Diseño y construcción de un sistema de procesamiento de datos compatible con la tecnología Z-Wave y acoplable a una cerradura biométrica.

Hernán Guillermo Osorio Quevedo.

Universidad de San Buenaventura

Facultad de Ingeniería
Ingeniería Mecatrónica
Bogotá DC
2008.

Diseño y construcción de un sistema de procesamiento de datos compatible con la tecnología Z-Wave y acoplable a una cerradura biométrica.

Hernán Guillermo Osorio Quevedo.

Proyecto de grado para optar por el titulo de ingeniero mecatrónico.

Universidad de San Buenaventura
Facultad de Ingeniería
Ingeniería Mecatrónica
Bogotá DC
2008.

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá D.C., 23 de Junio de 2008

Agradecimientos.

Quiero agradecer a mis padres y a mi hermano Andrés Felipe por todo el apoyo que me brindaron, ya que al salir del colegio ellos y yo sabíamos que no tenía las bases necesarias para ser ingeniero, debido a mis precarios conocimientos de las ciencias básicas necesarias. Sin embargo ellos siempre me apoyaron en este largo y difícil camino. Les debo todos mis logros a ellos. Gracias familia por siempre estar a mi lado.

TABLA DE CONTENIDO

1. INTRODUCCION 1

2. PLANTEAMIENTO DEL PROBLEMA
2.1 Antecedentes 4
2.2 Descripción y formulación del problema 5

3. JUSTIFICACION 7
3.1 Objetivo General 7
3.2 Objetivos Específicos 8
3.3 Alcances 8
3.4 Limitaciones 8

4. MARCO DE REFERENCIA
4.1 Marco Conceptual 9
4.2 Conceptos Generales de la biometría
11
4.3 Modalidades Biométricas
17
4.3.1 Reconocimiento de Huella Digital
17
4.3.2 Formato para guardar la imagen del dedo
18

5. MARCO TEORICO
5.1 Biometría
23
5.1.2 Funcionamiento y rendimiento
24
5.1.3 Procesos de Autenticación e Identificación biométrica
27
5.2 Cuestiones y Preocupaciones
27
5.2.1 Elementos importantes en una instalación de domótica
28
5.2.2 Bus de Instalación Europeo (EIB o EIBus)
28

5.2.3 Protocolo X10
29
5.2.4 Protocolo ZigBee
30
5.2.5 Características del Sistema
30
5.2.6 OSGI
30
5.2.7 Universal Plug and Play (UPnP)
31
5.2.8 Patrón básico de UPnP
31
5.2.9 Que beneficios tiene
32
5.3 Asociaciones
32

6. MARCO LEGAL O NORMATIVO

6.1 Jurisprudencia Colombiana en Radio Frecuencia, bandas de uso libre
34
6.2 Jurisprudencia Colombiana para biometría
34
6.2.1 Leyes
34
6.2.2 Código Penal colombiano
35
6.2.3 Seguridad Privada
35

7. METODOLOGIA

7.1 Enfoque de la investigación
37
7.2 Línea de investigación de USB/SUB-línea de facultad/ Campo temático del programa
37
7.3 Técnicas de recolección de información
37
7.4 Hipótesis
38
7.4.1 Variables independientes
38
7.4.2 Variables dependientes
38

8. PRESENTACION Y ANALISIS DE RESULTADOS

8.1 Estadísticas
39
8.2 Aplicación
40
8.2.1 Usuario #1
41
8.2.2 Usuario #2
41

9. DESARROLLO INGENIERIL
42
9.1 Análisis de la aplicación
43
9.2 Diseño propuesto para esta aplicación
43
9.2.1 GUI de interface Principal
51
9.2.2 Visualización de paquetes en formato RAW
52
9.2.3 Visualización de paquetes decodificados
53
9.3 Diagrama de flujo, programa principal
54
9.4 Diagrama de flujo, librería Serial
55
9.5 Diagrama de flujo, Emulador del Driver
56
9.6 Proceso de fabricación
63

10. CONCLUSIONES
69

11. RECOMENDACIONES
70

12. BIBLIOGRAFIA
71

13. ANEXOS
72

1. INTRODUCCIÓN

Existe una gran variedad de tecnologías que han sido desarrolladas para el control del hogar, mejor conocido como domótica. El término domótica es la unión de la palabra domus (la cual en latín significa casa) y robótica (robota que significa en esclavo en checo)[1]. Se entiende por domótica, un conjunto de sistemas capaces de automatizar una vivienda, aportando servicios de gestión de consumo energético, seguridad, confort y bienestar. Estos pueden ser integrados por redes externas o internas de comunicaciones, cableadas o inalámbricas. El control de estos sistemas esta situado en partes claves del hogar, tanto en el interior como en el exterior. La domótica se puede expresar como la integración de la tecnología con el diseño, de un recinto de vivienda o comercial.

En los principios, la domótica contaba con sistemas muy sencillos como temporizadores de luces o riego de los jardines. Sólo era posible tener acceso a sistemas de seguridad vía telefónica, y no llevaban a cabo ningún tipo de tarea automática. Esta tecnología ha venido evolucionando con el paso del tiempo. El siguiente avance, que fue logrado en este campo, fue el cableado estructurado.

A través del tiempo la tecnología avanza, es algo que es inevitable. De esta forma, los avances en la tecnología, utilizada en la domótica, dan pasos agigantados. Después del cableado estructurado, siguió la comunicación por corriente portadora, y actualmente ha llegado a su forma inalámbrica, por radio frecuencia o de forma digital, como el bluetooth o las redes inalámbricas de Internet.

Una gran parte de la domótica está enfocada en la seguridad del hogar, que a su vez se enfoca en gran parte en sistemas de alarma. Los sistemas de alarma constan de controles de acceso mediante tarjetas magnéticas, las cuales activan un mecanismo de electro imán, el cual libera una puerta y otorga el acceso al recinto. Aparte de este tipo de tecnología, existen diferentes tipos de cerraduras, que son más tecnológicas y seguras que la de llave convencional. Existen las cerraduras de seguridad con una llave especial, la cual no es fácilmente reproducida; y de igual manera existen las puertas de seguridad o blindadas, que siguen siendo un sistema de seguridad arcaico pero con algo de practicidad.

[1] Diccionario Esencial de la Real Academia de la Lengua Española. (2001). Segunda Edición. España: Espasa.

Las cerraduras que cuentan con mayor tecnología, son las que son una combinación de una cerradura mecánica con sistemas electrónicos de control y de seguridad. Existen las cerraduras con teclado numérico. El principio del funcionamiento de las cerraduras con teclado numérico, es la de introducción de una clave para obtener el acceso al recinto, algunas de estas están combinadas con el uso de una clave y una llave para mayor seguridad; sin embargo, pueden convertirse en un artilugio poco práctico.

Después de estas fueron desarrolladas las cerraduras a control remoto; existen dos tipos de estas cerraduras, las que funcionan mediante códigos infrarrojos o por radio frecuencia. La ventaja de estos sistemas de cerradura es que no es necesaria una llave para obtener acceso al recinto. Sólo es necesario tener el control remoto, y este da la ventaja de poder abrir la cerradura a una mayor distancia. Sin embargo las desventajas de este sistema son, que las distancias de funcionamiento son algo limitadas, y podría llegar a ser peligroso abrir la cerradura por error o a una larga distancia sin saber que podría pasar.

Con el pasar del tiempo, y con ayuda de la ciencia ficción, fue desarrollado el sistema de cerraduras y control de acceso mediante la biometría. Esta consiste en documentar y almacenar una característica física de las personas, de tal manera que solo esa persona o las autorizadas puedan obtener acceso al recinto. Esta solución aumenta el nivel de seguridad, ya que los rasgos biométricos de las personas no pueden ser duplicados, lo cual soluciona el problema de llaves perdidas, duplicación de las mismas o en caso de una cerradura mas tecnológica, el traspaso de la calve de acceso o la perdida del control remoto.

Mediante este proyecto se diseñó y se construyó un sistema de procesamiento de datos compatible con la tecnología Z-Wave, ésta siendo un estándar para la automatización de los hogares (domótica), la cual es 100% inalámbrica y con comunicación por radio frecuencia. Este sistema de procesamiento de datos fue acoplado a una cerradura biométrica, con el fin de ofrecer una solución de control de acceso y seguridad, combinada con una solución de domótica. En resumen lo que se logró fue un sistema que facilita y brinda comodidad al usuario, a través de la fusión de la cerradura y el acceso que ésta brinda a un mejor uso de la domótica.

Al lograr una fusión exitosa entre estas dos tecnologías, será posible brindar un mayor nivel de seguridad, ya que la cerradura podrá ser activada desde un control remoto de forma individual o a su vez podrá ser parte de un escenario preprogramado en el sistema de domótica, esto siendo su funcionamiento normal desde el interior del recinto para brindar una mayor comodidad y seguridad al usuario. El funcionamiento de esta cerradura desde el exterior será muy similar, ya que se tendrá acceso al sistema mediante una huella dactilar y el sistema de procesamiento de datos acoplado a esta cerradura emitirá las señales pertinentes para encender un escenario.

Está presupuestado que la cerradura pueda accionar diferentes escenarios, dependiendo de la huella que accione el mecanismo. De esta forma se brinda la posibilidad al usuario de tener un sistema más personalizado, y contar con la opción de encender diferentes dispositivos del recinto a los cuales esa persona esta mas propensa a utilizar, recién ingrese al mismo. De la misma forma está presupuestado que el sistema tenga un reloj interno, el cual lleva la hora del día; de esta forma se pueden programar diferentes escenarios o eventos, para la misma huella dactilar dependiendo de la hora del día, ya que lo más normal es que el comportamiento de una persona sea totalmente diferente, ya sea que la persona entra a trabajar en la mañana o ingresa a su hogar en las horas de la noche.

2. PLANTEAMIENTO DEL PROBLEMA

2.1 Antecedentes:

La biometría no se puso en practica en la cultura occidental hasta el siglo XIX pero era utilizada en china el siglo XV, cuando los mercaderes chinos lograban una impresión en tinta de las palmas de la mano de los niños con los que trabajaban para poder distinguirlos de forma más adecuada. No fue documentado el uso de la biometría en la sociedad occidental sino hasta el año 1883. Este caso particular de biometría fue creado por el jefe de fotografía de la policía francesa. Este método consiste en documentar rasgos faciales de diferentes criminales para poder identificarlos con mayor facilidad, y de igual manera tomar mediadas del rostro de la persona, de tal forma que puede ser identificado de forma fotográfica, este método también es conocido como *Bertillonage*. Al encontrarse con diferentes problemas en el método, especialmente con las medidas del rostro, la policía occidental empezó a utilizar el sistema de huella dactilar como un método más efectivo de identificación[2]. Actualmente, los sistemas de biometría son utilizados para lograr una forma de identificación, seguridad y muchas más aplicaciones.

El funcionamiento de la biometría está basado primordialmente en las características físicas de un individuo, las cuales pueden ser procesadas por un algoritmo numérico. El resultado de este es almacenado en una base de datos, de esta forma cuando otra persona intenta identificarse y los datos no concuerdan con los almacenados en la memoria, el sistema no le otorgara acceso.

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

Las huellas dactilares, las retinas, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, representan ejemplos de características físicas (estáticas), mientras que entre los ejemplos de características de comportamiento se incluye la firma, el paso y el tecleo (dinámicas). La voz se considera una mezcla de características físicas y de comportamiento, pero todos los rasgos biométricos comparten aspectos físicos y de comportamiento[3].

Los diferentes tipos de cerraduras de seguridad que utilizan sistemas biométricos son de gran variedad. En este caso en específico se utilizará una cerradura de seguridad fabricada por ADEL SECURITY LOCKS. Esta cerradura en especial tiene la capacidad de almacenar hasta 120 huellas dactilares, compuesta por : un

[2] Jain, Anil K., & Flynn, Patrick. Handbook of Biometrics. (2007). Primera edición. Michigan State University, EE.UU.: Springer.
[3] Ibid.

teclado numérico el cual va desde el numero 0 (cero) hasta el numero 3 (tres), y también es posible abrir la cerradura con una llave de seguridad la cual sólo puede ser fabricada por la persona que tenga en su poder el código de fabricación. Esta cerradura en particular tiene una tasa de falsa aceptación de .000001 por cada 100 intentos, lo cual la hace prácticamente inviolable. La tasa de falso rechazo es de 1 por cada 100 intentos haciendo de esta una cerradura bastante confiable. La resolución del sensor es de 5000DPI, con un ángulo de captura de 360 grados. Al combinar esta cerradura con la domótica, las posibilidades de controlar el hogar son incalculables.

Existen una gran variedad de sistemas de procesamiento de datos de la tecnología Z-wave y su uso en la domótica, ya que prácticamente cada una de las empresas que conforman la alianza tiene en el mercado un sistema de control. Ya sea un control remoto, control por computador, control por Internet o por teléfono. Cada uno de estos controles varia en la cantidad de equipos que pueden almacenar en su memoria y la cantidad de canales diferentes que pueden controlar para crear escenarios o manipular equipos de forma individual. Sin embargo, no existe en el mercado un sistema de procesamiento de datos que pueda ser utilizado con un sistema de cerradura biométrica. Los diferentes sistemas de procesamiento de datos controladores de esta tecnología, en cuanto a control de acceso se refiere, están basados en las tarjetas magnéticas mediante las cuales se activa un mecanismo de un electro imán el cual libera la puerta que está asegurando. Este sistema es ampliamente visto en puertas de oficinas para controlar el ingreso y egreso de personal, y a su vez es usado en las puertas eléctricas de los conjuntos residenciales. Hasta el momento no existe documentación sobre un sistema biométrico incorporado con la tecnología Z-Wave.

2.2 Descripción y formulación del problema

Colombia es un país con una larga historia de violencia, enmarcados en esta situación, el robo de los hogares puede ser clasificado como un tipo de esta. Es cierto que existen diferentes tipos de tecnología para prevenir estas eventualidades. No obstante no son perfectas o son de un alto valor comercial, como lo son las puertas de seguridad o blindadas, sistemas de alarma y monitoreo, vidrios blindados o un equipo personal de seguridad. En nuestro país son muy pocas las personas que pueden pagar por este tipo de artilugio de seguridad, ya que el mercado de estos está enfocado al estrato seis[4].

A través de este proyecto se quiere involucrar un sistema de seguridad muy sencillo, mediante la domótica y una cerradura de seguridad biométrica. La cerradura biométrica no es una cerradura de alto valor comercial, pero si es una cerradura que brinda un alto nivel de seguridad. Esta tiene sistemas de seguridad

[4] Según estadísticas publicadas por el DANE en 2007.

para bloquearse cuando es violentada, y a su vez no otorga acceso a menos de que su huella dactilar esté en la memoria.

Combinando esta cerradura biométrica con un sistema de procesamiento de datos de la tecnología Z-wave, sería posible incrementar la seguridad del recinto ya que a través de esta sería posible encender diferentes artefactos incluyendo la iluminación, equipos eléctricos, sistemas de alarma, etc., con tan solo abrir la puerta del recinto con su huella dactilar. Todo esto podría llegar a tener un valor comercial que la mayoría de los colombianos podrían adquirir, de tal forma que lograran hacer de sus lugares de trabajo u hogares, sitios más seguros, cómodos y eficientes para sus labores cotidianas.

3. Justificación

En el año 2006 más de cuarenta mil viviendas en Bogotá fueron ultrajadas y saqueadas en su totalidad (Datos tomados de estadísticas del DANE). Es imprescindible que la tecnología avance en cuanto a seguridad, ya que es necesario poder brindar sistemas de seguridad a un bajo costo y de alta confiabilidad, lo que ayudaría a reducir las alarmantes cifras que siguen creciendo todos los años en cuanto a robos de vivienda se refiera.

Si es posible diseñar un sistema de procesamiento de datos de la tecnología Z-wave, el cual funciona en conjunto con una cerradura biométrica de huella dactilar, sería posible incrementar la seguridad del recinto en varios niveles y de igual manera aumentar la comodidad y la eficiencia del lugar.

En primera instancia una cerradura biométrica de huella dactilar incrementa la seguridad, ya que no es posible violarla con una llave maestra u otras herramientas de cerrajería, lo cual dificultaría un acceso no permitido. De igual forma si es violentada, ésta se bloquea para que no otorgue el acceso a personal indeseado, y no otorga acceso a personas que no tengan su huella dactilar en la memoria del sistema.

Si a este sistema se le agrega un sistema de procesamiento de datos compatible con la tecnología Z-wave, la cerradura podría llevar a cabo diferentes actividades pre-programadas, como encender las luces y cerrar las cortinas a una hora predeterminada; y a su vez este sistema de cerradura al ser activada mediante una huella digital, la cual esta almacenada en la base de datos, la cerradura podrá llevar a cabo una secuencia de comandos para facilitar el ingreso al hogar encendiendo o apagando luces, abriendo o cerrando cortinas, encendiendo o apagando aplicaciones, etc. De esta forma, se incrementa la seguridad ya que mediante este sistema seria posible simular presencia en el recinto, y cuando se ingresa a este, nunca entraría con las luces apagadas o sin los equipos electrónicos de seguridad apagados. Así se incrementa la seguridad de forma sustancial, y a un bajo costo.

3.1 Objetivo General

Diseñar y construir un sistema de procesamiento de datos, compatible con la tecnología Z-Wave que es acoplable a una cerradura biométrica.

3.2 Objetivos Específicos:

1. Diseñar un sistema de procesamiento de datos, compatible con la tecnología Z-Wave y sistema de acople con una cerradura biométrica de huella dactilar.
2. Construir un sistema de procesamiento de datos, compatible con la tecnología Z-Wave y su acople con una cerradura biométrica de huella dactilar.
3. Realizar pruebas que permitan sintonizar y afinar el sistema.

3.3 Alcances:

Este proyecto tiene una variedad de alcances importantes. El control automático de diferentes aplicaciones del hogar como luces, cortinas, cafeteras, etc. Mejora la calidad y el estilo de vida de los propietarios de la vivienda, y a su vez la hace más segura, aumentado el nivel de seguridad en la puerta principal de su hogar. Mediante el uso de una cerradura biométrica el nivel de seguridad es incrementado sustancialmente, ya que una huella dactilar es imposible de falsificar.

3.4 Limitaciones:

La única limitación de este proyecto es bastante clara. El protocolo de comunicaciones entre los dispositivos Z-Wave no es un protocolo abierto o avalado por la IEEE[5]. El protocolo de comunicación es propio y privado para los dispositivos, esto es una gran limitación ya que la mayor parte del proyecto estará dedicada a la investigación de dicho protocolo. Entre otras limitaciones que se puedan presentar, se contemplan los materiales de construcción, ya que es posible que sean de difícil adquisición en nuestro país.

[5] Institute of Electrical and Electronics Engineers.

4. MARCO DE REFERENCIA

4.1 Marco Conceptual:

Después de una exhaustiva investigación sobre los diferentes tipos de tecnología utilizadas en la domótica, se llegó a la conclusión de que la tecnología Z-Wave es la más apropiada debido a sus características. Una característica muy importante de esta tecnología es que no es solamente una tecnología, es una alianza de fabricantes de más de ciento cincuenta empresas que desarrollan esta tecnología. Estas empresas fabrican interruptores para: control de iluminación, termostatos, controles de aplicaciones eléctricas, cualquier tipo de sistema de cortinas, sistemas de seguridad, instrumentación para piscinas y spas, motores para puertas eléctricas, sistemas de teatros en casa, entre otros. Z-Wave no es sólo una tecnología de automatización, es también una tecnología de energía verde, ya que está enfocada al mínimo consumo de electricidad y ayuda a controlar el consumo del hogar o lugar de trabajo, ya que los tiempos de encendido de los artefactos eléctricos se pueden programar, al igual que el tiempo de encendido de las luces y su intensidad.

Las especificaciones de radio frecuencia de esta tecnología, la hacen perfecta para nuestra sociedad. La tecnología Z-wave está compuesta por un ancho de banda de 9600 bits/s o 40 Kbits/s con un 100% de interoperabilidad entre la tecnología y sus diferentes fabricantes. El tipo de modulación es GFSK con un rango aproximado de 30 metros de alcance entre nodos. Esta tecnología trabaja en el rango de los 900 MHz ISM; para ser más exactos trabaja en 908.42 MHz.

En Europa la banda de 868 MHz tiene un limitación en el ciclo de trabajo de un 1%, en la banda internacional de 908.42 no tiene esta limitación. De igual forma los diferentes artefactos fabricados para la banda internacional están regidos por la norma de fabricación norte americana, lo cual implica que tiene que regirse a sus limitaciones. La limitación impuesta por la norma Norte Americana es basada en la potencia de trasmisión ya que esta limitada por 1mW a lo opuesto de la norma Europea la cual es de 25mW. De esta forma los diferentes equipos de la tecnología Z-Wave pueden estar en modo de descanso la mayoría del tiempo y trasmitir la información o llevar a cabo su función solo un 0.1% del tiempo, lo cual los hace muy efectivos para el consumo eléctrico.

La topología de este sistema está basada en una red de acoplamiento de dos vías, lo que quiere decir que cada nodo pude ser un emisor y receptor a la misma vez, ya que no existe un nodo maestro dentro de la red. Este sistema de topología y enrutamiento inteligente son muy útiles ya que si se requiere mandar un mensaje del punto **A** al punto **B** y estos no se encuentran en la distancia requerida para la comunicación, entra a jugar en el sistema un nodo **C**, permitiendo que los mensajes de comunicación no tengan que ir de forma directa de un punto a otro,

ya que estos pueden saltar de nodo en nodo para lograr una comunicación eficiente y sin limitaciones de distancia. En caso de que la ruta ideal para la comunicación este bloqueada, el sistema encontrará un ruta aleatoria para lograr la comunicación. Debido a la naturaleza de la red de acoplamiento de dos vías, entre mas aplicaciones de la tecnología Z-Wave existan, la red será más estable y los mensajes siempre podrán llegar a su destino ya que el número de rutas se incrementa. La red tiene una capacidad de sostener hasta 232 diferentes aplicativos de esta tecnología, no obstante esta red puede ser puenteada con otra existente y aumentar el número de dispositivos de una forma ilimitada.

Como fue mencionado previamente, el funcionamiento de la comunicación de este sistema es por radio frecuencia y está diseñada bajo los parámetros de GFKS por sus siglas en inglés, la modulación por desplazamiento de frecuencia gausiana (**Gaussian Frequency Shift Keying** o **GFSK),** es un tipo de modulación donde un uno lógico es representado por una desviación positiva, esto quiere decir en forma de incremento de la frecuencia de onda portadora, y un cero mediante una desviación negativa de la misma.

Figura 1. Desplazamiento GFSK (Gaussian Frequency Shift Keying).

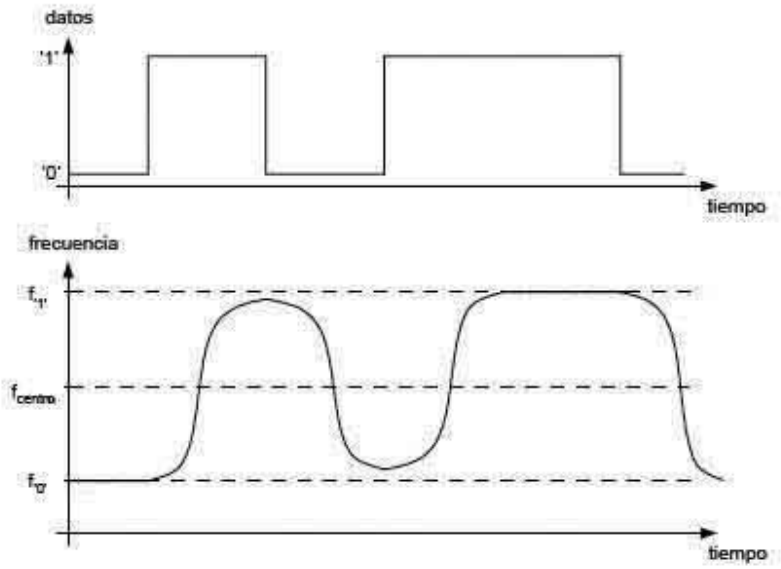


Figura tomada de la página de Internet: www.wikipedia.com. Recuperada el 23 de enero de 2008.

GFSK es una versión mejorada de la modulación por desplazamiento de frecuencia (**FSK**). En GFSK la información es pasada por un filtro gaussiano antes de modular la señal. De esta forma se traduce en un espectro de energía mas estrecho de la señal modular, lo cual permite mayores velocidades de transferencia de información sobre el mismo canal.

La banda ISM por sus siglas en inglés (Industrial, scientific and medial), son bandas reservadas internacionalmente para el uso no comercial de frecuencia electromagnética en áreas industrial, científica y médica. En la actualidad estas bandas se han popularizado por el uso en las comunicaciones como lo son el WlAN ejemplo WI-FI o WPAN por el bluetooth.

Las bandas ISM fueron definidas por la ITU en el artículo 5 de la regulación de radio (**RR**), concretamente en los puntos 5.138 y 5.150. Estas bandas están abiertas a todo el mundo sin necesidad de licencia, por lo cual son muy populares en todo el ámbito de comunicación como en los teléfonos inalámbricos de uso personal, no para teléfonos celulares. Sin embrago, esta banda tiene restricciones de potencia de trasmisión, lo cual limita su alcance de cobertura. Este echo fuerza a que este tipo de comunicaciones tenga cierto nivel de tolerancia con los errores y que utilice diferentes métodos y mecanismos para controlar las interferencias, como técnicas de ensanchado de espectro. Por este motivo, las redes que trabajan bajo este mecanismo son denominadas redes de espectro ensanchado.

4.2 Conceptos generales de la biometría:

El término biometría viene del griego *"bio"* que significa vida y *"metría"* que significa medida o medición. De acuerdo al diccionario de la Real Academia de la Lengua Española, biometría es el estudio mensurativo o estadístico de los fenómenos o procesos biológicos. Sin embargo más recientemente y para el tema que nos concierne el significado de biometría es el conjunto de métodos automatizados que analizan determinadas características humanas, para identificar o autentificar personas[6].

La biometría aprovecha que hay ciertas características biológicas o conductuales singulares e inalterables, por lo que pueden ser analizados y medidos para crear una huella biométrica. Estas características son difíciles de perder, transferir u olvidar y son perdurables en el tiempo.

La biometría se soporta en siete pilares o conceptos básicos que son:

- Universalidad: que tan común es encontrar este biométrico en los individuos.
- Singularidad: que tan único o diferenciable es la huella biométrica entre uno y otro individuo.
- Permanencia: que tanto perdura la huella biométrica en el tiempo de manera inalterable.
- Recolectable: Qué tan fácil es la adquisición, medición y almacenamiento de la huella biométrica.

[6] Woodward Jr. John D., & Orlans Nicholas M., & Higgins Peter D. (2002) Biometrics, identity assurance in the information age. Primera edición. EE.UU.: McGraw-Hill Osborne Media.

- Calidad: que tan preciso, veloz y robusto es el sistema en el manejo de la huella biométrica.
- Aceptabilidad: Qué tanta aprobación tiene la tecnología entre el público.
- Fiabilidad: Qué tan fácil es engañar al sistema de autenticación.

En la biometría se distinguen dos grupos de registros biométricos los fisiológicos o morfológicos y los conductuales.

Los biométricos morfológicos o fisiológicos son aquellos que se soportan sobre características físicas inalterables y presentes en la mayoría de los seres humanos tales como: huella dactilar, geometría de la mano, características del iris, patrones vasculares de la retina o mano.

Los biométricos conductuales son aquellos que se soportan sobre características de la conducta del ser humano tales como: pulsaciones del teclado, discurso, dinámica de la firma, etc.

Tabla 1. Tecnología biométrica emergente y su madurez

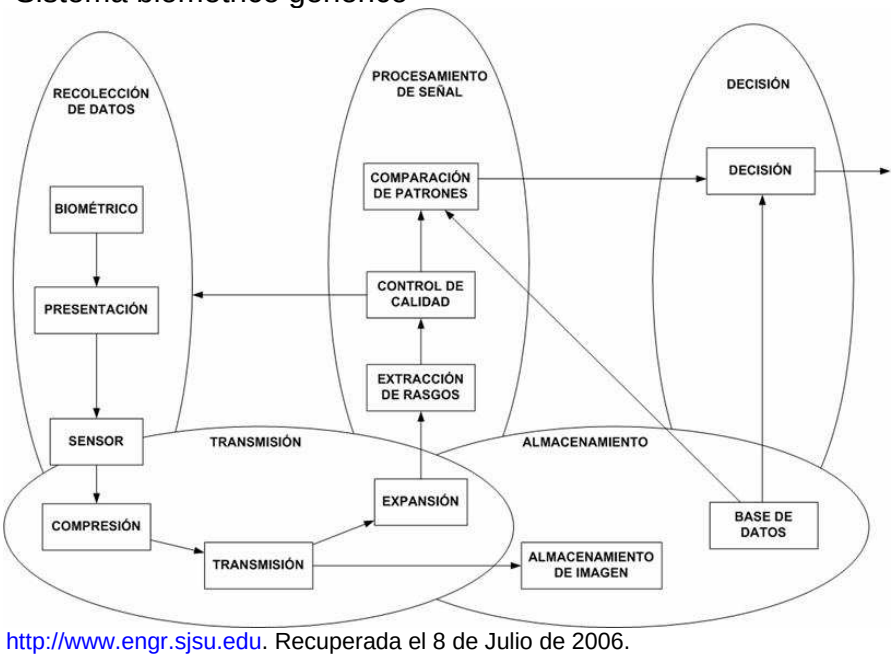
Tecnología	**Como Trabaja**	**Madurez**
Escaneo de venas	Captura imágenes del patrón del flujo sanguíneo	Comercialmente disponible
Termografía Facial	Cámaras infrarrojas detectan patrones de calor creados por el flujo sanguíneo y emitido por la piel.	Su comercialización inicial falló por el alto costo
Comparación de ADN	Compara muestras de ADN con plantillas generadas como muestra	Muchos años para implementación
Sensor de olor	Captura los químicos volátiles que los poros de la piel emiten	Muchos años para su comercialización
Medidor del pulso sanguíneo	Sensores infrarrojos medien el pulso de la sangre en el dedo	Experimental
Reconocimiento del patrón de la piel	Extrae distintos patrones ópticos por medidas de espectroscopia de la luz reflejada por la piel	Emergente
Identificación de la cama de la uña	Un interferómetro detecta las fases de cambio en la incidencia de luz en la uña del dedo; reconstruye distintas dimensiones de la cama de la uña y genera un mapa unidimensional	Emergente
Reconocimiento de movimiento	Captura una secuencia de imágenes para derivar y analizar las características de movimiento	Emergente: requiere desarrollo futuro
Reconocimiento de la forma de	Está basada en la distinción de la forma de la oreja y la estructura del cartílago,	Todavía un tópico de

oreja	proyectando parte del oído externo.	investigación

Tomado de: http://www.engr.sjsu.edu. Recuperada el 8 de Julio de 2006.

En general un sistema biométrico se puede esquematizar de la siguiente manera:

Figura 2. Sistema biométrico genérico



Tomado de: http://www.engr.sjsu.edu. Recuperada el 8 de Julio de 2006.

En la biometría hay tres términos de uso muy frecuente que son reconocimiento, verificación e identificación, cada uno de estos términos que a simple vista parecen muy similares, tienen significados muy diferentes.

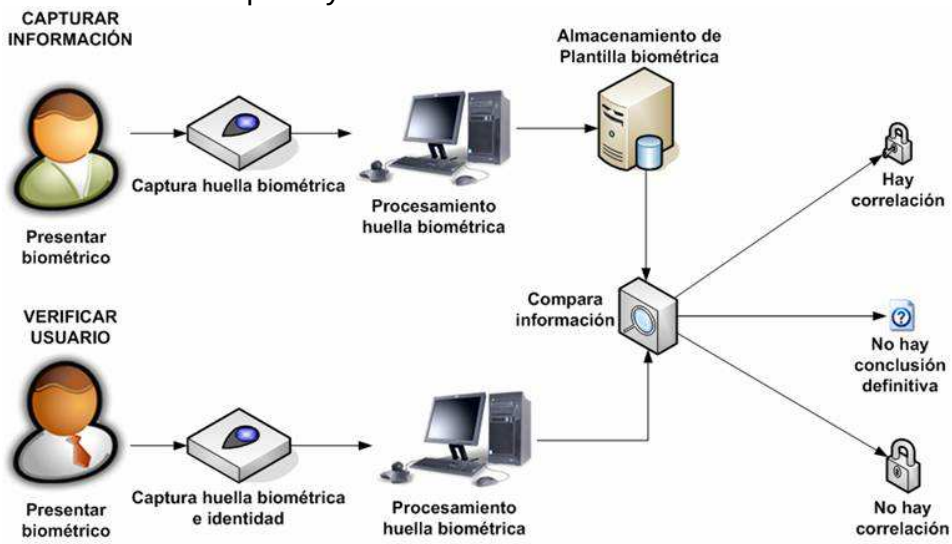
Reconocimiento: Es un término genérico que no implica por defecto una verificación o identificación de un individuo. Todos los sistemas biométricos realizan reconocimiento para "distinguir de nuevo" una persona que se ha ingresado previamente al sistema.

Verificación: Es una tarea de los sistemas biométricos que busca confirmar la identidad de un individuo que la reclama comparando una muestra biométrica con la plantilla biométrica previamente ingresada al sistema.

Identificación: Es una tarea donde los sistemas biométricos buscan determinar la identidad de un individuo. El dato biométrico es tomado y comparado contra las plantillas en la base de datos, la identificación puede ser cerrada (si se sabe que la persona existe en la base de datos) o abierta (si no se sabe con certeza si la persona existe en la base de datos), la identificación abierta también es llamada *watchlist.*

Partiendo de las definiciones anteriores sabemos que hay tres formas para comparar la muestra biométrica, la comparación uno a uno (Verificación), la comparación uno a muchos (Identificación cerrada) y la comparación uno a pocos que es una mezcla de los dos primeros (identificación abierta o watchlist).
Verificación: En el proceso de comparación uno a uno, el usuario presenta su(s) dato(s) biométrico(s) y este se compara con la plantilla biométrica almacenada en una base de datos o en un dispositivo portátil, verificando si hay o no coincidencia para esa identidad en la referencia establecida (ver Figura).

Figura 3. Proceso de captura y verificación de usuario



Tomado de: http://www.engr.sjsu.edu. Recuperada el 8 de Julio de 2006.

Identificación cerrada: En el proceso de comparación uno a muchos, el usuario presenta su(s) dato(s) biométrico(s) y el dato biométrico se compara contra la base de datos, donde se sabe que existe, buscando la identidad más probable del usuario.

Identificación abierta: Es un proceso híbrido entre la verificación y la identificación cerrada, donde la persona no reclama una identidad específica, entonces se compara contra toda la base de datos para verificar si existe en esta, una vez se verifica que posiblemente existe, dentro de las coincidencias más probables, determina quién es el usuario.

Para la toma de decisiones el resultado de cualquiera de las comparaciones que se hagan puede presentar una de tres posibilidades dependiendo de la puntuación que se alcance en la comparación de la plantilla y del dato biométrico, y del umbral que se le haya dado al sistema; las tres posibles alternativas son:

- **Hay correlación:** es decir que al comparar el dato biométrico capturado con la(s) plantilla(s) almacenada(s) la puntuación está dentro de los umbrales de coincidencia.

- **No hay correlación:** es decir que al comparar el dato biométrico capturado con la(s) plantilla(s) almacenada(s) la puntuación está fuera de los umbrales de coincidencia.
- **Imposibilidad de alcanzar conclusión definitiva:** es decir que hay falta de información para poder hacer una comparación adecuada.

La precisión de un sistema biométrico está determinado por una serie de pruebas, que están divididas en tres categorías: tecnología, escenario y funcional. Para su evaluación se consideran varios conceptos que se pueden generalizar en dos: la probabilidad de que alguien autorizado sea rechazado y la probabilidad de que alguien no autorizado sea aceptado. El término a usar varía, a grandes rasgos, dependiendo del tipo de comparación que se haga y en que categoría se haga la evaluación.

Los términos más comúnmente observados son los siguientes:

La Tasa de falsa aceptación: (FAR – False Acceptance Rate) Es una estadística que muestra la operación del sensor biométrico, típicamente cuando opera en la tarea de verificación. En general entre más bajo sea el valor de la tasa de falsa aceptación, más alta es la precisión del sistema biométrico. En esta tasa se muestra el porcentaje del número de veces que el sistema produce una falsa aceptación. Es decir, cuando un individuo es identificado como usuario de manera incorrecta. Este valor debe ser lo suficientemente bajo como para que no se impida el ingreso a los usuarios, pero no tanto que permita el ingreso de personal no autorizado. El valor depende de lo sensible del área o sistema a proteger y de la necesidad del usuario. A nivel de fabricantes la mayoría tienen esta tasa entre el 0.0001% y el 0.1%. La tasa dada normalmente asume intentos pasivos del impostor.

FAR= PR x FMR x (1-FTA)

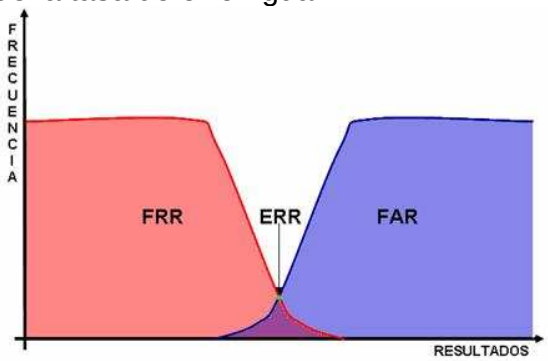
Tasa de Falso Rechazo (FRR - False Reject Rate): La probabilidad de que un dispositivo rechace una persona autorizada. Comercialmente su valor varía entre el 0.00066% y el 1%.

FRR=FTA+(1-FTA)x BER +(1-FTA)x(1-BER)x FNMR

El punto de intersección entre la tasa de falsa aceptación y la tasa de falso rechazo: Se conoce como la tasa de error igual (EER - Equal Error Rate), algunas veces se llama tasa de error cruzada (CER – Crossover Error Rate).Es una estadística que muestra la actuación del biométrico, típicamente cuando opera en

la tarea de verificación. En general entre más bajo sea el valor de la tasa de error igual, más alta es la precisión del sistema biométrico (ver Figura).

Figura 4. Definición de la tasa de error igual.



Tomado de: Williams, Ian. Biometric Technology for DLID. An introduction to the Science. EE.UU.

Otros términos utilizados son:

Tasa de Falsa alarma: (False Alarm Rate) Una estadística usada para medir la calidad del biométrico cuando opera en el modo de identificación abierta (watchlist ó comparación uno a pocos). Este es el porcentaje de veces que una alarma suena incorrectamente en un individuo que no está en el sistema de la base de datos (el sistema alarma en Carlos cuando Carlos no está en la base de datos), o una alarma suena pero la persona incorrecta es identificada (el sistema alarma en Edgar cuando Edgar está en la base de datos, pero el sistema piensa que Edgar es Carlos).

Tasa de falsa coincidencia: (FMR - False Match Rate) La probabilidad de que un sistema biométrico identifique incorrectamente un individuo o que falle para rechazar un impostor. Alternativa a Tasa de falsa aceptación (FAR).

Tasa de falsa no-coincidencia: (FNMR - False Non-Match Rate) es parecida a la tasa de falso rechazo (FRR), con la diferencia de que la FRR incluye la tasa de falla para capturar el error (Failure to Acquire error rate).

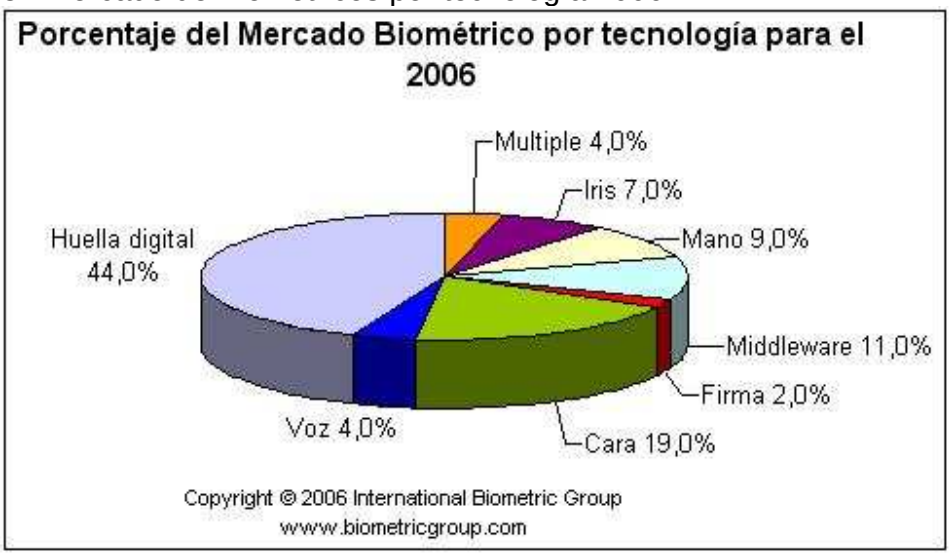
Error tipo I: Este tipo de error ocurre en una prueba estadística cuando una reclamación valida es rechazada. Es decir cuando falla al rechazar una reclamación válida. Por ejemplo Claudia reclama ser Claudia, pero el sistema niega el reclamo de manera incorrecta.

Error Tipo 2: Este tipo de error ocurre en una prueba estadística cuando una reclamación falsa es aceptada. Es decir cuando falla al aceptar una reclamación falsa. Por ejemplo Erika reclama ser Sandra y el sistema acepta el reclamo de manera incorrecta.

4.3 Modalidades biométricas.

Las tecnologías biométricas de mayor uso hoy y con más apoyo por las industrias comerciales son: la huella digital, el reconocimiento facial, la geometría de la mano, el iris, la voz, la firma.

Figura 5. Mercado de Biométricos por tecnología 2006



Tomado de: http://www.biometricgroup.com. Recuperada el 20 de mayo de 2007.

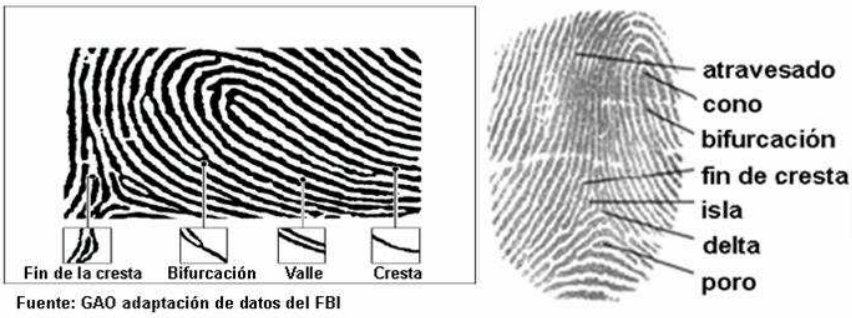
4.3.1 Reconocimiento de Huella digital.

La comparación de la huella digital es una de las técnicas más antiguas y ampliamente utilizadas y aceptadas a nivel global.

Los sistemas actuales de comparación de la huella digital tienen su base en los desarrollos realizados por Galton y Purkinje.

La huella digital aparece generalmente constituida por una serie de líneas oscuras que representan las crestas y una serie de espacios blancos que representan los valles. La identificación con huellas digitales está basada principalmente en las minucias (la ubicación y dirección de las terminaciones de crestas, bifurcaciones, deltas, valles y crestas), aunque existen muchas otras características de huellas digitales.

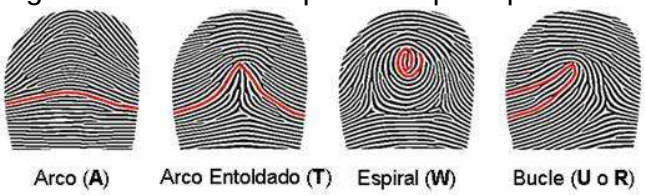
Figura 6. Características de Huellas digitales



Fuente: GAO adaptación de datos del FBI

Otra forma de distinguir las huellas digitales es por sus patrones, los cuales presentó Purkinje en su tesis doctoral.

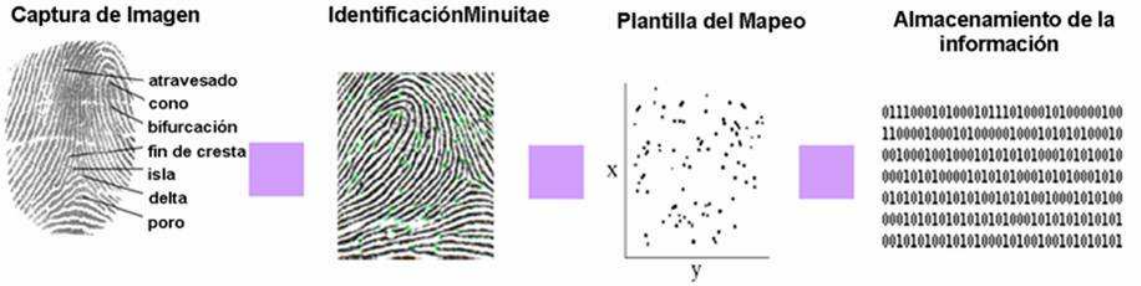
Figura 7. Los cuatro patrones principales



Tomado de: KEOGH, Eamonn. The Science of Fingerprints. Pp.4. EE.UU.

De manera general la forma de procesar una huella digital es la siguiente:

Figura 8. Proceso común de escaneo de la huella digital



Tomado de: Williams, Ian. Biometric Technology for DLID. An Introduction to the Science. EE.UU.

4.3.2 Formato para guardar la imagen del dedo

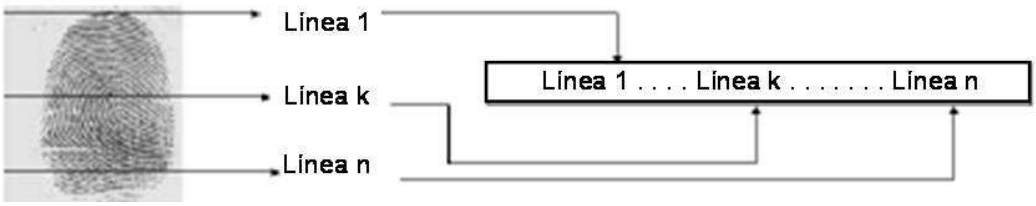
Cada record debe pertenecer a un solo individuo y debe contener una imagen guardada (consistente en una o mas vistas) por cada uno o más dedos. Registros de imágenes sencillas para múltiples dedos.

La organización del formato de registro es como sigue:

- Una sola longitud-fija (32-byte) general de encabezado de record que contiene la información acerca del registro global, incluyendo el número de imágenes de dedos representados y la longitud del registro global en bytes.

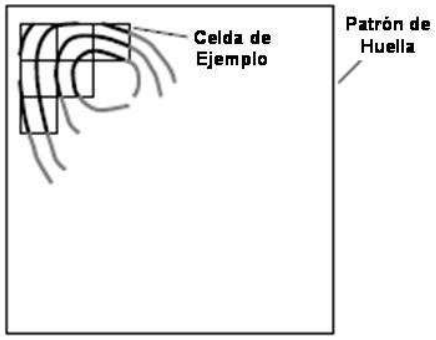
- Un solo registro digital por cada dedo, vista, imagen multi-dedos consistente en:
- Un encabezado de longitud fija (14-byte) que contiene la información perteneciente a los datos para una imagen sencilla o multi-dedos;
- Datos de la vista de imagen comprimida o descomprimida para sencillo o multi-dedos.

Figura 9. Orden de escaneo de las líneas.



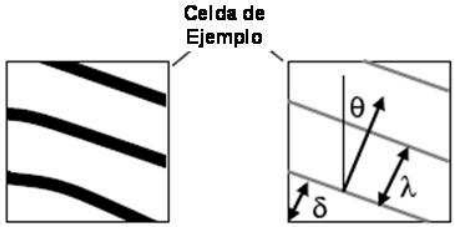
Tomado de: KEOGH, Eamonn. The Science of Fingerprints. Pp.4. EE.UU.

Figura 10. Diagrama que ilustra la representación celular del patrón de la huella.



Tomado de: KEOGH, Eamonn. The Science of Fingerprints. Pp.4. EE.UU.

Figura 11. Representación celular del patrón de la huella



Tomado de: KEOGH, Eamonn. The Science of Fingerprints. Pp.4. EE.UU.

Tabla 2. Niveles de escena adquisición de imagen

Ajuste de nivel	Resolución del escáner píxeles/cm.	Resolución del escáner píxeles/in	Píxeles de profundidad (bits)	Rango dinámico (nivel gris)	Certificación
10	49	125	1	2	Ninguna
20	98	250	3	5	Ninguna
30	197	500	8	80	Ninguna
31	197	500	8	200	EFTS/F
40	394	1000	8	120	Ninguna
41	394	1000	8	200	EFTS/F

Tomado de: KEOGH, Eamonn. The Science of Fingerprints. Pp.4. EE.UU.

Tabla 3. Encabezado de record general

Campo	Tam. Bytes	Valores validos	Notas
Identificador de formato	4	0x464952 (‘F’ ‘I’ ‘R’ 0X0)	“FIR” – Record de Imagen de dedo
Numero de versión	4	0X30313000 (‘0’ ‘1’ ‘0’ 0X0)	“010”
Longitud del record	4	32 + número de vistas * (14 bytes + Longitud del dato)	Incluye todas las vistas de dedos
Dispositivo de captura ID	6		Especificación vendedor
Nivel de adquisición de imagen	2	Ver tabla 5	Combinación de parámetros
Número de dedos/palmas	1	>=1	
Unidad de escala	1	1-2	Píxel/pulgada o píxel/cm
Resolución Scan (horiz)	2	Ver tabla 5	Hasta 1000 ppi
Resolución Scan (vert)	2	Ver tabla 5	Hasta 1000 ppi
Resolución imagen (horiz)	2	<= Resolución escáner (horiz)	Depende del nivel de calidad
Resolución imagen (vert)	2	<= Resolución escáner (horiz)	Depende del nivel de calidad
Profundidad píxel	1	1-16 bits	2-65536 niveles de gris
Algoritmo de compresión imagen	1	Ver tabla 7	No comprimido o algoritmo usado
Reservado	2		Bytes set para ‘0x0’

Tomado de: KEOGH, Eamonn. The Science of Fingerprints. Pp.4. EE.UU

Tabla 4. Código de algoritmo de compresión.

Código	**Algoritmo de compresión**
0	No comprimido – bit no empaquetado
1	No comprimido – bit empaquetado
2	Comprimido – WSQ
3	Comprimido – JPEG
4	Comprimido – JPEG2000
5	PNG

Tomado de: KEOGH, Eamonn. The Science of Fingerprints. Pp.4. EE.UU.

Tabla 5. Encabezado del record de imagen de dedo

Campo	**Tam**	**Valor valido**	**Notas**
Longitud del bloque de datos de dedo (bytes)	4 byte		Incluye encabezado, y bloque de datos de imagen más largo
Posición dedo/palma	1 byte	0-15; 20-36	Ver tabla 8 y 9
Conteo de vistas	1	1-256	
Número de vistas	1	1-256	
Calidad de imagen dedo/palma	1 byte	1-100	Especificaciones BioAPI
Tipo de impresión	1 byte		Tabla 10
Longitud línea Horizontal	2 bytes		Numero de pixeles por línea horizontal
Longitud línea vertical	2 bytes		Numero de líneas horizontales
Reservado	1 byte	---	Byte set a ‘0x0’
Dato de imagen dedo/palma	$<43x10^8$ bytes	---	Datos de imagen comprimido o descomprimido

Tomado de: KEOGH, Eamonn. The Science of Fingerprints. Pp.4. EE.UU.

Tabla 6. Código de posición de dedos, y dimensiones máximas

Posición de dedos	**Código dedo**	**Máx. área imagen (mm^2)**	**Ancho (cm)**	**Longitud (mm)**
Desconocido	0	1745	406	38.1
Pulgar derecho	1	1745	406	38.1
Índice derecho	2	1640	406	38.1
Corazón derecho	3	1640	406	38.1
Anular derecho	4	1640	406	38.1
Meñique derecho	5	1640	406	38.1
Pulgar izquierdo	6	1745	406	38.1
Índice izquierdo	7	1745	406	38.1
Corazón izquierdo	8	1640	406	38.1
Anular izquierdo	9	1640	406	38.1
Meñique izquierdo	10	1640	406	38.1
Derecha completa 4	13	6800	83.8	76.2

dedos				
Izquierda completa 4 dedos	14	6800	83.8	76.2
Pulgares completa (2)	15	4800	50.8	76.2

Tomado de: KEOGH, Eamonn. The Science of Fingerprints. Pp.4. EE.UU.

Tabla 7. Tipos de impresión de dedo y palma.

Código	Descripción
0	Escaneo vivo pleno
1	Escaneo vivo rollado
2	Escaneo no-vivo pleno
3	Escaneo no-vivo rollado

Código	Descripción
7	Latente
8	De Golpe
9	Escaneo vivo sin contacto

Tomado de: KEOGH, Eamonn. The Science of Fingerprints. Pp.4. EE.UU.

Tabla 8. Ejemplo de almacenamiento de la huella digital.

Campo	Bytes	Valor	Notas
Identificador de formato	1-4	46 49 52 00	"FIR" – Record de Imagen de dedo
Numero de versión	5-8	30 31 30 00	"010"
Longitud del record	9-14	00 00 00 03 93 b5	Una vista de dedo 32+1*(14+234,375)
Dispositivo ID	15-16	01 02	Vendedor proveedor
Nivel de adquisición de imagen	17-18	00 1F	Nivel 31
Número de dedos/palmas	19	01	
Unidad de escala	20	01	Píxel/pulgada
Resolución Scan (horiz)	21-22	01 F4	500 píxel/pulgada
Resolución Scan (vert)	23-24	01 F4	500 píxel/pulgada
Resolución imagen (horiz)	25-26	01 F4	500 píxel/pulgada
Resolución imagen (vert)	27-28	01 F4	500 píxel/pulgada
Profundidad píxel	29	08	256 niveles de gris
Algoritmo de compresión imagen	30	00	No comprimido (no paquetes de bit)
Reservado	31-32	00 00	

Tomado de: KEOGH, Eamonn. The Science of Fingerprints. Pp.4. EE.UU.

5. MARCO TEORICO

5.1 Biometría:

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

La "*biometría informática*" es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para “verificar” identidades o para “identificar” individuos.

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

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

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

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

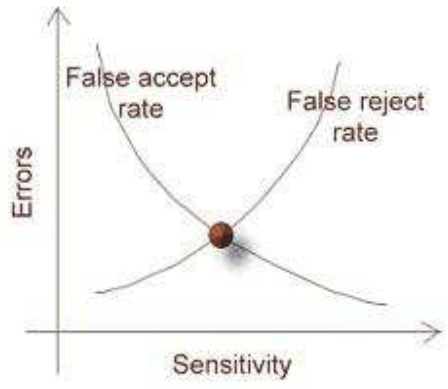
En estos últimos años la biométrica ha crecido desde usar simplemente la huella dactilar, a emplear muchos métodos distintos teniendo en cuenta varias medidas físicas y de comportamiento. Las aplicaciones de la biometría también han aumentado - desde sólo identificación hasta sistemas de seguridad y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

5.1.2 Funcionamiento y rendimiento:

En un sistema biométrico típico, la persona se registra con el sistema cuando una o más de sus características físicas y de conducta es obtenida, procesada por un algoritmo numérico, e introducida en una base de datos. Idealmente, cuando entra, casi todas sus características concuerdan; entonces cuando alguna otra persona intenta identificarse, no empareja completamente, por lo que el sistema no le permite el acceso. Las tecnologías actuales tienen tasas de error que varían ampliamente (desde valores bajos como el 60%, hasta altos como el 99,9%).

El rendimiento de una medida biométrica se define generalmente en términos de tasa de falso positivo (*False Acceptance Rate* o FAR), la tasa de falso negativo (*False NonMatch Rate* o FNMR), y el fallo de tasa de alistamiento (*Failure-to-enroll Rate*, FTR o FER).

Figura 12. Error vs. Sensibilidad



Tomado de: Williams, Ian. Biometric Technology for DLID. An Introduction to the Science. EE.UU.

En los sistemas biométricos reales el FAR y el FRR pueden transformarse en los demás cambiando cierto parámetro. Una de las medidas más comunes de los sistemas biométricos reales es la tasa en la que el ajuste en el cual acepta y rechaza los errores es igual: la tasa de error igual (*Equal Error Rate* o EER), también conocida como la tarifa de error de cruce (*Cross-over Error Rate* o CER). Cuanto más bajo es el EER o el CER, se considera que el sistema es más exacto.

Las tasas de error anunciadas implican a veces elementos idiosincrásicos o subjetivos. Por ejemplo, un fabricante de sistemas biométricos fijó el umbral de aceptación alto, para reducir al mínimo las falsas aceptaciones; en la práctica, se

permitían tres intentos, por lo que un falso rechazo se contaba sólo si los tres intentos resultaban fallidos (por ejemplo escritura, habla, etc.), las opiniones pueden variar sobre qué constituye un falso rechazo. Si entro a un sistema de verificación de firmas usando mi inicial y apellido, ¿puedo decir legítimamente que se trata de un falso rechazo cuando rechace mi nombre y apellido?

A pesar de estas dudas, los sistemas biométricos tienen un potencial para identificar a individuos con un grado de certeza muy alto. La prueba forense del ADN goza de un grado particularmente alto de confianza pública actualmente (ca. 2004) y la tecnología está orientándose al reconocimiento del iris, que tiene la capacidad de diferenciar entre dos individuos con un ADN idéntico.

Tabla comparativa de sistemas biométricos:

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

Tabla 9.

	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

Estándares asociados a tecnologías biométricas:

En los últimos años se ha notado una preocupación creciente por las organizaciones regulatorias respecto a elaborar estándares relativos al uso de técnicas biométricas en el ambiente informático. Esta preocupación es reflejo del creciente interés industrial por este ámbito tecnológico, y a los múltiples beneficios que su uso aporta. No obstante, aún la estandarización continua siendo deficiente

y como resultado de ello, los proveedores de soluciones biométricas continúan suministrando interfaces de software propietarios para sus productos, lo que dificulta a las empresas el cambio de producto o vendedor.

A nivel mundial el principal organismo que coordina las actividades de estandarización biométrica es el Sub-Comité 17 (SC17) del Joint Technical Committee on Information Technology (ISO/IEC JTC1), del International Organization for Standardization (ISO) y el International Electrotechnical Commission (IEC).

En Estados Unidos desempeñan un papel similar el Comité Técnico M1 del INCITS (InterNational Committee for Information Technology Standards), el National Institute of Standards and Technology (NIST) y el American National Standards Institute (ANSI).

Existen además otros organismos no gubernamentales impulsando iniciativas en materias biométricas tales como: Biometrics Consortium, International Biometrics Groups y BioAPI. Este último se estableció en Estados Unidos en 1998 compuesto por las empresas Bioscrypt, Compaq, Iridiam, Infineon, NIST, Saflink y Unisis. El Consorcio BioAPI desarrolló conjuntamente con otros consorcios y asociaciones, un estándar que promoviera la conexión entre los dispositivos biométricos y los diferentes tipos de programas de aplicación, además de promover el crecimiento de los mercados biométricos.

Los estándares más importantes son: Estándar ANSI X.9.84 Estándar creado en 2001, por la ANSI (American National Standards Institute) y actualizado en 2003, define las condiciones de los sistemas biométricos para la industria de servicios financieros haciendo referencia a la transmisión y almacenamiento seguro de información biométrica, y a la seguridad del hardware asociado.

Estándar ANSI / INCITS 358 Estándar creado en 2002 por ANSI y BioApi Consortium, que presenta una interfaz de programación de aplicación que garantiza que los productos y sistemas que cumplen este estándar son interoperables entre sí.

Estándar NISTIR 6529 También conocido como CBEFF (Common Biometric Exchange File Format) es un estándar creado en 1999 por NIST y Biometrics Consortium que propone un formato estandarizado (estructura lógica de archivos de datos) para el intercambio de información biométrica.

5.1.3 Procesos de Autenticación e Identificación biométrica:

En el proceso de autenticación (o verificación) los rasgos biométricos se comparan solamente con los de un patrón ya guardado, este proceso se conoce también como uno-para-uno (1:1). Este proceso implica conocer presuntamente la identidad del individuo a autenticar, por lo tanto, dicho individuo ha presentado algún tipo de credencial, que después del proceso de autenticación biométrica será validada o no.

En el proceso de identificación los rasgos biométricos se comparan con los de un conjunto de patrones ya guardados, este proceso se conoce también como uno-para-muchos (1:N). Este proceso implica no conocer la identidad presunta del individuo, la nueva muestra de datos biométricos es tomada del usuario y comparada una a una con los patrones ya existentes en el banco de datos registrados. El resultado de este proceso es la identidad del individuo, mientras que en el proceso de autenticación es un valor verdadero o falso.

El proceso de autenticación o verificación biométrica es más rápido que el de identificación biométrica, sobre todo cuando el número de usuarios (N) es elevado. Esto es debido a que la necesidad de procesamiento y comparaciones, es más reducido en el proceso de autenticación. Por esta razón, es habitual usar autenticación cuando se quiere validar la identidad de un individuo desde un sistema con capacidad de procesamiento limitada o se quiere un proceso muy rápido.

5.2 Cuestiones y preocupaciones:

Como con muchos otros progresos tecnológicos interesantes y de gran alcance, las excesivas dudas en lo referente a la biometría pueden ensombrecer una crítica más general. La biometría puede llegar a asociarse con fallos severos de la justicia en aquellos casos en los que la tecnología ha desviado la atención del verdadero foco, así, un individuo podría:

- introducir deliberadamente ADN en la escena de un crimen.
- relacionar sus propios parámetros biométricos con la identidad de otra persona.
- engañar a un detector de huellas dactilares mediante una superficie que tuviera una huella impresa en ella.
- engañar un reconocimiento ocular mediante una fotografía de un iris verdadero.
- interferir la señal del aparato de reconocimiento biométrico y el sistema informático que procesa dicha señal.

La domótica del latín *domus* (casa), a su vez del griego *doma*, δῶμα[7] (cúpula); y robótica, del checo *robota* (esclavo), es el conjunto de sistemas automatizados de una vivienda que aportan servicios de gestión energética, seguridad, bienestar y comunicación, y que pueden estar integrados por medio de redes interiores y exteriores de comunicación, alambradas o inalámbricas. Se centra en los servicios de bienestar, seguridad y comunicaciones que pueden facilitarse en la vivienda a sus habitantes. Se podría definir como la integración de la tecnología en el diseño inteligente de un recinto.

5.2.1 Elementos importantes en una instalación de domótica:

- Incremento en el confort.
- Automatización del control de luces, persianas, ventanas, cortinas y enchufes.
- Climatización automática. Calefacción y refrigeración.
- Optimización en la gestión de consumos: energía eléctrica, gas, recursos hídricos.
- Uso de energías renovables Energía solar, Energía geotérmica, Energía eólica.
- Automatización de tareas: riego, encendido de los servicios a ciertas horas,en función de eventos, etc.
- Ubicuidad en el control tanto externo como interno, control remoto desde Internet, PC, mandos inalámbricos (p.ej. PDA con WiFi), aparellaje eléctrico.
- Facilidad de uso, (GUI, Interfaz de usuario gráfico, front-end, aplicación).
- Gestión del ocio.
- Alarmas. Vigilancia anti-incendios. Temperatura. Detección de fugas de gas o agua.
- Control de accesos. Control biométrico.
- Control de servicios para emular la presencia de gente durante las ausencias prolongadas.
- Gestión alarmas técnicas: corte de suministros, posibilidad de visualización remota de la vivienda.

5.2.2 Bus de Instalación Europeo (EIB o EIBus)

El **Bus de Instalación Europeo** (**EIB** o **EIBus**) es un Bus de datos utilizado para domótica.

A diferencia del X10 (otro bus domótico), que utiliza la red eléctrica, el EIB utiliza su propio cableado.

[7] Palabra griega que traducida al español, significa “cúpula”. Término tomado de la página de Internet: **http://es.wikipedia.org/wiki/Domótica.** Recuperada el 8 de octubre de 2006.

El EIB puede ser utilizado en sistemas inalámbricos como los infrarrojos, radiofrecuencia o incluso empaquetado para enviar información por Internet u otra red TCP/IP.

Originariamente conocido por *Instabus*, ingeniería de donde salieron los primeros esbozos, esta abrazado por un conjunto de empresas (en su mayoría alemanas) y lleva más de 20 años en el mercado de la automatización sin haber penetrado profundamente, a pesar de que, a diferencia del X10, es un sistema robusto.

5.2.3 Protocolo X10

X10 es un protocolo de comunicaciones para el control remoto de dispositivos eléctricos. Utiliza la línea eléctrica (220V o 110V) para transmitir señales de control entre equipos de automatización del hogar en formato digital.

X10 fue desarrollada en 1975 por Pico Electronics of Glenrothes, Escocia, para permitir el control remoto de los dispositivos domésticos. Fue la primera tecnología domótica en aparecer y sigue siendo la más ampliamente disponible.

Las señales de control de X10 se basan en la transmisión de ráfagas de pulsos de RF (120 Khz) que representan información digital. Estos pulsos se sincronizan en el cruce por cero de la señal de red (50 Hz ó 60 Hz). Con la presencia de un pulso en un semiciclo y la ausencia del mismo en el semiciclo siguiente se representa un '1' lógico y a la inversa se representa un '0'. A su vez, cada orden se transmite 2 veces, con lo cual toda la información transmitida tiene cuádruple redundancia. Cada orden involucra 11 ciclos de red (220 mseg).

Primero se transmite una orden con el Código de Casa y el Número de Módulo que direccionan el módulo en cuestión. Luego se transmite otra orden con el código de función a realizar (Function Code). Hay 256 direcciones soportadas por el protocolo.

El protocolo X10 consta de bits de «direcciones» y de «órdenes». Por ejemplo, Vd. puede decir «lámpara #3», «¡enciéndete!» y el sistema procederá a ejecutar dicho mandato. Vd. puede direccionar varias unidades antes de dar la orden: «lámpara #3, lámpara #12», «¡encendeos!», son 6 las instrucciones utilizadas por el protocolo: ON, OFF, All Lights ON, All off, DIM, BRIGHT.

Los dispositivos están generalmente enchufados en módulos X10 (receptores). X10 distingue entre módulos de lámparas y módulos de dispositivos. Los módulos de dispositivos proporcionan energía a los dispositivos eléctricos y aceptan órdenes X-10. Los módulos de dispositivos son capaces de gestionar cargas grandes (ej. máquinas de café, calentadores, motores, entre otros), simplemente encendiéndolos y apagándolos.

Si desea controlar luces vía mandatos X-10, debería conectar la luz en un módulo de luz en la red y, a continuación, asignarle una dirección (A1, por ejemplo). Así, cuando envíe la orden «A1 encendido» a través de los cables de la red eléctrica, la luz se debería encender. Cabe destacar que los módulos de lámparas no pueden soportar grandes cargas y que es muy sensible a los ruidos eléctricos por lo que es considerado como un sistema para el "hazlo tu mismo".

5.2.4 Protocolo ZigBee

ZigBee es un protocolo de comunicaciones inalámbrico similar al bluetooth.

ZigBee es muy similar al Bluetooth pero con algunas diferencias:

- Menor consumo eléctrico que el ya de por sí bajo del Bluetooth
- Velocidad de transferencia también menor.

Ambos son pensados para aplicaciones portátiles (PDAs, móviles, etc.) aunque zigbee es más adecuado para la automatización del hogar (domótica).

Existe una versión que integra el sistema de radiofrecuencias característico de Bluetooth junto a interfaz de transmisión de datos vía infrarroja, desarrollado por IBM mediante un protocolo ADSI y MDSI.

5.2.5 Características del sistema:

Bandas en las que opera: 2.4 Ghz, 915 MHz y 868 MHz.

Métodos de transmisión: DSSS, se focaliza en las capas inferiores de red (Física y MAC).

Velocidad de transmisión: 20 kbit/s por canal

5.2.6 OSGI

Se refiere a **O**pen **S**ervices **G**ateway **I**nitiative, más precisamente el OSGi14. Fue creado en Marzo de 1999.

Su objetivo es el de definir las especificaciones abiertas de software, que permita diseñar plataformas compatibles, que puedan proporcionar múltiples servicios. Fue pensado principalmente para su aplicación en redes hogareñas, y por ende en la llamada domótica o informatización del hogar.

Aunque OSGi define su propia arquitectura, ha sido pensada para su compatibilidad con Jini o UPnP.

La arquitectura de OSGi posee dos elementos fundamentales, de los cuales el *Service Platform* está situado en la red local y conectada al proveedor de servicios a través de una pasarela en la red del operador. Este elemento será el responsable de permitir la interacción entre dispositivos o redes de dispositivos, que podrían utilizar distintas tecnologías para comunicarse.

La especificación de OSGi se ha definido con una serie de APIs básicas para el desarrollo de servicios, como los de logging, servidor HTTP y el Device Access Specification o DAS, que permite el descubrir los dispositivos y servicios ofrecidos por éstos.

5.2.7 Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) es una arquitectura software abierta y distribuida que de forma independiente al fabricante, sistema operativo, lenguaje de programación, etc. Permite el intercambio de información y datos, a los dispositivos conectados a una red. Según el Foro UPnP:

UPnP define protocolos y procedimientos comunes para garantizar la interoperatividad sobre pc's permitidos por red, aplicaciones y dispositivos inalámbricos.

La arquitectura UPnP soporta el trabajo de una red sin configurar, y automáticamente detecta cualquier dispositivo que puede ser incorporado a esta, obtiene su dirección IP, un nombre lógico, informando a los demás de sus funciones y capacidad de procesamiento, e informarle, a su vez, de las funciones y prestaciones de los demás. Los servidores DNS y DHCP son opcionales y son usados solamente si están disponibles en la red de trabajo.

UPnP se construye sobre protocolos y formatos existentes utilizándose juntos para definir un marco que permita la definición, muestra en la red, y control de los dispositivos de ésta.

5.2.8 Patrón básico de UPnP:

- **Dirección**: El dispositivo ensambla la red, adquiriendo una dirección única que las entidades puedan utilizar para comunicarse con el dispositivo.
- **Descripción**: El dispositivo resume sus servicios y capacidades en un formato estándar.
- **"Descubrimiento"**. El dispositivo es encontrado por los puntos de contro que aprenden sobre las capacidades del dispositivo recuperando una descripción del dispositivo.
- **Control**: El dispositivo queda a la escucha de los puntos de control.
- **Eventualidades**: El dispositivo notifica a los puntos de control registrados sobre los cambios internos del estado.

- **Presentación**: Proporciona un interfaz administrativo basado en HTML para permitir la manipulación y supervisión directas del dispositivo.

5.2.9 Que beneficios tiene:

- Independencia de medios y dispositivos: Puede funcionar sobre cualquier medio incluyendo líneas telefónicas, cables de la luz, Ethernet, RF, wireless, y 1394.Esto lo hace apropiado para usos en Domótica.
- Independencia de Plataformas: No importa el lenguaje de programación ni el sistema operativo para el desarrollo de productos con esta tecnología.
- Tecnologías basadas en Internet: Está desarrollada sobre IP, TCP, UDP, HTTP y XML entre otras.
- Control UI
- Control de programación: Ofrece una aplicación convencional de control de programación.
- Protocolos base comunes
- Extensible
- UPnP ha sido impulsado por Microsoft persiguiendo los mismos objetivos que el Jini de Sun Microsystems.

5.3 Asociaciones:

ARDE

Asociación de Robótica y Domótica de España

CENELEC

Comité Europeo de Normalización Electrotécnica. La Comisión CENELEC/ENTR/e-Europe/2001-03 es la encargada de elaborar normas a nivel internacional y la organización que ha promocionado el Smart House Forum.

ASIMELEC

La Comisión Multisectorial del Hogar Digital de ASIMELEC es la organización encargada de definir el servicio, los agentes involucrados y las tecnologías de la domótica.

AENOR

AENOR ha creado también una Subcomisión del Hogar Digital, dentro de la Comisión 133 (AEN/CTN 133 Telecomunicaciones) a fin de definir estándares

Después de realizar la investigación pertinente se llegó a la conclusión que la tecnología Z-Wave es la más adecuada para realizar este proyecto. Esta decisión fue tomada bajo los criterios de instalación, confiabilidad, costo de instalación y la cantidad de fabricantes. De esta forma podemos ver en la tabla comparativa los diferentes aspectos relacionados con todas las tecnologías y el porqué de esta decisión. (Ver anexo 6)

6. MARCO LEGAL O NORMATIVO

6.1 Jurisprudencia Colombiana en Radio Frecuencia bandas de uso libre:

Respecto a este tema la legislación colombiana específica varias normas, que regulan la utilización de bandas de frecuencia y anchos de banda. A continuación se citan algunas de estas, consideradas las más importantes para esta investigación.
De esta manera, es posible citar el TITULO II – DISPOSICIONES TECNICAS[8]. En los artículos 5 y 6 de esta norma, se habla acerca de las bandas de frecuencia. Allí se específica que es posible la utilización de estas bandas, sin causar ningún tipo de interferencia y sin necesidad de recurrir a otras instancias legales que puedan implicar mayores complicaciones, tanto para el instalador como para los usuarios.

En esta norma también se especifican cada uno de los rangos de frecuencia, y los procesos que se deben tener en cuenta con cada una de las aplicaciones y automatizaciones que se vayan a implementar en un lugar específico.
Este tipo de normas, facilitan el proceso de instalación así como la utilización de la tecnología comprendida en esta investigación. También es evidente que no va a implicar un sobrecosto (por pagos de permisos de instalación) para el instalador, lo cual quiere decir que tampoco se tendrá que contemplar un alza en el precio para el usuario ya que no se tendrá que cubrir lo que podría ser un precio extra.

6.2Jurisprudencia Colombiana para Biometría:

Aunque en las leyes colombianas no exista un artículo específico que se refiera a la biometría, la normativa colombiana también incluye este tema en algunas de sus leyes, que se mencionan y se anexan en este documento.

6.2.1 Leyes.

La ley 527 de 1999, reglamenta el uso de mensajes de datos, comercio electrónico y uso de mensajes de datos, lo que permite utilizar la tecnología Zwave sin ningún inconveniente y sin recurrir a ningún otro papeleo que pudiera complicar este proceso. Las leyes también permiten simplificar este proceso que busca ser de fácil manejo para el usuario.

[8] Anexo 1. Diario oficial 45.533. Miercoles 28 de abril de 2004. Resolución número 000689 de 2004. Tomada de la página de Internet: www.mincomunicaciones.gov.co. Recuperado el 13 de febrero de 2008.

6.2.2 Código Penal Colombiano.

El código penal también hace referencia a consideraciones que son básicas y se deben tener en cuenta para este tema. Los artículos 192, 193 y 195 son los que hacen mención a los castigos que pueden ser enfrentados al violar las normas que anteriormente se especificaron y otro tipo de infracciones. Esta es probablemente la parte más importante para tener en cuenta, ya que sería muy delicado e implicaría un gran problema el caer en alguna de estas violaciones. Al instalar es importante tener en cuenta no interferir con otro tipo de conexiones, sobre todo aquellas que pertenezcan a otras personas. Si alguna de estas interferencias se presentará se podría llegar a enfrentar de 2 a 4 años de cárcel, así que es muy importante el ser cuidadoso con las instalaciones de todos los equipos.

El artículo 193, también menciona un tema muy delicado. Este proyecto busca dar facilidades al usuario, pero también busca el bien común y la comodidad del usuario principal sin molestar a quienes lo rodean.
De esta manera, la venta o compra de instrumentos para interceptar o interferir con la privacidad de las personas esta absolutamente prohibido. Si se quisiera vender este tipo de artefactos, habría que recurrir a la solicitud de permisos especiales; de lo contrario, se estaría infringiendo la ley y la penalización comprendería el pago de una multa y probablemente una pena mayor. El software para espiar o conseguir información de otras personas, también se comprende en este artículo. Sin embargo, en este proyecto no se busca ofrecer este tipo de herramientas al usuario; simplemente se quiere señalar las prohibiciones y limitaciones a las que el usuario se vería enfrentado.

El artículo 195 básicamente recoge lo que se menciona en el art. 193. Exige que ninguna persona pueda introducirse en un sistema protegido, es decir que aquellas redes privadas deben respetarse y simplemente se debe trabajar con aquella que realmente nos compete para la instalación.

6.2.3Seguridad privada.

Aunque en Colombia no existe una legislación específica que regule la implementación y uso de mecanismos de registro biométrico para efectos de controlar el acceso a ciertos lugares, tales mecanismos son de uso legal no restringido, y susceptibles de producir documentos a título de evidencias o pruebas que puedan ser usados dentro de un proceso penal, siempre y cuando no implique vulneración a la Constitución, los tratados internacionales de derechos humanos suscritos por Colombia y la ley.

Así mismo, sobre el tema de uso de código de barras para el control de ingreso y salida de materiales y personas a las empresas, se tiene que sobre este, no existe en Colombia, una específica regulación legal vigente.

La Superintendencia de Vigilancia y Seguridad Privada es la encargada de ejercer vigilancia y control con respecto a la prestación de servicios de seguridad privada, y ella es la que posee dentro de sus funciones expedir las licencias de funcionamiento de las entidades que prestan estos servicios. Igualmente la Superintendencia le expide a estas empresas una licencia de modalidad, dentro de las cuales se encuentra la modalidad de medios, de caninos, escoltas o tecnológicos. Los llamados controles de acceso dentro de los cuales se encuentran los registros fotográficos y biométricos, hacen parte de la modalidad tecnológicos (acuerdo con el decreto 356 de 1994, el decreto 2187 de 2001)

En la circular 002 de 2002 de la Superintendencia de Vigilancia y Seguridad Privada, se establecen algunas normas en cuanto al control de parqueaderos.

7. METODOLOGIA

7.1 Enfoque de la investigación:

Este proyecto tiene un enfoque empírico analítico, ya que toda la investigación y el desarrollo se basan en las diferentes experiencias con los tipos de tecnología que se evaluaron para tomar una decisión final. A continuación se realizó un análisis de cada una de las ventajas y desventajas, que brindó cada uno de estos sistemas. De esta manera se tomó la determinación de utilizar la combinación entre la cerradura biométrica y la tecnología Z-Wave. Así mismo tiene su enfoque de investigación en protocolos de comunicación y sistemas de biometría, ya que esta basado en la capacidad de transferencia de información mediante radio frecuencia, y esta información es trasmitida una vez es activa mediante lectura de huella dactilar.

A su vez este proyecto tiene como fin, acoplar este sistema a una red existente de equipos de domótica, los cuales trabajan bajo la tecnología Z-wave. De esta forma se podrá hacer un hogar más seguro en diferentes niveles, y lograr desarrollar un nuevo dispositivo que sea compatible con esta tecnología.

7.2 Línea de investigación de USB/ SUB-línea de facultad/ Campo temático del programa:

1. **Línea de investigación:** Tecnologías Actuales y Sociedad.
2. **Sublínea de investigación:** Sistemas de Información y Comunicación.
3. **Campo temático del programa:** Automatización (Domótica).

7.3 Técnicas de recolección de información:

La información recolectada para este proyecto de grado fue recopilada, de varias fuentes de Internet, libros y papers. Para ser más especifico de la página web de la alianza de la tecnología Z-Wave. Para poder evaluar los diferentes tipos de tecnología disponibles en el mercado y hacer una escogencia apropiada de esta, se evaluaron las diferentes tecnologías a través de las páginas web del fabricante y en algunos casos con muestras reales obtenidas a través de proveedores.

Para conseguir la información pertinente sobre la biometría se indagó en las páginas supranacionales en la ISO e ICAO e internacionales como BioAPI y DoD. Estas páginas manejan cierta información sobre biometría y sus estándares internacionales. Para profundizar esta investigación se indagó en las páginas web de los diferentes fabricantes, los cuales fueron escogidos previamente basándose en el precio y funcionalidad de su producto, en algunos casos en específico se estudiaron las diferentes cerraduras de forma física ya que fue posible obtener diferentes modelos de estas a través de diferentes proveedores internacionales.

7.4 Hipótesis:

Mediante el diseño y construcción de un sistema de procesamiento de datos controlador de sistemas de domótica basados en la tecnología Z-Wave, y este siendo acoplable a una cerradura biométrica, será posible aumentar el nivel de seguridad en varios aspectos diferentes y a su vez en comodidad y eficiencia.

7.4.1 Variables Independientes:

- Estudio del puerto USB para entender la comunicación entre los diferentes dispositivos de domótica.
- Sistema de domótica instalado y funcional en una vivienda.
- Lograr un uso oportuno y correcto del laboratorio de telecomunicaciones.
- Logar un uso oportuno del laboratorio de electrónica.

7.4.2 Variables dependientes:

- Obtención de la codificación huellas dactilares.
- Obtención del protocolo de comunicación adecuado.
- Obtención de los paquetes de comunicación para enviar comandos.
- Diseño de sistema de procesamiento de datos compatible con la tecnología escogida.
- Diseño del sistema de acople con la cerradura biométrica.
- Construcción del sistema de procesamiento de datos.
- Construcción del acople entre el sistema de procesamiento de datos y la cerradura biométrica.

8. PRESENTACION Y ANALISIS DE RESULTADOS

8.1 Estadísticas[9]:

Este proyecto tuvo como fin el incrementar la seguridad de los hogares mediante la combinación de un sistema de cerradura biométrica y un sistema de procesamiento de datos controlador de la tecnología Z-Wave. Con esto lo que se intenta reducir son las alarmantes cifras que reporta el DANE en cuanto a hurto de viviendas se refiere. Las siguientes cifras fueron tomadas de la página Web oficial del DANE:

	Total Cantidad	cve
DELITOS	530872	4.1
Hurto a Personas	383179	4.3
Hurto a Residencias	69052	8.2
Cohecho por dar u ofrecer	18163	17.7
Hurto Automóvil	5986	14.8
CONTRAVENCIONES	28790	9.5
Riñas y Golpes	13604	12.6
Reuniones Ruidosas	6014	21.3
Arrojar basura en sitio público	2531	26.2
A quien amenace personas del barrio	2140	45.3

Aquí se pueden ver las alarmantes cifras que reporta el DANE para el periodo de Noviembre del 2002 hasta diciembre del 2003. Esta estipulado que si no se hace nada al respecto sobre esto, para el año presente estas cifras habrá un aumento en un 25%, sobre cada año que transcurre después de el periodo estudiado. Lo más alarmante no es esto, lo que más preocupa al gobierno y a la policía nacional es que después de haber ocurrido estos hechos no todos los afectados realizan la denuncia pertinente, estas son las alarmantes cifras que reporta el DANE para el periodo de Noviembre del 2002 hasta Diciembre del 2003:

	Total Denunció		No Denunció	
	Cantidad	cve	Cantidad	cve
Hurto a Personas	117510	6.5	340551	4.1
Hurto a Residencias	29445	16.8	51570	6.9
Hurto Automotor	7628	13.2	2039	22.2
Riñas y Golpes	4341	24.5	9263	13.8
Corrupción	1152	33.5	33707	12.8
Paseo Millonario	1598	26.9	1919	27.6
Extorsión	2898	21.2	4768	20.6

[9] Pagina de Internet del DANE:
http://www.dane.gov.co/index.php?option=com_content&task=section&id=55&Itemid=658
Recuperada 6 de septiembre del 2007.

Las cifras que reporta el DANE son alarmantes en cuanto a la denuncia de estos actos criminales, estas cifras también tienen una variación dependiendo del estrato en el cual se encuentra la vivienda. Estas son las cifras reportadas por el DANE para el periodo de Noviembre del 2002 hasta Diciembre del 2003:

	Total				Delitos				Contravenciones			
	Consumado		Tentativo		Consumado		Tentativo		Consumado		Tentativo	
	Cantidad	cve	Cantidad	cve	Cantidad	cve	Cantidad	cve	Cantidad	cve	Cantidad	cv
Total	559662	4	101888	6.1	530872	4.1	101888	6.1	28790	9.5	0	.
Estrato 1	49096	12.1	7463	26.1	45158	12.6	7463	26.1	3938	24.8	0	.
Estrato 2	162912	5.1	34344	9.8	155057	5.3	34344	9.8	7854	18.2	0	.
Estrato 3	257716	7.2	45406	10.2	243986	7.5	45406	10.2	13730	13.9	0	.
Estrato 4	49795	9	9709	16.3	47691	9.1	9709	16.3	2104	25.5	0	.
Estrato 5	26240	14.5	3414	17.2	25076	14.2	3414	17.2	1164	37.1	0	.
Estrato 6	13903	12.8	1552	25.9	13903	12.8	1552	25.9	0	.	0	.

	Total		Consumado		Tentativo	
	%	cve	%	cve	%	cve
Total	0.73	1.4	0.69	1.7	0.9	1.5
Estrato 1	0.74	5.9	0.7	6.5	1	0
Estrato 2	0.8	1.6	0.78	1.9	0.89	3.2
Estrato 3	0.71	2.1	0.68	2.3	0.89	2.3
Estrato 4	0.69	3.7	0.64	4.6	0.89	3.1
Estrato 5	0.51	8	0.45	9.5	0.95	2.8
Estrato 6	0.58	4.9	0.54	5.8	0.9	5.7

Al analizar esta tabla es muy claro que los estratos 1, 2, 3 y 4 son los estratos en los cuales se reportan más robos a viviendas. Esto tiene que ver con el hecho de que la mayoría de esta gente no puede pagar un sistema de seguridad privada para su hogar o un sistema de alarma monitoreada o un seguro contra robo o calamidades de su hogar. En comparación con los estratos 5 y 6, en los cuales podemos darnos cuenta que la cifra de denuncias es significativamente inferior. Por eso es imprescindible que la tecnología de seguridad avance y sea de acceso para todos, no solo para los estratos superiores. Gracias al desarrollo de este proyecto es posible brindar una mayor seguridad a todos los estratos ya que podría llegar a ser de un precio accesible y brindar una alta seguridad. De tal forma que estas alarmantes cifras puedan ser reducidas mediante el paso del tiempo.

8.2 Aplicación

El sistema de cerradura biométrica con un sistema de procesamiento de datos controlador de la tecnología Z-Wave fue instalado un una vivienda de 232 metros cuadrados. Esta vivienda es duplex en un primer piso, lo cual implica que la planta inferior de esta vivienda esta casi a nivel del sótano lo cual hace que esta nivel sea bastante oscuro. Esta vivienda consta con un sistema de domótica en la parte de iluminación. Sin embrago no tiene ningún tipo de sistema de alarma independiente o monitoreada, y a su vez no consta con un seguro de robo o calamidades. Después de entrevistar a los usuarios de esta vivienda; ellos

expresaron cierto aprecio por este tipo de desarrollo ya que esta vivienda fue robada una vez en el pasado y ellos son parte de las estadísticas que nunca denunciaron el hecho. Por esta razón sus testimonios resultan utiles para esta investigación, ya que muestra que los usuarios que cuentan con este sistema quedan satisfechos. A continuación podrán leer las cortas entrevistas que fueron realizados a los usuarios de esta vivienda.

8.2.1 Usuario #1:

"Este sistema nos ha facilitado la vida a todos, empezando por que no tengo que sacarle duplicado de las llaves a mis hijos cada ves que las pierden. En cuanto al sistema de iluminación nos brinda mas seguridad, yo soy la cabeza de familia por lo tanto tengo que viajar mucho por mi trabajo, y mis hijos no siempre están en la casa, por lo cual es un blanco fácil para los rateros. Sin embrago con este sistema se simula presencia por lo cual los ladrones ven mi casa como un imposible ya que creen que siempre esta alguien ahí. Es una bendición en altas horas de la noche, nunca más he tenido que entrar a oscuras y tambalearme buscando un interruptor de la luz, cada vez que abro mi puerta encuentro las luces de bienvenida prendidas[10]".

8.2.2 Usuario #2:

"Bueno, este sistema me ha facilitado la vida en diferentes formas. Para empezar siempre perdía las llaves o las dejaba adentro de la casa, siempre las considere un estorbo en mis bolsillos, o me picaban las piernas o me rallaban el celular. Desde la instalación de este sistema me quite el karma de las llaves por que ahora solo lo que necesito son mis dedos. Yo trabajo los fines de semana en un Bar, como mesero por lo cual siempre llego los fines de semana a altas horas de la noche y con un nivel de cansancio alto por así decirlo. Con este sistema no tengo que buscar las luces para poder bajar las escaleras, o entrar a la cocina, cada vez que abro la puerta las luces están dándome la bienvenida a mi casa después de una noche larga de trabajo. También me parece muy importante que este sistema simula presencia en el hogar, ya que la mayoría de los fines de semana nadie se encuentra en la casa a esas horas, o yo estoy trabajando o mi padre esta de viaje, en algunas ocasiones ambas situaciones se presentan en conjunto, por lo cual nos es atemorizante no tener ningún sistema de seguridad, pero ya con este instalado podemos dejar nuestro hogar sin mayor preocupación[11]".

Basado en estos testimonios de los usuarios del hogar en el cual fue instalado este sistema, se cree que el desarrollo de este proyecto fue todo un éxito debido a la respuesta de la gente y su funcionalidad. Es un sistema de seguridad de alta tecnología y a su vez es de gran utilidad, es de fácil comprensión y de un bajo costo, en comparación con los otros sistemas de seguridad en el mercado.

[10] Usuario 1: Cormaría Arboleda Murillo. Edad: 60 años.
[11] Usuario 2: Carolina Ochoa Arboleda. Edad: 24 años.

9. DESARROLLO INGENIERIL

La biometría es el estudio de métodos automáticos para el reconocimiento único de humanos en uno o más rangos conductuales o físicos intrínsecos. La "biometría informática" es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para “verificar” identidades o para “identificar” individuos[12]. Bajo los parámetros que se muestran y se comparan en la tabla a continuación, se escogió la cerradura de huella dactilar y no otras que manejan diferentes tecnologías, que se ofrecen en el mercado.

Tabla 10. Comparativo de las tecnologías biométricas más comunes.

Tecnología	Como Trabaja	Tamaño plantilla (bytes)	Fiabilidad	Facilidad De Uso	Posibles Incidencias	Costo	Aceptación Usuario
Huella digital	Captura y compara patrones de la huella digital	250-1000	Muy alta	Alta	Ausencia de miembro	Bajo	Alta
Geometría de la mano	Mide y compara dimensiones de la mano	9	Baja	Alta	Edad, Ausencia de miembro	Bajo	Alta
Retina	Captura y compara los patrones de la retina	96	Baja	Baja	Gafas	Alto	Baja
Iris	Captura y compara los patrones del iris	512	Baja	Baja	Luz	Muy alto	Baja
Geometría facial	Captura y compara patrones faciales	84 o 1300	Baja	Baja	Edad, Cabello, luz	Medio	Baja
Voz	Captura y compara cadencia, pitch, y tono de la voz	10000-20000	Alta	Media	Ruido, temperatura y meteorología	Alto	Media

[12] Tomado de la página de Internet: http://es.wikipedia.org/wiki/Biometr%C3%ADa. Recuperada 25 de junio del 2007.

Firma	Captura y compara ritmo, aceleración, y presión de la firma	1000 - 3000	Alta	Media	Edad, cambios, analfabetismo	Alto	Media

9.1 Análisis de la aplicación

El desarrollo logrado por esta investigación, es el combinar una cerradura de huella dactilar con un sistema de procesamiento de datos controlador de la tecnología Z-Wave. De esta forma podremos reemplazar las cerraduras existentes y aumentar la seguridad de las viviendas o lugares de trabajo.

El sistema de biometría propuesta en este proyecto es el reconocimiento de huella dactilar, ya que es de los más confiables y los que mayor tasa de estabilidad tiene. La huella dactilar de un humano es única como una firma y no es reproducible de manera fraudulenta.

La tecnología de domótica propuesta para esta solución es Z-wave, esta decisión fue tomada basándose en las características de radio frecuencia, su red de acople de dos vías y su protocolo de comunicación basado en GFSK por sus siglas en inglés.

Es importante recalcar que al lograr fusionar estas dos tecnologías, el incremento en seguridad para el hogar o recintos de trabajo aumenta en forma drástica y a un bajo costo, de igual manera aumenta la eficiencia y comodidad de las mismas.

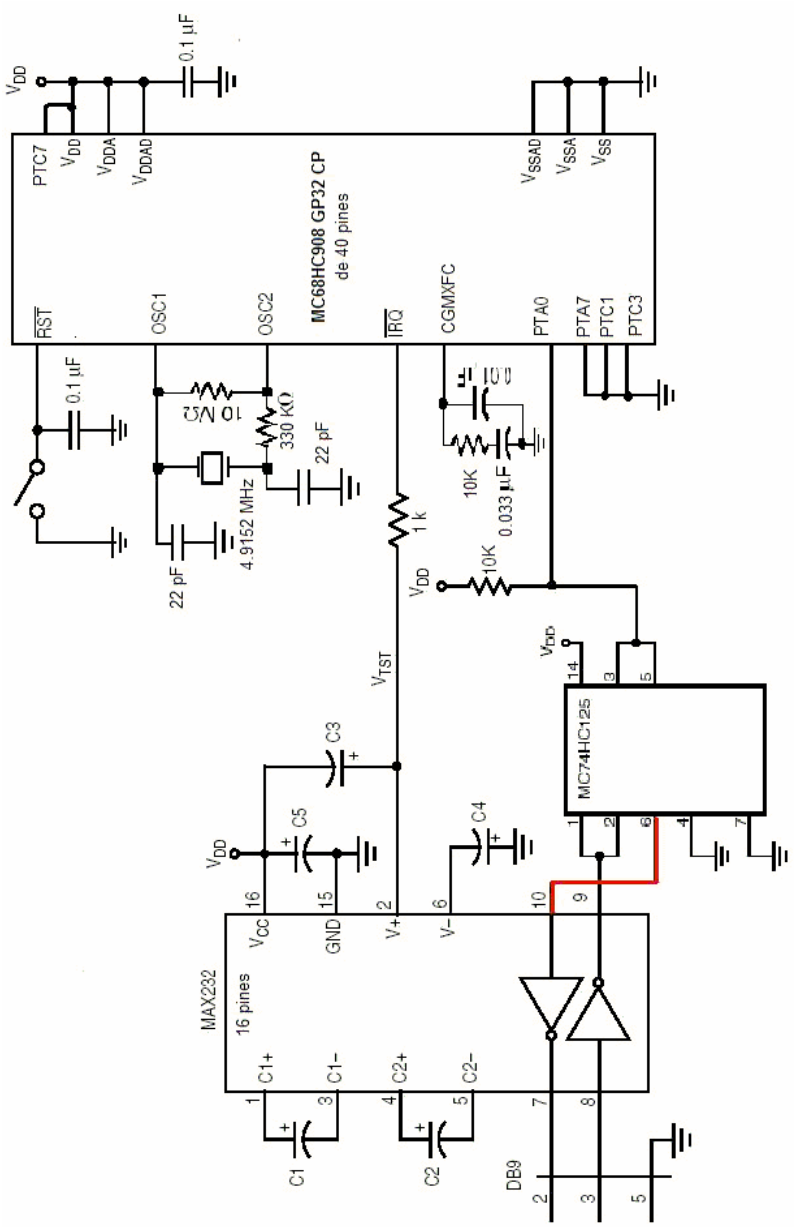
9.2 Diseño propuesto para esta aplicación

El diseño propuesto para esta aplicación está basado en el desarrollo a través de microcontroladores. Para este caso en específico, se utilizará un microcontrolador fabricado por motorola. Este microcontrolador tiene el número de referencia MC68HC908 GP32 CP. Este es un microntrolador de 40 pines, con la capacidad de tener comunicación serial. Esta trabaja a un baudaje de 9600 bitts por segundo, lo cual facilita la comunicación con el puerto USB, que trabaja con la misma velocidad. De esta manera es evidente que resulta esencial ya que después será convertida de serial a USB. La conversión es necesaria ya que el módulo de comunicación a utilizar, es un USB fabricado específicamente para cumplir con los protocolos de comunicación de la tecnología Z-Wave. La velocidad de trabajo de este modulo es de 9600 baudios.

El módulo USB es fabricado por Intermatic y su base de programación es en C#, la cual será llevada a lenguaje ensamblador. Esta conversión de lenguaje de

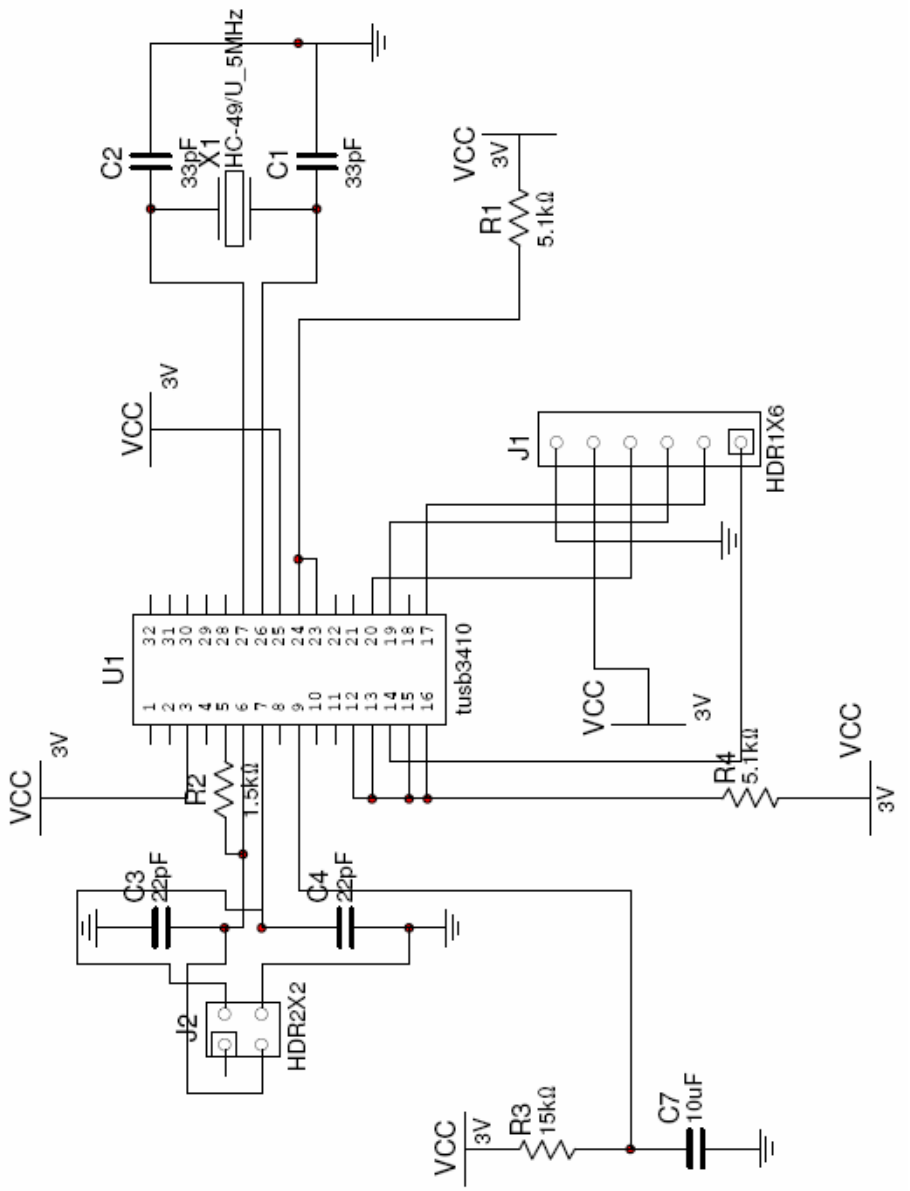
programación se hará a través de una versión gratuita del programa *Code Warrior.* Se utilizará la programación en lenguaje C, ya que es más sencillo construir las diferentes subrutinas y el programa en general; ayudando a ahorrar espacio y des esta forma dejando lugar en la memoria para diferentes expansiones, que se hagan en el futuro. La programación se llevará a cabo a través del esquema básico del programador sugerido por el fabricante, ya que es la forma más segura de obtener un funcionamiento óptimo. El esquema de este programador es el siguiente.

Figura 13. Modulo de programación.



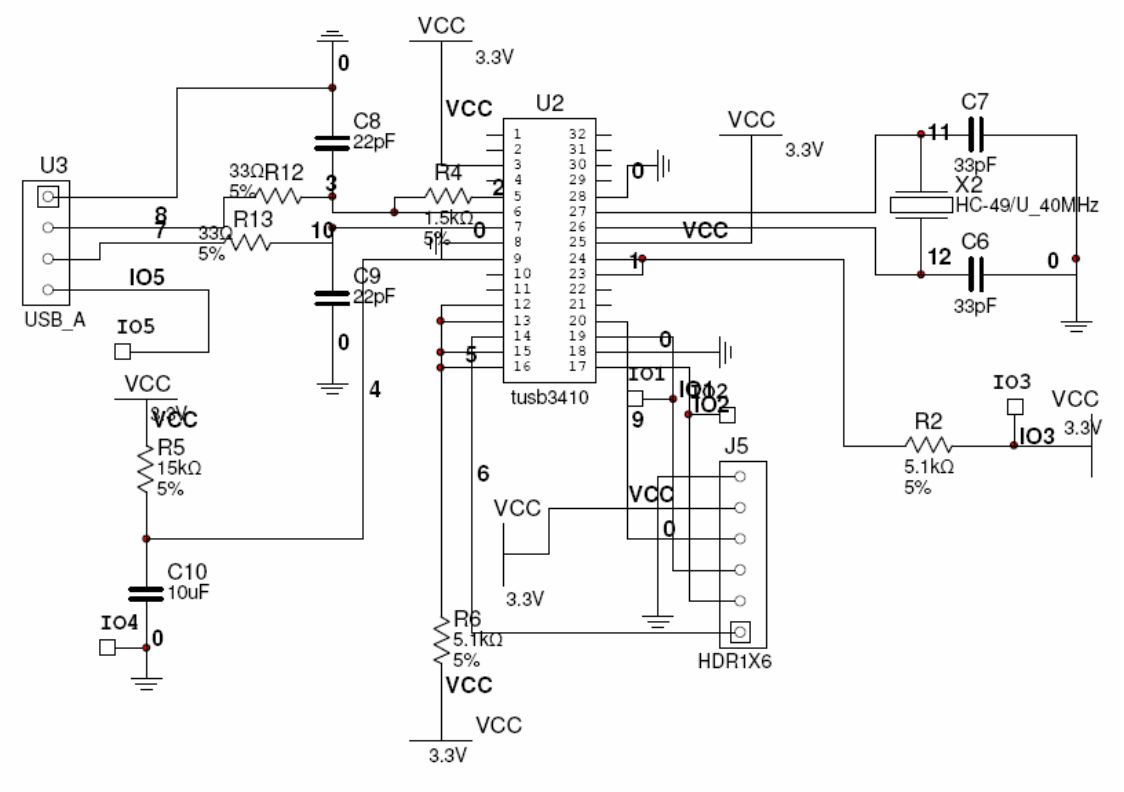
Este microprocesador se programará a través de una versión gratuita de Microsoft Visual Estudio, en el cual es posible programar en C o un Visual Basic. De esta forma no será posible exportar el Código al programa Code Warrior, mediante el cual se traducirá el código escrito en C a ensamblador. Una vez se lleve a cabo la programación de este, se utilizará el conversor de comunicación serial a USB, lo cual nos permitirá emitir las diferentes señales necesarias para lograr los diferentes escenarios y modelos de seguridad propuestos previamente. El esquema del conversor de comunicación serial a USB es el siguiente:

Figura 14. Modulo de funcionamiento.



Con una conexión entre el microcontrolador y el conversor de comunicación serial a USB, se podrá emitir y recibir las diferentes señales de radio frecuencia para poder obtener las diferentes aplicaciones que fueron propuestas por este proyecto. El esquema de esta conexión es la siguiente:

Figura 15. Modulo de funcionamiento con TUSB3410.



Este sistema estará conectado a una cerradura biométrica de huella dactilar, de tal forma que cuando el microcontrolador reciba una señal eléctrica a uno de sus puertos, este interpretará que la cerradura autenticó una huella dactilar y procederá a emitir las señales de radio frecuencia pertinentes para el caso dependiendo de la hora del día y del estado previo del sistema. Esta cerradura es fabricada por ADEL Security Locks, la cual fue descrita previamente con sus dividas especificaciones. Esta es la estructura interna de la cerradura biométrica la cual es utilizada:

Figura 16. Circuitería interna de la cerradura biométrica.

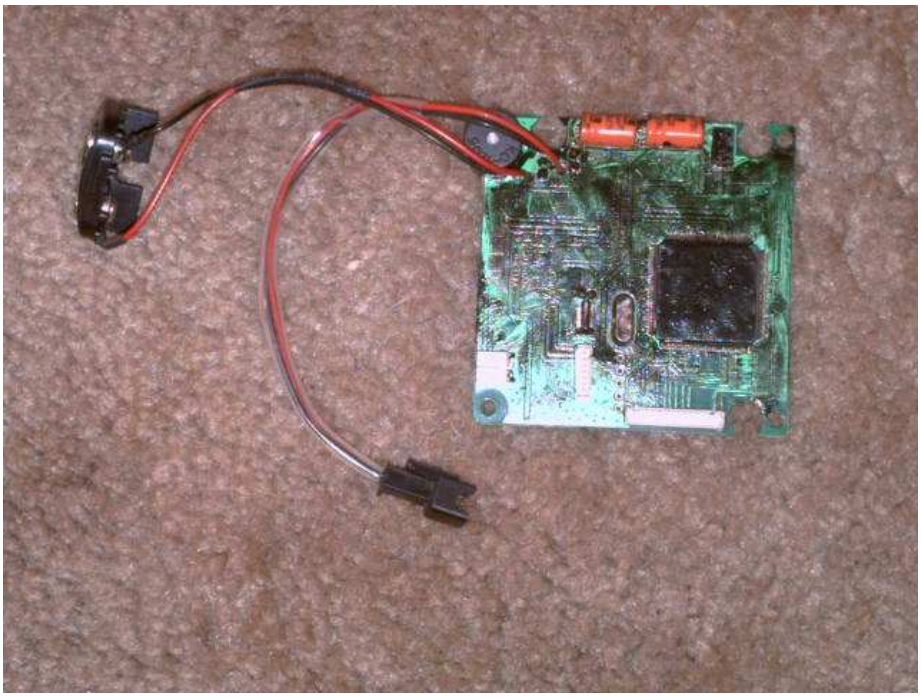


Figura 17. Circuitería interna de la cerradura biométrica.

Figura 18. Funcionamiento interno mecánico de la cerradura biométrica.

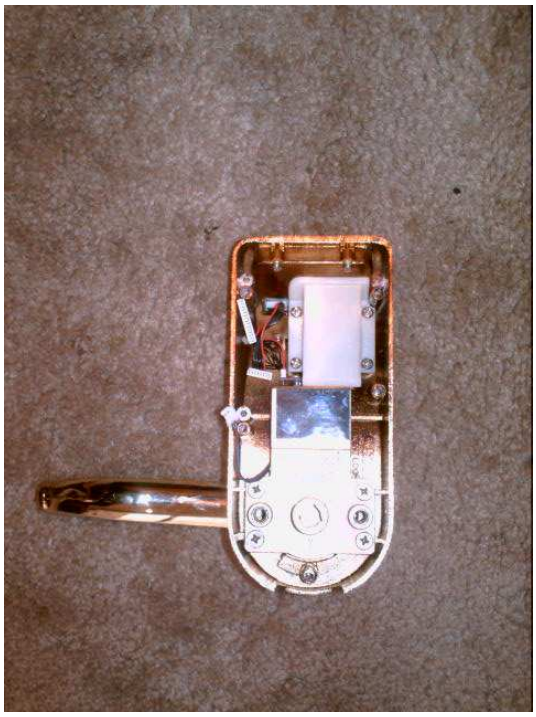
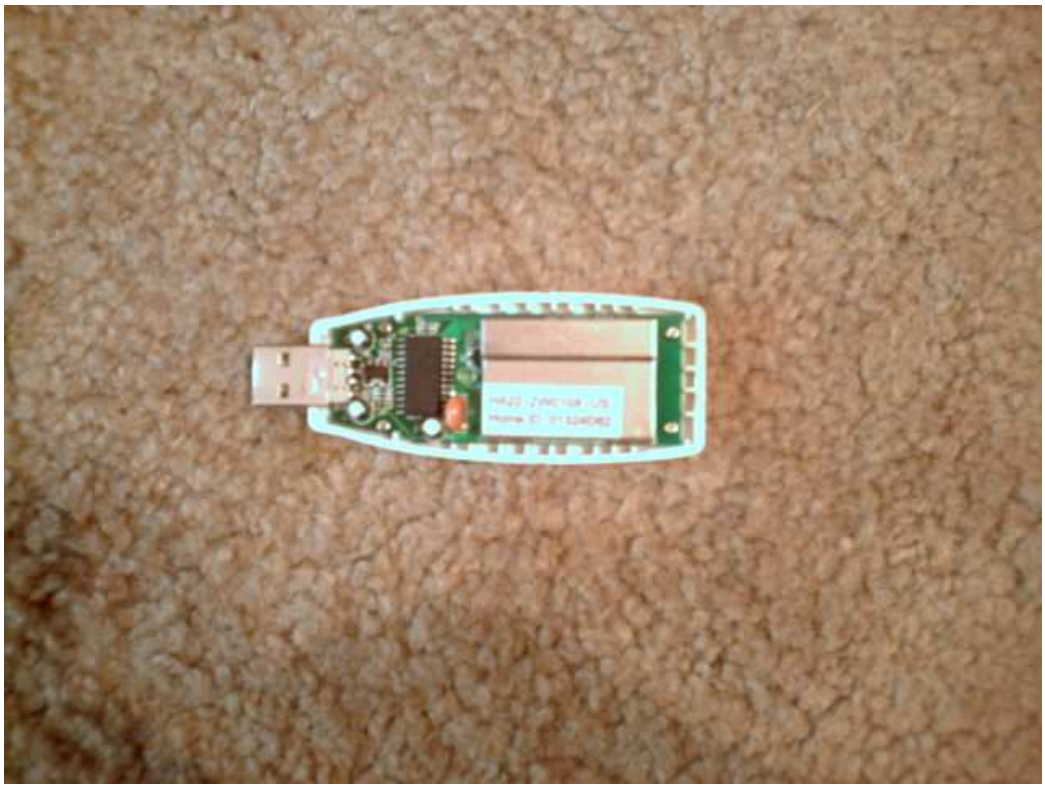


Figura 19. Exterior de la cerradura biométrica.

Como es posible visualizar en estas imágenes, todos los componentes electrónicos que son utilizados por esta empresa fabricante de esta tecnología, es imposible ver la referencia de estos y no es fácil descifrar el plano eléctrico que esta impreso el la váquela. A su vez también es posible ver en el interior, el sensor lector de huellas dactilares que está muy bien asegurado, y el desmantelarlo no revelará ningún dato importante, o algo que aporte a este proyecto.

Las señales que serán emitidas por este sistema tienen que ser compatibles con la tecnóloga Z-Wave. Para este caso se utilizó un emisor USB compatible con la tecnología, que es fabricado por la empresa INTERMATIC. Este emisor USB cumple con todas las normas impuestas por la FCC (Federal Comunication Comitte) y con las normativas internacionales de uso de frecuencia libre. Para que el dispositivo de la cerradura biométrica sea compatible con la tecnología Z-Wave es imprescindible utilizar este emisor, ya que incluye el micro chip Z-Wave para la emisión y recepción exacta de estas señales. A continuación las imágenes de este emisor:

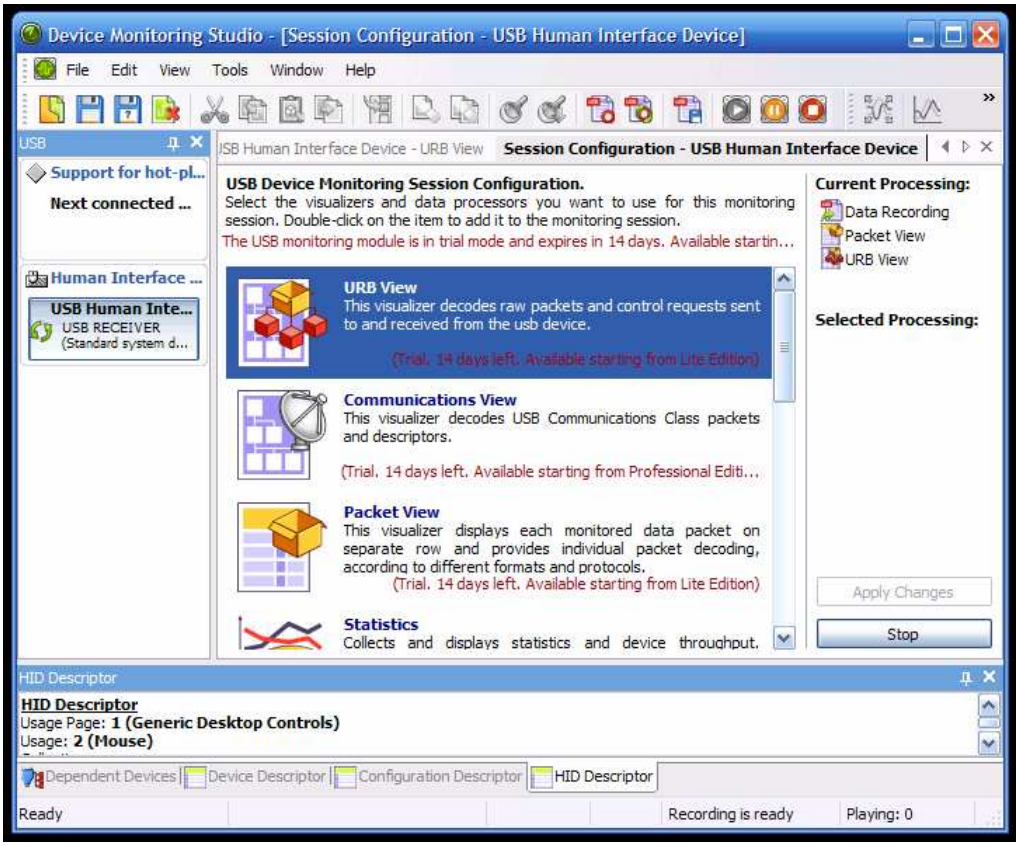
Figura 20. Emisor de frecuencia Z-Wave.



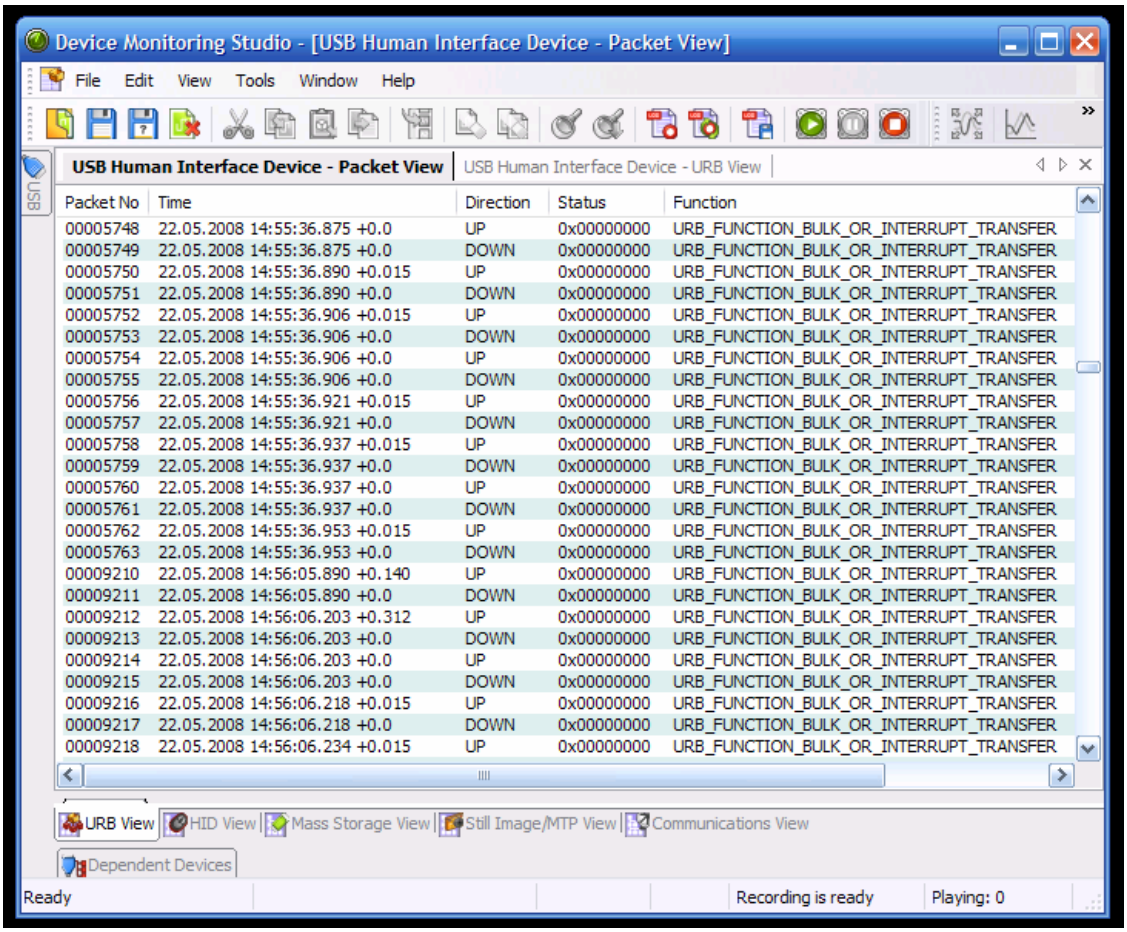
Una vez la conexión entre el sistema de procesamiento de datos y el sistema de cerradura sea logrado, entra a jugar el programa escrito para el control de esta aplicación. Este programa pone al microcontrolador en estado de escucha, en un

puerto determinado. Una vez la cerradura emita la señal de acceso otorgado, el micro controlador recibe la señal y ejecuta el programa por el puerto serial. Este programa inicia todos los puertos necesarios y llama a librería, donde se lleva a cabo la emulación del driver principal para el sistema emisor. De esta forma es posible emitir la señal de radio frecuencia para logar el propósito deseado de forma satisfactoria. Antes de poder escribir este programa, fue necesario llevar a cabo un procedimiento previo que consistió en estudiar el puerto USB del computador donde el adaptador USB Z-Wave estaba conectado. Se llevó a cabo este estudio, mientras se prendía y apagaba un controlador de aplicaciones. De esta forma se pudo identificar los paquetes enviados con la información pertinente. Después de identificar el código de estos paquetes fue fácil identificar las instrucciones de prendido y apagado, y la forma de direccionamiento mediante la cual se logra la comunicación. Este estudio del puerto USB fue llevado a cabo mediante un software gratuito llamado USB Monitor, mediante el cual fue posible visualizar los paquetes de comunicación y estudiar su estructura. A continuación las imágenes del proceso llevado a cabo:

9.2.1 GUI de interface Principal

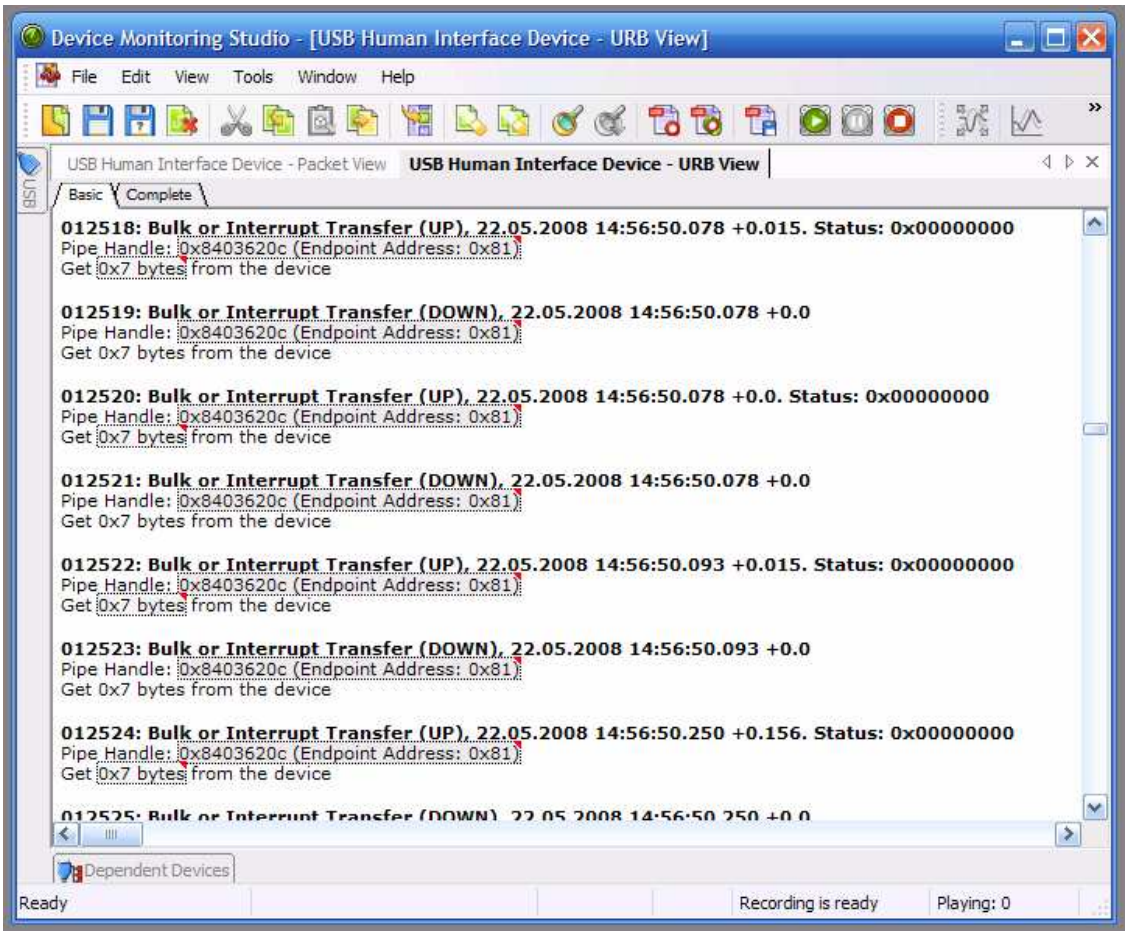


9.2.2 Visualización de paquetes en formato RAW



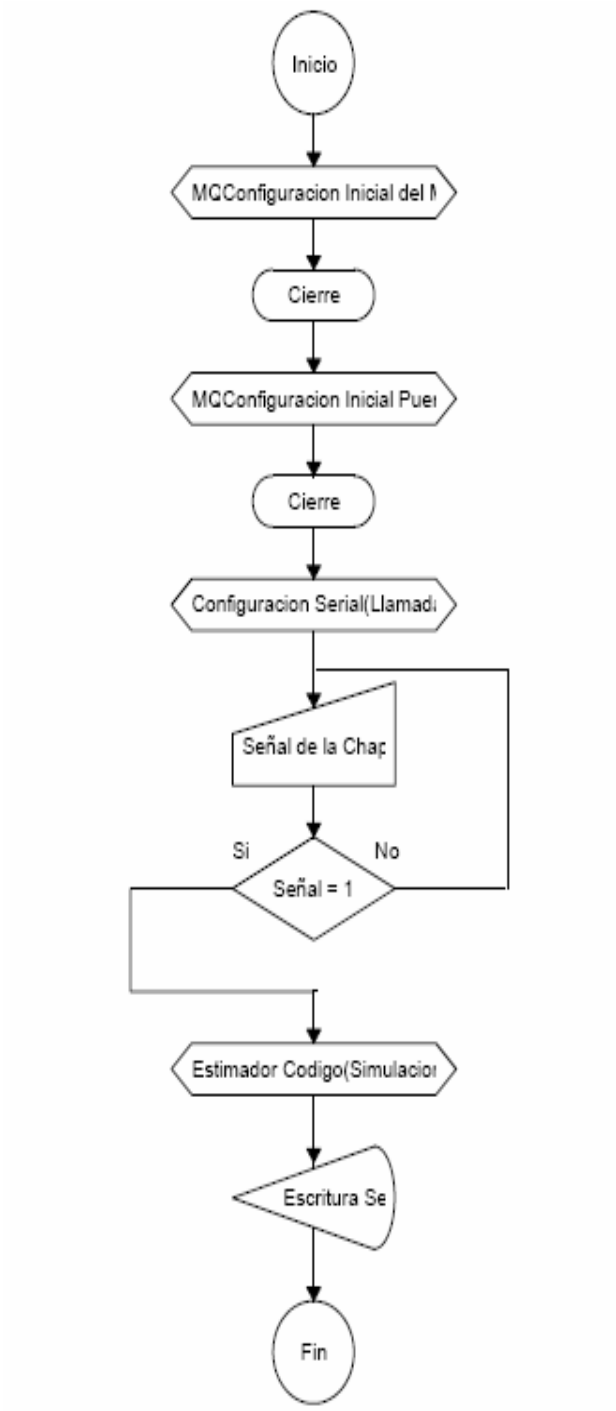
En esta imagen es posible ver los diferentes paquetes de comunicación enviados por la interface USB. De esta forma fue posible estudiar el modelo de comunicación propuesto para el diseño de la aplicación. La siguiente imagen muestra los paquetes decodificados y sus direcciones respectivas en ASCI. De esta forma fue posible lograr replicar el driver en el microcontrolador, y a su vez emitir las instrucciones necesarias para el prendido y apagado de diferentes aplicaciones.

9.2.3 Visualización de paquetes decodificados

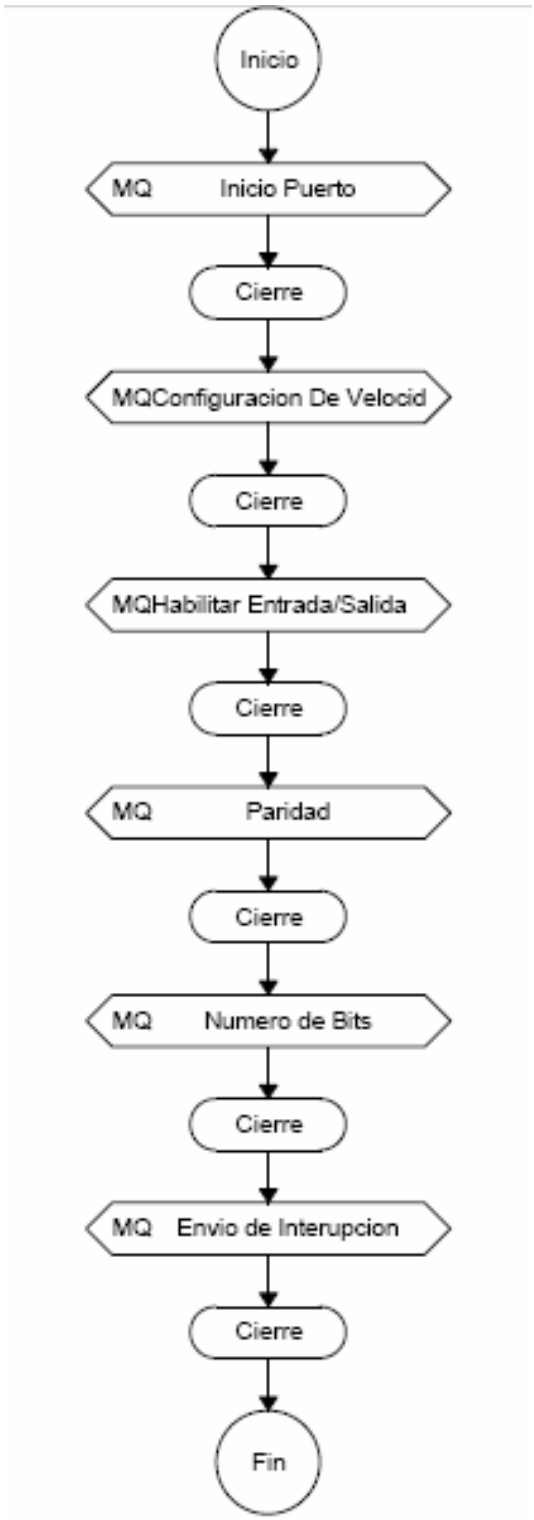


Después de lograr todo este estudio e investigación fue posible escribir el software necesario para el microcontrolador. Su respectivo diagrama de flujo puede ser visto a continuación, donde se ilustra el funcionamiento total con el uso respectivo de las librerías pertinentes para el caso dado.

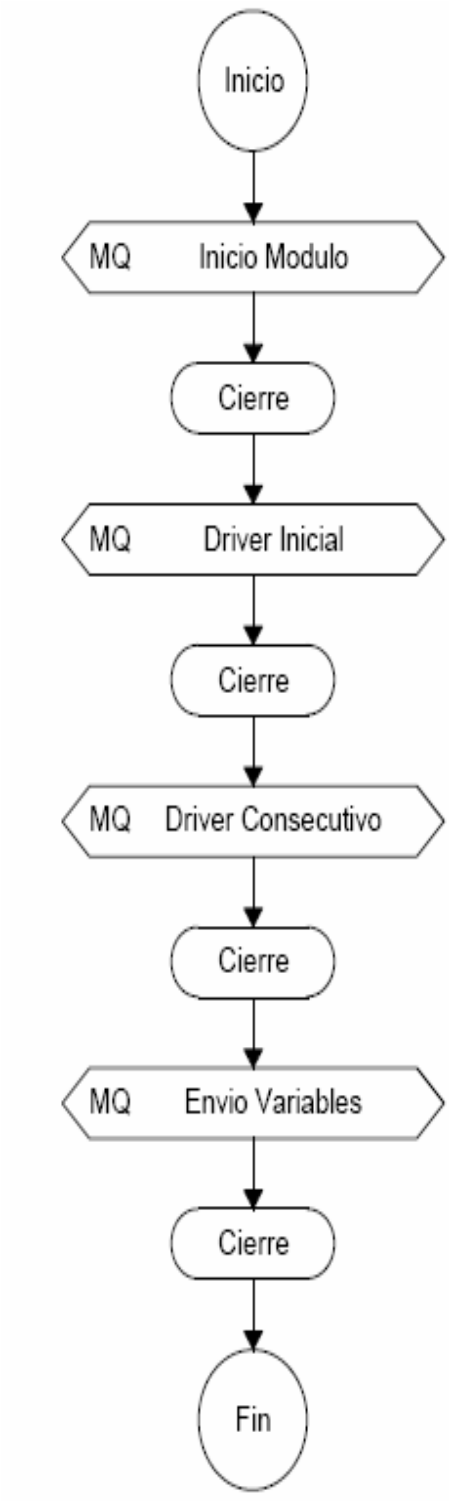
9.3 Diagrama de flujo, programa principal:



9.4 Diagrama de Flujo, librería Serial:



9.5 Diagrama de Flujo, Emulador del Driver:



El código del programa a ejecutar por el microcontrolador fue escrito en C y después traducido a asembler utilizando la aplicación gratuita de Code Warrior. El programa de ejecución es el siguiente:

```
$include 'gpgtregs.inc'

FLASH        EQU  $8000

RAM          EQU  $0040

VectorStart  EQU  $FFDC


        org RAM

del  ds 1

del1 ds 1

del0 ds 1

korn ds 1

war  ds 1

b1   ds 1

b2   ds 1

b3   ds 1

aux  ds 1

flag ds 1

        org FLASH

$include 'sci_ini.inc'

confini:

        bset   0,CONFIG1            ;deshabilita el cop

        rsp                         ;RESETEO DEL SP
```

```
        cli                     ;permite que ocurra una interrupcion
        clc                     ;inicia en 0 el carry
        clra                    ;limpia el acumulador
        MOV    #$01,CONFIG2

        mov    #%00000001,DDRB
        CLR    PTB
          MOV    #$30,b1
          MOV    #$00,b2
          MOV    #$d9,b3
          MOV    #$01,flag

          clr    aux

         jsr    sci_ini

inicio
           brclr  1,PTB,*

           mov    b1,SCDR
        BSET   0,PTC
        brclr  6,scs1,*
```

```
mov   b2,SCDR
BSET  0,PTC
brclr  6,scs1,*


mov    b3,SCDR
BSET   0,PTC
brclr  6,scs1,*

  LDA            b1
  adc    #$01
  STA    b1

  BRSET 0,flag,uno
BRCLR 0,flag,tres
  jmp inicio
```

```
uno
        LDA         b3
        SUB   #$01
        STA   b1
        BCLR  0,flag
tres
        LDA         b3
        add   #$03
        STA   b1
        Bset  0,flag

      MOV    #$30,ADCLK
      MOV    #$60,ADSCR
ciclo:
      nop
      jmp    ciclo

*************************************************************

dummy_isr:
        rti        ; return
```

```
save:
        mov     adr,SCDR
        brclr   7,scs1,*
        RTI
        RTI
        wait

************************************************************

     org  VectorStart

       dw  dummy_isr    ; Time Base Vector
       dw  save         ; ADC Conversion Complete
       dw  dummy_isr    ; Keyboard Vector
       dw  dummy_isr    ; SCI Transmit Vector
       dw  dummy_isr    ; SCI Receive Vector
       dw  dummy_isr    ; SCI Error Vector
       dw  dummy_isr    ; SPI Transmit Vector
       dw  dummy_isr    ; SPI Receive Vector
       dw  dummy_isr    ; TIM2 Overflow Vector
       dw  dummy_isr    ; TIM2 Channel 1 Vector
       dw  dummy_isr    ; TIM2 Channel 0 Vector
       dw  dummy_isr    ; TIM1 Overflow Vector
```

```
dw  dummy_isr    ; TIM1 Channel 1 Vector
dw  dummy_isr    ; TIM1 Channel 0 Vector
dw  dummy_isr    ; ICG/CGM Vector
dw  dummy_isr    ; ~IRQ1 Vector
dw  dummy_isr    ; SWI Vector
dw  confini      ; Reset Vector
```

9.6 Proceso de Fabricación

El Proceso de fabricación para este sistema de procesamiento de datos fue llevado a cabo en Microcircuitos S.A. la váquela es de 7cm X 7cm, con un espesor de 1.2mm. Le fue agregado SilkScreen para los componentes y antisolder verde, para poder diferenciar el camino de los circuitos de forma sencilla y evitar cortos circuitos. Las siguientes imágenes fueron creadas para poder realizar esta váquela con precisión y de acuerdo con el diseño final:

Figura 21. Negativo A para fabricación de baquela.

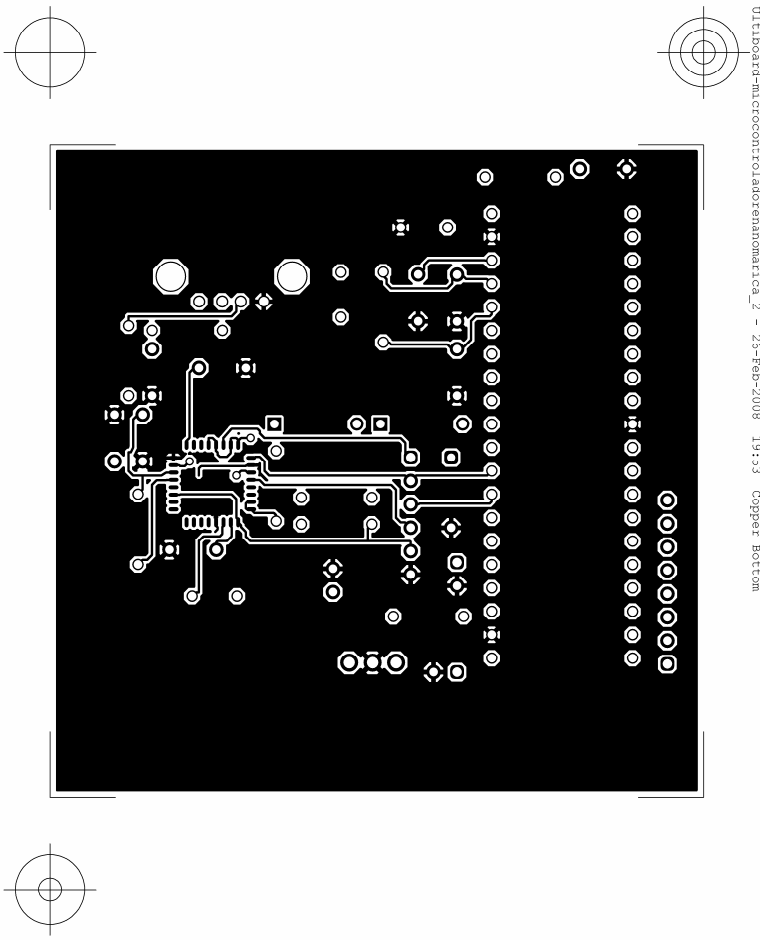


Figura 22. Lado B para fabricación de baquela.

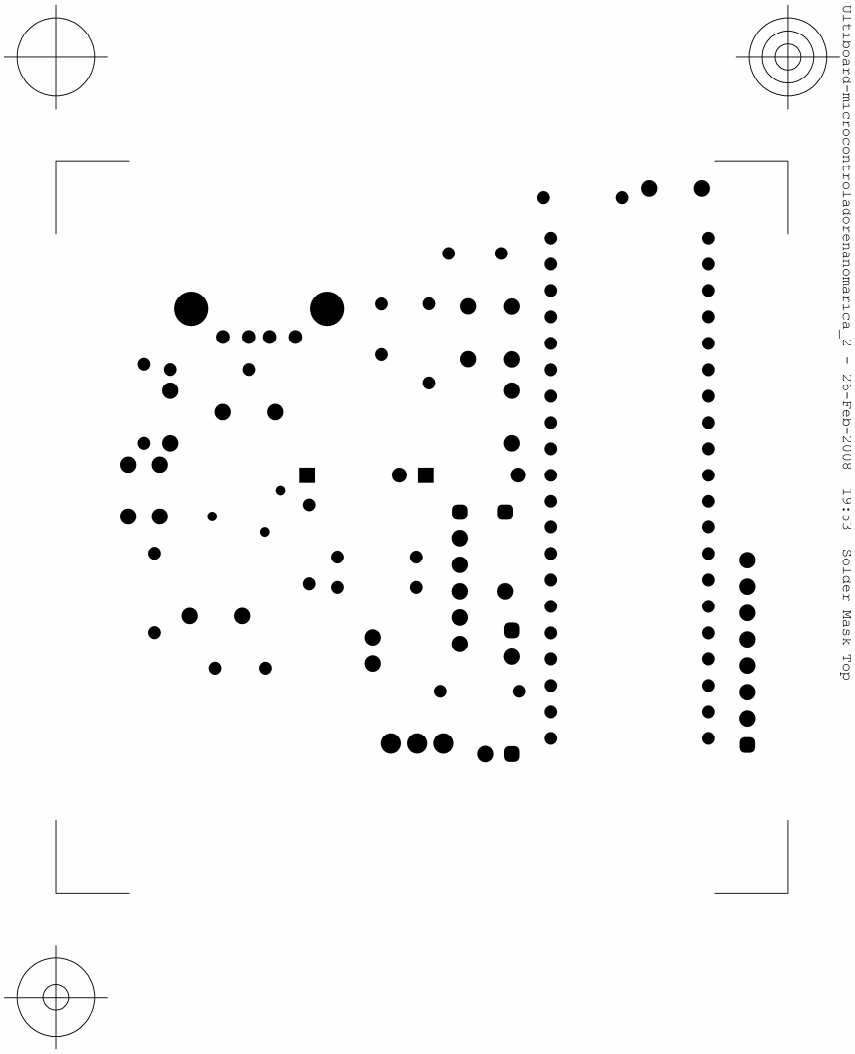
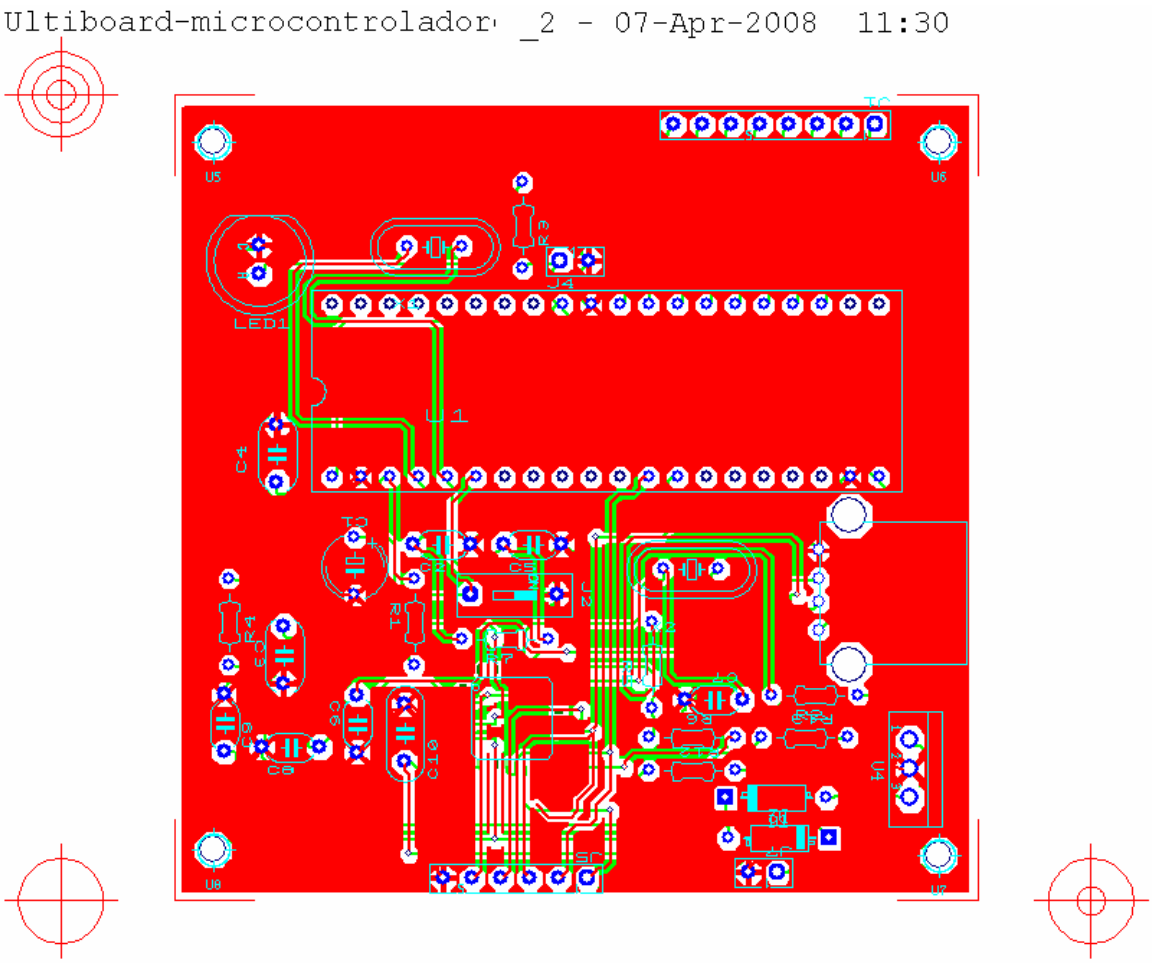
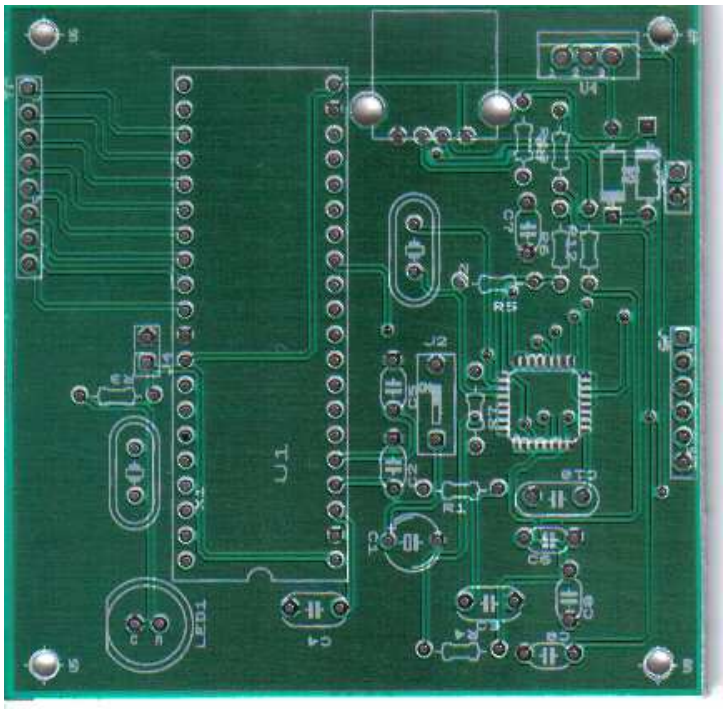


Figura 23. Diagrama completo de la baquela.

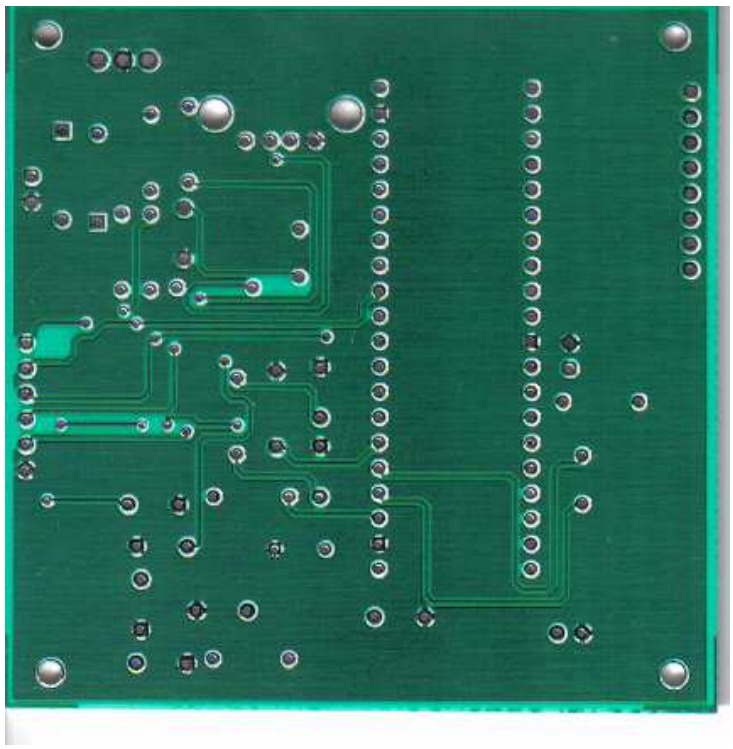


Una vez llevado a cabo este proceso de fabricación, obtenemos la váquela final sobre la cual soldaremos todos nuestros componentes electrónicos. Las siguientes imágenes muestran la váquela terminada con y sin componentes electrónicos soldados sobre esta:

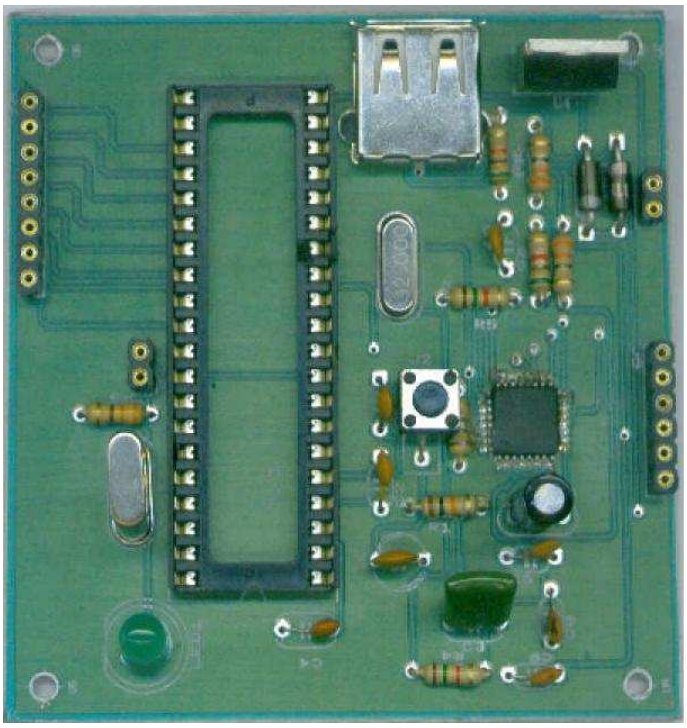
- **Baquela lado A**



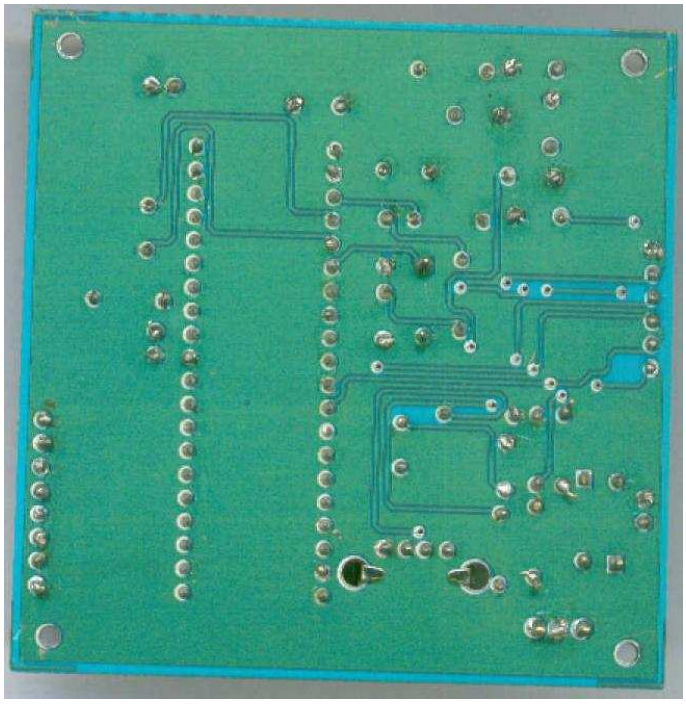
- **Baquela lado B**



- **Baquela lado A con componentes electrónicos**



- **Baquela lado B con componentes electrónicos:**



Una vez estén los componentes electrónicos soldados sobre la váquela, se puede proseguir a hacer la conexión física entre el sistema de cerradura y el sistema de procesamiento de datos. Esta conexión física consiste en obtener el pulso emitido por el sistema de cerradura, el cual activa el sistema de embrague para lograr una apertura exitosa. Una vez obtenido este pulso, obtenemos una conexión directa al puerto de entrada del microcontrolador esta es la única conexión física ya que es el único dato necesario para la operación del sistema. A continuación es posible ver las imágenes de la conexión física, entre el sistema de cerradura y el sistema de procesamiento de datos:

Figura 24. Conexión entre la cerradura biométrica y el sistema de procesamiento de datos.

10. CONCLUSIONES

Mediante la realización de este proyecto fueron claras las debilidades y fortalezas del mismo. La fortaleza mas grande que se puede considerar es el factor de aumento de seguridad asequible para todos los estratos, especialmente para los estratos menos privilegiados.

Otra fortaleza muy importante, o se podría decir que un futuro alcance, es la factibilidad de realizar la programación de este sistema de procesamiento de datos mediante redes neuronales, de tal forma que el sistema de procesamiento de datos pueda identificar una serie de patrones naturales que llevan a cabo los inquilinos del hogar o el establecimiento de trabajo. Así el sistema de procesamiento de datos podrá activar los diferentes equipos sin tener que programar tiempos de encendido ni secuencias necesarias.

La debilidad más grande de este proyecto es la fusión entre el emisor USB y el microcontrolador, ya que se dificultó la programación de este. Fue difícil hacer que el microcontrolador corriera las diferentes subrutinas, las cuales llevaban a cabo los diferentes escenarios y hacer que la emisión de la señal con los paquetes de la información fuera la precisa para lograr lo mencionado.

Dada la previa investigación y análisis del puerto USB llevado a cabo con el programa USB monitor, fue posible identificar los diferentes parámetros necesarios para esta programación. Sin este software no hubiera sido posible la comunicación que se logró, ya que hubiera sido imposible identificar los paquetes y el protocolo exacto de comunicación entre el módulo USB y los diferentes artilugios Z-Wave.

Fue imposible encontrar el algoritmo utilizado por la cerradura biométrica, el cual es utilizado para codificar y reconocer las diferentes huellas dactilares. Por lo tanto no fue posible programar un escenario diferente para cada usuario del recinto, esto es una debilidad clara pero para etapas futuras del proyecto será posible utilizar un algoritmo de biometría propio. De tal forma se podrá lograr el emparejamiento entre usuario y escenario predeterminado.

Como fue mencionado previamente la comunicación serial y USB fue bastante compleja, no solo desde el punto de vista de la electrónica, si no que su tamaño fisico fue un problema por sí solo. Esto es un contratiempo ya que cuando el sistema se va a implementar en la vida cotidiana, ya sea para un hogar o un recinto laboral, este es de gran volumen y es bastante notorio y podría llegar a estorbar en la puerta en la que se implemente

11. RECOMENDACIONES

Como fue mencionado previamente, la debilidad más fuerte que fue hallada en este proyecto, fue la conversión de comunicación serial a USB y la utilización del espacio de la misma. Para el futuro se recomienda la utilización de una micro chip de la tecnología Z-Wave, de tal forma que no sea necesario la conversión de comunicación serial a USB, y de igual forma se podría reducir el espacio a utilizar en el sistema de procesamiento de datos y hacer el módulo de acoplado de un menor tamaño. Esta tecnología no fue utilizada en este proyecto debido a que es un avance tecnológico reciente, y no fue una opción en el momento de la investigación ni en la etapa de desarrollo.

Como es posible visualizar en estas imágenes, todos los componentes electrónicos que son utilizados por la empresa fabricante de esta tecnología, es imposible ver la referencia de estos y no es fácil descifrar el plano eléctrico que esta impreso el la váquela. A su vez también es posible ver en el interior el sensor lector de huellas dactilares, el cual esta muy bien asegurado y el desmantelarlo no revelaría ningún dato importante o algo necesario para el aporte de este proyecto.

12. Bibliografía

- Alderman, Ellen., & Kennedy, Caroline. (1997). The Right to Privacy. Primera Edición. EE.UU.: First Vintage Books Edition.
- American Psychological Association. (2002) Manual de estilo de publicaciones de la American Psychological Association (adaptado para el español por Editorial El Manual Moderno) (2ª. Ed.). México D.F.: Manual Moderno.
- Chirillo, John., & Blaul, Scott. (2003). Implementing Biometric Security. Primera Edición. EE.UU.: Wiley.
- Diccionario Esencial de la Real Academia de la Lengua Española. (2001). Segunda Edición. España: Espasa.
- Jain, Anil K., & Flynn, Patrick. Handbook of Biometrics. (2007). Primera Edición. Michigan State University, EE.UU.: Springer.
- Lee, Henry C., & Gaensslen, R.E. (2001). Advances in Fingerprint Technology. Forensic and Police Science Series. Segunda Edición. EE.UU.: CRC Press.
- Ratha, Nalini., & Bolle, Ruud. (2004). Automatic Fingerprint Recognition Systems. Primera Edición. EE.UU.: Springer.
- Wayman, James., & Jain, Anil., & Maltoni, Davide., Maio, Dario. (2005). Biometric Systems: Technology, Design and Performance Evaluation. Primera edición. EE.UU.: Springer.
- Woodward Jr. John D., & Orlans Nicholas M., & Higgins Peter D. (2002). Biometrics, identity assurance in the information age. Primera edición. EE.UU.: McGraw-Hill Osborne Media.
- Woodward Jr., John D., & Webb, Katharine W., & Newton, Elaine M., & Bradley, Melissa., & Rubenson, David. (2001). Army Biometric Applications: Identifying and Adressing Sociocultural Concerns. Recopilación de Papers. EE.UU.: Rand.
- Página de Internet Wikipedia. http://es.wikipedia.org/wiki/Domótica. Recuperada el 8 de octubre del 2006.
- Página de Internet: KNX Association. http://www.knx.org/knx-standard. Recuperada el 8 de octubre del 2006.
- Página de Internet X10 PRO. http://www.x10pro.com/pro/pdf/technote.pdf Recuperada el 9 de octubre del 2006.
- Página de Internet ZigBee Alliance. http://www.zigbee.org. Recuperada el 9 de octubre del 2006.
- Página de Internet OSGI Alliance: http://www.osgi.org/osgi_technology/index.asp?section=2. Recuperada el 10 de octubre del 2006.
- Página de Internet Universal Plaug and Play. http://www.upnp.org/. Recuperada el 10 de octubre del 2006.

13. Anexos

- **Anexo 1: Resolución del Ministerio de Comunicaciones de la República de Colombia.**

DIARIO OFICIAL 45.533 MIERCOLES 28 de ABRIL de 2004

RESOLUCION NUMERO 000689 DE 2004

Por la cual se atribuyen unas bandas de frecuencias para su libre utilización dentro del territorio nacional, mediante sistemas de acceso inalámbrico y redes inalámbricas de área local, que utilicen tecnologías de espectro ensanchado y modulación digital, de banda ancha y baja potencia, y se dictan otras disposiciones.

La Ministra de Comunicaciones, en el ejercicio de sus facultades legales, en especial de las que le confieren la Ley 72 de 1989, el Decreto-ley 1900 de 1990, el Decreto 1620 de 2003, y el Decreto 1972 de 2003, y…

CONSIDERANDO:

Que el inciso 1º del artículo 75 de la Constitución Política establece: "El espectro electromagnético es un bien público inenajenable e imprescriptible sujeto a la gestión y control del Estado. Se garantiza la igualdad de oportunidades en el acceso a su uso en los términos que fije la ley"; Que el artículo 1º de la Ley 72 de 1989 establece que el Gobierno Nacional, por conducto del Ministerio de Comunicaciones, adoptará la política general del sector de comunicaciones y ejercerá las funciones de planeación, regulación y control de todos los servicios del sector; Que el artículo 18 del Decreto 1900 de 1990 establece que el espectro electromagnético es de propiedad exclusiva del Estado y como tal constituye un bien de dominio público, inenajenable e imprescriptible, cuya gestión, administración y control corresponden al Ministerio de Comunicaciones; Que según lo dispuesto en el artículo 19 del Decreto 1900 de 1990, las facultades de gestión, administración y control del espectro electromagnético comprenden, entre otras, las actividades de planeación y coordinación, la fijación del cuadro de frecuencias, la asignación y verificación de frecuencias, el otorgamiento de permisos para su utilización, la protección y defensa del espectro radioeléctrico, la comprobación técnica de emisiones radioeléctricas, el establecimiento de condiciones técnicas de equipos terminales y redes que utilicen en cualquier forma el espectro radioeléctrico, la detección de irregularidades y perturbaciones, y la adopción de medidas tendientes a establecer el correcto y racional uso del espectro radioeléctrico, y a restablecerlo en caso de perturbación o irregularidades; Que el numeral 32.6 del artículo 32 del Decreto 1972 de 2003 establece que "El uso del espectro radioeléctrico para aplicaciones industriales, científicas y médicas (ICM), así como para aparatos, equipos o sistemas cuya instalación y operación sean autorizadas de manera general y expresa por el Ministerio de Comunicaciones en las bandas y frecuencias atribuidas nacionalmente para el efecto, es libre"; Que el Comité Consultivo Permanente III

de la Comisión Interamericana de Telecomunicaciones CITEL, en su Recomendación CCP.III/REC.67 (XIX-2001) examinó el tema de los dispositivos de radiocomunicaciones de baja potencia, e instó a las administraciones de los países miembros a armonizar sus reglamentaciones sobre dichos dispositivos de radiocomunicaciones; Que el Comité Consultivo Permanente III de la Comisión Interamericana de Telecomunicaciones CITEL, en su Recomendación CCP.III/Res.122 (XVII- 2001), reconoció el interés de sus Estados miembros armonizar el desarrollo de los dispositivos WLAN en las bandas de frecuencias de 5150-5250 MHz, 5250- 5350 MHz y 5725-5825 MHz, y que su introducción internacional sería facilitada por la armonización de los países miembros, e instó a las Administraciones a considerar acciones apropiadas para que estas aplicaciones estén sujetas a procedimientos reconocidos de certificación y verificación; Que la Conferencia Mundial de Radiocomunicaciones CMR-03, decidió mediante la resolución COM 5/16-CMR-03, efectuar una atribución primaria para sistemas de acceso inalámbrico WAS incluidas las RLAN en las bandas de 5 150-5 250 MHz, 5 250-5 350 MHz y 5 470-5 725 MHz, e invitó a las Administraciones a adoptar la reglamentación apropiada para que los equipos funcionen de conformidad con dichas protecciones y a proseguir el trabajo sobre mecanismos reglamentarios y otras técnicas de atenuación, con el fin de evitar las incompatibilidades que pudieran resultar de la interferencia combinada como resultado de una posible proliferación del número de sistemas de acceso inalámbrico WAS/RLAN; Que en razón de los adelantos tecnológicos, se hace necesario atribuir, dentro del territorio nacional, para la operación sobre una base de no-interferencia y no protección de interferencia, unas bandas de frecuencias radioeléctricas para su libre utilización, en aplicaciones de telecomunicaciones que por su baja potencia puedan ser operadas sin que logren causar interferencia perjudicial a servicios de telecomunicaciones primarios o secundarios, con el fin de facilitar la coexistencia con otros servicios de telecomunicaciones, y ejercer un control efectivo sobre el uso del espectro radioeléctrico; En consecuencia,

RESUELVE:

T I T U L O I

DISPOSICIONES GENERALES

Artículo 1º. Objeto. La presente resolución tiene por objeto atribuir unas bandas de frecuencias radioeléctricas para su libre utilización dentro del territorio nacional, mediante sistemas de acceso inalámbrico y redes inalámbricas de área local, que utilicen tecnologías de espectro ensanchado y modulación digital, de banda ancha y baja potencia, en las condiciones establecidas por esta resolución.

Artículo 2º. Definiciones. Para los efectos de la presente resolución, se adoptan las definiciones que en materia de telecomunicaciones ha expedido la Unión Internacional de Telecomunicaciones, UIT, a través de sus Organismos Reguladores, y las definiciones que se establecen a continuación: Aplicaciones Industriales, Científicas y Médicas (ICM). Utilización de equipos destinados a producir y utilizar en un espacio reducido, energía radioeléctrica con fines industriales, científicos y médicos, domésticos o similares, con exclusión de todas las aplicaciones de telecomunicación.

Comunicación punto a punto. Comunicación proporcionada por un enlace radioeléctrico, entre dos estaciones situadas en unos puntos fijos determinados.
Comunicación punto multipunto. Comunicación proporcionada por enlaces radioeléctricos, entre una estación situada en un punto fijo determinado y un número de estaciones situadas en unos puntos fijos determinados.

Espectro ensanchado por salto de frecuencia (Frequency Hopping). Técnica de estructuración de la señal que conmuta automáticamente la frecuencia portadora transmitida; proceso que se realiza en forma seudoaleatoria a partir de un conjunto de frecuencias que ocupa un ancho de banda mucho mayor que el ancho de banda de información. El receptor correspondiente realiza el "salto" de frecuencia en sincronismo con el código del transmisor para recuperar la información deseada.

Espectro ensanchado por secuencia directa (Direct Sequence). Técnica de estructuración de la señal que utiliza una secuencia seudoaleatoria digital o código, con una velocidad de transmisión, muy superior a la velocidad de la señal de información. Cada bit de información de la señal digital se transmite como una secuencia seudoaleatoria de datos codificados, que produce un espectro semejante al ruido.

Interferencia. Efecto de una energía no deseada debida a una o varias emisiones, radiaciones, inducciones o sus combinaciones sobre la recepción en un sistema de radiocomunicación, que se manifiesta como degradación de la calidad, falseamiento o pérdida de la información que se podría obtener en ausencia de esta energía no deseada.

Modulación digital. Proceso por el cual las características de una onda portadora son variadas entre un sistema de valores discretos predeterminados de acuerdo con una función de modulación digital según lo especificado en el documento ANSI C63.17.1998.

Potencia Isotrópica Radiada Equivalente (PIRE). Producto de la potencia suministrada a la antena por su ganancia, con relación a una antena isotrópica en una dirección dada.

Sistemas de Baja Potencia. Acorde con la Recomendación CCP.III/REC.67 (XIX-2001) de la CITEL, son de baja potencia los dispositivos, aparatos o equipos transmisores de radiocomunicación que cuentan con poca capacidad para provocar interferencia en otro equipo de radiocomunicación y que operan sobre una base de no-interferencia, y no protección de interferencia.

Sistemas de Corto Alcance Radioeléctrico. Para los efectos de la presente resolución se consideran sistemas de corto alcance radioeléctrico los sistemas transmisores intencionales cuyo radio de cobertura de la señal guarda relación directa con la baja potencia de salida emitida por los transmisores sin que lleguen a producir interferencia a otras radiocomunicaciones.

Sistemas de Modulación Digital. Sistemas electrónicos que utilizan para el procesamiento de la señal la modulación digital.

Sistemas de Espectro Ensanchado. Sistemas de radiocomunicación en el que la energía media de la señal transmitida se reparte sobre un ancho de banda mucho mayor del ancho de banda de la información, con una densidad espectral de potencia más baja, y un mayor rechazo a las señales interferentes que operan en la misma banda de frecuencias, empleando un código independiente al de los datos, ofreciendo una capacidad de direccionamiento selectiva y la alternativa de compartir el espectro con otros sistemas de radiocomunicación. Los sistemas de espectro ensanchado presentan modalidades de funcionamiento, los sistemas de secuencia directa (directsequence -DS), los de salto de frecuencia (frecuency hopping-FH-), y los sistemas híbridos (FH/DS), que son una combinación de los anteriores.

Radiocomunicación. Toda telecomunicación transmitida por medio de las ondas radioeléctricas.

RLAN (Radio Local Area Network). Red inalámbrica de área local, que constituye una radiocomunicación entre ordenadores, aparatos y dispositivos físicamente cercanos.

U-NII (Unlicenced National Information Infrastructure). Radiadores intencionales de energía electromagnética de baja potencia que funcionan en las bandas de frecuencia de 5 150 a 5 350 MHz y de 5 470 a 5 825 MHz, que utilizan técnicas de modulación digital de banda ancha con alta transmisión de datos y proporcionan una amplia gama de comunicaciones móviles y fijas en beneficio general.

Uso libre del espectro. Uso sin necesidad de contraprestación o pago, de algunas frecuencias o bandas de frecuencias del espectro radioeléctrico, atribuidas, permitidas y autorizadas de manera general y expresa por el Ministerio de Comunicaciones.

WAS Wireless Access Systems, Forma de acceso en que los usuarios obtienen un servicio de telecomunicaciones mediante enlaces de radiofrecuencias. El término de sistemas de acceso inalámbrico se aplicará en adelante a todas las tecnologías de radiocomunicación de banda ancha y baja potencia que operen sobre una base de no-interferencia y no protección de interferencia.

Selección Dinámica de Frecuencia, DFS. Mecanismo que detecta dinámicamente señales de otros sistemas de radiocomunicación y evita la operación cocanal con estos sistemas, especialmente con sistemas de radar.

Control de Transmisión de Potencia, TPC. Característica que permite a un dispositivo U-NNI cambiar dinámicamente entre varios niveles de potencia de transmisión en el proceso de la transmisión de datos.

Artículo 3º. Campo de aplicación. La presente norma aplica a los sistemas de radiocomunicación de acceso inalámbrico y a las redes inalámbricas de área local, que utilicen tecnologías de espectro ensanchado y modulación digital, de banda ancha y baja potencia.

Para los efectos de la presente norma, a los sistemas que utilicen tecnologías de espectro ensanchado por secuencia directa les serán aplicables las disposiciones y condiciones operativas establecidas para los sistemas de modulación digital.

Artículo 4º. Habilitación general. La utilización del espectro radioeléctrico en las bandas de frecuencias atribuidas en el artículo 5º y bajo las condiciones establecidas en esta norma, no requiere habilitación distinta a la conferida de manera general por la presente resolución, sin perjuicio de la obligatoriedad de obtener la concesión respectiva cuando con este espectro radioeléctrico se pretenda prestar servicios de telecomunicaciones a terceros.

T I T U L O II
DISPOSICIONES TECNICAS

Artículo 5º. Bandas de frecuencias. Se atribuyen dentro del territorio nacional, a título secundario, para operación sobre una base de no-interferencia y no protección de interferencia, los siguientes rangos de frecuencias radioeléctricas, para su libre utilización por sistemas de acceso inalámbrico y redes inalámbricas de área local, que empleen tecnologías de espectro ensanchado y modulación digital, de banda ancha y baja potencia, en las condiciones establecidas por esta resolución.

a) Banda de 902 a 928 MHz;
b) Banda de 2400 a 2483,5 MHz;
c) Banda de 5150 a 5250 MHz;
d) Banda de 5250 a 5350 MHz;
e) Banda de 5470 a 5725 MHz;
f) Banda de 5725 a 5850 MHz.

Artículo 6º. Condiciones Operativas en las bandas de 902 a 928 MHz, 2400 a 2483,5 MHz y de 5725 a 5850 MHz. Son condiciones operativas para los sistemas de espectro ensanchado por salto de frecuencia y de modulación digital, en las bandas de 902 a 928 MHz, de 2400 a 2483,5 MHz, y de 5725 a 5850 MHz, las siguientes:

A.1. Los sistemas de salto de frecuencia tendrán frecuencias portadoras por canal de intercalamiento separadas como mínimo por el mayor valor entre 25 KHz y el ancho de banda del canal a 20 dB. El sistema saltará a los canales de frecuencias que son seleccionados, a la rata de salto del sistema, de una lista de frecuencias de salto ordenada seudoaleatoriamente. Cada frecuencia se debe utilizar igualmente en promedio, por cada transmisor. Los receptores del sistema harán coincidir sus anchos de banda de entrada con los anchos de banda del canal de

salto de sus transmisores correspondientes y cambiarán frecuencias en sincronización con las señales transmitidas.

A.2. Los sistemas de salto de frecuencia en la banda de 902 a 924 MHz deben operar de la siguiente forma: si el ancho de banda del canal de salto a 20 dB es menor que 250 KHz, el sistema utilizará por lo menos 50 frecuencias de salto y el tiempo medio de la ocupación de cualquier frecuencia no será mayor a 0.4 segundos dentro de un período de 20 segundos. Si el ancho de banda del canal de salto a 20 dB es de 250 KHz o mayor, el sistema utilizará por lo menos 25 frecuencias de salto y el tiempo medio de la ocupación de cualquier frecuencia no será mayor a 0.4 segundos dentro de un período de 10 segundos. El ancho de banda máximo permitido del canal de saltos, a 20 dB, es 500 KHz.

A.3. Los sistemas de salto de frecuencia que operan en la banda de 5725 a 5850 MHz, deben usar por lo menos 75 frecuencias de intercalamiento. El ancho de banda máximo permitido a 20 dB del canal de intercalamiento corresponde a 1 MHz. El tiempo promedio de ocupación de cualquier frecuencia no deberá ser mayor que 0.4 segundos dentro de un período de 30 segundos.

A.4. Los sistemas de Salto de Frecuencia en la banda de 2400 a 2483,5 MHz deberán utilizar al menos 15 canales no sobrelapados. El tiempo promedio de ocupación de cualquier canal no deberá ser mayor a 0.4 segundos dentro de un período de 0.4 segundos multiplicado por el número de canales de salto empleados. Los sistemas de salto de frecuencia que utilicen menos de 75 frecuencias de salto pueden emplear técnicas inteligentes de salto para evitar interferencias a otras transmisiones. Los sistemas de salto de frecuencia pueden evitar o suprimir transmisiones en una frecuencia particular de salto siempre y cuando se emplee un mínimo de 15 canales no sobrelapados.

A.5. Los sistemas que utilizan técnicas de modulación digital pueden operar en las bandas de 902 a 928 MHz, de 2400 a 2483,5 MHz, y de 5725 a 5850 MHz. El ancho de banda mínimo a 6 dB debe ser de por lo menos 500 kHz;

B. Potencia. La potencia de salida máxima del transmisor no excederá de lo siguiente:

B.1. Para los sistemas de salto de frecuencia en la banda de 2400 a 2483,5 MHz que empleen al menos 75 canales de salto, y para todos los sistemas de salto de frecuencia en la banda 5 725 a 5 850 MHz: 1 Vatio. Para los demás sistemas de salto de frecuencia en la banda 2 400 a 2 483,5 MHz: 0.125 Vatios;

B.2. Para sistemas de saltos de frecuencia que funcionan en la banda de 902 a 928 MHz:
Para los sistemas que emplean por lo menos 50 canales de saltos de frecuencia: 1 vatio.

Para los sistemas que emplean menos de 50 canales de saltos de frecuencia, pero por lo menos 25 canales, según lo permitido bajo el numeral A2 de este artículo: 0.25 vatios.

B.3. Para sistemas que utilicen modulación digital en las bandas de 902 a 928 MHz, de 2400 a 2483,5 MHz, y de 5725 a 5850 MHz: 1 Vatio.

B.4. Si se emplean antenas de transmisión de ganancia direccional mayor a 6 dBi, la potencia pico de salida de un transmisor debe ser reducida por debajo de los valores establecidos en los numerales B1, B2 y B3 de este artículo, como sea apropiado, por la cantidad en dB que la ganancia direccional de la antena exceda los 6 dBi.

B.4.1. Los sistemas que operen en la banda de 2 400 a 2 483,5 MHz que sean utilizados exclusivamente para operaciones fijas punto a punto, pueden emplear antenas de transmisión con ganancia direccional mayor a 6 dBi siempre y cuando la máxima potencia pico de salida del transmisor sea reducida en un 1 dB por cada 3 dB que la ganancia direccional de la antena exceda los 6 dBi.

B.4.2. Los sistemas que operen en la banda de 5 725 a 5850 MHz que sean utilizados exclusivamente para operaciones fijas punto a punto, pueden emplear antenas de transmisión con ganancia direccional mayor a 6 dBi sin la correspondiente reducción en la potencia pico de salida del transmisor.

B.4.3. La operación fija punto a punto, como se utiliza en los numerales B.4.1 y B.4.2 de este artículo, excluye el uso de sistemas punto a multipunto, aplicaciones omnidireccionales, y emisores colocalizados transmitiendo la misma información.

B.5. Los sistemas deben ser operados de tal forma que se asegure que el público no sea expuesto a niveles de energía de radiofrecuencia que exceda las normas que expida el Ministerio de Comunicaciones o el organismo estatal pertinente.

C.1. En cualquier ancho de banda de 100 kHz fuera de la banda de frecuencias en la cual está operando el transmisor de espectro ensanchado o de modulación digital, la potencia de radiofrecuencia que es producida por el transmisor deberá ser al menos 20 dB menor que en los 100 KHz de ancho de banda dentro de la banda que contiene el más alto nivel de la potencia deseada, basado en una medición de RF bien sea conducida o radiada.

D.1. Para sistemas modulados digitalmente, la densidad espectral de potencia conducida desde el transmisor a la antena no debe ser mayor a 8 dBm en cualquier segmento de 3 kHz durante cualquier intervalo de tiempo de transmisión continua.

E.1. En la presente resolución no se aplicará el parámetro denominado: Ganancia del Proceso.

F.1. Para los propósitos de esta norma, sistemas híbridos son aquellos que emplean una combinación de técnicas de salto de frecuencia y de modulación digital. La operación de salto de frecuencia del sistema híbrido, con la operación en secuencia directa o modulación digital interrumpida, deberá tener un tiempo promedio de ocupación de cualquier frecuencia que no exceda 0.4 segundos dentro de un período de tiempo en segundos igual al número de frecuencias de salto empleadas multiplicado por 0.4. La operación en modulación digital del sistema híbrido, con la operación en salto de frecuencia interrumpida, cumplirá con los requerimientos de densidad de potencia del numeral D1 de este artículo.

G.1. Los sistemas del espectro ensanchado por saltos de frecuencia no requieren emplear todos los canales disponibles durante cada transmisión. Sin embargo, el sistema debe diseñarse conforme las normas de la presente resolución si el transmisor se presenta como una corriente continua de datos o información. Además, un sistema que emplee cortas ráfagas de transmisión debe cumplir con la definición de un sistema de saltos de frecuencia y debe distribuir sus transmisiones sobre el número mínimo de canales de salto especificado en esta resolución.

H.1 Es permitida la incorporación de inteligencia dentro de un sistema de espectro ensanchado por saltos de frecuencia que posibilite al sistema reconocer a otros usuarios dentro de la banda del espectro de modo que elija y adapte individual e independientemente sus puntos de salto para evitar caer en los canales ocupados. La coordinación de sistemas de salto de frecuencia de cualquier otra forma, con el propósito expreso de evitar que múltiples transmisores ocupen simultáneamente frecuencias individuales de salto, no es permitida.

Artículo 7º. Condiciones Operativas en las bandas de 5150 a 5250 MHz; 5250 a 5350 MHz, 5470 a 5725 MHz y DE 5725 a 5825 MHz, para Sistemas U-NII. Son condiciones operativas de los sistemas de acceso inalámbrico y redes inalámbricas de área local, que utilicen técnicas de modulación digital, para el correcto funcionamiento de los llamados sistemas para el desarrollo de la infraestructura de la información U-NII, en las bandas de 5150 a 5250 MHz, de 5250 a 5350 MHz, 5470 a 5725 MHz y de 5725 a 5825 MHz, las siguientes:

A. Límites de potencia
A.1 Para la banda de 5 150 a 5 250 MHz, la potencia de transmisión pico sobre la banda de frecuencia de operación no debe exceder el menor valor entre 50 mW ó 4 dBm + 10 logB, donde B es el ancho de banda de emisión en MHz a 26 dB. Además, la densidad espectral de potencia pico no debe exceder 4 dBm en cualquier banda de 1 MHz. Si son utilizadas antenas de transmisión de ganancia direccional mayor a 6 dBi, la potencia de transmisión pico y la densidad espectral de potencia pico deberán ser reducidas en la cantidad de dB que la ganancia direccional de la antena exceda los 6 dBi.

A.2 Para las bandas de 5 250 a 5 350 MHz y de 5 470 a 5 725 MHz, la potencia de transmisión pico sobre la banda de frecuencia de operación no debe exceder el

menor valor entre 250 mW ó 11 dBm + 10 logB, donde B es el ancho de banda de emisión en MHz a 26 dB. Además, la densidad espectral de potencia pico no debe exceder 11 dBm en cualquier banda de 1 MHz. Si son utilizadas antenas de transmisión de ganancia direccional mayor a 6 dBi, la potencia de transmisión pico y la densidad espectral de potencia pico deberán ser reducidas en la cantidad de dB que la ganancia direccional de la antena exceda los 6 dBi.

A.3 Para la banda de 5 725 a 5 825 MHz, la potencia de transmisión pico sobre la banda de frecuencia de operación no debe exceder el menor valor entre 1 W ó 17 dBm + 10 log. B, donde B es el ancho de banda de emisión en MHz a 26 dB. Además, la densidad espectral de potencia pico no debe exceder 17 dBm en cualquier banda de 1 MHz. Si son utilizadas antenas de transmisión de ganancia direccional mayor a 6 dBi, la potencia de transmisión pico y la densidad espectral de potencia pico deberán ser reducidas en la cantidad de dB que la ganancia direccional de la antena exceda los 6 dBi. Sin embargo, los dispositivos U-NII en operación fija punto-a-punto en esta banda pueden emplear antenas de transmisión con ganancia direccional hasta de 23 dBi sin la correspondiente reducción de la potencia de salida pico del transmisor, ni en la densidad espectral de potencia pico.

Para transmisores U-NII fijos punto-a-punto que empleen una ganancia direccional de la antena mayor a 23 dBi, será requerida una reducción de 1 dB en la potencia pico del transmisor y en la densidad espectral de potencia pico por cada dB que la ganancia de la antena exceda los 23 dBi. La operación fija punto-a-punto excluye el uso de sistemas punto-a-multipunto, aplicaciones omnidireccionales, y transmisores múltiples colocalizados transmitiendo la misma información. El operador de un dispositivo U-NII, es responsable de asegurar que los sistemas que emplean antenas con alta ganancia direccional sean utilizados exclusivamente para operaciones fijas punto-a-punto.

A.4 La potencia de transmisión pico debe ser medida sobre cualquier intervalo de transmisión continua utilizando instrumentación calibrada en términos de un voltaje rms equivalente.

B. Límites de emisiones indeseadas. Las emisiones pico fuera de las bandas de frecuencia de operación deberán ser atenuadas de acuerdo con los siguientes límites:

B.1 Para transmisores que operen en la banda de 5 150 a 5 250 MHz: todas las emisiones fuera de la banda de 5 150 a 5 350 MHz no deberán exceder una PIRE de -27 dBm/MHz.

B.2 Para transmisores que operen en la banda de 5 250 a 5 350 MHz: todas las emisiones fuera de la banda de 5 150 a 5 350 MHz no deberán exceder una PIRE de -27 dBm/MHz. Dispositivos que operen en la banda de 5 250 a 5 350 MHz que generen emisiones en la banda de 5 150 a 5 250 MHz deben cumplir todos los requerimientos técnicos aplicables para la operación en la banda de 5150 a 5250

MHz (incluyendo el uso en interiores o recintos cerrados) o como alternativa, cumplir con una PIRE límite de emisión fuera de banda de -27 dBm/MHz en la banda de 5150 a 5250 MHz.

B.3.1 Para transmisores que operen en la banda de 5 470 a 5 725 MHz: todas las emisiones fuera de la banda de 5 470 a 5 725 MHz no deberán exceder una PIRE de -27 dBm/MHz.

B.3.2 Para transmisores que operen en la banda de 5 725 a 5 825 MHz: todas las emisiones dentro del rango de frecuencia comprendido desde el borde de la banda hasta 10 MHz por encima o por debajo del borde de la banda, no deberán exceder una PIRE de -17 dBm/MHz; para frecuencias 10 MHz o más, por encima o por debajo del límite de la banda, las emisiones no deberán exceder una PIRE de -27 dBm/MHz.

B.4 Las mediciones de emisión deberán ser efectuadas utilizando una resolución mínima de ancho de banda de 1 MHz. Una resolución de ancho de banda más baja puede ser empleada cerca del borde de la banda, cuando sea necesario, siempre y cuando la energía medida sea integrada para mostrar la potencia total sobre 1 MHz.

B.5 Emisiones indeseadas por debajo de 1 GHz deben presentar límites generales de intensidad de campo menores a 500 micro-voltios/metro a 3 metros de distancia.

B.6 Cuando se midan los límites de emisión, la frecuencia portadora nominal deberá ser ajustada tan cerca de los bordes de los bloques de frecuencia superior e inferior como el diseño del equipo permita.

C.1 El dispositivo deberá interrumpir automáticamente la transmisión en caso de ausencia de información a transmitir o en caso de falla operacional. Estas disposiciones no tienen la intención de impedir la transmisión de la información de control o señalización o el uso de códigos repetitivos utilizados por ciertas tecnologías digitales para completar los intervalos entre tramas o ráfagas.

D.1 Cualquier dispositivo U-NII que opere en la banda de 5 150 a 5 250 MHz deberá utilizar una antena de transmisión que sea parte integral del dispositivo.

E.1 Dentro de la banda de 5 150 a 5 250 MHz, los dispositivos U-NII estarán restringidos a operaciones en interiores o recintos cerrados para reducir cualquier potencial de producir interferencias perjudiciales a las operaciones del servicio móvil por satélite MSS co-canal.

F.1 Todos los dispositivos U-NII deberán ser considerados para operar en un ambiente público e incontrolado. Los dispositivos deben ser operados de tal forma que se asegure que el público no sea expuesto a niveles de energía de radio

frecuencia que exceda las normas que expida el Ministerio de Comunicaciones o el organismo estatal pertinente.

G.1 Los operadores y fabricantes de dispositivos U-NII son responsables de asegurar una estabilidad de frecuencia tal que una emisión sea mantenida dentro de la banda de operación bajo todas las condiciones de operación.

H. Control de Transmisión de Potencia (TPC) y Selección Dinámica de Frecuencia (DFS).

H.1 Control de Transmisión de Potencia TPC. Los dispositivos U-NII que operen en la banda de 5250 a 5350 MHz y de 5470 a 5725 MHz deberán emplear un mecanismo de TPC. Los dispositivos U-NNI deberán tener capacidad para operar al menos 6 DB por debajo del valor medio PIRE de 30 dBm. No se requiere mecanismo de TPC para sistemas con una PIRE menor a 500 mW.

H.2 Función de detección de radar de DFS. Los dispositivos U-NII que operen en la banda de 5250 a 5350 MHz y de 5470 a 5725 MHz deberán emplear un mecanismo de detección de radar de dfs para detectar la presencia de sistemas de radar y evitar la operación co-canal con estos sistemas. El umbral de detección del DFS para dispositivos con una PIRE entre 200 mW a 1 W es de -64 dBm. El umbral de detección es la potencia promedio recibida en 1microsegundo a una antena de referencia de 0 dBi.

H.2.1 Modos de operación. El requisito de Selección dinámica de frecuencia DFS aplica a los siguientes modos de operación:
A. El requisito de comprobación del tiempo de disponibilidad del canal aplica en el modo maestro de operación;

B. El requisito del tiempo de cambio del canal aplica en ambos modos, en los modos de operación maestro y esclavo.

H.2.2 Comprobación del tiempo de disponibilidad del canal. El dispositivo UNNI deberá comprobar si existe un sistema de radar operando alrededor del canal, antes de poder iniciar una transmisión en ese canal y, cuando este ha de ser trasladado a un nuevo canal. El dispositivo U-NII puede comenzar a usar el canal si no se detecta ninguna señal de radar con un nivel de la potencia mayor que los valores de umbral de interferencia, enunciados, en el plazo de 60 segundos.

H.2.3 Tiempo de cambio del canal. Después de ser detectada la presencia de un radar, todas las transmisiones cesarán en la operación de canal dentro de los 10 segundos. Las transmisiones durante este período consistirán de un tráfico normal, de máximo 200 milisegundos después de ser detectada la señal del radar. Adicionalmente una señal de gestión y control intermitente puede ser enviada durante el tiempo remanente para facilitar la liberación del canal.

H.2.4 Período de no-ocupación. Un canal que ha sido advertido de la presencia de un sistema de radar, bien sea por verificación de disponibilidad del canal o bajo un servicio de monitoreo, está sujeto a un período de no-ocupación de por lo menos 30 minutos. El período de no-ocupación empieza en el momento en que el sistema de radar sea detectado.

Artículo 8°. Banda de 2300 A 2400 MHz. Se permite, a título secundario, el uso de la banda de 2300 a 2400 MHz para aplicaciones de sistemas de acceso inalámbrico y redes inalámbricas de área local, que utilicen tecnologías de espectro ensanchado y modulación digital, de banda ancha y baja potencia, previo registro ante el Ministerio de Comunicaciones, bajo las condiciones operativas generales y particulares de los sistemas de acceso inalámbrico en la banda de 2400 a 2483,5 MHz, establecidas por la presente resolución.

Parágrafo. A los sistemas de acceso inalámbrico y redes inalámbricas de área local, que utilicen tecnologías de espectro ensanchado y modulación digital, de banda ancha y baja potencia, en la banda de 2300 a 2400 MHz, les será aplicable el artículo 39.2 del decreto 1972 de 2003, por el cual se establece el régimen unificado de contraprestaciones, por concepto de concesiones, autorizaciones, permisos y registros en materia de telecomunicaciones y los trámites para su liquidación, cobro, recaudo y pago.

Artículo 9º. Antenas omnidireccionales. La utilización de antenas omnidireccionales solo será permitida en sistemas inalámbricos cuya potencia radiada sea menor o igual a 100 mW. Los sistemas que excedan esta potencia deberán emplear antenas direccionales con un ancho de lóbulo no mayor a 90 grados.

Artículo 10. Interferencias. La utilización de sistemas de acceso inalámbrico y redes inalámbricas de área local, que utilicen tecnologías de espectro ensanchado y modulación digital, de banda ancha y baja potencia, está condicionada al cumplimiento de las siguientes condiciones:

1. No deben causar interferencia perjudicial a las estaciones de un servicio primario a las que se les hayan asignado frecuencias con anterioridad o se les puedan asignar en el futuro.

2. No pueden reclamar protección contra interferencias perjudiciales causadas por estaciones de un servicio primario a las que se les hayan asignado frecuencias con anterioridad o se les puedan asignar en el futuro.

Si un dispositivo ocasiona interferencia perjudicial a una radiocomunicación autorizada a título primario, aunque el aparato cumpla con las normas técnicas establecidas en los reglamentos de radiocomunicación o los requisitos de autorización de equipo, se deberá suspender la operación del dispositivo. La utilización no podrá reanudarse hasta que se haya subsanado el conflicto interferente, de comprobarse la continua interferencia perjudicial a una

radiocomunicación autorizada, el Ministerio de Comunicaciones podrá ordenar la suspensión definitiva de las operaciones, sin perjuicio de las sanciones previstas en las normas legales.

Artículo 11. Referencia a normas técnicas. Para la correcta operación de los sistemas de acceso inalámbrico y redes inalámbricas de área local, que utilicen tecnologías de espectro ensanchado y modulación digital, de banda ancha y baja potencia, sólo se aceptarán equipos de conformidad con las normas técnicas de la Federal Communications Comission FCC, CFR 47 Part 15 Subpart C § 15.247 y CFR 47 Part 15 Subpart E, la presente norma, y otros estándares internacionales que se ajusten a estas especificaciones.

T I T U L O III
DISPOSICIONES FINALES

Artículo 12. Transición. A partir de la entrada en vigencia de la presente resolución, quedan sin efectos los títulos habilitantes expedidos para el uso del espectro radioeléctrico mediante la utilización de equipos de espectro ensanchado o sistemas U-NII, en las bandas de frecuencias atribuidas en el artículo 5º de esta norma.
Quienes cuenten con título habilitante para el uso del espectro radioeléctrico mediante la utilización de equipos de espectro ensanchado en la banda de 2025 MHz a 2400 MHz, obtenido de acuerdo con las disposiciones de la Resolución 5927 de 1996, deberán hacer uso de la banda de 2300 MHz a 2400 MHz, a la que se refiere el artículo 8º de esta norma. Los respectivos títulos habilitantes quedan modificados por lo aquí dispuesto.

Los trámites en curso para registrar sistemas de acceso inalámbrico y redes inalámbricas de área local, que utilicen tecnologías de espectro ensanchado y modulación digital, de banda ancha y baja potencia, en las bandas de frecuencias atribuidas en el artículo 5º de esta norma, se entenderán concluidos a la fecha de ejecutoria de la presente resolución.

Artículo 13. Infracciones y sanciones. El incumplimiento de las normas previstas en la presente resolución constituye una infracción al ordenamiento de las telecomunicaciones, y generará las sanciones previstas en las normas legales.

Artículo 14. Vigencia. Esta resolución rige a partir de su publicación y deroga en su totalidad las Resoluciones 3382 de 1995; 5927 de 1996; 1833 de 1998; la Tabla número 3.6 del artículo 3º de la Resolución 0797 de 2001, y las normas que le sean contrarias.

Publíquese y cúmplase.
Dada en Bogotá, D. C., a 21 de abril de 2004.
La Ministra de Comunicaciones,
Martha Elena Pinto de De Hart.

- **Anexo 2:**

La ley 527 de 1999 que define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y establece las entidades de certificación y dicta otras disposiciones.

Decreto 1485 de diciembre de 1996 “Por el cual se reglamenta parcialmente el Decreto 3466 de 1982, en materia de fijación pública de precios”, así como en los Conceptos 02014785 del 11 de Abril de 2002, 02047297 del 17 de junio de 2002 y 02043386 del 30 de mayo de 2002 de la Superintendencia de Industria y Comercio, se trata de manera tangencial el tema de los códigos de barras.

- **Anexo 3:**

Artículo 192 - Violación ilícita de comunicaciones: El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle, o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido, incurrirá en prisión de uno a tres años, siempre que la conducta no constituya delito sancionado con pena mayor.

Si el autor de la conducta revela el contenido de la comunicación, o la emplea en provecho propio o ajeno o con perjuicio de otro, la pena será de prisión de dos (2) a cuatro (4) años.

Se entiende por comunicación un intercambio de información entre dos sistemas informáticos, tal sería el caso de los mensajes de datos. De esta manera cuando se intercepta una comunicación del sistema de mensajería instantánea (Messenger) se presenta una comunicación ilícita de comunicaciones.

Artículo 193 - Ofrecimiento, venta o compra de un instrumento apto para interceptar la comunicación privada entre personas. El que sin permiso de autoridad competente, ofrezca, venda o compre instrumentos aptos para interceptar la comunicación privada entre personas, incurrirá en multa siempre que la conducta no constituya delito sancionado con pena mayor.
En este artículo se incluye el ofrecimiento a través de una página web de software que pueda servir como instrumento para interceptar una comunicación privada, como los sniffers de redes, software para ataques de fuerza bruta o contraseñas de acceso.

Artículo 195 - Acceso abusivo a un sistema informático. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo incurrirá en multa.

- **Anexo 4: Estándares de la Organización Internacional de Estándares (ISO)**

ISO/IEC 3166 Códigos para la representación de los nombres de los países y sus subdivisiones.

Parte 1: Código de países.
Parte 2: Códigos de subdivisión de países.
Parte 3: Códigos para el nombre formal usado por los países.

ISO/IEC 4217 Códigos para la representación de monedas y fondos.
ISO/IEC 4909 Tarjetas de Identificación – Tarjetas para transacción financiera – Contenido de banda Magnética para el Track 3.

ISO/IEC 7501 Tarjetas de Identificación - Máquina lectora de documentos de viaje.
Parte 1: Máquina lectora de pasaportes.
Parte 2: Máquina lectora de visas.
Parte 3: Máquina lectora de documentos oficiales de viaje.

ISO/IEC 7810 Tarjetas de Identificación - Características físicas.

ISO/IEC 7811 Tarjetas de Identificación - Técnica de grabación.
Parte 1: Propia marca.
Parte 2: Banda Magnética - Baja coercitividad.
Parte 3: Localización de caracteres repujados.
Parte 4: Localización de Tracks 1 y 2.
Parte 5: Localización de Track 3.
Parte 6: Banda Magnética - Alta Coercitividad.
Parte 7: Banda Magnética - Alta Coercitividad, Alta Densidad.
Parte 8: Banda Magnética - Coercitividad de 51,7 KA/m (650 Oe).

ISO/IEC 7812 Tarjetas de Identificación - Identificación de emisores.
Parte 1: Sistema numérico.
Parte 2: procedimientos de aplicación y registro.

ISO/IEC 7813 Tecnología de Información - Tarjetas de Identificación - Tarjetas de transacción financiera.

ISO/IEC 7816 Tarjetas de Identificación - Tarjetas con circuitos integrados.
Parte 1: Tarjetas con contactos - Características físicas.
Parte 2: Tarjetas con contactos - Dimensiones y localización de los contactos.
Parte 3: Tarjetas con contactos - Protocolos eléctricos.
Parte 4: Organización, seguridad y comandos de intercambio.
Parte 5: Registro de aplicación de proveedores.
Parte 6: elementos para intercambio de datos ínter industria.

Parte 7: comandos ínter industria para Lenguaje estructurado de consulta de tarjetas (SCQL).
Parte 8: Comandos para operaciones seguras.
Parte 9: Comandos para administración de tarjetas.
Parte 10: Señales electrónicas y respuesta a restablecer para tarjetas síncronas.
Parte 11: Verificación personal a través de métodos biométricos.
Parte 12: Interfaz eléctrica USB y procedimientos de operación.
Parte 13: Comandos para administración de aplicación en un ambiente multi-aplicación.
Parte 15: Aplicación de información criptográfica.

ISO/IEC 8484 Bandas magnéticas en libros de ahorros.

ISO/IEC 8583 Mensajes originados en tarjetas de transacciones financieras.
Parte 1: Mensajes, elementos de datos y valor de códigos.
Parte 2: Aplicación y procedimientos de registro para códigos de identificación de institución (IIC).
Parte 3: procedimiento de mantenimiento de mensajes, elementos de datos y valores de código.

ISO/IEC 8825 Tecnología de Información - ASN.1 reglas de codificación:
Parte 1: Especificación de reglas básicas de codificación (BER), Reglas de codificación canónica (CER) y Reglas distintivas de codificación (DER).
Parte 2: Especificación de reglas de codificación empaquetadas (PER).
Parte 3: Especificación de Notaciones de Codificación de control (ECN).
Parte 4: Reglas de codificación XML (XER).
Parte 5: definición de esquemas de mapeo W3C XML en ASN.1.

ISO/IEC 9796 Tecnología de Información - Técnicas seguras - Esquemas de firma digital dando mensajes de recuperación.
Parte 1: Esquema de firma.
Parte 2: Mecanismo basado en factorización de enteros.
Parte 3: Mecanismo basado en algoritmos discretos.

ISO/IEC 9797 Tecnología de información - Técnicas seguras -- códigos de autenticación de mensajes (MACs).
Parte 1: Mecanismos usando un bloqueo cipher.
Parte 2: Mecanismos usando una función-hash dedicada.

ISO/IEC 9979 Tecnología de información - Técnicas seguras -- Procedimiento para el registro de algoritmos criptográficos.

ISO/IEC 9992 Tarjetas de transacción financiera - Mensajes entre tarjetas de circuito integrado y dispositivo receptor de tarjeta.
Parte 1: Concepto y estructura.

Parte 2: Funciones, mensajes (comandos y respuestas), elementos y estructura de datos.

ISO/IEC 10118 Tecnología de información - Técnicas seguras - Funciones-Hash.
Parte 1: General.
Parte 2: Funciones-hash usando un block cipher n-bit.
Parte 3: funciones-hash dedicadas.
Parte 4: Funciones-hash usando aritmética modular.

ISO/IEC 10202 Tarjetas para transacciones financieras - Arquitectura de seguridad de sistemas de transacción financiera usando tarjetas con circuitos integrados.
Parte 1: ciclo de vida de la tarjeta.
Parte 2: principios generales y visión general.
Parte 3: relaciones de llaves criptográficas.
Parte 4: módulos de aplicación segura.
Parte 5: uso de algoritmos.
Parte 6: verificación de tarjeta habiente.
Parte 7: administración de llave.

ISO/IEC 10373 Tarjetas de Identificación - métodos de prueba.
Parte 1: Características generales.
Parte 2: Tarjetas con banda magnética.
Parte 3: tarjetas con circuito integrado con contactos y dispositivo de interfaz relativo.
Parte 4: Tarjetas con circuito integrado sin contacto.
Parte 5: tarjetas con memoria óptica.
Parte 6: tarjetas de proximidad.
Parte 7: Tarjetas de vecindad.

ISO/IEC 10536 Tarjetas de identificación -- tarjetas con circuito integrado no contacto.
Parte 1: Características físicas.
Parte 2: Dimensiones y localización de las áreas de acople.
Parte 3: señales electrónicas y procedimientos de respuesta.
Parte 4: respuesta a restablecer y protocolos de transmisión.

ISO/IEC 11693 tarjetas de identificación - tarjetas con memoria óptica -- Características generales.

ISO/IEC 11694 Tarjetas de identificación - tarjetas con memoria óptica -- método de grabación lineal.
Parte 1: Características físicas.
Parte 2: Dimensiones y localización del área óptica accesible.
Parte 3: propiedades ópticas y características.
Parte 4: estructura lógica de datos.

Parte 5: formato de datos para el intercambio de información para aplicaciones usando ISO/IEC 11694-4, Anexo B.
Parte 6: Uso de biométricos en una tarjeta con memoria óptica.

ISO/IEC 14443 Tarjetas de identificación -- tarjetas con circuito integrado no contacto -- tarjetas de proximidad.
Parte 1: Características físicas.
Parte 2: poder de radio frecuencia y señal de interfaz.
Parte 3: Inicialización y anticolisión.
Parte 4: protocolo de transmisión.

ISO/IEC 14496: Tecnología de información – Codificación de objetos audio-visuales.
Parte 1: Sistemas.
Parte 2: Visual.
Parte 3: Audio.
Parte 4: prueba de conformidad.
Parte 5: Referencia de Software.
Parte 6: Estructura de entrega de integración multimedia (DMIF).
Parte 7: Referencia de software optimizado.
Parte 8: Transporte en redes IP.
Parte 9: Referencia de Hardware.
Parte 10: Codificación avanzada de video (AVC).
Parte 11: Descripción de escena y motor de aplicación.
Parte 12: Formato ISO base de archivos de media.
Parte 13: Manejo de propiedad intelectual y Protección de extensiones.
Parte 14: Formato de archivo MPEG-4.
Parte 15: Formato de archivo AVC.
Parte 16: Extensión de formato de animación (AFX).
Parte 17: Formato de subtitulo de texto de cronometro.
Parte 18: Compresión de formato de streaming (para fuentes de tipo abierto).
Parte 19: Textura sintetizada de stream.
Parte 20: Representación de escena ligera (LASeR).
Parte 21: Extensión de formato gráfico MPEG-J (GFX).
Parte 22: Especificación de formato de fuente abierta (OFFS).
Parte 23: Representación Simbólica de música (SMR) .

ISO/IEC 15415 Tecnología de información -- identificación automática y técnica de captura de datos -- especificaciones de prueba de calidad de impresión de código de barras -- símbolos de dos dimensiones.

ISO/IEC 15416 Tecnología de información -- identificación automática y técnica de captura de datos -- especificaciones de prueba de calidad de impresión de código de barras -- símbolos lineales.

ISO/IEC 15417 Tecnología de información -- Identificación automática y técnicas de captura de datos -- especificación de simbología de código de barras -- Código 128.

ISO/IEC 15418 Tecnología de información -- Identificadores de aplicaciones EAN/UCC e identificadores de factores de datos y mantenimiento.

ISO/IEC 15419 Tecnología de información -- Identificación automática y técnicas de captura de datos -- Identificadores de cargadores de datos (incluyendo identificadores de simbología).

ISO/IEC 15420 Tecnología de información -- Identificación automática y técnicas de captura de datos -- imagen digital del código de barras y pruebas de calidad de impresión.

ISO/IEC 15424 Tecnología de información -- Identificación automática y técnicas de captura de datos -- especificación de simbología de código de barras -- EAN/UPC.

ISO/IEC 15426 Tecnología de información -- Identificación automática y técnicas de captura de datos -- especificación de verificación de conformación del código de barras.
Parte 1: símbolos lineales.
Parte 2: símbolos de dos dimensiones.

ISO/IEC 15438 Tecnología de información -- Identificación automática y técnicas de captura de datos -- especificación simbología código de barras PDF417.

ISO/IEC 15457 Tarjetas de identificación -- Tarjetas flexibles delgadas.
Parte 1: Características físicas.
Parte 2: técnica de grabación magnética.
Parte 3: métodos de prueba.

ISO/IEC 15460 Tarjetas de identificación -- Tarjetas con circuitos integrados con contactos -- Circuitos integrados con voltajes inferiores a 3 voltios.

ISO/IEC 15693 Tarjetas de identificación -- Tarjetas con circuitos integrados sin contactos -- Tarjetas de vecindad.
Parte 1: Características físicas.
Parte 2: Interfaz e inicialización aérea.
Parte 3: protocolo de transmisión y anticolisión.
Parte 4: Registro de aplicaciones / emisores.

ISO/IEC 15961 Tecnología de información – Identificación de Radio Frecuencia (RFID) para administración de artículos – protocolo de datos: interfaz de aplicación.

ISO/IEC 15962 Tecnología de información – Identificación de Radio Frecuencia (RFID) para administración de artículos – Identificación única para etiquetas RF.

ISO/IEC 16022 Tecnología de información -- Identificación automática y técnicas de captura de datos -- especificación de simbología de código de barras Data Matrix.

ISO/IEC 16023 Tecnología de información -- Especificación de simbología internacional – MaxiCode.

ISO/IEC 16388 Tecnología de información -- Identificación automática y técnicas de captura de datos -- especificaciones de simbología de código de barras -- código 39.

ISO/IEC 16390 Tecnología de información -- Identificación automática y técnicas de captura de datos -- especificaciones de simbología de código de barras -- Entrelazado 2 de 5.

ISO/IEC 18000 Tecnología de información -- Identificación por radio frecuencia para administración de artículos.
Parte 1: Arquitectura de referencia y definición de parámetros a ser estandarizados.
Parte 2: parámetros para interferencia de comunicaciones aéreas por debajo de 135 Khz.
Parte 3: parámetros para interferencia de comunicaciones aéreas a 13,56 MHz.
Parte 4: parámetros para interferencia de comunicaciones aéreas a 2.45 GHz.
Parte 5: parámetros para interferencia de comunicaciones aéreas a 5.8 GHz (Retirado).
Parte 6: parámetros para interferencia de comunicaciones aéreas a 860 MHz a 960 MHz.
Parte 7: parámetros para interferencia de comunicaciones aéreas a 433 MHz.

ISO/IEC 18004 Tecnología de información -- Identificación automática y técnica de captura de datos -- Especificaciones de simbología de código de barras Código QR 2005.

ISO/IEC 18013 Tecnología de información -- Identificación personal -- Licencias de conducción ISO-compliant.
Parte 1: Características físicas y juego básico de datos.
Parte 2: Tecnologías de máquina lectora.

ISO/IEC 18020 Tarjetas de identificación -- Tarjetas con circuitos integrados con contactos -- verificación personal a través de métodos biométricos en tarjetas con circuitos integrados.

ISO/IEC 19092 Servicios Financieros – Biométricos.

Parte 1: estructura de seguridad.

ISO/IEC 19762 Tecnología de información – técnicas de Identificación automática y de captura de datos (AIDC) – Vocabulario armonizado.
Parte 1: Términos generales relacionados con AIDC.
Parte 2: Medio de lectura óptico (ORM).
Parte 3: Identificación por radiofrecuencia (RFID).

ISO/IEC 19784 Tecnología de información – programación de interfaz aplicaciones biométricas.
Parte 1: Especificación BioAPI.
Parte 2: función del proveedor de interfaz de archivo biométrico.
Parte 3: aplicación biométrica programación interfaz.

ISO/IEC 19785 Tecnología de información -- Estructura de formato de intercambio de biométricos comunes.
Parte 1: Especificación de elemento de datos.
Parte 2: Procedimientos para la operación de la autoridad de registro biométrico.
Parte 3: Especificación del patrón del formato.

ISO/IEC 19794 Formato de intercambio de datos biométricos.
Parte 1: Estructura.
Parte 2: datos de minutiae de huella digital.
Parte 3: datos de espectro pattern de huella digital.
Parte 4: datos de imagen de huella digital.
Parte 5: datos de imagen facial.
Parte 6: datos de imagen del iris.
Parte 7: datos de series de tiempo de firma.
Parte 8: esqueleto de datos de pattern de huella digital.
Parte 9: imagen de datos vasculares.
Parte 10: datos de la silueta de la geometría de la mano.
Parte 11: procesamiento dinámico de los datos de la firma.
Parte 12: datos de la identificación facial.

ISO/IEC 24723 Tecnología de información – Identificación automática y técnica de captura de datos – Especificación simbología código de barras compuesto EAN.UCC.

ISO/IEC 24724 Tecnología de información -- Identificación automática y técnica de captura de datos – Especificación simbología de código de barras simbología de espacio reducido (RSS).

ISO/IEC 24728 Tecnología de información -- Identificación automática y técnica de captura de datos – Especificación simbología de código de barras MicroPDF417.

ISO/IEC 24778 Identificación automática y técnica de captura de datos – Especificación simbología de código de barras – Código Aztec.

ISO/IEC 28219 Embalaje – Etiquetado y mercadeo directo de producto con código de barras lineal y símbolos de dos dimensiones.

- **Anexo 5: Estándares del Instituto Colombiano de Normas Técnicas (ICONTEC)**

NTC 1238 Documentación. Código para la representación de nombres de países.

NTC1387 Sistema Internacional para la numeración de libros ISBN.

NTC 2444 Banca. Código para la presentación de monedas corrientes y fondos.

NTC 2579 Banca. Tarjetas de identificación. Sistemas de numeración y procedimientos de registro para los identificadores del emisor.

NTC 2869 Banca. Tarjetas bancarias. Banda magnética. Contenido de datos de la pista 3 – Track 3.

NTC 2969 Banca y servicios financieros. Tarjetas. Tarjetas de identificación. Técnicas de registro. Localización de pistas de sólo lectura. Pistas 1 y 2.

NTC 2970 Banca y servicios financieros. Tarjetas. Tarjetas de identificación. Técnicas de registro. Localización de caracteres realizados en tarjetas de tipo ID-1.

NTC 3214 Banca y servicios financieros. Tarjetas. Tarjetas de identificación. Técnicas de registro. Banda Magnética.

NTC 3431 Banca y servicios financieros. Tarjetas. Tarjetas de identificación. Técnicas de registro. Localización de la pista de lectura-escritura. Pista 3.

NTC 3451 Banca y servicios financieros. Tarjetas. Tarjetas de identificación. Tarjetas de circuitos integrados con contactos. Características físicas.

NTC 3839 Codificación por barras. Especificaciones de simbología. Código 128.

NTC 3840 Codificación por barras. Especificaciones de simbología. Código intercalado 2 de 5.

NTC 3841 Codificación por barras. Terminología.

NTC 3842 Codificación por barras. Especificaciones de simbología. Descripción del formato.

NTC 3843 Codificación por barras. Especificaciones de simbología. Codabar.

NTC 3844 Codificación por barras. Especificaciones de simbología. Código 39.

NTC 4053 Guía de calidad de impresión de código de barras.

NTC 4769 Código de barras para las facturas recaudadas por el sector financiero.

NTC-EN 796 Codificación por barras. Identificadores de simbología.

NTC-EN 797 Codificación por barras. Especificaciones de simbología. Código EAN/UPC.

- **Anexo 6: Estándares de la Organización para el avance de estándares de información estructurada (OASIS)**

Formato común biométrico XML (XCBF)", versión 1.1, Agosto 2003, Organización para el avance de estándares de información estructurada.

- **Anexo 7: Organización Internacional de Aviación Civil (ICAO)**

Documento 9303.
Parte 1: Para pasaportes.
Parte 2: para visas.
Parte 3: para documentos de oficiales de viaje (Tarjetas).

Nota: no se están referenciado estándares de organizaciones nacionales de estandarización de otros países.

- **Anexo 8: Tabla 11.**

NOMBRE	INSTALACION	COMUNICACION	TECNOLOGIA	CONFIABILIDAD	COSTO DE INSTALACION	CANTIDAD DE FABRICANTES
EBI	Cableado Estructurado	Punto a Punto	Cableado punto a punto	Alta	Alto	Bajo
X10	Remplazo Elemento	Punto a Punto	Portador linea de corriente	Baja	Medio	Medio
ZigBee	Remplazo Elemento	Punto a Punto	Radio Frecuencia	Media	Bajo	Medio
UPnP	En red Locla	Punto a Punto	En red punto a punto	Media	Alto	Bajo
Z-Wave	Remplazo Elemento	Enmallado General	Radio Frecuencia	Alta	Bajo	Alto