionar la base de datos conforme la presencia de ciertos patrones particulares para cada indicador biométrico. Una decisión tomada para un sistema biométrico distingue personal autorizado o impostor y para cada decisión existe dos posibles salidas de verdadero o falso, se tiene entonces cuatro posibles respuestas del sistema.

- Una persona autorizada es aceptada,
- Una persona autorizada es rechazada,
- Un impostor es rechazado,
- Un impostor es aceptado

[7] http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm

El grado de confidencialidad asociado a las diferentes decisiones puede ser distinguido por la distribución estadística del número de personas autorizadas e impostores. Con las estadísticas anteriores se establecen dos tasas de errores:

- Tasa de falsa aceptación (FAR: False Acceptance Rate), que se define como la frecuencia relativa con que un impostor es aceptado como un individuo autorizado,
- Tasa de falso rechazo (FRR: False Rejection Rate), definida como la frecuencia relativa con que un individuo autorizado es rechazado como un impostor

La FAR y la FRR son funciones del grado de seguridad anhelado. En efecto, usualmente el resultado del proceso de identificación o verificación será un número real normalizado en el intervalo [0, 1], que indicará el "grado de parentesco" o correlación entre la característica biométrica proporcionada por el usuario y la(s) almacenada(s) en la base de datos

La FAR y la FRR están íntimamente relacionadas, efectivamente son duales una de la otra: una FRR pequeña usualmente entrega una FAR alta, y viceversa, como muestra la figura 1.5

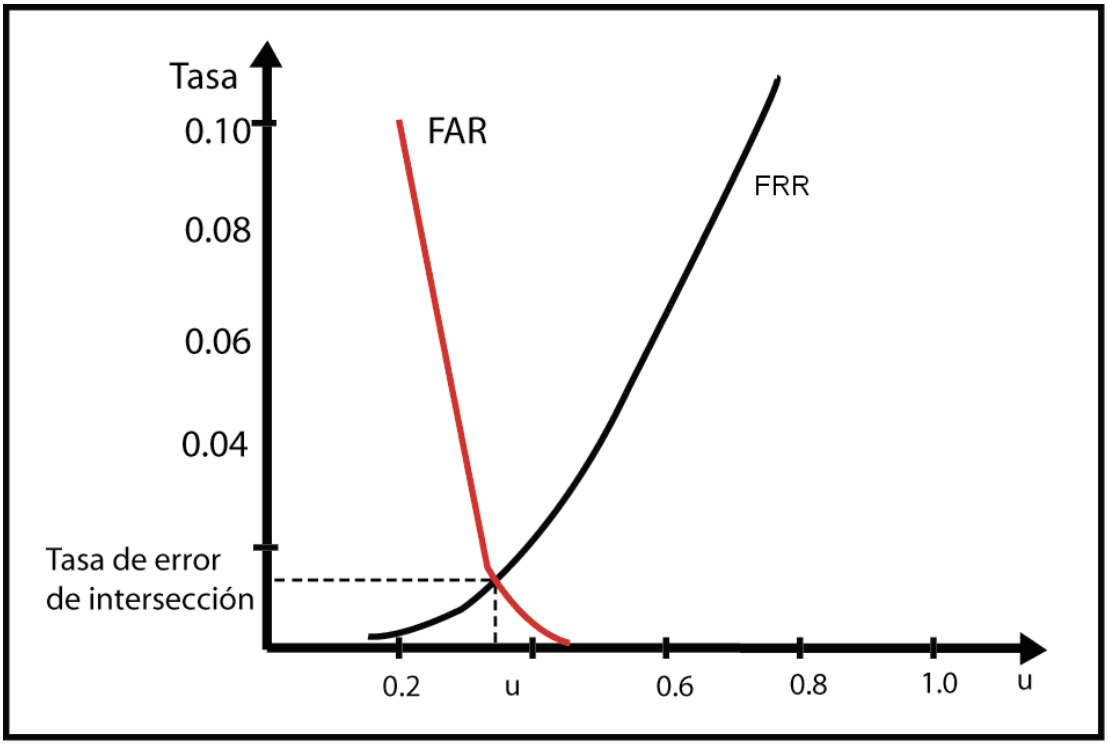


Figura 1.5 Gráfica típica de la tasa de falso rechazo (FRR) y la de falsa aceptación (FAR) como funciones del umbral de aceptación u para un sistema biométrico.[8]

1.3 SISTEMAS BASADOS EN TARJETAS MAGNETICAS

1.3.1 DEFINICIÓN

Son tarjetas que utilizan uno o varios medios de identificación única o especial como son banda magnética, código de barras, panel de firma, chip, banda para raspar, etc., para aplicaciones de todo tipo, que van desde sistemas de identificación hasta programas de probidad.

1.3.2 FUNCIONAMIENTO

El uso intensivo y extendido de tarjetas magnéticas ha hecho necesaria la aparición de estándares que definan sus dimensiones, propiedades físicas (flexibilidad, resistencia, etc.), número de pistas, medidas de las pistas, forma de codificar la información y demás características.

[8] http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm

La banda oscura en las tarjetas es una banda magnética, hecha de un pigmento a base de pequeñas partículas ferromagnéticas, cada partícula produce un pequeño campo magnético pero, al estar cada uno orientado en distinta dirección, el efecto neto que producen es como si no existiera campo magnético en absoluto.

En el momento de la grabación, un solenoide o electroimán va pasando a lo largo de la banda. De esta forma, cuando la banda ha sido grabada, tendremos en ella una fila de zonas en las que las partículas estarán magnetizadas en la misma dirección. Estas zonas actuarán ahora como pequeños imanes, presentando sus polos norte o sur a la superficie de la tarjeta.

La lectura se realizará con otro solenoide (estos solenoides son lo que llamamos normalmente cabezales).

La técnica utilizada para codificar la información digital es conocida como "bifase Aiken", "codificación por doble frecuencia de fase coherente" o simplemente "F/2F". Los bits están representados por celdas entre las que existe una inversión de flujo magnético. Si en el interior de la celda (en la mitad) existe también una inversión del flujo, la celda será un uno, en caso contrario será un cero. Es decir, los unos están representados por una onda de frecuencia doble que la de los ceros, y cada bit tiene una "longitud" igual al período de la onda que representa el cero.

1.3.3 COERCITIVIDAD

La coercitividad es la fuerza electromagnética requerida para magnetizar o codificar la banda. Los "Oersteds" son las unidades con las cuales se mide la "coercitividad". En la industria son usadas tarjetas de baja (300 oersteds). Y alta (3.600-6.000 oersteds) coercitividad

En un principio, las tarjetas personalizadas en alto relieve fueron las primeras en desarrollar la personalización de carnets.

Con el paso del tiempo, fue evidente que un método más rápido era necesario, por lo que se desarrolló la codificación de la banda magnética, la banda magnética generalmente se ubica en la cara posterior de la tarjeta y está hecha de un material magnético similar a los materiales usados para cintas de audio y video.

La información es magnéticamente codificada en la banda, posteriormente, un lector de banda magnética puede ser usado para leer esta información. Usando la tecnología de máquinas lectoras, la posibilidad de errores humanos se reduce y la velocidad de transacciones de la información es mucho más rápida

Estándares ANSI / ISO

The American National Standard Institute (ANSI), y The International Organization for Standarization (ISO), son dos de las organizaciones que desarrollan el conjunto de estándares y especificaciones para codificar la banda magnética.

Estas especificaciones dan la pauta para poder utilizar la banda con la codificación de los datos de tal manera que pueda ser utilizada a nivel mundial.

Al considerar las capacidades de codificación de sus tarjetas, es necesario identificar el tipo de lectores a usar en la aplicación, para así asegurar que la tarjeta sea compatible con el lector.

1.3.4 TRACKS

La opción para banda magnética de las impresoras “Datacard”, permiten codificar información en bandas magnéticas, dependiendo del tipo de codificación que se adquiera, la opción puede codificar tarjetas de coercitividad alta o baja, con dos o tres pistas de datos.

- El formato IATA (International Air Transport Association): permite 79 caracteres alfa numéricos. Esto permite espacios, números, letras, así como caracteres especiales.

- El formato ABA (American Bankers Association): permite sólo caracteres numéricos, así como caracteres especiales. ·
- El formato TTS (Thrift Third Standard): permite sólo caracteres numéricos, así como caracteres especiales.

Tracks	Densidad de Grabación (bits per inch)	Configuración de caracteres (including parity bit)	Contenido de información
Tracks 1	210 bpi	7 bits por caracter	79 caracteres alfanuméricos
Tracks 2	75 bpi	5 bits por caracter	40 caracteres alfanuméricos
Tracks 3	210 bpi	5 bits por caracter	107 caracteres alfanuméricos

Tabla 1.2 Tabla para la codificación de las tarjetas

1.3.5 CÓMO GRABAR TARJETAS MAGNÉTICAS

La información digitalizada es almacenada al alterar la polaridad de diminutas partículas incrustadas en una resina. Los datos de una tarjeta son codificados en un formato binario, con la polaridad de las partículas determinando los bits con valores de 0 y 1. Un lector detecta y decodifica los cambios de polaridad y traduce el código binario a alfanumérico.

La tecnología de banda magnética involucra la grabación digital (llamada codificación) de la información en una banda con una capa magnética de forma similar a la que se utiliza en las cintas de audio y video, la cual puede ser leída de manera repetida. Una de las principales características de las bandas magnéticas es que pueden ser re-codificadas y usadas de nuevo, lo cual es trascendental en muchas aplicaciones.

1.4 CÓDIGOS DE BARRAS

1.4.1 DEFINICIÓN

El código de barras radica en una serie de barras negras y espacios en blanco de diferentes anchos que permiten la captura automática de información. Las impresiones de código de barras son leídas con un scanner (unidad de rastreo), el cual mide la luz reflejada e interpreta la clave en números y letras para luego alimentar esta información a otros sistemas.

El código de barras, almacena datos que pueden ser reunidos en él de manera rápida y con una gran precisión. Los códigos de barras representan un método simple y fácil para codificación de información de texto que puede ser leída por dispositivos ópticos.

Para codificar datos dentro de un símbolo impreso, se usa una barra predefinida y patrones de espacios o simbología.

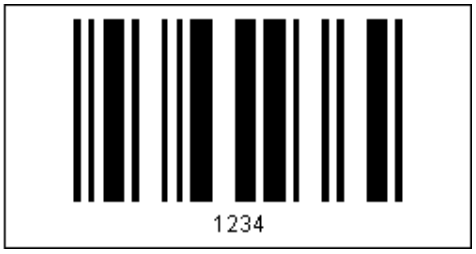


Figura 1.6 Código de Barras[9]

Un símbolo de código de barras es la visualización física, es la impresión de un código de barras. Una simbología es la forma en que se codifica la información en las barras y espacios del símbolo de código de barras.

1.4.2 BENEFICIOS DEL CÓDIGO DE BARRAS

El código de barras es el mejor sistema de colección de datos mediante identificación automática, y presenta muchos beneficios, entre otros.

[9] http://www.geocities.com/SoHo/Cafe/8909/barcode.html

- Virtualmente no hay retrasos desde que se lee la información hasta que puede ser usada
- Se mejora la exactitud de los datos, hay una mayor precisión de la información.
- Se tienen costos fijos de labor más bajos
- Se puede tener un mejor control de calidad, mejor servicio al cliente
- Se pueden contar con nuevas categorías de información.
- Se mejora la competitividad.
- Se reducen los errores.
- Se capturan los datos rápidamente
- Se mejora el control de la entradas y salidas
- Precisión y contabilidad en la información, por la reducción de errores.
- Eficiencia, debido a la rapidez de la captura de datos.

1.4.3 APLICACIONES

"Las aplicaciones del código de barras cubren prácticamente cualquier tipo de actividad humana, tanto en industria, comercio, instituciones educativas, instituciones médicas, gobierno, etc., es decir, cualquier negocio se puede beneficiar con la tecnología de captura de datos por código de barras, tanto el que fabrica, como el que mueve, como el que comercializa los productos." [10]

- Entre las aplicaciones que tiene podemos mencionar:
- Control de material en procesos
- Control de inventario
- Control de movimiento
- Control de tiempo y asistencia
- Control de acceso

[10] http://www.microsoft.com/latam/technet/articulos/articulos_seguridad/NewsAbril06/abr06-01.mspx

- Punto de venta
- Control de calidad
- Control de embarques y recibos
- Control de documentos y rastreos de los mismos
- Rastreos preciso en actividades
- Rastreos precisos de bienes transportados
- Levantamiento electrónico de pedidos
- Facturación
- Bibliotecas

1.4.4 SIMBOLOGÍA DEL CÓDIGO DE BARRAS

Podría decirse que los códigos de barras vienen en muchas formas o presentaciones. Muchos son familiares porque se los mira en las tiendas en los negocios, pero existen algunos otros que son estándares en varias industrias. La industria de la salud, manufacturas, almacenes, etc. tienen terminologías únicas para su industria y que no son intercambiables.

La existencia de varios tipos de códigos de barras, se debe a que las simbologías están diseñadas para resolver problemas específicos. De acuerdo al tipo de necesidad de identificación interna del negocio, de acuerdo con los requisitos que se deben cumplir para poder comerciar según las normas del mercado, se debe optar por el sistema de codificación más adecuado.

Las simbologías se dividen en:

- Primera dimensión
- Segunda dimensión

CÓDIGO DE BARRAS DE PRIMERA DIMENSION

1.4.4.1.1 *Universal Product Code (U.P.C.)*

UPC es la simbología más utilizada en el comercio minorista de EEUU, pudiendo codificar solo números. El estándar UPC (denominado **UPC-A)** es un número de

12 dígitos. El primero es llamado "número del sistema". La mayoría de los productos tienen un "1" o un "7" en esta posición. Esto indica que el producto tiene un tamaño y peso determinado, y no un peso variable. Los dígitos del segundo al sexto representan el número del fabricante. Esta clave de 5 dígitos (adicionalmente al "número del sistema") es única para cada fabricante, y la asigna un organismo rector evitando códigos duplicados. Los caracteres del séptimo al onceavo son un código que el fabricante asigna a cada uno de sus productos, denominado "número del producto". El doceavo carácter es el "dígito verificador", resultando de un algoritmo que involucra a los 11 números previos.
Este se creó en 1973 y desde allí se convirtió en el estándar de identificación de productos, se usan desde entonces en la venta al detalle y la industria alimenticia.

Figura 1.7 Simbología UPC[11]

1.4.4.1.2 *European Article Numbering (E.A.N.)*

El EAN es la versión propia del UPC europea, se creó en 1976. El sistema de codificación EAN es usado tanto en supermercados como en comercios. Es un estándar internacional, creado en Europa y de aceptación mundial. Identifica a los productos comerciales por intermedio del código de barras, indicando país-empresa-producto con una clave única internacional.
El EAN-13 es la versión más difundida del sistema EAN y consta de un código de 13 cifras (uno más que el UPC) en la que sus tres primeros dígitos identifican al país, los seis siguientes a la empresa productora, los tres números posteriores al artículo y finalmente un dígito verificador, que le da seguridad al sistema. Este dígito extra se combina con uno o dos de los otros dígitos para representar un código, indicando el origen de la mercancía.

Para artículos de tamaño reducido se emplea el código EAN-8.

[11] http://www.ent.ohiou.edu/~amable/autoid/history.htm

Figura 1.8 Simbología E.A.N[12]

1.4.4.1.3 *Código 39*

El Code 39 (o Code 3 de 9) es el código de barras de uso más común para aplicaciones regulares. Es popular debido a que puede contener texto y números (A - Z, 0 - 9, +, -, ., y), puede ser leído por casi cualquier lector de código de barras en su propia configuración, además es uno de los más viejos entre los códigos de barras modernos. El Code 39 es un código de barras de ancho variable y puede tolerar cualquier número de caracteres que el lector pueda barrer. El Code 39 se encuentra en muchas especificaciones militares y de gobierno. Estos códigos de barras son de auto revisión y no están propensos a errores de sustitución

Figura 1.9 Código 39[13]

1.4.4.1.4 *Código 128.*

Esta simbología es un código de barras muy compacto para toda aplicación alfanumérica. "El conjunto de caracteres ASCII completo (128 caracteres) puede ser codificado en esta simbología sin duplicar caracteres como en el Code 39 extendido. Si el código de barras tiene 4 o más números consecutivos (0 - 9), los números están codificados en modo doble densidad (donde dos caracteres están codificados en una sola posición)." [14] El Code 128 tiene cinco caracteres especiales para funciones no de datos. Estas son usadas para poner o regresar los parámetros del lector.

[12] http://www.ent.ohiou.edu/~amable/autoid/history.htm
[13] http://www.ent.ohiou.edu/~amable/autoid/history.htm
[14] http://www.ent.ohiou.edu/~amable/autoid.html

Figura 1.10 Código 128[15]

1.4.4.1.5 *Entrelazado 2 de 5.*

Es conocido también como el 2 de 5, es un código de barras exclusivamente numérico cuya figura es ligeramente más larga que el código de barras UPC-A cuando está codificado con 10 dígitos. Esta simbología tiene la flexibilidad para codificar cualquier número par de dígitos. Si el número es impar se coloca un cero al principio. Este código de barras es un excelente candidato para aplicaciones exclusivamente numéricas y es la mejor simbología para lectores de montaje fijo.

Figura 1.10 Entrelazado 2 de 5[16]

1.4.4.1.6 *Codabar*.

Los códigos de barras codabar pueden incluir caracteres numéricos, caracteres de seis puntuaciones (-$:/.+) y espacios. Hay también 4 caracteres especiales de inicio/alto, los cuales son A, B, C, y D. El Codabar es útil para codificar símbolos de pesos y de matemáticas. Estos códigos de barras son ligeramente más largos que los de Interleaved(intercalado). El Codabar requiere caracteres para iniciar y parar.

Figura 1.11 Codabar[17]

[15] http://www.ent.ohiou.edu/~amable/autoid/history.htm
[16] http://www.ent.ohiou.edu/~amable/autoid/history.htm

1.4.4.1.7 *Posnet* .

Es sólo para el Servicio Postal de Estados Unidos, esta simbología codifica los códigos postales para un procesamiento más rápido de entrega del correo. Este aparece en el año 1980.

Figura 1.12 Posnet[18]

CÓDIGO DE BARRAS DE SEGUNDA DIMENSION

1.4.4.1.8 *PDF 417*

Conocido como un código de dos dimensiones, es una simbología de alta densidad no lineal que recuerda un rompecabezas. Pero la diferencia entre éste y los otros tipos de código de barras, es que el PDF417 es en realidad un Portable Data File (Archivo de Información Portátil, PDF) es decir, no se requiere consultar a un archivo, este contiene toda la información, ya que tiene una capacidad de hasta 1800 caracteres numéricos, alfanuméricos y especiales.

Este tipo de códigos de barras tiene diversas aplicaciones:

- Industria en general.
- Sistemas de paquetería: cartas porte.
- Compañías de seguros: validación de pólizas.
- Instituciones gubernamentales: aduanas.
- Bancos: reemplazo de tarjetas y certificación de documentos.
- Transportación de mercadería: manifiestos de embarque.
- Identificación personal y foto credencial.
- Registros públicos de la propiedad

[17] http://www.ent.ohiou.edu/~amable/autoid/history.htm
[18] http://www.ent.ohiou.edu/~amable/autoid/history.htm

Figura 1.13 PDF 417[19]

1.4.4.1.9 *Mexicode.*

Es utilizado para procesamiento de información a alta velocidad, la estructura del Maxicode consiste de un arreglo de 866 hexágonos utilizados para el almacenamiento de datos en forma binaria. Estos datos son almacenados en forma seudo-aleatoria. Posee un blanco o "bull" utilizado para localizar a la etiqueta en cualquier orientación.

Es posible codificar hasta 100 caracteres en un espacio de una pulgada cuadrada. Este símbolo puede ser decodificado sin importar su orientación con respecto al lector óptico.

La simbología utiliza el algoritmo de Reed-solomon para corrección de error. Esto permite la recuperación de la información contenida en la etiqueta cuando hasta un 25 por ciento de la etiqueta esté dañado.

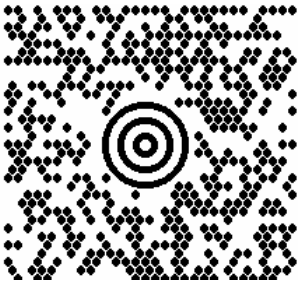


Figura 1.14 Mexicode[20]

1.4.4.1.10 *Datamatrix.*

Tiene una capacidad alfanumérica de 2334 caracteres.

Algunas de las aplicaciones que tiene son:

[19] http://www.ent.ohiou.edu/~amable/autoid/history.htm
[20] http://www.geocities.com/SoHo/Cafe/8909/barcode.html

- Codificación de dirección postal en un símbolo bidimensional (usos en el servicio postal para automatizar ordenado del correo).
- Marcado de componentes para control de calidad.
- Los componentes individuales son marcados identificando al fabricante, fecha de fabricación y número de lote, etc.
- Etiquetado de desechos peligrosos (radioactivos, tóxicos, etc.) para control y almacenamiento a largo plazo.
- Industria farmacéutica, almacenamiento de información sobre composición, prescripción, etc.
- Boletos de lotería, información específica sobre el cliente puede codificarse para evitar la posibilidad de fraude, Instituciones financieras, transacciones seguras codificando la información en cheques

Figura 1.15 DataMatrix[21]

1.4.5 TIPOS DE LECTORES.

El lector de código de barras decodifica la información a través de la digitalización proveniente de una fuente de luz reflejada en el código y luego se envía la información a una computadora como si la información hubiese sido ingresada por teclado.

El procedimiento: el símbolo de código de barras es iluminado por una fuente de luz visible o infrarrojo, las barras oscuras absorben la luz y los espacios las reflejan nuevamente hacia un escáner.

El escáner transforma las fluctuaciones de luz en impulsos eléctricos los cuales copian las barras y el modelo de espacio en el código de barras. Un decodificador

[21] http://www.geocities.com/SoHo/Cafe/8909/barcode.html

usa algoritmos matemáticos para traducir los impulsos eléctricos en un código binario y transmite el mensaje decodificado a un terminal manual, PC, o sistema centralizado de computación.

El decodificador puede estar integrado al escáner o ser externo al mismo. Los escáners usan diodos emisores de luz visible o infrarroja (LED), láser de Helio-Neón o diodos láser de estado sólido (visibles o infrarrojos) con el fin de leer el símbolo.

Los cuatro principales tipos de lectores son:

Lápiz Óptico o Wand.

Debe ser deslizado haciendo contacto a lo ancho del código. Como se menciona anteriormente, envía una señal digital pura de las barras y espacios a una frecuencia igual a la velocidad con que se desliza el lápiz.

- Ventajas: es económico
- Desventajas: es lento, requiere que el usuario tenga práctica, tiene un bajo “first read rate”, requiere un decodificador de teclado, depende de la calidad de impresión del código.

Láser de pistola.

Realiza un barrido mediante una luz láser y que genera una señal similar a la del lápiz óptico, pero a una mayor frecuencia. Esta señal es conocida como HHLC (Hand Held Laser Compatible)

- Ventajas: es rápido, puede no requerir decodificador de teclado, puede leer a distancia (estándar 5 a 30 cm, especial hasta 15m con etiquetas de papel retroreflectivo), tiene un alto FRR.
- Desventajas: es relativamente caro (aunque existen modelos de $ 545 USD), puede presentar problemas de durabilidad debido a sus partes

móviles (espejos giratorios), puede tener problemas para leer con demasiada luz ambiental.

CCD (CHARGE COUPLED DEVICE).

Mediante un arreglo de fotodiodos toma una 'foto' del símbolo de código de barras y la traduce a una señal, que puede ser similar a la enviada por el láser (HHLC) o a la del lápiz óptico.

- Ventajas: es rápido, es económico, es muy durable por no tener partes móviles, puede no necesitar decodificador de teclado, tiene un alto FRR.
- Desventajas: requiere estar muy cerca del código (0-1.5cm), no puede leer símbolos que rebasen el ancho de su ventana

Láser Omnidireccional.

Es un lector que envía un patrón de rayos láser y que permite leer un símbolo de código de barras sin importar la orientación del mismo.

- Ventajas: Todas las ventajas del láser de pistola más un FRR de prácticamente 100%.
- Desventajas: es caro (aquí no hay modelos económicos), el operador requiere que los artículos etiquetados no sean muy voluminosos pues el scanner se monta en posición fija

Lectores autónomos.

No requieren atención, se usan en aplicaciones automatizadas o de cinta transportadora. Varían en velocidad de lectura según la producción y la orientación requerida de los códigos de barras, línea única, multilínea y omnidireccional.

Lectores de código de barras de 2D.

Leen códigos en dos dimensiones como PDF, DATAMATRIX y MAXICODE.

La estructura básica de un código de barras 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.

La información es leída por dispositivos ópticos los cuales envían la información a una computadora como si la información hubiese sido tecleada.

CAPITULO 2

TECNOLOGÍA DE IDENTIFICACIÓN POR RADIO FRECUENCIA (RFID)

Cada vez es más frecuente la necesidad de tener una identificación automática por medio de varias tecnologías las mismas que son usadas para identificar objetos o personas de acuerdo al caso, la identificación automática viene de la mano con la colección automática de datos (CAD), esto con el objetivo de aumentar la eficiencia, reducir el número de errores y principalmente dejar de lado la intervención del factor humano en tareas que son de mucho valor para una empresa.

Una de las tecnologías de identificación más importantes de la actualidad es RFID (Radio Frequency Identification) es un sistema que transmite la identidad de un objeto o persona a través de ondas de radio, en este sistema los lectores o interrogadores transmiten los datos de las etiquetas (TAGs) a un sistema de computación para que dichos datos sean procesados.

En el presente capitulo se hará una mención en detalle acerca de esta tecnología de identificación, para lo cual es fundamental conocer los conceptos asociados con RFID que se los presenta en la siguiente sección.

2.1 FUNDAMENTOS DE RFID.

La onda es una perturbación que trasporta energía de un lugar a otro. Las ondas electromagnéticas son creadas por electrones en movimiento y consiste de oscilaciones eléctricas y campos magnéticos, estas ondas pueden pasar a través de diferentes tipos de materiales.

2.1.1 PARTES DE UNA ONDA.

Una onda electromagnética está formada de las siguientes partes:

Cresta.- Es punto más alto de la onda electromagnética

Valle.- Es el punto más bajo de la onda electromagnética

Longitud de onda.- Es la distancia que existe entre dos crestas consecutivas.

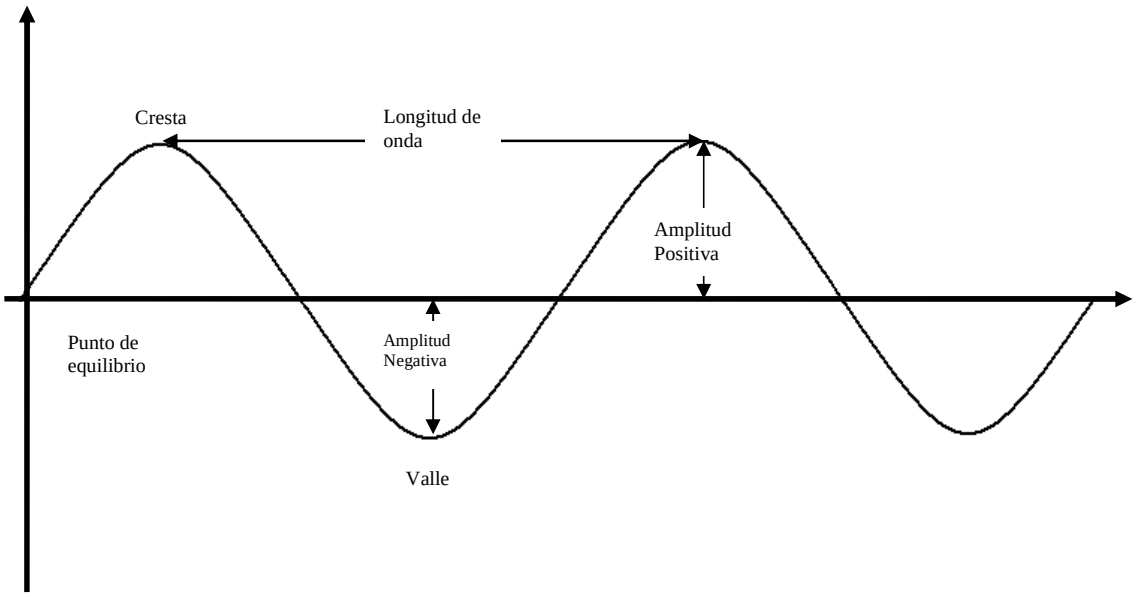


Figura 2.1 Diferentes partes de una onda

Ciclo.- Viene dado por la longitud de onda que es el parámetro físico que indica el tamaño de una onda.

Período.- Es el tiempo que tarda la onda en recorrer un ciclo, viene dado en segundos.

Frecuencia.- Es el número de ciclos que se presentan en un segundo. La frecuencia viene medida en Hertz.

Amplitud.- Es la altura de la cresta (Amplitud Positiva) o la profundidad del valle (Amplitud Negativa) medido desde el punto de equilibrio.

RFID usa ondas de radio que generalmente están entre las frecuencias de 30 KHz y 5.8 Ghz

Onda continua.- es aquella que no tiene variación de amplitud con el tiempo, una de las ventajas en las comunicaciones es que este tipo de onda no tiene embebida ninguna información pero puede ser modulada con el objetivo de transmitir una señal.

Modulación.- es el proceso de colocar la información contenida en una señal generalmente de baja frecuencia sobre una señal de alta frecuencia.
La señal de alta frecuencia denominada portadora, sufrirá la modificación de alguno de sus parámetros, siendo dicha modificación proporcional a la amplitud de la señal de baja frecuencia denominada moduladora. La señal resultante de este proceso se denomina señal modulada y la misma es la señal que se transmite.

2.1.2 PROPIEDADES DE RF.

"Una señal de radio frecuencia (RF) puede ser afectada por el material a través del cual se propaga. Cuando parte de la señal se topa con un obstáculo parte de su energía se absorbe y se convierte en otro tipo de energía". [22] En base al comportamiento de las señales frente al choque con cierto material se tienen las siguientes propiedades.
RF-Lucent.- Es aquel material que a una cierta frecuencia permite el paso de las señales de RF sin que exista una pérdida sustancial de energía.
RF-Opaque.- Aquel material que a una cierta frecuencia bloquea, refleja, y esparce las señales de RF,

[22] http://wireless.itworld.com/4985/051004_book_rfidsourcebook/page_1.html

RF-Absorbent.- Permite el paso de las señales a través de él pero con una pérdida sustancial de energía.

La propiedad RF-Absorbent o RF-Opaque de un material son relativas, ya que dependen de la frecuencia de operación. Es decir, un material puede ser RF-Opaque en una cierta frecuencia y podría ser RF-Absorbent en otra frecuencia diferente.

En la tabla 2.1 se proporcionan las propiedades de RF de ciertos materiales.

Material	LF	HF	UHF	Microondas
Ropa	RF-lucent	RF-lucent	RF-lucent	RF-lucent
Madera seca	RF-lucent	RF-lucent	RF-lucent	RF-absorbent
Grafito	RF-lucent	RF-lucent	RF-opaque	RF-opaque
Líquidos (Algunos tipos)	RF-lucent	RF-lucent	RF-absorbent	RF-absorbent
Metales	RF-lucent	RF-lucent	RF-opaque	RF-opaque
Aceite de Motor	RF-lucent	RF-lucent	RF-lucent	RF-lucent
Productos de papel	RF-lucent	RF-lucent	RF-lucent	RF-lucent
Plásticos	RF-lucent	RF-lucent	RF-lucent	RF-lucent (Algunos tipos)
Shampoo	RF-lucent	RF-lucent	RF-absorbent	RF-absorbent
Agua	RF-lucent	RF-lucent	RF-absorbent	RF-absorbent
Madera mojada	RF-lucent	RF-lucent	RF-absorbent	RF-absorbent

Tabla 2.1 Propiedades de RF de algunos materiales

Una vez revisados los conocimientos básicos de RF se procederá a analizar cómo trabaja la tecnología RFID.

Un dispositivo de radio llamado etiqueta se adjunta al objeto que necesita ser identificado. Los datos de identificación del portador son almacenados en la etiqueta. Cuando un objeto que lleva esta etiqueta es interrogado por un lector de RFID adecuado, la etiqueta transmite los datos contenidos en la etiqueta al lector (vía la antena del lector). El lector lee los datos y está en la capacidad de reenviar estos datos utilizando los canales de comunicación adecuados en una red o una conexión serial, a una aplicación de software que corre en un computador central. Esta aplicación se encarga de validar los datos para identificar el objeto presentado al lector. Luego se puede llevar a cabo una serie de acciones como por ejemplo la actualización y ubicación de este objeto en la base de datos, envío

de una alerta al personal de planta, o ignorar completamente el objeto (si se produjo una lectura doble).

Como se puede ver en esta descripción, RFID también es una tecnología de colección de datos. Sin embargo, esta tecnología tiene algunas únicas características que les permiten a los usuarios aplicarla en áreas que van más allá del alcance de las tecnologías tradicionales de colección de datos como es el código de barras.

Una aplicación de RFID es implementada por un medio de un sistema RFID, el cual constituye una completa tecnología extremo a extremo.

2.2 SISTEMA RFID.

Un sistema RFID es una colección integrada de componentes que implementan una solución de RFID.

El sistema RFID está formado de los siguientes componentes:

- **Etiqueta.-** Éste es un componente obligatorio de cualquier sistema RFID.
- **Lector.-** Éste también es un componente obligatorio.
- **Antena del lector.-** Éste es otro componente obligatorio. Actualmente algunos lectores tienen las antenas incorporadas
- **Controladora.-** Éste es un componente obligatorio. Sin embargo, la mayoría de los lectores de la nueva generación tienen este componente incluido en ellos.
- **Sensor, actor y anunciador.-** Estos componentes opcionales se necesitan para la entrada y salida externa del sistema.
- **Host y Sistema de software.-** Teóricamente, un sistema RFID puede funcionar independientemente sin este componente. Prácticamente, un sistema RFID pierde su valor sin este componente.

- **Infraestructura de Comunicación.-** Componente obligatorio, es la asociación de una red alámbrica e inalámbrica y una infraestructura de comunicación serial la cual se usa para conectar los componentes previamente listados para tener una comunicación efectiva entre sí.

La figura 2.2 muestra un diagrama esquemático del sistema RFID y en la figura 2.3 se muestra una instancia de este esquema con un ejemplo de sus componentes.

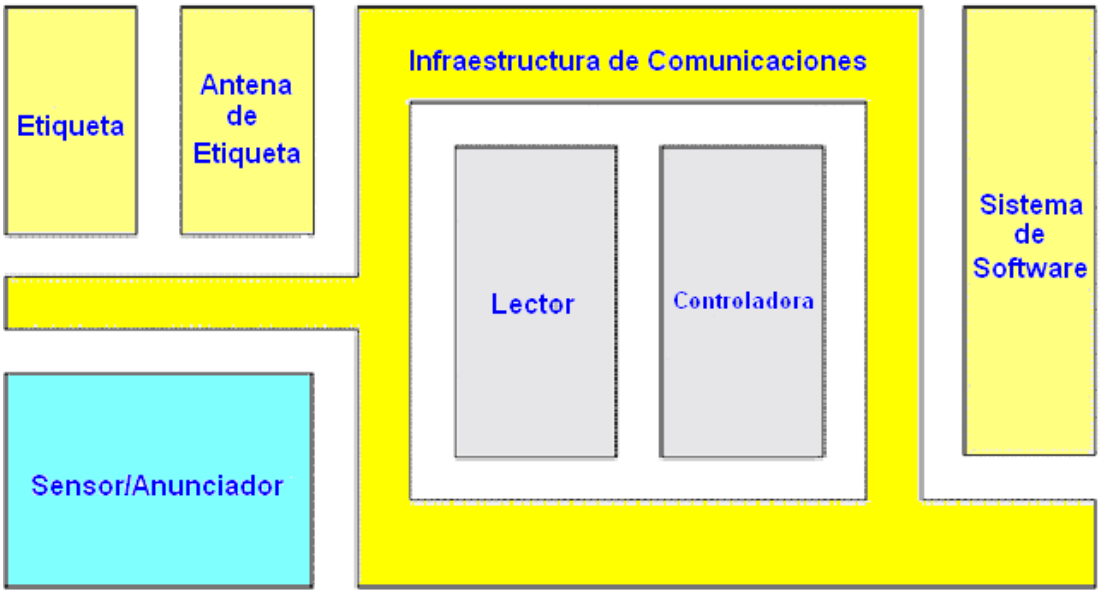


Figura 2.2 Diagrama esquemático de un sistema RFID

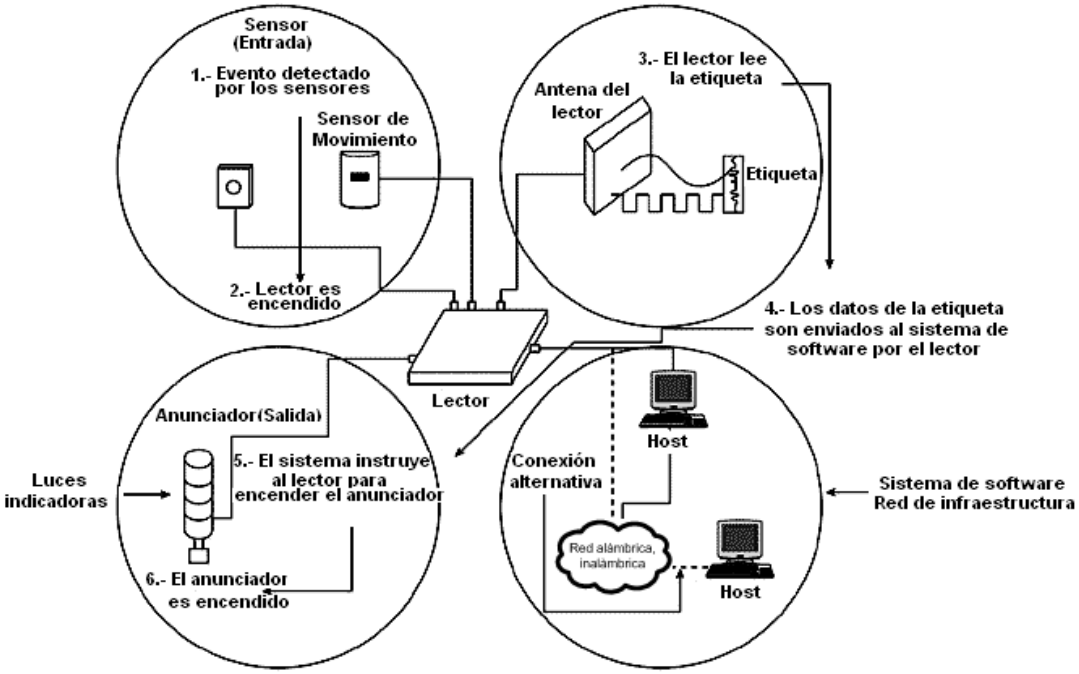


Figura 2.3 Ejemplo de componentes de un sistema RFID[23]

En estas figuras se puede apreciar al lector como un elemento central de todo el sistema ya que este elemento viene a ser el dispositivo que integra el segmento de hardware y software de un sistema RFID.

En la siguiente figura se muestra otra perspectiva del sistema RFID.

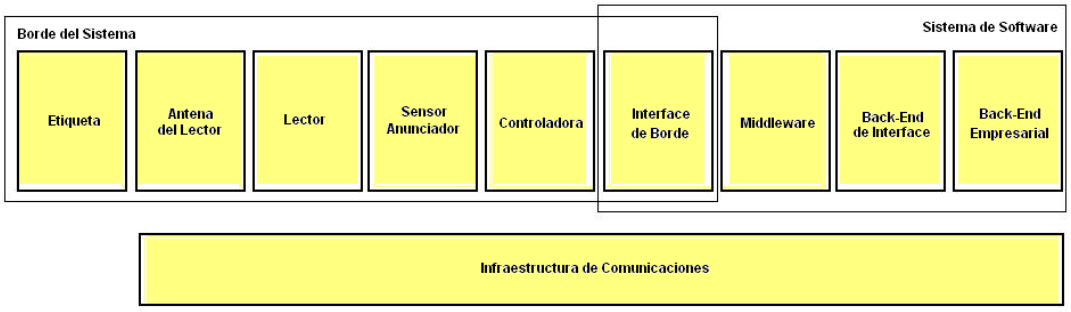


Figura 2.4 Sistema RFID desde la perspectiva de IT

[23] http://wireless.itworld.com/4985/051004_book_rfidsourcebook/page_1.html

En la Figura 2.4 se puede apreciar que el lector junto con la antena y la etiqueta están localizados al borde del sistema. Esta figura podría interpretarse como sistema RFID visto desde la perspectiva de un integrador de IT.

Un sistema RFID tiene dos partes la primera el borde del sistema el cual está gobernado por las capas físicas y la segunda parte aquella que involucra las tecnologías de información (IT). Las dos partes son primordiales en el sistema RFID ya que por ejemplo al ponerlo en marcha sin un sistema de IT, se pierde la capacidad de tener un sistema inteligente que administre y procese los datos que se generan en el sistema RFID.

A continuación se discuten a detalle cada uno de los componentes del sistema RFID.

2.3 ETIQUETAS Y LECTORES RFID

"Una etiqueta RFID es un dispositivo que puede almacenar y transmitir datos a un lector por medio de ondas de radio." [24]

Las etiquetas RFID se las clasifica de la siguiente manera:

- Pasivas
- Activas
- Semi-activas (También conocidas como el semi-pasivas)

2.3.1 ETIQUETAS PASIVAS

Este tipo de etiquetas no tienen una fuente de energía incorporada, y para su funcionamiento utilizan la energía que es proporcionada por el lector para transmitir los datos almacenados hacia el lector. Una etiqueta pasiva tiene un largo período de vida y es generalmente resistente a las condiciones

[24] LAHIRI Sandip; RFID Sourcebook; IBM Fress Books, EE.UU. 2006, Pág. 9

medioambientales. Por ejemplo, algunas etiquetas pasivas pueden resistir los químicos corrosivos como el ácido y temperaturas de hasta 204℃, etc.

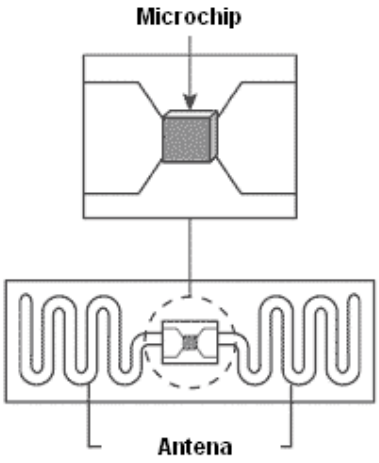


Figura 2.5 Componentes de una etiqueta pasiva.[25]

En este tipo de etiquetas para la comunicación el lector siempre se comunica primero seguido de la etiqueta. Una etiqueta pasiva es típicamente más pequeña que una etiqueta activa o semi-activa. Tiene una variedad de rangos de lectura que van desde 1 pulgada hasta aproximadamente 9 metros. Generalmente son más baratas en comparación a una etiqueta activa o semi-activa.

Una tarjeta inteligente sin contacto es un tipo especial de etiqueta pasiva que actualmente se usa en varias áreas. Los datos en esta tarjeta se leen cuando se está en una proximidad íntima con el lector.

Una etiqueta pasiva está formada de los siguientes elementos:

- Microchip
- Antena

2.3.1.1 Microchip

[25] http://wireless.itworld.com/4985/051004_book_rfidsourcebook/page_1.html

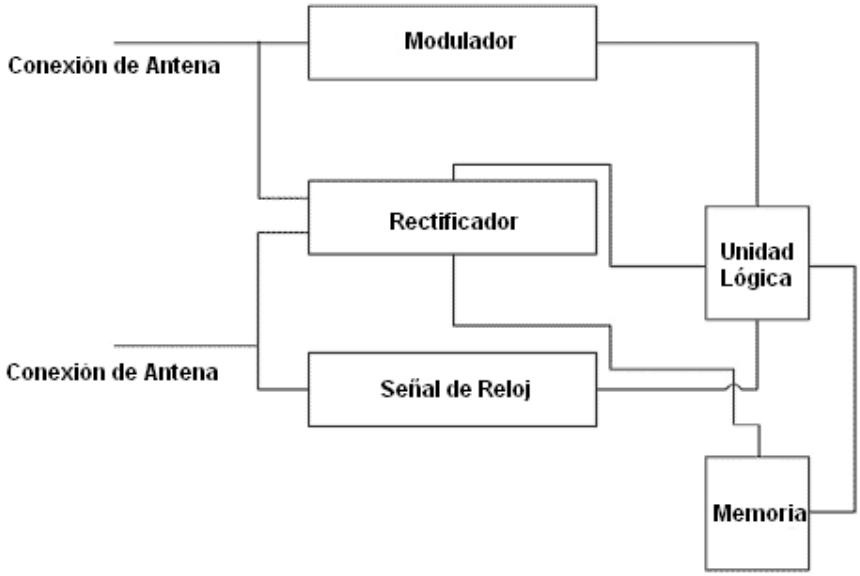


Figura 2.6 Componentes básicos de un microchip

Un microchip está formado por los componentes mostrados en la Figura 2.6, dichos componentes se los describe a continuación.

El rectificador convierte la señal de AC de la antena del lector a una señal de DC y a su vez provee de energía a los otros componentes del microchip. La señal de reloj es extraída de la señal que llega a la antena. El modulador demodula la señal recibida del lector y modula la señal que se transmite al lector. Los datos de la etiqueta son incluidos en la señal modulada que se transmite al lector. La unidad lógica se encarga de la implementación del protocolo de comunicación entre la etiqueta y el lector. La memoria del microchip se usa por guardar los datos, puede ser de lectura o escritura, esta memoria puede almacenar diferentes tipos de datos como los datos de identificación del objeto etiquetado, checksum que es una forma de control de redundancia. Lo recientes avances de la tecnología permiten tener tamaños del microchip hasta de un grano de arena. Sin embargo, las dimensiones físicas de la etiqueta no vienen determinadas por el tamaño del microchip sino más bien por el tamaño de su antena.

2.3.1.2 Antena

La antena de la etiqueta es utilizada para captar la energía que es enviada por el lector así como también para enviar y recibir los datos desde el lector. Esta antena está físicamente unida al microchip. La longitud de la antena es directamente proporcional a la longitud de onda a la cual opera la etiqueta.

Existen diferentes tipos de antenas diseñadas para UHF y especialmente para etiquetas RFID, entre los principales tipos tenemos:

Dipolo.- "Consiste en un hilo conductor de media longitud de onda a la frecuencia de trabajo, cortado por la mitad, en cuyo centro se coloca un generador o una línea de transmisión tal como se muestra en la figura 2.7. Dado que el generador actúa como si solamente empujara los electrones de un lado a otro, la longitud total de una antena dipolo es la mitad de la longitud de onda a la frecuencia de trabajo." [26]

Dipolo dual.- Consiste en dos dipolos los cuales pueden reducir en un buen grado la sensibilidad de alineación de la etiqueta frente al lector. Como resultado el lector puede leer las etiquetas en diferentes orientaciones.

Dipolo Doblado.- Consiste en dos o más conductores eléctricos rectos conectados en paralelo. Cuando dos conductores están conectados en paralelo, el resultando es un dipolo doblado de 2 hilos. Si tres conductores están conectados en paralelo, el resultando es un dipolo doblado de 3 hilos.

---

[26] LAHIRI Sandip; RFID Sourcebook; IBM Fress Books, EE.UU. 2006, Pág.11

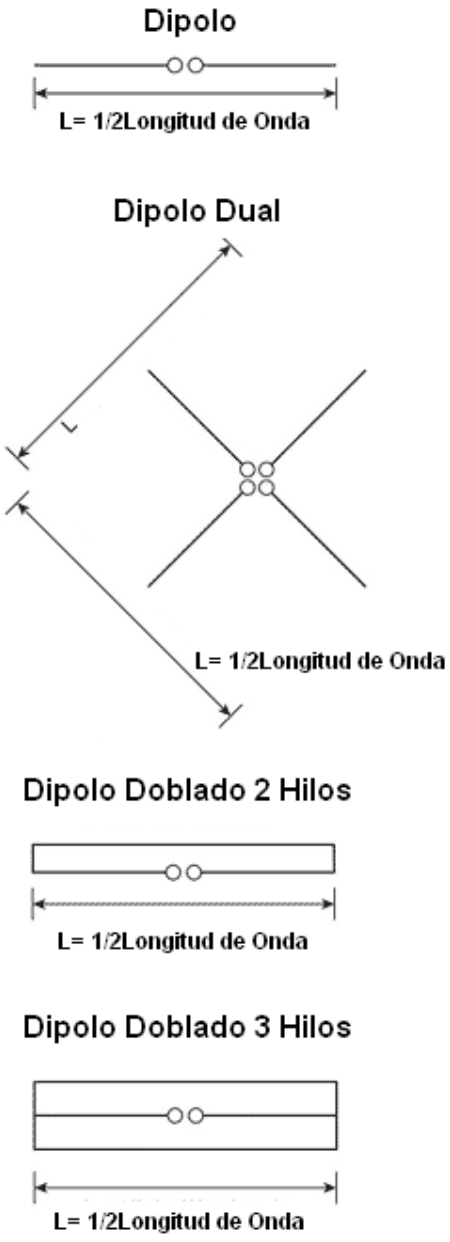


Figura 2.7 Tipos de antena dipolo[27]

La longitud de la antena de las etiquetas por lo general es mucho más grande que el microchip de la etiqueta y en base al tamaño de estos elementos se puede determinar las dimensiones físicas de la antena. Una antena puede ser diseñada en base a varios factores como los siguientes:

[27] http://wireless.itworld.com/4985/051004_book_rfidsourcebook/page_1.html

- La distancia de lectura de la etiqueta al lector
- Orientación conocida de la etiqueta al lector
- Orientación arbitraria de la etiqueta al lector
- El tipo de producto
- La velocidad de paso de la etiqueta por el lector
- Condiciones de operación específicas
- Polarización de la antena del lector

La conexión entre el microchip y la antena de la etiqueta es el punto más débil, si alguna de las conexiones en este punto son averiadas, la etiqueta puede volverse no funcional o a su vez podría tener un rendimiento degradado. Cambiar la geometría de la antena aleatoriamente no es buena idea ya que esto puede terminar en un mal funcionamiento de la misma y por ende tener una transmisión errónea de los datos

Actualmente la antena de la etiqueta se construye con una tira delgada de metal; éste puede ser cobre, plata o aluminio. Sin embargo en el futuro será posible imprimir las antenas directamente en la etiqueta, y en el empaquetado del producto para lo cual se usa una tinta conductiva que contiene cobre, carbono, o níquel. La meta también es determinar si el microchip podría imprimirse con tal tinta. Estas mejoras futuras permitirán que se imprima una etiqueta RFID con la facilidad que se imprime un código de barras. Como resultado de estos avances, el costo de una etiqueta RFID bajaría significativamente con precios bajo los $0.05. Incluso si el microchip no se puede imprimir, una antena impresa podría unirse al microchip para crear una etiqueta RFID completa y más rápido que atando una antena de metal.

En las siguientes figuras se muestran algunos ejemplos de etiquetas pasivas.

Figura 2.8 Etiquetas pasivas de LF

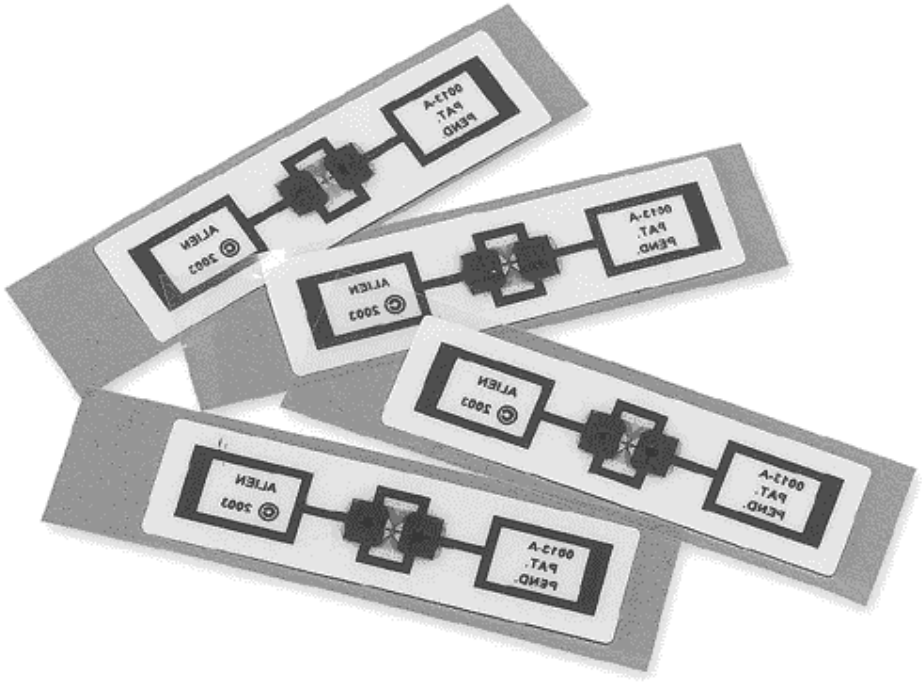


Figura 2.9 Etiquetas de 2.45 GHz[28]

[28] http://wireless.itworld.com/4985/051004_book_rfidsourcebook/page_1.html

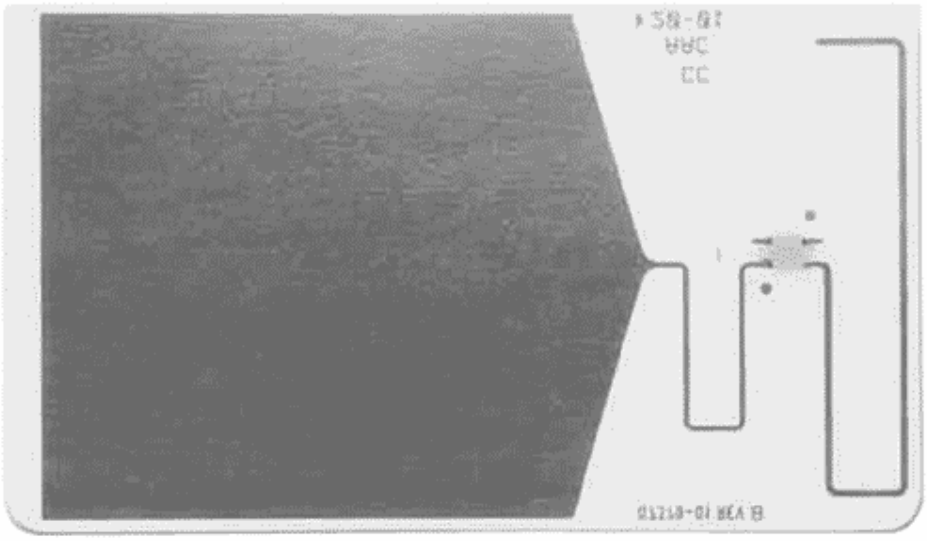


Figura 2.10 Etiquetas de 915 MHz[29]

2.3.2 ETIQUETAS ACTIVAS

Las etiquetas activas tienen incluida una fuente de poder por ejemplo una batería. Una etiqueta activa usa su fuente poder para poder transmitir sus datos al lector y no necesita que el lector emita una señal de poder para la transmisión de datos.

La electrónica a bordo de la etiqueta puede contener microprocesadores, sensores y puertos E/S, todos alimentados por la fuente de poder a bordo. Por ejemplo estos componentes pueden medir la temperatura del medio y pueden generar un promedio de los datos de temperatura. Los componentes pueden usar luego estos datos para determinar otros parámetros como la fecha de vencimiento del artículo etiquetado, etc. para que luego la etiqueta transmita esta información al lector.

En la comunicación etiqueta-lector para este tipo de etiqueta, la etiqueta siempre se comunica primero, seguido por el lector. Debido a que la presencia del lector

[29] http://wireless.itworld.com/4985/051004_book_rfidsourcebook/page_1.html

no es necesaria para la transmisión de datos, una etiqueta activa puede difundir sus datos incluso en ausencia del lector. A este tipo de etiqueta activa que continuamente transmite datos con o sin la presencia de un lector también se la llama *transmisor.* Ciertos tipos de etiquetas activas entran en un estado de reposo o consumo de baja potencia en ausencia de interrogación del lector. Para sacar del estado de reposo a una etiqueta el lector envía un comando apropiado. Este estado de la etiqueta permite el ahorro de energía, y por lo tanto, una etiqueta de este tipo generalmente tiene un tiempo de vida mayor que la etiqueta denominada transmisor. Además, esta etiqueta permite reducir la cantidad de ruido generado en su ambiente ya que emite señales de RF solo cuando el lector así lo requiere a este tipo de etiquetas se las conoce con el nombre *transponder*. De esto se puede concluir que no a todas las etiquetas se las puede llamar con precisión transponder ya que esto depende de su forma de operación.

La distancia de lectura de una etiqueta activa puede ser de 100 pies (30.5 metros aproximadamente). Una etiqueta activa está formada por los siguientes elementos:

- **Microchip.-** El tamaño del microprocesador y sus capacidades son generalmente mayores que los microchips de las etiquetas pasivas.
- **Antena.-** Esta puede estar en la placa del módulo de RF y puede transmitir señales de la etiqueta y recibir señales de respuesta del lector. Para una etiqueta semi-activa, la antena está compuesta de una delgada tira de metal que puede ser de cobre, similar al de una etiqueta pasiva.
- **Fuente de poder.-** Este componente se lo describe en la sección 2.3.2.1
- **Electrónica.** Este componente se lo describe en la sección 2.3.2.2

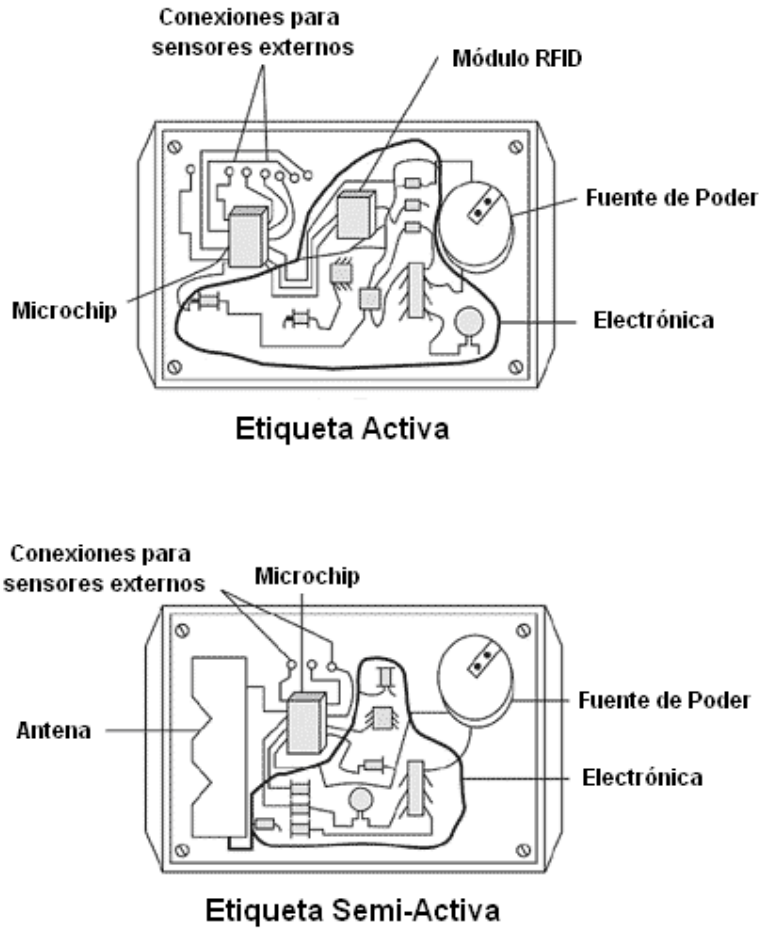


Figura 2.11 Etiqueta activa y semi-activa[30]

Los dos primeros componentes ya fueron descritos en la anterior sección, los últimos dos componentes se los describe a continuación

2.3.2.1 Fuente de Poder

Toda etiqueta activa lleva una fuente de alimentación a bordo (por ejemplo, una batería) para proporcionar energía a su electrónica a bordo. Una batería que es usada en una etiqueta activa generalmente tiene un tiempo de vida de aproximadamente 2 a 7 años. Uno de los factores determinantes en la duración de una batería es con qué frecuencia se trasmite los datos es decir mientras más grande sea el intervalo de tiempo que existe entre una transmisión y otra, mayor

[30] http://wireless.itworld.com/4985/051004_book_rfidsourcebook/page_1.html

será el tiempo de vida de la batería. Los procesadores y los sensores a bordo también consumen energía y pueden acortar el tiempo de vida de batería.

“Cuando la batería de una etiqueta activa está completamente descargada, la etiqueta deja de transmitir los mensajes. Un lector que estaba leyendo estos mensajes no sabe si la batería de la etiqueta se ha agotado o si el producto etiquetado ha salido de su zona de cobertura a menos que la etiqueta transmita el estado de la batería al lector.” [31]

2.3.2.2 Electrónica

La electrónica permite a la etiqueta actuar como un transmisor, y adicionalmente le permite realizar tareas especializadas como: cómputo, mostrar valores de ciertos parámetros dinámicos, actuar como un sensor, etc. Este componente también puede proveer la opción de conexión para sensores externos. Por lo tanto, dependiendo del tipo de sensor conectado, una etiqueta puede realizar una variedad de tareas. En otros términos, el rango de funcionalidad de este componente es casi ilimitado. Hay que notar que la funcionalidad crece con el tamaño físico de la etiqueta. Este crecimiento es aceptable ya que no existen limitantes físicos que afecten el tamaño de las etiquetas activas con tal que puedan plegarse al objeto que va a ser etiquetado.

2.3.3 ETIQUETAS SEMI-ACTIVAS (SEMI-PASIVAS)

Las etiquetas Semi-activas tienen una fuente de poder a bordo y la electrónica respectiva para realizar tareas especializadas. La fuente de alimentación provee de energía a la etiqueta para su funcionamiento. Sin embargo, por transmitir sus datos, una etiqueta semi-activa usa la energía transmitida por el lector. En la comunicación del lector con la etiqueta, el lector siempre se comunica primero, seguido de la etiqueta. El objetivo de utilizar una etiqueta semi-activa en lugar de un etiqueta pasiva es debido a que una etiqueta semi-activa no usa la señal del lector para su excitación a diferencia de la etiqueta pasiva que si usa dicha señal,

---

[31] LAHIRI Sandip; RFID Sourcebook; IBM Fress Books, EE.UU. 2006, Pág.16

además estas etiquetas pueden ser leídas a una gran distancia en comparación de las etiquetas pasivas, al igual que cuando un objeto etiquetado está desplazándose una alta velocidad los datos de la etiqueta pueden leerse sin problema. Finalmente, una etiqueta semi-activa ofrece una buena legibilidad para etiquetar materiales del tipo RF-opaco y RF-absorbente. La presencia de estos materiales podría impedir la lectura de los datos en una etiqueta pasiva. Sin embargo, éste no es el caso en una etiqueta semi-activa.

"La distancia de lectura de una etiqueta semi-activa puede ser 100 pies (30.5 metros aproximadamente) bajo condiciones ideales." [32] En la figura 2.12 se muestran algunos ejemplos de etiquetas activas y semi-activas de varios fabricantes.

Figura 2.12 Etiquetas Activas y Semi-Activas[33]

[32] LAHIRI Sandip; RFID Sourcebook; IBM Fress Books, EE.UU. 2006, Pág.17

[33] http://wireless.itworld.com/4985/051004_book_rfidsourcebook/page_1.html

La próxima clasificación está basada en la capacidad de soporte para lectura y escritura de datos.

- Solo lectura (RO)
- Una sola escritura, muchas lecturas (WORM)
- Lectura Escritura (RW)

Las etiquetas activas y pasivas pueden ser RO, WORM y RW. Las siguientes secciones describen esta clasificación

2.3.4 SÓLO LECTURA (RO)

Una etiqueta RO puede ser programada una sola vez. Los datos pueden quemarse en la etiqueta en la fábrica durante la fase industrial. Para lograr esto, se queman los fusibles individuales en el microchip de la etiqueta usando rayos láser. Luego de esto no se pueden volver a escribir más datos en la etiqueta. El fabricante de la etiqueta proporciona los datos de la etiqueta. Este tipo de etiqueta sólo es bueno para las aplicaciones pequeñas, pero es impráctico cuando la etiqueta necesita ser personalizada basados en la aplicación que se maneje.

2.3.5 UNA SOLA ESCRITURA, MUCHAS LECTURAS (WORM)

Una etiqueta WORM puede programarse o escribirse una sola vez generalmente no se lo hace por el fabricante sino ya por el usuario de la etiqueta el momento que necesita ser creada. En la práctica, sin embargo, es posible sobrescribir ciertas etiquetas WORM (aproximadamente 100 veces). Si los datos se vuelven a escribir más de un cierto número de veces, la etiqueta puede dañarse permanentemente.

Estas etiquetas en la actualidad son ampliamente usadas en el sector de negocios, proveen un razonable nivel de seguridad y menor precio por etiqueta.

2.3.6 LECTURA ESCRITURA (RW)

Una etiqueta RW puede reprogramarse o puede volverse a escribir un número grande de veces. Típicamente, este número varía entre 10,000 y 100,000 veces.

Esta posibilidad de sobrescribir ofrece una tremenda ventaja porque los datos o pueden escribirse por los lectores o por la propia etiqueta (en el caso de las etiquetas activas). Una etiqueta RW contiene una memoria flash o FRAM para almacenar sus datos. La seguridad de datos es un desafío para las etiquetas RW. Además, este tipo de etiquetas son muy caras. No se usan etiquetas RW ampliamente en las aplicaciones actuales, hecho que podría cambiar en el futuro con el crecimiento de la tecnología y decrecimiento de los costos.

Antes de continuar con el próximo tema es importante describir un tipo de etiqueta RFID llamado etiqueta de superficie de onda acústica (SAW).

2.3.7 ETIQUETA DE SUPERFICIE DE ONDA ACÚSTICA (SAW)

Una etiqueta SAW difiere fundamentalmente de las etiquetas basadas en el microchip. Los dispositivos SAW son ampliamente utilizados en teléfonos celulares, televisiones a color, entre otros.

Usan señales de RF de baja potencia cuya frecuencia de operación está en la banda de los 2.45 GHz. Al contrario de una etiqueta basada en microchip una etiqueta SAW no necesita una fuente de DC para la transmisión de datos.

Estas etiquetas están formadas por una antena dipolo ligada a un transductor interdigital (IDT) situado en una superficie piezoeléctrica. Una serie de electrodos individuales bien situados que actúan como reflectores también están en esta superficie. La antena aplica un impulso eléctrico al IDT cuando recibe una señal del lector. Este impulso genera unas ondas de superficie (Raleigh waves) algunas de las cuales son reflejadas por los reflectores haciendo un patrón único que representa la información de la etiqueta.

Las principales ventajas de los SAW son: Utilizan muy poca energía, mayor rango de lectura (por ser a 2,45GHz), trabajan con ráfagas cortas de señales lo que los hace más rápidos a la lectura, son de muy fácil diseño y no necesitan implementar protocolos de colisión.

2.3.8 ETIQUETAS NO RFID

Es destacable el hecho de que la comunicación inalámbrica no sólo se puede realizar por medio de ondas electromagnéticas, existen tags que se comunican mediante ultrasonidos. O con otro rango de frecuencias como los infrarrojos.

2.3.9 LECTORES RFID

Un lector RFID, también es conocido como un *interrogador*, es un dispositivo que puede leer y escribir datos en las etiquetas RFID que sean compatibles. El tiempo durante el cual el lector puede emitir energía de RF para leer las etiquetas se denomina ciclo de lectura del lector.

El lector emite ondas electromagnéticas o de radio frecuencia dirigidas a la antena de la etiqueta, en el caso de la etiqueta pasiva, la energía de esas ondas activa el circuito integrado de la etiqueta que contiene la información que se desea leer y ésta es enviada de regreso al lector a través de la antena de la etiqueta, también por medio de ondas de radio frecuencia, esto ocurre de forma tal que esta información puede luego ser convertida a formato digital y procesada por una computadora.

Básicamente tienen la habilidad de localizar, identificar o rastrear objetos. Los lectores no tienen las restricciones de "línea de lectura" que tienen los lectores de código de barras. Pueden leer simultáneamente varias etiquetas (hasta 200 por segundo) o focalizar la lectura en una sola etiqueta en particular.

"La máxima distancia a la que puede establecerse la comunicación entre el lector y la etiqueta depende de la potencia del lector y de la frecuencia de se utiliza para la comunicación entre el lector y la etiqueta." [34]

Un lector tiene principalmente los siguientes elementos:

- Transmisor

[34] LAHIRI Sandip; RFID Sourcebook; IBM Fress Books, EE.UU. 2006, Pág. 22

- Receptor
- Microprocesador
- Memoria
- Canales de Input/Output para sensores externos, actuadores y anunciadores (Aunque, hablando estrictamente, éstos son componentes optativos, que se proporcionan casi siempre un lector comercial.)
- Controladora(La cual puede residir como un componente externo)
- Interfaz de comunicación
- Fuente de poder

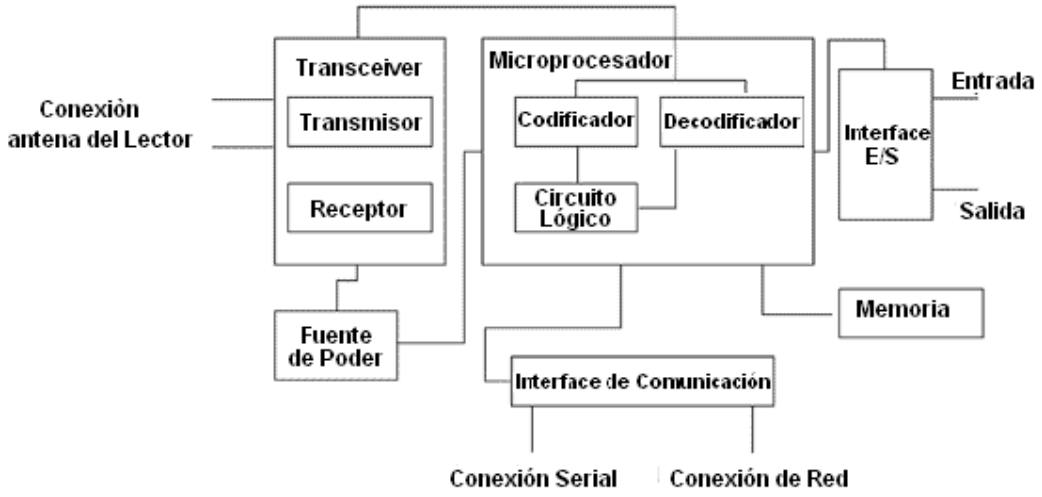


Figura 2.13 Componentes de un lector

2.3.9.1 Transmisor

El transmisor se utiliza para transmitir energía de AC y la señal de reloj por medio de sus antenas a las etiquetas que se encuentran en su zona de lectura. Este elemento forma parte del transceiver, a su vez es el responsable de enviar al lector las señales del ambiente cercano y receptar las respuestas de la etiqueta

por medio de la antena del lector, dicha antena es conectada a los puertos del transceiver, actualmente un lector puede tener hasta cuatro antenas.

2.3.9.2 Receptor

Este componente también es parte del transceiver. Recibe las señales análogas de la etiqueta por medio de la antena del lector. Este luego envía estas señales al microprocesador dónde toda esta información se convierte a un formato digital.

2.3.9.3 Microprocesador

Este componente es responsable de la implementación del protocolo de comunicaciones entre el lector y la etiqueta, esto es realizar la decodificación y chequeo de errores en la transmisión. Además, el microprocesador puede contener la lógica personalizada para hacer un filtrado a bajo nivel y procesamiento de datos producto de la lectura de la etiqueta.

2.3.9.4 Memoria

La memoria es utilizada para almacenar datos como los parámetros de configuración del lector y la lista de lecturas de la etiqueta. Por consiguiente, si la conexión entre el lector y el sistema de control/software se pierde, no se leerán todas las etiquetas originándose una pérdida de datos. Dependiendo del tamaño de memoria, los límites de almacenamiento dependen de la cantidad de lecturas que la memoria puede almacenar en cualesquier instante de tiempo, existe un tiempo de tolerancia para una desconexión durante este tiempo el lector puede leer las etiquetas pero si se sobrepasa este tiempo los datos se pueden perder, ya que éstos se sobrescriben con los otros datos que se leen después.

2.3.9.5 Canales de Entrada/Salida para sensores externos, actuador y anunciador

Los lectores no tienen que ser encendidos para leer las etiquetas en todo momento. Después de todo, las etiquetas podrían aparecer sólo en ciertos momentos en la zona de lectura, dejando continuamente encendidos a los lectores gastarían su energía. Para lo cual es necesario implementar un mecanismo de encendido y apagado del lector dependiendo de los eventos

externos. La presencia de un sensor de cierto tipo, como de movimiento o de luz, descubre la presencia de objetos etiquetados en la zona de lectura y habilita al lector para la lectura de etiquetas. De igual manera, este componente también permite al lector proporcionar una salida local dependiendo del evento que se presente, vía un anunciador (por ejemplo activando una alarma de audio) o actuator (por ejemplo, abriendo o cerrando una puerta de seguridad o moviendo un brazo del robot).

2.3.9.6 Controladora

La controladora es una entidad que permite a una entidad externa, un humano o un programa de computación, comunicarse con el lector, también permite controlar el anunciador y actuador que están asociados al lector. A menudo, los fabricantes integran este componente en el propio lector. Sin embargo, también es posible empaquetar esto como un componente de hardware/software separado que debe comprarse junto con el lector.

2.3.9.7 Interfaz de comunicación

Proporciona las instrucciones de comunicación al lector que le permiten interactuar con entidades externas por medio de la controladora, para transferir los datos almacenados, receptar comandos y enviar las respuestas correspondientes. Por tal motivo se puede asumir que este componente es parte de la controladora y es el medio que se encuentra entre la controladora y las entidades externas. Tiene características importantes que hacen necesario tratarlo como un componente independiente. Un lector puede tener una interfaz serial o de red para la comunicación. Una interfaz serial es probablemente el tipo de interfaz más utilizado pero actualmente se están creando lectores que traen una interfaz de red como una característica común. Los lectores sofisticados ofrecen características especiales para interactuar con ciertas aplicaciones, por ejemplo tener un servidor Web incluido el cual permita al lector aceptar órdenes y desplegar los resultados por medio de un navegador Web normal.

2.3.9.8 Fuente de Poder

Este componente proporciona energía a los componentes del lector. La energía es suministrada a través de un cable que es conectado a una toma de corriente eléctrica externa apropiada.

Como las etiquetas, los lectores también pueden ser clasificados usando diferentes criterios. El primer criterio es la interfaz que el lector provee para la comunicación. Basado en esto, los lectores pueden ser clasificados de la siguiente manera:

- Lector Serial
- Lector de Red

Las siguientes subdivisiones describen estos tipos de lectores.

2.3.9.9 Lector Serial

Este tipo de lectores utilizan un enlace de comunicación serial para la comunicación con una aplicación. El lector se conecta físicamente al puerto serial de la computadora utilizando una conexión serial RS-232 o RS-485. Para cada una de las conexiones se tiene un límite en la longitud del cable que se puede utilizar para conectar el lector con el computador. Así, RS-485 permite una longitud del cable mayor que RS-232.

La ventaja de estos lectores es que su enlace de comunicación es confiable frente a los lectores de red. Por consiguiente, el uso de estos lectores es recomendable para minimizar la dependencia en un canal de comunicaciones.

Su desventaja es la dependencia en la longitud máxima de cable que puede utilizar para conectar un lector a un computador. Adicional a esto, el número de puertos seriales es limitado en un host, por lo que se puede necesitar de una mayor cantidad de hosts para conectar varios lectores de este tipo. Otro problema es el mantenimiento, si el firmware necesita ser actualizado el personal de mantenimiento podría tener que estar físicamente en cada lector para realizar

dicha actualización. También, la velocidad de transmisión de datos vía puerto serial es más baja que la transmisión por medio de interfaz de red. Estos factores podrían producir que los costos y el tiempo de mantenimiento suban.

2.3.9.10 Lector de Red

Los lectores de red pueden conectarse a un computador utilizando redes alámbricas e inalámbricas. En efecto, el lector se comporta como un dispositivo de red y su instalación no requiere un conocimiento especializado del hardware. Sin embargo, pocos son los lectores que traen consigo el protocolo SNMP. Por lo tanto, la mayoría de estos lectores no pueden ser administrados como los dispositivos de red normales.

La ventaja de este tipo de lectores es que no hay mucha dependencia en la longitud máxima de cable para conectar el lector con una computadora. Se necesita un número menor de hosts en comparación con los lectores seriales. Además, el firmware del lector puede ser actualizado remotamente sin necesidad de estar físicamente cerca del lector. Esto permite ahorrar el tiempo y recursos al momento de realizar el mantenimiento del lector.

La desventaja de los lectores de red es que sus enlaces de comunicación no son tan fiables como en los lectores seriales. Cuando se pierde el enlace de comunicación, el back end no puede acceder. Como resultado de esto, el sistema RFID podría venir a un colapso completo. Por lo general, los lectores tienen una memoria interna para almacenar la información de las etiquetas que han sido leídas. Esto podría aliviar cortas caídas de la red.

La siguiente clasificación de los lectores está basada en su movilidad, teniendo los siguientes tipos:

- Estacionario
- Portátil (Handheld)

Las siguientes subdivisiones describen a estos tipos de lectores.

2.3.9.11 Lector estacionario

Un lector estacionario, también es llamado lector fijo. Estos lectores están montados en una pared, portal, o alguna estructura conveniente en la zona de lectura. La estructura en la cual el lector está montado puede no ser estática por ejemplo, se puede montar a estos lectores dentro de los camiones de entrega. En contraste con las etiquetas, los lectores no son generalmente muy tolerantes a duras condiciones medioambientales. Por lo tanto, si se instala el lector en ambientes externos es recomendable proteger el elector de las amenazas del ambiente externo. Los lectores estacionarios generalmente necesitan antenas externas para leer las etiquetas. Un lector puede proporcionar hasta cuatro puertos para antenas externas.

El costo de un lector estacionario generalmente es más bajo que un lector portátil. Los lectores estacionarios son los más utilizados actualmente.

La figura 2.14 muestra unos ejemplos de lectores estacionarios.

Figura 2.14 Lectores estacionarios de UHF[35]

Un tipo de lector estacionario llamado impresora *RFID* puede imprimir el código de barras y crear una etiqueta RFID (proceso de escritura en la etiqueta) con una operación integrada. Una etiqueta inteligente está formada por un código de

[35] http://wireless.itworld.com/4985/051004_book_rfidsourcebook/page_1.html

barras y una etiqueta RFID, esta etiqueta contiene varios tipos de información como la información del remitente, información del producto, etc. Una impresora RFID una vez que imprime la etiqueta inteligente lee esta información con el objetivo de validar la operación, si la validación falla la impresora anula la etiqueta inteligente impresa. En la figura 2.15 se muestra un ejemplo de una etiqueta inteligente y una impresora RFID.

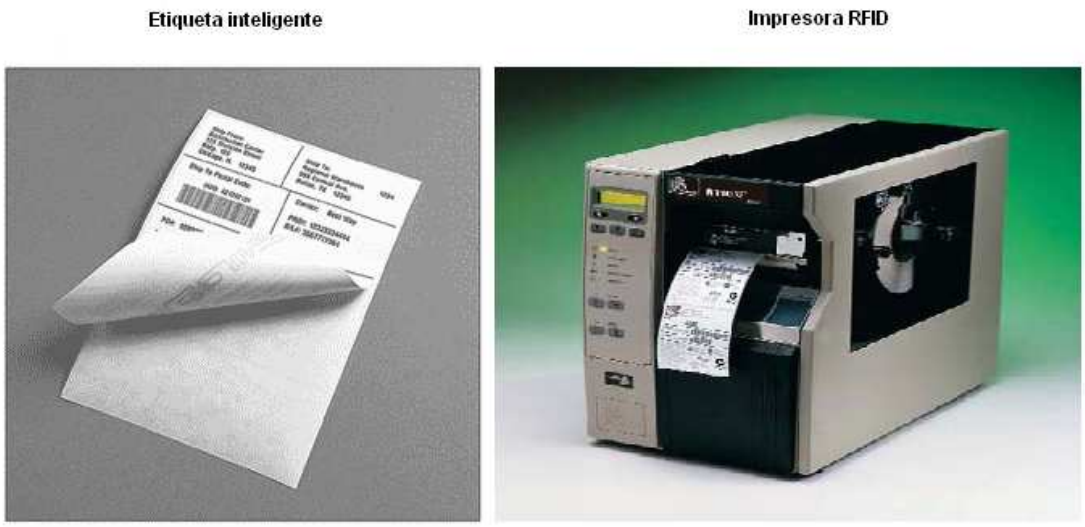


Figura 2.15 Etiqueta inteligente e impresora RFID[36]

Un lector estacionario puede generalmente opera en los siguientes modos:

- Autónomo
- Interactivo

Las siguientes subdivisiones describen estos modos.

2.3.9.11.1 Modo autónomo

En el modo autónomo, un lector lee continuamente las etiquetas que se encuentran en su zona de lectura. Cada vez que una etiqueta se lee se almacena en una lista, normalmente a ésta se la llama *lista de presencia.* Un artículo en la

[36] http://wireless.itworld.com/4985/051004_book_rfidsourcebook/page_1.html

lista de presencia está asociado con un tiempo de persistencia. Si una entrada expira se elimina de la tabla interna de datos. Una *lista de presencia* contiene información como la siguiente:

- Identificador único de etiqueta
- Tiempo de lectura
- Cuántas veces una etiqueta en particular ha sido leída desde que ha sido descubierta.
- La identificación de la antena que leyó una etiqueta en particular
- Nombre del lector

2.3.9.11.2 Modo interactivo

Los lectores que operan bajo esta modalidad responderán a los comandos proporcionados por las aplicaciones de gestión almacenadas en servidores. El servidor puede indicar al lector que reúna una lista de etiquetas dentro del rango de lectura o que busque una etiqueta específica. En ambos casos el lector comienza por recoger una lista. Una vez completado el comando instruido por el servidor, el lector espera hasta recibir el siguiente comando.

2.3.9.12 Lector portátil

Un lector portátil es un lector móvil que un usuario puede operar como una unidad portátil. Un lector portátil generalmente tiene las antenas incorporadas. Aunque estos lectores son típicamente los más caros, los recientes adelantos en la tecnología del lector están produciendo a los lectores portátiles sofisticados a los más bajo precios.

Figura 2.16 Lector Portátil de UHF [37]

La siguiente sección introduce los mecanismos de comunicación entre una etiqueta y un lector.

2.3.9.13 Comunicación Entre un Lector y una Etiqueta

Dependiendo del tipo de la etiqueta, la comunicación entre un lector y la etiqueta puede ser de los siguientes tipos:

- Modulación Backscatter
- Tipo Transmisor
- Tipo Transponder

La escritura de una etiqueta dura más tiempo que la lectura en las mismas condiciones ya que para la escritura se realizan varios pasos más incluyendo la lectura inicial, borrado de los datos existentes, escritura verificación final. Además de tener que hacer esto para cada bloque de memoria. Por ello la escritura de la etiqueta puede llevar cientos de milisegundos, mientras que se pueden leer muchas etiquetas en el mismo tiempo.

El proceso de escritura ha de hacerse con la etiqueta muy próxima a la antena del lector para poder asegurarse de que se deriva suficiente energía como para que el microchip pueda ejecutar las instrucciones de escritura. Y es que el proceso de escritura requiere generalmente mucho más nivel de corriente. No hay que olvidar

[37] http://wireless.itworld.com/4985/051004_book_rfidsourcebook/page_1.html

que durante el proceso de escritura no debe haber otra etiqueta cerca de la zona de escritura ya que podría modificarse accidentalmente. En cambio para el proceso de lectura no existen tantas restricciones y pueden estar bastante más lejos de la antena.

2.3.9.13.1 Modulación Backscatter

Este tipo de comunicación se emplea tanto para las etiquetas pasivas como para las semi-activas. En este proceso el lector envía una señal de RF continua que contiene corriente alterna y el reloj de la señal a la frecuencia en la que trabaja la etiqueta. La etiqueta obtiene la energía transformándola a corriente continua para alimentar los sistemas. Son alrededor de 1,2 Voltios los necesarios para hacer funcionar le microchip en modo lectura, mientras que para escribirlo se suelen utilizar 2,2 Voltios. El microchip modula o pausa la señal de entrada que representa los datos a transmitir al lector.

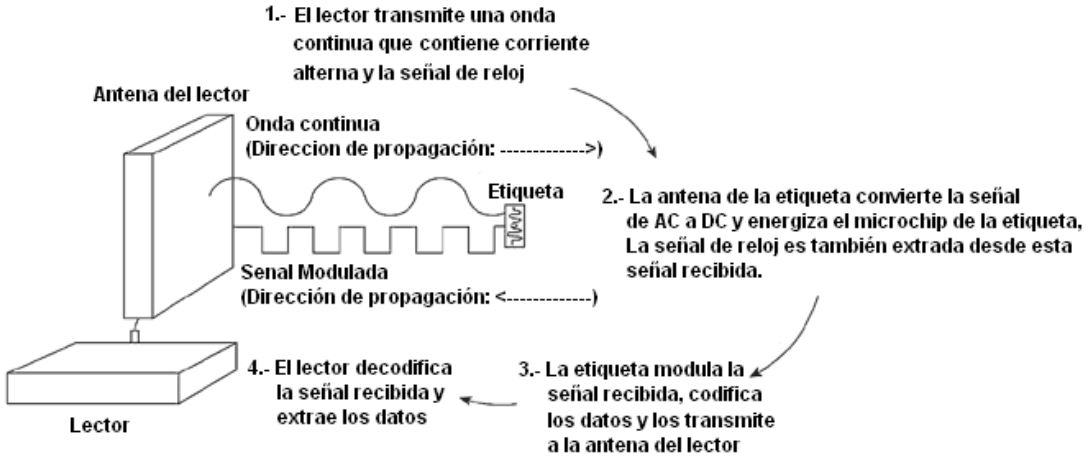


Figura 2.17 Comunicación Backscatter

2.3.9.13.2 Tipo Transmisor

Este tipo de comunicación se utiliza sólo para las etiquetas activas. La etiqueta emite su mensaje al entorno en intervalos regulares independientemente de la existencia o no de un lector.

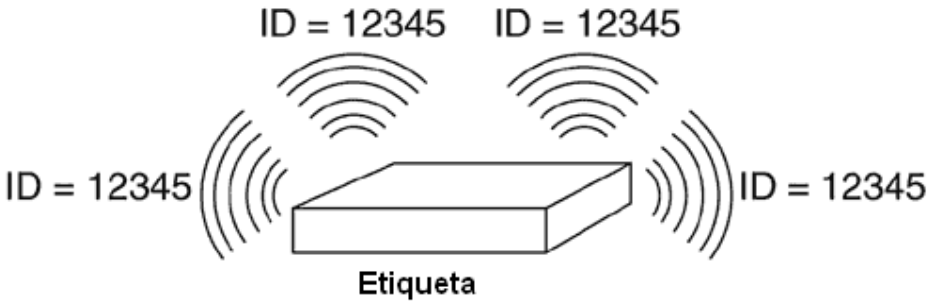


Figura 2.18 Comunicación tipo transmisor[38]

2.3.9.13.3 Tipo Transponder

Este tipo de comunicación sólo se usa para las etiquetas llamadas transponder. La etiqueta está en un estado de reposo cuando no recibe peticiones del lector. En este estado la etiqueta periódicamente envía un mensaje para consultar la existencia del lector. En este momento, el lector puede decidir responder con un "wake up" con lo que la etiqueta comienza a mandar su mensaje periódicamente.

2.3.9.14 Antena del lector

El lector se comunica con las etiquetas a través de la antena del lector, que suele estar separada físicamente del lector y conectada con ésta a través de un cable. La longitud del cable también está limitada y como se mencionó anteriormente un lector puede soportar varias antenas a la vez. La antena es la que crea el campo electromagnético que induce la corriente a la antena de la etiqueta. Por consiguiente para conseguir que se lea una etiqueta deberá estar próximo a la antena del lector. Hay algunos lectores que pueden llevar integrada la antena.

[38] http://wireless.itworld.com/4985/051004_book_rfidsourcebook/page_1.html

La figura 2.19 muestra unos ejemplos de antenas de un lector.

Figura 2.19 Antena UHF de un lector [39]

2.3.9.14.1 Antena footprint

Las huellas de la antena del lector determinan su zona de lectura, es una región tridimensional en forma de un elipsoide o un globo que se proyecta hacia afuera de la antena. En esta región, la energía de la antena es muy eficaz; por consiguiente, un lector puede leer una etiqueta que se encuentra dentro de esta región con la menor dificultad. La figura 2.20 muestra un ejemplo de una antena footprint simple.

[39] http://wireless.itworld.com/4985/051004_book_rfidsourcebook/page_1.html

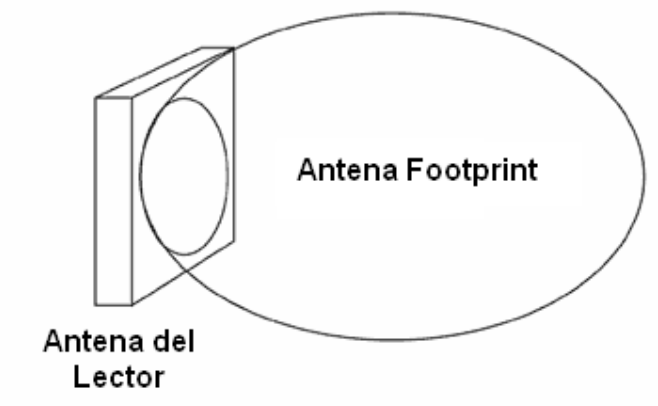


Figura 2.20 Antena Footprint simple [40]

En la realidad, debido a las características de la antena, la huella de una antena nunca se forma uniformemente como un elipsoide casi siempre contiene deformidades. Cada deformación rodea las zonas muertas. La figura 2.21 muestra un ejemplo de esta antena.

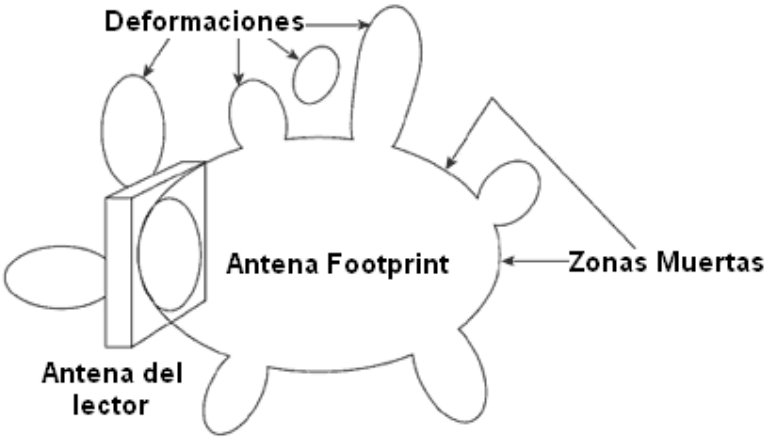


Figura 2.21 Antena Footprint con deformaciones[41]

Estas zonas muertas están debidas a interferencias destructivas a la hora de generar la señal, por tal motivo es muy importante hallar el rango de acción de la antena.

"La reflexión de la señal de la antena del lector en ciertos objetos causa el fenómeno conocido como *multipath.* En este caso, las ondas de RF reflejadas se

[40] http://wireless.itworld.com/4985/051004_book_rfidsourcebook/page_1.html
[41] http://wireless.itworld.com/4985/051004_book_rfidsourcebook/page_1.html

esparcen y pueden llegar a la antena del lector por diferentes caminos. Algunas de las ondas podrían llegar en fase." [42] En este caso, la señal original es mejorada y puede dar lugar a la aparición de perturbaciones en la señal, a este fenómeno se lo conoce como *interferencia constructiva.* Algunas ondas también podrían llegar fuera de fase. En este caso, la señal original es cancelada y por tal motivo se generan zonas muertas, a este fenómeno se lo denomina interferencia destructiva. En la figura 2.22 se muestra los ejemplos de multipath.

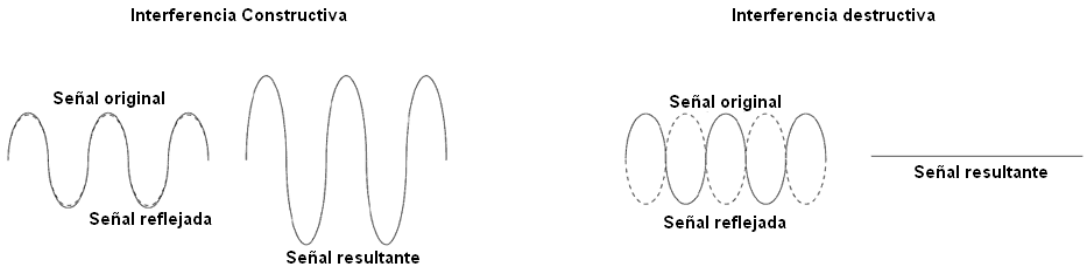


Figura 2.22 Esquema Multipath

Una etiqueta que es ubicada en la zona de deformación puede ser leída pero si ésta se mueve ligeramente puede ya no ser leída por el hecho de que ésta puede entrar en una zona muerta. Por consiguiente, cuando se pone una antena para cubrir una cierta área de lectura, es importante no depender de las zonas de deformación para aumentar al máximo la distancia de la lectura. La mejor estrategia es estar dentro de la región del elipsoide principal aún cuando esto signifique sacrificar el rango de lectura.

La polarización de la antena del lector es otro factor importante que se describe a continuación.

[42] LAHIRI Sandip; RFID Sourcebook; IBM Fress Books, EE.UU. 2006, Pág. 36

2.3.9.14.2 Polarización de la antena

"La polarización de la antena es la dirección de oscilación en la que son emitidas las ondas. Este aspecto es relevante en la robustez de lectura así como en el rango o alcance de lectura." [43]

Las principales antenas de UHF se encuentran polarizadas de la siguiente manera:

- Polarización lineal
- Polarización circular

Las siguientes subdivisiones describen estos dos tipos de polarización.

2.3.9.14.2.1Antena polarizada linealmente

Tienen más alcance que las antenas polarizadas circularmente pero es sensible a la orientación de la etiqueta con relación a la dirección de polarización. Sólo se usan cuando ya está predefinida y predicha la orientación de la etiqueta.

En la siguiente figura se muestra cómo deben estar orientadas las etiquetas para este tipo de antenas.

[43] http://www.rfid-handbook.de/rfid/types_of_rfid.html

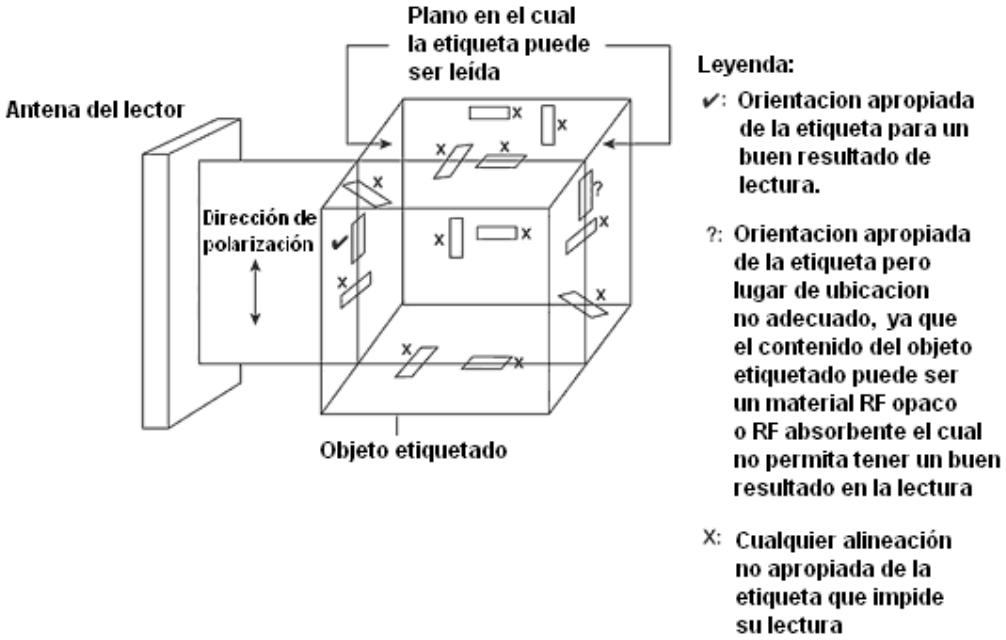


Figura 2.23 Consideraciones para orientación de una etiqueta con polarización lineal

2.3.9.14.2.2Antena polarizada circularmente

Utilizan un patrón de irradiación circular. Están constituidas por dos ondas de igual amplitud y magnitud pero con una diferencia de fase de 90º.

Al tener esta polarización la antena no se ve afectada por la orientación de la etiqueta y permite cubrir una mayor área.

Debido a su naturaleza de polarización, este tipo de antena es ideal para aplicaciones donde la orientación de la etiqueta es impredecible. Una antena polarizada circularmente tiene un área de lectura mayor que una antena polarizada linealmente. Esta antena es adecuada para un sistema RFID que usa UHF o frecuencia de microondas y en un ambiente dónde existe un alto grado de refracción de RF (debido a la presencia de metales). La siguiente figura muestra cómo debe orientarse una etiqueta con respecto a una antena polarizada circularmente para su lectura apropiada.

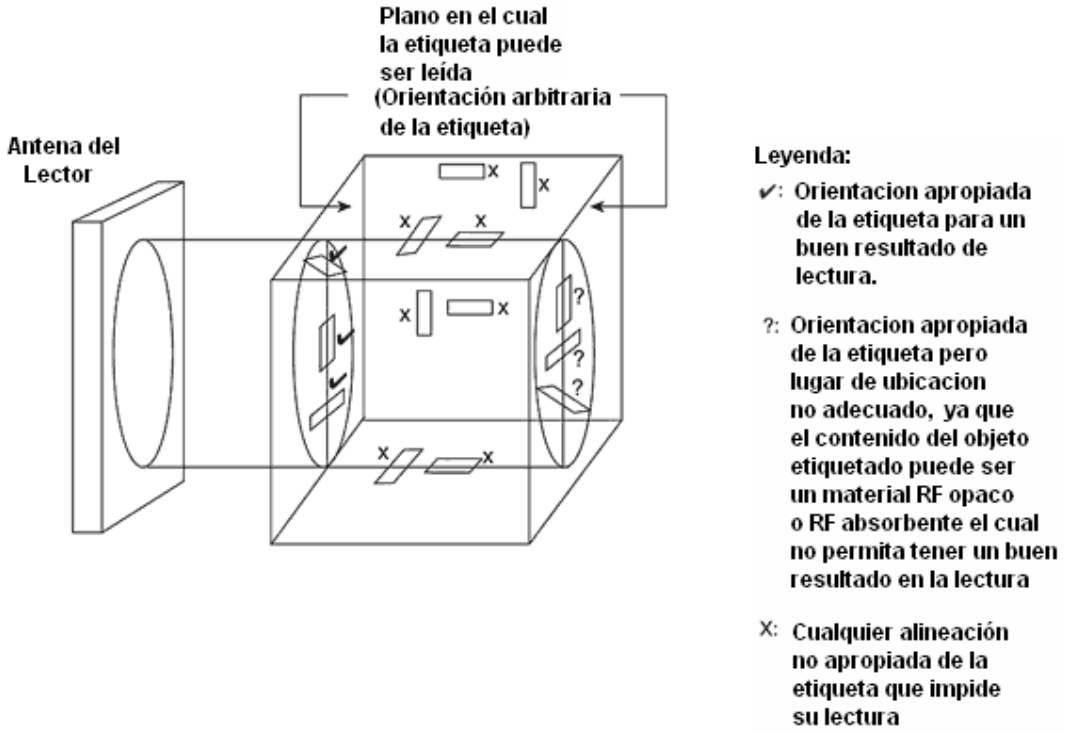


Figura 2.24 Consideraciones para orientación de una etiqueta con polarización circular

2.3.9.14.3 Potencia de la antena

La potencia que emite una antena se mide en ERP (effective radiated power) unidades en el sistema europeo o su equivalente EIRP (equivalent isotropic radiated power) en el sistema americano. ERP y EIRP no son similares pero están relacionadas por la siguiente relación EIRP=1.64 ERP, el máximo valor de potencia de una antena está limitado por las regulaciones nacionales e internacionales y para aumentar esta potencia es necesario solicitar permisos legales a las autoridades competentes. Se puede reducir la potencia de la antena con un atenuador en la línea de transmisión por ejemplo entre el conector de la antena y el puerto del lector. Utilizar un atenuador puede ser necesario si se necesita controlar solamente una pequeña zona para la lectura de etiquetas.

2.3.10 CONTROLADOR

El controlador es un agente intermedio que le permite comunicarse con una entidad externa y controlar el comportamiento del lector junto con los indicadores y los actuadores asociados con este lector. Un controlador es el único componente de un sistema RFID a través del cual las comunicaciones son posibles.

Un controlador también provee un interfaz de comunicación con las entidades externas para interactuar con él.

2.3.11 SENSOR, ANUNCIADOR Y ACTUADOR

Un lector no tiene por qué estar conectado todo el tiempo, puede ser encendido y apagado automáticamente si es necesario. Un sensor puede estar añadido con el lector para este objetivo. Este sensor es el encargado de encender y apagar el lector cuando algún evento producido en el exterior sea detectado por el sensor.

Un anunciador es una señal electrónica. Ejemplo de anunciadores son las alarmas audibles, señales luminosas, etc. Un conjunto de luces podría ayudar a diferenciar los distintos estados siendo cada estado de un color diferente. Por ejemplo el rojo indicaría que hay una etiqueta inválida o mala en la zona de lectura, verde podría indicar que es una etiqueta válida y ámbar podría decir que se ha interrumpido la conexión entre el lector y el controlador.

Un actuador es un dispositivo mecánico para controlar o mover objetos. Como ejemplos de actuadores tenemos al PLC (Controlador lógico programable), brazos de robot, brazos mecánicos de un torno para el acceso de una entrada, etc. Un PLC es uno de los actuadores más versátiles, y son ampliamente usados en las plantas de producción. Los PLCs activan una variedad de acciones para ser realizadas (como monitorear y controlar una línea de ensamblaje).

Los anunciadores y actuadores pueden también ser usados para proveer algún tipo de salida local desde un sistema RFID, como las alarmas audiovisuales en caso de un error de lectura, abriendo una entrada en caso de una lectura exitosa, y otras tareas similares.

2.3.12 EQUIPO Y SISTEMA SOFTWARE

El equipo y el sistema software es un término que engloba los componentes de hardware y software, y que están separados del hardware propio RFID (eso es el lector, tag y antena); el sistema está compuesto por los siguientes componentes:

- Interfaz/sistema terminal
- Middleware
- Interfaz de la empresa
- Servidor de la empresa

En un sistema RFID no trivial, todos estos componentes pueden o no estar presentes. Las siguientes secciones describen estos componentes.

2.3.12.1 Interfaz/sistema terminal

Este componente integra el equipo y el sistema de software completo con el hardware de RFID. Esta integración se cumple estableciendo comunicación y control del sistema nervioso central del hardware RFID: los lectores. Por tanto, la tarea de este componente es coger datos de los lectores, controlar el comportamiento de los lectores y usar los lectores para activar la asociación de actuadores y anunciadores externos.

Este componente es lógicamente y físicamente cercano al hardware del sistema RFID y puede ser considerado de estar en el borde cuando es visto desde la perspectiva del equipo y sistema software. Por tal razón, este es también el correcto lugar para que este componente active los actuadores y anunciadores externos sin ninguna necesidad de ir a través del lector. Esta colocación resulta

ser muy útil porque entonces la elección y las capacidades de control de los anunciadores y actuadores no están limitadas por el soporte del lector, pero pueden estar extendidas cómo y cuándo sean necesitadas para la personalización del sistema terminal.

El sistema terminal es también el perfecto lugar para esconder los detalles esenciales de la interacción con un lector específico (a través de su controlador) de un fabricante en particular. Por eso, este componente también provee una capa de abstracción para todos los tipos de lectores necesitados por el sistema RFID. Esta capa de abstracción es muy esencial porque entonces el resto del equipo y el sistema de software pueden usar esta abstracción para interactuar con cualquier tipo de lectores soportados, sin necesidad de cambiarse a sí mismo.

Además, este componente puede realizar otro tipo de tareas diferentes que están más allá de las responsabilidades de un controlador, como son las siguientes:

- Filtrar lecturas duplicadas desde diferentes lectores
- Permitir la configuración de disparadores basados en eventos que pueden automáticamente activar un anunciador o un actuador.
- Proveer funciones inteligentes como agregar y enviar selectivamente información de una etiqueta a un equipo y sistema informático.
- Administración remota del lector.
- Administración remota de sí mismo.

Este componente puede ser hospedado en un hardware especial o en un sistema integrado. Entonces el resto del equipo y sistema de software pueden interactuar con este sistema integrado a través de una red cableada o sin cables. Este componente puede ser implementado usando un estándar como el Open Services Gateway initiative (OSGi), el cual define un sistema estándar para la entrega de los servicios software a los dispositivos de red. Puede darse el caso de que este componente no esté presente.

2.3.12.2 Middleware

El middleware puede estar definido como todo lo que hay entre el interfaz terminal y el interfaz de la empresa. Este componente puede estar visto como el sistema nervioso central del sistema RFID desde la perspectiva del software (los lectores RFID pueden estar considerados igualmente desde la perspectiva del hardware) en eso provee una funcionalidad básica del sistema, incluyendo lo siguiente:

- Intercambio de datos entre el exterior e interior de una empresa.
- Administración eficiente de los datos masivos producidos por un sistema RFID.
- Está basado en un estándar abierto, entonces puede ser compatible con un amplio rango de sistemas de software.
- Habilitar la desconexión entre el interfaz terminal y el interfaz de la empresa.

Puede darse el caso de que este componente no esté presente. Este es el componente más importante y complejo del equipo y el sistema de software.

2.3.12.3 Interfaz de la empresa

Este componente es habitual que integre el componente middleware con el componente servidor de la empresa. Este es el lugar para implementar los procesos de integración del negocio. Los procesos que sean necesarios integrar con el sistema RFID determinarán la cantidad de esfuerzo para implementar este componente. Ya que el middleware es un componente genérico, algunas configuraciones son casi siempre necesarias para las transacciones y la transmisión de datos entre él y el servidor de la empresa.

2.3.12.4 Servidor de la empresa

Este componente engloba la suite completa de aplicaciones y sistemas IT de la empresa. Esto es el almacenamiento de datos y el motor de procesos del negocio para la empresa. En el contexto del sistema RFID, este componente provee el directorio de datos de los objetos etiquetados al middleware.

Esta componente ocupa el mínimo esfuerzo de implementación de un sistema RFID porque ya es funcional.

2.3.13 INFRAESTRUCTURA DE COMUNICACIÓN

Este componente provee conectividad y habilita la seguridad y las funciones administrativas de los sistemas para diferentes componentes de un sistema RFID. Esta incluye la red alámbrica e inalámbrica, y las conexiones seriales entre lectores, controladores y ordenadores. El tipo de red inalámbrica puede albergar desde una red personal (PAN, la que provee Bluetooth), a una red local (LAN), WAN, etc. Las comunicaciones por satélite están creciendo realmente para los sistemas RFID que necesitan trabajar en una zona geográficamente muy extensa.

2.3.14 CONCEPTOS BÁSICOS

Esta sección trata sobre los términos que son comúnmente usados en referencia a un sistema RFID:

- Frecuencia
- Colisión de etiquetas
- Colisión de lectores
- Legibilidad de etiquetas
- Robustez de lectura

La frecuencia es el atributo más importante de un sistema RFID.

2.3.14.1 Colisión de etiquetas

Un lector sólo puede comunicarse con una etiqueta a la vez. Cuando más de una etiqueta intenta comunicarse con el lector al mismo tiempo, ocurre una colisión de etiquetas. Para lo cual el lector tiene que comunicarse con las etiquetas

conflictivas utilizando un protocolo de singulación. El algoritmo que se usa para tratar las colisiones de etiquetas se llama algoritmo anti-colisión. Los dos algoritmos más utilizados son:

- Tree Walking para UHF
- ALOHA para HF

2.3.14.1.1 Tree Walking

El algoritmo más conocido para el manejo de colisión de etiquetas es el recorrido de árboles (tree walking), se utiliza en etiquetas que operan a 915Mhz, este algoritmo conlleva una pregunta que deberán responder todas las etiquetas cuyo identificador comience bien con 0, bien con 1. Si más de uno responde, el lector puede pedir que respondan todos los que tengan un identificador que comience por (siguiendo con el 0 inicial) 00 ó 01, y así sucesivamente añadiendo bits en la secuencia deseada (010, por ejemplo, a continuación, tras 01) hasta que se encuentre la etiqueta. Si el lector tiene información sobre ciertas etiquetas que desea encontrar puede optimizar el orden de búsqueda. Por ejemplo, si el lector sospecha que hay etiquetas que están presentes puede indicarles que no respondan a las preguntas para evitar su interferencia. Finalmente, las etiquetas pueden consultarse una a una.

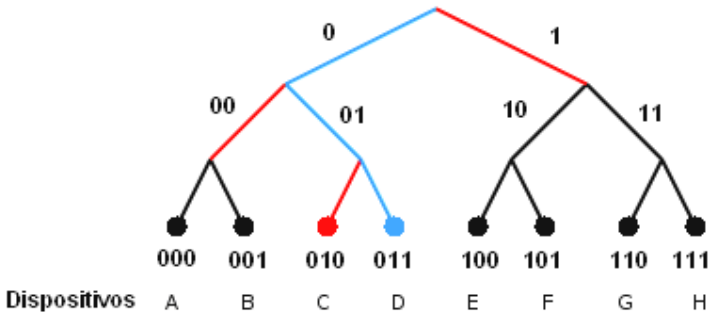


Figura 2.25 Método Tree Walking[44]

[44] http://es.wikipedia.org/wiki/Archivo:RFID_search_environment.png

Este algoritmo sencillo hace visible mucha información al exterior, ya que cualquiera que pueda escuchar al lector puede conocer todos los bits de una etiqueta menos el último, por lo que una etiqueta es muy identificable con tal de que se reciba la señal del lector, y esto puede suceder en un rango de distancias mucho mayor que para una etiqueta típicamente. Debido a esto se ha desarrollado dos protocolos más avanzados que pretenden resistir este tipo de ataques (UHF clases 0 y 1). Aunque se basan en recorrido de árboles incluyen otros aspectos y pueden recorrer más de 1000 etiquetas por segundo.

Este protocolo puede bloquearse total o parcialmente utilizando etiquetas bloqueadoras (*blocker tag*).

2.3.14.1.2 Aloha

Este algoritmo se utiliza en etiquetas que operan a 13.56 Mhz, muy parecido en lo básico al CSMA/CD. En ALOHA las etiquetas detectan la ocurrencia de colisiones e intentan un reenvío pasado un determinado tiempo aleatorio. Se puede doblar el rendimiento de este método si se sincronizan las transmisiones con ciertos slots de tiempo, que en este caso provee el lector. ALOHA no filtra información como el método de recorrido de árbol y es mucho menos vulnerable a la acción de etiquetas bloqueadoras.

Si el campo del lector está muy poblado ALOHA puede ser mucho menos eficiente que un recorrido de árbol optimizado, y puede llegar a colapsar las prestaciones. Se está intentando estandarizar una versión de ALOHA que se denomina HF clase 0, con un rendimiento de hasta 200 etiquetas por segundo.

2.3.14.2 Colisión de lectores

Cuando la zona de lectura de dos o más lectores se solapa, la señal de un lector puede interferir con la señal del otro. A este fenómeno se le denomina colisión de lectores. Como resultado, la energía de radiofrecuencia de una de las antenas de un lector cancela la energía de radiofrecuencia de alguna antena del otro lector. Para evitar este problema, la posición de las antenas de los lectores no deben

estar encaradas. En caso de no poder evitar esta posición, se deben separar lo suficiente sus zonas para que no se solapen. Se puede usar además atenuadores.

“Dos antenas de un mismo lector no tienen porqué solaparse si sólo hay una antena activa cada vez.” [45] También se puede usar la técnica TDMA (time division multiple access) para evitar este tipo de colisión. En su esquema, los lectores están programados para leer en diferentes instantes de tiempo. Por eso, muchos mecanismos de filtrado inteligente deben de ser implementados por el controlador o el sistema/interfaz terminal para filtrar las lecturas duplicadas de tags.

2.3.14.3 Legibilidad de etiquetas

La legibilidad de etiquetas de un sistema RFID puede estar definida como la capacidad del sistema de leer adecuadamente los datos de una etiqueta específica. Desde una simple perspectiva, un sistema RFID necesita leer una etiqueta satisfactoriamente sólo para proveer una buena legibilidad de la etiqueta. Para garantizar esto, el sistema debe estar diseñado para leer una etiqueta varias veces, y que acierte continuadamente. Esto es muy importante para que un sistema RFID sea robusto.

2.3.14.4 Robustez de lectura

La robustez de lectura es el número de veces que una etiqueta en particular pueda ser leída satisfactoriamente cuando esté dentro de una zona de lectura. Como comentamos anteriormente, un sistema RFID tiene que estar diseñado para que tenga robustez en las lecturas de las etiquetas. “La velocidad de un objeto etiquetado puede impactar negativamente la robustez de lectura así como también el tiempo que permanece la etiqueta en la zona de lectura disminuye con

[45] LAHIRI Sandip; RFID Sourcebook; IBM Fress Books, EE.UU. 2006, Pág.46

el incremento de velocidad.” [46] Esto resulta en un decremento de robustez para la etiqueta. El número de etiquetas presentes en un instante en la zona de lectura también puede dificultar la robustez de lectura porque el número de etiquetas que puede ser leído por un lector por unidad de tiempo está limitado.

2.3.15 CARACTERIZACIÓN DE UN SISTEMA RFID

Un sistema RFID puede estar caracterizado de tres formas basado en los siguientes atributos:

- Frecuencia operacional
- Rango de lectura
- Método de conexión físico

Estos criterios están interrelacionados. El primer criterio requiere un análisis a detalle el cual se lo realiza en la sección 2.4.

2.3.15.1 Caracterización basada en el rango de lectura

El rango de lectura de un sistema RFID está definido como la distancia de lectura entre la etiqueta y el lector. Usando este criterio, un sistema RFID puede estar divido entre los siguientes tres tipos:

- Enganche cercano.- El rango de lectura es menor que 1cm. Operan a frecuencias de LF y HF.
- Enganche remoto.- El rango de lectura es de 1cm a 100cm. Operan a frecuencias de LF y HF.
- Rango largo.- El rango de lectura es mayor a 100cm. Operan a frecuencias de UHF y microondas.

[46] LAHIRI Sandip; RFID Sourcebook; IBM Fress Books, EE.UU. 2006, Pág. 46

2.3.15.2 Caracterización basada en el método de conexión físico

La conexión física se refiere al método usado para enganchar la etiqueta con la antena (eso es, el mecanismo por el cual la energía es transferida a la etiqueta desde la antena). Basados en este criterio, son posibles tres tipos de sistemas RFID:

- Magnético
- Eléctrico
- Electromagnético

2.3.15.2.1 Sistema de conexión magnético

Estos tipos de sistemas RFID también son conocidos como sistemas de conexión inductiva o sistemas radio-inductivos. Pertenecen a esta categoría los sistemas RFID que operan en LF y HF.

2.3.15.2.2 Sistema de conexión eléctrico

Estos tipos de sistemas RFID también son conocidos como sistemas de conexión capacitivos. Pertenecen a esta categoría los sistemas RFID que operan en LF y HF.

2.3.15.2.3 Sistema de conexión electromagnético

La mayoría de los sistemas RFID que pertenecen a esta clase son también llamados “Backscatter Systems”. Pertenecen a esta categoría los sistemas RFID que operan en UHF y microondas.

2.4 FRECUENCIAS DE OPERACIÓN DE UN SISTEMA RFID

La frecuencia de operación es el atributo más importante de un sistema RFID. Es la frecuencia a la cual los lectores transmiten su señal. Está cercanamente asociado con el típico atributo de la distancia de lectura. En la mayoría de los

casos, la frecuencia de un sistema RFID está determinada por su típico requerimiento de la distancia de lectura.

Los diferentes tipos de frecuencias utilizadas en RFID son las siguientes:

- Baja frecuencia (LF)
- Alta frecuencia (HF)
- Ultra alta frecuencia (UHF)
- Microondas

BAJA FRECUENCIA (LF).- Son consideradas frecuencias bajas aquellas que se encuentran entre 30 KHz y 300 KHz, y los sistemas RFID normalmente usan las frecuencias del rango de 125 KHz a 134 KHz. “Un sistema RFID típico de LF es el que opera a 125 KHz o 134.2 KHz.” [47] Sistemas RFID de LF generalmente usan las etiquetas pasivas (aquellas que no disponen de una propia fuente de alimentación), teniendo una baja velocidad de transmisión de datos entre la etiqueta y el lector, y es especialmente bueno si el ambiente de operación contiene metales, líquidos, suciedad, nieve, o fango. Las etiquetas activas (aquellas que disponen de su propia fuente de alimentación) de LF también están disponibles en el mercado, esto debido a la estabilidad que presentan las mismas. El rango de LF es aceptado a nivel mundial.

Su principal ventaja es su aceptación en todo el mundo, funciona cerca de los metales y está ampliamente difundida. La distancia de lectura es inferior a 1,5 metros, por lo que las aplicaciones más habituales son la identificación de animales, barriles de cerveza, auto key and lock o bibliotecas.

---

[47] http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd

ALTA FRECUENCIA (HF).- Las frecuencias altas se encuentran en los rangos de 3 MHz a 30 Mhz, un sistema RFID típico de HF opera normalmente a una frecuencia de 13.56 MHz utilizando etiquetas pasivas donde se tiene una baja velocidad de transmisión de datos entre la etiqueta y el lector, ofrece un rendimiento aceptable en materiales como líquidos y metales, estos sistemas de HF se usan frecuentemente en los hospitales donde no interfiere con el equipo existente. Este rango es aceptado a nivel mundial.

El próximo rango de frecuencia es Very High Frequency (VHF) y está comprendido entre 30 y 300 MHz. Ninguno de los sistemas RFID actuales opera en este rango de frecuencia, razón por la cual no se discute a detalle este tipo de frecuencia.

Esta frecuencia también está muy difundida, pero a diferencia de la frecuencia baja no funciona cerca de los metales. Normalmente se utiliza en aplicaciones tales como la trazabilidad de los productos, movimientos de equipajes de avión o acceso a edificios.

ULTRA ALTA FRECUENCIA (UHF).- Está comprendido entre 300 MHz y 1 GHz. Un típico sistema pasivo UHF RFID opera a 915 MHz en EE.UU. y a 868 MHz en Europa. Un típico sistema activo UHF RFID opera a 315 MHz y 433 MHz en Europa. Un sistema UHF puede utilizar etiquetas activas y pasivas con una rápida transferencia de datos entre etiqueta y lector, sin embargo se tiene una transferencia lenta en presencia de metales y líquidos (excepto en 315 MHz y 433 MHz). Los sistemas RFID de UHF han empezado a ser desplegados ampliamente debido a recientes mandatos RFID de grandes empresas públicas y privadas. El rango de UHF no es aceptado a nivel mundial porque no existen regulaciones globales para su uso y su aplicación depende de la legalidad del país. Este tipo de frecuencia se usa para aplicaciones de trazabilidad con etiquetad activas.

MICROONDAS.- La frecuencia de microondas va desde 1 GHz. Un sistema de microondas RFID opera a 2.45 GHz o 5.8 GHz, aquí se utiliza etiquetas semi-activas y pasivas con la más rápida transferencia de datos entre la etiqueta y

el lector y velocidades muy pobres ante la presencia de materiales como líquidos y metales. Debido a que la longitud de la antena es inversamente proporcional a la frecuencia, la antena de una etiqueta pasiva que opera en la frecuencia de microondas tiene la longitud más pequeña. La frecuencia de 2.4 GHz se lo denomina ISM (Industry, Scientific and Medical) y es aceptada a nivel mundial.

Estas frecuencias son las más habituales para las etiquetas activas, además ofrecen largas distancias de lectura y altas velocidades de transmisión. Las etiquetas activas que operan en el rango de las microondas son muy usadas para el seguimiento y trazabilidad de personas u objetos.

País/ Región	LF	HF	UHF	Microondas
EE.UU.	125-134 KHz	13.56 MHz 10W ERP	902-928 MHz, 1W ERP or 4W ERP	2400-2483.5 MHz, 4W ERP 5725-5850 MHz, 4W ERP
Europa	125-134 KHz	13.56 MHz	865-865.5 MHz, 0.1W ERP, LBT. 865.6-867.6 MHz, 2W ERP, LBT. 867.6-868 MHz, 0.5W ERP, LBT.	2.45 GHz
Japón	125-134 KHz	13.56 MHz	N/A.	2.45 GHz
Singapore	125-134 KHz	13.56 MHz	923-925 MHz. 2W ERP.	2.45 GHz
China	125-134 KHz	13.56 MHz	N/A.	2446-2454 MHz, 0.5W ERP

Tabla 2.2 Regulaciones internacionales de frecuencia para RFID

Existen restricciones internacionales que se aplican a las frecuencias de RFID. Por lo tanto, algunas de las frecuencias previamente discutidas pueden no ser válidas a nivel mundial. La tabla 2.2 presenta el estado actual de las regulaciones de los principales países para el uso de RFID.

En la figura 2.26 se muestra la distribución del espectro electromagnético donde se señala cada una de las frecuencias de operación de la tecnología RFID.

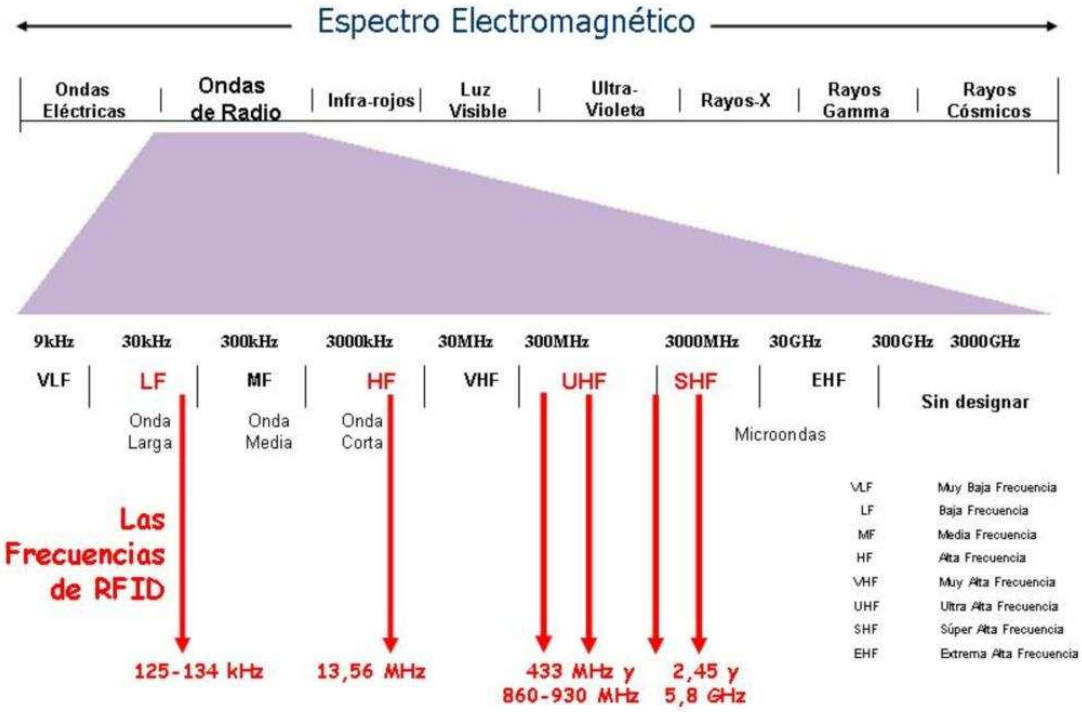


Figura 2.26 Frecuencias de operación RFID[48]

2.5 ESTÁNDARES PARA RFID

Una discusión acerca de la tecnología RFID no está completa sin los estándares de los diferentes cuerpos y organizaciones apuntados a resolver y estandarizar los diferentes aspectos de la tecnología. Las razones por las que se discuten los estándares son las siguientes:

- **Diseño e implementación de un sistema de trabajo robusto y bien pensado.-** En lugar de gastar recursos en manufacturar un sistema apropiado de marca, el cual podría ser propenso a errores y deficiencias, el estándar apropiado podría especificar una solución que tiene sometido a varias iteraciones y mejoras, el cual le habilitará para producir una solución que sea bien definida, robustecida, tratada y probada en implementaciones del mundo real.

[48] http://control-accesos.es/wp-content/rfid-spectrum.JPG

- **Diseñar una implementación de un sistema abierto.**- El estándar puede proveer especificaciones estrictas para la solución de los componentes que los vendedores e integradores proveen a las estanterías, y así se puede evitar cualquier esfuerzo de desarrollo muy extenso.
- **Diseñar e implementar un sistema compatible.-** Que la solución resultante sea compatible con una amplia gama de sistemas relacionados. Por lo tanto, se requerirá pocos recursos y menos esfuerzo para integrar esta solución con otros sistemas.

Este capítulo discute los estándares para RFID que están en existencia hoy. Las siguientes organizaciones han producido estándares relacionados a algún aspecto de RFID o han provisto funciones regulatorias relacionadas:

- **ANSI** (Instituto Nacional De Estándares Americanos)
- **AIAG** (Grupo de Acción de La Industria Automotriz)
- **EAN.UCC** (Asociación Internacional de Numeración de Artículos Europeos, Consejo de Código Uniforme)
- **EPCGlobal**
- **ISO** (Organización Internacional Para la Estandarización)
- **CEN** (Comité Europeo de Normalización)
- **ETSI** (Instituto de Estándares para las Comunicaciones Europeas)
- **ERO** (Oficina de Radiocomunicaciones Europeas)
- **UPU** (Unión Postal Universal)
- **ASTM** (Sociedad Americana para la Prueba y los Materiales)

2.5.1 ESTÁNDARES ANSI

"ANSI es una organización sin fines de lucro que administra y coordina la estandarización voluntaria. Su misión es agrandar la competitividad global de los negocios en Estados Unidos y la calidad de vida promoviendo y facilitando los estándares para el desarrollo tecnológico." [49]

A continuación se enlistan los principales estándares ANSI que están relacionados con la tecnología RFID.

- **ANS INCITS 256-2001.** Estándar para la promoción de los dispositivos RFID interoperables, operando en bandas internacionales que están disponibles libremente y niveles de energía con licencia gratuita. Este estándar también apoya las aplicaciones de manejo de artículos.
- **ANS INCITS 371.** Tecnología de la Información-Sistemas de Localización en Tiempo Real (RTLS). Este está compuesto de las siguientes partes:
  - Protocolo de Interface Aérea a una frecuencia de 2.4 GHz
  - Protocolo de Interface Aérea a una frecuencia de 433 MHz
  - Interface de Programación de la Aplicación (API)
- **ANS MH10.8.4.** Estándar de RFID para contenedores de plástico reusables. Este estándar es compatible con ISO 17364.

2.5.2 ESTÁNDAR AIAG

Es una asociación sin fines de lucro, las metas primarias de AIAG son reducir el costo y la complejidad dentro de la cadena de suministros automotrices y para mejorar la velocidad del mercado, calidad del producto, salud y seguridad de los empleados, y el ambiente.

- **AIAG B-11.** Estándar para identificar neumáticos y ruedas con RFID. La versión actual provee un número de 96-bits en EPCglobal (discutido más adelante) formato de datos para etiquetas RFID.

---

[49] http://www.rfid-handbook.de/rfid/standardization.html

2.5.3 ESTÁNDAR EAN*UCC

El sistema EAN*UCC es dirigido conjuntamente por el consejo de código uniforme, Incorporado y GS1 (antiguamente EAN Internacional). El sistema EAN*UCC estandariza los números de identificación, esquemas XML y otras soluciones a la cadena de suministros que permiten tener procesos más eficientes en los negocios.

El consejo de código uniforme (UCC) es una organización sin fines de lucro dedicada al desarrollo e implementación de estándares basados en soluciones de una cadena global de suministro. Bajo estos auspicios, la UCC opera tres subsidiarias: UCC, RosettaNet, y EPCglobal US y éste maneja conjuntamente el sistema global EAN*UCC con GS1.

EPCglobal, Sociedad Anónima es una consecuencia del UCC y EAN Internacional. Las soluciones basadas en UCC, incluyendo los procesos de negocios, estándares XML, grupos de transacción EDI (Intercambio electrónico de datos), y los estándares de identificación del código de barras del Sistema EAN*UCC son correctamente utilizados por más de un millón de compañías miembros a nivel mundial.

Las soluciones en la cadena de suministros ofrecida por el sistema EAN*UCC incluye códigos de identificación únicos mundialmente, medios de transporte de datos, comercio electrónico, y estándares comunicacionales. Estas herramientas apoyan a las industrias estabilizadas así como también a los mercados emergentes.

La siguiente iniciativa de estandarización RFID está provista por este cuerpo de estándares:

- **GTAG** (Etiqueta Global). Esto apunta a facilitar las operaciones en la cadena de suministro global en la banda de los 862-928 MHz. Provee de una fundación técnica con grupos de datos y lineamientos de aplicaciones.

Las etiquetas RFID en cumplimiento con la etiqueta Global están actualmente disponibles por varios fabricantes.

2.5.4 ESPECIFICACIÓN EPCGLOBAL

EPCglobal, es una iniciativa que se junta entre el UCC y la EAN internacional. El objetivo de EPCglobal es establecer estándares a nivel mundial, para diseñar, implementar y adoptar un *Código de Producto Electrónico* (EPC) y una Red EPCglobal. La especificación EPCglobal apunta a las operaciones de cadenas de suministro y es probablemente la especificación global más prometedora para RFID.

Como una breve historia, EPCglobal absorbió las responsabilidades administrativas de su predecesor el Centro Auto-ID el 1 de Noviembre de 2003. Las funciones de investigación del Centro Auto-ID fueron transferidas a varios laboratorios Auto-ID a nivel mundial. EPCglobal, mantiene una relación muy cercana con los laboratorios Auto-ID para realzar la tecnología y encontrar necesidades futuras. El Centro Auto-ID se fundó en Octubre de 1999 como un programa de investigación auspiciado por 100 compañías y 5 de las universidades líderes en el mundo. Esta fue responsable de conceptualizar, crear y promover la especificación original llamada *Centro Auto-ID* especificación que involucró la tecnología EPC. Después que la tecnología EPC fue suficientemente desarrollada en la configuración de la investigación, la necesidad de un cuerpo de estándares fue necesaria para comercializar y dirigir la adopción global de la tecnología. Ambos EAN y UCC tienen varios años de experiencia en manejar estándares, y la combinación de estos dos cuerpos verdaderamente hace una de las entidades globalmente más capaces para adelantar la Red EPC y EPCglobal.

La siguiente sección discute la Red EPCglobal, la cual es el componente fundamental de la especificación EPCglobal.

2.5.4.1 Red EPCglobal

La Red EPCglobal es una colección de tecnologías que pueden proveer una identificación en tiempo real y datos inteligentes automáticos partiendo de una filosofía, ambos dentro y fuera de una empresa. Aunque esto se dirigió hacia las operaciones de cadena de suministro de una empresa, puede ser aplicado en otros tipos de aplicaciones por ejemplo, rastreo y localización de un artículo.

Los principales componentes tecnológicos que hacen la Red EPCGlobal son los siguientes:

- Código Electrónico del Producto (EPC).
- Material de colección de datos consistente de etiquetas y lectores EPC. Esto es también colectivamente conocido como *sistema ID.*
- Soporte físico y lógico EPCglobal.
- Servicios de descubrimiento (DS).
- Servicios de Información EPC (EPCIS)

Así, la “ecuación” de la Red EPCglobal puede ser resumida como sigue:
Red EPCglobal=Sistema ID+EPC+Middleware+DS+EPCIS

Además, EPCglobal provee una arquitectura referencial para la red.

Las siguientes sub secciones discuten estos componentes en detalle. Estas descripciones son seguidas por una sección que explica como interactúan estos componentes juntos para formar la Red EPCglobal.

2.5.4.1.1 Código Electrónico del Producto (EPC)

El Código Electrónico del Producto (EPC) es un identificador que puede *únicamente* identificar cualquier artículo en una cadena de suministro. Este es un esquema simple y compacto que puede generar extremadamente grandes

cantidades de identificadores únicos. Al mismo tiempo, este esquema permite alojar códigos de legado y estándares tales como los siguientes:

- **Número Mundial de artículo comercial (GTIN).** Un GTIN en sí mismo no se ajusta a la definición de una identidad pura de EPC, porque no identifica a un solo objeto físico de manera única e inequívoca. En su lugar, un GTIN identifica a una clase de objeto en particular, tal como un tipo particular de producto o SKU.

- **Identificador Mundial de Bienes Retornables (GRAI).** A diferencia del GTIN, GRAI se utiliza para la asignación de objetos individuales y, por lo tanto, no requiere campos adicionales que sirvan como identidad pura de EPC. El GRAI está formado por los siguientes elementos de información:

    - El Prefijo de Compañía asignado por EAN o UCC para una entidad administradora. El Prefijo de Compañía está constituido por los mismos dígitos del Prefijo de Compañía dentro de un código decimal GRAI de EAN.UCC.
    - El Tipo de Bien asignado por la entidad administradora a una clase particular de bienes.
    - El Número Seriado asignado por la entidad administradora a un objeto individual. EPC sólo puede representar un subconjunto de Números Seriados permitidos en las Especificaciones Generales EAN.UCC. En especial están permitidos sólo aquellos Números Seriados formados por uno o más dígitos, sin ceros de encabezado.

- **Identificador Único (UID).** Este es un esquema de numeración del Departamento de Defensa de los Estados Unidos para activar el rastreo.

- **Número mundial de Localización (GLN).** Un GLN puede representar ya sea una localización física única y separada tal como una puerta en un dock o una abertura del depósito o bien una localización física en su totalidad, tal como la totalidad del depósito. Asimismo, un GLN puede

representar una entidad lógica tal como una “organización” que realiza una función comercial, como por ejemplo, la emisión de una orden de pedido.

- **Identificador Mundial de Bienes Individuales (GIAI).** está definido en las Especificaciones Generales EAN.UCC. A diferencia del GTIN, el GIAI se asigna para objetos individuales y, por lo tanto, no requiere campos adicionales que sirvan como una identidad pura EPC.
  El GIAI está formado por los siguientes elementos de información:

  - El Prefijo de Compañía asignado por EAN o UCC para administrar la entidad. El Prefijo de Compañía constituido por los mismos dígitos del Prefijo de Compañía dentro de un código decimal GIAI de EAN.UCC.
  - La Referencia de Bienes Individual asignada únicamente por la entidad administradora para un bien específico. Mediante EPC sólo se puede representar un subconjunto de Referencias de Bienes Individuales en las Especificaciones Generales EAN.UCC. En especial, sólo aquellas Referencias de Bienes Individuales de uno o más dígitos, sin ceros de encabezado, están permitidas

- **Código Seriado de Contenedor de Embarque (SSCC).** Está definido en las Especificaciones Generales EAN.UCC. A diferencia del GTIN, el SSCC se asigna para objetos individuales y, en consecuencia, no requiere ningún campo adicional que sirva como entidad pura EPC.

  Muchas aplicaciones de SSCC históricamente han incluido el Identificador de Aplicación (00) en el campo Identificador SSCC cuando se lo almacena en una base de datos. Este no es un requisito estándar, sino que surge de una práctica generalizada. El Identificador de Aplicación es un tipo de encabezado utilizado en las aplicaciones de código de barras y se lo puede inferir directamente de los encabezados EPC que representan el SSCC. En

otras palabras, se puede interpretar que un SSCC EPC necesita incluir el (00) como parte del identificador SSCC o que esto tal vez no sea necesario.

El SSCC está formado por los siguientes elementos de información:

- El Prefijo de Compañía asignado por EAN o UCC para una entidad administradora. El Prefijo de compañía está formado por los mismos dígitos del Prefijo de Compañía dentro un código decimal SSCC de EAN.UCC.

- La Referencia Seriada asignada de manera única e inequívoca por la entidad administradora a una unidad de embarque específica. La Referencia Seriada, a los fines de la codificación EPC, deriva del SSCC al concatenar el Dígito de Extensión del SSCC y los dígitos de Referencia Seriados y tratar el resultado como un número entero único.

Una compañía que utiliza código de barras en esta operación puede tener un camino de migración para RFID utilizando EPC. Un código EPC puede ser utilizado para determinar varios atributos de un artículo, tales como los siguientes:

- Versión utilizada del EPC.
- Identificación del fabricante
- Tipo de Producto
- Número de serie único de un artículo

Dos EPCs pueden ser de tamaños diferentes. Actualmente, de 64 bits y de 96 bits son los más predominantemente utilizados en las etiquetas EPC en la práctica; las etiquetas EPC de 128 bits han empezado ahora a aparecer en el mercado con etiquetas EPC de 256 bits en la etapa prototipo de especificación. Cabe recalcar que un EPC de 96 bits es suficiente para la mayoría de operaciones de cadena de

suministro. La estructura del EPC como está prescrita primariamente por la especificación global EPC consiste de cuatro partes que corresponde a los atributos precedentes:

- Cabecera que denota la versión EPC utilizada
- Número de administración que especifica el nombre o el dominio de la compañía
- Clase de objeto que representa el tipo de clase del objeto etiquetado
- Numero serial, que en este caso viene a ser el número del objeto etiquetado

La Figura 2.27 muestra estos campos de un EPC de 96 bits.

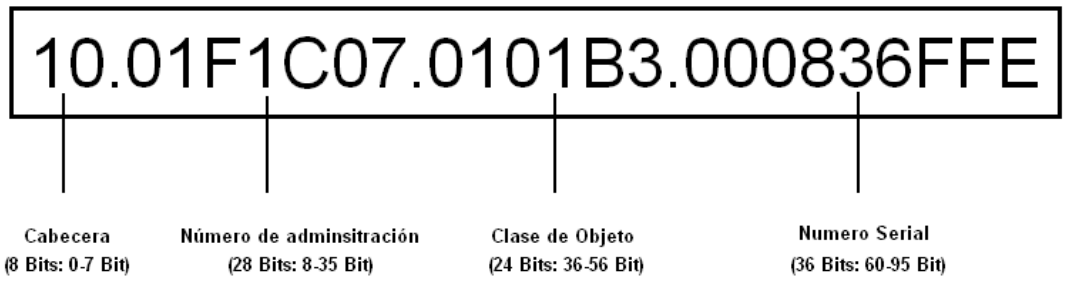


Figura 2.27 Estructura del EPC de 96 Bits[50]

Un EPC también puede incorporar un valor de filtro opcional basado en que los EPCs de objetos etiquetados pueden ser filtrados de una manera eficiente. Utilizando 96 bits, usted puede generar un total de 79,228,162,514,264,337,593,543,950,336 (o más o menos 80,000 trillones de trillones) de números únicos. Otra forma de considerar un EPC de 96 bits es que puede proveer identificadores únicos para 268 millones de compañías con cada compañía capaz de representar sobre los 16 millones de clases de objetos.

[50] LAHIRI Sandip; RFID Sourcebook; 2005

“Un EPC es estrictamente un identificador único y nada más. Por lo tanto, cualquier información específica de un producto tiene que residir separadamente en la empresa en los sistemas de respaldo.” [51]

La siguiente sub sección discute un concepto muy importante llamado clases de etiquetas EPC.

2.5.4.1.1.1 Clases de Etiquetas EPC

EPCglobal ha definido las siguientes cuatro clases de etiquetas EPC RFID para proveer diferentes capacidades a varios rangos de precio:

- Clase 0/Clase 1
- Clase 2
- Clase 3
- Clase 4

Las siguientes sub secciones discuten esta clasificación a detalle.

2.5.4.1.1.1.1 EPC Clase 0/Clase 1

Ambos tipos de etiqueta son etiquetas pasivas que pueden almacenar ya sea 64 bits o 96 bits o datos EPC. Los datos de una etiqueta de Clase 0 consisten de un número serial único que ya ha sido grabado por el fabricante antes que esta etiqueta sea entregada a un cliente. La Clase 0 opera a una frecuencia de UHF (900 MHz) mientras que la Clase 1 opera en las frecuencias de UHF (860-930 MHz) y HF (13.56 MHz). Todos estos tipos de etiqueta utilizan una tecnología avanzada para una comunicación lector-etiqueta. Estos son los tipos de etiqueta disponibles más económicos. Actualmente, Las etiquetas de Clase 0 y Clase 1 no son interoperables, es decir un lector que puede leer una etiqueta de Clase 0 no podría ser capaz de leer una etiqueta de Clase 1 y viceversa.

[51] LAHIRI Sandip; RFID Sourcebook; 2005

Una etiqueta *de Generación 2 UHF* se la conoce simplemente como una etiqueta Gen 2, es una nueva generación de etiquetas EPC basadas en el Protocolo de Fundación UHF Generación 2 que reemplazará a las etiquetas de Clase 0 y Clase 1. La especificación fue ratificada como un estándar EPC por EPCglobal el 16 de Diciembre de 2004. Una etiqueta Gen 2 opera a una frecuencia de UHF (860-930 MHz) y consistirá de una etiqueta RW de 128 bits con 96 bits reservados para los datos EPC y 32 bits para corrección de errores.

2.5.4.1.1.1.2 EPC Clase 2

Esta es una etiqueta RW pasiva que puede almacenar un EPC juntamente con los datos del usuario. La capacidad mínima de los datos del usuario por cada etiqueta es de 224 bits. Una etiqueta de clase 2 es activada con emisión de energía. Estos son los nuevos tipos de etiquetas más económicos después de la clase 0/ Clase 1.

2.5.4.1.1.1.3 EPC de clase 3

Esta es una etiqueta activa RW con una gran capacidad para datos de usuario que esta vez no está especificada. Una etiqueta de clase 3 EPC soporta capacidad de procesamiento de datos de entrada/salida. Esta etiqueta utiliza tecnología avanzada para la comunicación lector-etiqueta y es transmisora de energía. Estos son los próximos tipos de etiqueta más económicos después de la clase 2.

2.5.4.1.1.1.4 EPC de clase 4

Esta es una etiqueta activa RW con una gran capacidad para datos de usuario que aún no está especificada. Soporta capacidad de procesamiento de datos de entrada/salida. Esta etiqueta utiliza una avanzada tecnología de transmisión para la comunicación lector-etiqueta. El rango mínimo de lectura es de 300 pies (cerca de 91 metros). Estos son los tipos de etiquetas más costosos.

2.5.4.1.2 Hardware de colección de datos.

El EPCglobal ha lanzado especificaciones para las etiquetas EPC y protocolos de interface basados en que los lectores y las etiquetas pueden ser interoperables desde el punto de vista de diferentes fabricantes o marcas. Por ejemplo, una etiqueta de clase 1 EPC de un fabricante podría ser leído por un lector compatible de Clase EPC de otro fabricante. Esta naturaleza de apertura provee gran flexibilidad y promueve la competencia entre diferentes fabricantes para brindar productos superiores a un bajo costo.

2.5.4.1.3 Servicios de Descubrimiento

Esto provee de servicios mediatos y el acceso a los datos EPC. ONS (Servicio de Nombramiento de Objeto) Este es un componente de estos servicios, y es descrito en la siguiente sección.

2.5.4.1.3.1 Servicio de Nombramiento de Objeto (ONS)

El ONS es un servicio público que puede ser utilizado para buscar servidores EPCIS (servicios de información EPC) desde los cuales se pueden extraer datos de un cierto producto. Este provee de un mecanismo de mapeo entre un EPC y el conjunto de instancias EPCIS que contienen información acerca de este EPC. En conclusión el ONS es muy similar al servicio DNS que es utilizado para buscar un determinado host asociado con una dirección de Internet en particular. El servicio ONS tiene que ejecutarse en tiempo real para que de esta manera puedan rápidamente manejarse un gran número de pedidos de una manera confiable.

2.5.4.1.4 Middleware de EPCglobal

Una etiqueta que puede ser leída múltiples veces por el mismo o diferentes lectores en diferentes puntos en la cadena de suministro. Cada una de estas

lecturas genera datos de la etiqueta en el lado del lector y consecuentemente en la Red EPCglobal. Como resultado, una cantidad enorme de datos se genera en la Red EPCglobal como consecuencia de la lectura de etiquetas. Una porción sustancial de estos datos puede ser comprimida porque esto sólo consistiría de datos leídos duplicados, lecturas que pueden ser combinadas con otras lecturas, y lecturas que no son significativas en términos de lógica comercial, y así por el estilo. Si estos datos fueran almacenados y transportados como están, la mayoría de los sistemas de almacenamiento y redes colapsaría. Para manejar estos datos eficientemente, necesita que sea ordenado, filtrado, y procesado para que pueda de esta manera ser manejado en tiempo real. Esta es la funcionalidad del middleware de EPCglobal. Además de las tareas previamente descritas, este es también responsable del movimiento de información relevante a través de la red para EPCIS u otros sistemas de respaldo comercial de una empresa. Como resultado, el volumen de los datos es reducido y los datos son transmitidos selectivamente en la red, haciendo el uso de dichos datos eficiente y útil.

2.5.4.1.5 Servicios de Información EPC (EPCIS)

Estas son entradas alojadas en servidores seguros que contienen información acerca de los artículos con números EPC en una Red EPCglobal. Un EPCIS asocia los datos de un EPC con eventos comerciales e información.

La información capturada mediante la utilización de EPC en cualquier punto del mundo, puede ser compartida por los empresarios con sus socios de negocio, a través de EPCIS, una plataforma global y estándar a la que los empresarios tendrán acceso a través de Internet.

EPCIS provee una capacidad sin precedentes de visibilidad del movimiento, localización y disposición de bienes, activos y servicios alrededor del mundo. Esto permitirá el intercambio seguro de información en cada punto del ciclo de vida de los productos y servicios.

Es un estándar abierto y público que provee nuevas capacidades que mejorarán los niveles de eficiencia, seguridad y visibilidad en la cadena de abastecimiento. Ha sido diseñado para complementar los sistemas de información de las empresas y no para reemplazarlos.

Su principio de funcionamiento se basa en que la información capturada por el sistema EPC durante una transacción en la cadena de abastecimiento brinda la información acerca del QUÉ (objeto), CUÁNDO (tiempo), DÓNDE (lugar) y POR QUÉ (momento del negocio y su estatus). Esto significa que los socios de negocio que utilizan EPC pueden intercambiar información acerca del progreso de sus productos a lo largo de los procesos logísticos y lo más importante: pueden hacerlo en el momento en que sucede, en tiempo real.

2.5.4.1.5.1 Lenguaje Físico Markup (PML)

Este es un esquema XML abierto para representar la información del producto tan bien como la comunicación. Actualmente, el PML puede ser dividido en las siguientes partes:

- **Núcleo PML**. Los componentes del núcleo de la Red EPCglobal utiliza este esquema XML abierto para comunicarse mutuamente. Este tipo PML ya ha sido especificado.
- **PML Extendido.** La especificación EPCglobal utiliza este esquema XML abierto para representar las características físicas de los productos. Este tipo PML aún no ha sido completamente especificado. Ejemplos de de este XML son la fecha de expiración del artículo, historia de la localización, información sobre el reciclaje, información de la composición, fecha de elaboración, etc.

La próxima sección discute cómo estos componentes trabajan juntos para formar la Red EPC global.

2.5.4.1.6 Esquema de la Red EPCglobal

Los datos EPC sobre las etiquetas son leídos por los lectores. Estos datos son entonces pasados al middleware para un manejo apropiado por medio de una red cableada o inalámbrica. Los servicios de Descubrimiento proveen información de localización de la instancia EPCIS al middleware. El middleware añade la localización e informaron del evento para procesar los datos y moverlos a la instancia EPCIS apropiada para su almacenamiento y acción. La figura 2.28 muestra el proceso descrito.

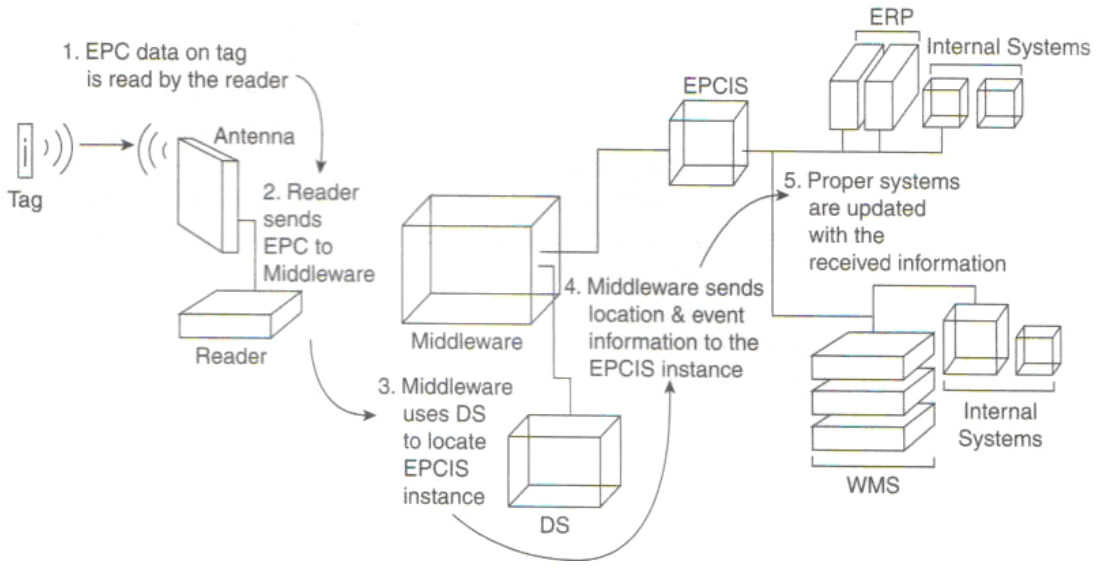


Figura 2.28 Esquema de la red EPCglobal[52]

2.5.5 DEPARTAMENTO DE DEFENSA DE LOS ESTADOS UNIDOS (DOD)

El DoD ha lanzado oficialmente su política RFID el 30 de Julio del 2004, para lo cual la entrega material de productos de consumo y comodidad embarcados a cualquier instalación DoD debe tener etiquetas RFID. Algunas de las políticas más importantes son las siguientes:

[52] http://www.rfid-handbook.de/rfid/standardization.html

- Las etiquetas Pasivas deben ser añadidas a pallets y cases. Esto también aplica a los artículos de alto valor individual que tienen *un código de identificación único* (UID).
- Un proveedor puede utilizar cualquiera de los formatos de datos EPC o UID para codificar la identidad del artículo.
- La utilización de etiquetas pasivas UHF opera entre 860-960 MHz con una distancia de lectura mínima de 9 pies (alrededor de 2.7 metros). La Clase 0 EPC (64 y 96 bits) y la Clase 1 EPC (64 y 96 bits) son aceptables. Estas etiquetas serán eliminadas automáticamente después de que las etiquetas UHF Gen2 y los lectores estén disponibles.
- Todos los contenedores de 20 y 40 pies embarcados fuera de los Estados Unidos deberían tener una etiqueta activa que contenga el listado de los datos escritos en el punto de origen. Esto se aplica a ambos contenedores de carga aérea o marítima.

El DoD ya está convencido de los potenciales beneficios de RFID a través de pilotos múltiples que corren sobre un período de varios meses. Es esperado que RFID provea mejor manejo y control del inventario.

2.5.6 ISO (ORGANIZACIÓN INTERNACIONAL DE ESTANDARIZACIÓN)

El ISO es una red de los institutos de estándares nacionales de 146 países, sobre la base de 1 miembro por país, con una Secretaría Central en Ginebra, Suiza, que coordina el sistema. El ISO es una organización no gubernamental.
El ISO tiene los siguientes TCs (Comités Técnicos) y JTCs (Consejos Técnicos Conjuntos) que están involucrados en formular estándares relacionados con RFID.

- ISO JTCI SC31
- ISO JTCI SC17
- ISO TC 104/SC4
- ISO TC 23/SC19

- ISO TC 204
- ISO TC 122

La lista precedente no es exhaustiva. Los siguientes estándares ISO están relacionados a la tecnología RFID y su uso en aplicaciones de tiempo real:

- **ISO 6346.** Contenedores de transporte –Codificación, identificación y marca.
- **ISO 7810.** Tarjetas de Identificación—características físicas. Provee criterios de rendimiento, requerimientos para intercambios internacionales, y criterios mínimos con características hombre-máquina.
- **ISO 7816.** Tarjetas de identificación –tarjetas con circuito integrado con contactos. Esto está compuesto actualmente de las 12 partes siguientes:
  - Parte 1. Características físicas
  - Parte 2. Dimensiones y localización de los contactos
  - Parte 3. Señales electrónicas y protocolos de transmisión
  - Parte 4. Comandos Inter industriales para el intercambio
  - Parte 5. Sistema de numeración y procedimiento de registro para los identificadores de aplicación
  - Parte 6. Elementos de datos inter industriales para el intercambio
  - Parte 7. Comandos inter industriales para Tarjetas de Lenguaje Estructurado de Consulta (SCQL)
  - Parte 8. Comandos para operaciones de seguridad
  - Parte 9. Comandos para manejo de tarjetas
  - Parte 10. Señales electrónicas y respuesta para resetear tarjetas sincronizadas
  - Parte 11. Verificación personal a través de métodos biométricos
  - Parte 12. Aplicación de información criptográfica

- **ISO 9798.** Información Tecnológica-Técnica de Seguridad-Autenticación de la entidad. Esto está compuesto actualmente de las siguientes partes:
  - Parte 1. General
  - Parte 2. Mecanismos que utilizan algoritmos simétricos cifrados
  - Parte 3. Mecanismos que utilizan técnicas de firma digital

- Parte 4. Mecanismos que utilizan una función de verificación criptográfica
- Parte 5. Mecanismos que utilizan técnicas de cero conocimientos

- **ISO 9897.** Normas para contenedores. Equipamiento, intercambio de información, códigos de comunicación.

- **ISO 10373**. Tarjetas de identificación. Métodos de test. Está dividido en 6 partes

  - Parte 1. Tests de características generales
  - Parte 2. Tarjetas con banda magnética
  - Parte 3. Tarjetas con circuitos integrados y con su respectiva interfaz
  - Parte 5. Tarjetas con memoria óptica
  - Parte 6. Tarjetas de proximidad (10 cm.)
  - Parte 7. Tarjetas de vecindad (1 metro)

- **ISO 10374**. Normas para contenedores. Identificación automática.

- **ISO 10536**. Tarjetas de identificación. Circuitos integrados para tarjetas sin contactos. Está dividido en 3 partes.

  - Parte 1. Características físicas
  - Parte 2. Dimensiones y localización de las áreas de acoplamiento
  - Parte 3. Señales electrónicas y procedimientos para restablecimiento

- **ISO 11784**. RFID para identificación de animales. Estructura del código. Aquí no se especifica el proceso de transmisión entre etiqueta y lector.
- **ISO 11785**. RFID para identificación de animales. Conceptos técnicos. Especifica el proceso de transmisión entre etiqueta y lector.
- **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.
    - Parte 1. Características físicas
    - Parte 2. Radio frecuencia , potencia y señales de la interfaz
    - Parte 3. Inicialización y anticolisión
    - Parte 4. Protocolo de transmisión
- **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.
    - Parte 1. Estándar técnico
    - Parte 2. Procedimiento de registro
- **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 etiquetas 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):
  - Parte 1. Parámetros generales para la interfaz aire y correspondencia con las frecuencias mundialmente admitidas.
  - Parte 2. Interfaz aire para 135 KHz
  - Parte 3. Interfaz aire para 13.56 MHz
  - Parte 4. Interfaz aire para 2.45 GHz
  - Parte 6. Interfaz aire desde 860 MHz hasta 930 MHz
  - Parte 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 test. Similar al ISO 18000. Se divide en 3 partes.
  - Parte 1. Métodos de test para interfaz aire a 13.56 MHz
  - Parte 2. Métodos de test para interfaz aire a 2.45 GHz
  - Parte 3. Métodos de test para interfaz aire a 433 MHz
- **ISO 18185**. Normas para contenedores. Protocolo de sellado eléctrico. (En desarrollo). Está dividido en 7 partes.
  - Parte 1. Protocolo de comunicación
  - Parte 2. Requerimientos de aplicaciones
  - Parte 3. Características del medio
  - Parte 4. Protección de datos
  - Parte 5. Interfaz de sensor
  - Parte 6. Mensaje establecido para transferencia entre el lector y el computador central
  - Parte 7. Capa física
- **ISO 19762.** Información tecnológica. Técnicas AIDC. Dividida en 3 partes.
  - Parte 1. Términos generales relacionados con AIDC
  - Parte 2. Medio óptico de lectura (ORM)
  - Parte 3. Identificación por radio frecuencia
- **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.

2.5.7 ETSI (INSTITUTO EUROPEO DE ESTÁNDARES DE TELECOMUNICACIONES)

El ETSI es una organización independiente, sin fines de lucro en Europa cuya misión es desarrollar los estándares de telecomunicaciones para hoy y para el futuro.
Los siguientes estándares ETSI son relevantes para RFID:

- **ETSI TR 101 445 V1.1.1.** Asuntos de Compatibilidad electromagnética y Espectro de radio (ERM); Dispositivos de Corto Rango (SRD) intencionados para operar en la banda de los 862 MHz hasta los 870 MHz.

- **ETSI I-ETS 300 220 ed.1.** Equipos y Sistemas de Radio (RES); Dispositivos de Rango Corto (SRD); características Técnicas y métodos de prueba para equipos de radio para ser utilizados en el rango de frecuencia de 25 MHz a 1,000 MHz alcanzando niveles de potencia de 500 mW.

- **ETSI EN 300 330 V1.2.2.** Características técnicas y métodos de verificación para equipos RF en la banda de 9KHz a 25MHz y para sistemas de bucle inductivo en la banda de 9KHz a 30MHz.

- **ETSI I-ETS 300 440/C1 ed.1.** Equipos y Sistemas de Radio (RES); Dispositivos de Rango Corto (SRD); características Técnicas y métodos de prueba para equipos de radio para ser utilizados en el rango de frecuencia de 1 GHz hasta los 25 GHz

- **ETSI EN 300 674 V1.1.1.** Equipos y Sistemas de Radio (RES); Dispositivos de Rango Corto (SRD); teletransporte, características técnicas y métodos de test para comunicaciones de corto alcance, equipos de transmisión

(500Kbps/250Kbps) operando en la banda industrial científica y médica de los 5.8 GHz

- **ETSI ETS 300 683 ed.1.** Equipos y sistemas de Radio (RES) ; compatibilidad electromagnética estándar para dispositivos de corto alcance operando en las frecuencias comprendidas entre 9 KHz y 25 GHz

- **ETSI EN 300 761 V1.1.1.** Compatibilidad electromagnética y composición del espectro electromagnético (ERM); identificación automática de vehículos (AVI) para ferrocarriles.

- **ETSI EN 301 489.** Compatibilidad electromagnética y composición del espectro electromagnético (ERM); compatibilidad electromagnética estándar para equipos de radio.

- **ETSI EN302208.** Define los requerimientos y métodos de medida para equipos RFID operando en la banda de 865 a 868MHz con niveles de potencia de hasta 2W.

2.5.8 ERO (OFICINA EUROPEA DE RADIOCOMUNICACIONES)

- **ERC/DEC(91) 02.** Decisión ERC del 12 de Marzo del 2001 acerca de la armonización de frecuencias, características técnicas y excepción de la licencia individual de los dispositivos de rango pequeño sin especificar que operan en la banda de 26.957-27.238 MHz.

- **ERC/DEC(91) 03**. Decisión ERC del 12 de Marzo del 2001 acerca de la armonización de frecuencias, características técnicas y excepción de la licencia individual de los dispositivos de rango pequeño sin especificar que operan en la banda de 40.660-40.700 MHz.

- **ERC/DEC(91) 04.** Decisión ERC del 12 de Marzo del 2001 acerca de la armonización de frecuencias, características técnicas y excepción de la licencia individual de los dispositivos de rango pequeño sin especificar que operan en las bandas de frecuencia de 868.0-868.6 MHz, 868.7-869.2MHz, 869.4-869.65 MHz y 869.7-870.0 MHz.

- **ERC/DEC(91) 05.** Decisión ERC del 12 de Marzo del 2001 acerca de la armonización de frecuencias, características técnicas y excepción de la licencia individual de los dispositivos de rango pequeño sin especificar que operan en la banda de 2,400-2,483.5 MHz.

- **ERC/DEC(91) 08.** Decisión ERC del 12 de Marzo del 2001 acerca de la armonización de frecuencias, características técnicas y excepción de la licencia individual de los dispositivos de rango pequeño sin especificar utilizados para la detección y alerta del movimiento operando en la banda de frecuencia 2,400-2,483.5 MHz.

- **ERC/DEC(91) 13.** Decisión ERC del 12 de Marzo del 2001 acerca de la armonización de frecuencias, características técnicas y excepción de la licencia individual de los dispositivos de rango pequeño sin especificar utilizados para aplicaciones inductivas operando en las bandas de frecuencia 9-59.750 kHz, 59.750-60.250 KHz, 60.250-70 KHz, 70-119 KHz, 119-135 KHz.

- **ERC/DEC(91) 14.** Decisión ERC del 12 de Marzo del 2001 acerca de la armonización de frecuencias, características técnicas y excepción de la licencia individual de los dispositivos de rango pequeño sin especificar utilizados para aplicaciones inductivas operando en las bandas de frecuencia 6,765-6,795 kHz, 13.553-13.567 MHz.

- **ERC/DEC(91) 15.** Decisión ERC del 12 de Marzo del 2001 acerca de la armonización de frecuencias, características técnicas y excepción de la licencia individual de los dispositivos de rango pequeño sin especificar

utilizados para aplicaciones inductivas operando en la banda de frecuencia 7,400-8,800 kHz.

- **ERC/DEC(91) 16.** Decisión ERC del 12 de Marzo del 2001 acerca de la armonización de frecuencias, características técnicas y excepción de la licencia individual de los dispositivos de rango pequeño sin especificar utilizados para aplicaciones inductivas operando en la banda de frecuencia 26.957-27283 MHz.

- **ERC/DEC(92) 02.** Decisión ERC del 22 de Octubre de 1992 sobre las bandas de frecuencia a ser designadas para la introducción coordinada de sistemas telemáticos de transporte de carretera.

- **ERC/REC 70-03.** Procedimiento para reconocimiento mutuo de tipo probatorio y de tipo aprobado por el equipo de radio.

- **ERC/REC 70-03.** Relacionada a la utilización de dispositivos de rango pequeño (SRD).

2.5.9 LA INICIATIVA DE ENTRADA DE LOS SERVICIOS ABIERTOS

La especificación de esta organización popular consistente de 60 compañías miembros) no es un RFID específico, pero puede ser utilizado para manejar los sistemas y controladoras de borde RFID. Lo siguiente resume los aspectos principales de esta organización y su especificación en la plataforma de servicio:

La Iniciativa de entrada de los servicios abiertos (OSGi) fue fundada en Marzo de 1999. Su misión es crear especificaciones abiertas para la entrega en red de servicios dirigidos a dispositivos y redes locales. La especificación de la plataforma de servicios de OSGi provee una arquitectura común abierta para proveedores de servicio, desarrolladores, vendedores de software, operadores de entrada y vendedores de equipos para desarrollar, utilizar y dirigir servicios en una

manera coordinada. Éste habilita completamente una nueva categoría de dispositivos debido a su utilización flexible y manejable de servicios. Los destinos primarios para las especificaciones OSGi son establecer casillas superiores, entradas, cable módems, electrónica del consumidor, computadores personales, carros y más. Estos dispositivos que implementan las especificaciones OSGi permitirán a los proveedores del servicio como telcos, operadores de cable, servicios públicos, y otros para entregar servicios valiosos y diferenciados sobre sus redes.

2.6 RFID FRENTE A OTRAS TECNOLOGIAS DE IDENTIFICACION

Existen muchos tipos de tecnologías de identificación. Sin embargo, la tecnología de identificación más usada y la más conocida es el código de barras la misma que se la estudio a detalle en el capítulo I. En esta sección se realizará un análisis comparativo entre estas dos tecnologías de identificación.

La tecnología RFID está en el mercado como una versión mejorada o más inteligente del código de barras. Los medios de comunicación afirman que los días del código de barras están contados y que la tecnología RFID lo remplazará pronto. De hecho, la tecnología RFID tiene algunas ventajas sobre el código de barras, pero el mismo también ofrece ciertas ventajas sobre la tecnología RFID.

2.6.1 BENEFICIOS DEL CÓDIGO DE BARRAS

Entre los mayores beneficios del código de barras describimos los siguientes:

- **Recolección de datos rápida y certera.** Un código de barras automatiza la recolección de datos. Utilizando lectores láser, se puede escanear algunos códigos de barras en un periodo de tiempo corto. La lectura de los códigos es precisa, con un promedio de error de uno en tres millones de lecturas.

- **Eficiencia en operaciones incrementadas**. La información decodificada por un lector de código de barras puede ser alimentada directamente a una aplicación en un sistema. Por lo tanto, se puede automatizar varias operaciones, tales como recuperación de precios, identificación personal (por ejemplo; miembros de una biblioteca), monitoreo de inventario y control entre otros.
- **Costos de operación más bajos**. El código de barras ofrece ahorros en el costo mediante la reducción de errores al momento de recolectar la información, y eliminar procesos ineficaces.

2.6.2 DESVENTAJAS DEL CÓDIGO DE BARRAS

Las desventajas más grandes del código de barras están descritas a continuación.

- **Se dañan fácilmente**. Un código de barras se puede dañar fácilmente debido a causas tales como el polvo, pintura, detenimientos debido a la exposición a la luz del sol o humedad.
- **Las operaciones de los lectores puede verse afectadas por la humedad en el ambiente**. Los rayos de un lector son refractados mediante partículas de agua suspendidas en el ambiente, lo que da lugar a la distorsión de enfoque. Por lo tanto este lector puede experimentar una pérdida en la eficacia de la lectura.
- **Presencia de obstáculos.** Un código de barras necesita tener línea de vista hacia el código de barras que se supone va a leer. Cualquier obstáculo entre el lector y el código de barras puede evitar que la lectura del mismo se realice.
- **Velocidad.** Un lector de código de barras no puede ser capaz de leer todos los códigos si éstos se mueven a alta velocidad (por ejemplo, cuando la tasa del lector es excedida por la velocidad de movimiento de los códigos de barras).

2.6.3 VENTAJAS DE LA TECNOLOGÍA RFID

Las ventajas de la tecnología RFID pueden ser ampliamente clasificadas dentro de los siguientes tipos.

- **Actual.** Ventajas de productos tecnológicos que existen actualmente.
- **Futuro.** Ventajas que están disponibles en la actualidad o estarán disponibles como características mejoradas en cuanto la tecnología avance.

Estos no son terminologías oficiales, pero son utilizados por lo conveniente de su uso y para ayudar a comprender de mejor manera los beneficios. La siguiente lista cubre las dos ventajas, y a continuación se describe cuanto beneficio está disponible hoy en día en contraste a cuanto beneficio estará disponible en el futuro:

- **Sin contacto**. Una etiqueta RFID se puede leer sin ningún contacto físico entre la etiqueta y el lector.
- **Escritura de datos**. La información de una etiqueta RFID (reader / writer) puede ser re-escrita una gran cantidad de veces.
- **Ausencia de línea de vista**. Una línea de vista no es generalmente requerida por un lector RFID para leer una etiqueta.
- **Variedad de rangos de lectura**. Una etiqueta RFID puede tener rangos de lectura tan pequeños como de unas pocas pulgadas de distancia hasta de más de 100 pies.
- **Rango de datos de amplia capacidad.** RFID puede almacenar desde pocos bytes hasta una gran cantidad de datos.
- **Soporte para lectura de múltiples etiquetas.** Esto es posible utilizarlo en un lector RFID el mismo que estará en capacidad de leer todas las etiquetas que se encuentran en su zona de cobertura por un cierto periodo de tiempo.
- **Rugged.** Una etiqueta puede sufrir alteraciones en su estructura dependiendo del ambiente en el que se encuentre.

- **Tareas de desempeño inteligente.** La etiqueta a más de ser un portador y transmisor de datos, en RFID la etiqueta puede estar diseñada también para realizar otras tareas.

La siguiente característica es más bien un beneficio y no una ventaja de RFID.

- **Eficacia de lectura.** RFID tiene el 100% de precisión.

2.6.3.1 Sin contacto

Las etiquetas RFID no necesitan establecer un contacto físico con el lector para transmitir los datos, lo que provee ventajas desde las siguientes perspectivas.

- Ausencia de desgaste
- No reduce la velocidad de operación
- Lectura automática de varias etiquetas en un corto período de tiempo

2.6.3.2 Escritura de datos

Las etiquetas RFID RW que están actualmente disponibles pueden ser rescritas desde 10,000 hasta 100,000 veces o más, aunque el uso de este tipo de etiquetas está actualmente limitado comparado con las etiquetas WORM, actualmente no existe un amplio uso de estas etiquetas por las siguientes razones:

- Justificación comercial acerca del reciclaje de etiquetas
- Problemas de seguridad
- Necesidad de escritura dinámica
- Velocidad de operación más lenta

2.6.3.3 Ausencia de línea de vista

La ausencia de línea de vista es probablemente la característica más distintiva de la tecnología RFID. Un lector RFID puede leer una etiqueta a través de materiales que obstruyan como son los RF–lucent para la frecuencia usada. Por ejemplo, si una etiqueta es ubicada dentro de una caja, un lector operando en UHF puede leer la misma aún si la caja está sellada por todos los lados. Esta capacidad prueba cuán servicial puede ser la tecnología RFID para inspeccionar el

contenido de un contenedor sin ni siquiera abrirlo. Esta característica de la tecnología RFID tiene implicaciones pues infringe los derechos de privacidad, en caso de que una persona está llenando alguna información sin el consentimiento de otra persona. Si esta información personal está asociada con los ítems de la información etiquetada (por ejemplo al punto de venta) puede ser posible acceder a esta información (usando un aplicación adecuada) sin el consentimiento de la persona, lo cual puede constituirse en una violación de los derechos de privacidad. Para prevenir esto, un lector debería no leer estas etiquetas hasta que la venta sea realizada, o bajo la explícita necesidad o autorización por parte del comprador. Hay ciertas maneras de lograr este objetivo, una de ellas puede ser el bloqueo de etiquetas dentro de un rango de alcance del lector. Hay que notar que en algunas situaciones una línea de vista es necesaria para ayudar a configurar la distancia de lectura de las etiquetas, la energía del lector y la antena para establecer el contacto ambiental. Estas situaciones implican la presencia de etiquetas UHF y una gran cantidad de materiales reflectivos, tales como metales, en el ambiente de operación dando lugar al multipath. Por ejemplo, consideremos una línea de producción de maquinaria donde virtualmente todo está hecho de metal. Una gran cantidad de energía RF por parte de los lectores instalada en este medio obtiene refección por parte de los objetos en el medio ambiente. En este caso, para lograr una lectura de buena calidad, una etiqueta y un lector deben ser ubicados de tal manera que no haya obstáculos entre ellos.

2.6.3.4 Variedad de rangos de lectura

"Una etiqueta de baja frecuencia RFID generalmente tiene una distancia de lectura de unas pocas pulgadas; para una tarjeta pasiva de baja frecuencia, la distancia es de cerca de tres pies." [53] La distancia de lectura de una etiqueta

[53] http://wireless.itworld.com/4985/051004_book_rfidsourcebook/page_2.html

pasiva de UHF es de aproximadamente 30 pies. Una etiqueta activa de UHF (por ejemplo, de 433 MHZ) puede leer a una distancia de 300 pies y una etiqueta activa en el rango de GHz puede tener una distancia de lectura de más de 100 pies. Estas distancias de lectura se realizan usualmente bajo condiciones ideales. Por lo tanto, la distancia de lectura de una etiqueta de un sistema RFID en la realidad puede ser sustancialmente menor a estas cifras. Por ejemplo, la distancia de lectura de una etiqueta de 13.56 MHz en general no excede más que unas cuantas pulgadas. Esta amplia cantidad de lecturas hace posible aplicar la tecnología RFID en una amplia variedad de aplicaciones.

Hoy en día, las etiquetas para cada tipo de frecuencia están comercialmente disponibles. Además, la localización de una etiqueta activa o pasiva puede estar asociada con el lector que la lee. Por lo tanto, si un lector instalado en cierta puerta de un muelle de un almacén lee la etiqueta que se encuentra en su zona de acción, la localización de esta etiqueta se asume esté en la puerta al momento de la lectura. Esta información de localización puede entonces ser accesible privadamente o a través de una red pública. (Por ejemplo el Internet) en una amplia área geográfica. Como resultado, la etiqueta puede ser leída a miles de millas de distancia desde su posición real. Futuros avances en la tecnología tendrán un limitado impacto en este aspecto porque el rango de distancia de lectura total es usado utilizando medios directos (a través del lector) e indirectos (a través de una red). Por esta razón, esta característica es una ventaja de la tecnología RFID.

2.6.3.5 Rango de datos de amplia capacidad

"Una etiqueta pasiva puede obtener unos pocos bits de almacenamiento de datos hasta cientos de bits de capacidad." [54] Por ejemplo, las series pasivas ME- Y

[54] RFID JOURNAL; Editorial Mark Roberti Vol. 5, Nº3, Junio 2008, Pág.19

2000, las etiquetas en miniatura RW de Maxell operando en el rango de 13.56 MHz pueden llevar hasta 4 Kbytes de información dentro de su espacio de 2.5 X 2.5 milímetros.

Una etiqueta activa teóricamente no tiene límite de almacenamiento porque las dimensiones físicas y capacidades de la misma no son limitadas.

Hay dos acercamientos para el uso de una etiqueta RFID. La primera almacena solamente un número de identificación en la etiqueta, similar a la placa de un automóvil que únicamente identifica al objeto etiquetado; la segunda almacena dos partes: un único número de identificadores y los datos relacionados con un objeto etiquetado. Un gran número de identificadores únicos puede ser generado con un número relativamente pequeño de bits. Por ejemplo, utilizando 96 bits, un total de 80,000 trillones de trillón de identificadores únicos pueden ser generados Por lo tanto, un número relativamente bajo de bits es suficiente para etiquetar virtualmente cualquier objeto en el mundo. Una etiqueta de memoria de alta capacidad será más cara que las tarjetas que pueden almacenar solamente a un solo identificador. Por lo tanto, solo porque ésta esté disponible, usar una memoria de alta capacidad en una aplicación no parece ser una buena idea a no ser de que la aplicación así lo requiera (especialmente para aplicaciones que tienen un tiempo específico para realizar una tarea). Una etiqueta activa, sin embargo, utiliza una gran capacidad de almacenamiento de soporte para sus tareas. Una pequeña cantidad de la cual, más probablemente contiene los resultados de estas tareas, las cuales pueden ser transmitidas por esta etiqueta (lo cual es perfectamente aceptable puesto que esta información es dinámica y sólo puede ser determinada por la etiqueta misma mediante el escaneo de su medio).

Este es un futuro beneficio. La mayoría de las tarjetas disponibles en el mercado hoy en día están restringidas en el tamaño de la memoria. Estas tarjetas son utilizadas en aplicaciones de “disco de licencia”, y por lo tanto prueban ser adecuadas para la tarea a realizar. Las tarjetas con una mayor cantidad de memoria estarán disponibles en el futuro.

2.6.3.6 Soporte para lectura de múltiples etiquetas

El soporte para estas etiquetas se clasifica como uno de los beneficios más importantes de la tecnología RFID. Utilizando un algoritmo anti-colisión, un lector RFID puede automáticamente leer algunas tarjetas en su zona de lectura en un periodo corto de tiempo. Generalmente, utilizando este esquema un lector puede únicamente identificar de pocas a algunas etiquetas por segundo dependiendo de las etiquetas y la aplicación. Este beneficio permite que la información de una colección de objetos etiquetados, sean estáticos o en movimiento (dentro de los límites del lector), puedan ser leídos por un lector, obviando la necesidad de leer uno a la vez. Consideremos por ejemplo una de las tareas clásicas de una institución financiera: contar un paquete de billetes para determinar su valor total. Asumiendo que estos billetes tienen una etiqueta, la información de estas puede ser leída utilizando un lector RFID, el cual puede ser utilizado entonces para determinar el valor de los billetes en total en un periodo corto de tiempo, automáticamente. Este método es mucho más eficiente comparado al método tradicional de contar en forma manual. Ahora consideremos otro ejemplo clásico: cargar un camión con contenedores de mercadería en un puerto de embarque y la recepción del mismo en otro puerto. Generalmente, para esta clase de aplicaciones, ni las cajas están inventariadas en lo absoluto utilizando códigos de barras (tarea manual y que lleva mucho tiempo). Como resultado, un negocio puede perder una considerable cantidad de dinero en el proceso de inventariar la mercadería. Si es que las etiquetas RFID pueden ser aplicadas a las cajas antes de que sean embarcadas se usará un lector estático ubicado cerca del camión de carga. Así, el negocio puede tener una lista muy bien detallada de los ítems que son embarcados a un distribuidor o a un vendedor. Además, significativos costos de mano de obra serán ahorrados eliminando el escaneo manual de las etiquetas, que podría haber sido inevitable si la tecnología de código de barras hubiese sido utilizada. La información recogida de estas tarjetas puede ser chequeada sobre el orden actual para verificar si una caja debería ser cargada en el camión, reduciendo así el número de embarques inválidos. Como se puede comprender, esta ventaja particular de RFID puede acelerar y racionalizar las operaciones de negocios considerablemente.

Contraponiéndose a la creencia popular que dice que, un lector puede comunicarse localmente con sólo una etiqueta en su área de lectura a la vez. Si más de una etiqueta intenta comunicarse con el lector al mismo tiempo, ocurre lo que se conoce como "colisión de etiquetas". Un lector tiene que solucionar este problema para identificar apropiadamente todas las tarjetas en su área de lectura. Por lo tanto, un lector impone las reglas sobre la comunicación de tal manera que una sola tarjeta pueda comunicarse con el lector a la vez, en este periodo las otras etiquetas deben permanecer fuera de lectura. Eso es lo que se llama un algoritmo anticolisión. Hay que notar que hay una diferencia entre leer la información de una etiqueta en respuesta a un algoritmo anticolisión y leer la información de una etiqueta completamente. En el caso anterior, solo ciertos bits de información son leídos. Además, hay una teoría en cuanto a la limitación práctica acerca de cuántas etiquetas pueden ser identificadas por un lector dentro de un periodo de tiempo.

Este es un beneficio corriente, pero es posible que futuras mejoras en la tecnología de los lectores RFID puedan mejorar sustancialmente el número de etiquetas que puedan ser identificadas por segundo (dentro de los límites teóricos y prácticos).

2.6.3.7 Rugged

Una etiqueta pasiva RFID puede ser hecha para soportar condiciones de medios tales como calor, humedad, químicos corrosivos, vibración mecánica, etc. Por ejemplo, algunas etiquetas pasivas pueden soportar temperaturas que van de los 40℉ hasta los 400℉ (-40℃ hasta 204℃). Generalm ente estas etiquetas son hechas dependiendo de las condiciones de operación medio ambientales de una aplicación específica. Hoy en día, ni una sola etiqueta puede soportar todas las condiciones del ambiente. Una etiqueta activa y semiactiva que tiene un tablero electrónico con una batería es generalmente más susceptible al daño comparado con una etiqueta pasiva.

Este es un beneficio puesto que etiquetas con una variedad de resistencia a ambientes operacionales si están disponibles. Sin embargo, hay un amplio

espacio para las mejoras, y en cuanto la tecnología mejore, se espera que más etiquetas puedan resistir de mejor manera ambientes fuertes y que de hecho superen las presentes contrapartes. Por lo tanto, esto se podría también llamarse un futuro beneficio.

2.6.3.8 Tareas de desempeño inteligente

La electrónica y el abastecimiento de energía de una etiqueta activa puede ser utilizado para realizar tareas especializadas tales como monitorear el medio ambiente circundante (por ejemplo, detectar movimiento). La etiqueta puede ser entonces utilizada para determinar dinámicamente otros parámetros y transmitir esta información a un lector disponible. Por ejemplo, supongamos que una etiqueta activa está adherida a un artículo de alto valor para detección de robos: Asumamos que esta etiqueta activa tiene un sensor de movimiento. Si alguien intenta moverlo, la etiqueta detecta el movimiento y empieza a difundir el mismo en sus alrededores. Un lector puede recibir esta información y adelantar la información a un detector de robos. El cual a su vez puede activar una alarma para alertar al personal. Puede parecer que sólo por el hecho de levantar el objeto y volverlo a poner en el mismo sitio podría entorpecer la etiqueta y hacer pensar que el objeto está siendo movido otra vez. La etiqueta puede entonces enviar otro tipo de mensaje que signifique el evento en mención.

Este aspecto de la tecnología RFID tiene el más grande potencial para mejorar puesto que etiquetas activas con funciones especializadas están ya disponibles. De igual manera, éste también puede ser llamado un futuro beneficio.

2.6.3.9 Eficacia de Lectura

La lectura de etiquetas en RFID es mencionada como “muy certera” “100 por ciento correcta”, y así sucesivamente, pero ningún estudio objetivo muestra cuán certeras son las lecturas RFID. Sería definitivamente deseable sustentar estas declaraciones con información científica porque de hecho ninguna tecnología puede ofrecer un 100 por ciento de eficacia en todos los ambientes operacionales

y todo el tiempo. Factores sobre los cuales la eficacia de la lectura RFID depende de ciertos factores como los siguientes.

- **Tipo de etiqueta**. Qué etiquetas, a qué frecuencia están siendo usadas, el diseño de la antena de la etiqueta, son factores que pueden bajar el nivel de eficacia de un sistema RFID.

- **Los objetos etiquetados**. La composición del objeto, cómo está empacado, el material usado para empacarlo, entre otros juegan un papel importante al momento de la lectura y por ende en la eficacia de la misma. También se debe considerar que el impacto de este factor depende de la frecuencia del sistema RFID usado.

- **El medio de operación**. La interferencia de objetos móviles existentes, las descargas electroestáticas, la presencia de cuerpos de metal y líquidos, entre otros factores, pueden representar un problema para obtener una lectura eficaz en las frecuencias UHF y microondas.

- **La consistencia.** La orientación de la etiqueta y la ubicación relativa de las antenas del lector puede causar un impacto significativo en la eficacia de las lecturas.

Otro asunto con la tecnología RFID son las llamadas lecturas falsas o lecturas fantasmas. En esta situación al parecer información válida de la etiqueta es grabada por el lector por un período corto de tiempo. Después de este periodo de tiempo, la información de la etiqueta no puede ser leída por el lector. El problema surge cuando el lector recibe información errónea de la etiqueta, lo cual puede ocurrir por varias razones (como por ejemplo un protocolo de corrección de errores mal estructurado). Las lecturas fantasmas son “bugs” en el sistema de abastecimiento. Instalaciones incorrectas pueden también ser la causa de estos problemas. En general las lecturas fantasmas no son un problema. Sin embargo, esto muestra que determinar la eficacia de las lecturas RFID no es fácil, esta depende de algunos factores. Es posible que dos sistemas idénticos puedan

variar sus lecturas por condiciones del ambiente diferentes. Es posible que se pueda incrementar la eficacia de las lecturas y el grado de automatización de sistemas que están en existencia hoy en día.

Este es un beneficio debido a que algunas aplicaciones demuestran eficiencia para los requerimientos de un negocio. Sin embargo, la eficacia de la lectura RFID, tiene un buen potencial para mejorar con etiquetas mejoradas. De igual manera, que lectores y antenas para los mismos estén a disposición en el futuro, constituye un futuro beneficio.

2.6.4 LIMITACIONES DE LA TECNOLOGÍA RFID

La tecnología RFID no está libre de limitaciones. Cabe recalcar que algunas de las limitaciones existentes en la actualidad tienen un buen potencial ser solucionadas en cuanto la tecnología avance. Por lo que es aconsejable mirar estas limitaciones como oportunidades para soluciones creativas.
Las limitaciones de la tecnología se resumen de la siguiente manera.

- **Bajo rendimiento con materiales RF opacos y objetos absorbentes**.
  Este es un comportamiento dependiente de los materiales. La tecnología disponible no trabaja bien con estos materiales y en algunos casos falla completamente.
- **El impacto de factores ambientales**.
  Las condiciones del medio pueden impactar grandemente en las soluciones RFID.
- **Lectura limitada de etiquetas**.
  Un límite práctico se aplica al hecho de la cantidad de etiquetas que pueden ser leídas en un tiempo determinado.
- **Impacto por interferencia de Hardware**.
  Una solución RFID puede tener un impacto negativo con el hardware instalado (por ejemplo, la ubicación de la antena y la orientación de la misma).

- **Limitada penetración de energía de RF**.
  Aunque la tecnología RFID no necesita una línea de visión, hay un límite de que tanto la energía RF puede alcanzar, aún a través de objetos RF luminosos.
- **Tecnología en desarrollo**.
  Aunque es una buena noticia el hecho que la tecnología RFID esté rápidamente evolucionando, estos cambios pueden significar un inconveniente para quien no esté al tanto de los mismos.

A continuación se discuten cada una de estas limitaciones en detalle.

2.6.4.1 Bajo rendimiento con materiales RF opacos y objetos absorbentes.

Si son utilizadas frecuencias UHF y microonda, y si el objeto etiquetado es elaborado de un material RF opaco tal como metal, algún tipo de material absorbente como agua o si el objeto está empacado en un material opaco, un lector RFID puede fallar parcial o completamente al leer la información de la etiqueta. Están disponibles en el mercado etiquetas que alivian de alguna manera algunos los problemas de lectura para algunos tipos de material opacos y absorbentes. Además, el empacar se pueden presentar problemas si se lo hace utilizando materiales opacos tales como láminas de metal.

Se espera que las mejoras en la tecnología resuelvan algunos de los problemas que existen hoy en día y que están asociados a los materiales opacos y absorbentes.

2.6.4.2 El impacto de factores ambientales.

Si el medio en el que se opera tiene grandes cantidades de metal, líquidos entre otros. Éstos pueden afectar la eficacia de la lectura de las etiquetas, dependiendo de la frecuencia. La reflexión de las señales del lector de la antena sobre objetos opacos causa lo que se conoce como multipath. Es aconsejable en estos tipos de medios operacionales, proveer una línea directa de visión del lector a las etiquetas. Aunque la distancia de lectura de las etiquetas, la energía del lector, y la configuración de la antena sean parámetros más grandes que necesitan ser

configurados en estos casos para contrarrestar el impacto del ambiente, una línea de vista ayuda a lograr esta configuración. En algunos casos, sin embargo, esto no puede ser posible (por ejemplo, en un ambiente operacional donde hay una gran cantidad de tráfico humano). El cuerpo humano posee una gran cantidad de agua, la cual se constituye en una material absorbente en frecuencia UHF y microonda. Por lo tanto, cuando una persona se encuentra entre una etiqueta y el lector es posible que este no pueda realizar la lectura hasta que la persona se aleje de la etiqueta. Por lo tanto, en este caso una seria degradación del rendimiento de puede ocurrir. Además, la existencia de casi todo tipo de conexión en una red inalámbrica dentro del ambiente operacional puede interferir con el trabajo del lector. Motores eléctricos y controladores de motor puede también ser una fuente de ruido que impacta en el desempeño del lector. Algunas wireless LANs inalámbricas en el rango de los 900 MHz pueden interferir con los lectores.

Es probable que estos inconvenientes se mantengan por algún tiempo. Algunos de estos problemas pueden de igual manera permanecer sin solución.

2.6.4.3 Lectura limitada de etiquetas.

El número de etiquetas que un lector puede leer por unidad de tiempo (por ejemplo por segundo) es limitado. Por ejemplo, hoy en día un lector en promedio puede identificar algunas etiquetas por segundo. Para alcanzar este número, este lector tiene que leer las respuestas de las etiquetas algunos cientos de veces por segundo, debido a que el lector tiene que emplear algún algoritmo de anticolisión para identificar estas etiquetas.

La mejoras en la tecnología de los lectores indudablemente incrementara la cantidad de etiquetas que puedan ser identificadas por unidad de tiempo, pero siempre habrá un tope el cual el lector no podrá exceder.

2.6.4.4 Impacto por interferencia de HARDWARE.

En el caso de estar mal colocados los lectores pueden presentarse una colisión del lector. Este problema ocurre cuando las áreas de cobertura de dos lectores coinciden y la señal de uno de estos interfiere en el área de lectura del otro lector. Este problema debe ser tomado en cuenta cuando la instalación de los lectores ha sido muy mal planificada. Por otro lado, la degradación en el rendimiento del lector puede ocurrir.

De alguna manera este problema puede ser solucionado hoy en día haciendo uso de TDMA (Acceso múltiple por división de tiempo). Esta técnica permite a los lectores funcionar en tiempos diferentes antes que ambos al mismo tiempo. Como resultado de esto, los lectores no interfieren más entre ellos. Sin embargo, una etiqueta ubicada en el área común de los dos lectores puede ser leída dos veces. Por lo tanto, las aplicaciones RFID deben tener un mecanismo de filtro para eliminar la duplicación de lectura de etiquetas.

2.6.4.5 Limitada penetración de energía de RF.

Este factor depende de la potencia de transmisión del lector y del ciclo de vida, los cuales están regulados en algunos países alrededor del mundo. Por ejemplo, un lector puede fallar al leer en algunos casos en el que las cajas están apiladas. Aún si las cajas están hechas de un material RF luminoso para la frecuencia utilizada. La respuesta a cuántas cajas pueden apilarse para tener una lectura eficiente se la puede obtener luego de la experimentación con cajas reales apiladas en un medio real de operación utilizando hardware RFID real. Esta cantidad puede además variar de país a país, dependiendo de las restricciones de la potencia de emisión del lector y el ciclo de vida, por lo tanto, la respuesta necesita ser determinada bajo la experimentación.

Desafortunadamente, esta limitación permanecerá en tanto las restricciones internacionales sobre la potencia de emisión del lector y del ciclo de vida permanezcan. Por lo tanto, si se necesita desplegar una solución en diferentes países, se debe considerar muy seriamente este problema.

2.6.4.6 Tecnología en desarrollo.

La tecnología en desarrollo es un problema práctico que enfrenta la tecnología RFID hoy en día. Una solución RFID en relación al hardware está disponible en el mercado. Los fabricantes están haciendo su mejor esfuerzo para desarrollar productos mejorados, pero productos cien por ciento mejorados no estarán disponibles por algún tiempo. Por ejemplo, no es común que se dañen etiquetas UHF pasivas normalmente utilizadas en cadenas de almacenamiento con tasas de error aproximadas al 20 por ciento.

Los mismos tipos de etiquetas (por ejemplo de 915 MHz para metales) de diferentes fabricantes pueden tener un desempeño diferente. Es posible que una etiqueta que brinde una lectura eficaz para una aplicación específica no esté actualmente disponible.

Los lectores han tenido una larga evolución en los últimos años, gradualmente se han ido transformando de simples interrogadores a aparatos de red bien definidos con una inteligencia propia para dar soporte a diversas funciones que necesita una aplicación RFID. Algunas de estas funciones son el filtrar la información, almacenar lecturas recientes, alimentaciones de sensores externos, entre otros. De igual forma, la tecnología está haciendo antenas mucho más pequeñas y baratas. Sin embargo, un efecto de estos avances es que el nuevo hardware RFID está saliendo muy rápidamente lo que también implica que los negocios igualmente tengan que actualizar sus equipos en periodos de tiempo cortos. Dichas actualizaciones no son generalmente necesarias debido a que los productos tienen respaldo en la mayoría de los casos. Los negocios tienen que implementar soluciones reales de manera que la inversión en hardware RFID no constituya un gasto al tener que realizar actualizaciones en periodos de tiempo corto.

Este problema seguirá siendo parte de esta tecnología en un futuro cercano. La estabilización de la tecnología en términos de productos y estándares

globalmente aceptables erradicara el problema, sin embargo hacer una predicción de cuándo esto sucederá es una tarea bastante difícil.

2.6.5 VENTAJAS DE RFID SOBRE EL CÓDIGO DE BARRAS.

Las ventajas de la tecnología RFID sobre el código de barras son las siguientes:

- **Soporte de información no estática**.
  Una etiqueta RFID puede ser re-escrita algunas veces (asumiendo por supuesto que la etiqueta es RW). La información en un código de barras es estática y no puede ser cambiada.
- **No necesita línea de vista**.
  Generalmente, un lector RFID no necesita una línea de vista para leer la información de una etiqueta RFID. Un lector de código de barras si necesita línea de vista para leer el código.
- **Rango más amplio de lectura**.
  Una etiqueta RFID puede tener un rango más amplio de lectura que el de un código de barras. Dependiendo de algunos factores, éste puede ir desde unos pocos pies a unos cientos de pies.
- **Capacidad de almacenamiento más grande**.
  Una etiqueta RFID puede almacenar mayor información que un código de barras.
- **Lecturas múltiples**.
  Un lector apropiado puede leer algunas etiquetas RFID dentro de un corto período de tiempo, automáticamente, utilizando una característica llamada anti-colisión. Un código de barras, sin embargo, puede solamente escanear un código a la vez.
- **Sostenibilidad.**
  Una etiqueta RFID es generalmente resistente a ambientes operaciones severos. Un código de barras se daña fácilmente (por ejemplo, debido a la humedad o el polvo).
- **Comportamiento inteligente**.
  Una etiqueta RFID puede ser usada para realizar otras tareas además de simplemente ser un acarreador y transportador de datos. Un código de

barras, sin embargo, no tiene inteligencia y es sólo un vehículo para almacenar datos.

Los siguientes, aunque a menudo son mencionados en los medios, son dudosos y por lo tanto no son considerados como claras ventajas de la tecnología RFID sobre los códigos de barras.

- **Eficacia en la lectura**.
  La tecnología RFID es mucho más eficiente que la tecnología de código de barras.
- **Soporte para etiquetado a nivel de ítem**.
  Un código de barras no brinda soporte en este tipo de circunstancia.

Las siguientes secciones discuten estos puntos de una manera más detallada.

2.6.5.1 Soporte de información no estática.

"Se puede re-escribir la información en una etiqueta RFID reader/writer muchas veces. En general se puede re-escribir por lo menos unas 10,000 veces, el re-escribir se hace útil si se usa la etiqueta para grabar información que no estaba disponible cuando fue creada." [55] Una etiqueta se crea cuando alguna información es inicialmente escrita sobre esta para ser utilizada. Esta información pueden ser unas capas de identificación que permiten identificar esta etiqueta de todo el grupo de posibles etiquetas. Otro tipo de información adicional (generalmente acerca del objeto sobre el cual esta etiqueta está fijado) es también posible. La necesidad de re-escribir la información en la etiqueta

[55] GLOVER Bill; RFID Essentials; Editorial O Reilly, 2006, Pág. 57

depende de la aplicación para la cual la etiqueta es usada. Por ejemplo, supongamos que una etiqueta R/W está fijada a un ítem que está siendo construido en cuanto pasa por la línea de producción, el tiempo que se toma en completar cada fase puede ser almacenado en la etiqueta. Finalmente, cuando el ítem ha sido terminado, la información grabada en la etiqueta puede ser ultimada para analizar, por ejemplo, los retrasos en la línea de producción (esto quiere decir, los lugares en donde el ítem pasa más tiempo mientras está siendo manufacturado). Además, si una etiqueta RFID necesita ser recicladas en una aplicación, la información previa puede necesitar ser re–escrita junto con la nueva información.

Un código de barras, en contraste, puede solamente almacenar información estática (información que no puede ser re-rescrita con información nueva): Un nuevo código de barra tiene que ser creado cada vez que se desee almacenar nueva información.

2.6.5.2 No necesita línea de vista.

Una de las ventajas de la tecnología RFID es que no necesita una línea de vista. El lector no necesita ver la etiqueta para leer su información. En algunas situaciones, sin embargo esto no es del todo verdad. En estas situaciones, se debe establecer una línea de visión entre el lector y la etiqueta para que la información sea leída en forma confiable. (Aunque el establecer una línea de visión no garantiza mejor lectura, ayuda a configurar los factores críticos tales como la distancia, la energía del lector, y la posición de la antena lectora para contar el impacto ambiental). Si hay una significativa cantidad de materiales reflectivos en el ambiente operacional, se utilizan las etiquetas de UHF. Un clásico ejemplo es una línea de producción de automóviles, donde esencialmente todo es hecho de metal y hay un alto grado de ondas reflectivas en el medio. Si una etiqueta UHF/ RFID está ubicada en un vehículo que está en la línea de producción, la etiqueta y los lectores deben estar ubicados de tal manera que la línea de visión pueda ser claramente establecida en los puntos donde las lecturas

van a tener lugar para evitar señales multipath, en este caso RFID no ofrece ninguna ventaja sobre el código de barras.

Un lector de código de barras necesita siempre de una clara línea de visión para escanear un código. Por lo tanto, puede desempeñarse pobremente en algunas aplicaciones típicas, tales como en manejo de equipaje en las aerolíneas, donde los objetos etiquetados están orientados al azar en el cinturón de equipajes. En este escenario, hay una buena posibilidad de que coincidentes equipajes obstruyan la línea de visión a un código o a otros equipajes. Además, un código de barras en una maleta puede estar orientado de tal manera que el lector de código de barras no pueda leerlo. Estos factores conducirán a un pobre desempeño. Por el contrario si se utilizan etiquetas y lectores RFID apropiados la orientación de la etiqueta no puede tener un impacto significativo en comparación a los códigos de barras. Además, debido a que la línea de vista no es necesaria, la mayoría de estas etiquetas pueden ser leídas a través de equipajes coincidentes. Por lo tanto, la eficacia de lectura RFID es sustancialmente mayor que la lectura con código de barras.

2.6.5.3 Rango más amplio de lectura.

Una etiqueta pasiva RFID operando en el rango UHF tiene un rango de lectura aproximado de 30 pies (9 metros) bajo condiciones ideales. Una etiqueta activa en el rango bajo UHF (433 MHz) tiene un rango de lectura aproximado de 300 pies (91 metros): Una etiqueta activa operando en el rango de 2.45 GHz tiene un rango de lectura de más de 100 pies (30.5 metros).

El principio de lectura del código de barras está atado a la óptica, y la lectura del rango de un lector de código de barras depende del rango focal del lector, el rango de lectura de los lectores comercialmente disponibles es de 30 pies o menos.

2.6.5.4 Capacidad de almacenamiento más grande.

Un código de barras de dos dimensiones, como el azteca, puede codificar hasta 3750 caracteres de información de un total de 256 caracteres ASCII, lo cual es

sustancial. Hoy en día no existe una gran diferencia en la capacidad de información en cuanto a lo que las etiquetas pasivas se refieren, pero esto puede cambiar en el futuro. Las etiquetas comerciales activas, teóricamente, tienen una ilimitada capacidad de almacenar información.

Una etiqueta activa con una gran cantidad de memoria es una ventaja ya que puede realizar tareas especializadas. Pero en lo referente a la cantidad de información transmitida, el tiempo de transmisión y la tasa de error crecen con la cantidad de datos transmitidos.

2.6.5.5 Lecturas múltiples.

Un lector RFID puede automáticamente identificar de unas pocas a algunas etiquetas en su zona de lectura en un periodo de tiempo corto. Esta capacidad de identificar automáticamente múltiples etiquetas acelera las operaciones de lectura de las etiquetas.

Un lector de código de barras puede solamente leer un código a la vez, lo cual significa un mayor tiempo de lectura de estos códigos en relación al mismo número de etiquetas RFID leídas con un lector con esta misma tecnología.

2.6.5.6 Sostenibilidad.

Una etiqueta RFID puede sobrellevar condiciones ambientales difíciles tales como calor, humedad, químicos corrosivos, vibración mecánica, todo esto en un grado aceptable. Generalmente, una etiqueta en particular de un fabricante específico es resistente a una o a varias de estas condiciones.

Un código de barras es tan bueno como el material en el cual está impreso. Por lo tanto, un código de barras impreso en papel se daña fácilmente en presencia de humedad o calor. Un código de barras puede dañarse en presencia de humedad, calor y no puede soportar altas temperaturas.

2.6.5.7 Comportamiento inteligente.

Una etiqueta activa RFID puede llevar componentes electrónicos y una batería para ejecutar funciones tales como monitorear la temperatura del medio, humedad entre otras. La etiqueta puede entonces utilizar esta información para calcular dinámicamente otros parámetros y transmitirlos a un lector adecuado.

En contraste, un código de barras es sólo un depósito de información estática y nada más.

2.6.5.8 Eficacia en la lectura.

Retomando el problema de la eficacia en la lectura. Una teoría muy común hoy en día es que la tecnología RFID es mucho más precisa que el código de barras. Sin embargo, esta teoría tiene dos problemas. Mediante la presencia de datos valederos acerca de la precisión del código de barras, no es legal decir que la tecnología RFID es mucho más precisa que el código de barras.

En un estudio realizado acerca de la precisión del código de barras realizado por la Universidad de Ohio, el peor de los márgenes de error fue de 1 por 10.5 millones; el mejor margen de error fue de 1 por 612.9 millones de lecturas. La precisión de las lecturas de códigos de barras está típicamente en el rango del 90 por ciento o más. Por lo tanto la ventaja acerca de la precisión en la tecnología RFID sobre el código de barras parece igual o menor al 10 por ciento para ciertos tipos de soluciones. En algunas situaciones, esto puede difícilmente ser llamada una diferencia sustancial, asumiendo por supuesto, que la tecnología RFID de hecho incrementará el margen de precisión a este nivel. Si el medio no es el apropiado para la tecnología RFID, la mejora del rango de precisión utilizando la tecnología RFID sobre el código de barras puede ser de cero. Luego entonces otra vez, dependiendo de la aplicación, la tecnología RFID puede ofrecer beneficios superiores al 10 por ciento, como por ejemplo en el manejo de equipaje en una aerolínea. Además, para una aplicación en particular, un

incremento de un par de puntos en porcentaje de mejora puede traer un valor sustancial a los negocios.

2.6.5.9 Soporte para etiquetado a nivel de ítem.

Parece ser una creencia creciente el hecho de que solamente la tecnología RFID puede soportar el etiquetado a nivel de ítem, mientras que el código de barras no puede hacerlo. Esto no es verdad. Diferentes tipos de códigos de barras tienen una capacidad para almacenar información. El código de barras lineal es utilizado más ampliamente para este nivel de etiquetado (por ejemplo, UPC) no tiene suficiente almacenamiento para identificar a un solo ítem. Sin embargo, otros tipos de códigos de barras, de ser usados, tienen más que suficientes caracteres para identificar un solo ítem. Por ejemplo asumiendo el almacenamiento de datos alfanumérico, la matriz de datos puede almacenar hasta 3,116 bytes; el Azteca 3,750 bytes; y el PDF417 1,850 bytes. Estas capacidades son más que suficientes para contener un número de 1,024 bits, el cual por sí mismo es más que suficiente para identificar un ítem en particular.

En este punto, se puede pensar que, con tantas ventajas, la tecnología RFID es la clara ganadora sobre el código de barras. Mantengamos este pensamiento. Aunque la tecnología RFID tiene algunas ventajas sobre el código de barras, la siguiente sección describe las ventajas que tiene el código de barras sobre la tecnología RFID.

2.6.6 VENTAJAS DEL CÓDIGO DE BARRAS SOBRE LA TECNOLOGÍA RFID.

Las ventajas de los códigos de barras sobre la tecnología RFID son las siguientes:

- **Bajo costo.**

  El costo de implementar una solución de código de barras es generalmente menor a la de una solución RFID.

- **Tasas de precisión comparables**.
  En algunos casos, la precisión de las soluciones empleando códigos de barras es casi la misma, si no mejor comparada a una solución RFID.
- **Independencia por el tipo de material**.
  Un sistema de código de barras puede ser usado para etiquetar exitosamente casi en cualquier material.
- **Ausencia de restricciones internacionales**.
  Los sistemas de código de barras son utilizados en todo el mundo sin ninguna limitación legal sobre el uso de esta tecnología.
- **Ausencia de problemas sociales**.
  Hoy en día, se puede encontrar códigos de barras para casi cualquier ítem en el planeta.
- **Tecnología ya desarrollada con gran base instalada**.
  La tecnología de código de barras es probablemente la más utilizada en el mundo.

La siguiente sección discute estos puntos en detalle.

2.6.6.1 Bajo costo.

El costo de un código de barras es casi cero, mientras que el costo de una etiqueta RFID es de cerca de 20 centavos o más para etiquetas UHF cuando son compradas en grandes cantidades. Además, el precio promedio de un lector de código de barras manual es de menos de 400 dólares, el costo de un lector manual de tecnología RFID es de más de 800 dólares para lectores UHF. De igual manera, los lectores de códigos de barras estáticos en promedio cuestan menos de 700 dólares, mientras que los lectores RFID cuestan más de 900 dólares para lectores UHF. Para lectores manuales y estáticos de 13.56 Mhz, el costo es generalmente menor que los lectores de UHF. Pero las etiquetas de 13.56 Mhz son generalmente más caras. Para la tecnología RFID se requiere hardware adicional como lo son las antenas para el lector. El costo de una antena RFID típicamente oscila entre los 150 y los 500 dólares. También existen antenas más caras. Por otro lado para tener una buena calidad y un alto rango de

lectura en el código de barras se puede utilizar lectores de códigos estacionarios cuyo valor puede oscilar entre unos miles de dólares. Sin embargo, estos lectores de códigos de barras caros pueden no ser necesarios para una aplicación típica. Aún asumiendo la diferencia de costo entre los lectores de códigos de barras de más alto precio y el más barato de los lectores, antenas y el costo de las etiquetas RFID excederá cualquier ahorro logrado, pero esta comparación en tan sólo a nivel de costos de equipos que se requieren para implementar la infraestructura física de estas tecnologías, pero no hay que dejar de lado los beneficios que puede ofrecer la tecnología RFID tal como se lo analizó en las secciones anteriores.

2.6.6.2 Porcentajes de efectividad comparable.

Los sistemas de código de barras actuales, instalados en sistemas de producción tienen generalmente una alta efectividad de lectura. La efectividad de lectura en el rango del 90 por ciento es común, una efectividad del 98 por ciento no es tan común. Sin embargo, para estos tipos de aplicaciones, RFID no puede ofrecer más de un 10 por ciento de incremento en la efectividad, asumiendo, por supuesto, un sistema equivalente RFID que en realidad trabajará mejor. Dependiendo del ambiente de operaciones y de otros factores, tales como el material del objeto etiquetado y el tipo de contenido una solución RFID en realidad lo haría peor que la solución de código de barras equivalente.

2.6.6.3 No es afectado por el Tipo de Material.

Un código de barras puede ser puesto sobre un objeto hecho de casi cualquier material, sin tener en cuenta de que si es un RF lucent o un RF opaco para la respectiva frecuencia RFID. Las etiquetas RFID pueden ser leídas con dificultad, sobre materiales como metal y algunos líquidos en UHF y en ciertos rangos de frecuencia de microondas. Por consiguiente, si un ambiente tiene demasiado metal en el, un sistema RFID no podría trabajar bien cuando opera en estas frecuencias.

2.6.6.4 Ausencia de Restricciones Legales Internacionales.

La tecnología de código de barras trabaja sobre principios ópticos, mientras que la tecnología RFID trabaja sobre los principios de las ondas RF. Esta distinción ejerce una presión importante sobre los límites legales de uso de la tecnología. No aplica límites internacionales a la frecuencia de la luz, pero bastantes restricciones aplican a las ondas RF. Una gran variedad de límites internacionales aplican a los porcentajes de frecuencia del sistema RFID y con la potencia de transmisión. Sin embargo, un sistema RFID construido para un tipo de frecuencia particular en un país no podría ser legalmente compatible en otro país o podría requerir modificaciones no triviales que resultan en sistemas múltiples para la misma aplicación en esencia. Como evoluciona RFID e incrementa la aceptación, alguna de estas restricciones podría desaparecer así como los gobiernos cooperan a la pérdida de restricciones de frecuencia y energía para cosechar los beneficios del RFID, los lectores multifrecuencia de los vendedores ofrecen una solución alternativa a este tema.

2.6.6.5 Ausencia de problemas sociales.

"Un código de barras no tiene un tema social atado a su uso ya que el tipo de código de barras es para identificar un tipo de producto y proveer cierta información tal como el precio de una manera genérica." [56] Citando un ejemplo, un código de barras sobre un paquete de papas fritas identifica el paquete que contiene las papas fritas y el precio. Sin embargo, este no identifica una funda de papas fritas de manera única de otra funda de papas fritas similar. Esto ni siquiera se puede logar utilizando un tipo de código de barras que almacene más datos.

[56] KLEIST Robert; RFID Labeling; Editorial Printronix, 2004, Pág. 53

Esta anonimidad obvia los temas sociales, tales como el infringimiento a los derechos de privacidad, eso actualmente impacta la aceptación del RFID. Etiquetar un ítem con un código de barra es aceptado hoy a nivel mundial sin ningún problema, pero los esfuerzos de prueba utilizando RFID han causado alborotos públicos de los grupos que trabajan a favor de las leyes de los derechos de privacidad. Hasta que los intereses legales, de negocios y tecnológicos establezcan este debate, podría presentarse un obstáculo para ubicar la aceptación del RFID.

2.6.6.6 Tecnología ya desarrollada con gran base instalada.

El código de barra ha estado en existencia por los últimos 30 años. En estos años, la tecnología ha madurado tremendamente. Más de 50 códigos de barras estándares están difundidos actualmente para ser utilizados hoy, y varios de estos estándares por ejemplo, UPC y EAN disfrutan de un soporte de difusión alrededor del mundo. Hoy, los códigos de barra están ubicados en todas las facetas de la economía. Actualmente, se estima que cada día, alrededor de cinco billones de de códigos de barras son escaneados.

Comparado al éxito del código de barras, el éxito del RFID hoy puede decirse que es limitado. La tecnología RFID por el momento está considerada como una tecnología emergente y es así que todavía tiene muchos desafíos que vencer. El precio y rendimiento del hardware, la complejidad involucrada en diseñar un medio para una gran solución, y lo que concierne al infringimiento a los derechos de privacidad para el etiquetado a nivel de ítem podría demorar la adopción de la tecnología RFID por un cierto tiempo.

La tecnología RFID y el código de barras tomados conjuntamente no cubren todas las aplicaciones posibles. Ambos tienen desventajas comunes, las cuales están cubiertas en la siguiente sección.

2.6.7 DESVENTAJAS DE RFID Y LOS CÓDIGOS DE BARRAS.

Las mayores desventajas de estas dos tecnologías se las presenta a continuación:

- **Presencia de Obstáculos.**

  Un lector de código de barras no puede leer un código si hay algún obstáculo entre el lector y el código de barras. Un lector RFID, depende de sus frecuencias de operación y otros factores, tales como la energía y el área de trabajo, esta tecnología no podría ser capaz de leer una etiqueta si hay algunos obstáculos, tales como metal, o material absorbente, tal como agua presente entre el lector y la etiqueta.

- **Presencia de humedad.**

  Para los lectores de código de barras la emisión de luz podría ser refractada por las partículas de agua suspendidas en la atmósfera, resultando en un foco de distorsión. Para lectores RFID operando en UHF y microondas, las partículas de agua suspendidas en la atmósfera podrían absorber la energía RF, resultando en energía insuficiente para alcanzar las etiquetas para una apropiada transferencia de datos.

- **Velocidad.**

  Si el rango de escaneo de un lector excede la velocidad de movimiento de los códigos de barra, podría resultar una pérdida de precisión en la lectura, conjuntamente con la falla para leer un código de barras. Para los lectores RFID, si la velocidad de la etiqueta es tan grande que la etiqueta no tiene tiempo suficiente para energizarse apropiadamente por sí misma se puede provocar errores en la transmisión de datos al lector por la existencia de una lectura imprecisa.

- **Esquemas de identificación extrínseca.**

  Un código de barra o un RFID tiene que ser aplicado externamente a un objeto; estas no son parte de las características físicas del objeto. Sin

embargo, si tal objeto es mal puesto el nombre o mal etiquetado, la identidad del objeto está en peligro. Sin embargo quizá las propiedades intrínsecas podrían ser utilizadas únicamente para identificar un objeto. Por ejemplo, una huella digital o un escaneo de retina de una persona pueden únicamente identificar a la persona.

2.6.8 ¿REEMPLAZARÁ PRONTO RFID AL CÓDIGO DE BARRAS?.

Una vez analizadas las ventajas y desventajas de estas tecnologías de identificación se puede concluir que la tecnología RFID no puede reemplazar en su totalidad al código de barras, para que esto suceda RFID debe superar los siguientes obstáculos:

- **Etiquetar cualquier artículo que un código de barras pueda etiquetar hoy.**

  Aquellos ítems incluyen casi todo tipo de mercadería física en existencia en la economía mundial y hacer esto a un costo aceptable, para lo cual los siguientes obstáculos deben ser superados:

  - **Materiales baratos con etiquetas que cuesten menos de 5 centavos.**

    El margen de ganancia de algunas empresas es un factor clave para su crecimiento económico cualquier costo extra que no vaya enfocado a una línea de crecimiento puede comprometer a la empresa.

  - **Aceptación del consumidor.**

    El consumidor debe aceptar el uso del RFID para etiquetar cada artículo que el código de barras puede hacerlo hoy.

  - **Avance técnico para etiquetar satisfactoriamente cualquier artículo posible.**

    RFID es una tecnología emergente, de tal manera que las capacidades de las etiquetas, lectores y antenas están sufriendo

cambios rápidos. En este punto, las capacidades no son suficientes para etiquetar cada artículo al cual un código de barras puede ser fijado.

- **La aceptación a nivel mundial de las frecuencias comunes de operación.**

  Cuando las bandas de frecuencia comunes para las operaciones de RFID son estandarizadas la utilización de las implementaciones definitivamente se acelerará. Aún si estos obstáculos son superados, hay aún el siguiente y último obstáculo más difícil de vencer.

- **Reemplazar una enorme base de soluciones de trabajo del código de barras.**

  Aún sí el RFID resuelve todos los temas precedentes para estar a la par con los códigos de barras, surge la pregunta del porqué en un negocio se debería reemplazar a una solución de trabajo perfectamente funcional como lo es el código de barras. Aquí es conveniente hacer un análisis costo beneficio de la nueva solución que se desea implementar.

Estos obstáculos son ahora discutidos en detalle en las siguientes secciones.

2.6.8.1 Etiquetar cualquier artículo que un código de barras puede etiquetar hoy.

Claramente, si RFID es para desalojar al código de barra de su estatus actual como “etiquetador superior”, éste necesita etiquetar cualquier artículo que un código de barra pueda hacerlo hoy. Este tema tiene tres componentes principales: económico, técnico y social. Cada uno de estos tres componentes debe ser resuelto antes de que el RFID pueda nivelar el campo de juego con el código de barra. Las siguientes subsecciones discuten los componentes económico y social respectivamente, seguidos por una discusión del componente técnico.

2.6.8.1.1 Material barato con etiquetas que cuesten menos de 5 centavos.

Para competir satisfactoriamente con los códigos de barras, las etiquetas RFID necesitan tener un costo efectivo. El costo para producir un código de barras es próximo a la gratuidad, pero el costo de una etiqueta RFID es muy costosa y esto ocasiona un bajo margen de ganancia en artículos que tienen un bajo costo. Los fabricantes y minoristas quieren maximizar sus ganancias y cualquier gasto adicional que no ayude a sus ingresos son casi siempre descartados. Parece ser un consenso común que hoy en día los artículos del consumidor tiene un etiquetado individual, el precio de una etiqueta individual debe estar por bajo los 5 centavos y para varios otros artículos, el precio tiene que ir bajo el 1 centavo. Al mismo tiempo el precio de los lectores y antenas RFID tienen que bajar a menos de 100 dólares. Estas son altos desafíos considerando que el proceso de manufactura y el costo de producción actual del material RFID.

2.6.8.1.2 Aceptación del consumidor.

Los debates y protestas de los grupos de derechos de privacidad, y los intentos de los legisladores para imponer regulaciones legales parecen solamente empezar a tomar forma con respecto al uso del RFID para etiquetar los artículos del consumidor individuales. Un consenso entre los financistas de la tecnología y los que apoyan los derechos de la privacidad no parece estar cerca. Por lo tanto, aunque la tecnología podría proveer etiquetas lo suficientemente baratas para etiquetar artículos individuales de aquí a cinco años, este hecho no solo implica que el nivel de etiquetamiento de artículos RFID será en realidad puesto en práctica en ese punto.

Debido a las regulaciones y estándares que se podría aplicar al RFID en el futuro, el RFID podría ser utilizado solo para etiquetar ciertos tipos de artículos y utilizar códigos de barras para etiquetar los artículos restantes.

2.6.8.1.3 Avance técnico para etiquetar satisfactoriamente cualquier artículo posible.

La tecnología RFID está aún empezando a madurar cuando se vienen a etiquetar diferentes tipos de artículos. Las propiedades RF de un artículo, sus características físicas, ambientes, de operación, y así sucesivamente tienen todos soportes importantes en el tamaño y propiedades de la etiqueta. Un amplio arreglo de etiquetas con varias características podría ser necesitado para satisfacer estos requerimientos. Este campo está experimentando mejoras rápidas, pero aún así, la tecnología de la etiqueta está lejos de alcanzar un nivel de madurez.

2.6.8.1.4 Aceptación Mundial de las frecuencias comunes de operación.

Un estándar común a nivel mundial de la frecuencia RFID (UHF en particular) actuará como un acelerador de aceptación de la tecnología. Con esto, un único sistema RFID implementado para una aplicación de negocios particular puede ser utilizado a nivel mundial sin ningún cambio costoso para encajar en las regulaciones específicas de cada país. Esta estandarización reducirá los esfuerzos para mantener las soluciones y podría permitir que las soluciones se estandaricen para una aplicación particular. Las soluciones RFID pueden ser entonces compradas virtualmente fuera de las estanterías y puestas en uso en cualquier parte del mundo, actuarán como un catalizador fuerte para la aceptación. Hay que notar que para sortear este asunto, los fabricantes están elaborando lectores que pueden operar en frecuencias múltiples, las cuales podrían ofrecer una solución a este tema.

2.6.8.2 Reemplazar una enorme base de soluciones de trabajo del código de barras.

Actualmente el hecho que la tecnología RFID reemplace en su totalidad al código de barras es prácticamente imposible, la razón es principalmente económica. Cuando el artículo se mueve desde las grandes fábricas a los minoristas para negocios pequeños, las oportunidades de ganar enormes ganancias en productividad parecen ser lejanas, además el costo de implementación y mantenimiento de un sistema RFID tiene que ser menos que el costo de mantenimiento del sistema de código de barra existente a menos que existan

conductores de negocios fuertes para compensar el costo de diferencia con las ganancias de productividad. Qué RFID pueda hacer esto por cada sistema de código de barras existente en el mundo es difícil, si no imposible.

Del análisis de esta sección, se puede entender que hay poca posibilidad de que RFID reemplace completamente al código de barras en la carrera larga, al final más bien lo que se llegará a tener es una coexistencia como tecnologías complementarias.

2.7 APLICACIONES DE LA TECNOLOGIA RFID.

"El ámbito de aplicación de esta tecnología es de los más amplios, abarcando completamente cadenas productivas y de suministros, desde los procesos y operaciones extractivas, pasando por las de manufactura y ensamblaje, luego, por las de distribución y comercialización hasta llegar a los consumidores." [57]

Desde sus orígenes, en los años 20 del siglo pasado, hasta la fecha, se han ido sucediendo una serie de desarrollos, adaptaciones y mejoras que actualmente están convergiendo hacia aplicaciones concretas, de probada factibilidad técnica, en todas las variantes, modalidades operativas y lógicas y, cómo no, también con muy favorables experiencias, a nivel industrial y comercial, de la viabilidad técnico-operacional.

RFID permite aportar soluciones que hasta hoy eran impensables mediante la utilización de las demás tecnologías disponibles. Las características diferenciales que aporta esta tecnología frente a las demás es la identificación sin contacto ni visión y multilectura.

Podemos hacer una división muy simple entre estos dos estados de tiempo, el hoy que son proyectos con un solo actor y el mañana son aplicaciones con

---

[57] HARTMANN Paul, IEEE Applications & Practice RFID; Vol. 45 Nº9, Septiembre 2007, Pág. 21

diversos actores, o dicho de otra forma, actualmente son viables proyectos en los cuales la utilización de la etiqueta la realiza una única empresa, un “único actor”.

Difícilmente podemos plantearnos hoy aplicaciones en las cuales una empresa incorpora una etiqueta en un producto, para que otra lo utilice en la logística, cadenas de venta, comercios y posteriormente otras empresas puedan utilizarlo para la gestión de garantías o asistencia técnica. Todo esto “técnicamente” puede funcionar, pero no es todavía viable debido al costo de las etiquetas. No porque la suma de los ahorros de todas ellas no sea suficiente para su amortización, si no porqué hoy no sabemos todavía cómo compartir ese costo y nadie está dispuesto todavía a sufragar con dicho costo, si sólo por si mismo no le es rentable.

El siguiente punto clave de un análisis es determinar en qué momento finaliza el servicio de la etiqueta. En el caso de utilizarla para identificar un producto de consumo, y desechar la etiqueta una vez realizada la venta del producto, el análisis de viabilidad deberá estudiar en cuantos elementos de la cadena se utiliza dicha información y en que aporta. Si una misma empresa produce un bien, controla su logística y dispone de sus propios puntos de venta, probablemente las posibilidades de que la RFID sea una buena inversión son muy altas.

En las aplicaciones donde se haya determinado que las características diferenciales como: lectura sin contacto, línea de vista y multilectura son claves para nuestra aplicación y además que la etiqueta sea reutilizable, las probabilidades de encontrarnos ante una aplicación muy interesante en la que se emplee RFID son muy altas.

Algunos ejemplos de reutilización de etiquetas son la identificación de materiales de alquiler, donde se entrega un producto que luego será devuelto posteriormente; en ropa profesional donde se entrega ciertas piezas de ropa que serán devueltas para su lavado; en la identificación de todo tipo de contenedores donde se almacena o transporta un producto y la vida y utilización de dicho elemento es muy elevada; en bibliotecas, una aplicación parecida al alquiler; en procesos productivos donde se incorpore una etiqueta a cada lote; se puede

utilizar para la trazabilidad de un producto y que después de un proceso se pueda recuperar la etiqueta.

Como se puede apreciar RFID actualmente tiene muchas aplicaciones, en las siguientes subsecciones se exponen las aplicaciones más importantes de hoy en día.

- Trazabilidad de objetos.
- Inventario, monitoreo y control.
- Monitoreo y administración de recursos.
- Sistemas antirrobo.
- Control de accesos.
- Sistemas anti sabotaje.

2.7.1 TRAZABILIDAD DE OBJETOS.

La trazabilidad de objetos está caracterizada por dos aspectos principales:

- Poner una etiqueta que contiene un identificador único en un objeto para ser monitoreado.
- Lectura del identificador de esta etiqueta para especificar su localización mientras el objeto se mueve.

El identificador de la etiqueta cuando está asociado con una lectura en el instante y una información de localización, puede proveer una información en tiempo real acerca del paradero del objeto. Se puede utilizar una lista de rastreo de objetos durante un cierto ciclo de vida, además se puede obtener información de que personal movió un objeto de un lugar a otro. Esta información puede ser utilizada para reducir el nivel de responsabilidad del personal. También se puede asociar varias acciones con la actividad de rastreo como por ejemplo el disparo de una alarma si un objeto no se encuentra en la localización y tiempo acertados.

Algunas de las más importantes aplicaciones que pertenecen a este tipo de aplicaciones son las siguientes:

- Cadenas de distribución
- Rastreo de materiales peligrosos
- Rastreo del equipaje en líneas aéreas

2.7.1.1 Cadenas de distribución.

Un objeto puede ser rastreado en la cadena de distribución desde el lugar que es producido hasta el punto donde es consumido o reciclado sin necesidad de intervención humana, que generalmente es requerida con sistemas basados en códigos de barras. De esta manera, esta tecnología previene la falta de inventario en los puntos de venta, el hurto y los errores administrativos. A continuación se muestra una visión de RFID en la cadena de distribución:

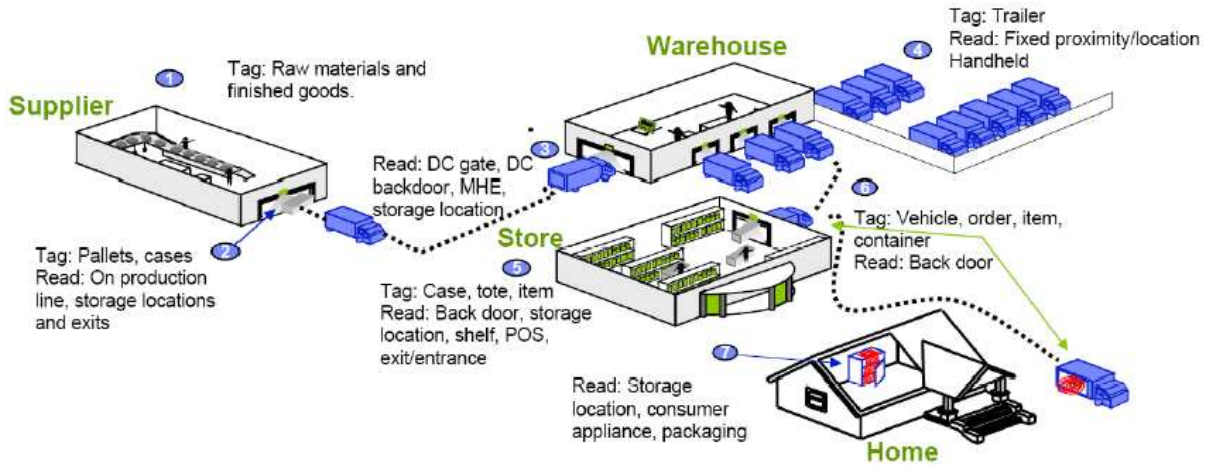


Figura 2.29 Etapas de la cadena de distribución.[58]

[58] http://sociedaddelainformacion.telefonica.es/img/elementos/articulos/upload/202-img-05.jpg

2.7.1.1.1 Fabricación.

En esta etapa se aplican físicamente las etiquetas RFID a los productos (o embalajes) y les son grabados un ID único (EPC), que son asociados con los detalles de la orden o del pedido para facilitar el rastreo y la gestión de excepciones. Durante el proceso de construcción del pallet, los productos son identificados automáticamente para asistir con la configuración de las órdenes de los clientes. Finalmente, los pallets son identificados y rastreados mientras son movilizados a la zona de despacho.

2.7.1.1.2 Fabricante.

Mientras el transportista llega a la plataforma de carga del fabricante, un lector RF ubicado en la plataforma de carga se comunica con su etiqueta RFID, para confirmar si el vehículo está autorizado para recoger los productos. Luego de la aprobación, las etiquetas de los pallets se comunican con el lector RFID de la plataforma de carga, con la finalidad de alertar a los sistemas B2B y a los sistemas ERP, dando inicio a las transacciones electrónicas, confirmaciones de recojo y potencialmente iniciar la facturación de envíos.

2.7.1.1.3 Despacho --> Centro de Distribución.

Al llegar la mercadería al centro de distribución, el lector RFID identifica el ID único de la etiqueta RFID y junto al middleware inician un evento, registrando la llegada del manifiesto, actualizando el inventario e iniciando el ruteo automático de los productos al siguiente vehículo (consolidación de carga). Todo esto sin necesidad de abrir los embalajes. El desarrollo del estándar EPC es una iniciativa que tiene el soporte de EAN Internacional.

2.7.1.1.4 Centro de distribución --> Despacho.

Mientras los pallets son cargados al vehículo, las etiquetas RFID transmiten su ID único al lector RFID ubicado en la plataforma de carga, y vía el middleware RFID, se transfiere la información a los sistemas del negocio (ERP) indicando que el manifiesto ha sido cargado.

2.7.1.1.5 Despacho --> Tienda.

Conforme los productos llegan a la plataforma de descarga de la tienda, éstos son detectados por lectores RFID, sus sistemas ERP son actualizados para controlar sus niveles de inventario (automáticamente, con precisión y a bajo costo) y se da inicio al envío de mensajes B2B con el proveedor para dar inicio al proceso de facturación.

2.7.1.1.6 Tienda --> Consumidor (visión de largo plazo).

El lector RFID ubicado en los estantes puede detectar el retiro de los productos y a través del middleware RFID iniciar el requerimiento de abastecimiento de productos adicionales. Con sistemas de este tipo, se reduce la necesidad de mantener costosos volúmenes de inventario, y en lugar de ello, el cliente inicia la generación directa de demanda en el proceso de gestión de la cadena de abastecimiento.

2.7.1.1.7 Consumidor (visión de largo plazo).

En lugar de hacer colas esperando la atención de un cajero, el consumidor pasa a través de un lector RFID ubicado cerca de la puerta, el cual identifica a todos los productos por su ID único, haciendo necesario solamente que el consumidor deslice su tarjeta de débito o de crédito para finalizar la compra.

2.7.1.2 Rastreo de materiales peligrosos.

Plantas de procesamiento químico tienen diferentes tipos de materiales químicos, los químicos arriban desde diferentes cadenas de suministro y son consumidos o procesados en la planta. La planta envía esos productos fabricados con esos químicos a sus distribuidores y clientes. Algunos de estos químicos pueden ser peligrosos y por consiguiente requieren un especial cuidado al momento de manipularlos. Considerando que estos materiales químicos pueden ser peligrosos y es muy importante que información como la siguiente este siempre disponible con el objetivo de evitar cometer errores al momento de manipular estos químicos peligrosos:

- Qué tipo de químico es, su composición, concentración, etc.
- Cuándo arribó el contenedor al muelle para el desembarco.
- Quién solicitó el producto.
- Cuándo y por donde ingresó el producto a la planta.
- Si el producto está en movimiento dentro de la planta, saber de dónde hacia dónde se moviliza el producto.
- Si el producto ha salido de la planta saber si se ha entregado al distribuidor o cliente adecuado.

Los principales beneficios que ofrece esta aplicación son los siguientes:

- **Seguridad pública.**
  El rastreo apropiado puede prevenir que los materiales peligrosos sean manipulados de una manera inapropiada, ciertos materiales si son maltratados o caen en manos equivocadas pueden causar sustanciales daños a la planta y a quienes están expuestos.
- **Disminuir la contaminación del medio ambiente**.
  La propiedad de reciclaje y descontaminación de los materiales peligrosos y los contenedores puedes ayudar a prevenir la contaminación ambiental.

2.7.1.3 Rastreo del equipaje en líneas aéreas.

Las etiquetas embebidas en los equipajes de las líneas aéreas pueden ser utilizadas para proveer un efectivo rastreo del equipaje, estas etiquetas pueden ser leídas en cualquier orientación y a unos cuantos metros de distancia por el lector RFID, resultando así una lectura más rápida que la ofrecida por el código de barras.

Los pasajeros entregan su equipaje en el mostrador de facturación, como antes, donde el personal de tierra le adosa una cinta de papel. Pero esta cinta lleva una etiqueta integrada con una antena, un microprocesador y una memoria en la que se registra toda la información pertinente. Las maletas se desplazan por una cinta transportadora hasta un túnel equipado con máquinas de lectura y escritura RFID sin contacto. Los datos se leen en tiempo real, se procesan con rapidez con algoritmos eficientes y se envían al sistema de gestión de equipajes que controla el movimiento de todos los bultos. El sistema identifica de forma exclusiva el chip de radiofrecuencia cualquiera que sea su posición, y, a diferencia del código de barras, no precisa el contacto óptico para el escaneo.

Figura 2.30 Lectura de equipajes en líneas aéreas[59]

Con esto se reducirá notablemente los errores de escaneo que dan lugar a errores de clasificación y entrega. Se han realizado pruebas en ciertos aeropuertos acerca del funcionamiento de esta tecnología y se tienen resultados de lectura de etiquetas con una tasa de éxito del 99,9 por ciento, una cifra muy superior a la de los códigos de barras utilizados anteriormente.

2.7.2 INVENTARIO, MONITOREO Y CONTROL.

Las actividades de control de inventarios suponen siempre grandes gastos tanto económicos como de tiempo. Es fundamental contar con un sistema tecnológico que permita realizar estos procesos con total confiabilidad y de forma mucho más eficiente, y la tecnología RFID aporta con las bases de cualquier solución de inventario, pudiendo clasificarlas fundamentalmente en:

[59] http://blogingenieria.com/wp-content/uploads/2008/05/0011.jpg

- **Entrada/Salida.**

  El primer sistema de inventariado opera chequeando la entrada y la salida de los elementos mediante tecnología RFID. La ventaja de su utilización respecto a otras tecnologías, es la posibilidad de automatizar los procesos de identificación simplemente situando los elementos en el campo de lectura, pudiéndose además realizar múltiples lecturas simultáneamente.

  Una posible solución se compone de una pequeña instalación con un puesto de lectura con un lector RFID con sus respectivas antenas. Los elementos etiquetados con RFID que se introduzcan por el paso de entrada quedaran registrados en el inventario.

  Otra posible solución se basa en la utilización de un lector RFID portátil o de mano. Esta solución de movilidad permite chequear todos los elementos del inventario de forma mucho más eficaz aproximando el lector de mano y registrando así todos los elementos en el campo de lectura

- **Tiempo Real.**

  El segundo sistema de control de inventario consiste en obtener cada cierto periodo de tiempo, en ocasiones un instante, todo el inventario disponible. Aunque una solución costosa y en ocasiones no realizable físicamente, proporciona la solución de auto identificación perfecta, automatizando todos los procesos y eliminando por completo la tarea de inventariado.

  Esta solución consiste en la instalación de antenas cubriendo todos los campos que precisen inventariado conectadas a un lector RFID. De esta forma al situar un elemento etiquetado con RFID en el inventario, quedará registrado automáticamente por el sistema informático de gestión, que recibirá la lectura del interrogador RFID

2.7.3 MONITOREO Y ADMINISTRACIÓN DE ACTIVOS.

Lo básico de esta clase de aplicación es la determinación de localización de objetos en tiempo real utilizando etiquetas RFID. Se puede utilizar etiquetas activas o pasivas para el monitoreo de activos. En este contexto hay que notar que para este tipo de aplicación existe un estándar ANSI denominado ANS INCITS 371, donde se hace mención a la localización de usuarios, administración y optimización de activos móviles a través de las cadenas de distribución. Generalmente los lectores estacionarios leen las etiquetas de los activos, esta información que ha sido obtenida por medio de los lectores es transferida al back-end el mismo que alimenta al sistema de monitoreo de activos. Se puede tener un monitoreo local y remoto, para el monitoreo remoto se utiliza una comunicación satelital la misma que permite enlazarse con el sistema de monitoreo RFID.

Esta aplicación tiene en parte relación con la trazabilidad, de hecho el objeto a ser rastreado puede ser visto como un activo que puede ser monitoreado. Sin embargo un aspecto relevante de este tipo de aplicación es la recopilación de las propiedades de los activos en tiempo real, junto con el identificador único para ayudar a la administración de activos.

2.7.4 SISTEMAS ANTIRROBO.

RFID puede ser una efectiva herramienta contra robo. Este tipo de solución está caracterizado por lo siguiente:

- Adición de una etiqueta a un ítem para ser monitoreado por robo.
- Lectura del ID de la etiqueta en los puntos vulnerables.
- Características adicionales como la habilidad de remover una etiqueta del ítem sólo después que el pago se haya realizado, habilidad de detectar el desplazamiento de un ítem y reportarlo al lector más cercano, y así sucesivamente.

Se puede utilizar etiquetas activas o pasivas para este propósito. Para ítems de alto valor como por ejemplo computadoras portátiles, se puede utilizar una

etiqueta activa construida con un detector de movimiento, cuando el equipo es movido, el sensor de movimiento de la etiqueta detecta este evento y transmite esta información al lector más cercano para que esta se transmita al back-end del sistema y se realicen las acciones necesarias. Por ejemplo se puede bloquear la salida de este ítem de una cierta área por medio del disparo de una alarma o puede iniciar una video grabación del lugar donde el ítem se encuentra localizado. En el caso que se haga uso de una etiqueta pasiva este evento puede ser detectado en el punto de salida, o la ausencia de esta etiqueta en el caso que se la haya desprendido del ítem puede ser detectado en el back-end del sistema utilizando lectores estacionarios.

Cabe recalcar que la solución antirrobo con RFID actualmente no es barata. Por lo tanto al momento de realizar una implementación de este tipo hay que realizar un análisis costo beneficio.

2.7.5 CONTROL DE ACCESOS.

RFID ha sido utilizado satisfactoriamente en soluciones que proveen control de accesos. Una solución de este tipo está caracterizada por lo siguiente:

- La etiqueta que tiene identificador único de datos es portada por el objeto o persona para obtener acceso a un cierto sitio. Esta etiqueta puede ser ubicada en el parabrisas del vehículo, puede ser embebida en la tarjeta de identificación de una persona o sobre su piel.

- Lectura del identificador único de datos en los puntos de control de accesos. Una vez leído el ID estos datos son enviados al sistema de seguridad el cual decide permitir o no el acceso.

Este tipo de aplicación es madura comparada con otros tipos de aplicaciones, en términos de la tecnología RFID y sistemas que van junto con ella. Una de las características de madurez de esta tecnología es la existencia de estándares. El

estándar ISO 15693 relacionado con las tarjetas de vecindad está ampliamente aceptado por los productos de control de accesos que operan a la frecuencia de 13.56 MHz.

Como ejemplos principales que pertenecen a esta aplicación tenemos la construcción de perímetros de seguridad y los sistemas para parqueo de vehículos.

2.7.6 SISTEMAS ANTISABOTAJE.

Las aplicaciones anti sabotaje están caracterizadas por lo siguiente:

- Adherir una etiqueta que contiene un identificador único para ser monitoreado contra eventos anti sabotaje. La etiqueta es ubicada en la tapa del contenedor donde se encuentra el ítem, formando esencialmente un sello electrónico.
- Al detectar la ruptura del sello. Varios métodos pueden ser utilizados para determinar la ruptura. Por ejemplo comparar la posición original del etiquetado con una alta precisión utilizando las características ópticas del sello.

Una etiqueta RFID utilizada para este tipo aplicación actúa como un sello inviolable. Este sello está cerca de identificarse como un sellado del ítem de manera única, también puede proveer una evidencia de saboteo. Al integrar esta aplicación con otra como el control de accesos también se puede proveer la identificación de la persona o personas involucradas en el sabotaje del sello. Aunque puede parecer fácil violar este sistema abriendo el sello con cuidado y luego volviendo a sellar, esto es muy difícil y hasta imposible en ciertos casos. En este tipo de aplicaciones se puede utilizar tanto etiquetas activas como pasivas. Esta es una de las aplicaciones que necesita mucha investigación y se espera tener comercialmente sofisticadas etiquetas RFID anti sabotaje en el futuro.

CAPITULO 3

DISEÑO E IMPLEMENTACION DEL SISTEMA DE CONTROL DE ACCESO UTILIZANDO RFID.

El presente capítulo tiene como objetivo principal mostrar el diseño e implementación del prototipo para control de acceso. En éste se realizará un análisis de la situación actual de control de acceso, los requerimientos para implementar esta tecnología para luego pasar a detallar el desarrollo del prototipo con sus respectivas pruebas de funcionamiento las cuales permitirán llegar a mostrar los aportes de este proyecto.

3.1 ANÁLISIS DE LA SITUACIÓN ACTUAL DE CONTROL DE ACCESOS A ESPECTÁCULOS.

En la actualidad los escenarios del país no cuentan con una adecuada administración, esto conduce a tener una falta de seguridad e infraestructura adecuadas. Esto convierte al escenario en un espacio obsoleto e incómodo para los espectadores y muchos de ellos son poco funcionales de modo que hasta a veces pueden resultar peligrosos. Por estas y muchas razones es importante implementar una solución que permita tener un escenario inteligente, con inteligente se hace referencia a implementar una tecnología de seguridad, identificación y telecomunicaciones, con el objetivo de tener seguridad, control y administración de todo un escenario.

El uso de una tecnología de identificación permite controlar el acceso de todos los asistentes a un escenario, dicha tecnología permite ya tener un control en tiempo real de cualquier anormalidad que pueda presentarse al momento del ingreso a un escenario. Dicha anormalidad puede surgir por diferentes motivos como por ejemplo ingreso de credenciales o tickets falsificados, duplicados, accesos a áreas no permitidas, etc. Todas estas anormalidades no se las podría controlar si el acceso fuera realizado de una manera manual donde el factor humano es quien decide quién está o no permitido de acceder, la falta de control en un escenario

puede conducir a grandes pérdidas económicas y lo que es más grave, puede ocasionar desastres dentro del mismo por una sobre-ocupación de ciertas áreas.

Como beneficios acerca del uso de las tecnologías de identificación tenemos los siguientes:

- **Beneficios para los empresarios.**
  - Proceso de acceso rápido y seguro al escenario.
  - Reducción del personal necesario para operar un evento.
  - Se reducen los abusos y malos manejos.
  - Reportes detallados de asistencia en tiempo real.
- **Beneficios para el público.**
  - Acceso fácil y rápido.
  - Reducción del tiempo de espera en filas.
  - Salvaguardo de su integridad física.
  - Mayor sensación de orden y seguridad.

Actualmente el control de accesos en ciertos escenarios se lo maneja utilizando la tecnología de código de barras. Dicha tecnología como se analizó en el capítulo anterior tiene sus respectivas ventajas pero a su vez existen muchos temas relacionados con la administración de un evento, que hacen necesario el usar otro tipo de tecnología como es RFID. En la siguiente sección se detalla la operación total de un evento con sus diferentes etapas en las cuales se introduce el uso de la tecnología RFID.

3.2 DEFINICIÓN DE CONTROL DE ACCESO DE LA EMPRESA SOLUCIONES G CUATRO DEL ECUADOR CÍA. LTDA.

Introducción.

La empresa Soluciones G4 del Ecuador tiene como actividad principal la emisión de tickets y control de accesos a un inmueble de uso masivo, estas tareas son administradas por medio de un software que permite administrar todas las operaciones. Dicho software está diseñado para resolver las necesidades de

comercialización, seguridad, operación y administración de un inmueble bajo el concepto de “Escenario Inteligente”. Como se mencionó en la sección anterior la tecnología de identificación que actualmente se utiliza para el efecto es el código de barras, a continuación se describen las diferentes etapas por las que se atraviesa para llevar a cabo la ejecución de un evento, se presentan dichas etapas a detalle con el objetivo de ir definiendo en cuál de ellas es justificable ir involucrando el uso de esta tecnología para finalmente llegar a tener una solución óptima en este campo de aplicación.

La implementación de un evento o proyecto se encuentra vinculado con factores que relacionan tanto recursos como tiempos, por lo que la implementación de una metodología está pensada para desarrollar las habilidades necesarias, las mismas que servirán en la ejecución de las tareas que lo integran, faciliten la comprensión y también para que éstas se desarrollen de una manera muy sencilla en la implementación; esto tiene un impacto significativo en la mejora de los tiempos de implementación.

3.2.1 VALIDACIÓN DE LA VENTA.

La validación de venta tiene por objetivo dar a conocer al cliente[1] los servicios principales que la empresa brinda y la manera como se implementan dichos servicios, adicional a esto se definen los alcances y costos de cada uno de ellos con fin de proponer al cliente una propuesta comercial la misma que conlleve a la firma de un contrato.

3.2.1.1 Análisis de Solución.

La empresa Soluciones G Cuatro, cuando realiza el proceso de venta de sus servicios, inicia con un análisis de la solución ofertada. Para ello se realiza un análisis de las necesidades del cliente y se determina el mejor tipo de solución.

[1] Persona u organización que contrata los servicios de la empresa

Como consecuencia de este análisis, se genera una propuesta comercial, la cual está conformada por:

- Presentación de la empresa y servicios que presta.
- Descripción de los servicios y alcance de la solución.
- Costos.
- Acuerdos comerciales.

La propuesta se realiza bajo la visión de que el servicio debe cumplir con las expectativas del cliente.

3.2.1.2 Cierre de venta.

Una vez liberada y aceptada la propuesta comercial, viene la realización y firma del contrato. El contrato debe contener al menos los siguientes puntos:

- Todo lo descrito en la propuesta comercial.
- Acuerdos llevados a cabo en negociaciones.
- Responsabilidades de servicio por ambas partes.
- Un listado del personal involucrado para la toma de decisiones y una descripción de la responsabilidad que tiene dicha persona en el proyecto.

3.2.2 PLANEACIÓN.

De manera general la planeación consiste en planificar la ejecución de todas las actividades que están relacionadas con un evento, dichas actividades serán ejecutadas de manera cronológica y ordenada tal como se estipule en dicho plan. En las siguientes subsecciones se contemplan las actividades mencionadas.

3.2.2.1 Generación e Información del plan de trabajo tipo.

El plan de trabajo es un documento que se lo elabora en base a la propuesta comercial y/o contrato realizado, se anexa la información del evento al plan de trabajo generado para controlar todas las actividades involucradas.

En el plan de trabajo se encuentran delimitadas todas las actividades necesarias para la implementación, bajo una experiencia previa con el objetivo de mantener el orden de las tareas o procesos a realizar. Este plan de trabajo es elaborado con base al estándar que la empresa tiene en la organización de eventos.

El plan está dividido y estructurado de la siguiente manera:

- Nombre de la función o proyecto.
- Junta inicial en donde se realiza la recopilación de información.
    - Secciones, aforos y tipos de boleto
        - Secciones son las localidades que se venderán en un evento
        - Aforo es la cantidad de personas que ingresaran en las diferentes secciones
        - Tipos de boleto es la clasificación del boleto; adulto, niños, tercera edad o cortesías.
    - Distribución de puertas y secciones.
        - Distribución de puertas se refiere a la cantidad de equipos que serán distribuidos en las puertas de acceso que haya para un determinado espectáculo
        - Secciones se refiere a la distribución de puestos por localidad del evento.

- Software.
    - Alta de credenciales: aquí se contempla el ingreso de toda la información del cliente VIP[2] a la base de datos por medio del

[2] Usuario portador de las credenciales RFID

software de registro de usuarios los datos a ingresar son los siguientes

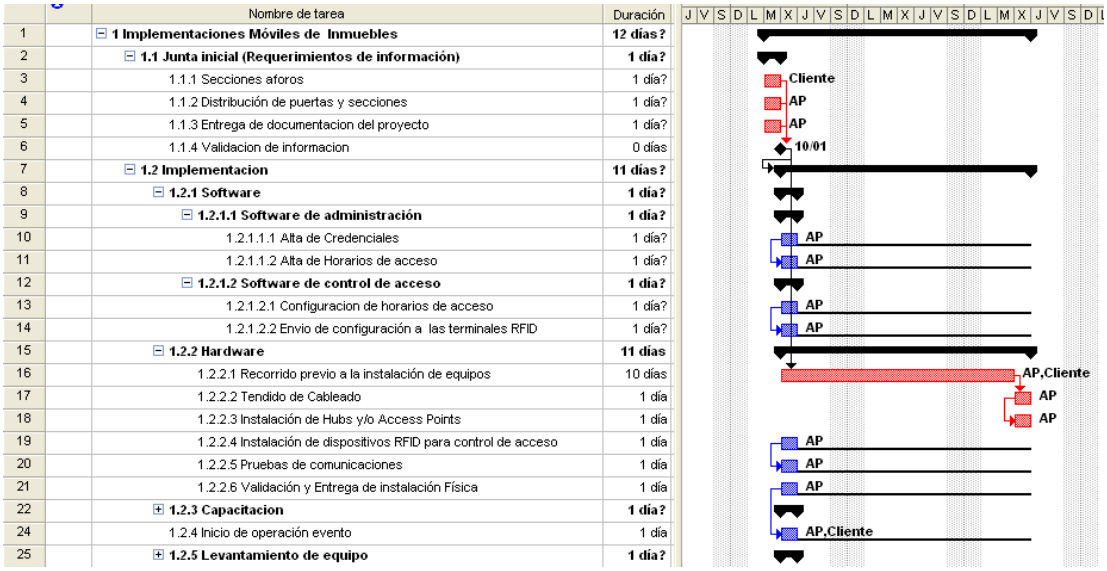
- Nombre.
- Apellido Materno.
- Apellido Paterno.
- Nombre del evento.
- Fecha del evento.
- Imagen del evento.
- Número de credencial RFID.
- Horario de acceso.
- Fotografía del usuario.

  - Alta de horarios de acceso: Asignar a cada usuario VIP el respectivo horario de acceso.

- Hardware (instalación).
  - Recorrido previo; Realizar una inspección física de todo el inmueble con el objetivo de planificar la distribución y ubicación de los equipos en cada acceso.
  - Instalación de cableado y equipos de control de acceso
  - Pruebas de funcionamiento: verificar conectividad de equipos validación de credenciales de prueba y verificación de la funcionalidad total del sistema.

- Capacitación y medidas de contingencia al personal encargado de operar los equipos.

- Levantamiento del equipo, que se lo hace una vez terminada la operación del control de accesos que se lo realiza hasta máximo culminado el evento.



	Nombre de tarea	Duración
1	**1 Implementaciones Móviles de Inmuebles**	**12 días?**
2	**1.1 Junta inicial (Requerimientos de información)**	**1 día?**
3	1.1.1 Secciones aforos	1 día?
4	1.1.2 Distribución de puertas y secciones	1 día?
5	1.1.3 Entrega de documentacion del proyecto	1 día?
6	1.1.4 Validacion de informacion	0 días
7	**1.2 Implementacion**	**11 días?**
8	**1.2.1 Software**	**1 día?**
9	**1.2.1.1 Software de administración**	**1 día?**
10	1.2.1.1.1 Alta de Credenciales	1 día?
11	1.2.1.1.2 Alta de Horarios de acceso	1 día?
12	**1.2.1.2 Software de control de acceso**	**1 día?**
13	1.2.1.2.1 Configuracion de horarios de acceso	1 día?
14	1.2.1.2.2 Envio de configuración a las terminales RFID	1 día?
15	**1.2.2 Hardware**	**11 días**
16	1.2.2.1 Recorrido previo a la instalación de equipos	10 días
17	1.2.2.2 Tendido de Cableado	1 día
18	1.2.2.3 Instalación de Hubs y/o Access Points	1 día
19	1.2.2.4 Instalación de dispositivos RFID para control de acceso	1 día
20	1.2.2.5 Pruebas de comunicaciones	1 día
21	1.2.2.6 Validación y Entrega de instalación Física	1 día
22	**1.2.3 Capacitacion**	**1 día?**
24	1.2.4 Inicio de operación evento	1 día
25	**1.2.5 Levantamiento de equipo**	**1 día?**

Figura 3.1 Actividades de un evento

Todas las actividades mencionadas en la figura anterior se las ejecuta de manera cronológica tal como se muestra en los ítems de la figura 3.1

3.2.2.2 Definición de parámetros de operación.

3.2.2.2.1 Coordinación y presentación.

En la coordinación se dispone las actividades a realizarse para dicho evento en el control de accesos, disponiendo cómo se va a ejecutar la operación.

En base al tipo de usuarios que asistan al evento y el trato especial que se desee brindar, se escoge el tipo de tecnología.

Cuando se requiere un máximo control de acceso se escogerá tecnología RFID. Esta tecnología se utiliza para las siguientes tareas:

- Emisión de credenciales para empleados afines a la coordinación logística y operativa del evento.
- Emisión de credenciales para usuarios VIP
- Emisión de tickets para todo un evento. Es importante mencionar que la decisión para la emisión total o no de tickets para un evento con la tecnología RFID depende del análisis costo-beneficio. Actualmente el costo es de $1.05 por credencial, a futuro se espera tener un costo razonable de estas etiquetas y de los equipos lectores con lo que se superaría el principal factor limitante que es el económico. Cabe recalcar que también existen otros factores limitantes como por ejemplo:
    - Distancia de lectura de las credenciales, esto dependerá del tipo de lector que se utilice y la frecuencia de operación. Haciendo referencia al presente proyecto las distancias de lectura requeridas son de aproximadamente 2cm.
    - Interferencia por el tipo de materiales u condiciones ambientales que puedan existir. Por ejemplo materiales conductores, como el cobre. Este limitante se presenta en el proyecto, ya que el ambiente de trabajo está sometido a varias interferencias como: la inducción de los cables que utilizan los generadores de energía.
    - Cultura por parte de los usuarios en adaptarse a una nueva tecnología de identificación. Este también es un punto muy importante que hay que tomar en cuenta ya que si no existe una cultura adecuada del usuario ante una nueva tecnología, puede ocasionar que todo el trabajo haya sido en vano ya que el principal agente que es el usuario no estaría aceptando dicho cambio. Este proceso que se lo va implementado paulatinamente con el objetivo de evitar el fracaso en la aceptación de una nueva tecnología por parte usuario, por tal motivo se plantea implementar la tecnología RFID en la emisión de credenciales para el personal operativo y clientes VIP. Como se mencionó anteriormente, se ha seleccionado este tipo de clientes debido a que éstos son los que están más familiarizados con el uso de nuevas tecnologías de identificación.

Por otra parte, la afluencia de público por estas puertas no tienen un uso masivo a diferencia de las puertas críticas[3] en donde un mínimo retardo por parte del usuario en la lectura de una credencial ocasiona una aglomeración de personas lo que puede conducir a un colapso del sistema no por temas de mal funcionamiento del mismo sino por la falta de control físico en el acceso.

En esta etapa es indispensable la explicación concisa de lo que comprende la implementación del control de accesos, aquí se define los alcances y limitantes del mismo. Alcances que se dé a conocer de manera detallada al cliente.

Con una clara explicación de los componentes de hardware a colocar, así como también las especificaciones técnicas de la implementación (según los acuerdos comerciales).

Presentación del plan de trabajo tipo, haciendo conocer al cliente acerca de los tiempos estimados de implementación.

3.2.2.2.2 Distribución de equipos por puerta y horario de acceso.

En los espectáculos que se realizan en el país existen perfiles de usuarios VIP los cuales tienen acceso al escenario en base a un horario específico. Por tal razón se realizará un control de accesos basándose principalmente en el horario de acceso.

En base a pruebas realizadas en la rapidez de lectura de una Terminal y la rapidez de desplazamiento del público por la puerta se ha elaborado un archivo Excel el cual permite determinar automáticamente cuantas terminales RFID son necesarias para permitir el ingreso a cierta cantidad de personas en un determinado período de tiempo, tal como se muestra en la figura 3.2. El cálculo respectivo se lo realiza en base al tiempo que toma cada equipo de control de acceso en realizar una lectura de la etiqueta RFID.

[3] Puerta por la cual ingresa la mayor afluencia de público.

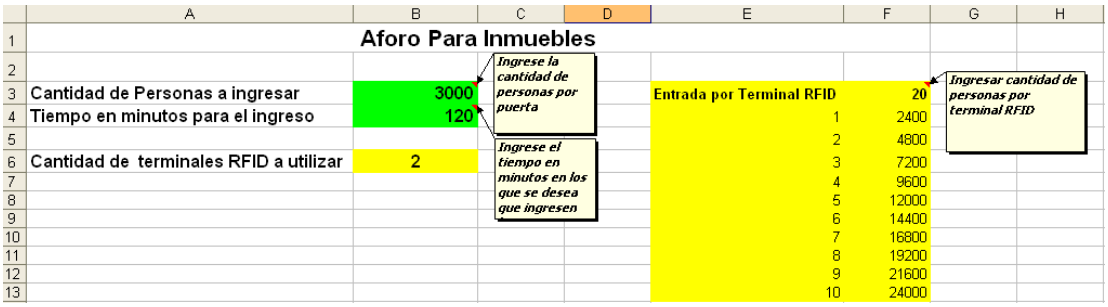


Figura 3.2 Cálculo del Aforo para inmuebles

En la tabla de cálculo del aforo se presentan los siguientes parámetros:

- Cantidad de personas a ingresar: Es la cantidad total de personas que se desea ingresar por un determinado acceso.
- Tiempo en minutos para el ingreso: Es el tiempo máximo durante el cual se desea que ingrese una cierta cantidad de personas.
- Cantidad de terminales RFID a utilizar: Es la cantidad de equipos que se necesitan para procesar la lectura de una cierta cantidad de personas.
- Entrada por la Terminal RFID: Indica la cantidad de credenciales RFID que pueden ser leídas por cada Terminal RFID basado en el tiempo en minutos para el ingreso. Para este punto se toma como base un promedio estadístico de lectura de una Terminal RFID la cual lee 20 credenciales por minuto.

3.2.2.2.3 Recorrido previo a la instalación.

Para ejecutar esta actividad se realiza un recorrido previo del inmueble con el objetivo de determinar la distribución de los equipos de control de acceso, esto es:

- Handhelds (Computador de mano, que para este caso hace el papel de controladora).
- Lectores RFID.
- Switchs.

- Access Points.

Este recorrido se lo debe realizar con el debido tiempo de anticipación, con el objetivo de saber el estado y colocación de tomas de corriente e instalación del cableado de datos. Si éstos no existen es necesario prever la instalación de los mismos.

3.2.3 EJECUCIÓN.

3.2.3.1 Inicio y descripción de operaciones.

En esta etapa se dan inicio a todas las actividades planeadas y marcadas previamente en el plan de trabajo.

Tras obtener la información necesaria para la operación del evento, las actividades siguientes involucran la configuración de software y equipos. La operación lleva el siguiente cronograma:

- Generación del inmueble:
  Tiene como objetivo que el área comercial y de operaciones definan las secciones y tipo de credencial a generar. El documento también servirá para definir las secciones o localidades, puertas del inmueble, cantidad de terminales RFID, y el personal a utilizar para la operación de los equipos.

Como ejemplo para explicar este proceso, vamos a utilizar el evento denominado “Mana” que consiste en la presentación de este grupo musical en el Estadio Olímpico Atahualpa.

Evento, Estadio Olimpico Atahualpa							
Seccion		Aforo	Puerta	Equipos			Personal de seguridad
Tipo	Sub Tipo			Terminales RFID	Hubs	Access Point	
General	Norte	5150	Norte	4	1	1	8
	Sur	5150	Sur	4	1	1	8
Tribuna		1600	P10- P11	2	1	1	4
Cancha		5250	P8	3	1	1	6
		5250	P2	3			6
Super Vip		212	P7	2	1	1	4
Vip		680					
		23292		18	5	5	36

Tabla 3.1 Generación del inmueble

En la distribución de los equipos es recomendable siempre colocar una Terminal RFID de backup en cada una de las puertas por incidentes como bloqueo de la terminal. Adicionalmente a esto se deben de tener listas más terminales RFID que permitan el acceso a todas las secciones, por si la carga de público se concentra en alguna puerta y así poder validar con aquella terminal y permitir más rápidamente el ingreso del aforo.

3.2.3.2 Carga de información al sistema.

Una vez que se han definido el tipo de usuarios VIP que están hábiles para el ingreso durante el espectáculo, con sus respectivos horarios de acceso se procede a llenar la información de todos estos usuarios. A partir de este momento es posible empezar a generar las credenciales de acuerdo a los requerimientos operativos del organizador del evento.

Para ello se dispone de un software de registro de usuarios, mediante el cual se llenan las bases de datos con la información de quienes tienen autorización para ingresar.

3.2.3.3 Carga de configuración a las terminales RFID.

Previo a la fecha del evento se procede a descargar la información de la base de datos donde se encuentra toda la información de las credenciales para luego dicha información transferirla a las terminales RFID para la validación de las credenciales. Para ello se precede de la siguiente manera:

Se envía la información de la base de datos a las terminales RFID mediante una aplicación denominada Driver. Esta aplicación permite realizar el envió de horarios y configuraciones a las terminales móviles para que éstas puedan realizar la validación de las credenciales. Adicionalmente a esto, el Driver permite recolectar la información de las credenciales y almacenar esta información en la base de datos respectiva a medida que las credenciales son leídas por las terminales RFID.

3.2.3.4 Instalación física en el inmueble.

En base a los accesos designados se habrá generado un mapa en el cual se trazan todas las rutas de cableado y puertas con la cantidad de equipos necesarios, en el mapa se debe de tener una información similar a la mostrada en la figura 3.3.

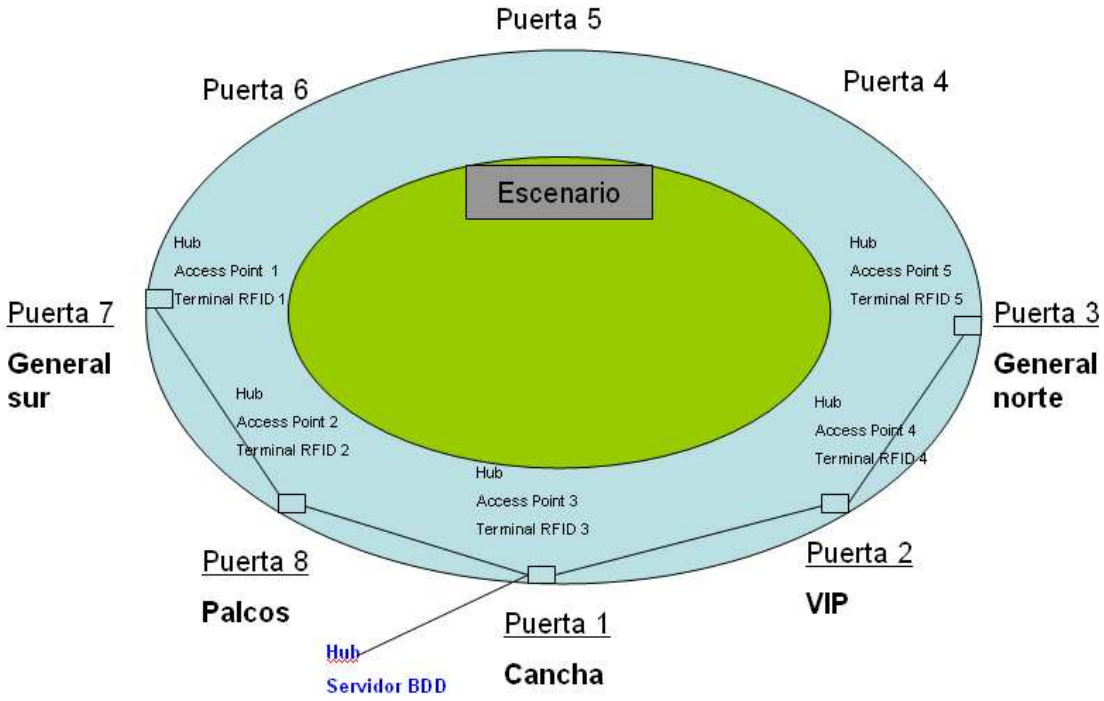


Figura 3.3 Distribución de Equipos.

La instalación del cableado de datos y eléctrico se lo realiza en base a la distribución mostrada en el mapa, una vez terminada toda la instalación se pondrá a operar el recolector de datos (Driver), para hacer pruebas de comunicación y enviar las configuraciones a las terminales RFID.

3.2.3.5 Capacitación y medidas de contingencia.

En esta etapa del desarrollo de un evento es muy importante transmitir el conocimiento acerca del funcionamiento de los equipos de una forma clara y concisa, basados en la experiencia y conocimiento del sistema. Esta capacitación se da al personal que opera las terminales RFID y se lo realiza con la debida anticipación con el objetivo de tener un considerable tiempo de reacción en el caso de la existencia de posibles fallas, los principales puntos sobre los que se hará énfasis son:

- Funcionamiento de las terminales RFID.
- Mensajes posibles para retroalimentación y toma de decisiones
- Medidas a tomar en caso de alguna contingencia

La apertura de puertas para el control de accesos se realiza en base a una hora acordada en base al horario de accesos de los usuarios VIP para los cuales aplica el uso de esta tecnología de identificación.

3.2.4 ADMINISTRACIÓN DEL PROYECTO.

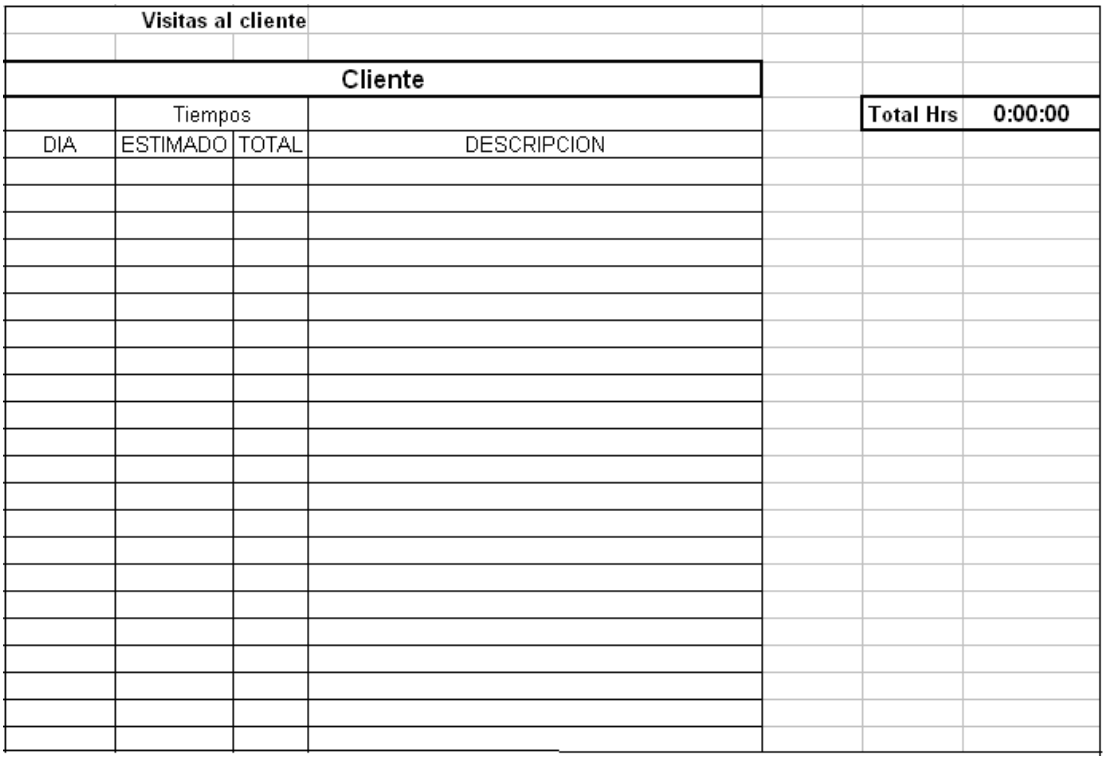
La administración del proyecto se lleva a cabo principalmente por el responsable del área de operaciones, este es el encargado de supervisar y hacer lo necesario para que todos los integrantes del grupo de trabajo cumplan con su parte en el proyecto y con ello cumplir el objetivo inicial. La administración del proyecto comprende:

- Dar seguimiento a todas las tareas del plan de trabajo y generar los avances correspondientes al mismo.
- Respetar los tiempos marcados en el plan de trabajo.
- Documentar formalmente los retrasos que afecten la ejecución del proyecto para que todas las partes estén enteradas.
- Programar la capacitación del personal asignado, por parte del cliente, donde se dará una breve plática de la operación de cada uno de los equipos y las medidas de contingencia que se deben de llevar a cabo para toda situación anormal.

Con el objetivo de determinar el tiempo de implementación se manejará una bitácora interna de visitas y actividades tal como se muestra en la Figura 3.4.
En esta bitácora se llevará un registro de los siguientes parámetros:

- Día: Fecha de la visita al cliente
- Estimado: Es el tiempo de duración que se ha planificado para la visita al cliente.

- Total: Es el tiempo total que toma la visita al cliente.
- Descripción: Detalle de las actividades principales que han sido motivo de la reunión.
- Total Hrs: Es el tiempo total que se ha invertido en todas la reuniones con el cliente.



Visitas al cliente					
Cliente					
	Tiempos			Total Hrs	0:00:00
DIA	ESTIMADO	TOTAL	DESCRIPCION		

Figura 3.4 Bitácora para implementación del proyecto

Así mismo en la administración del proyecto se deben manejar estos puntos como importantes para llevar mejor acabo la implementación.

- Orientación y sensibilización de los miembros del grupo de trabajo, para que exista siempre una comunicación directa con los líderes de proyecto.

- Supervisión continúa por parte del líder de proyecto y todos los responsables para poder detectar cualquier posible retraso y ajustarlo.

- Acontecimiento negativo en el que por ambas partes se genere retrasos o malos entendidos durante la ejecución del proyecto, donde se deberá comunicar a los responsables directos para tomar las acciones pertinentes.

3.3 DESARROLLO DE SOFTWARE DEL PROTOTIPO BÁSICO PARA CONTROL DE ACCESOS UTILIZANDO RFID.

El diseño del prototipo está basado en la filosofía de control de accesos utilizando la tecnología de identificación RFID. Como se mencionó en la sección anterior el prototipo se enfocará en el control de accesos para usuarios VIP y no se lo extiende por el momento a todo el público principalmente por el alto costo de las etiquetas o credenciales RFID ya que actualmente una entrada con código de barras tiene un costo de $0,12 y una credencial RFID $1,05. RFID.

En la siguiente sección se presenta el desarrollo de software para el prototipo utilizando la metodología RUP (Rational Unified Process). Se ha escogido esta metodología debido a que es una metodología estándar más utilizada para el análisis, implementación y documentación de sistemas.

3.3.1 REQUERIMIENTOS DE SOFTWARE

3.3.1.1 Propósito

El desarrollo de este prototipo proporcionará a la empresa soluciones G4 del Ecuador brindar un servicio más de seguridad a los asistentes de un evento por medio de un control de acceso que utiliza una tecnología de identificación de alta confiabilidad. El prototipo está compuesto por módulos de hardware y software los cuales están contemplados para acoplarse a las necesidades actuales y futuras de la empresa.

3.3.1.2 Ámbito del sistema

El prototipo RFID permitirá realizar el ingreso de toda la información de los usuarios VIP al sistema, en base a esta información se generan las credenciales RFID para que luego estas credenciales sean distribuidas a los usuarios respectivos. Al momento del acceso al inmueble el usuario portador de la credencial deberá presentarla para la respectiva validación, proceso que se realizará utilizando las lectoras RFID y así determinar si el usuario esta o no permito ingresar al inmueble.

.

3.3.2 DESCRIPCIÓN GENERAL

En esta sección se detallan todos los factores que afectan al correcto funcionamiento del prototipo.

3.3.2.1 Perspectiva del Producto

La parte de software de este prototipo deberá ser instalado en la plataforma Windows XP, además se necesita el software de base de datos Microsoft Access.

3.3.2.2 Funciones del Producto

Las funciones que proporciona el prototipo son las siguientes:

- Ingreso de usuario y clave para acceso al software de registro de usuarios.
- Creación de eventos
- Ingreso de toda información que se requiere para crear una credencial RFID para un usuario.
- Se realizará la lectura de las credenciales por medio de las lectoras RFID
- El sistema guardará la información producto de la lectura de accesos en la base de datos y se enviará un mensaje indicando si el usuario esta o no permitido ingresar
- Finalmente el sistema generará un reporte de accesos de todos los usuarios que hayan ingresado al inmueble.

3.3.2.3 Características de los Usuarios

Este producto será utilizado por el departamento de sistemas de la empresa Soluciones G4 del Ecuador, los usuarios de dicho departamento serán los encargados de la operación y puesta en marcha del prototipo.

3.3.2.4 Restricciones

- La administración del prototipo estará a cargo del jefe del departamento de sistemas quién debe tener los suficientes conocimientos acerca de tecnologías de control de accesos y administración de bases de datos.
- El ingreso al sistema por parte del administrador se efectuará por medio de su respectivo login y password.
- La frecuencia de operación de las lectoras RFID es de 13,56 MHz
- Para la comunicación inalámbrica de las Terminales RFID con el resto del sistema se utilizará el estándar de comunicaciones IEEE 802.11b.
- El presente proyecto luego de entrar en operación será susceptible a cualquier comentario o sugerencia que contribuyan a su mejoramiento.

3.3.2.5 Requisitos Futuros

El presente proyecto está sujeto a mejoras en la funcionalidad, mejoras que no afectarán en sus requisitos de software a futuro, debido a la flexibilidad de su diseño y de las herramientas con que fue diseñado.

3.3.3 REQUISITOS ESPECÍFICOS

En esta sección se describen los requisitos tanto de software como de hardware para el desarrollo del prototipo.

3.3.3.1 Requisitos de Software

Los paquetes utilizados para la implementación del prototipo RFID, son los siguientes:

- Microsoft Visual Basic 6.0 (Herramienta de desarrollo para el software de generación de credenciales)
- Microsoft Visual.NET (Herramienta de desarrollo para el software de control de accesos)
- Microsoft Windows XP Profesional. (Sistema Operativo)
- Microsoft Windows CE.NET Versión 4.10 (Sistema Operativo de la Terminal RFID)
- Microsoft Access 2003. (Base de Datos)

3.3.3.2 Requerimientos de Hardware

Los componentes de hardware que forman parte del prototipo son:

- Lector RFID HF MIFARE DESFire contactless.
- Terminal Lan Point Mobile Texas Instruments.
- Etiquetas MIFARE HF.
- Access Point.
- Equipo servidor de BDD.
- Impresora Evolis Dualys 3 ID.

Se ha escogido este hardware con el objetivo de dar un uso óptimo a los equipos ya existentes en la empresa especialmente a la LanPoint Mobile (Terminal) la cual tiene un costo considerable ($1600), actualmente esta Terminal se la utiliza para la lectura de boletos a espectáculos cuya tecnología de identificación es el código de barras y con la implementación de esta solución se le da un doble uso en una misma eventualidad ya que este equipo trabajaría con 2 tecnologías de identificación.

3.3.3.2.1 Lector RFID HF MIFARE DESFire contactless.

Descripción:

El lector RFID forma parte de la Terminal y es el encargado de realizar el proceso de lectura de las credenciales que portan los usuarios VIP. Para el proceso de lectura se procede a instalar el lector en la interfaz COMPACT FLASH de la Terminal, el usuario debe aproximar su credencial al lector a una distancia máxima de 2cm para que ésta sea validada. La selección de este hardware se lo ha realizado basándose en la compatibilidad que éste tiene con la Terminal LanPoint para darle el uso antes mencionado.

Figura 3.5 Lector RFID HF Mifare

En la tabla 3.2 se muestran las principales características técnicas del lector

Lector RFID HF MIFARE	
Característica Técnica	**Descripción**
Frecuencia de operación	13,56 MHz
Interface de comunicación	Compact Flash
Normalización	ISO 14443ª ISO 14443B ISO 15693 ISO 18000-3 ICODE NFC(Near Field Communication)
Velocidad de transmisión	848 Kbps
Protocolo de Comunicación	ASCII Binario

Tabla 3.2 Características técnicas Lector RFID HF MIFARE

Mas especificaciones técnicas y características del equipo se muestran en el Anexo A.

3.3.3.2.2 Terminal LAN Point Mobile Texas Instruments.

Descripción:

La Terminal LAN POINT MOBILE es un computador de mano la cual tiene las mismas características y funcionalidades de un computador cualquiera, para efectos del prototipo la terminal realiza la función de la controladora la cual se encargará de enviar una orden de disparo a un equipo el cual permitirá el acceso o no del usuario, para este caso la Terminal enviará únicamente una señal en pantalla indicando si el usuario puede o no acceder al sitio.

Toda la información que sea validada por la Terminal será enviada al Driver utilizando su interfaz de Red inalámbrica la misma que tiene un alcance de aproximadamente 10m bajo nuestras condiciones de trabajo, se menciona este parámetro para poder determinar la distancia máxima que puede estar separada la Terminal del Access Point respectivo; cabe también recalcar que estas distancias varían en base al ambiente de trabajo es decir depende de las interferencias de las señales de radio y de los obstáculos existentes, por estos motivos es importante realizar las pruebas de conectividad de los equipos.

Figura 3.6 Terminal LAN Point Mobile.

Con el objetivo de realizar una comparación con otros fabricantes se ha escogido el modelo de handheld Symbol Motorola MC9090, dicho equipo tiene un costo de $3300 frente al costo de la LanPoint Mobile de $1600 es conveniente seguir utilizando el equipo propuesto.

Desde el punto de vista técnico el fabricante Motorola ofrece mejor características ya que es netamente una Terminal RFID pero nuestra Terminal satisface en su totalidad nuestras necesidades por lo que se opta por utilizar la Terminal LanPoint Mobile.

En la tabla 3.3 se muestran las principales características técnicas del equipo.

Terminal Lan Point Mobile Texas Instruments	
Característica	**Descripción**
Sistema Operativo	Windows CE .NET 4.2
Procesador	Intel Xscale PXA255, 400MHz
Memoria RAM	128 MB
Memoria Flash	96 MB
Interface de comunicación	Compact Flash
Estándar WLAN	IEEE802.11b

Tabla 3.3 Características técnicas Terminal LAN Point Mobile

Más especificaciones técnicas y características del equipo se muestran en el Anexo B

3.3.3.2.3 Etiqueta MIFARE HF.

Descripción:

Las etiquetas o credenciales RFID contienen un numero único de 10 dígitos dicho número es asociado a un usuario del sistema por medio del módulo de software de registro de usuarios a partir de esta asociación el usuario queda atado a una única credencial RFID la cual es inviolable e intransferible por lo que sólo el usuario permitido podrá hacer uso de la misma.

Figura 3.7 Etiqueta RFID Mifare HF.

En la tabla 3.4 se muestran las principales características técnicas de la etiqueta.

Etiqueta RFID Mifare HF	
Característica	**Descripción**
Estándar	MIFARE
Tipo	Lectura/Escritura
Capacidad de almacenamiento	1 Kbyte

Tabla 3.4 Características técnicas etiqueta RFID MIFARE HF

Más especificaciones técnicas y características de la etiqueta se muestran en el Anexo C.

3.3.3.2.4 Access Point Linksys WAP11.

Descripción:

Este quipo lo que permite es realizar una interconexión inalámbrica entre la Terminal RFID y el servidor de Base de Datos. Tal como se muestra en la siguiente figura:

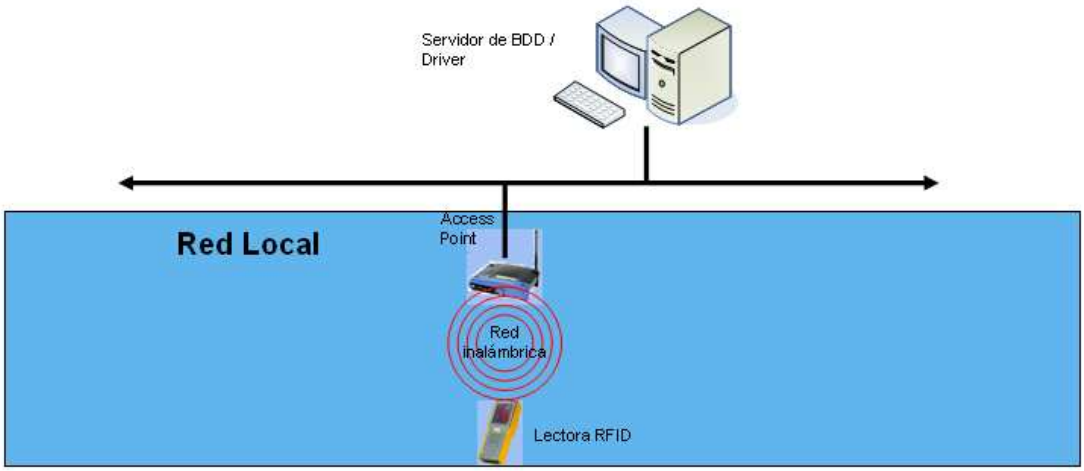


Figura 3.8 Diagrama de la Red de accesos

Para la selección de este equipo se ha comparado con la otro fabricante similar DLINK 2100AP los costos son más económicos ($65) pero este fabricante no ofrece la robustez debida ante interferencias del medio como las señales de radio, televisión, equipos de audio y sonido que se suelen instalar en los escenarios de eventos. Se han realizado pruebas en el ambiente de trabajo que son los escenarios de espectáculos públicos y el access point DLINK 2100AP no mantiene estable la comunicación, esto por las interferencias antes mencionadas, este es un factor muy importante para la aplicación ya que el ambiente de trabajo está sometido a muchas interferencias. Razón por la cual se ha escogido este modelo de access point que es el Lynksys WAP11 ($95) ya que éste brinda más estabilidad en las comunicaciones del medio en el cual opera el prototipo.

En la tabla 3.5 se muestran las principales características técnicas del equipo.

Access Point Linksys WAP11	
Característica Técnica	**Descripción**
Modelo	WAP11 ver. 2.2
Estándar WLAN	IEEE 802.11b
Algoritmo de cifrado	WEP 256 bits
Rango de operación	Indoor: 90 m Outdoor: 300 m

Tabla 3.5 Características técnicas Access Point Linksys WAP11

.

Más especificaciones técnicas y características del los access points mencionados se muestran en el Anexo D

3.3.3.2.5 Equipo servidor de BDD.

En este equipo se encuentran alojadas las Bases de Datos **accesos_db.mdb** y **res_110208_XOCH.mdb** donde se almacena la información tanto de los usuarios así como también de los accesos. El módulo de recolección de datos se ejecuta en este equipo y es el encargado de consultar y almacenar la información producto de los accesos tal como se explica en la guía de usuario contemplada en el ANEXO F

3.3.3.2.6 Impresora Evolis Dualys 3 ID.

Descripción:

Este equipo se lo utiliza para la impresión de las credenciales RFID, se ha escogido este equipo principalmente por las características que éste presenta las mismas que permiten tener un uso óptimo para de esta manera poder justificar su precio.

Figura 3.9 Impresora Evolis Dualys 3 ID

Cabe recalcar que para el presente proyecto no se adquiere la impresora por su alto costo ($1900), solamente se rentará el producto para efectos de demostración de la funcionalidad del prototipo.

En la tabla 3.6 se muestran las principales características técnicas del equipo.

Impresora Evolis Dualys 3 ID	
Característica	**Descripción**
Resolución	300 dpi
Codificación	Credenciales RFID de 13.56 Mhz Banda Magnética
Velocidad de impresión	50 Tarjetas/Hora
Interface	USB
Memoria RAM	16 MB

Tabla 3.6 Características Impresora Evolis Dualys 3 ID

Más especificaciones técnicas y características de este equipo se muestran en el Anexo E

3.3.4 DISEÑO E IMPLEMENTACIÓN DEL PROTOTIPO RFID

En esta sección se define el proceso de desarrollo de software de los diferentes módulos que componen el Prototipo RFID.

3.3.4.1 Proceso de desarrollo de Software

Un proceso de desarrollo de software define quién debe hacer *Qué, Cuándo y Cómo* debe hacerlo. No existe una metodología de desarrollo de software universal. Las características de cada proyecto exigen que el proceso sea configurable y adaptable.

3.3.4.2 RUP (Rational Unified Process)

RUP (Rational Unified Process) es un proceso de desarrollo de software que define claramente quien, cómo, cuándo y qué debe hacerse; además su enfoque

está basado en modelos que utilizan un lenguaje bien definido conocido como UML. Utiliza herramientas como los casos de uso, que definen los requerimientos; la ejecución iterativa y control de riesgos. Se centra en la producción y mantenimiento de modelos del sistema más que en producir documentos.

3.3.4.2.1 Características de RUP

Las características principales de RUP son:

- **Dirigido por los Casos de Uso:** Los casos de uso y los escenarios permiten captar los requerimientos necesarios, para el diseño, implementación y pruebas.
- **Centrado en la Arquitectura:** Se debe diseñar una arquitectura base ejecutable, la cual debe ser: flexible, fácil de modificar y comprensible.
- **Guiado por los Riesgos:** La funcionalidad es esencial pero también se debe tomar en cuenta el rendimiento y la confiabilidad, los cuales apoyan a: planificar, diseñar, implementar, ejecutar y evaluar pruebas que verifiquen estas cualidades.
- **Promueve la reutilización de componentes:** Con una estructura base y flexible, la reutilización de los componentes será más fácil para cualquier implementación futura.
- **Iterativo e Incremental:** Un proceso iterativo permite una comprensión creciente de los requerimientos a la vez que se va haciendo crecer el sistema, con lo cual los riesgos del proyecto disminuyen.
- **Modelamiento visual del software:** UML es la base del modelamiento visual de RUP.
- **Control de cambios:** Los cambios son inevitables, pero se debe evaluar si éstos son necesarios y además se debe indagar su impacto.

3.3.4.2.2 Elementos de RUP

Los elementos presentes en la metodología RUP son los siguientes:

- **Actividades**: Procesos que se llegan a determinar en cada iteración.
- **Trabajadores:** Personas involucradas en cada proceso.
- **Artefactos:** Un artefacto puede ser un documento, un modelo, o un elemento de modelo.

3.3.4.2.3 Fases del desarrollo del Software

La metodología RUP se divide en 4 fases de desarrollo:

- **Inicio o Conceptualización**: El objetivo es determinar la visión y alcance del proyecto. Aquí se identifican todas las entidades externas, todos los casos de uso describiendo algunos en detalle.
- **Elaboración:** Los objetivos de esta etapa son: analizar el dominio del problema, establecer una arquitectura sólida y eliminar los elementos de mayor riesgo para tener éxito en el proyecto.
- **Construcción:** En esta etapa el objetivo es llegar a obtener la capacidad operacional inicial. Construir una versión BETA, la cual es probada a profundidad. Realizar un manual de usuario.
- **Transmisión o Transición:** El objetivo es llegar a obtener el producto final y proporcionar la aplicación a los usuarios finales.

El ciclo de vida que se desarrolla en cada iteración, trabaja bajo dos disciplinas:

- **Disciplina de Desarrollo**
    - Ingeniería de Negocios.
    - Requerimientos.
    - Análisis y Diseño.
    - Implementación.

- Pruebas.

➢ **Disciplina de Soporte**

- Configuración y administración del cambio.
- Administrando el proyecto.
- Ambiente.
- Distribución.

Las fases e iteraciones se encuentran representadas en la figura 3.10.

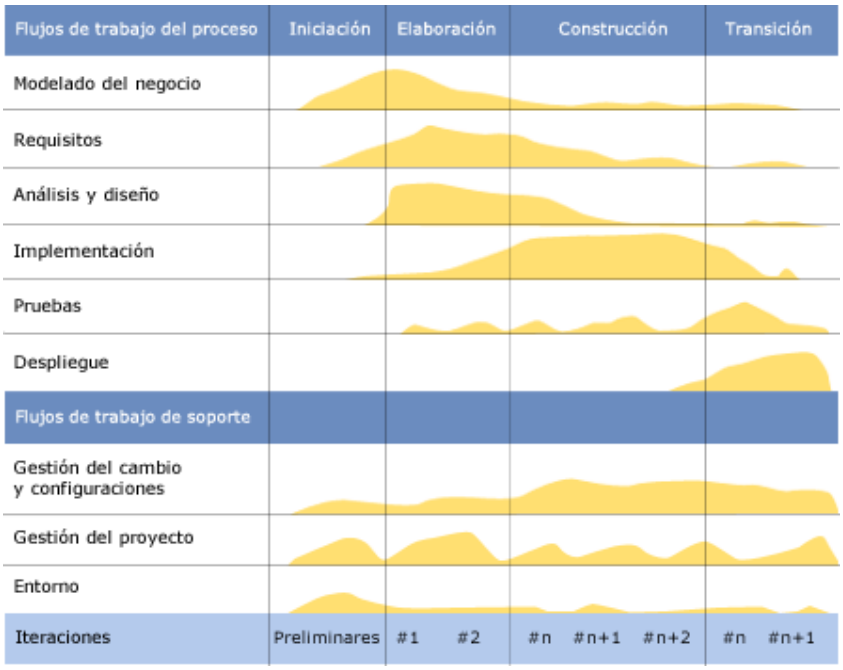


Figura 3.10 Fases e Iteraciones de la Metodología RUP[60]

3.3.4.2.4 Fase de Inicio

El proyecto tiene como visión proporcionar a la empresa Soluciones G4 del Ecuador un prototipo el cual permita ilustrar el uso de una nueva tecnología de identificación para eventos masivos como lo es la tecnología RFID,

El prototipo se enfocará al control de accesos para usuarios VIP(Personas muy importantes) y no se lo extiende por el momento a todo el público principalmente por el alto costo de las etiquetas o credenciales RFID ya que actualmente una

[60] www.informatizate.net/articulos/metodologias_de_desarrollo_de_software_07062004.html

entrada con código de barras tiene un costo de $0,12 y una credencial RFID $1,05. RFID.

El alcance del proyecto será desarrollar e implementar un prototipo básico que permita ilustrar el uso y la funcionalidad de la tecnología RFID para control de accesos.

3.3.4.2.4.1 Casos de Uso

- **Proceso de generación de credenciales RFID:**

  Actor Principal: Administrador

  Personal Involucrado e intereses:

  Administrador: Registrar toda la información del usuario para el cual se va a generar la credencial RFID, revisar que la información esté correctamente almacenada en el sistema y además imprimir la credencial RFID.

  Precondiciones: El administrador necesita un archivo en formato Excel el cual contenga toda la información de los usuarios para los que se van a generar las credenciales RFID.

  Garantías de éxito: Se registra toda la información del usuario para luego generar una vista previa de la credencial y seguidamente proceder a imprimirla.

  Escenario de éxito (Flujo Básico):

  - El administrador ingresa a su computador, abre el "**Software de Registro de usuarios",** se autentica y luego escoge la opción **Usuarios->Administración de Usuarios**
  - El administrador selecciona el botón **Nuevo** para crear un nuevo usuario e iniciar el proceso de creación de una credencial.

- Aquí el administrador ingresa el nombre, código de credencial RFID, nombre del evento, horario permitido para el acceso. Luego da clic en **Guardar** para guardar la información del usuario
- Una vez que está almacenada la información del usuario el administrador da clic en **Imprimir** para generar la vista previa del diseño de la credencial RFID.
- Se procede a presionar el icono de imprimir el cual permite generar la credencial RFID con la información del usuario.
- Una vez que se termina de generar las credenciales se procede a realizar la distribución a los usuarios respectivos.
- Si se presenta algún problema durante el proceso el sistema enviará el mensaje indicando un detalle del problema.

Extensiones (Flujo Alternativo):

a. La información del usuario debe ser ingresada correctamente:

- Para ingresar la información del usuario cada campo del formulario de ingreso de datos tendrá su propio cuadro de ayuda el cual se mostrará automáticamente al momento que se apunte con el mouse sobre el campo respectivo.
- El proceso de ingreso de un nuevo usuario finaliza cuando se de clic en guardar y el sistema confirmará que la información ha sido almacenada correctamente.

b. La información impresa en la credencial RFID no es la correcta:

- Una vez que se ha terminado de guardar la información del usuario se procede a imprimir la credencial RFID, si la información no es la correcta se procede a editar la información del usuario, para lo cual se debe escoger al usuario y presionar doble clic, luego se mostrara la pantalla que contiene todos los datos del usuario para la modificación respectiva, una vez que se

termine de editar la información se procede a dar clic sobre el botón guardar.

- Al momento de editar la información de un usuario por un error de impresión de debe actualizar también el numero de la credencial, caso contrario el sistema de accesos no podrá validar esa credencial RFID.

- **Configuración de la Red Accesos**

Actor Principal: Administrador.

Personal Involucrado e intereses:

Administrador del Sistema: Diseñar la red de control de accesos en base a las puertas o accesos que se desee habilitar.
Jefe de Instalaciones: Realizar la instalación de toda la Red para control de accesos en base al diseño propuesto por el administrador del sistema.
Precondiciones: El Administrador realiza las pruebas de conectividad y funcionamiento de los equipos que forman parte de la red de control de accesos.

Garantías de éxito: Se tiene una Red para transmisión de datos lista para ser puesta en marcha.

Escenario de éxito (Flujo Básico):

- El administrador diseñará una Red de infraestructura la cual se adaptará a los requerimientos de accesos, es decir en base a las puertas que se desee habilitar en cada puerta deberá existir una lectora RFID la cual se comunicará de manera inalámbrica con el resto de los equipos en la red.

- Una vez realizado el diseño de la red se entregará dicho diseño al jefe de instalaciones el cual se encargará de realizar el cableado y las pruebas de conectividad respectivas.
- El administrador deberá validar las pruebas de conectividad y además verificar el funcionamiento adecuado de todos los equipos de la red de control de acceso.

Extensiones (Flujo Alternativo):

b. Falla en las pruebas de conectividad:

- Si se presentan errores de conectividad se deberán hacer pruebas de conectividad segmento a segmento en la red con el objetivo de determinar que segmento tiene problemas de conectividad y determinar la falla existente.

- **Cargar el Software para control accesos**

Actor Principal: Administrador.

Personal Involucrado e intereses: Administrador del Sistema: Enviar todas las configuraciones para control de acceso a las lectoras RFID.

Precondiciones: El Administrador verifica que el envío de configuraciones se ha realizado correctamente.

Garantías de éxito: Se tiene todas las Terminales RFID con las configuraciones adecuadas y listas para empezar la lectura de credenciales.

Escenario de éxito (Flujo Básico):

- El administrador abre el software de control de accesos (Driver)
- Selecciona la opción de **Envíos**

- Escoge las Terminales RFID que estarán activas para el control de acceso.
- Escoge los parámetros **Fecha-Hora** y **Configuración**
- Presiona el botón **Enviar** para que se realice el proceso de envío de todos los parámetros hacia las terminales RFID
- El administrador deberá validar que el envío de parámetros sea satisfactorio caso contario debe realizar nuevamente el envío.

Extensiones (Flujo Alternativo):

c. Falla en el envío de parámetros de Fecha-Hora y Configuración :

- Si se presentan errores en el envío de estos parámetros, en la terminal RFID no se verán reflejados la fecha y hora del Equipo servidor de Base de Datos. En este caso es necesario realizar nuevamente el envío de estos parámetros.

3.3.4.2.4.2 Pronóstico Financiero y Criterios de Éxito

En lo referente al pronóstico financiero sería muy difícil expresarlo debido a que durante la elaboración del prototipo se encontrarán algunas inconvenientes, los cuales podrán tomar más o menos tiempo para solucionarlos. El análisis financiero se explica detalladamente en la sección 3.5, aquí se hará mención al tiempo empleado para la realización del prototipo, compra de equipos y realización de pruebas.

Los criterios de éxito serán: desarrollar un prototipo que no posea ninguna falencia, garantizando así la seguridad en los accesos al inmueble; que sea de fácil uso y comprensión para las personas encargadas de su administración; escalable, lo que permitirá a la empresa añadir mejoras para el prototipo.

3.3.4.2.4.3 Identificación Inicial de riesgos

Los riesgos que pueden presentarse al inicio, transcurso y finalización del proyecto se detallan a continuación:

- No permitir el uso del software recolector de datos (Driver), herramienta que se encuentra actualmente en desarrollo en la empresa Soluciones G4 del Ecuador, esta herramienta es un componente esencial para el desarrollo del proyecto.

- Existir un fallo en el funcionamiento de la tarjeta lectora de credenciales RFID con lo cual las garantías de éxito se verían retardadas o no se cumplirían ya que se tendría que importar una nueva tarjeta.
- Que no se tenga el apoyo total de la empresa para el desarrollo e implementación del prototipo.
- Los objetivos de aumento de seguridad en los accesos a inmuebles no se lleguen a cumplir, debido a que no exista una aceptación debida por parte de los usuarios.
- Que al momento que se efectúa el control de acceso exista un sabotaje contra los componentes del sistema por un agente desconocido, por lo que el funcionamiento del sistema se vería afectado en un cierto porcentaje.
- Catástrofes naturales.

3.3.4.2.5 Fase de Elaboración.

Es la parte más crítica del proceso, a partir de aquí la arquitectura, los requerimientos y los planes de desarrollo deben ser estables; existen menos riesgos y se puede planificar el resto del proyecto con menor incertidumbre. Esta fase se encuentra contemplada en las siguientes secciones.

.

3.3.4.2.5.1 Analizar el dominio del problema y requerimientos adicionales para el administrador durante el proceso de generación de credenciales y control de accesos.

Como requerimiento adicional para una correcta realización del proceso de generación de credenciales se necesita tener a la mano el archivo en formato Excel que contenga toda la información de los usuarios para los que se va a generar las credenciales RFID

Existe un gran problema que son las aglomeraciones que se pueden formar en las puertas al momento del ingreso al inmueble. Para brindar una solución a esto se tendrá un las puertas más criticas una Terminal RFID de respaldo la cual permita solventar este problema.

Otro inconveniente es que al tener instalada en el inmueble una red de comunicaciones la cual contiene equipos activos se tiene el riesgo de no tener una disponibilidad total de la energía eléctrica lo que conduce a un fallo en la red de comunicaciones. Para contrarrestar este inconveniente las Terminales RFID tendrán la opción automática de almacenar en su memoria RAM todos los registros leídos mientras se restablece la red de comunicaciones y una vez que todo vuelva a la normalidad las Terminales enviarán sus registros almacenados hacia el servidor que recolecta toda la información de los accesos.

3.3.4.2.5.2 Establecer una arquitectura sólida

En la figura 3.11 se detalla la interacción del administrador con el sistema para realizar el proceso de generación de las credenciales RFID, para la representación de los diagramas de caso de uso se utilizará el modelo de dominio, el cuál es una representación de los objetos conceptuales del mundo real en un dominio de interés.

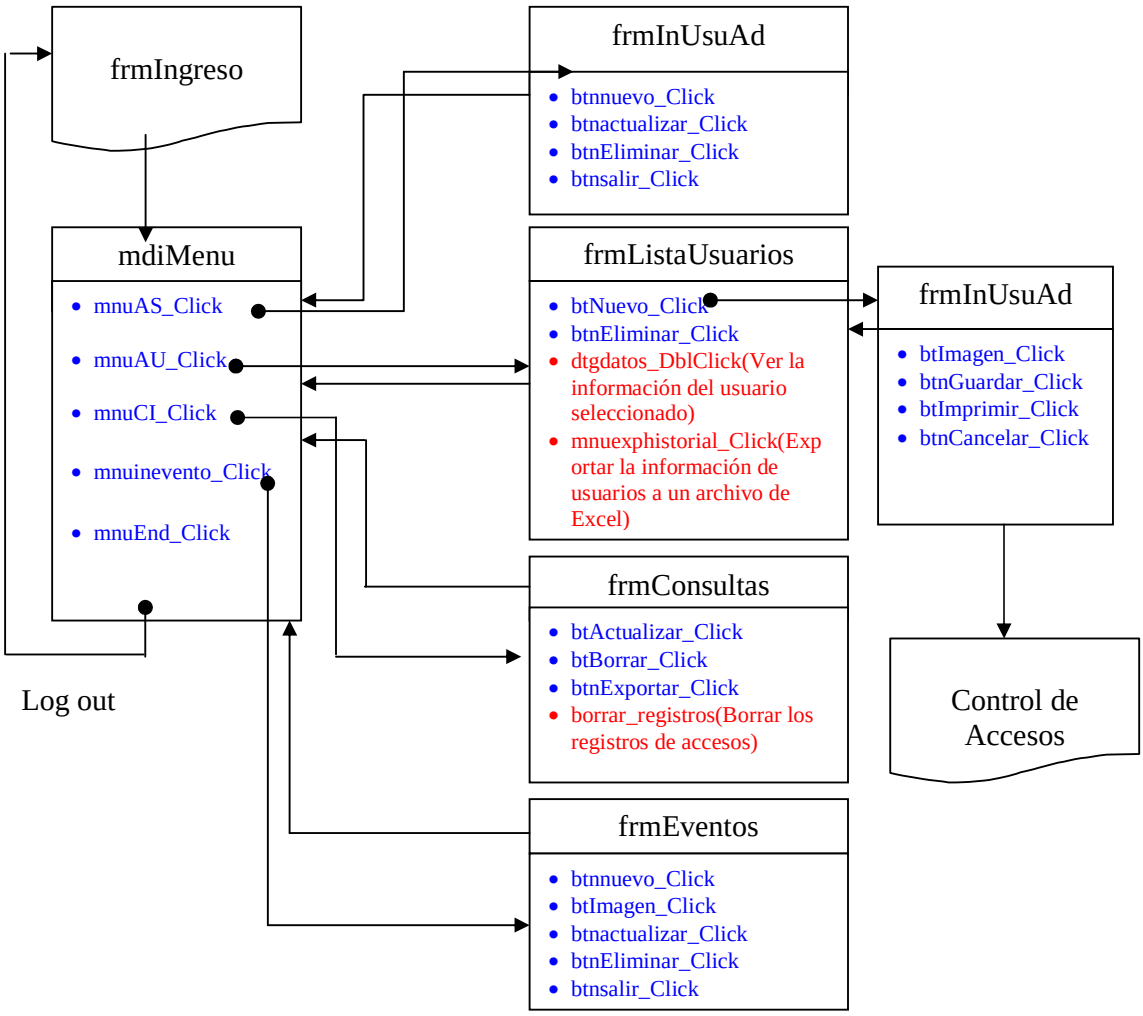


Figura 3.11 Diagrama de caso de uso del Software de registro de Usuarios.

3.3.4.2.5.3 Eliminación de los elementos de mayor riesgo.

Durante esta fase los elementos de mayor riesgo son solucionados para así alcanzar el éxito del proyecto y cumplir con los objetivos propuestos. Los elementos de mayor riesgo superados son:

- Permitir el uso del software recolector de datos (Driver).
- Fallo en el funcionamiento de la tarjeta lectora de credenciales RFID.
- Apoyo total de la empresa para el desarrollo e implementación del prototipo.
- Sabotaje contra los componentes del sistema

3.3.4.2.6 Fase de construcción

En esta fase todos los componentes restantes se desarrollan e incorporan al producto. Todo es probado en profundidad, se pone énfasis en la producción de la herramienta para que ésta sea eficiente y no contenga ninguna falencia. En esta fase se presenta la herramienta final que será utilizada en el ambiente real.

3.3.5 DESARROLLO DE SOFTWARE DE LOS MÓDULOS DEL PROTOTIPO RFID

El prototipo está compuesto por los siguientes módulos.

- Software de registro de usuarios.
- Software recolector de datos (Driver).
- Software de la Terminal RFID.

Es importante aclarar que el Software recolector de datos (Driver) y el Software de la Terminal RFID son módulos propietarios de la empresa Soluciones G4 del Ecuador, dichos módulos se encuentran actualmente en desarrollo y por tal razón no se entrará en detalles de desarrollo de estos dos módulos y para el presente proyecto se los utiliza como una herramienta que permita ilustrar la funcionalidad del prototipo. El módulo que si se ha desarrollado como aporte al presente proyecto es el Software de registro de usuarios cuyo detalle del desarrollo se lo presenta a continuación.

3.3.5.1 Desarrollo de Software de Registro de Usuarios

3.3.5.1.1 Fase de elaboración.

3.3.5.1.1.1 Analizar el dominio del problema y requerimientos adicionales para los usuarios del sistema.

Un serio problema para un usuario es que pierda su credencial RFID si se da este caso el usuario deberá notificar al administrador del sistema para que proceda a anular la credencial en el sistema y proceder a generar una nueva credencial para ese usuario.

Un serio problema para el administrador es no disponer de un respaldo de toda la información de las credenciales generadas. Para evitar esto es muy importante se realice un respaldo de la Base de Datos apenas se termine de generar las credenciales para un cierto evento.

3.3.5.1.1.2 Establecer una arquitectura sólida

En la figura 3.12 se detalla el proceso para la generación de las credenciales RFID. Para esto el administrador debe ingresar su respectivo login y password los cuales serán validados por el sistema luego se ingresará al módulo de usuarios donde se realizará el proceso de generación de un nuevo usuario y luego de esto proceder a imprimir la credencial RFID.

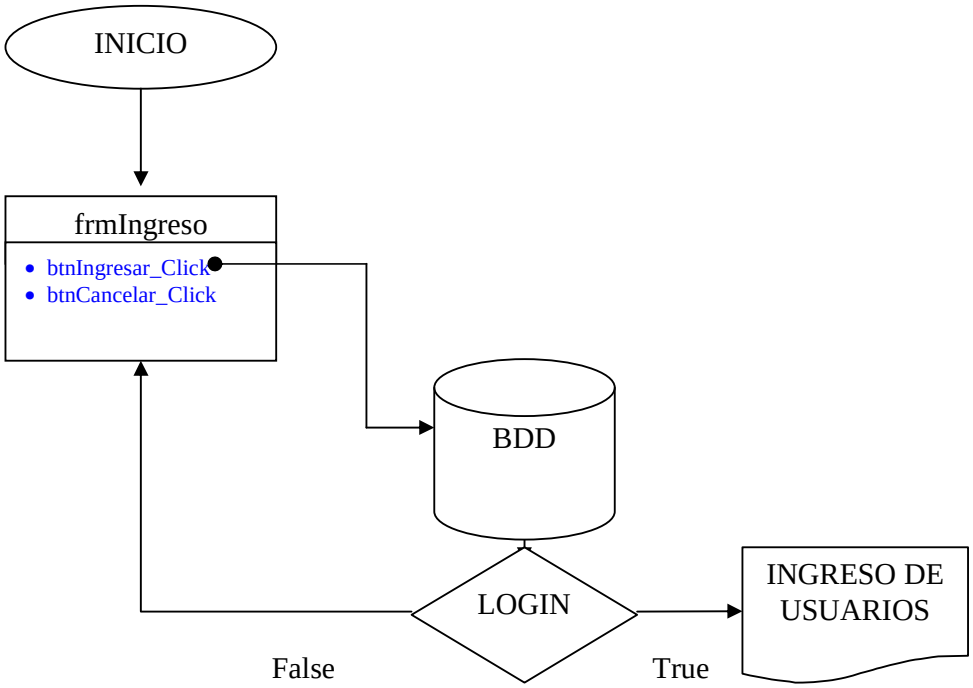


Figura 3.12 Diagrama de caso de uso del Software de Registro de usuarios para el Administrador

3.3.5.1.2 Diagrama de diseño

Los diagramas de diseño tienen como objetivo proporcionar una representación gráfica de cómo está implementado el sistema. Existen varios tipos de diagramas que permiten representar el diseño de un sistema, pero el más utilizado es el Diagrama Clase – Objeto.

3.3.5.1.2.1 Diagrama Clase - Objeto

El gráfico de la figura 3.13 representa el diagrama de clase – objeto del proyecto. Esto es una forma de representar gráficamente como se encuentra desarrollado el proyecto en base a sus clases y objetos utilizados para su implementación.

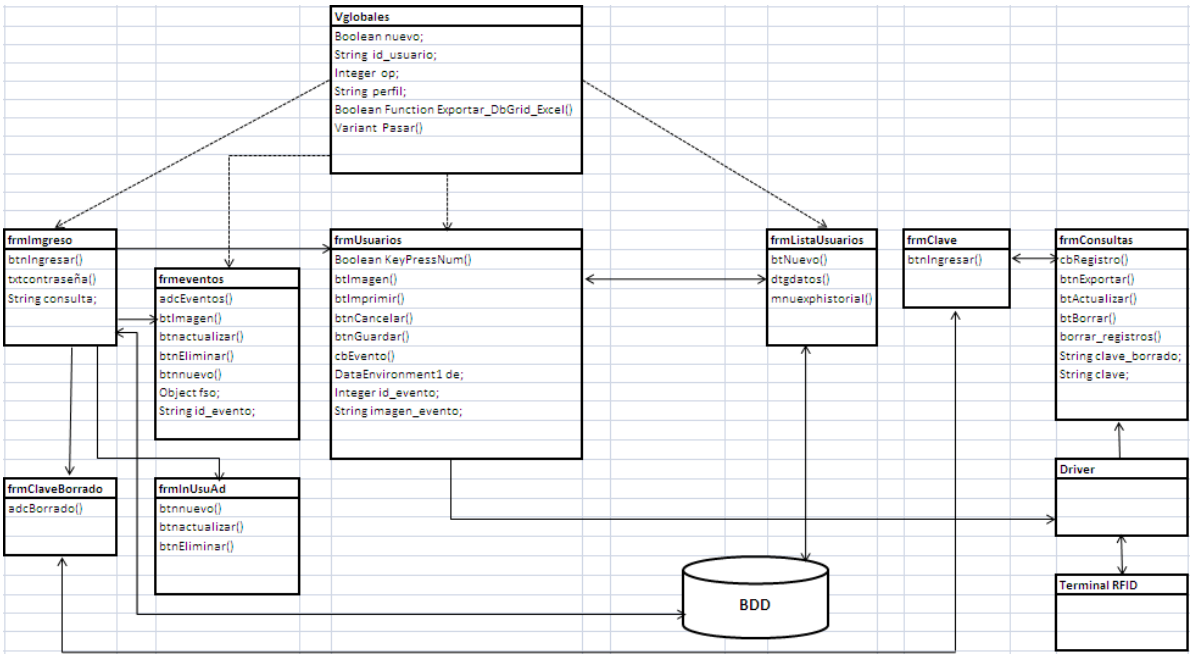


Figura 3.13 Diagrama Clase-Objetos

3.3.5.1.3 Diagrama de interfaz

Los diagramas de interfaz tienen como objetivo proporcionar una representación gráfica del interfaz del sistema y como se navega a través de él. Existen algunos tipos de diagramas que permiten representar la interfaz de un sistema, pero los más utilizados son: diagrama secuencial y diagrama de estado.

3.3.5.1.3.1 Diagrama Secuencial

Este diagrama representa un escenario específico del flujo de éxito del caso de uso, los eventos que generan los actores externos, el orden y los eventos entre los sistemas. La secuencia avanza hacia abajo y la ordenación de los eventos sigue el orden del flujo de éxito del caso de uso. En la figura 3.14 se ilustra el diagrama secuencial del prototipo RFID.

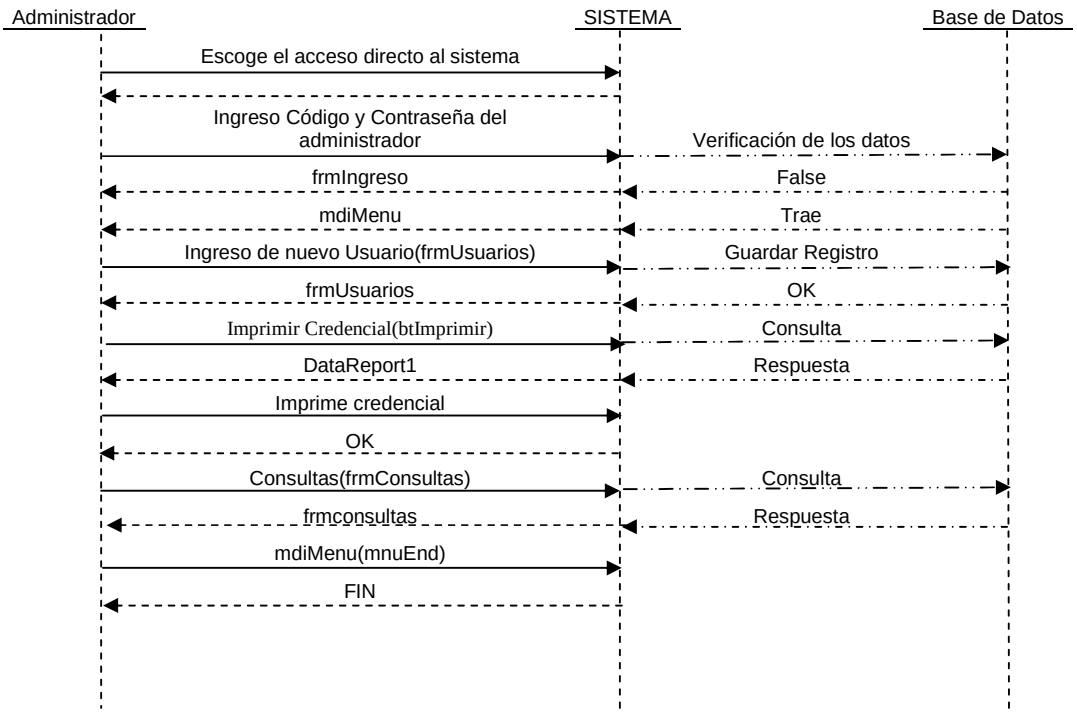


Figura 3.14 Diagrama secuencial para el Administrador

3.3.5.1.3.2 Diagrama de Estado

Cada uno de los objetos en un sistema pasa a través de una serie de estados. Un estado es la condición de un objeto en un momento dado. Los diagramas de estado proporcionan a los desarrolladores una manera de expresar cómo y bajo qué condiciones, los objetos cambian de estado en un sistema. A través de estos diagramas se modela el flujo de trabajo de los objetos durante la ejecución de los sistemas. En la figura 3.15 se ilustra el diagrama de estado para el prototipo RFID.

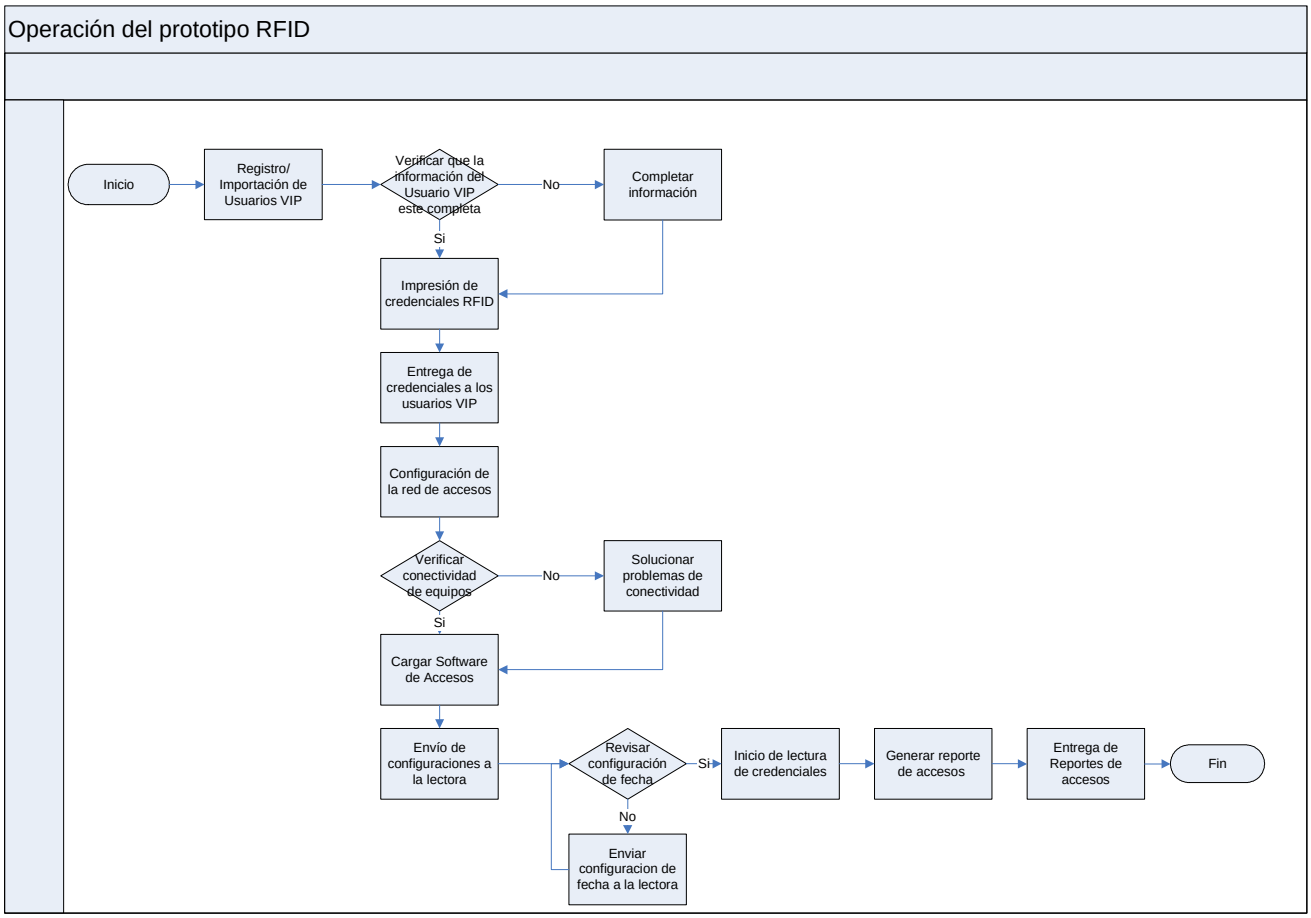


Figura 3.15 Diagrama de estado para el registro de usuarios

3.3.6 DESCRIPCIÓN TÉCNICA DE LOS MÓDULOS DEL PROTOTIPO RFID

3.3.6.1 Software

La parte de software está estructurada de los siguientes módulos:

- Software de registro de usuarios.
- Software recolector de datos (Driver).
- Software de la Terminal RFID.

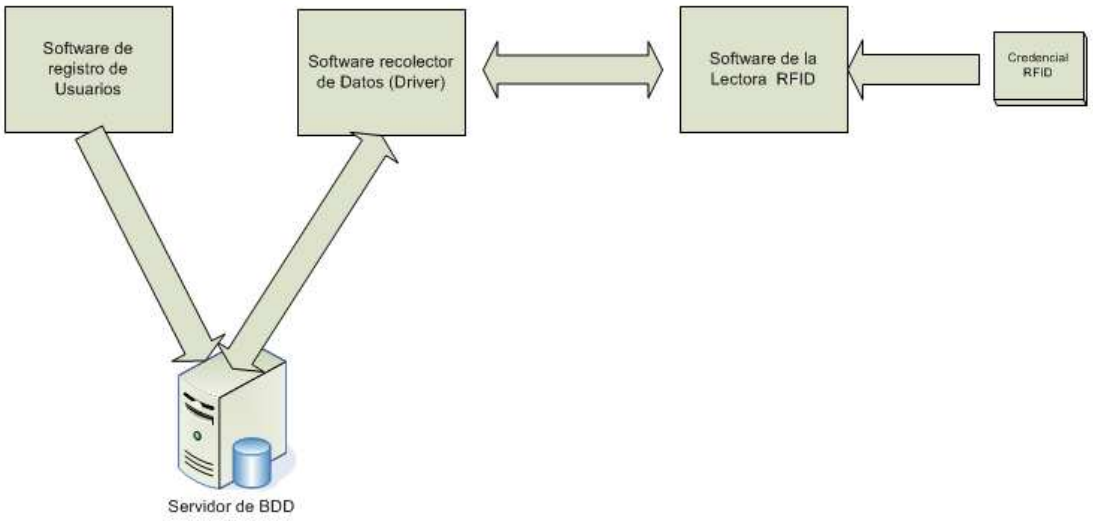


Figura 3.16 Diagrama de Bloques del prototipo RFID

En la figura 3.16 se muestra cada uno de los módulos del prototipo, los mismos que tienen su funcionalidad específica dentro del mismo. A continuación se presenta la descripción del diseño de cada uno de los módulos.

3.3.6.1.1 Software de registro para usuarios VIP

El desarrollo de este módulo se lo ha realizado utilizando las siguientes herramientas de software:

- Base de Datos: Microsoft Access 2003.
- Diseño de interfaz: Visual Basic 6.0.

Se escogido como Base de Datos a Microsoft Access por las siguientes razones:

- La aplicación no va a manejar una gran cantidad de registros y por ende su rendimiento no se vería afectado, ya que como se menciona en la sección 3.5.1.4 la cantidad de credenciales RFID promedio que se va a emitir por evento es de 600 y en promedio al año se tendrían 7200 registros, cantidad que no afectaría en su rendimiento óptimo. Adicional a esto se realizará un mantenimiento de la base de datos cada 6 meses.

- La empresa ya cuenta con la licencia de software para esta base de datos y por un tema de ahorro de costos se ha optado escoger esta base de datos.

Como herramienta de desarrollo se ha escogido Visual Basic 6.0 por las siguientes razones:

- La empresa ya cuenta con la licencia de software para el desarrollo y por un tema de ahorro de costos se ha optado escoger esta herramienta de desarrollo.
- La aplicación básica para el prototipo planteada en el alcance del proyecto opera en modo cliente servidor y esta herramienta de desarrollo se adapta a esta necesidad.
- Integración ya que la aplicación funcionará sobre el sistema Windows.

En este módulo se efectúa el ingreso de toda la información de los usuarios VIP al Servidor de Base de Datos, en base a esta información se generan las credenciales RFID.

La base de datos accesos_db.mdb está compuesta por las siguientes tablas:

TABLA ADMIN:

En esta tabla se almacena el login, password y perfiles de los usuarios del sistema. Los campos de esta tabla son:

- LOGIN_USU TEXT50 Login del usuario.
- CLAVE_USU TEXT50 Clave del usuario
- PERFIL_USU TEXT50 Perfil del usuario (Administrador, consultas)

TABLA EVENTOS:

En esta tabla se guarda la información relacionada a un evento, está compuesta por los siguientes campos:

- ID_EVENTO Autonumérico
- NOMBRE_EVENTO TEXT50
- LUGAR TEXT50
- FECHA FECHA/HORA
- HORA FECHA/HORA
- IMAGEN STRING

TABLA CATPER:

La información que se almacena en esta tabla es:

- Nombre.
- Apellido Materno.
- Apellido Paterno.
- Número de credencial RFID.
- Tipo de acceso (Áreas de ingreso permitidas) .
- Nombre del evento.
- Fecha del evento.
- Imagen del evento.
- Horario de acceso (Horario en cual está permitido ingresar el usuario).
- Foto del usuario VIP.

El registro para los usuarios VIP está contemplado de la siguiente manera:
CATÁLOGO DE USUARIOS:

En la primera opción del sistema, presenta una pantalla para: crear usuarios, eliminar usuarios, cambios y consultas de las personas o usuarios que serán controladas por el sistema de accesos. Los campos de la base de datos para este propósito son:

- CLA_PER INTEGER Clave de la persona llave única numérica.
- PAT_PER TEXT 50 Apellido paterno.
- MAT_PER TEXT50 Apellido materno.
- NOM_PER TEXT50 Nombre.

- NOM_EVENTO TEXT50 Nombre del evento.
- FECHA_EVENTO TEXT50 Fecha del evento.
- TIPO_ACCESO TEXT50 Tipo de acceso (Localidades, camerinos, todo acceso).
- STA_PER Integer Status de la persona (1=alta, 2=baja).
- TAG_PER TEXT10 Número de credencial.
- HOI_ACC Integer Intervalo inicial de registro.
- HOF_ACC Integer Intervalo final de registro.
- IMAGEN TEXT50 Dirección de imagen del usuario.
- IMAGEN_EVENTO TEXT50 Dirección de imagen del evento.

Los campos HOI_ACC y HOF_ACC guardan el intervalo de tiempo durante el cual cada persona puede registrar su acceso.

TABLA BORRADO.

En esta tabla se almacena la clave para el borrado de los registros de acceso, está formada por los siguientes campos.

- CLAVE_BORRADO TEXT50

TABLA REGACC.

En esta tabla se guardaran los registros de acceso efectuados en la Terminal RFID, los cuales son recolectados por el driver. Los campos de la base de datos son:

- FEC_RAC DateTime Fecha y Hora de registro
- TAG_RAC TEXT10 Número de etiqueta RFID
- PER_RAC Integer Persona (***Este es el campo CLA_PER de la tabla CATPER***)
- STA_RAC Integer Resultado del registro:
  1-ACCESO NORMAL
  2-FUERA DE HORARIO
  3-CREDENCIAL INVALIDA/USUARIO DADO DE BAJA

Las tablas anteriores son las que componen la base de datos del módulo de registro de usuarios VIP. El respectivo código del desarrollo de software de éste módulo se presenta en el anexo G

3.3.6.1.2 Software Recolector de Datos (Driver)/Software de la Terminal RFID.

El modulo de software Driver así como también el de la Terminal RFID son módulos propietarios de la empresa Soluciones G4 del Ecuador módulos que están actualmente en desarrollo para la implementación de esta tecnología en la empresa, el objetivo principal de este proyecto es ilustrar la aplicación práctica de esta tecnología aplicada al área de control de accesos para espectáculos públicos, razón por la cual no se entrará en detalles del diseño e implementación de código de estos módulos antes mencionados, únicamente se mostrará la vista de diseño de las tablas de la base de datos res_110208_XOCH.mdb. Por lo tanto simplemente se realiza una guía de cómo está estructurado el funcionamiento de las aplicaciones antes mencionadas, dicha guía se encuentra detallada en ANEXO F.

Las tablas que se utilizan en la base de datos res_110208_XOCH.mdb para la aplicación se muestran a continuación:

MONAEN (Archivos de entrada)

Campo	Descripción	Tipo	Valor	Key
CLAV_AEN	Clave del archivo	Integer	1 – 9999	*
DESC_AEN	Descripción del archivo	Varchar* 80		
NOMB_AEN	Nombre del archivo	Varchar* 3		
CONE_AEN	Conexión	Integer		
TABL_AEN	Tabla	Varchar* 40		

MONASA (Archivos de Salida)

Campo	Descripción	Tipo	Valor	Key
CLAV_ASA	Clave del archivo	Real	1 – 9999	*
DESC_ASA	Descripción del archivo	Text* 80		
NOMB_ASA	Nombre	Varchar*3		
CONE_ASA	Conexión	Real		
TABL_ASA	Tabla	Varchar* 40		

MONASO (Archivos de Solaria)

Campo	Descripción	Tipo	Valor	Key
CLAV_AS0	Clave del archivo	Integer	1 – 9999	*

DESC_AS0	Descripción del archivo	Varchar* 80		
NOMB_AS0	Nombre del archivo	Varchar* 3		

MONATE (Archivos asignados a la terminal)

Campo	Descripción	Tipo	Valor	Key
TERM_ATE	Clave de la Terminal	Integer	1-9999	*
ARCH_ATE	Archivo Asignado	Real	1-9999	*

MONCON(Catalogo de conexiones)

Campo	Descripción	Tipo	Valor	Key
CLAV_CON	Clave de la conexión	Integer	1 – 9999	*
DESC_CON	Descripción	Varchar* 20		
TIPO_CON	Tipo	Integer		
JETC_CON	Conexión jet	Integer		
PATH_CON	Path base de datos jet	Varchar*255		
OLED_CON	OLEDB Provider (ADO)	Varchar*255		
SERV_CON	Servidor conexión (ADO)	Varchar*255		
DRVR_CON	Driver ODBC (ADO)	Varchar*255		
USUA_CON	Usuario	Varchar*255		
PASW_CON	Contraseña	Varchar*255		
BASE_CON	Nombre base de datos (ADO)	Varchar*255		
CSTR_CON	Cadena de la conexión	Varchar*250		
CNUM_CON	Caracteres especiales (carácter numérico)	Varchar*20		
CTXT_CON	Caracteres especiales (carácter de Varchar)	Varchar*20		
CBUS_CON	Caracteres especiales (carácter de búsquedas	Varchar*20		
CFEC_CON	Caracteres especiales (carácter de fecha)	Varchar*20		
FFEC_CON	Caracteres especiales (formato de fecha)	Varchar*100		

MONDAE (Detalle de Archivos de entrada)

Campo	Descripción	Tipo	Valor	Key
CLAV_DAE	Clave de archivo de entrada	Integer	1 – 9999	*
CONS_DAE	Consecutivo	Integer		*
DESC_DAE	Descripción	Varchar* 80		
NOMB_DAE	Nombre	Varchar* 3		
CAMP_DAE	Campos	Varchar*20		
KEY1_DAE	Indica si es un campo Llave	Integer		
PINI_DAE	Posición de inicio	Integer		
PFIN_DAE	Posición final	Integer		
TCAM_DAE	Tipo de campo	Integer		

MONDAO (Detalle de Archivos Solaria)

Campo	Descripción	Tipo	Valor	Key
CLAV_DAO	Clave del archivo	Integer	1 – 9999	*
CCAM_DAO	Campo seleccionado	Varchar* 5		
DESC_DAO	Descripción	Varchar* 80		
CSCT_DAO	Consecutivo	Integer		*
PINI_DAO	Posición de inicio	Integer		
PFIN_DAO	Posición final	Integer		

MONDAS (Detalle de Archivos de Salida)

Campo	Descripción	Tipo	Valor	Key

CLAV_DAS	Clave de archivo de Salida	Integer	1 – 9999	*
CONS_DAS	Consecutivo	Integer		*
DESC_DAS	Descripción	Varchar* 80		
CAMP_DAS	Campos	Varchar* 30		
VALO_DAS	Valor	Varchar* 30		
TCAM_DAS	Tipo de campo	Integer		

MONDCE (Detalle Edas CE)

Campo	Descripción	Tipo	Valor	Key
SITE_DCE	Site	Integer	1 – 9999	*
TERM_DCE	Terminal	Integer		*
TIPO_DCE	Tipo	Integer		*
NUME_DCE	Número de terminal	Integer		*
DISP_DCE	Dispositivo	Integer		

MONDEV (Detalles de los eventos)

Campo	Descripción	Tipo	Valor	Key
CLAV_DEV	Clave de evento	Integer	1 – 9999	*
CONS_DEV	Consecutivo	Integer		*
TEXT_DEV	Instrucciones del evento	Varchar* 100		

MONDIS (Catalogo de dispositivos)

Campo	Descripción	Tipo	Valor	Key
CLAV_DIS	Clave del dispositivo	Integer	1 – 9999	*
TIPO_DIS	Tipo de dispositivo	Integer		
DESC_DIS	Descripción	Varchar* 80		
SERI_DIS	Número de serie	Varchar* 20		

MONDME (Detalles de Menús)

Campo	Descripción	Tipo	Valor	Key
MENU_DME	Clave de menú	Integer	1 – 9999	*
CONS_DME	Consecutivo	Integer		*
CORT_DME	Varchar en display corto	Varchar* 16		
LARG_DME	Varchar en display largo	Varchar* 40		
VALO_DEM	Valor que regresa	Varchar* 20		

MONDSA (Detalles de envíos de archivos)

Campo	Descripción	Tipo	Valor	Key
SITE_DSA	Clave de site	Real	1-9999	*
TERM_DSA	Clave de terminal	Integer	1-9999	*
CONS_DSA	Consecutivo	Real		*
ARCH_DSA	Clave del archivo al que se va a hacer el envío	Real	1-9999	
TIPO_DSA	Tipo de envío que se va a hacer	Real		
DIAE_DSA	Día en el que se va a hacer el envío	Real		
HORA_DSA	Hora en la que se va a hacer el envío	Varchar* 4		

MONDSI (Detalles de los Sites)

Campo	Descripción	Tipo	Valor	Key
SITE_DSI	Clave de site	Integer	1 – 9999	*
TERM_DSI	Clave de terminal	Integer		*
COOR_DSI	Coordenadas de la terminal en el site	Varchar* 20		
UBIC_DSI	Ubicación de la terminal	Varchar* 80		

DTCP_DSI	Dirección TCP/IP	Varchar* 20	
LIN1_DSI	Dispay Línea 1	Varchar* 40	
LIN2_DSI	Display Línea 2	Varchar* 40	
LIN3_DSI	Display Línea 3	Varchar* 40	
LIN4_DSI	Dispaly Línea 4	Varchar* 40	
EVEN_DSI	Clave de los eventos	Varchar* 150	1-9999
NTER_DSI	Número de Terminal	Integer	1-9999
IN01_DSI	Dispositivos de entrada del 1-50	Varchar* 150	
IN02_DSI	Dispositivos de entrada del 51-100	Varchar* 150	
IN03_DSI	Dispositivos de entrada del 101-150	Varchar* 150	
OUT1_DSI	Dispositivos de salida del 1-50	Varchar* 150	
CO01_DSI	Dispositivos de conectados en puertos COM	Varchar* 150	
CSCT_DSI	Consecutivo	Varchar*50	
CRED_DSI	Credencial	Varchar*9	

MONDST (Detalle de sites)

Campo	Descripción	Tipo	Valor	Key
NSIT_DST	Número site	Integer	1 – 9999	*
NTER_DST	Número terminal	Integer		
NROW_DST	Número file	Integer		
NCOL_DST	Número columna	Integer		
DIIP_DST	Dirección IP	Varchar*30		
DSP1_DST	Línea de display 1	Varchar*30		
DSP2_DST	Línea de display 2	Varchar*30		
DSP3_DST	Línea de display 3	Varchar*30		
DSP4_DST	Línea de display 4	Varchar*30		
UBIC_DST	Ubicación	Varchar*80		
EVEN_DST	Evento	Varchar*180		

MONECO (Eventos compilados)

Campo	Descripción	Tipo	Valor	Key
OPER_COM	Operador	Integer	1 – 9999	
TIPO_COM	Tipo	Integer		
NUME_COM	Número	Integer		
DIRE_COM	Dirección	Integer		
EVEN_COM	Evento	Integer		
TERM_COM	Terminal	Integer		
COEV_COM	Consecutivo	Integer		

MONEVE (Catalogo de eventos)

Campo	Descripción	Tipo	Valor	Key
CLAV_EVE	Clave de evento	Integer	1 – 9999	*
DESC_EVE	Descripción	Varchar* 80		
ACTI_EVE	Activación del evento	Integer		
TIPO_EVE	Tipo de Evento	Integer		
NOMB_EVE	Nombre del evento	Varchar*80		
ARGU_EVE	Argumento	Varchar*80		
TIPF_EVE	Tipo de formula	Integer		

MONFRA (Frecuencia de envío de archivos)

Campo	Descripción	Tipo	Valor	Key
TERM_FRA	Número de terminal a actualizar	Integer	1-9999	*
ARCH_FRA	Archivo a actualizar	Integer	1-9999	*
CONS_FRA	Consecutivo	Integer		*
ENVI_FRA	Tipo de envío	Integer		
DIAS_FRA	Día del envío	Integer		
HORA_FRA	Hora del envío	Integer		

MONFSU (Configuración de Funciones)

Campo	Descripción	Tipo	Valor	Key
CLAV_FSU	Clave de la función	Varchar* 30		*
DESC_FSU	Nombre de la Función	Varchar* 100		
ARGU_FSU	Argumentos de la función	Varchar* 255		
TIPO_FSU	Tipo de función	Integer		

MONMNU (Catálogo de menús)

Campo	Descripción	Tipo	Valor	Key
CLAV_MNU	Clave del menú	Integer	1 - 9999	*
DESC_MNU	Descripción del Menú	Varchar* 40		

MONMSG (Catálogo de Mensajes)

Campo	Descripción	Tipo	Valor	Key
CLAV_MSG	Clave del mensaje	Integer	1 - 9999	*
DESC_MSG	Descripción del mensaje	Varchar* 80		
COR1_MSG	Mensaje corto línea 1	Varchar* 16		
COR2_MSG	Mensaje corto línea 2	Varchar* 16		
LAR1_MSG	Mensaje largo línea 1	Varchar* 40		
LAR2_MSG	Mensaje largo línea 2	Varchar* 40		
EXT1_MSG	Mensaje extendido linea1	Varchar* 40		
EXT2_MSG	Mensaje extendido línea 2	Varchar* 40		
EXT3_MSG	Mensaje extendido línea 3	Varchar* 40		
EXT4_MSG	Mensaje extendido línea 4	Varchar* 40		
MULT_MSG	Ruta de archivo wav	Varchar* 100		
DURA_MSG	Duración en segundos	Integer		
TIPS_MSG	Tipo de sonido	Integer		
FREC_MSG	Frecuencia del sonido	Integer		
DURM_MSG	Duración del sonido	Integer		

MONQRY (Configuración de Filtros)

Campo	Descripción	Tipo	Valor	Key
SITE_QRY	Site	Integer	1-9999	*
NTER_QRY	Clave de la terminal	Integer	1-9999	*
CONS_QRY	Consecutivo	Integer		*
ARCH_QRY	Archivo al que se aplicará el filtro	Integer	1-9999	
OPER_QRY	Operador utilizado en la selección	Varchar* 20		
CAMP_QRY	Campo utilizado como filtro	Varchar* 50		
COMP_QRY	Operadores relacionales utilizados	Varchar* 20		
VALO_QRY	Valor definido como parámetro	Varchar* 80		

MONQSO (Configuración de Filtros Archivos Solaria)

Campo	Descripción	Tipo	Valor	Key
SITE_QSO	Site	Integer	1-9999	*
TERM_QSO	Clave de la terminal	Integer	1-9999	*
CSCT_QSO	Consecutivo	Integer		*
ARCH_QSO	Archivo al que se aplicará el filtro	Integer	1-9999	*
SIGN_QSO	Operador utilizado en la selección	Varchar2* 15		
CAMP_QSO	Campo utilizado como filtro	Varchar2* 10		
COMP_QSO	Operadores relacionales utilizados	Varchar2* 15		
VALO_QSO	Valor definido como parámetro	Varchar2* 80		

MONSAS (Envíos de Archivos Solaria)

Campo	Descripción	Tipo	Valor	Key
SITE_SAS	Site	Numeric*4	1-9999	*
TERM_SAS	Clave de la terminal	Integer	1-9999	*
TIPO_SAS	Tipo de envío	Integer		
CLAV_SAS	Clave del archivo	Integer	1-9999	*
DIA_SAS	Día del envío	Integer		
HORA_SAS	Hora	Varchar* 6		
CSCT_SAS	Consecutivo	Integer		*

MONSET (Eventos asignados a la terminal)

Campo	Descripción	Tipo	Valor	Key
TERM_SET	Clave de la Terminal	Integer	1-9999	*
EVEN_SET	Evento asignado a la terminal	Integer	1-9999	*

MONSIT (Catalogo de Sites)

Campo	Descripción	Tipo	Valor	Key
CLAV_SIT	Clave de site	Integer	1 – 9999	*
DESC_SIT	Descripción	Varchar* 80		
TIPO_SIT	Tipo de Site	Integer		
SOCK_SIT	Socket Service	Varchar* 30		
MODE_SIT	Módem	Integer		
BAUD_SIT	Bauds	Integer		
DBIT_SIT	Bit de Datos (Data bit) del Site serial	Integer		
SBIT_SIT	Bit de Parada (Stop bit) del Site serial	Integer		
PARI_SIT	Paridad del Site serial	Integer		
PCOM_SIT	Puerto COM	Integer		
MSET_SIT	Configuración del módem (Setup)	Varchar*200		
MDIA_SIT	Configuración del módem (Dial-up)	Varchar*200		
MHAN_SIT	Configuración del módem (Hangup)	Varchar*200		

PASS_SIT	Password	Varchar*20		

MONTCE (Terminales CE)

Campo	Descripción	Tipo	Valor	Key
CLAV_TCE	Clave	Integer	1 - 9999	*
CSCT_TCE	Consecutivo	Integer		*
TIPO_TCE	Tipo	Integer		
COMM_TCE	Puertos com	Integer		
DINP_TCE	Líneas input	Integer		
DOUT_TCE	Líneas output	Integer		

MONTDI (Catálogo de tipos de dispositivos)

Campo	Descripción	Tipo	Valor	Key
CLAV_TDI	Clave del tipo de dispositivo	Integer	1 - 9999	*
DESC_TDI	Descripción del tipo de dispositivo	Text* 80		
ICON_TDI	Icono	Image		
CONE_TDI	Conexión dispositivo	Integer		
SERI_TDI	Dispositivos seriales	Integer		
BAUD_TDI	BAUDS por segundo	Integer		
DATA_TDI	Bits de Datos (Data bits)	Integer		
PARI_TDI	Paridad	Integer		
STOP_TDI	Bits de parada (Stop bits)	Integer		
OUTP_TDI	Formato de Salidas (Output format)	Integer		
ESTA_TDI	Estado inicial del dispositivo de salida digital (control line)	Integer		
TDIS_TDI	Tiempo de disparo (segundos)	Integer		

MONTER (Catalogo de terminales)

Campo	Descripción	Tipo	Valor	Key
CLAV_TER	Clave de terminal	Numeric*4	1 – 9999	*
DESC_TER	Descripción	Varchar* 80		
TIPO_TER	Tipo de terminal	Integer		
SERI_TER	Número de serie	Varchar* 20		
COM0_TER	Puerto COM	Integer		
PRED_TER	Puerto de red	Integer		
DINP_TER	Entradas Digitales (líneas sensoras)	Integer		
DOUT_TER	Salidas digitales (líneas de control)	Integer		
DISP_TER	Display	Integer		
TECL_TER	Teclado	Integer		
MEMO_TER	Memoria	Integer		
CBAI_TER	Ranura interna de código de barras	Integer		
CBAX_TER	Puerto externo de código de barras	Integer		
MAGS_TER	Ranura interna de banda magnética	Integer		
COM1_TER	Puerto COM 1	Integer		
COM2_TER	Puerto COM 2	Integer		
COM3_TER	Puerto COM 3	Integer		
COM4_TER	Puerto COM 4	Integer		
COM5_TER	Puerto COM 5	Integer		
COM6_TER	Puerto COM 6	Integer		
COM7_TER	Puerto COM 7	Integer		
COM8_TER	Puerto COM 8	Integer		
COM9_TER	Puerto COM 9	Integer		

MONVAR (Configuración de Variables)

Campo	Descripción	Tipo	Valor	Key

CLAV_VAR	Clave de la variable	Varchar* 20	*
TIPO_VAR	Tipo de variable	Integer	
DESC_VAR	Nombre de la Variable	Varchar* 100	
SIZE_VAR	Longitud de la variable	Integer	
VALO_VAR	Valor de la variable	Varchar* 255	
SIST_VAR	Sistema	Integer	

3.3.7 INSTALACIÓN Y MANUAL DE USUARIO DE LOS MÓDULOS DE SOFTWARE.

La instalación de estos módulos se lo realiza independiente partiendo del software de registro de usuarios, el proceso de instalación y la guía de uso del prototipo se lo detalla en el ANEXO F.

3.4 PRUEBAS DE FUNCIONAMIENTO

Para explicar las pruebas de funcionamiento se realizará un análisis de cada uno de los módulos de software que forman parte del prototipo.

3.4.1 SOFTWARE DE REGISTRO DE USUARIOS

El software de registro de usuarios permite crear en el sistema los usuarios VIP para los cuales se va a generar las credenciales RFID, para validar las pruebas de funcionamiento se procede a seguir los siguientes pasos.

- En la figura 3.17 al dar doble clic en el acceso directo del software de registro de usuarios se tiene la pantalla donde se ingresa el **Nombre de Usuario y Contraseña**.

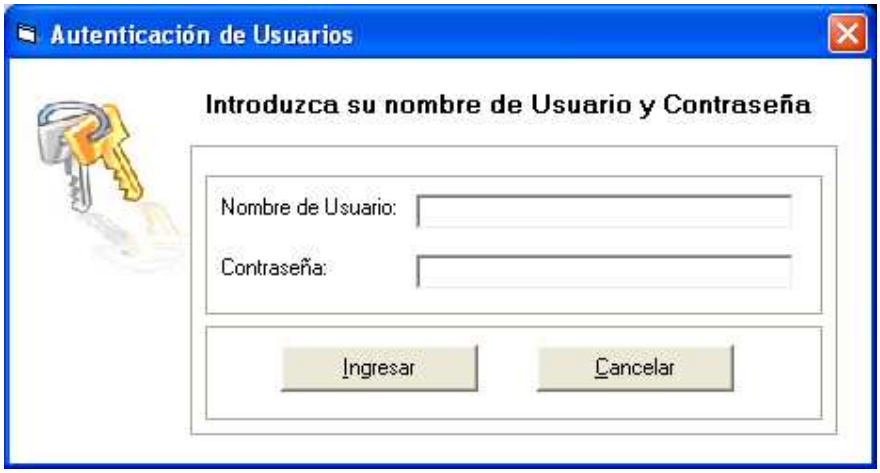


Figura 3.17 Ingreso de Usuario y Contraseña.

- Si se ingresa de forma incorrecta el **usuario** o **contraseña,** aparecerá un mensaje del sistema informando este error, tal como se observa en la figura 3.18.

Figura 3.18 Ingreso incorrecto de usuario, contraseña

- Luego de haber ingresado correctamente estos datos se podrá observar la interfaz principal del sistema donde se encuentran habilitados todos los menús para su uso, como se muestra en la figura 3.19

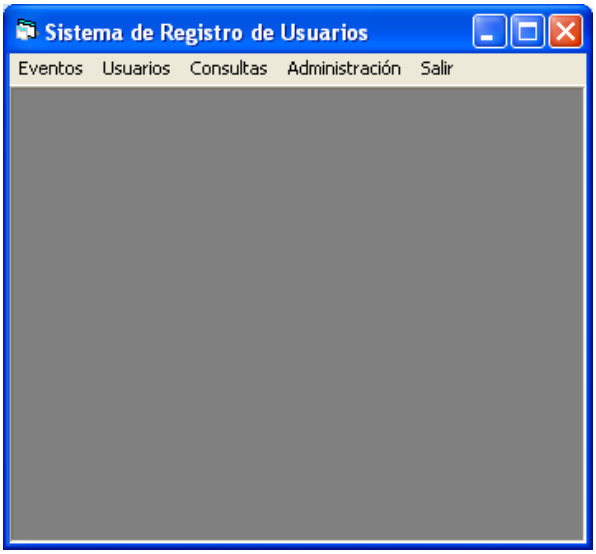


Figura 3.19 Interfaz del sistema

Una vez que se haya ingresado al sistema se procede a escoger el catalogo de ***USUARIOS->ADMINISTRACION DE USUARIOS***

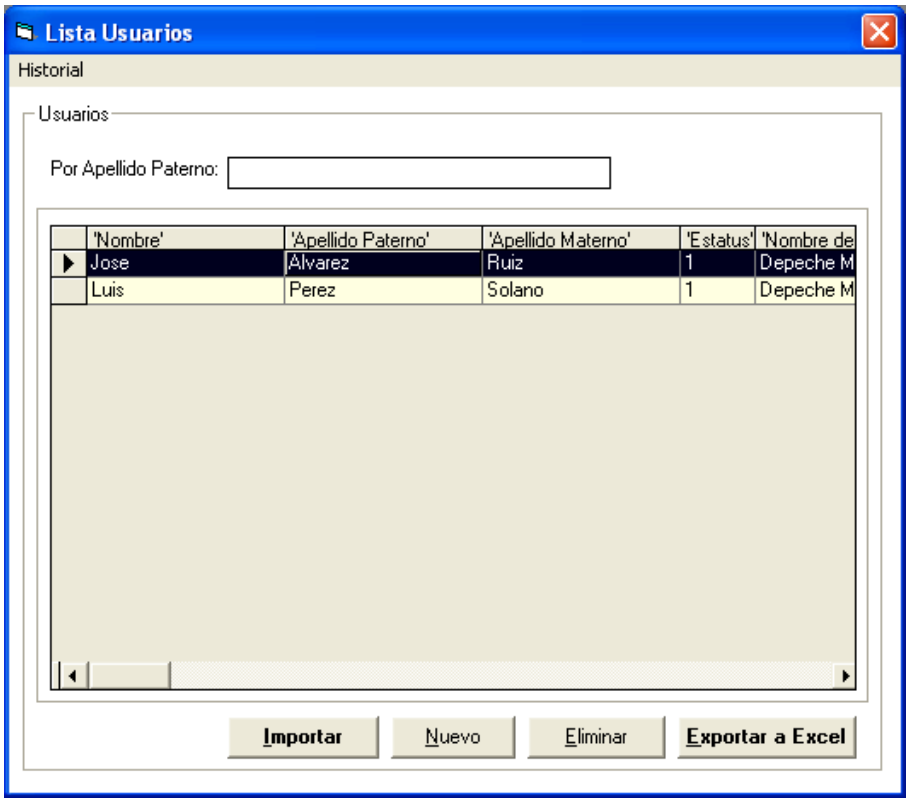


Figura 3.20 Catálogo de usuarios

- Se procede a dar clic sobre **Nuevo** para crear un nuevo usuario VIP

Figura 3.21 Crear un nuevo usuario

Una vez que se haya ingresado todos los datos se procede a **Guardar** y el usuario queda ya almacenado en el sistema.

Para imprimir la información en la credencial se escoge el botón **Imprimir** y se muestra una vista previa de la credencial, como se muestra en la figura 3.22

Figura 3.22 Vista previa de la credencial RFID

Al clic en el botón Eliminar de la figura 3.20 se procede a eliminar el usuario seleccionado y para editar la información de un usuario se procede a dar doble clic sobre el usuario seleccionado y una vez que se haya modificado la información necesaria se procede a guardar la información tal como se muestra en la figura 3.23

Figura 3.23 Modificar información de un usuario

Una vez que esté lista la impresión de las credenciales se procede a la entrega de las mismas a los usuarios VIP y aquí finaliza la primera etapa que la emisión de credenciales.

3.4.2 SOFTWARE DE ACCESOS

Una vez que se tenga lista la configuración de la red de accesos tal como se lo detalla en el anexo F se procede a la configuración del software de accesos.

El software de accesos este formado por siguientes módulos:

- Software recolector de datos (Driver)
- Software de la Terminal RFID

3.4.2.1 Software recolector de datos (Driver).-

- Ejecutar el Driver desde el escritorio de Windows.

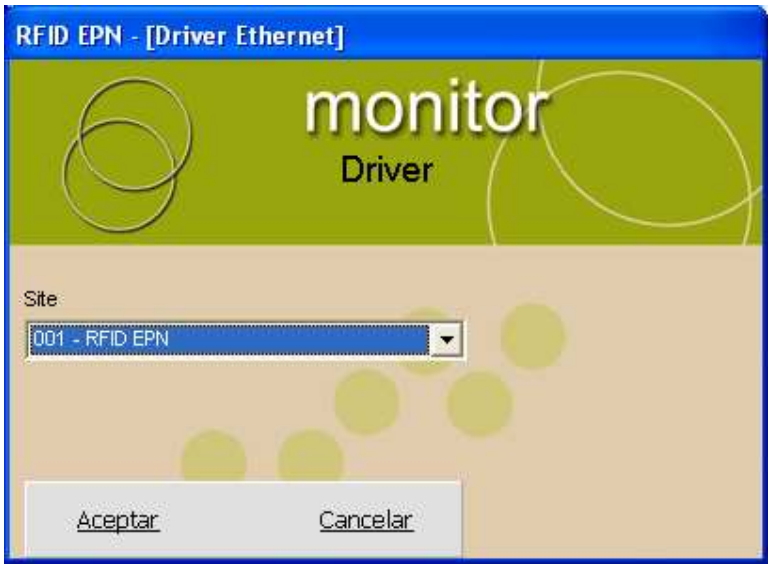


Figura 3.24 Recolector de datos (Driver)

Damos clic en **Aceptar** y la aplicación procede a realizar las conexiones con las dos bases de datos del sistema:

- accesos_db.mdb
- res_110208_XOCH.mdb

Una vez que se haya cargado el driver tenemos ya la interfaz de usuario:

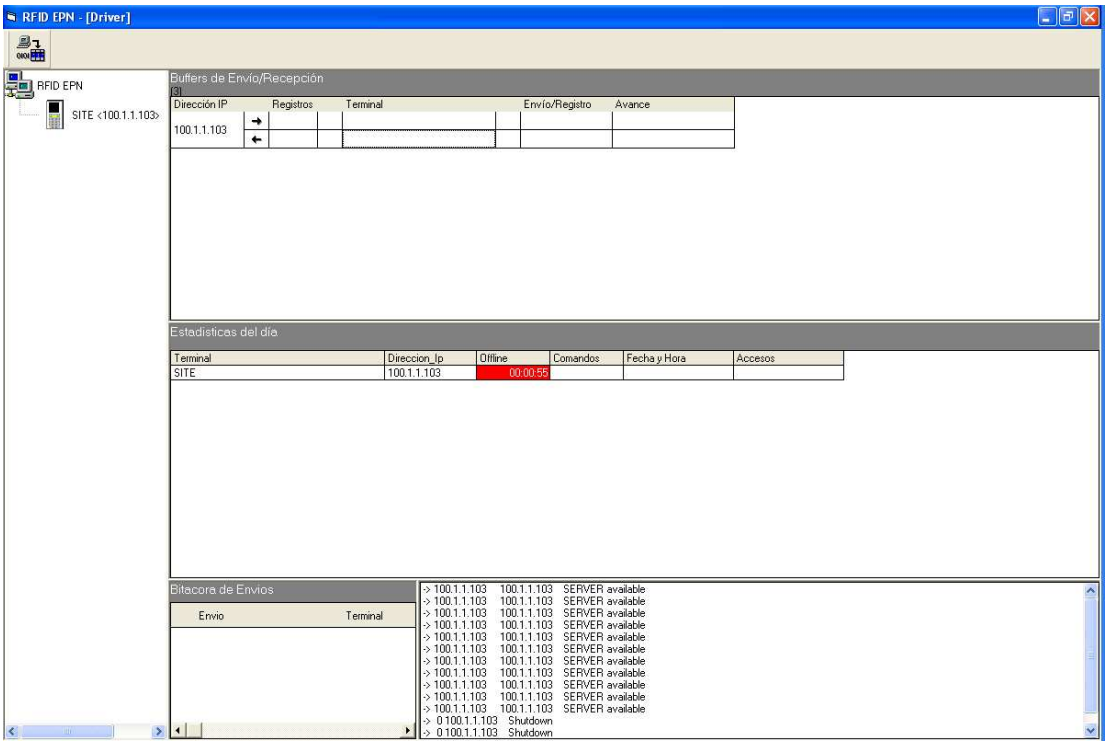


Figura 3.25 Interfaz de usuario del Driver

En la figura 3.25 podemos apreciar 4 bloques de operación de la aplicación:

- Site: es la lectora RFID con su respectiva dirección IP
- Buffers de Envío/Recepción: En esta parte se muestran los paquetes de envío y recepción de la lectora por medio del driver:
- Estadísticas del día: En esta parte se aprecian las estadísticas de envío de información
- Bitácora de envíos: En esta aparecen todos los envíos de información que se realizan a la lectora, además se muestra el proceso de comunicación entre la lectora y el driver al momento de enviar cada paquete

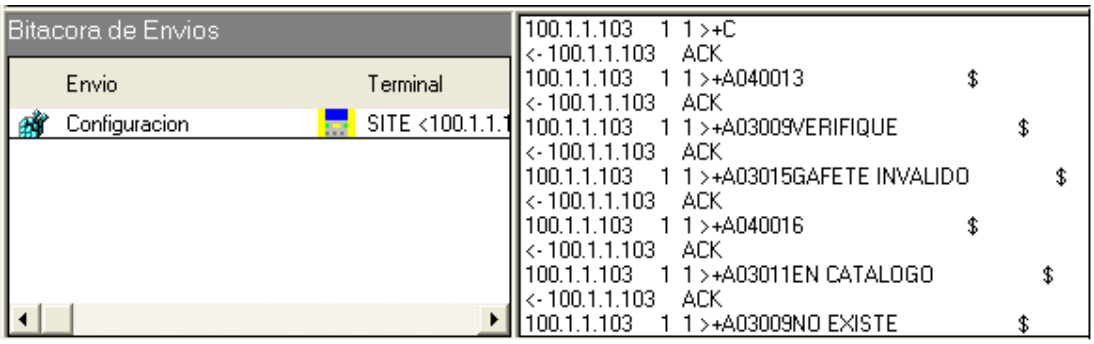


Figura 3.26 Bitácora de envíos

3.4.2.2 Software de la Terminal RFID.

Para operar el software de la Terminal se ejecuta el acceso directo que existe en el escritorio de la Terminal una vez realizado esto la aplicación carga las librerías que permiten activar a la tarjeta lectora luego la tarjeta lectora empezará a emitir una luz intermitente la misma que indica que el dispositivo está listo para operar.

En la figura 3.27 se muestra la interfaz de operación de la Terminal, en dicha interfaz se tiene la fecha y hora, la cual esta sincronizada con la fecha del servidor.

Figura 3.27 Software de la controladora RFID

3.4.2.2.1 Envío de configuración a la Terminal RFID

Para realizar el envío se procede a seleccionar el Software recolector de datos (Driver) y se da clic sobre el icono de envíos  . Luego se presenta la pantalla para seleccionar los envíos a la Terminal, como se muestra en la figura 3.28

Los envíos que se realizan son los siguientes:

- Fecha y Hora: Se envía la fecha y hora del servidor a la Terminal para que ésta se sincronice con el servidor.
- Configuración: Se envía la configuración de los mensajes que se muestran en la Terminal, el tipo de lector, el indicador de conectividad, etc.

- Accesos: Se envía a la Terminal la información de los usuarios VIP, los códigos de identificación de cada credencial y los respectivos horarios de acceso.

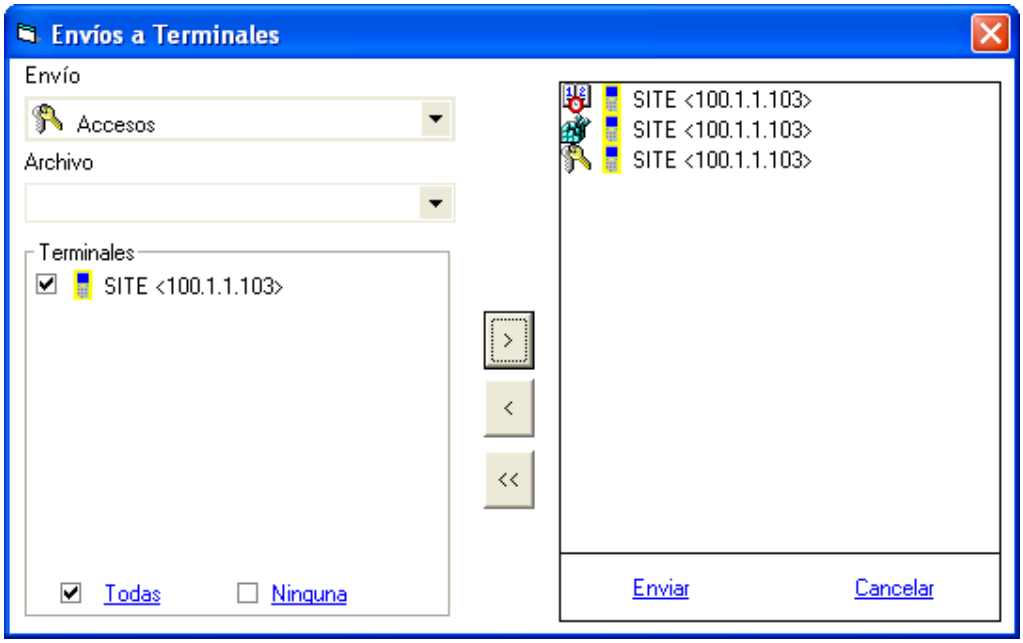


Figura 3.28 Programación de envíos

Escogemos la Terminal a la cual deseamos enviar las configuraciones, para este caso escogemos la única que está disponible (SITE<100.1.1.103>) y seleccionamos el envío correspondiente damos clic en el botón  y agregamos el envío, repetimos el mismo proceso la el resto de envíos. Una vez que estén agregados los envíos correspondientes se procede a enviar la configuración a las terminales presionando el botón **Enviar**.

La figura 3.29 se muestra el proceso de envío de configuraciones a la Terminal. Una vez que se termine el envío la sección de Bitácora de Envíos quedará totalmente vacía lo que implica que todas las configuraciones se realizaron con éxito.

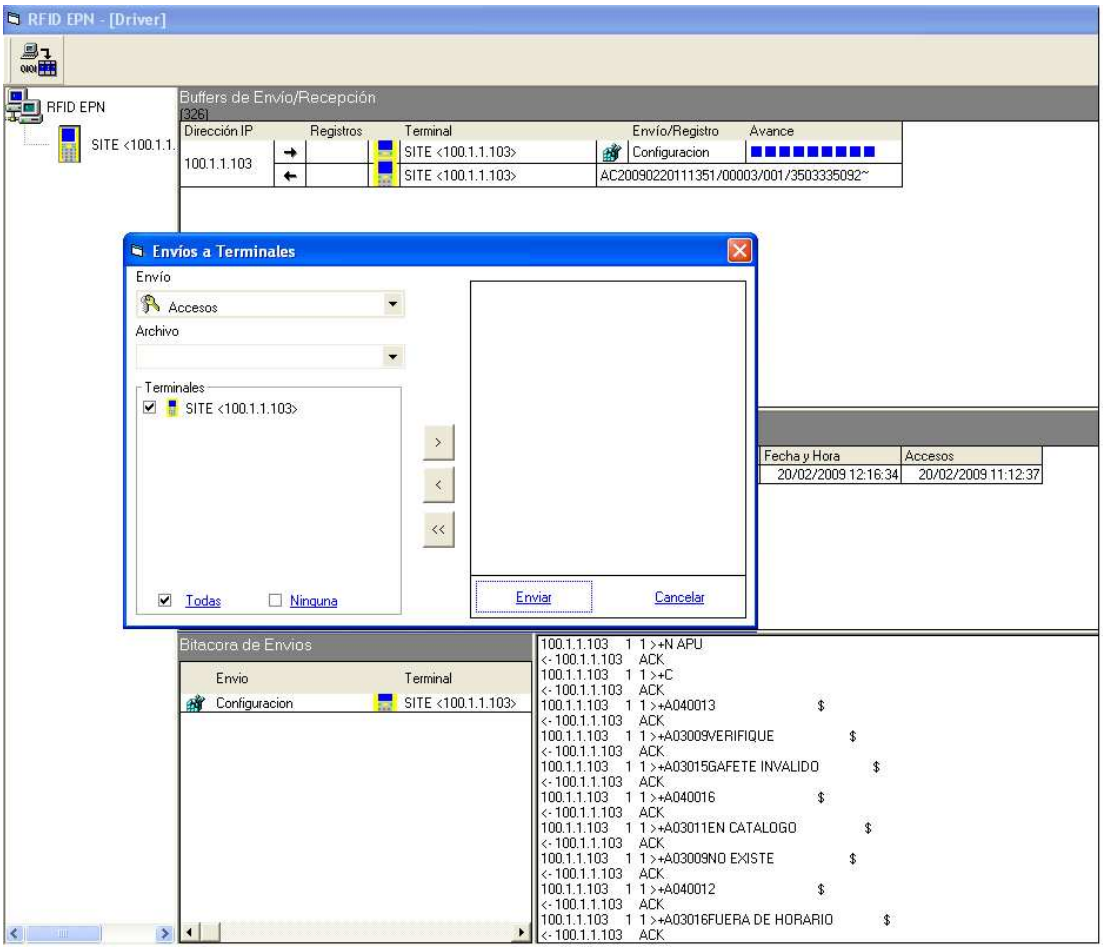


Figura 3.29 Proceso de envío de configuraciones

Al finalizar el envío la Terminal sincroniza su fecha y hora con la del servidor

3.4.2.3 Lectura de credenciales RFID.

Se procede a realizar la lectura de las credenciales RFID aproximándolas a la lectora a una distancia aproximada de 2 cm. Al momento que se efectúe satisfactoriamente la lectura, el software de la Terminal indicará primero el número de la credencial como se muestra en la figura 3.30

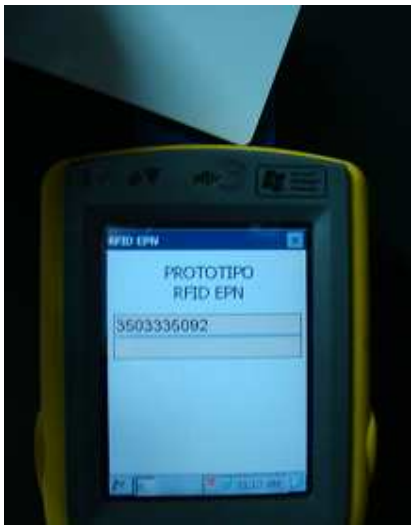


Figura 3.30 Lectura de la credencial

Seguidamente la terminal presenta el resultado del acceso, los posibles resultados de acceso para una lectura son:

- **ENTRADA VALIDA**: Indica que el usuario está permitido a ingresar

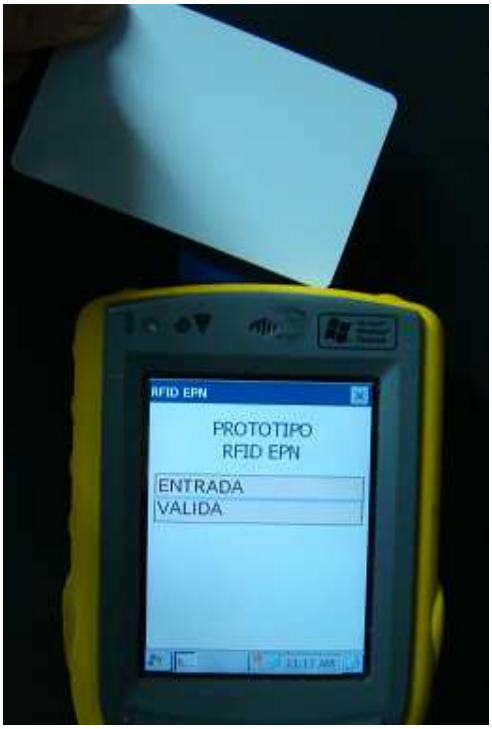


Figura 3.31 Credencial Válida

- **FUERA DE HORARIO:** Indica que el usuario está intentando acceder en un horario no permitido.

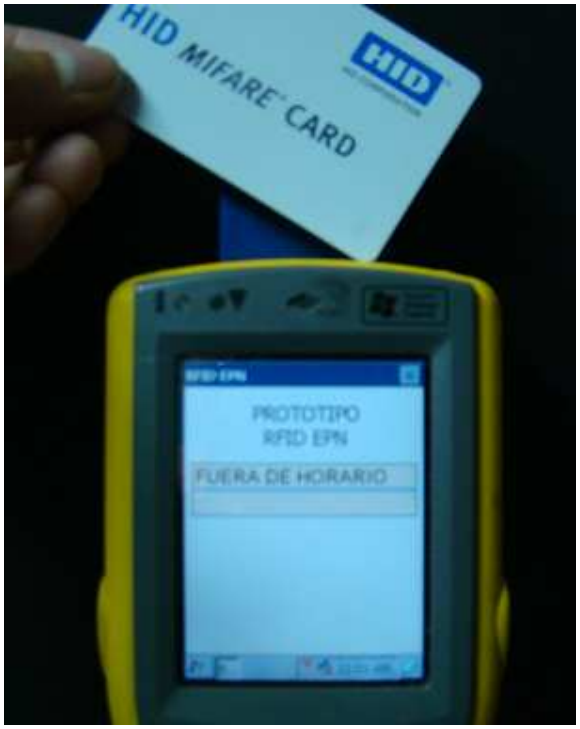


Figura 3.32 Credencial fuera de horario

- **GAFETE INVALIDO VERIFIQUE:** Indica que dicha credencial corresponde a un usuario no permitido o que esta dado de baja en el sistema.

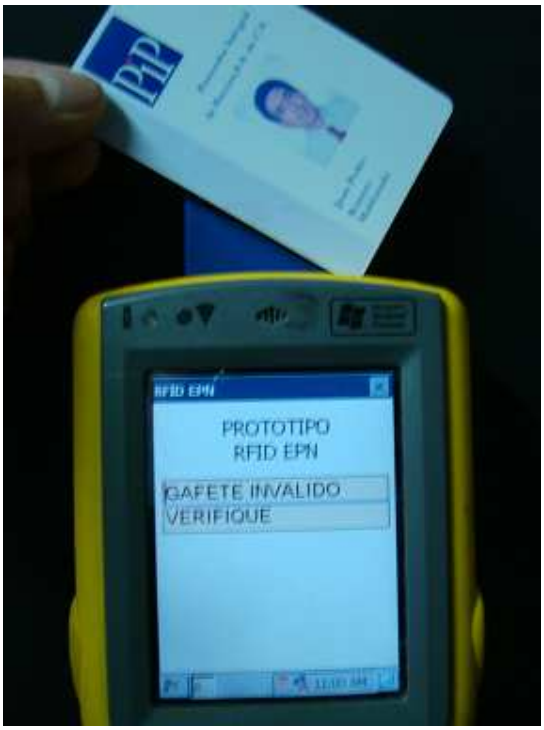


Figura 3.33 Credencial Inválida

Cada lectura que se efectué en la Terminal será enviada por medio de la interface de red inalámbrica de la Terminal hacia el Driver que se encuentra instalado en el servidor para el respectivo almacenamiento de datos.

3.4.3 GENERAR REPORTE DE ACCESOS

Una vez finalizado el control de accesos se procede a generar un reporte en Excel de accesos, para esto se utiliza en el sistema de registro de usuarios el catálogo de **consultas->consultas de accesos**, este reporte muestra todos los usuarios que ingresaron al inmueble con el respectivo seguimiento de fecha y hora de acceso, como se muestra en la figura 3.34.

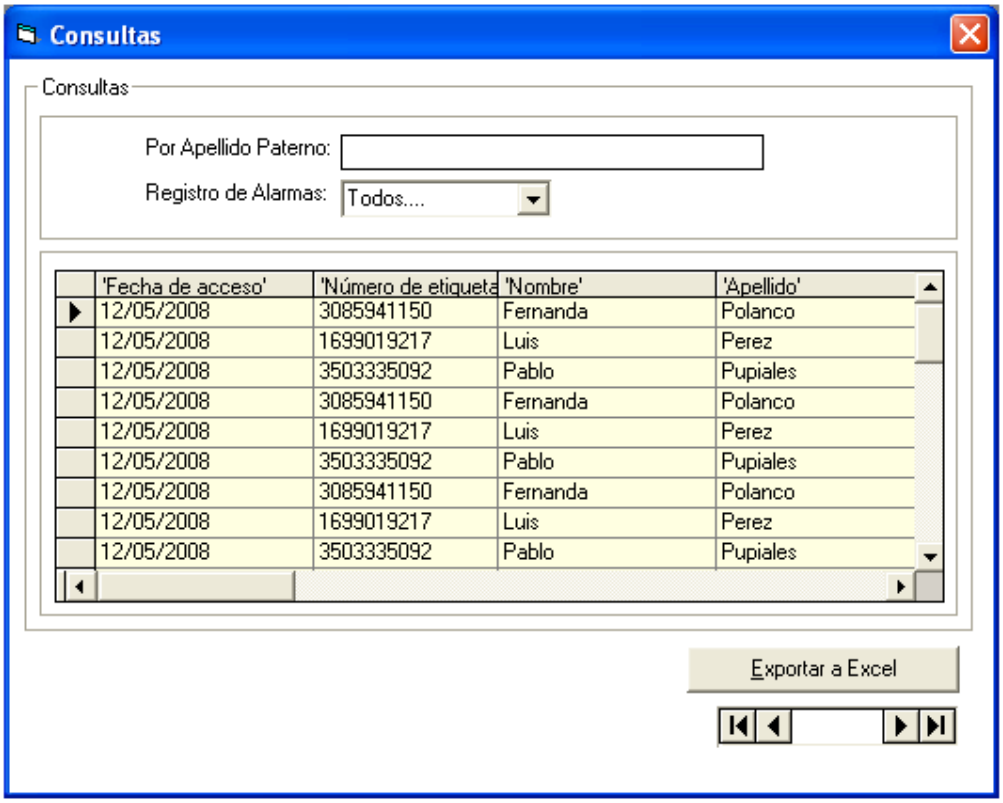


Figura 3.34 Consultas de accesos

Al dar clic en el botón **Exportar a Excel** se procede a exportar estos datos de accesos a una hoja de Excel, luego se procede a la entrega respectiva de esta información al organizador del evento tanto en impreso como en un archivo de datos.

De esta manera se concluye con la demostración total del funcionamiento del prototipo.

3.5 FACTIBILIDAD ECONÓMICA

En esta sección se realizará una cuantificación de los costos y beneficios que generará el presente proyecto y el cálculo de la relación costo – beneficio. La

relación costo – beneficio permitirá tener una idea clara de que tan rentable sería implementar o no dicho proyecto.

3.5.1 COSTOS DE INVERSIÓN

Estos valores corresponden a costos por estudios, equipos e instalación hasta su funcionamiento. El presente proyecto será financiado en parte por recursos propios y también por la empresa auspiciante del proyecto.

3.5.1.1 Costo de Equipos

En el desarrollo del proyecto, se necesitó 5 equipos, con diferentes características, dependiendo de su utilidad en el proyecto. Las características de los equipos y sus costos se los detalla en la tabla 3.7

EQUIPOS			
ITEM	**CANTIDAD**	**DESCRIPCIÓN**	**COSTO(USD)**
1	**1**	**Servidor de Base de Datos y Aplicaciones** 1. Mainboard Intel 865 GLV Pentium IV bus de 800MHz DDR400/533 2. Memoria RAM de 1GB PC400 3. Disco duro 120GB IDE 7200rpm 4. Procesador Intel Pentium IV 2,8GHz 5. Tarjeta de red 10/100 Mbps 6. Tarjeta de red inalámbrica 54 Mbps 7. Monitor Samsung 17' 8. Unidad de CD-rewritable 9. Teclado y Mouse	**575**
2	**1**	**Terminal Lan Point Mobile Texas Instruments** 1. Windows CE .NET 4.2 with .NET Compact Framework 1.0, or Windows CE 5.0 with .NET Compact Framework 2.0 2. Procesador Intel Xscale PXA255, 400MHz 3. Memoria RAM 128MB 4. Memoria Flash 96MB 5. Compact Flash Slot 6. RS232/USB host/USB client 7. WLAN IEEE802.11b	**1600**
3	**1**	**Lector RFID HF MIFARE DESFire contactless** 1. Interface Compact Flash 2. Frecuencia de operación 13,56 MHz 3. Distancia de lectura: hasta 60 mm dependiendo del tag 4. Velocidad de transmisión: hasta 848 kbit/s	**620**
4	**1**	**Access Point Linksys WAP11** 1. Protocolo IEEE 802.11b 2. Banda de frecuencia 2.4 GHz 3. Algoritmo de cifrado WEP de 128 bits 4. Dos antenas externas	**80**
5	**1**	**Impresora Evolis Dualys 3 ID** 1. Resolución de 300 dpi 2. Impresora a color 3. Velocidad de impresión 150 Tarjetas/Hora	**1900**
		Total	**4775***

Tabla 3.7 Costos de Equipos

*Los costos de los equipos fueron proporcionados el departamento contable de la empresa.

3.5.1.2 Costo de Software

Las herramientas de desarrollo que se han utilizado para el proyecto son propietarias cuyo costo se detalla en la tabla 3.8.

SOFTWARE			
ITEM	**CANTIDAD**	**DESCRIPCIÓN**	**COSTO(USD)**
1	**1**	**Sistema Operativo:** Windows XP Profesional	**167**
2	**1**	**Herramienta de Programación:** Visual Basic 6.0	**400**
3	**1**	**Base de Datos:** Microsoft Access 2003	**380**
		TOTAL:	**947**

Tabla 3.8 Costos de Software

3.5.1.3 Costos de Desarrollo

Este rubro tiene que ver con el costo del desarrollo de la aplicación referente a las horas que tomó realizar la aplicación hasta su operación. En la tabla 3.9 se presentan los días que tomó realizar el proyecto, según las tareas realizadas hasta alcanzar la operación del proyecto.

TAREAS	DIAS
ESTUDIO Y ANÁLISIS DE LAS HERRAMIENTAS	5
DESARROLLO DEL PROTOTIPO	60
INSTALACIÓN DE LAS APLICACIONES	1
REDACCIÓN DEL TERCER CAPÍTULO	15
REALIZACIÓN DE LAS PRUEBAS	5
TOTAL DIAS:	86

Tabla 3.9 Tareas por Días

Los días de la tabla anterior son solo días laborables, en que no se consideran sábados, domingos ni feriados.

En la tabla 3.10 se presenta el costo de desarrollo mensual del proyecto.

DESARROLLO			
ITEM	**CANTIDAD**	**DESCRIPCIÓN**	**COSTOxMES(USD)**
1	**2**	**Desarrolladores:**	
		1. Egresado en Ingeniería Electrónica y Redes de Información	**800**
		2. Curso de equipos y tecnología de control de accesos	**120**
		TOTAL:	**920**

Tabla 3.10 Costo de Desarrollo

Un mes tiene en promedio 21 días laborables, lo que da un valor de 43.80 USD por costo de desarrollo diario, lo que en los 86 días que tomó realizar el software da como costo total 3.766,8 USD.

3.5.1.4 Costos de Operación y Mantenimiento

Los costos por operación y mantenimiento se refieren básicamente a los rubros que se detalla en la tabla 3.11. Estos rubros se repiten en cada evento en promedio se tiene un evento mensual.

COSTOS DE OPERACIÓN		
ITEM	**DESCRIPCIÓN**	**COSTOxEVENTO(USD)**
1	Administrador del sistema	**150**
2	Instaladores de la red de comunicaciones del inmueble	**80**
3	600 Tarjetas RFID	**600**
	Subtotal Operación	**830**
COSTOS DE MANTENIMIENTO		
4	Repuestos, Mantenimiento y otros	**50**
	Subtotal Mantenimiento	**50**
	TOTAL:	**880**

Tabla 3.11 Costos de Operación y Mantenimiento

En conclusión el costo de inversión, que se refiere a los costos de: equipos, software, de la herramienta, desarrollo, operación y mantenimiento es de 10.368,80 USD.

3.5.2 BENEFICIOS

Dadas las características del Proyecto, los beneficios proporcionados por el proyecto son muy difíciles de cuantificar, por lo que se los dividirá en dos secciones, beneficios cuantificables y beneficios no cuantificables.

3.5.2.1 Beneficios Cuantificables

Para poder medir este beneficio, se tomó en cuenta los costos que implicaba realizar la emisión de una credencial normal que no utiliza la tecnología RFID.
La cantidad de credenciales que se emiten en un evento es el 3% de la capacidad total del inmueble, para este análisis se toma como promedio un inmueble con una capacidad de 20.000 personas por lo tanto la cantidad de credenciales RFID que se va a emitir por evento son 600.

En la tabla 3.12 se detalla el costo de generar las credenciales normales sin utilizar la tecnología RFID

Costos de generación de credenciales				
ITEMS	**CANTIDAD**	**DESCRIPCION**	**COSTO UNITARIO(USD)**	**TOTAL(USD)**
1	600	Credenciales para eventos	1,5	**900**
			TOTAL:	**900**

Tabla 3.12 Costos de generación de credenciales

Para la generación y control de acceso de las credenciales se utilizaba: 1 diseñador gráfico que se encargado del diseño e impresión de credenciales, 6 ayudantes encargados de llevar un registro manual de las credenciales que ingresan, 1 supervisor, 1 secretaria. El costo ahorrado al no utilizar estos recursos se lo detalla en la tabla 3.13.

PERSONAL						
ITEMS	**DESCRIPCIÓN**	**CANTIDAD**	**SUELDO MENSUAL (USD)**	**SUELDO DIARIO (USD)**	**CANTIDAD DE DIAS**	**TOTAL (USD)**
1	Diseñador Gráfico	1	750	35.71	3	**107.14**
2	Ayudante	6	550	26.19	1	**157.14**
3	Supervisor	1	750	35.71	3	**107.14**
4	Secretaria	1	550	26.19	2	**52.38**
					TOTAL:	**423.81**

Tabla 3.13 Beneficios por personal

Existe un rubro adicional que se ahorra con la implementación de este sistema que es el alquiler de Motorolas, equipos que se utilizaban para la comunicación de entre los ayudantes y el supervisor. Los detalles se los muestra en la tabla 3.14

Costo de Alquiler de Motorolas				
ITEMS	**CANTIDAD**	**DESCRIPCION**	**COSTO UNITARIO**	**TOTAL(USD)**
1	7	Motorolas	15	**105**
			TOTAL:	**105**

Tabla 3.14 Alquiler de Motorolas

Estos beneficios cuantificables son los que se consideran los más importantes. Existen otros como alimentación y transporte que no son considerados debido a que su valor es marginal.

Así se tiene que el costo por beneficios cuantificables es de 1428.81 USD, que se lo obtiene de las tablas 3.12, 3.13, 3.14, en cada mes que se realiza un evento.

3.5.2.2 Beneficios No Cuantificables

Los beneficios no cuantificables no se presentarán en los índices económicos de este proyecto, pero se los detalla a continuación.

- Seguridad de la integridad física de los asistentes al inmueble, especialmente al equipo de producción del espectáculo, garantizando que el acceso al sitio sea únicamente al personal autorizado, ya que como actualmente se lo maneja existe un alto grado de falsificación de credenciales o gafetes y esto podría conducir a tener personas infiltradas en áreas críticas del inmueble.
- Lectura de la credencial mediante un lector, por medio de esto se descarta el error del factor humano el cual únicamente se limita a realizar un chequeo visual de la credencial. Al insertar los componentes de lector y credencial RFID se garantiza una lectura electrónica la cual deja de lado el criterio humano al momento de un acceso.
- Proceso de acceso rápido y seguro al escenario, la lectura electrónica de una credencial RFID es muy rápida y sencilla ya que quien toma la decisión de permiso o delegación del acceso es el lector RFID proceso que toma milisegundos.
- Reportes detallados de asistencia en tiempo real, lo que permite hacer un seguimiento de cada uno de los usuarios del sistema y a su vez ver la cantidad de usuarios que ingresaron.
- Evitar situaciones de sabotaje que principalmente son ocasionadas por personas cuyo acceso no se lo realizó de manera autorizada, este tipo de situaciones conducen a grandes pérdidas económicas, humanas, etc.

3.5.3 ANÁLISIS COSTO - BENEFICIO

Los beneficios del sistema se pueden observar a partir del mes 18 de implementación, con un ahorro de aproximadamente 389,78 USD y la recuperación de los costos por desarrollo y de hardware, como se indica en la

sección 3.5.3.1.2 El beneficio que provee el sistema radica principalmente en la seguridad y versatilidad que brinda al momento del acceso al inmueble.

Este análisis consiste en la cuantificación de los costos y beneficios que generará el presente proyecto y el cálculo de la relación Costo / Beneficio. La relación costo - beneficio ayuda a la evaluación de que tan rentable es el proyecto y si es conveniente realizarlo o no, radicando ahí su importancia.
Para este análisis se utilizará el método Relación Costo / Beneficio

3.5.3.1 Relación costo - beneficio

Este método consiste en la cuantificación de los costos y los beneficios que generará el proyecto y el cálculo de la relación Costo - Beneficio.
Hay dos maneras de calcular la RCB:

- Cociente del valor presente de los beneficios brutos para el valor presente de los costos brutos.

- Cociente del valor presente de los beneficios netos para el valor presente de los costos netos.

- El criterio de decisión es el siguiente.

    - Si RCB < 1 se acepta el proyecto.
    - Si RCB = 1 es indiferente.
    - Si RCB > 1 se rechaza el proyecto.

3.5.3.1.1 RCB (Relación costo - beneficio) para el primer mes de operación

Para este análisis tomamos en cuenta que la empresa realiza en promedio un evento al mes por lo que el análisis costo beneficio se lo va a realizar en un período mensual.

Al terminar el desarrollo del proyecto, los costos acumulados, que son la suma de los costos detallados en las secciones: 3.5.1.1, 3.5.1.2, 3.5.1.3, 3.5.1.4; ascienden a 10.368,80 USD; y los beneficios calculados en la sección: 3.5.2.1, alcanzan un valor de 1.428,81 USD; así se tiene que:

$$RCB_{1er\_Mes} = \frac{Costos\_Totales}{Beneficios\_Totales} = \frac{10.368{,}80USD}{1.428{,}68USD} = 7{,}256$$

Calculando la relación costo - beneficio se obtiene un valor mayor a 1 para el primer mes de implementación, pero este valor positivo solo se presenta en el primer mes.

3.5.3.1.2 RCB del segundo mes de implementación

En el segundo mes de implementación, no se toman en cuenta los costos por desarrollo y equipos que ascendían a 9.488,80 USD; por lo que los costos totales están solo representados por los costos de operación que ascienden a 880 USD. Los beneficios calculados anteriormente se mantienen, así se tiene que:

$$RCB_{2do\_mes\_en\_adelante} = \frac{Costos\_Totales}{Beneficios\_Totales} = \frac{880USD}{1.428{,}81USD} = 0{,}616$$

Calculando la relación costo - beneficio del segundo mes de implementación en adelante se obtiene un valor de 0,616 que es menor a 1 con lo que el proyecto queda justificado económicamente.

Calculando las ganancias que se obtendrá para el segundo mes de implementación del proyecto, se tiene que los costos del segundo mes ascienden a 11.248,80 USD (10.368,80 USD del primer período y 880 USD del segundo período, cuyos valores se detallaron en la sección: 3.5.1 y 3.5.1.4) y los beneficios son de 2.857,62 USD (1.428,81 USD por cada período, cuyo valor fue detallado en la sección 3.5.2.1), como se puede apreciar tenemos una diferencia negativa de 8.391,18 USD lo que indica que al segundo mes tampoco existe ganancia.

Para determinar en cual mes se obtiene ganancia se realiza un cálculo similar hasta llegar a obtener un valor positivo y ese valor se lo obtiene en el mes 18 tal como se ilustra en la tabla 3.15, partir de este mes el proyecto habrá cubierto los costos de desarrollo y de equipos, teniendo ganancias de este mes en adelante.

Relación Costo-Beneficio					
Mes	Costo (USD)	Beneficio (USD)	Acumulado de Costo (USD)	Acumulado de Beneficio (USD)	Ganancia
1	10368.8	1428.81	10368.8	1428.81	-8939.99
2	880	1428.81	11248.8	2857.62	-8391.18
3	880	1428.81	12128.8	4286.43	-7842.37
4	880	1428.81	13008.8	5715.24	-7293.56
5	880	1428.81	13888.8	7144.05	-6744.75
6	880	1428.81	14768.8	8572.86	-6195.94
7	880	1428.81	15648.8	10001.67	-5647.13
8	880	1428.81	16528.8	11430.48	-5098.32
9	880	1428.81	17408.8	12859.29	-4549.51
10	880	1428.81	18288.8	14288.1	-4000.7
11	880	1428.81	19168.8	15716.91	-3451.89
12	880	1428.81	20048.8	17145.72	-2903.08
13	880	1428.81	20928.8	18574.53	-2354.27
14	880	1428.81	21808.8	20003.34	-1805.46
15	880	1428.81	22688.8	21432.15	-1256.65
16	880	1428.81	23568.8	22860.96	-707.84
17	880	1428.81	24448.8	24289.77	-159.03
18	880	1428.81	25328.8	25718.58	389.78
19	880	1428.81	26208.8	27147.39	938.59
20	880	1428.81	27088.8	28576.2	1487.4
21	880	1428.81	27968.8	30005.01	2036.21
22	880	1428.81	28848.8	31433.82	2585.02
23	880	1428.81	29728.8	32862.63	3133.83
24	880	1428.81	30608.8	34291.44	3682.64

Tabla 3.15 Relación Costo-Beneficio mensual

3.6 COMPARACIÓN DE LA SOLUCIÓN RFID CON LA SITUACIÓN ACTUAL

En la actualidad el control de accesos para credenciales de usuarios VIP se lo maneja de manera manual esto es, se procede a generar una impresión de

credenciales en material PVC con la información del usuario, el problema radica en que esta credencial no tiene ninguna seguridad electrónica y esto abre una alta probabilidad de que existan falsificaciones de las credenciales ya que estas no se las puede someter a ningún proceso de validación electrónica y esto conduce a tener serios problemas al momento que se lleva a cabo un evento en un determinado inmueble, convirtiéndolo en un inmueble inseguro desde diferentes puntos de vista principalmente el de salvaguardar la integridad de los asistentes. Para evitar estas y muchas otras situaciones negativas es importante implementar una solución que permita tener un escenario inteligente es decir un escenario que permita implementar una tecnología de identificación, con el objetivo de tener seguridad, control y administración de todo un escenario.

Con la implementación de esta tecnología lo que se ha logrado es tener un mejor control en el acceso de todos los asistentes a un escenario, dicha tecnología permite ya tener un control en tiempo real de cualquier anormalidad que pueda presentarse al momento del ingreso. Estas anormalidades pueden surgir por diferentes motivos como por ejemplo el intento de ingreso de credenciales falsificadas. Todas estas anormalidades no se las podría controlar si el acceso fuera realizado de una manera manual donde el factor humano es quien decide quién está o no permitido de acceder, la falta de control en un escenario puede conducir a grandes pérdidas económicas y lo que es más grave, puede ocasionar desastres dentro del mismo por una sobre-ocupación de ciertas áreas.

Los beneficios que se obtienen al implementar la tecnología RFID propuesta para el presente proyecto frente a la situación actual son los siguientes:

- Proceso de acceso rápido y seguro al escenario.
- Reducción del tiempo de espera en filas.
- Reducción del personal necesario para operar un evento.
- Se reducen los abusos y malos manejos.
- Salvaguardo de la integridad física de los asistentes
- Reportes detallados de asistencia en tiempo real.
- Mayor sensación de orden y seguridad.

3.7 CONDICIONES PARA EL USO DE RFID EN LA EMPRESA.

El presente proyecto está enfocado a brindar una solución para la administración de usuarios VIP de un evento u espectáculo al hacer mención a un usuario VIP se hace referencia a las personas que están involucradas directamente en la organización de un evento.

Actualmente se ha dedicado esfuerzos para brindar una seguridad electrónica a los tickets que se generan para los eventos, pero se ha dejado de lado el control de las credenciales que se emiten al personal que está involucrado en la organización de un evento. Es muy importante controlar este segmento de accesos ya que este personal tiene un perfil muy crítico en el sentido que no es un usuario cualquiera sino más bien es un usuario que tiene privilegios de acceso a muchas áreas y si no se mantiene un control minucioso de estos usuarios se puede tener problemas serios tanto en seguridad como en la integridad de los asistentes a un evento ya que en caso de que un individuo falsifique una credencial la cual tenga acceso a áreas críticas puede comprometer verdaderamente la seguridad de dichas áreas ocasionando verdaderos problemas.

Los parámetros de uso de este proyecto vienen definidos por dos factores principales:

- Factor económico.
- Factor nivel de aceptación del producto.

3.7.1 FACTOR ECONÓMICO.

Este factor influye directamente en una inversión inicial, inversión que se encuentra contemplada en el análisis de costos del proyecto dependiendo de la

magnitud del mercado se tendrá que hacer una inversión considerable la misma que permita satisfacer las necesidades del mercado actual.

El proyecto está sujeto a los cambios que se requieran, lo mismos que permitirán adaptarse a una solución, estos cambios pueden involucrar el hardware del prototipo pero en sí la concepción básica del funcionamiento de la solución viene a ser la misma.

Comercialmente es importante que la empresa venda esta solución en conjunto con el producto principal (Ticketing y Control de acceso para usuarios comunes) estas dos soluciones irán de la mano ya que la una es complemento de la otra y como se mencionó anteriormente la solución del presente proyecto lo que busca es brindar una mayor seguridad a un inmueble basándose en el control específicamente del personal involucrado en la organización de un evento.

3.7.2 FACTOR NIVEL DE ACEPTACIÓN DEL PRODUCTO.

Este factor es principalmente un tema social el cual involucra la aceptación de la solución tanto del empresario y de los usuarios directos ya que inicialmente se ha tenido una aceptación negativa a los cambios tecnológicos por parte del público. Siempre hay resistencia a este tipo de cambios especialmente en el campo de control de acceso a espectáculos. Este es un factor que afecta la implementación del proyecto ya que se puede tener una solución bien planteada desde el punto de vista tecnológico y puede ser que desde otro punto de vista no tenga la aceptación debida, lo que finalmente conduce al fracaso de este tipo de soluciones.

Para controlar estas situaciones, la empresa debe atravesar por varias etapas para que las soluciones tecnológicas, especialmente las de control de accesos a espectáculos tengan un buen nivel de aceptación. Una de las fortalezas de este proyecto es basarse en el nivel de aceptación que ha tenido la solución de ticketing y control de acceso para junto con esto ir insertando en el mercado la solución propuesta en el presente proyecto.

CAPITULO 4

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- Al haber finalizado el presente proyecto, se ha alcanzado el objetivo de proporcionar a la empresa Soluciones G4 del Ecuador una solución de seguridad basada en la tecnología RFID la cual permita brindar seguridad, control y administración de los accesos a un inmueble.

- Para el desarrollo del software se utilizó la metodología RUP (Rational Unified Process) debido a que es una de las metodologías más adaptables para proyectos de largo plazo, ya que este método se basa en enfoque iterativo el cual permitió una compresión creciente del problema a través de refinamientos sucesivos que permitieron llegar a una solución efectiva

- La tecnología de identificación por radiofrecuencia tiene muchas ventajas, las cuales están basadas principalmente en ofrecer una seguridad electrónica inviolable, ya que la información de identificación asociada a un objeto o usuario está almacenada en un chip, lo que impide la alteración del mismo por parte de terceros, a diferencia de un código de barras el cual puede ser clonado simplemente con una fotocopia.

- El nivel de aceptación en las tecnologías de identificación depende de un factor social, el mismo que está totalmente desligado de un tema técnico, pero viene a ser un factor muy importante al momento de implementar dicha tecnología. En Ecuador específicamente en el área de espectáculos se han presentado situaciones en las cuales técnicamente una solución tecnológica ha sido exitosa, pero al momento de implementarla el nivel de aceptación por parte del público ha sido nula, ocasionando de esta manera

que el sistema de accesos quede fuera de operación. Con esto concluimos que los sistemas de identificación dependen directamente de dos factores que son el factor técnico y el factor social.

- La solución que ofrece el presente proyecto tiene ciertos beneficios, los cuales podemos analizar principalmente desde dos puntos de vista:

  - **Beneficios para empresarios.**

    - Proceso de acceso rápido y seguro al escenario
    - Reducción del personal necesario para operar un evento
    - Se reducen los abusos y malos manejos
    - Reportes detallados de asistencia en tiempo real

  - **Beneficios para el público.**

    - Acceso fácil y rápido
    - Reducción del tiempo de espera en filas
    - Salvaguardo de su integridad física
    - Mayor sensación de orden y seguridad

- El campo de aplicación de este proyecto está orientado directamente al control de accesos de usuarios, cuyo perfil está vinculado directamente a la organización de un evento o espectáculo, razón por la cual se ha visto la necesidad de implementar un sistema seguro el cual permita hacer un seguimiento que a su vez evite falsificaciones o mal uso de las credenciales entregadas a cada uno de los usuarios, garantizando la integridad física de los asistentes y del artista.

- Haciendo referencia al análisis de costos del proyecto podemos afirmar que la inversión se recupera a partir del mes 18. Para el análisis de la inversión se han tomado en cuenta los parámetros que están involucrados

directamente en la elaboración del proyecto, el valor de dichos parámetros tienen un margen de variación dependiendo del mercado que los provee. Últimamente se ha experimentado muchas variaciones de costos en los equipos utilizados, dicha variación tiene una tendencia a subir los costos.

- Como mejora del proyecto se deja abierta la posibilidad de implementar un sistema de control de acceso híbrido que combine la seguridad de un sistema RFID junto con la seguridad de sistema de identificación por huella digital, combinación que incrementará el nivel de seguridad.

4.2 RECOMENDACIONES.

- Al momento de poner a operar el sistema, se recomienda asegurarse que no exista ninguna fuente de interferencia cercana al campo de acción del lector con la credencial RFID, ya que dicha interferencia puede impedir la transmisión de datos entre la credencial y el lector.
- Es recomendable tener un cuidado en el manejo de los equipos, especialmente con el lector, ya que al ser un equipo crítico dentro del sistema, cualquier interferencia puede ocasionar un mal funcionamiento del mismo, lo que afecta directamente en la operación total del sistema RFID.
- Los equipos utilizados tienen estándares definidos para su operación, los mismos que deben ser respetados para garantizar un desempeño óptimo de los equipos y por ende tener una operatividad garantizada del sistema. Una recomendación principal es cumplir el estándar de la distancia de lectura entre el lector con la credencial RFID.
- Al ser este un sistema de seguridad el cual implica una comunicación en tiempo real entre todos los elementos que forman parte del sistema, se recomienda utilizar equipos de comunicación inalámbrica que sean robustos ante interferencias del medio como por ejemplo las señales de radio y televisión, ya que en el pruebas realizadas en el presente proyecto se encontraron diferentes resultados de comunicación al utilizar equipos inalámbricos de diferentes marcas.

- Se recomienda tener equipos de backup como medida de contingencia ya que es común que al momento de la operación total del sistema se tengan fallas en los equipos, especialmente los equipos más críticos, fallas que podrían conducir al fracaso total del sistema. Adicional a esto es recomendable utilizar las debidas protecciones eléctricas.

- Los resultados de la validación de las credenciales dependen de la interacción que el usuario tenga con el sistema, ya que si el usuario no realiza adecuadamente la lectura de su credencial no se validará su acceso, por lo tanto es recomendable tener una supervisión adecuada con el objetivo de garantizar una interacción óptima entre el usuario y el sistema.

- Es importante implementar una capacitación acerca del manejo adecuado del sistema al personal de supervisión, capacitación que permitirá definir el procedimiento a seguir en el caso de posibles problemas que se presenten en los accesos. Haciendo énfasis en este punto podemos acotar que es muy importante tener establecido un procedimiento que permita solucionar inconvenientes relacionados con errores en la validación de una credencial lícita.

REFERENCIAS BIBLIOGRAFICAS

- ROBERT KLEIST, “RFID Labeling”, Primera edición, Agosto 2004, Printronix, EE.UU.
- AMAL GRAAFSTRA, “RFID Toys”, 2006, Wiley Publishing, Canada
- BILL GLOVER & HIMANSHU BHATT, “RFID Essentials”, Primera Edición, 2006,O´Reilly Media, EE.UU.
- SANDIP LAHIRI, “RFID Sourcebook “, Primera Edición, 2006, IBM Press Books, EE.UU
- STALLINGS WILLIAM, “Comunicaciones y Redes de computadoras”, Sexta edición, Prentice Hall, México.
- TANENBAUM ANDREW S: “Redes de computadoras”, Tercera edición, Prentice Hall, Madrid.
- ING. HIDALGO PABLO, “Folleto de redes LAN”, Octubre 2003.
- ING. AVILA NELSON, “Folleto de Seguridad en Redes”
- IEEE,”RFID Journal”,Junio 2008
- RFID JOURNAL; Editorial Mark Roberti Vol. 5, Nº3, Junio 2008
- GLOVER Bill; RFID Essentials; Editorial O Reilly, 2006
- KLEIST Robert; RFID Labeling; Editorial Printronix, 2004
- HARTMANN Paul, IEEE Applications & Practice RFID; Vol. 45 Nº9, Septiembre 2007

- http://www.rfid-handbook.de/rfid/
- http://www.autoidlabs.com/whitepapers/MIT-AUTOID-WH-008.pdf
- http://www.autoidlabs.org/whitepapers/MIT-AUTOID-WH-002.pdf
- http://www.autoidcenter.org/publishedresearch/mit-autoid-tr009.pdf.
- Internet Engineering Task Force Request for Comments RFC-2141
- http://www.ietf.org/rfc/rfc2141.txt.
- http://www.rfidjournal.com/article/articleview/421
- http://www.eff.org/Privacy/Surveillance/RFID/rfid_position_statement.php
- http://www.nyjournalnews.com/newsroom/012204/d0122rfid.html
- http://www.epcglobalinc.com
- http://www.aimglobal.org/technologies/rfid/

- http://occonsultores.com/mifare.html
- http://www.idensis.com/tecnologias_elementos.html
- http://www.tec-mex.com.mx/promos/bit/bit0703-msr.htm
- http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm
- http://www.ent.ohiou.edu/~amable/autoid/history.htm
- http://wireless.itworld.com/4985/051004_book_rfidsourcebook/page_1.htm

ANEXOS

ANEXO A

LECTOR RFID HF MIFARE DESFIRE CONTACTLESS

Descripción:

Lector para equipos portátiles con conectividad *Compact Flash* y alta velocidad de transferencia de datos. Lee tags y tarjetas HF (13,56 MHz), compatibles con las normativas ISO 14443A, ISO 14443B, ISO 15693, ISO 18000-3, dispositivos RFID EPC (*Electronic Product Code*), Mifare ®, NFC (*Near Field Communication*) e ICODE.

Frecuencia

13,56 MHz

Compatible con las normativas ISO

ISO 14443A
ISO 14443B
ISO 15693
ISO 18000-3
NFC (*Near Field Communication*)
ICODE

Tags soportados

Mifare ® Standard
Mifare ® 4k
Mifare ® Pro
Mifare ® Ultralight
Mifare ® DESFIRE

Mifare ® SmartMX
I-CODE SLI (SL2 ICS 20)
I-CODE EPC (SL2 ICS 10)
I-CODE UID (SL2 ICS 11)
I-CODE
NFC (Reader To Tag Mode)
SLE 55Rxx
SRF55VxxP +S
SLE 66CL160S
SLE 66CLX320P
SR176
SRIX4K
LRI 64
LRI 512
EM4135
KSW Temp Sens ®
Tag-it™ HF-I Standard
Tag-it™ HF-I Pro
Jewel Tag
Sharp B
ASK GTML
ASK GTML2ISO
TOSMART P032/P064
ISO14443A Tags
ISO14443B Tags
ISO15693 Tags

Antena

Interna incluida

Interface de comunicación

Compact Flash Card Type II
De 6900 bit/s a 115kbit/s, N, 8, 1

Protocolo de comunicación con el host

ASCII
Binario

Software y drivers

No requiere driver
API - DLL

Alimentación y consumo

200mA en modo activo máx. 310mA

<65 mA Antenna Off
< 1m A en modo bajo consumo

Transmisión

Distancia de lectura: hasta 60 mm dependiendo del tag
Velocidad de transmisión: hasta 848 kbit/s

Dimensiones y peso

86,5 x 43 x 10 mm ± 0,1mm
26 gr ± 10%

Ambiente

Temperatura de funcionamiento: 0ºC a 70ºC
Temperatura de almacenaje: -20ºC a 85ºC

Normativa

De acuerdo a la normativa RoHS
ETS 300-330
CE
FCC

Aplicaciones habituales

Aplicaciones con equipos portátiles
Acceso a ordenadores
Logística y gestión de suministros
Ticketing para eventos y transporte público
Autenticación
Equipos de producción

ANEXO B

TERMINAL LAN POINT MOBILE TEXAS INSTRUMENTS

Especificaciones Técnicas

Construction	Palmheld or Pistol-Grip Integrated Stylus Holder Hand Strap or Lanyard (stretchable, adjustable and removable) Co-molded, not over-molded, for ruggedness Ergonomic design
Operating System	Windows CE .NET 4.2 with .NET Compact Framework 1.0, or Windows CE 5.0 with .NET Compact Framework 2.0
	Intel Xscale PXA255, 400MHz processor 128MB RAM, 96MB Flash Persistent Storage (Data, System Files, Registry) Compact Flash Slot (Integrated or Optional User Accessible) SD/MMC (User Accessible)
End Cap or Docking Station Accessories for expanded	RS232/USB host/USB client

functionality	
	Modem/RS232/USB host/USB client
	Mag stripe reader (future)
Communications	IEEE802.11b/g (WLAN)(optional)
	Cingular GSM/GPRS (WWAN)(optional)
	Bluetooth (WPAN)(optional)
	Full RS-232
	USB 1.1 host for barcode scanners, keyboard, printers, etc.
	USB 1.1 client for syncing with a host
Display	3.5" QVGA (240x320)
	64K Color
	Transflective/Sunlight Readable
	Touch Screen with stylus or finger
	Integral, convenient stylus holder
	Backlit (varying levels software controlled and keyboard on/off)
Indicators	Front panel LED’s
	Charge Indication (Yellow/Green)
	Programmable LED (Green)
	Integrated Vibrator
Keypad	49 key, full alphanumeric, plus 2 side Scan keys
	12 Function Keys, (4 dedicated, 8 shifted)
	Backlit, software controlled (on/off)
	One centrally located Scan key, Two side Scan Keys (ergonomic/right or left-hand operation). Pistol-grip models have an additional trigger in the grip.
	2 " Enter " Keys (right/left-hand accessible)
	Large Numeric Keys
	Flat, rubberized, non-glare keys
	One-hand (sticky key) operation
	Programmable Audible " key clic "
	Software Keypad
	Shift & Navigation Key LED indicators
Audio Capabilities	Integrated Speaker
	Integrated Microphone
	Beeper/Buzzer: 90dBA programmable volume, pitch and duration
	Headset jack, 3.5mm
Power	Removable Li-Ion rechargeable battery
	3.7V, 4400mAh min. (one comes with each unit, standard)
	Back-up Li-Ion 3.7V, 120mAh
	8 hr. minimum live use (scanner, keyboard and radio use)

	No data loss and uninterrupted operation during battery change
	Power jack for external power and charging
	Gas Gauge
Environmental	Operating Temp: 14º to 131ºF (-10º to 55º C)
	Storage Temp: -13º to 140ºF (-25º to 60ºC)
	IP64, NEMA-3
	Drop test rating: 5 feet, multiple times to concrete
	Relative Humidity: 5 to 95% non-condensing
	UL flame Rating: 94V/0
	FCC Part 15 Class B
	European CE
Physical	Dimensions - palmheld, without endcap: 8.60” L x 3.80” W (at display), 3.16” W (at keypad) x 1.40” D
	Dimensions - pistol-grip, without endcap: 8.60” L x 3.80” W (at display), 3.16” W (at keypad) x 6.53” D
	Weight - palmheld: 25.5 oz. (Long Range Laser & WLAN); 28.5 oz. (Standard Laser & WLAN)
	Weight - pistol-grip: 27 oz. (Long Range Laser & Bluetooth)
AutoID Choice	None - keyboard only
	Integrated standard-range laser (SE1224HP or SE923 - SE923 is the only scanner available in models with the user-accessible Compact Flash slot)
	Integrated long-range laser (SE1524ER)
	Integrated 2D laser (SE2223)
	Integrated imager (IT5180SR)
Supported Symbologies& Scan Ranges	See below
Optional Input Devices - via RS232 or USB interface	Wands
	External Lasers
	Barcode Slot
	Handheld CCD’s
	Magnetic Stripe
Application and 3rd Party Software	ActiveSync
	Inbox - Email
	Internet Explorer 6.0 (Full CE Version)
	Windows Messenger
	WordPad
	Windows Media Player
	Hand writing recognition
	Download tool for upgrades
	Signature Capture

Development Tools	Voice recorder Terminal Emulation (optional license required for production use) Remote Desktop Protocol optional MS Office Viewers, Excel, Image, PDF, PowerPoint, Word Software Developer's Kit (SDK)– Support for eVC++, Visual Basic.NET, Visual C# Custom Control for Super Wedge interface Sample/Demo applications available XML, Jscript, VBScript NDIS 5.1 Network Utilities Object Exchange Protocol (OBEX) Speech API TCP/IP Active Template Library (ATL) DCOM, DirectX, MFC SNMP, SOAP, Pocket Outlook Object Model API SQL Server

ANEXO C

ETIQUETAS MIFARE HF

- Tarjeta inteligente sin contacto
- Tecnología Mifare
- RF interface: ISO 14443A
- Material: PVC
- Temperatura: -10ºC a +50ºC
- Dimensión: Largo 85.6 mm , Ancho 53.98 mm, Grosor 0.88 mm
- Lectura / escritura
- 1 KByte

ANEXO D

ACCESS POINT LINKSYS WAP11

General

MPN: WAP11-EU, WAP11-FR, WAP11

Tipo de dispositivo: Punto de acceso inalámbrico

Anchura: 22.6 cm

Profundidad: 12.7 cm

Altura: 4.1 cm

Peso: 0.3 kg

Localización: Europa, Francia

Conexión de redes

Factor de forma: Externo

Tecnología de conectividad: Inalámbrico

Velocidad de transferencia de datos: 11 Mbps

Formato código de línea: CCK, BPSK, QPSK

Protocolo de interconexión de datos: Ethernet, IEEE 802.11b

Método de espectro expandido: DSSS

Protocolo de gestión remota: SNMP

Banda de frecuencia: 2.4 GHz

Alcance máximo en interior: 150 m

Alcance máximo al aire libre: 500 m

Nº de canales seleccionables: 13

Indicadores de estado: Actividad de enlace, alimentación

Características: Soporte de DHCP, equilibrio de carga, filtrado de paquetes, filtrado de dirección MAC, Soporte de DHCP, equilibrio de carga, filtrado de

dirección MAC, filtrado de direcciones IP, Equilibrio de carga, filtrado de dirección MAC

Algoritmo de cifrado: WEP de 128 bits

Cumplimiento de normas: IEEE 802.3, IEEE 802.11b, IEEE 802.3, IEEE 802.11b, Wi-Fi CERTIFIED, IEEE 802.11b

Red / Protocolo de transporte: TCP/IP

Antena

Cantidad de antenas: 2

Antena: Externa desmontable

Expansión / conectividad

Interfaces:

- 1 x red - Ethernet 10Base-T - RJ-45
- 1 x red - Radio-Ethernet
- 1 x gestión - USB, 1 x red - Ethernet 10Base-T - RJ-45
- 1 x red - Radio-Ethernet
- 1 x USB - 4 PIN USB tipo B

Software / requisitos del sistema

Software incluido: Controladores y utilidades

Sistema operativo requerido: Microsoft Windows 95/98, Microsoft Windows 2000 / NT4.0, Microsoft Windows Millennium Edition, Microsoft Windows 95/98, Microsoft Windows 2000 / NT4.0, Microsoft Windows Millennium Edition, Microsoft Windows XP, Microsoft Windows NT 4.0, Microsoft Windows 95/98, Microsoft Windows 2000, Microsoft Windows Millennium Edition

Parámetros de entorno

Temperatura mínima de funcionamiento: 0 ℃

Temperatura máxima de funcionamiento: 55 ℃

Ámbito de humedad de funcionamiento: 0 - 70%

Acces Point Dlink DWL 2100AP

Product Specifications

Standards
- IEEE 802.11b/g wireless LAN
- IEEE 802.3/u Ethernet

Network Data Transfer Rate
(With auto-fall back) *
- For 802.11g:
  108 (Turbo), 54, 48, 36, 24, 18, 12, 9 and 6Mbps
- For 802.11b:
  11, 5.5, 2, and 1Mbps

Media Access Control
- CSMA/CA with ACK

Wireless Frequency Range
- 802.11b: 2400 to 2483.5MHz ISM band
- 802.11g: 2400 to 2483.5MHz ISM band

RF Modulation Schemes
- 802.11b: DQPSK, DBPSK and CCK
- 802.11g: BPSK, QPSK, 16QAM, 64QAM, OFDM

Receive Sensitivity (802.11b)
@ 8% PER (packet error rate)
- 11 Mbps: -83 dBm
- 2 Mbps: -89 dBm

Receive Sensitivity (802.11g)
Frame: 1000byte PDUs, @ 10% PER (packet error rate)
- - 54 Mbps: -66 dBm
- - 48 Mbps: -71 dBm
- - 36 Mbps: -76 dBm
- - 24 Mbps: -80 dBm
- - 18 Mbps: -83 dBm
- - 12 Mbps: -85 dBm
- - 9 Mbps: -86 dBm
- - 6 Mbps: -87 dBm

Typical Transmit Output Power*
17 dBm (typical)

Antenna
2dBi Gain detachable dipole antenna with reverse SMA connector

Operation Modes
- Access Point
- WDS With AP
- WDS (Bridge)
- Universal Repeater
- AP Client

Security
- 64/128/152-bit WEP data encryption
- WPA-PSK, WPA2-PSK
- WPA-EAP WPA2-EAP (AP mode only)
- TKIP, AES
- MAC address filtering
- WLAN STA partitioning
- 8 SSID for network segmentation
- SSID broadcast disable function
- 802.1Q VLAN Tagging

QoS & Performance Enhancement
- WMM (Wi-Fi Multimedia) certified
- AP grouping for load balance

Device Configuration/Management
- Web-based management: Internet Explorer v.6 or later; Netscape Navigator v.7 or later; or other
- Java-enabled browsers
- SNMP v.1, v.3
- MIB-I, MIB-II
- Telnet
- Windows-based AP Manager utility
- SSL/SSH protocol support
- Factory reset button

LEDs Power
- WAN
- LAN (10/100Mbps)
- WLAN

Physical & Environmental

Power Input
- DC 5V, 2.0A
- Through external power adapter

Power Consumption
5 watts (max.)

Dimensions
142 (L) x 109 (W) x 31 (H) mm

Operating Temperature
0° to 40°C

Storage Temperature
-20° to 65°C

Humidity
95% maximum (non-condensing)

Certification
- FCC Class B
- CE
- C-Tick
- CSA
- Wi-Fi™

ANEXO E

IMPRESORA EVOLIS DUALYS 3 ID

Modo de impresión de tarjetas
- » Sublimación color y transferencia térmica monocromo
- » Impresión estándar de tarjeta a sangre (borde a borde)

Características de impresión
- » Nuevo sistema de limpieza de tarjetas a doble cara
- » Economizador de cinta integrado para impresión en monocromo

Velocidad de impresión
- » 150 tarjetas / hora en color (YMCKO), una cara
- » 125 tarjetas / hora en color (YMCKO/K), dos caras
- » Hasta 1.000 tarjetas / hora[1] en monocromo, una cara
- » Hasta 350 tarjetas / hora en monocromo, dos caras

Resolución
- » 300 dpi (11,8 puntos/mm)

Software suministrado
- » Cardream3 para creación e impresión de tarjetas
- » Compatible con Windows™ NT4, 2000, Xp y Vista

Drivers
- » Para Windows ™ Me / 2000, Xp y Vista

Garantía
- » Impresora: 3 años
- » Cabezal de impresión: 3 años, número ilimitado de impresiones

Tipo de Cinta
- » Cinta monocromo: 1.000 tarjetas / rollo
- » Colores monocromos: negro, azul, rojo, verde, blanco, dorado, plateado y tinta rascable
- » Cinta monocromo de 2 paneles (KO): 500 tarjetas / rollo
- » Cinta de color de 5 paneles (YMCKO): 200 tarjetas / rollo
- » Cinta de color de 1/2 paneles (YMCKO): 400 tarjetas / rollo

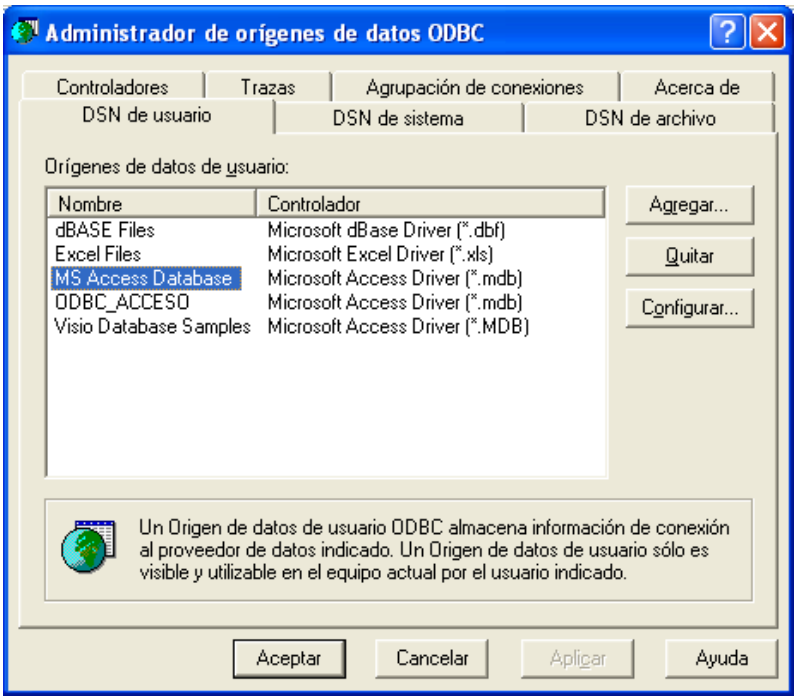
ANEXO F

MANUAL DE USUARIO

1 Instalación de módulos de software

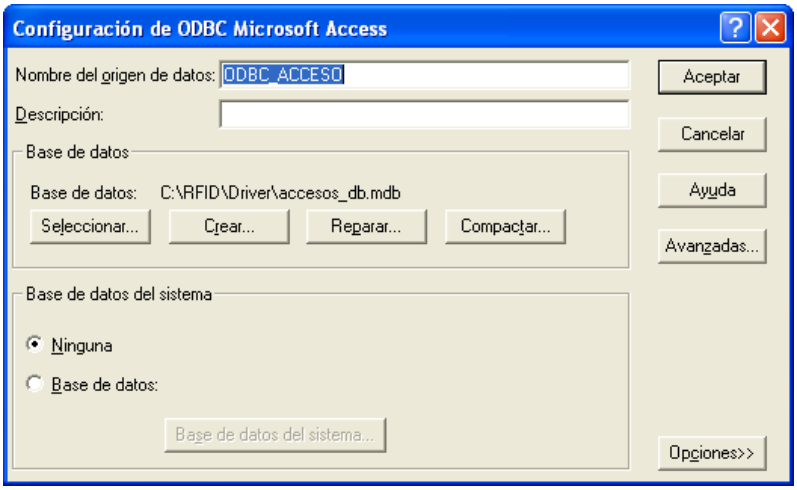
1.2 Instalación del Software de registro de usuarios

Generar el ODBC con la base de datos accesos_db.mdb, de la siguiente manera: En el panel de control de Windows en Herramientas Administrativas seleccionamos la opción **ORIGENES DE DATOS ODBC**, tal como se muestra en la figura 3.6 escogemos la opción **MS Access DataBase**



Interfaz para crear la conexión ODBC

Seleccionamos la opción de **Configurar** y tenemos la siguiente interfaz en la cual seleccionamos la dirección donde está ubicada la base de datos **accesos_db.mdb.** Esta base debe estar ubicada en la siguiente dirección: C:\RFID\Driver\



Selección de la Base de datos

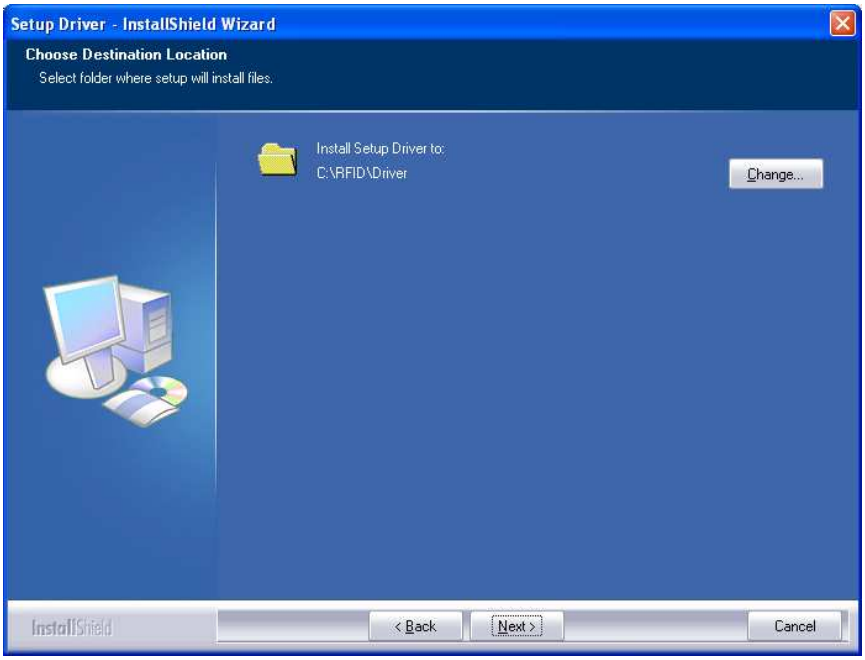
Una vez que hayamos seleccionado la base de datos en la parte de Nombre del origen de Datos ponemos: **ODBC_ACCESO.**

Finalmente damos clic en crear

Ubicar el ejecutable del software de registro de usuarios en el escritorio para que esté listo para su uso.

1.3 Instalación del Software recolector de Datos (Driver)

Se procede a ejecutar el instalador llamado **Setup Driver** luego de esto el sistema mostrara la dirección en la cual se desea instalar la aplicación



Instalación del Driver

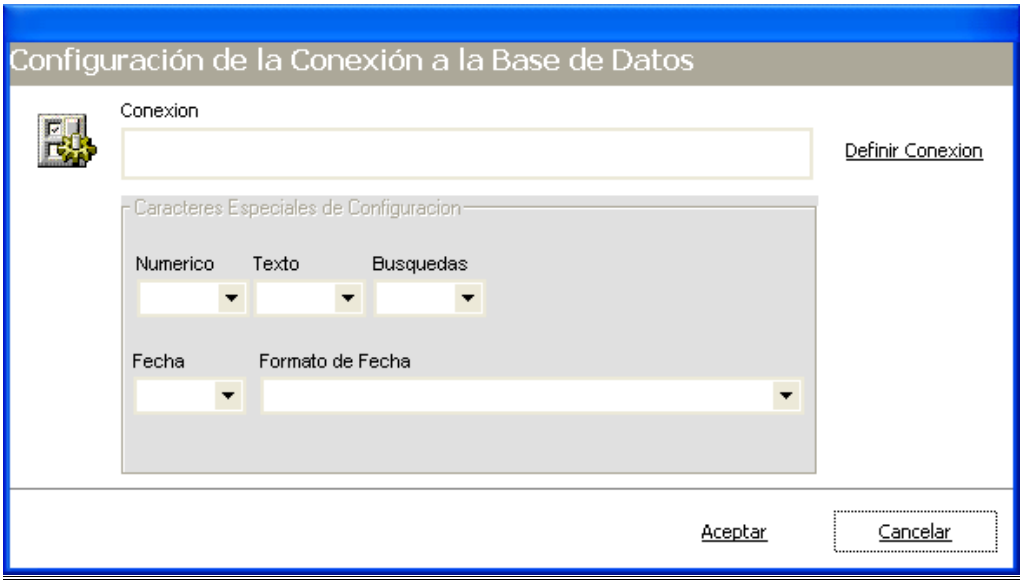
La aplicación se procede a instalar en la dirección: C:\RFID\Driver\.

Una vez terminada la instalación el programa automáticamente genera en el escritorio un acceso directo llamado **Driver**.

Ejecutar este acceso directo y seguidamente el programa presenta una pantalla donde se define la conexión con las dos bases de datos del sistema: res_110208_XOCH y accesos_db, las conexiones se deben definir en el orden que se menciona a continuación:

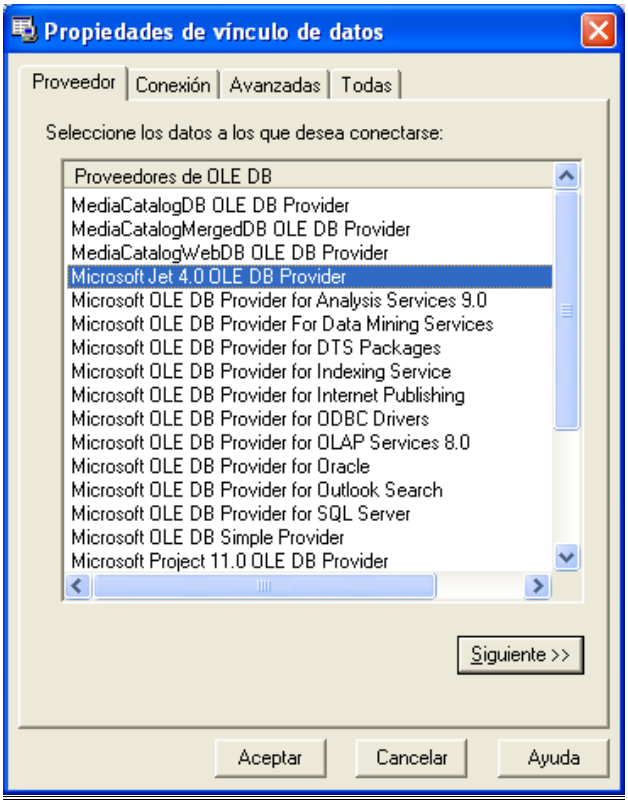
1.- res_110208_XOCH

2.- accesos_db



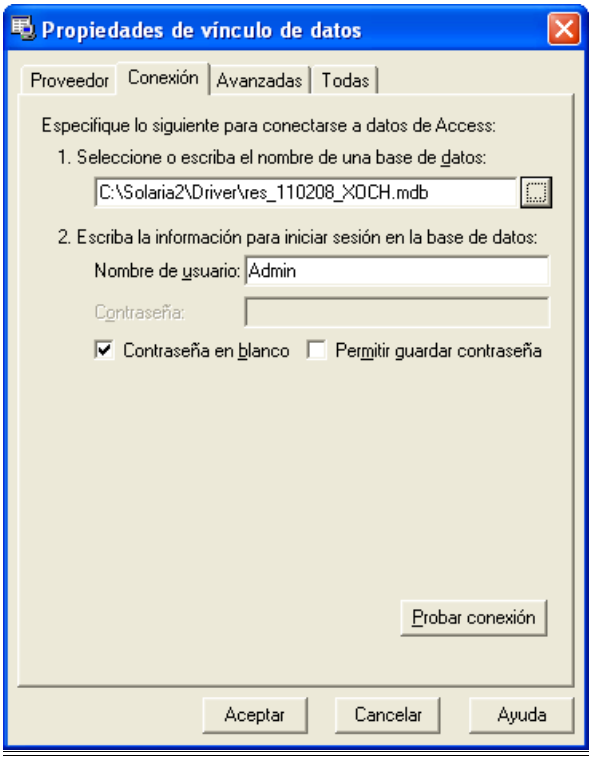
Configuración de conexión a la Base de Datos

Damos clic en definir conexión para y se mostrará la siguiente pantalla donde se escoge la opción seleccionada.



Selección del vínculo de datos

Finalmente se define la dirección donde está ubicada la base de datos y se da clic en aceptar.



Selección de la Base de Datos

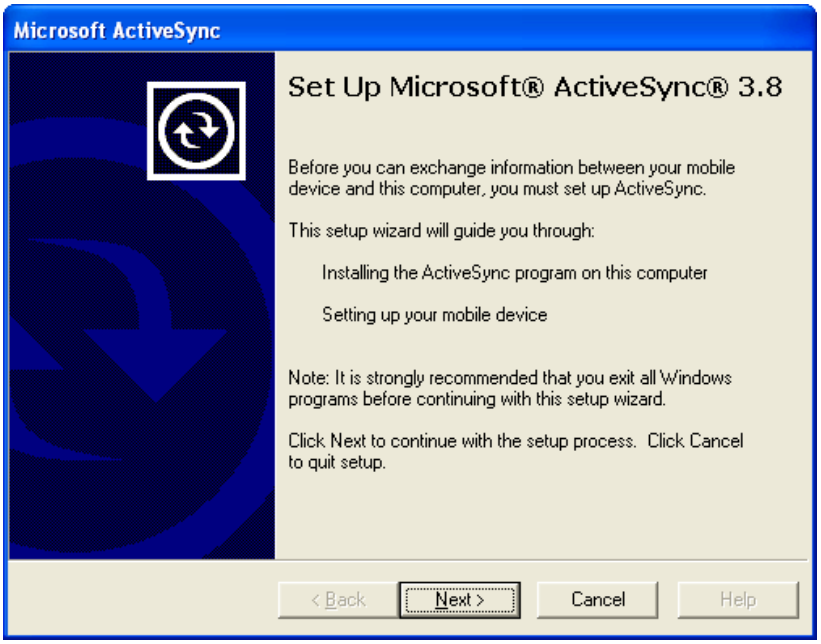
1 Para establecer la conexión con la otra base de datos (accesos_db) seguimos los mismos pasos anteriores.

2 Una vez realizadas estas dos conexiones el Driver procede a abrirse por primera vez y queda listo para su uso.

1.4 Instalación del Software de la Terminal RFID

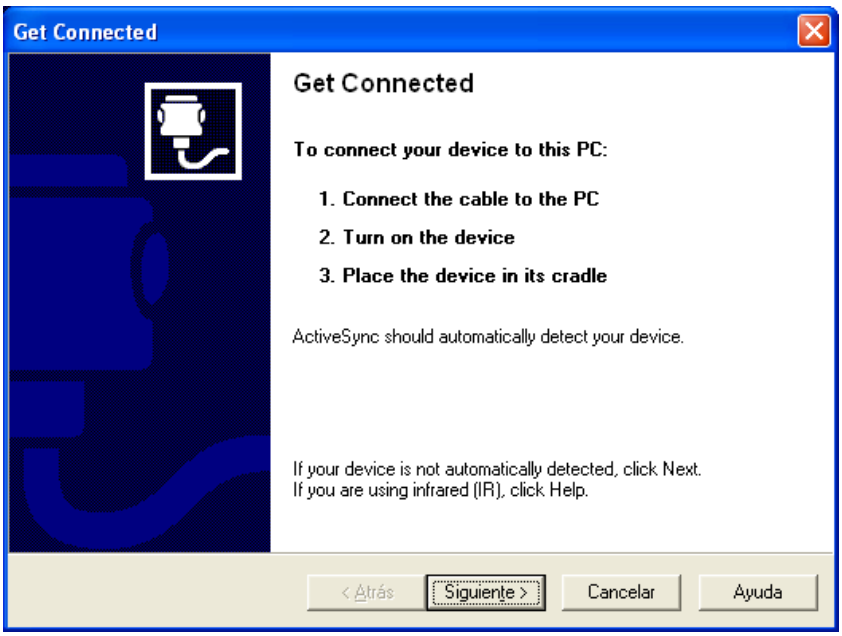
Para realizar la conexión de la Terminal Móvil con la PC es necesario tener a disposición la aplicación ACTIVESYNC y los drivers de la Terminal Móvil.

- Para empezar se debe instalar primero el ACTIVESYNC esto para sincronizar la Terminal móvil con el PC.



Instalación de ActiveSync

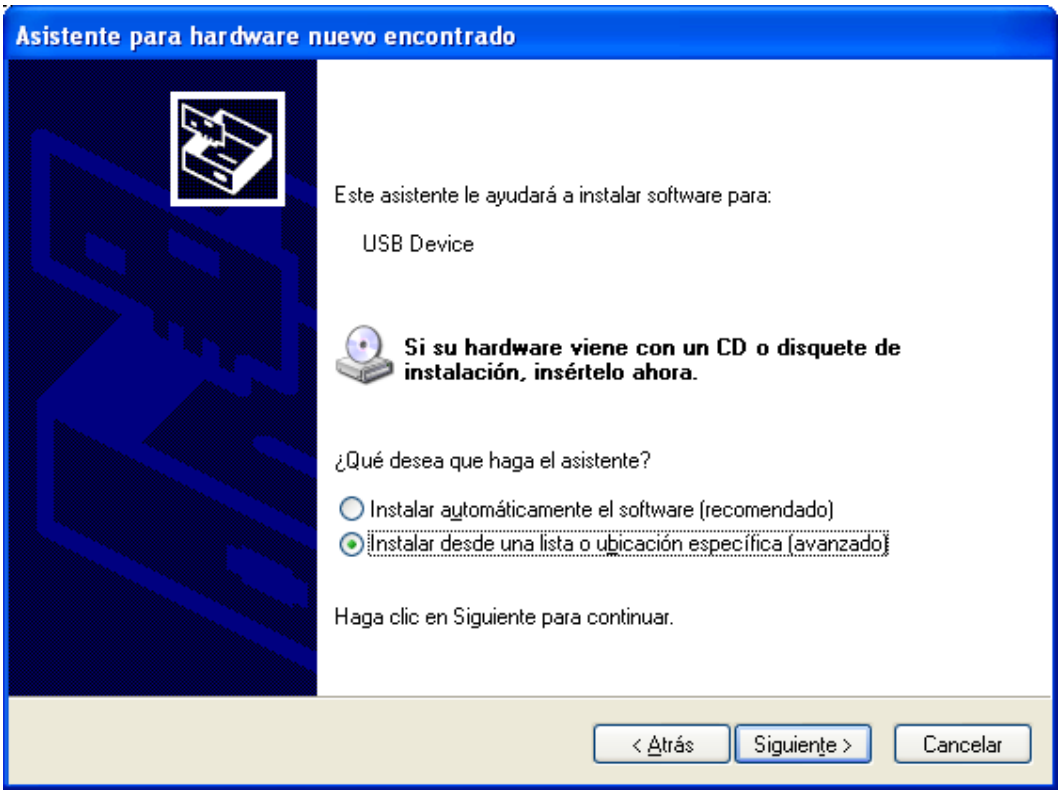
Se debe seguir los pasos hasta llegar a la siguiente ventana de dialogo.



Interfaz de conexión del dispositivo móvil con la PC

Aquí ponemos **Cancelar** ya que la aplicación está solicitando que se realice la conexión con el dispositivo móvil.

- Una vez hecho esto procedemos a conectar por medio del cable USB la Base y la PC, cabe recalcar que sobre la base debe estar conectada la Terminal Móvil y demás debe estar encendida. Luego el sistema operativo de la PC detectará automáticamente que se ha encontrado un nuevo hardware, y escogemos el modo de instalación avanzado



Instalación de dispositivo móvil

Luego buscamos la ubicación del driver **wceusbsh** y ponemos **Aceptar** para que inicie el proceso de instalación.

Aquí tendremos una ventana de diálogo en cual el Sistema Operativo advierte sobre la integridad del software que se está instalando hacemos clic en **Continuar.**

Validación de la integridad de software

Luego tendremos una ventana de dialogo que indicará que el Hardware se instaló correctamente y está listo para usarse.

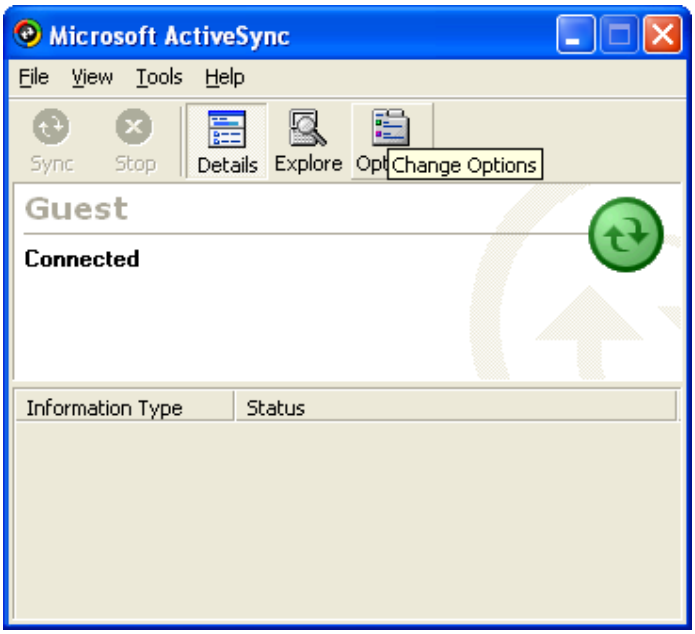
- Procedemos a retirar la Terminal Móvil de la Base y nuevamente a ponerla.
- Abrimos la aplicación Microsoft ActiveSync.

Ejecutar ActiveSync

Y se sincronizarán ya Terminal Móvil y la PC y tendremos la siguiente ventana de diálogo en la cual presionamos **Cancelar**

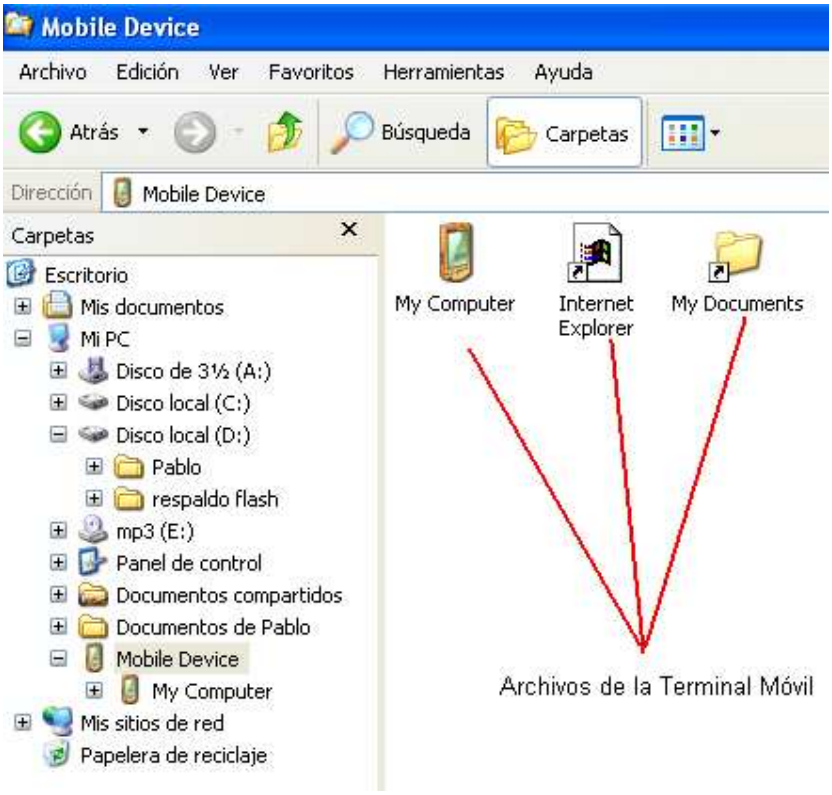
Sincronización de dispositivo móvil con la PC

Y luego tendremos la ventana en la cual se indica que se ha conectado la Terminal Móvil y cerramos esta ventana para terminar.



Estado de conexión ActiveSync

- Ahora verificamos que el contenido de la Terminal Móvil este visible en el explorador de la siguiente manera:



Archivos de dispositivo móvil

Aquí podemos ver los archivos de la Terminal móvil.

- Copiamos los archivos de instalación **LPMobile_WCE4.ARMV4** desde la PC a la Terminal Móvil en el siguiente path: ***\Windows***

  NOTA: *Para realizar este paso la Terminal Móvil debe estar conectada con la PC*.
- Procedemos a retirar la Terminal Móvil de la Base y con el Lápiz puntero damos doble clic en el icono de **Mi Computer** y dentro de esta carpeta estarán varias carpetas entre ellas **Windows** damos doble clic en esta carpeta para ver su contenido y aquí encontraremos los archivos de

instalación **LPMobile_WCE4.ARMV4** que copiamos anteriormente en la Terminal Móvil damos doble clic sobre éste para ejecutarlo y instalar la aplicación para el control de acceso, seguimos los pasos que nos pide el instalador hasta finalizarlo.

- Una vez finalizada la instalación procedemos a copiar las librerías de la lectora RFID(**CFReader.dll y CFReaderDLLWrapper.dll**) y el ejecutable(**RFIDEPN**) en la misma dirección que se instaló el software, esto es en **\Flash\Rfid**
- Procedemos a insertar la tarjeta lectora en la Terminal utilizando la interface COMPACT FLASH

Finalmente verificamos que la aplicación se haya instalado de la siguiente manera:

Inicio->Programs->**RFIDEPN**

Damos clic y la aplicación y se abre encendiendo a su vez el led indicador de la tarjeta lectora RFID.

2 Manual de operación del sistema

Con el objetivo de hacer más comprensible el uso de la aplicación, se procederá a utilizar como guía base el siguiente diagrama de flujo

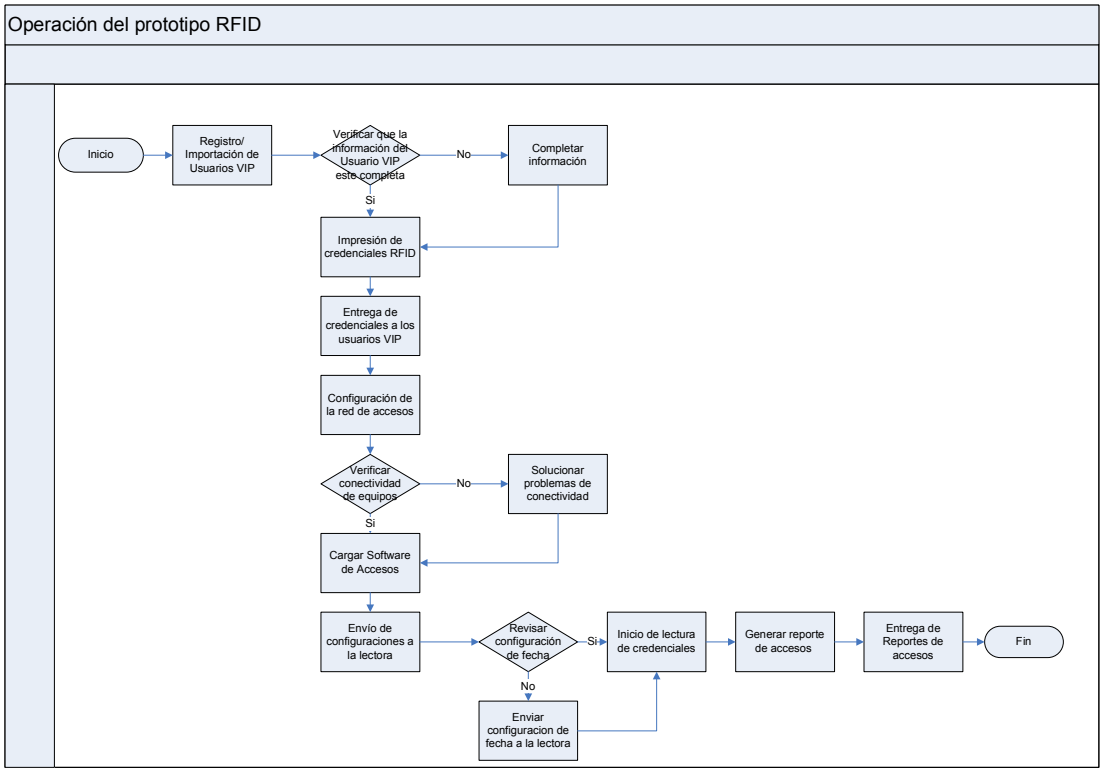
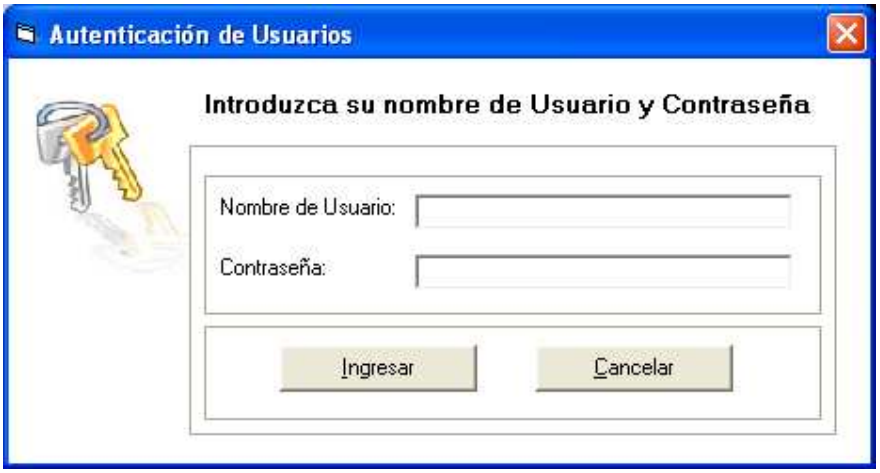


Diagrama de flujo para la funcionalidad del sistema RFID

Registro / Importación de Usuarios VIP

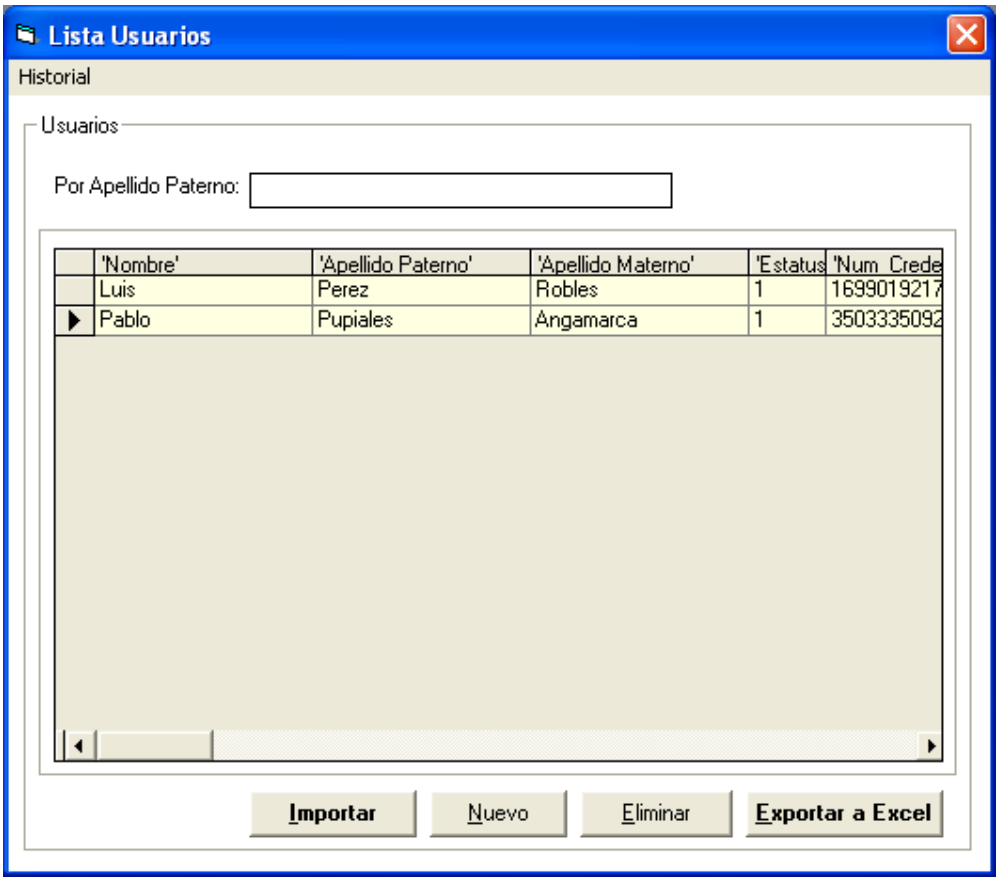
Abrimos la aplicación por medio del acceso directo del escritorio llamado **ControlAcceso**

Digitamos el usuario y la respectiva contraseña



Autenticación del software de registro de usuarios

Una vez que se haya ingresado al sistema se procede a escoger el catalogo de ***USUARIOS->ADMINISTRACION DE USUARIOS***



Catálogo de usuarios

Este catálogo tiene las siguientes funcionalidades.

- Importar: Esta opción permitirá importar información desde un archivo de Excel a la base de datos accesos_db.mdb con el objetivo de almacenar esta información en el caso que se tenga la información en el formato Excel.
- Nuevo: Permite crear un nuevo usuario VIP, los parámetros que se ingresan en este catálogo son:
    - Apellido Paterno
    - Apellido Materno
    - Nombres
    - Nombre del evento: Evento para el cual esta permita la credencial
    - Fecha del evento: Fecha del evento para la cual está permitida la credencial
    - Estatus: Estado del usuario (1=Usuario activo 2=Usuario inactivo)
    - Numero de credencial: Numero de la credencial RFID
    - Inicio de Acceso: Hora desde la cual está permitido ingresar el usuario VIP
    - Fin de Acceso: Hora hasta la cual está permitido ingresar el usuario.

Crear un nuevo usuario

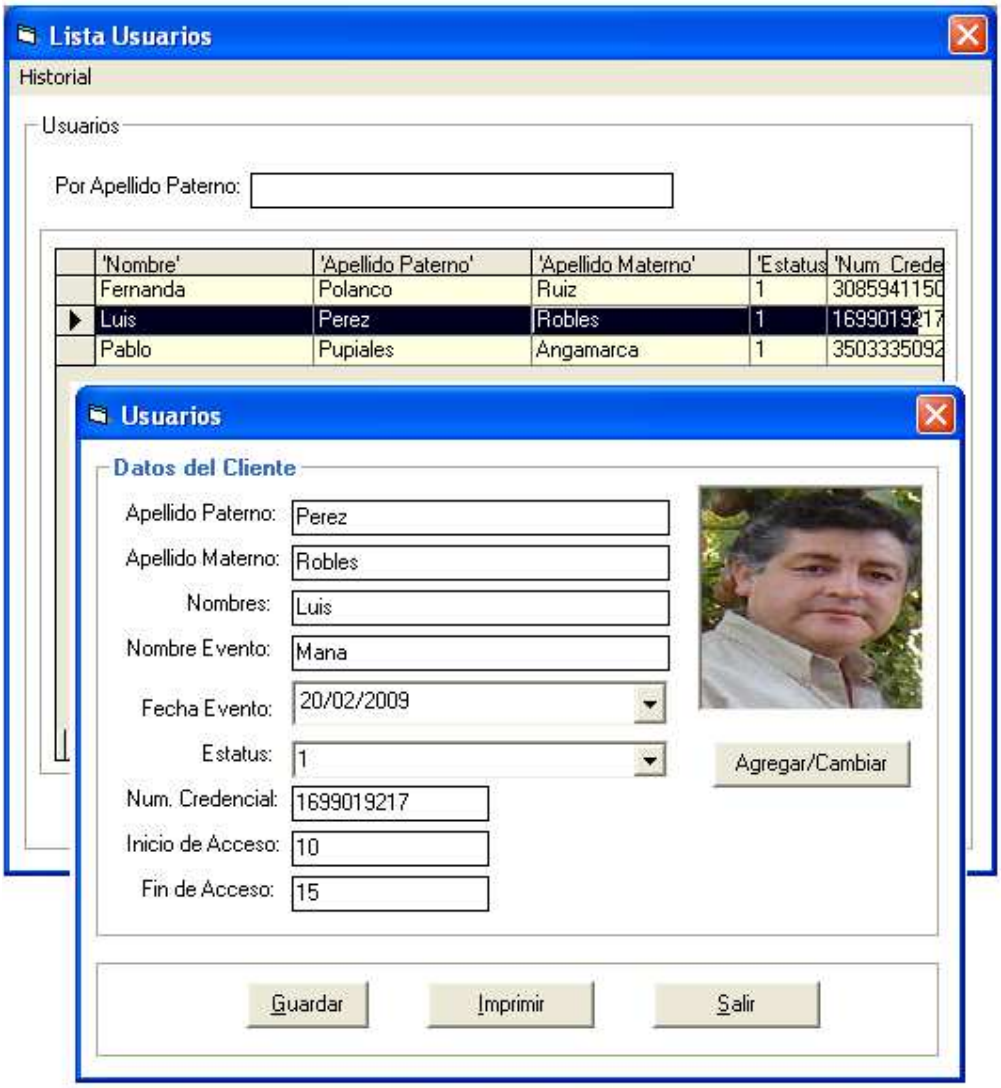
Una vez que se haya ingresado todos los datos se procede a **Guardar** y el usuario queda ya almacenado en el sistema.

Para imprimir la información en la credencial se escoge el botón **Imprimir** y automáticamente se envía a imprimir en la impresora de tarjetas PVC predeterminada de Windows.

- Eliminar: Permite eliminar un usuario seleccionado de la lista
- Exportar a Excel: permite exportar a un archivo de Excel los usuarios registrados.

Verificar que la información del usuario VIP este completa

Es importante revisar que la información de los usuarios VIP este completa si no este el caso se procede a editar al usuario y adicionar la información faltante. Para esto nos dirigimos al catálogo de usuarios y damos doble clic sobre el usuario que desea modificar



Modificar un usuario

Ingresamos toda la información faltante y procedemos a guardar la información.

Impresión de credenciales RFID

Antes de realizar la impresión el sistema se mostrará una vista previa del diseño a imprimir una vez que se revise que toda esta información está en orden se procede a dar clic en el botón Imprimir para proceder con la impresión de la credencial RFID.

Impresión de credenciales RFID.

La información básica que se imprime en la credencial es:

- Nombre del evento
- Fecha del evento
- Nombre del usuario VIP
- Foto del usuario
- Imagen del evento.

Una vez que esté lista la impresión de las credenciales se procede a la entrega de las mismas a los usuarios VIP y aquí finaliza la primera etapa que la emisión de credenciales.

Configuración de la Red de Accesos

La red de accesos está compuesta por los siguientes elementos:

- Servidor de Base de Datos
- Access Point
- Lectora (LanPoint Mobile y Tarjeta de Lectura RFID)

Tanto el servidor de Base de Datos como la Lectora tienen sus respectivas interfaces de red inalámbrica por lo que es necesario definir una red utilizando el protocolo de comunicaciones TCP/IP, para lo cual se define el direccionamiento IP utilizando la Red 100.1.1.1, por lo que la distribución de red queda estructurada de la siguiente manera:

Direccionamiento de la Red de Accesos			
Equipo	**Dirección IP**	**Mascara de Red**	**Puerta de enlace**
Servidor de Base de Datos	100.1.1.2	255.255.0.0	100.1.1.254
Lectora 1	100.1.1.101	255.255.0.0	100.1.1.254
Lectora 2	100.1.1.102	255.255.0.0	100.1.1.254
Lectora 3	100.1.1.103	255.255.0.0	100.1.1.254
Access Point	100.1.1.201	255.255.0.0	100.1.1.254

Direccionamiento de la Red de accesos

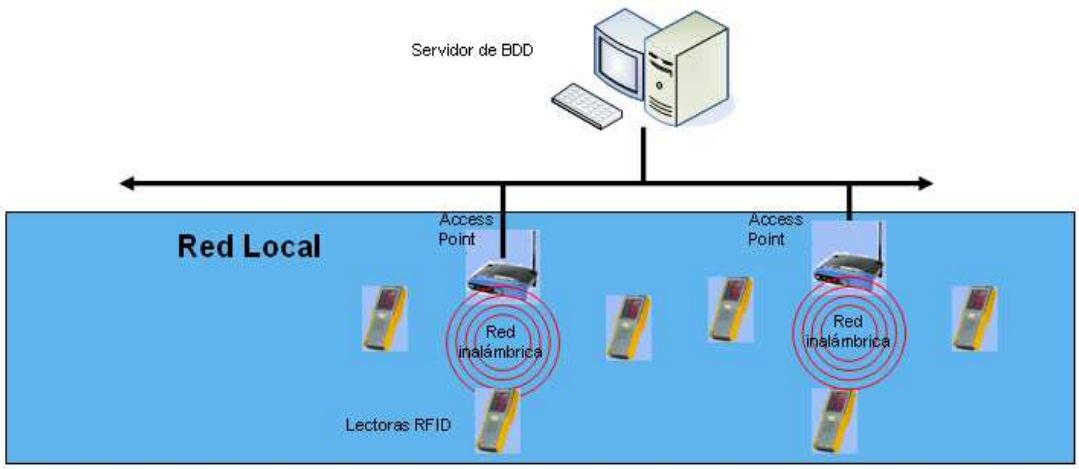
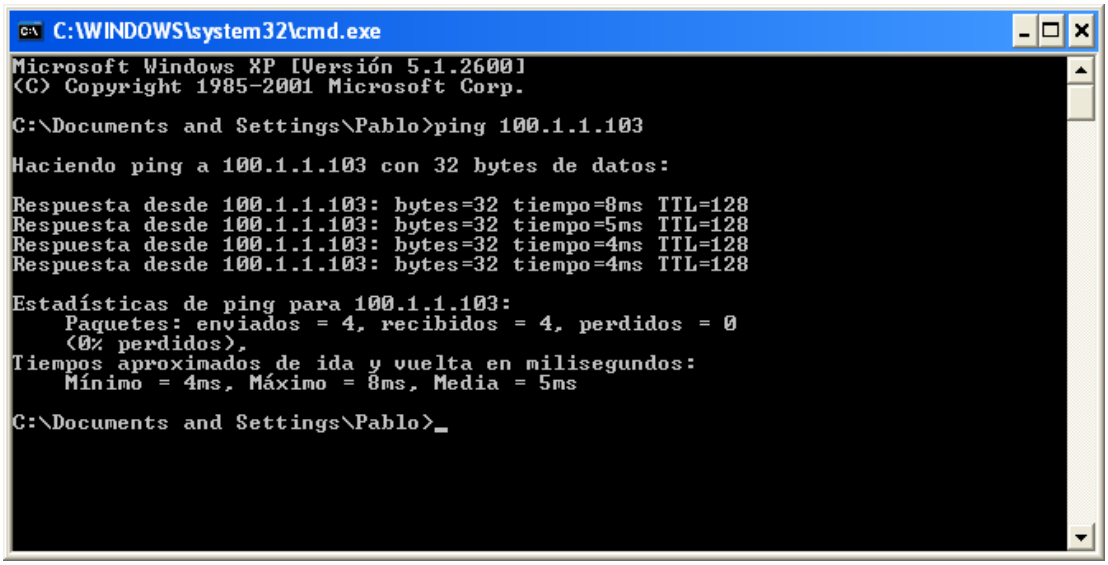


Diagrama de conexión de la Red de accesos

Verificar conectividad de equipos

La conectividad de los equipos se la realiza utilizando el comando ping tal como se muestra en la siguiente figura.



Test de conectividad de equipos

Como se puede apreciar en la figura anterior se realiza una prueba de conectividad entre el servidor y la lectora cuya dirección IP es la 100.1.1.103 y se puede concluir que si hay la conectividad de estos equipos.

En el caso de que no exista respuesta de conexión entre estos dos equipos hay que revisar principalmente los dos parámetros.

- Configuración del access point: Revisar que la configuración de encripcion WEP este correctamente realizada.

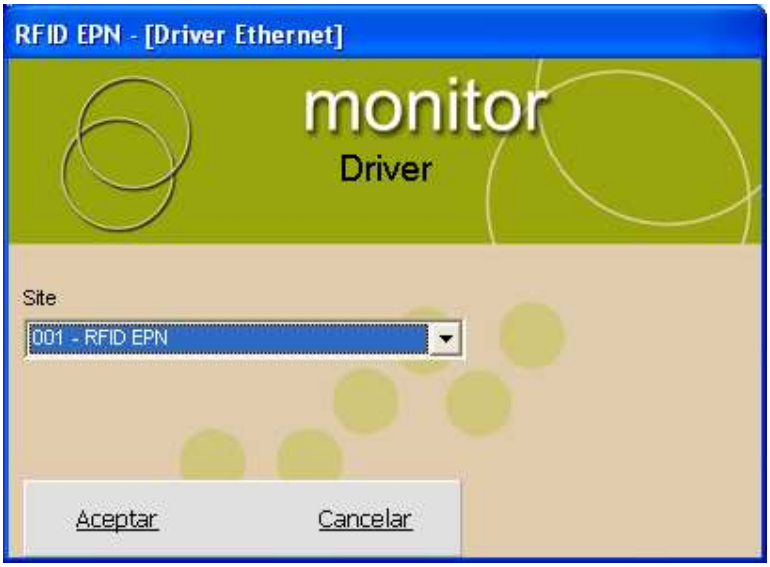
- Configuración de parámetros IP: Revisar que los parámetros IP estén configurados tal como se muestra en la tabla de direccionamiento.

Cargar software de accesos

El software de accesos este formado por siguientes módulos:

- Software recolector de datos (Driver)
- Software de la Terminal RFID

Software recolector de datos (Driver).- Ejecutar el Driver desde el escritorio de Windows.

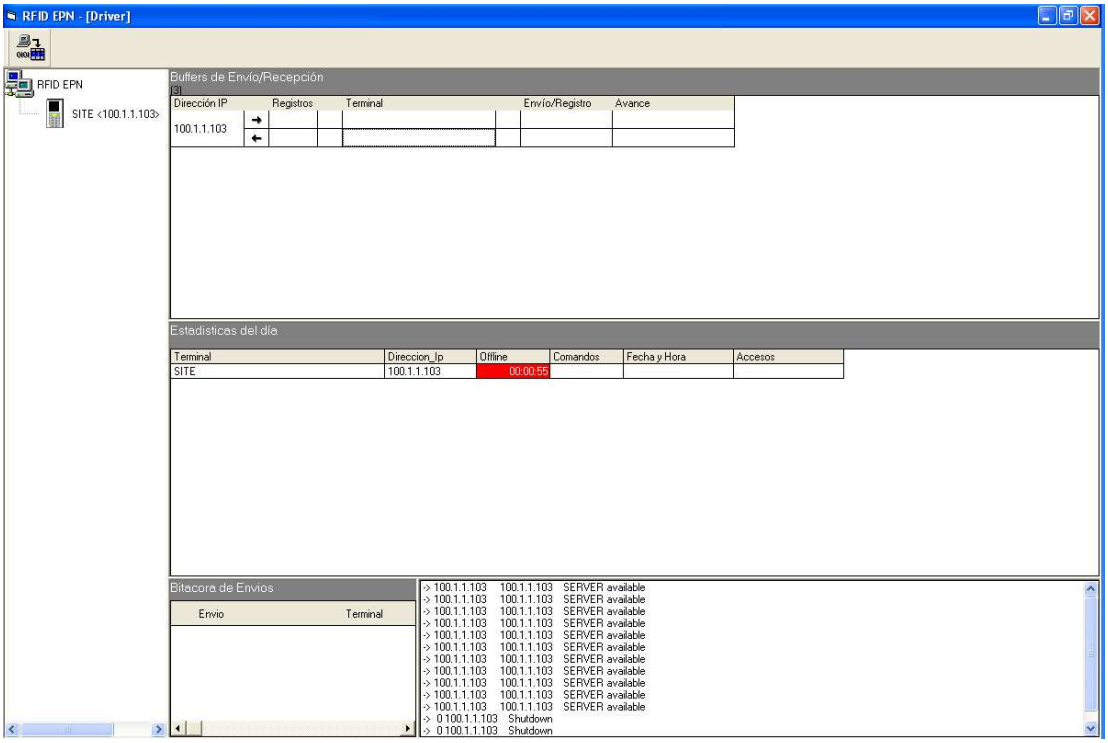


Recolector de datos (Driver)

Damos clic en Aceptar y la aplicación procede a realizar las conexiones con las dos bases de datos del sistema:

- accesos_db.mdb
- res_110208_XOCH.mdb

Una vez que se haya cargado el driver tenemos ya la interfaz de usuario:

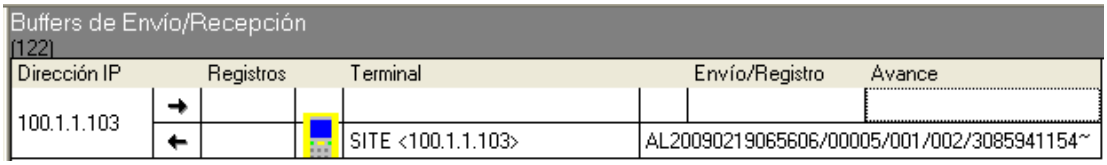


Interfaz de usuario del Driver

En la figura anterior podemos apreciar 4 bloques de operación de la aplicación:

- Site: es la lectora RFID con su respectiva dirección IP

- Buffers de Envío/Recepción: En esta parte se muestran los paquetes de envío y recepción de la lectora por medio del driver. Se tienen los siguientes campos:



Buffers de Envío/Recepción del Driver

  - Dirección IP: Es la dirección IP de la lectora RFID
  - Registros-Terminal: Se muestra si la dirección IP a la que se realiza el proceso de envío/recepción de la información.

- Envío/Registro: Se muestra el tipo de registro que se envía este puede ser: Fecha-Hora, configuración y accesos.

- Avance: Muestra una barra de progreso indicando el avance del envío de la información.

- Estadísticas del día: En esta parte se muestran las estadísticas de envío de información, tenemos los siguientes campos:

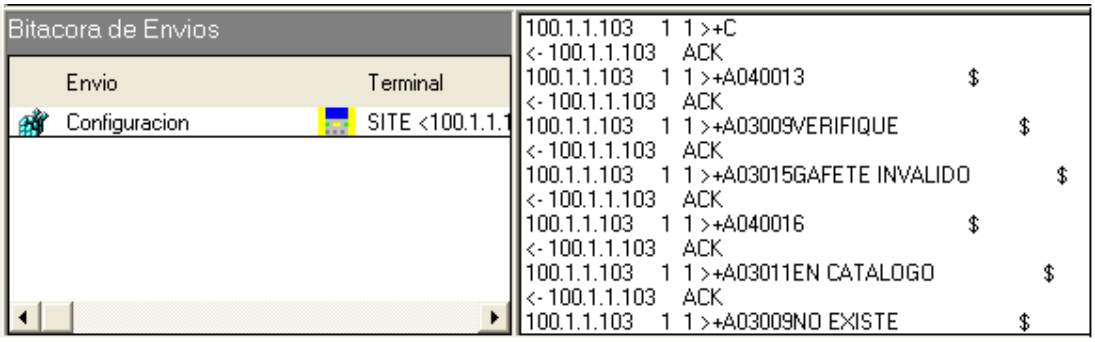
Estadisticas del día

Terminal	Direccion_Ip	Offline	Comandos	Fecha y Hora	Accesos
SITE	100.1.1.103			19/02/2009 06:59:05	19/02/2009 06:59:37

Estadísticas del día

- Terminal: Alias de la Terminal RFID
- Dirección IP: Es la dirección IP de lectora sobre la cual se muestran las estadísticas.
- Offline: Muestra si la lectora esta o no en línea si la Terminal está fuera de línea se pintará este cuadro de color rojo y además se indicara el tiempo está dicha lectora fuera de línea.
- Fecha y Hora: Se almacena la fecha y la hora a la cual se inició el envío de configuraciones a la lectora
- Accesos: Se almacena la fecha y hora a la cual se realizó el envío del registro de accesos a la lectora.

- Bitácora de envíos: En esta parte se muestran todos los envíos de información que se realizan a la lectora, además se muestra el proceso de comunicación entre la lectora y el driver al momento de enviar cada paquete



Bitácora de envíos

Software de la Terminal RFID.-

Para operar el software de la Terminal se ejecuta el acceso directo que existe en el escritorio de la Terminal una vez realizado esto la aplicación carga las librerías que permiten activar a la tarjeta lectora la misma que se encuentra conectada a la Termina LanPoint Mobile por medio el interfaz COMPACT FLASH una vez que se abra la aplicación la tarjeta lectora empezará a emitir una luz intermitente la misma que indica que el dispositivo está listo para operar.

En la siguiente figura se muestra la interfaz de operación de la Terminal, en dicha interfaz se tiene la fecha y hora, la cual esta sincronizada con la fecha del servidor.

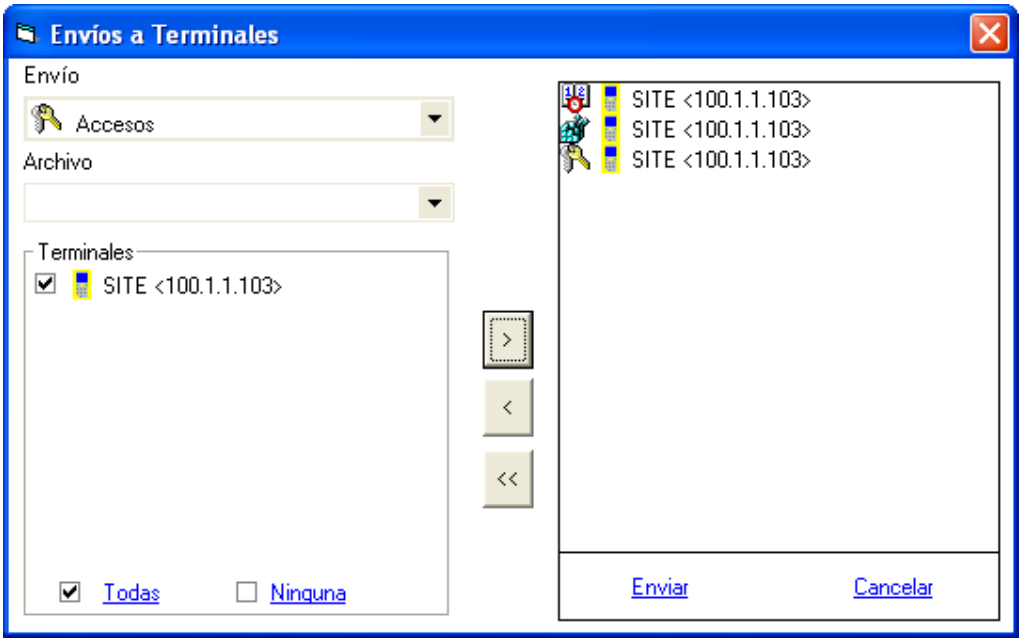
Software de la controladora RFID

Envío de configuración a la lectora (Terminal)

Para realizar el envío se da clic sobre el icono de envíos  . Luego se presenta la pantalla para seleccionar los envíos a la Terminal.

Los envíos que se realizan son los siguientes:

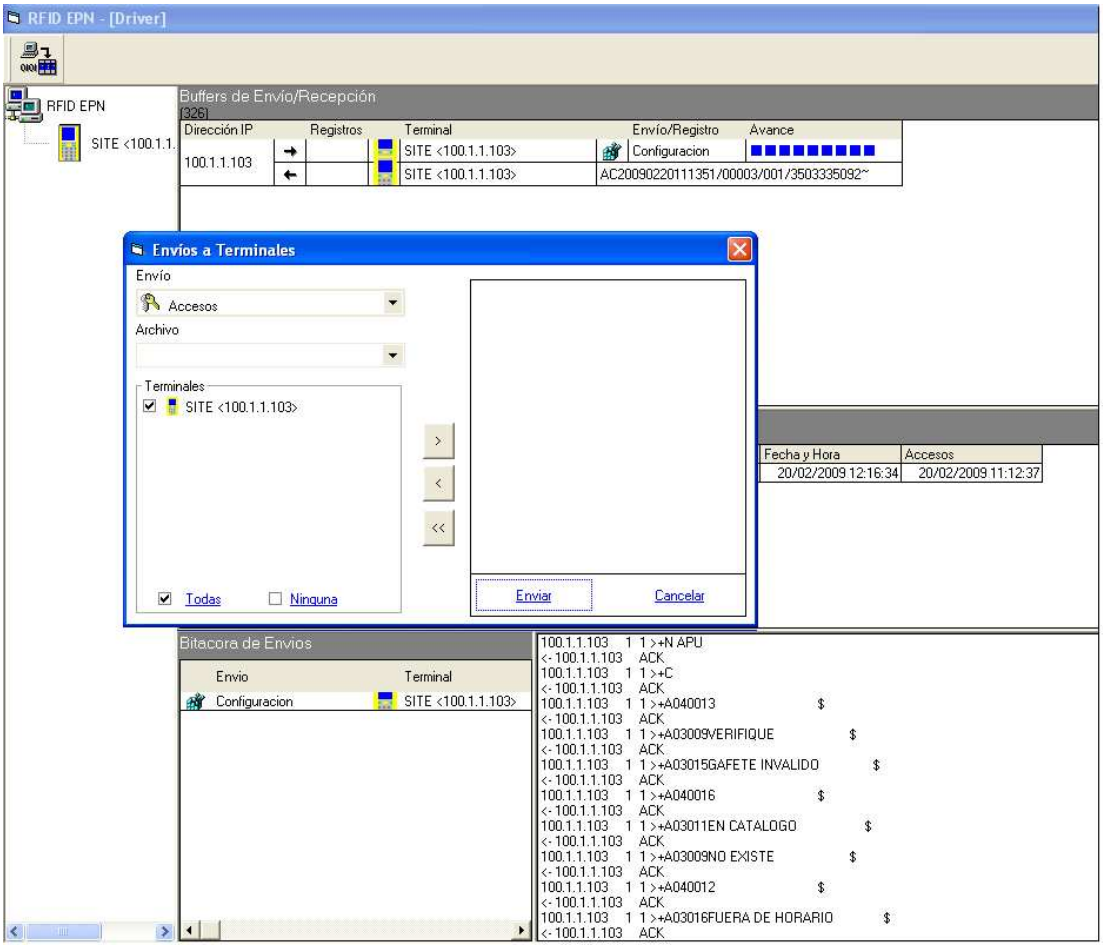
- Fecha y Hora: Se envía la fecha y hora del servidor a la Terminal para que ésta se sincronice con el servidor.
- Configuración: Se envía la configuración de los mensajes que se muestran en la Terminal, el tipo de lector, el indicador de conectividad, etc.
- Accesos: Se envía a la Terminal la información de los usuarios VIP, los códigos de identificación de cada credencial y los respectivos horarios de acceso.



Programación de envíos

Para seleccionar los envíos escogemos la Terminal a la cual deseamos enviar las configuraciones, para este caso escogemos la única que está disponible (SITE<100.1.1.103>) y seleccionamos el envío correspondiente damos clic en el botón  y agregamos el envío, repetimos el mismo proceso la el resto de envíos. Una vez que estén agregados los envíos correspondientes se procede a enviar la configuración a las terminales presionando el botón **Enviar**.

La siguiente figura muestra la interface de usuario al momento que está procesando el envío de configuraciones a la Terminal. Una vez que se termine el envío la sección de Bitácora de Envíos quedará totalmente vacía lo que implica que todas las configuraciones se realizaron con éxito.



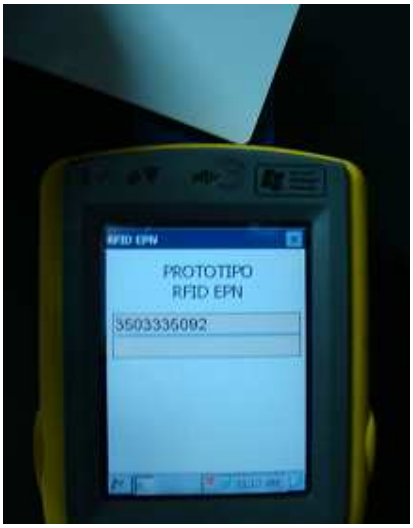
Proceso de envío de configuraciones

Revisar la sincronización de Fecha y Hora

Al finalizar el envío la Terminal debe automáticamente sincronizar su fecha y hora con la del servidor en caso de que esto no suceda se procede nuevamente a realizar el envío de la Fecha y Hora siguiendo los mismos pasos que se mencionó en la sección anterior.

Inicio de lectura de las credenciales.

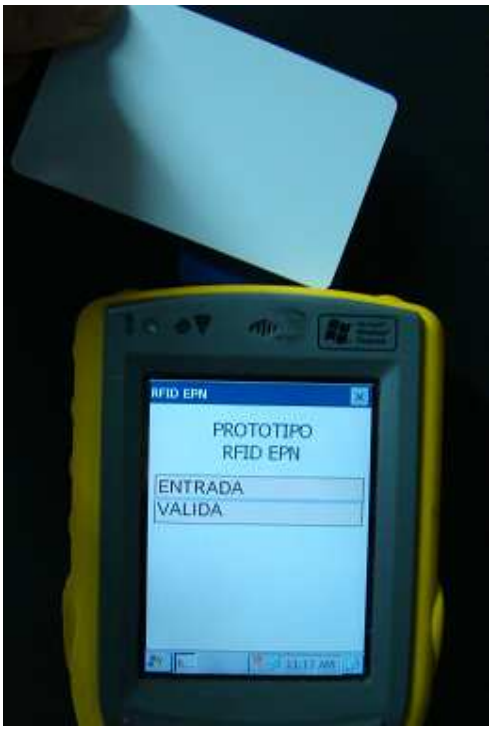
La lectura se la realiza aproximando la credencial RFID a la lectora a una distancia aproximada de 2 cm. Al momento que se efectúe satisfactoriamente la lectura, el software de la Terminal indicará primero el número de la credencial



Lectura de la credencial

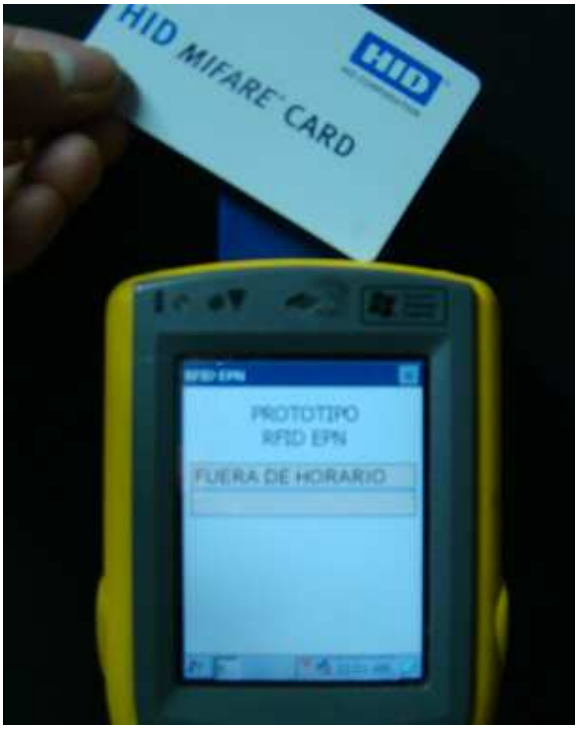
Y seguidamente el resultado de acceso, los posibles resultados de acceso para una lectura son:

ENTRADA VALIDA: Indica que el usuario está permitido a ingresar



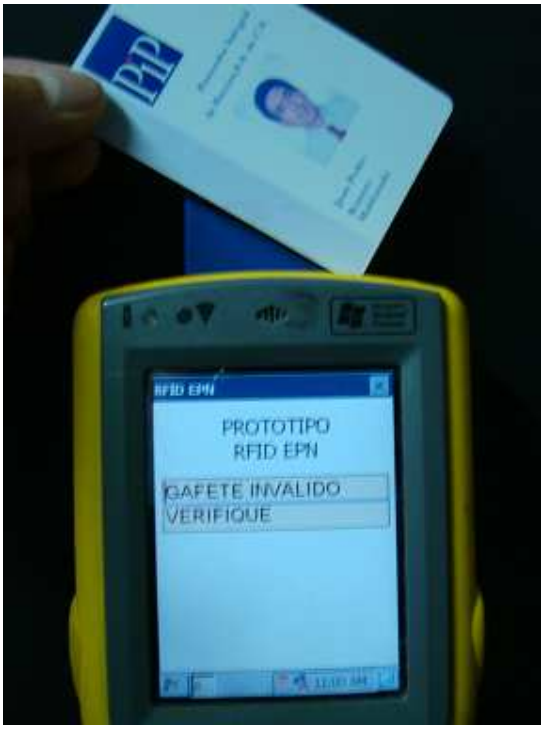
Credencial Válida

FUERA DE HORARIO: Indica que el usuario está intentando acceder en un horario no permitido.



Credencial fuera de horario

GAFETE INVALIDO VERIFIQUE: Indica que dicha credencial corresponde a un usuario no permitido o que esta dado de baja en el sistema.



Credencial Inválida

Cada lectura que se efectué en la Terminal será enviada por medio de la interface de red inalámbrica de la Terminal hacia el Driver que se encuentra instalado en el servidor.

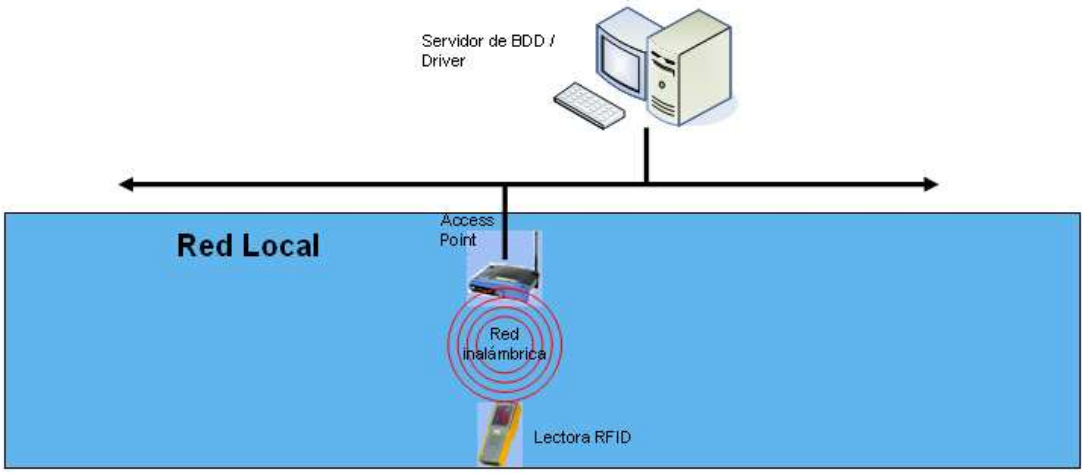
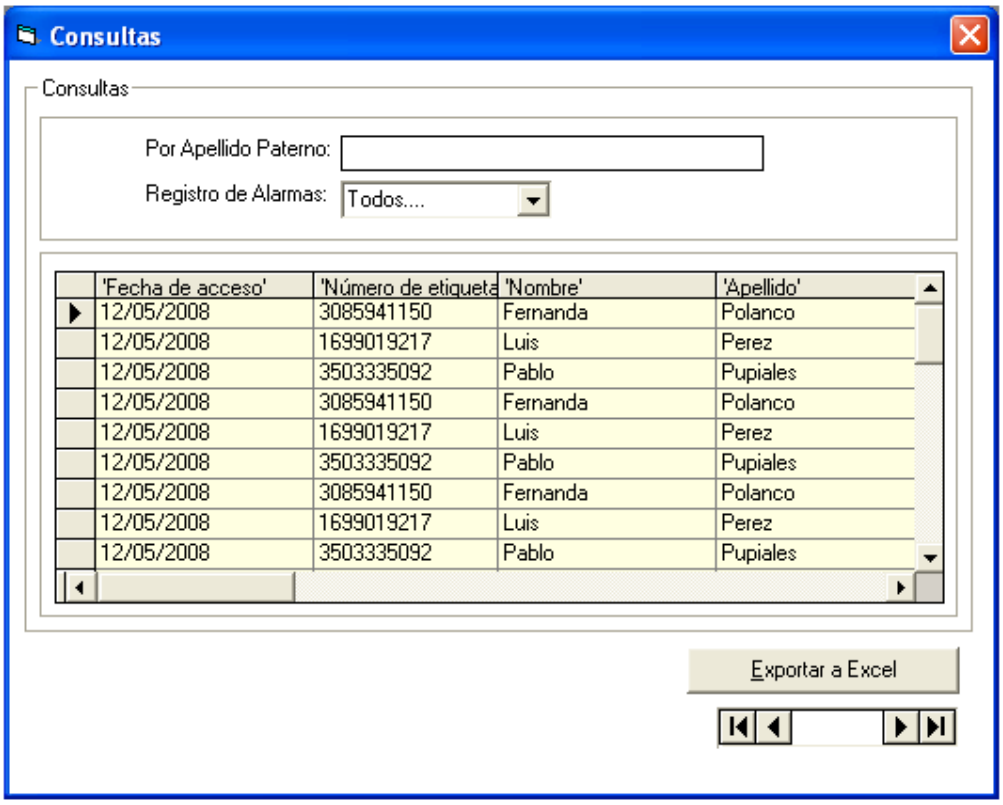


Diagrama de conexión de la Red de accesos

Generar reporte de accesos

Una vez finalizado el control de accesos se procede a generar un reporte en Excel de accesos, para esto se utiliza en el sistema de registro de usuarios el catálogo de consultas, este reporte muestra todos los usuarios que ingresaron al inmueble con el respectivo seguimiento de fecha y hora de acceso.

Para generar el reporte de accesos nos dirigimos al catalogo de **consultas->consultas de accesos**



Consultas de accesos

Luego se procede a exportar estos datos a una hoja de Excel dando clic en botón **Exportar a Excel**

Entrega de reportes al cliente

Una vez que se tenga generado el reporte de accesos en Excel, se procede a la entrega respectiva de esta información al organizador tanto en impreso como en un archivo de datos.

De esta manera se concluye con la demostración total del funcionamiento del prototipo y de todas sus etapas por las que atraviesa su funcionamiento.

ANEXO G

CÓDIGO FUENTE

INGRESO AL SISTEMA

```
Private Sub btnCancelar_Click()
End
End Sub

Private Sub btnIngresar_Click()
Dim consulta As String
If txtUsuario.Text <> "" And txtcontraseña.Text <> "" Then
   consulta = "Select * from ADMIN where LOGIN_USU = '" + txtUsuario.Text + "' and
CLAVE_USU = '" + txtcontraseña.Text + "'"
   adcIngreso.RecordSource = consulta
   adcIngreso.Refresh
   If adcIngreso.Recordset.RecordCount > 0 Then
      perfil = adcIngreso.Recordset.Fields("PERFIL_USU").Value
      mdiMenu.Show
      Unload Me
   Else
      MsgBox "Usuario o Contraseña incorrectos", vbCritical, "Error"
      txtUsuario.SetFocus
      txtcontraseña.Text = ""
   End If
Else
   MsgBox "Ingrese todos los campos correctamente", vbCritical, "Error"
   txtUsuario.SetFocus
End If
End Sub

Private Sub txtcontraseña_KeyPress(KeyAscii As Integer)
If KeyAscii = 13 Then
   btnIngresar_Click
End If
End Sub
```

MENU PRINCIPAL DEL SISTEMA

```
Private Sub MDIForm_Load()
If perfil <> "Administrador" Then
   mnuUsuarios.Enabled = False
   mnuAdmin.Enabled = False
End If
End Sub
```

```
Private Sub mnuAS_Click()
frmInUsuAd.Show
Me.Enabled = False
End Sub

Private Sub mnuAU_Click()
frmListaUsuarios.Show
Me.Enabled = False
End Sub

Private Sub mnuBorrado_Click()
frmClaveBorrado.Show
Me.Enabled = False
End Sub

Private Sub mnuCI_Click()
frmConsultas.Show
Me.Enabled = False
End Sub

Private Sub mnuEnd_Click()
End
End Sub

Private Sub mnuinevento_Click()
nuevo = False
frmEventos.Show
Me.Enabled = False
End Sub
```

CREACION DE EVENTOS

```
Dim fso As Object
 Dim id_evento As String

Private Sub adcEventos_MoveComplete(ByVal adReason As
ADODB.EventReasonEnum, ByVal pError As ADODB.Error, adStatus As
ADODB.EventStatusEnum, ByVal pRecordset As ADODB.Recordset)
If Not adcEventos.EOFAction = adStayEOF Then
   If adcEventos.Recordset.AbsolutePosition > 0 Then
      lbltotal.Caption = adcEventos.Recordset.AbsolutePosition
   End If
End If

If adcEventos.Recordset.EOF = False And adcEventos.Recordset.BOF = False And nuevo
= False Then
   If adcEventos.Recordset.AbsolutePosition > 0 Then
      If IsNull(adcEventos.Recordset.Fields("NOMBRE_EVENTO").Value) Then
```

```
            txtNombre.Text = ""
        Else
            txtNombre.Text = adcEventos.Recordset.Fields("NOMBRE_EVENTO").Value
        End If
        If IsNull(adcEventos.Recordset.Fields("LUGAR").Value) Then
            txtLugar.Text = ""
        Else
            txtLugar.Text = adcEventos.Recordset.Fields("LUGAR").Value
        End If
        If IsNull(adcEventos.Recordset.Fields("FECHA").Value) Then
            'dtpFecha.Value = ""
        Else
            dtpFecha.Value = adcEventos.Recordset.Fields("FECHA").Value
        End If
        If IsNull(adcEventos.Recordset.Fields("HORA").Value) Then
            'dtpHora.Value = ""
        Else
            dtpHora.Value = adcEventos.Recordset.Fields("HORA").Value
        End If
 'Instanciar el objeto FSO para poder _
  usar las funciones FileExists y FolderExists
 Set fso = CreateObject("Scripting.FileSystemObject")
 ' Comprobar archivo
    If IsNull(adcEventos.Recordset.Fields("IMAGEN").Value) Then
         ptbFoto.Picture = Nothing
    Else
        If fso.FileExists(adcEventos.Recordset.Fields("IMAGEN").Value) Then
        ptbFoto.Picture = LoadPicture(adcEventos.Recordset.Fields("IMAGEN").Value)
        Else
            ptbFoto.Picture = Nothing
        End If
        Set fso = Nothing
    End If

    End If
End If

End Sub

Private Sub btImagen_Click()
CommonDialog1.Filter = "Archivos de imágenes (*.bmp; *.jpg; *.gif; *.tiff; *.png) |
*.bmp;*.jpg;*.gif;*.tiff;*.png"
  CommonDialog1.DialogTitle = " Seleccionar imagen para Guardar"
    CommonDialog1.ShowOpen
    If CommonDialog1.FileName = "" Then Exit Sub
    ptbFoto.Picture = LoadPicture(CommonDialog1.FileName)

End Sub
```

```
Private Sub txtcontraseña2_Change(Index As Integer)

End Sub

Private Sub btnactualizar_Click()
If txtNombre.Text <> "" And txtLugar.Text <> "" Then
   adcEventos.Recordset.Fields("NOMBRE_EVENTO").Value = txtNombre.Text
   adcEventos.Recordset.Fields("LUGAR").Value = txtLugar.Text
   adcEventos.Recordset.Fields("FECHA").Value = dtpFecha.Value
   adcEventos.Recordset.Fields("HORA").Value = dtpHora.Value
   If CommonDialog1.FileName <> "" Then
   adcEventos.Recordset.Fields("IMAGEN").Value = CommonDialog1.FileName
   End If
   adcEventos.Recordset.Update
   CommonDialog1.FileName = ""
   nuevo = False
   lbltotal.Caption = adcEventos.Recordset.RecordCount
   btnnuevo.Enabled = True
   btnactualizar.Caption = "&Actualizar"
   btnsalir.Caption = "&Salir"
   MsgBox "Evento Ingresado Exitosamente", vbOKOnly, "Requerimientos"
   adcUsuarios.RecordSource = "Select * from CATPER where ID_EVENTO=" &
adcEventos.Recordset.Fields(0).Value
   adcUsuarios.Refresh
   If adcUsuarios.Recordset.RecordCount > 0 Then
      Do While Not adcUsuarios.Recordset.EOF
      adcUsuarios.Recordset.Fields("IMAGEN_EVENTO").Value =
adcEventos.Recordset.Fields("IMAGEN").Value
      adcUsuarios.Recordset.MoveNext
      Loop
   End If
Else
   MsgBox "Ingrese todos los campos correctamente", vbCritical, "Error"
   txtLogin.SetFocus
End If

End Sub

Private Sub btnEliminar_Click()
If MsgBox("Desea Eliminar el registro actual??", vbYesNo, "Sistema de manejo de
Clientes") = vbYes Then
   adcEventos.Recordset.Delete
   adcEventos.Refresh
   adcEventos.RecordSource = "Select * from EVENTOS"
   adcEventos.Refresh
   nuevo = False
End If

End Sub
```

```
Private Sub borrar_textos()
   txtNombre.Text = ""
   txtLugar.Text = ""
   ptbFoto.Picture = Nothing
End Sub
Private Sub btnnuevo_Click()
   adcEventos.RecordSource = "Select * from EVENTOS"
   adcEventos.Refresh
   adcEventos.Recordset.AddNew
   nuevo = True
   borrar_textos
   txtNombre.SetFocus
   btnsalir.Caption = "&Cancelar"
   btnactualizar.Caption = "&Guardar"
   btnnuevo.Enabled = False
End Sub

Private Sub btnsalir_Click()
nuevo = False
adcEventos.Recordset.Cancel
adcEventos.Refresh
If btnsalir.Caption = "&Cancelar" Then
   btnsalir.Caption = "&Salir"
   btnactualizar.Caption = "&Actualizar"
   btnnuevo.Enabled = True
Else
   mdiMenu.Enabled = True
   mdiMenu.SetFocus
   Unload Me
End If
End Sub

Private Sub Form_Load()
   adcEventos.RecordSource = "Select * from EVENTOS"
   adcEventos.Refresh
   dtpFecha.Value = Format(Date, "Short Date")
End Sub

Private Sub Form_Unload(Cancel As Integer)
btnsalir_Click
End Sub
```

ADMINISTRACION DE USUARIOS VIP

```
Private Sub btExcel_Click()
 Call Exportar_DbGrid_Excel("Hoja1", adcUsuarios)
End Sub
```

```
Private Sub btnEliminar_Click()
If adcUsuarios.Recordset.RecordCount > 0 Then
   If MsgBox("Desea Eliminar el registro actual??", vbYesNo, "Sistema de manejo de
Clientes") = vbYes Then
      adcUsuarios.Recordset.Delete
      adcUsuarios.Refresh
      adcUsuarios.Recordset.Update
      adcUsuarios.RecordSource = "Select CLA_PER, NOM_PER as 'Nombre', PAT_PER
as 'Apellido Paterno', MAT_PER as 'Apellido Materno', STA_PER as 'Estatus',
NOM_EVENTO AS 'Nombre del Evento', FECHA_EVENTO as 'Fecha del
evento',TAG_PER as 'Num_Credencial', HOI_ACC as 'Inicio de Acceso', HOF_ACC as
'Fin de Acceso' from CATPER order by NOM_PER"
      adcUsuarios.Refresh
      dtgdatos.Columns(0).Visible = False
   End If
Else
  MsgBox "No hya registros para eliminar", vbCritical, "Error"
End If
End Sub

Private Sub btNuevo_Click()
op = 1
frmUsuarios.Show
Me.Enabled = False
End Sub

Private Sub dtgdatos_DblClick()
id_usuario = adcUsuarios.Recordset.Fields("CLA_PER").Value
op = 2
frmUsuarios.Show
Me.Enabled = False

End Sub

Private Sub Form_Load()
dtgdatos.Columns(0).Visible = False
End Sub

Private Sub Form_Unload(Cancel As Integer)
mdiMenu.Enabled = True
End Sub

Private Sub mnuexphistorial_Click()
adcUsuarios.RecordSource = "Select * from CATPER"
adcUsuarios.Refresh
If adcUsuarios.Recordset.RecordCount <= 0 Then Exit Sub
adcUsuarios.Recordset.MoveFirst
adcUsuarios1.RecordSource = "Select * from HIST_CATPER"
adcUsuarios1.Refresh
```

```
Do While Not adcUsuarios.Recordset.EOF
   adcUsuarios1.Recordset.AddNew
   adcUsuarios1.Recordset.Fields("PAT_PER").Value =
adcUsuarios.Recordset.Fields("PAT_PER").Value
   adcUsuarios1.Recordset.Fields("NOM_PER").Value =
adcUsuarios.Recordset.Fields("NOM_PER").Value
   adcUsuarios1.Recordset.Fields("MAT_PER").Value =
adcUsuarios.Recordset.Fields("MAT_PER").Value
   adcUsuarios1.Recordset.Fields("NOM_EVENTO").Value =
adcUsuarios.Recordset.Fields("NOM_EVENTO").Value
   adcUsuarios1.Recordset.Fields("FECHA_EVENTO").Value =
adcUsuarios.Recordset.Fields("FECHA_EVENTO").Value
   adcUsuarios1.Recordset.Fields("TIPO_ACCESO").Value =
adcUsuarios.Recordset.Fields("TIPO_ACCESO").Value
   adcUsuarios1.Recordset.Fields("STA_PER").Value =
adcUsuarios.Recordset.Fields("STA_PER").Value
   adcUsuarios1.Recordset.Fields("TAG_RAC").Value =
adcUsuarios.Recordset.Fields("TAG_PER").Value
   adcUsuarios1.Recordset.Fields("HOI_ACC").Value =
adcUsuarios.Recordset.Fields("HOI_ACC").Value
   adcUsuarios1.Recordset.Fields("HOF_ACC").Value =
adcUsuarios.Recordset.Fields("HOF_ACC").Value
   adcUsuarios1.Recordset.Fields("IMAGEN").Value =
adcUsuarios.Recordset.Fields("IMAGEN").Value
   adcUsuarios1.Recordset.Fields("IMAGEN_EVENTO").Value =
adcUsuarios.Recordset.Fields("IMAGEN_EVENTO").Value
   adcUsuarios1.Recordset.Update
   adcUsuarios.Recordset.MoveNext
Loop

adcUsuarios.RecordSource = "Select * from CATPER"
adcUsuarios.Refresh
adcUsuarios.Recordset.MoveFirst
Do While Not adcUsuarios.Recordset.EOF
   adcUsuarios.Recordset.Delete
   adcUsuarios.Recordset.MoveNext
Loop
adcUsuarios.RecordSource = "Select CLA_PER, NOM_PER as 'Nombre', PAT_PER as
'Apellido Paterno', MAT_PER as 'Apellido Materno', STA_PER as 'Estatus', TAG_PER as
'Num_Credencial', HOI_ACC as 'Inicio de Acceso', HOF_ACC as 'Fin de Acceso' from
CATPER"
adcUsuarios.Refresh
dtgdatos.Columns(0).Visible = False
frmListaUsuarios.adcUsuarios.Refresh
End Sub

Private Sub mnuimportardehistorial_Click()
frmImportar_Historial.Show
Me.Enabled = False
```

```
End Sub

Private Sub txtUsuario_Change()
adcUsuarios.RecordSource = "Select CLA_PER, NOM_PER as 'Nombre', PAT_PER as
'Apellido Paterno', MAT_PER as 'Apellido Materno', STA_PER as 'Estatus',
NOM_EVENTO AS 'Nombre del Evento', FECHA_EVENTO as 'Fecha del
evento',TAG_PER as 'Num_Credencial', HOI_ACC as 'Inicio de Acceso', HOF_ACC as
'Fin de Acceso' from CATPER where PAT_PER like '%" + txtUsuario.Text + "%' order by
NOM_PER"
adcUsuarios.Refresh
dtgdatos.Columns(0).Visible = False
End Sub
```

CREACION DE USUARIOS

```
Dim de As DataEnvironment1
Dim id_evento As Integer
Dim imagen_evento As String
Private Sub btImagen_Click()
CommonDialog1.Filter = "Archivos de imágenes (*.bmp; *.jpg; *.gif; *.tiff; *.png) |
*.bmp;*.jpg;*.gif;*.tiff;*.png"
  CommonDialog1.DialogTitle = " Seleccionar imagen para Guardar"
    CommonDialog1.ShowOpen
    If CommonDialog1.FileName = "" Then Exit Sub
    ptbFoto.Picture = LoadPicture(CommonDialog1.FileName)
End Sub

Private Sub btImprimir_Click()
Set de = New DataEnvironment1
Call de.Imprimir_Grouping(id_usuario)
With DataReport1
Set .Sections.Item("Imprimir_Detail").Controls("Image2").Picture = ptbFoto.Picture
Set .Sections.Item("Imprimir_Grouping_Header").Controls("logoevento").Picture =
ptbEvento.Picture
End With
DataReport1.Show
End Sub

Private Sub btnCancelar_Click()
adcUsuarios.Recordset.Cancel
adcUsuarios.Refresh
If btnCancelar.Caption = "&Cancelar" Then
   btnCancelar.Caption = "&Salir"
End If
frmListaUsuarios.Enabled = True
frmListaUsuarios.Show
Unload Me
```

```
frmListaUsuarios.adcUsuarios.Refresh
frmListaUsuarios.dtgdatos.Columns(0).Visible = False
End Sub

Private Sub btnGuardar_Click()
If txtPaterno.Text <> "" And txtMaterno.Text <> "" And txtNombres.Text <> "" And
cbEvento.Text <> "" And txtFEvento.Text <> "" And cbEstatus.Text <> "" And
txtNumCredencial.Text <> "" And txtInicial.Text <> "" And txtFinal.Text <> "" Then
   If op = 1 Then
   adcUsuarios2.RecordSource = "Select * from CATPER where TAG_PER='" +
txtNumCredencial.Text + "'"
   adcUsuarios2.Refresh
   If adcUsuarios2.Recordset.RecordCount > 0 Then
      MsgBox "El numero de credencial ya existe"
   Else
      adcUsuarios.Recordset.Fields("PAT_PER").Value = txtPaterno.Text
      adcUsuarios.Recordset.Fields("NOM_PER").Value = txtNombres.Text
      adcUsuarios.Recordset.Fields("MAT_PER").Value = txtMaterno.Text
      adcUsuarios.Recordset.Fields("NOM_EVENTO").Value = cbEvento.Text
      adcUsuarios.Recordset.Fields("FECHA_EVENTO").Value = txtFEvento.Text
      adcUsuarios.Recordset.Fields("STA_PER").Value = cbEstatus.Text
      adcUsuarios.Recordset.Fields("TAG_PER").Value = txtNumCredencial.Text
      adcUsuarios.Recordset.Fields("HOI_ACC").Value = txtInicial.Text
      adcUsuarios.Recordset.Fields("HOF_ACC").Value = txtFinal.Text
      If CommonDialog1.FileName <> "" Then
      adcUsuarios.Recordset.Fields("IMAGEN").Value = CommonDialog1.FileName
      Else
         If adcUsuarios.Recordset.Fields("IMAGEN").Value = "" Then
            adcUsuarios.Recordset.Fields("IMAGEN").Value = ""
         End If
      End If
      adcUsuarios.Recordset.Fields("ID_EVENTO").Value = id_evento
      adcUsuarios.Recordset.Fields("IMAGEN_EVENTO").Value = imagen_evento
      adcUsuarios.Recordset.Update
      MsgBox "Usuario Ingresado exitosamente", vbInformation, "Ingreso de Usuarios"
      id_usuario = adcUsuarios.Recordset.Fields(0).Value
      btnCancelar.Caption = "&Salir"
      btImprimir.Visible = True
      frmListaUsuarios.adcUsuarios.Refresh
      frmListaUsuarios.dtgdatos.Columns(0).Visible = False
   End If
   Else
      adcUsuarios.Recordset.Fields("PAT_PER").Value = txtPaterno.Text
      adcUsuarios.Recordset.Fields("NOM_PER").Value = txtNombres.Text
      adcUsuarios.Recordset.Fields("MAT_PER").Value = txtMaterno.Text
      adcUsuarios.Recordset.Fields("NOM_EVENTO").Value = cbEvento.Text
      adcUsuarios.Recordset.Fields("FECHA_EVENTO").Value = txtFEvento.Text
      adcUsuarios.Recordset.Fields("STA_PER").Value = cbEstatus.Text
      adcUsuarios.Recordset.Fields("TAG_PER").Value = txtNumCredencial.Text
```

```
        adcUsuarios.Recordset.Fields("HOI_ACC").Value = txtInicial.Text
        adcUsuarios.Recordset.Fields("HOF_ACC").Value = txtFinal.Text
        If CommonDialog1.FileName <> "" Then
        adcUsuarios.Recordset.Fields("IMAGEN").Value = CommonDialog1.FileName
        Else
           If adcUsuarios.Recordset.Fields("IMAGEN").Value = "" Then
              adcUsuarios.Recordset.Fields("IMAGEN").Value = ""
           End If
        End If
        If id_evento <> 0 Then
           If adcUsuarios.Recordset.Fields("ID_EVENTO").Value <> "" Then
              If adcUsuarios.Recordset.Fields("ID_EVENTO").Value <> id_evento Then
              adcUsuarios.Recordset.Fields("ID_EVENTO").Value = id_evento
              End If
           End If
        End If
        If imagen_evento <> "" Then
           If adcUsuarios.Recordset.Fields("IMAGEN_EVENTO").Value <> "" Then
              If adcUsuarios.Recordset.Fields("IMAGEN_EVENTO").Value <>
imagen_evento Then
                 adcUsuarios.Recordset.Fields("IMAGEN_EVENTO").Value =
imagen_evento
              End If
           Else
              adcUsuarios.Recordset.Fields("IMAGEN_EVENTO").Value = imagen_evento
           End If
        End If
        adcUsuarios.Recordset.Update
        MsgBox "Información Actualizada", vbInformation, "Usuarios"
        id_usuario = adcUsuarios.Recordset.Fields(0).Value
        btnCancelar.Caption = "&Salir"
        btImprimir.Visible = True
        frmListaUsuarios.adcUsuarios.Refresh
        frmListaUsuarios.dtgdatos.Columns(0).Visible = False
     End If
Else
     MsgBox "Ingrese todos los campos correctamente", vbCritical, "Error"
     txtNombres.SetFocus
End If
End Sub

Public Function KeyPressNum(KeyAscii As Integer) As Boolean
     KeyPressNum = True
     Select Case KeyAscii
        Case vbKeyDelete, vbKeyBack
        Case 40 To 57
        Case 13
        Case Else
           KeyPressNum = False
```

```
   End Select
End Function

Private Sub cbEvento_Click()
adcEventos.RecordSource = "Select * from Eventos where NOMBRE_EVENTO='" +
cbEvento.Text + "'"
adcEventos.Refresh
id_evento = adcEventos.Recordset.Fields(0).Value
txtFEvento.Text = adcEventos.Recordset.Fields("FECHA").Value
imagen_evento = adcEventos.Recordset.Fields("IMAGEN").Value
Set fso1 = CreateObject("Scripting.FileSystemObject")
' Comprobar archivo

If fso1.FileExists(adcEventos.Recordset.Fields("IMAGEN").Value) Then
ptbEvento.Picture = LoadPicture(adcEventos.Recordset.Fields("IMAGEN").Value)
End If
Set fso1 = Nothing


End Sub

Private Sub Form_Load()
adcEventos.RecordSource = "Select * from Eventos"
adcEventos.Refresh
cbEvento.Clear

Do While Not adcEventos.Recordset.EOF
   cbEvento.AddItem (adcEventos.Recordset.Fields("NOMBRE_EVENTO").Value)
   adcEventos.Recordset.MoveNext
Loop

If op = 1 Then
   adcUsuarios.Recordset.AddNew
   btnCancelar.Caption = "&Cancelar"
   btnGuardar.Caption = "&Guardar"
   btImprimir.Visible = False
End If
If op = 2 Then
   adcUsuarios.RecordSource = "select * from CATPER where CLA_PER=" + id_usuario
   adcUsuarios.Refresh
    Dim fso, fso1 As Object
    'Instanciar el objeto FSO para poder _
     usar las funciones FileExists y FolderExists
    Set fso = CreateObject("Scripting.FileSystemObject")
    ' Comprobar archivo
    If fso.FileExists(adcUsuarios.Recordset.Fields("IMAGEN").Value) Then
    ptbFoto.Picture = LoadPicture(adcUsuarios.Recordset.Fields("IMAGEN").Value)
    Else
      MsgBox "No se encuentra el archivo de imagen", vbCritical, "Error"
```

```
    End If
    Set fso = Nothing
    'Instanciar el objeto FSO para poder _
     usar las funciones FileExists y FolderExists
    Set fso1 = CreateObject("Scripting.FileSystemObject")
    ' Comprobar archivo

    If fso1.FileExists(adcUsuarios.Recordset.Fields("IMAGEN_EVENTO").Value) Then
    ptbEvento.Picture =
LoadPicture(adcUsuarios.Recordset.Fields("IMAGEN_EVENTO").Value)
    End If
    Set fso1 = Nothing


    'dtpFEvento.Value = adcUsuarios.Recordset.Fields("FECHA_EVENTO").Value
   ' cbEvento.Text = adcUsuarios.Recordset.Fields("NOMBRE_EVENTO").Value
End If
End Sub

Private Sub Form_Unload(Cancel As Integer)
frmListaUsuarios.Enabled = True
Unload Me
End Sub

Private Sub mnuRegistros_Click()
frmConsultas.Show
Me.Enabled = False
End Sub

Private Sub txtClave_KeyPress(KeyAscii As Integer)
If KeyPressNum(KeyAscii) = False Then
      KeyAscii = 0
End If

End Sub

Private Sub txtFinal_KeyPress(KeyAscii As Integer)
If KeyPressNum(KeyAscii) = False Then
      KeyAscii = 0
End If
End Sub

Private Sub txtInicial_Change()
If txtInicial.Text <> "" Then
   If txtInicial.Text > 24 Then
      MsgBox "El intervalo ingresado no es valido, ingrese un número del 0 al 24",
vbInformation, "Error"
   End If
End If
```

```
End Sub

Private Sub txtInicial_KeyPress(KeyAscii As Integer)
If KeyPressNum(KeyAscii) = False Then
      KeyAscii = 0
End If
End Sub

Private Sub txtNumCredencial_KeyPress(KeyAscii As Integer)
If KeyPressNum(KeyAscii) = False Then
      KeyAscii = 0
End If
End Sub
```

ADMINISTRACION DE PERFILES DEL SISTEMA

```
'Private Sub adcUsuarios_MoveComplete(ByVal adReason As
ADODB.EventReasonEnum, ByVal pError As ADODB.Error, adStatus As
ADODB.EventStatusEnum, ByVal pRecordset As ADODB.Recordset)
'If Not adcUsuarios.EOFAction = adStayEOF Then
'    If adcUsuarios.Recordset.AbsolutePosition > 0 Then
'       lbltotal.Caption = adcUsuarios.Recordset.AbsolutePosition
'    End If
'End If
'End Sub

Private Sub btnactualizar_Click()
If txtLogin.Text <> "" And txtContraseña1.Text <> "" And txtContraseña2.Text <> "" And
cmbPerfil.Text <> "" Then
      If txtContraseña1.Text <> txtContraseña2.Text Then
         MsgBox "Los campos de la contraseña no coinciden", vbCritical, "Error"
         txtContraseña1.SetFocus

      Else
         adcUsuarios.Recordset.Fields("LOGIN_USU").Value = txtLogin.Text
         adcUsuarios.Recordset.Fields("CLAVE_USU").Value = txtContraseña1.Text
         adcUsuarios.Recordset.Fields("PERFIL_USU").Value = cmbPerfil.Text
         adcUsuarios.Recordset.Update
         lbltotal.Caption = adcUsuarios.Recordset.RecordCount
         btnnuevo.Enabled = True
         btnactualizar.Caption = "&Actualizar"
         btnsalir.Caption = "&Salir"
         MsgBox "Usuario Ingresado Exitosamente", vbOKOnly, "Requerimientos"
      End If
   Else
      MsgBox "Ingrese todos los campos correctamente", vbCritical, "Error"
      txtLogin.SetFocus
End If
```

```
End Sub

Private Sub btnEliminar_Click()
If MsgBox("Desea Eliminar el registro actual??", vbYesNo, "Sistema de manejo de
Clientes") = vbYes Then
   adcUsuarios.Recordset.Delete
   adcUsuarios.Refresh
   adcUsuarios.RecordSource = "Select * from ADMIN"
   adcUsuarios.Refresh
End If
End Sub

Private Sub btnnuevo_Click()
   adcUsuarios.RecordSource = "Select * from ADMIN"
   adcUsuarios.Refresh
   adcUsuarios.Recordset.AddNew
   txtLogin.SetFocus
   btnsalir.Caption = "&Cancelar"
   btnactualizar.Caption = "&Guardar"
   btnnuevo.Enabled = False
End Sub

Private Sub btnsalir_Click()
adcUsuarios.Recordset.Cancel
adcUsuarios.Refresh
If btnsalir.Caption = "&Cancelar" Then
   btnsalir.Caption = "&Salir"
   btnactualizar.Caption = "&Actualizar"
   btnnuevo.Enabled = True
Else
   mdiMenu.Enabled = True
   mdiMenu.SetFocus
   Unload Me
End If
End Sub


Private Sub Form_Unload(Cancel As Integer)
btnsalir_Click
End Sub
```

CONSULTAS DE ACCESOS

```
Public clave_borrado, clave As String

Private Sub btActualizar_Click()

adcConsulta.RecordSource = "Select FEC_RAC as 'Fecha de acceso',CATPER.TAG_PER
as 'Número de etiqueta', NOM_PER as 'Nombre',PAT_PER as 'Apellido',NOM_EVENTO
```

```
as 'Evento' from CATPER,REGACC where CATPER.TAG_PER=REGACC.TAG_RAC
order by FEC_RAC"
adcConsulta.Refresh
cbRegistro.Text = "Todos...."
End Sub

Private Sub btBorrar_Click()
If MsgBox("Desea Eliminar los registros del REGISTRO DE ACCESO??", vbYesNo,
"Sistema de manejo de Clientes") = vbYes Then
   Me.Enabled = False
   frmClave.Show
End If
End Sub
Public Sub borrar_registros()
   If clave_borrado = clave Then
      adcRegAcc.RecordSource = "Select * from REGACC"
      adcRegAcc.Refresh
      adcRegAcc.Recordset.MoveFirst
      Do While Not adcRegAcc.Recordset.EOF
         adcRegAcc.Recordset.Delete
         If Not adcRegAcc.Recordset.EOF Then
            adcRegAcc.Recordset.MoveNext
         End If
      Loop
      dtgdatos.Refresh
      MsgBox "Registros borrados exitosamente", vbInformation, "Sistema de manejo de
Clientes"
   Else
      MsgBox "Contraseña Incorrecta", vbCritical, "Sistema de manejo de Clientes"
   End If
End Sub


Private Sub btnExportar_Click()
 Call Exportar_DbGrid_Excel("Hoja1", adcConsulta)
End Sub

Private Sub cbRegistro_Click()
Select Case cbRegistro.Text
Case "Acceso Normal"
   adcConsulta.RecordSource = "Select FEC_RAC as 'Fecha de
acceso',CATPER.TAG_PER as 'Número de etiqueta', NOM_PER as 'Nombre',PAT_PER
as 'Apellido', NOM_EVENTO as 'Evento' from CATPER,REGACC where STA_RAC =1
and CATPER.TAG_PER=REGACC.TAG_RAC order by FEC_RAC"
Case "Fuera de Horario"
   adcConsulta.RecordSource = "Select FEC_RAC as 'Fecha de
acceso',CATPER.TAG_PER as 'Número de etiqueta', NOM_PER as 'Nombre',PAT_PER
as 'Apellido',NOM_EVENTO as 'Evento' from CATPER,REGACC where STA_RAC =2
and CATPER.TAG_PER=REGACC.TAG_RAC order by FEC_RAC"
```

```
Case "No existe credencial"
   adcConsulta.RecordSource = "Select FEC_RAC as 'Fecha de
acceso',CATPER.TAG_PER as 'Número de etiqueta', NOM_PER as 'Nombre',PAT_PER
as 'Apellido',NOM_EVENTO as 'Evento' from CATPER,REGACC where STA_RAC =3
and CATPER.TAG_PER=REGACC.TAG_RAC order by FEC_RAC"
Case Else
   adcConsulta.RecordSource = "Select FEC_RAC as 'Fecha de
acceso',CATPER.TAG_PER as 'Número de etiqueta', NOM_PER as 'Nombre',PAT_PER
as 'Apellido',NOM_EVENTO as 'Evento' from CATPER,REGACC where
CATPER.TAG_PER=REGACC.TAG_RAC order by FEC_RAC"
End Select
adcConsulta.Refresh
dtgdatos.Refresh
End Sub


Private Sub Form_Load()
adcBorrado.RecordSource = "Select * from BORRADO"
adcBorrado.Refresh
clave_borrado = adcBorrado.Recordset.Fields("CLAVE_BORRADO").Value
End Sub

Private Sub Form_Unload(Cancel As Integer)
mdiMenu.Enabled = True
Unload Me
End Sub

Private Sub txtUsuario_Change()
adcConsulta.RecordSource = "Select FEC_RAC as 'Fecha de acceso',CATPER.TAG_PER
as 'Número de etiqueta', NOM_PER as 'Nombre',PAT_PER as 'Apellido',NOM_EVENTO
as 'Evento' from CATPER,REGACC where PER_RAC=CLA_PER and PAT_PER like
'%" + txtUsuario.Text + "%'"

adcConsulta.Refresh
dtgdatos.Refresh
End Sub
```

CREACION DE CLAVE DE BORRADO PARA ACCESOS

```
Private Sub adcBorrado_WillMove(ByVal adReason As ADODB.EventReasonEnum,
adStatus As ADODB.EventStatusEnum, ByVal pRecordset As ADODB.Recordset)
If adcBorrado.Recordset.EOF = False And adcBorrado.Recordset.BOF = False Then
   If adcBorrado.Recordset.AbsolutePosition > 0 Then
      If IsNull(adcBorrado.Recordset.Fields("CLAVE_BORRADO").Value) Then
         txtContraseña1.Text = ""
      Else
         txtContraseña1.Text =
adcBorrado.Recordset.Fields("CLAVE_BORRADO").Value
      End If
```

```
   End If
End If
End Sub

Private Sub btnAceptar_Click()
If txtContraseña1.Text <> "" And txtContraseña2.Text <> "" Then
   If txtContraseña1.Text = txtContraseña2.Text Then
      adcBorrado.Recordset.Fields("CLAVE_BORRADO").Value = txtContraseña1.Text
      adcBorrado.Recordset.Update
      MsgBox "Contraseña almacenada exitosamente", vbOKOnly, "Información"
      btnCancelar_Click
   Else
      MsgBox "Las contraseñas no coinciden", vbCritical, "Error"
      txtContraseña1.SetFocus
   End If
Else
      MsgBox "Ingrese los datos correctamente", vbCritical, "Error"
      txtContraseña1.SetFocus
End If
End Sub

Private Sub btnCancelar_Click()
mdiMenu.Enabled = True
Unload Me
End Sub

Private Sub Form_Load()
adcBorrado.RecordSource = "select * from BORRADO"
adcBorrado.Refresh
If adcBorrado.Recordset.RecordCount <= 0 Then
   adcBorrado.Recordset.AddNew
End If
End Sub

Private Sub Form_Unload(Cancel As Integer)
btnCancelar_Click
End Sub
```