1.- Marco teórico y conceptos básicos.

1.1 Sistemas de Identificación.

La necesidad de identificar los vehículos nos lleva, necesariamente, a revisar las distintas tecnologías disponibles en el mercado para la identificación de objetos y validar, en primer término, que la opción de radiofrecuencia es la más conveniente. Esta tecnología es de evolución relativamente reciente y ha sido posible, al converger en ella las telecomunicaciones, la informática y la electrónica en general.

Los elementos requeridos para un sistema de identificación son:

- Elemento codificado: Portador de la información.
- Elemento lector: Capaz de leer la información.

La información reconocida alimenta a la computadora donde la identificación es decodificada, verificada y aceptada para luego tomar una decisión lógica. En el caso de identificación de personas, por ejemplo: acceso a una cuenta de banco, un área restringida, una computadora, una línea telefónica, una empresa, una casa; los controles remotos, las tarjetas de crédito, etc.

Los sistemas modernos son automáticos, agilizando así su proceso, evitando errores y aumentando su confiabilidad y eficiencia. Estos mismos sistemas se utilizan también para la identificación de objetos especialmente cuando están afectando a una actividad comercial: cuanto más grande es la comercialización, más necesaria es la exacta identificación del producto, que le permite conocer al industrial, comerciante, distribuidor y cliente los siguientes elementos: características del producto, origen, ubicación y destino, costo y precio de venta, verificación y control, contabilidad y administración, estadística e inventarios.

De referencias documentales, se enuncian algunos de estos sistemas:

- Código de barras.
- Reconocimiento óptico de caracteres: OCR.
- Tarjetas de cinta magnética.
- Tarjetas de radio frecuencia.
- Reconocimiento de imágenes o visión electrónica.
- Reconocimiento de la Voz Humana.
- Reconocimiento de retina.
- Imagen térmica.

Si bien el proyecto se centra en el análisis de las tecnologías RFID, se considera importante revisar los sistemas de identificación que la tecnología ha permitido que se desarrollen en el mercado ya que su análisis envuelve variables que son importantes conocer por su simetría, analogía o complementariedad para los problemas que se pretenden resolver, a través de los sistemas de radiofrecuencia.

1.1.1. Código de Barras.

Es, sin duda, el método con más expansión actualmente en el mercado. Se emplea principalmente en el comercio de artículos de consumo, en procesos de manufactura, en diversos campos industriales, en el sector médico, la industria automotriz y en contenedores de barcos, entre otros. Consiste en una etiqueta que contiene una serie de líneas verticales o barras con espacios entre ellas, de diferente grosor y espacios, que proporcionan en código números o letras, como se aprecia en la figura 2.1.

Figura 1.1 Numeración Estándar + Símbolo = Código de Barras

- Numeración estándar: Identificación única del producto, reconocido a nivel mundial.
- Símbolo: representación gráfica que permite su lectura automática, a través de lectores ópticos.
- Código de Barras: conjunto de barras y espacios que representan la numeración estándar, ambos otorgados por la Asociación correspondiente.

La numeración estándar de productos es única y por lo tanto, se convierte en una llave de acceso a los archivos de la computadora, de toda la información referente al producto para emplearla con diversos fines.

Con un código estándar cada empresa puede manejar la información que requiere, de acuerdo a sus necesidades, de sus propios análisis y de sus propios sistemas, no importando en qué etapa de la cadena de comercialización se encuentre.

En la figura 1.2, se representa un sistema de lectura de código de barras. Los códigos se leen mediante un dispositivo óptico láser o escáner, que registra el código por reflexión de la luz en las barras y los espacios.

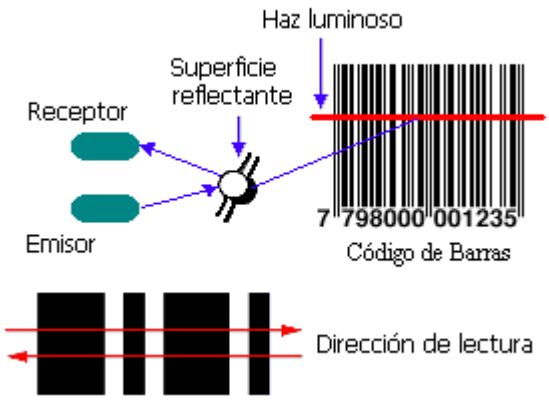


Figura 1.2.- Sistemas de lectura de un código de barras.

Entre las primeras justificaciones de la implantación del código de barras se encontraron la necesidad de agilizar la lectura de los artículos en las cajas y la de evitar errores de captura. Otras ventajas que se pueden destacar de este sistema son:

- Agilidad en etiquetar precios, pues no es necesario hacerlo sobre el artículo ya que el código viene de fábrica y simplemente se relaciona con el código en una base de datos.
- Rápido control del stock de mercancías.
- Estadísticas comerciales. El código de barras permite conocer los artículos vendidos en cada momento pudiendo extraer conclusiones de mercadotecnia.
- El consumidor obtiene una relación de artículos en el ticket de compra lo que permite su comprobación y eventual reclamación.

Entre las desventajas que se le atribuyen, se encuentra la imposibilidad de conocer el precio del producto directamente de este y la facilidad de su reproducción; lo que la hace una aplicación orientada directamente a la identificación de artículos que tienen impreso el código en el envase y/o que existe control en los procesos que se emplean.

Existen diversas simbologías que pueden utilizarse para distintos fines. Sin embargo, en el plano comercial, las más usadas en el mundo son el UPC y el EAN.

European Article Number (EAN).- Es un sistema de Códigos de Barras adoptado por más de 100 países y cerca de un millón de empresas (2003). En el año 2005, la asociación EAN se fusionó con la UCC para formar una

nueva y única organización mundial identificada como GS1, con sede en Bélgica.

El código EAN más usual es EAN13, constituido por 13 dígitos y con una estructura dividida en 4 partes:

Los primeros dígitos del Código de Barras EAN no identifican el país de origen del producto, sino, únicamente a través de qué Organización Nacional se ha adscrito una determinada empresa al Sistema EAN. Por ejemplo, en México se encarga de ello la Asociación Mexicana de Estándares para el Comercio Electrónico (AMECE) y su código es el “750”.

La referencia del artículo está compuesta de:

- Código de empresa. Es un número compuesto por entre 5 y 8 dígitos, que identifica al propietario de la marca.
- Código de producto. Completa los 12 primeros dígitos.

Dígito de control.- Para comprobar el dígito de control (por ejemplo, por el computador y el escáner de código de barras) se suman los dígitos de las posiciones pares, el resultado se multiplica por 3, se le suman los dígitos de las posiciones impares y este resultado se le resta a su múltiplo de 10, más próximo. El resultado final ha de coincidir con el dígito de control.

Por ejemplo, para 123456789041 el dígito de control será:

Suma de los números en los lugares pares: 2+4+6+8+0+1 = 21

Multiplicado x 3: 21 x 3 = 63

Suma de los números en los lugares impares: 1+3+5+7+9+4 = 29

Suma total: 63 + 29 = 92

Próximo múltiplo de 10 = 100

Dígito de control: 100 - 92 = 8

El código quedará: 1234567890418

Existe una cierta tendencia en sustituir el código de barras por sistemas de RFID, cuya generalización está limitada por el costo del dispositivo o “tag” ya que le añade un costo al producto, porcentualmente relevante, cuando se trata de sustituir el código de barras en artículos de consumo; no obstante, las ventajas del sistema RFID se encuentran en que:

- No requieren localizar y leer el código como en el caso de las barras.
- Con la información del tag se puede identificar a un artículo en particular, no sólo su tipo.

- El código de barras es fácilmente reproducible, pudiera alguien fácilmente sobreponer una etiqueta o cambiarla.
- El código de barras es más susceptible de daño que un “tag”.

Existen variaciones sobre el código de barras, una de ellas es las de dos dimensiones (2-D) (ver figura 1.3), que han empezado a usarse en documentos para controlar su envío o en seguros médicos y, en general, en documentos que requieren la inserción de mensajes más grandes (de hasta 2,725 dígitos), como un expediente clínico completo.

Figura 1.3.- Códigos de Barra de dos dimensiones o 2D

Beneficios del Código de Barras

El código de barras es un buen sistema de colección de datos mediante identificación automática y presenta muchos beneficios, entre otros:

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

El incremento de la velocidad y exactitud en la toma de datos, nos lleva a reducir errores, a un ahorro de tiempo y dinero.

Aplicaciones.

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

Entre las aplicaciones que tiene podemos mencionar:

- Control de material en procesos.
- Control de inventario.
- Control de movimiento.
- Control de tiempo y asistencia.
- Control de acceso.
- Punto de venta.
- Control de calidad.
- Control de embarques y recibos.
- Control de documentos y rastreos de los mismos.
- Rastreos preciso en actividades
- Rastreos precisos de bienes transportados.
- Levantamiento electrónico de pedidos.
- Facturación.
- Bibliotecas.

1.1.2 Reconocimiento Óptico de Caracteres: OCR

El sistema OCR (Optical Caracter Recognition) que tuvo su origen en la década de los 60´s se utiliza principalmente en producción, servicios administrativos y en Bancos, para registro de cheques.

El software de reconocimiento óptico de caracteres, abreviado habitualmente como OCR, extrae de una imagen los caracteres que componen un texto para almacenarlos en un formato con el cual puedan interactuar programas de edición de texto o aplicaciones de bases de datos.

Mientras que en una imagen los caracteres se describen por cada uno de los puntos que los forman, al convertirlos a un formato de texto (por ejemplo ASCII o Unicode), pasan a describirse por un solo número, por lo que se produce una reducción significativa del espacio en la memoria que ocupan.

A partir de ahí “la imagen” se reconoce como texto, de modo que se pueden buscar en él cadenas de caracteres, exportar el texto a un editor de textos, o a otras aplicaciones, etc.

Actualmente, junto con el texto, se registra también el formato con el que fue escrito.

Una variante es el OMR (optical mark recognition) que se utiliza para reconocimiento de marcas. Un ejemplo, es la corrección automática de exámenes de tipo test, en los que la respuesta correcta se marca con un círculo.

A día de hoy, el reconocimiento preciso en textos mecanografiados con escritura en caracteres latinos se considera un problema resuelto en la gran mayoría de sus aspectos.

El reconocimiento de la impresión manual, es decir, aquella que proviene de la caligrafía humana e incluso las versiones escritas a máquina, que se encuentran impresas en otras grafías (especialmente aquellas con un número muy grande de caracteres), sigue siendo una fuente de intensa investigación.

Los sistemas para el reconocimiento de los textos escritos a mano alzada han disfrutado, en años recientes, de algunos éxitos comerciales. Entre estos, se encuentran los dispositivos conocidos como asistentes digitales personales, tales como los que se encuentran instalados en el Palm OS. El Newton de Apple fue el pionero en este tipo de asistentes. Los algoritmos que usa el software de estos aparatos se aprovecha por el hecho de que se conocen el orden, la velocidad y la dirección de los segmentos de línea, como información de entrada. El usuario se puede entrenar y ayudar al dispositivo usando solamente formas específicas de letras. Estos mismos métodos no se pueden trasladar a los programas que se encargan de interpretar los caracteres de documentos escaneados y sigue siendo un problema, en cierta medida.

La proporción de texto reconocido se encuentra, en la actualidad, entre el 80 y el 90, en el caso de caracteres escritos a mano con gran claridad y pulcritud, pero estos porcentajes disminuyen sensiblemente en el caso de los escaneos de texto y es muy frecuente encontrar docenas de errores por página escaneada. Este problema condiciona la tecnología OCR haciéndola una tecnología útil en un reducido número de contextos. Esta variedad de OCR se conoce comúnmente en la industria como ICR (Intelligent Character Recognition).

El reconocimiento de textos cursivos, en el que todas las letras se encuentran conectadas formando una palabra, es un área de intensa investigación, con proporciones de reconocimiento incluso más bajas que las que se dan en los textos impresos a mano pero mediante caracteres individualizados. Para elevar los porcentajes de aciertos en la escritura caligráfica se requiere adicionar otro tipo de información, ya sea gramatical o contextual. Por ejemplo, el reconocimiento de palabras enteras que se encuentran, previamente, clasificadas en un diccionario es un problema

más fácil de resolver que tratar de analizar, de manera individual, los caracteres de la escritura.

Un claro ejemplo de información contextual, es la lectura de la línea donde se escribe la cantidad en un cheque (que se encuentra siempre escrita como un número). Aquí, el uso de un diccionario de reducidas dimensiones puede incrementar de manera considerable el porcentaje de aciertos. El conocimiento de la sintaxis gramatical de una lengua, que es traducida por OCR, puede también ayudar para determinar si una palabra es un verbo o un sustantivo permitiendo, de esta manera, una mayor exactitud.

Existen otras áreas de colaboración, donde los humanos ayudan a las máquinas y viceversa. Las técnicas de procesamiento de imágenes pueden ayudar a una lectura extraordinariamente compleja para un ser humano tales como el Palimpsesto de Arquímedes o los Manuscritos del Mar Muerto. Para problemas de reconocimiento muy complejos se usan las redes neuronales ya que pueden efectuar, de manera indistinta, tanto transformaciones no lineales como transformaciones afines.

Los inconvenientes de los sistemas de reconocimiento de caracteres se deben a que son más costosos que otros sistemas de identificación que pueden alcanzar las mismas expectativas y el costo se debe a la complejidad de los lectores.

1.1.3 Sistemas Biométricos.

Entenderemos por sistema biométrico a un sistema automatizado que realiza labores de biometría. Es decir, un sistema que fundamenta sus decisiones de reconocimiento mediante una característica personal que puede ser reconocida o verificada de manera automatizada. En esta sección se describen algunas de las características más importantes de estos sistemas.

Con la evolución de las tecnologías asociadas a la información, nuestra sociedad está cada día más conectada electrónicamente. Labores que tradicionalmente eran realizadas por seres humanos son, gracias a las mejoras tecnológicas, realizadas por sistemas automatizados. Dentro de la amplia gama de actividades que pueden automatizarse, aquella relacionada con la capacidad para establecer la identidad de los individuos ha cobrado importancia y como consecuencia directa, la biometría se ha transformado en un área emergente. La biometría es la ciencia que se dedica a la identificación de individuos a partir de una característica anatómica o un rasgo de su comportamiento. Una particularidad anatómica posee la cualidad de ser relativamente estable en el tiempo, tal como una huella dactilar, la silueta de la mano y patrones de la retina o el iris. Un rasgo del comportamiento es menos estable, pues depende de la disposición

psicológica de la persona, por ejemplo, la firma. No cualquier característica anatómica puede utilizarse con éxito en un sistema biométrico. Para que esto así sea debe cumplir con las siguientes características: Universalidad, Unicidad, Permanencia y Cuantificación.

Características de un Indicador Biométrico.

Este sensor, con el cual se puede realizar una biometría, debe cumplir los siguientes requerimientos:

- Universalidad: cualquier persona posee esa característica.
- Unicidad: la existencia de dos personas con una característica idéntica tiene una probabilidad muy pequeña.
- Permanencia: la característica no cambia en el tiempo y
- Cuantificación: la característica puede ser medida en forma cuantitativa.

Las características anteriores, sirven como criterio para descartar o aprobar algún requerimiento como indicador biométrico. Luego de seleccionar algún indicador que satisfaga los requisitos antes señalados, es necesario imponer restricciones prácticas sobre el sistema que tendrá como misión recibir y procesar a estos indicadores.

Los sistemas biométricos están principalmente orientados a la identificación de personas, que tienen precisamente asociada una o varias características biométricas.

Modelo del Proceso de Identificación Personal.

Cualquier proceso de identificación personal puede ser comprendido mediante un modelo simplificado. Este postula la existencia de tres indicadores de identidad que definen el proceso de identificación:

- Conocimiento: la persona tiene conocimiento (por ejemplo: un código).
- Posesión: la persona posee un objeto (por ejemplo: una tarjeta) y
- Característica: la persona tiene una característica que puede ser verificada (por ejemplo: una de sus huellas dactilares).

Cada uno de los indicadores anteriores genera una estrategia básica para el proceso de identificación personal. Además, pueden combinarse con el objeto de alcanzar grados de seguridad más elevados y brindar, de esta forma, diferentes niveles de protección. Distintas situaciones requerirán de diferentes soluciones para la labor de identificación personal. Por ejemplo, con relación al grado de seguridad, se debe considerar el valor que se está protegiendo, así como los diversos tipos de amenazas. También es importante considerar la reacción de los usuarios y el costo del proceso.

Las características básicas que un sistema biométrico para identificación personal debe cumplir, pueden expresarse mediante las restricciones que

deben de satisfacerse. Ellas apuntan, básicamente, a la obtención de un sistema biométrico con utilidad práctica.

Las restricciones antes señaladas se dirigen a que el sistema considere el desempeño, la aceptabilidad y la fiabilidad.

El desempeño, que se refiere a la exactitud, la rapidez y la robustez alcanzada en la identificación, además de los recursos invertidos y el efecto de factores ambientales y/u operacionales. El objetivo de esta restricción es comprobar si el sistema posee exactitud y rapidez aceptables, con un requerimiento de recursos razonable.

La aceptabilidad, que indica el grado en que la gente está dispuesta a aceptar un sistema biométrico en su vida diaria. Es claro que el sistema no debe representar peligro alguno para los usuarios y debe inspirar “confianza” a los mismos. Factores psicológicos pueden afectar esta última característica. Por ejemplo, el reconocimiento de una retina, que requiere un contacto cercano de la persona con el dispositivo de reconocimiento, puede desconcertar a ciertas personas debido al hecho de tener su ojo sin protección frente a un “aparato”. Sin embargo, las características anteriores están subordinadas a la aplicación específica. En efecto, para algunas aplicaciones la repercusión psicológica de utilizar un sistema basado en el reconocimiento de características oculares será positiva, debido a que este método es eficaz implicando mayor seguridad.

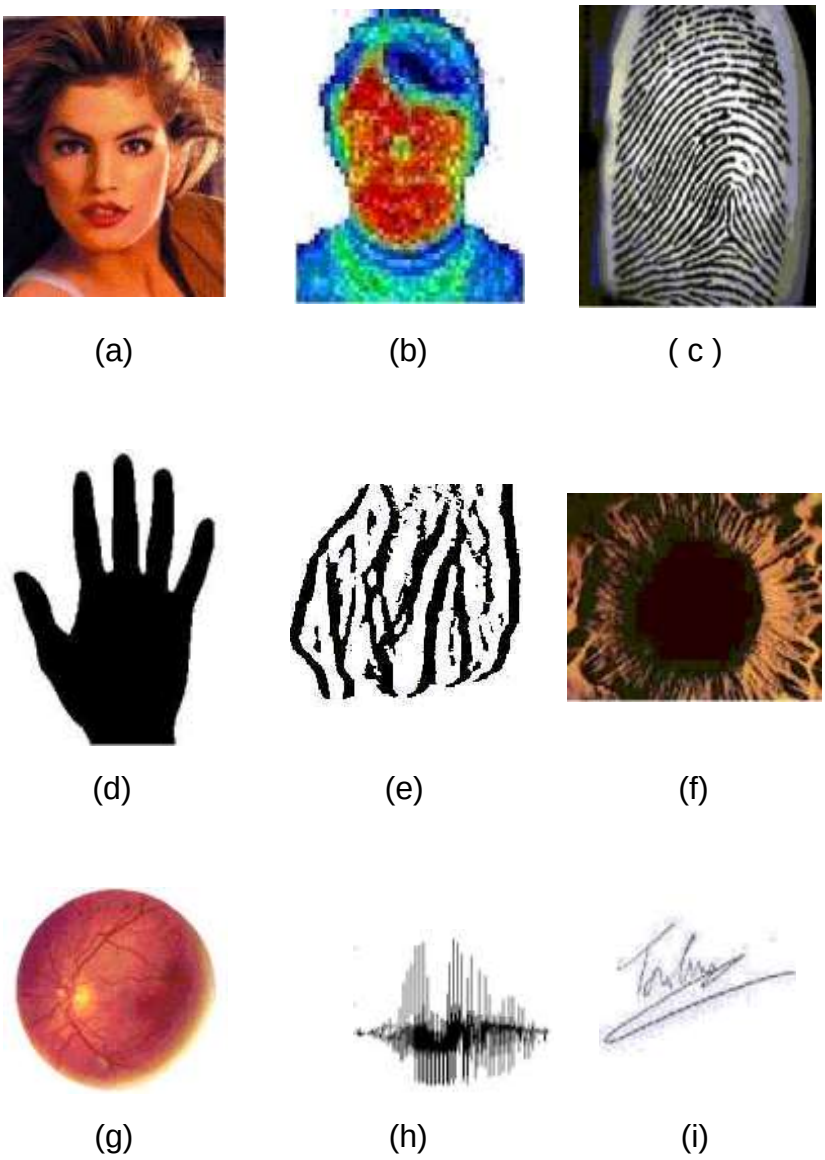
La fiabilidad, que refleja cuán difícil es burlar al sistema. El identificador biométrico debe reconocer características de una persona viva, pues es posible crear dedos de látex, grabaciones digitales de voz, prótesis de ojos, etc. Algunos sistemas incorporan métodos para determinar si la característica bajo estudio, corresponde o no a la de una persona viva. Los métodos empleados son ingeniosos y usualmente más simples de lo que uno podría imaginar. Por ejemplo, un sistema basado en el reconocimiento del iris, revisa patrones específicos en las manchas de éste; un sistema infrarrojo para chequear las venas de la mano, detecta flujos de sangre caliente y los lectores de ultrasonido para huellas dactilares revisan estructuras subcutáneas de los dedos.

Sistemas Biométricos Actuales.

Actualmente, existen sistemas biométricos que basan su acción en el reconocimiento de diversas características, como puede apreciarse en la figura 1.4. Las técnicas biométricas más conocidas son nueve y están basadas en los siguientes indicadores biométricos:

a) Rostro.
b) Termograma del rostro.
c) Huellas dactilares.
d) Geometría de la mano.

e) Venas de las manos.
f) Iris.
g) Patrones de la retina.
h) Voz.
i) Firma.



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Figura 1.4.- Técnicas biométricas actuales.

Cada una de las técnicas anteriores, posee ventajas y desventajas comparativas, las cuales deben tenerse en consideración al momento de decidir que técnica utilizar para una aplicación específica. En particular, deben considerarse las diferencias entre los métodos anatómicos y los de comportamiento. Una huella dactilar, salvo daño físico, es la misma día a

día, a diferencia de una firma que puede ser influenciada tanto por factores controlables como por psicológicos no intencionales. También las máquinas que miden características físicas tienden a ser más grandes y costosas que las que detectan comportamientos. Debido a diferencias como las señaladas, no existe un único sistema biométrico que sea capaz de satisfacer todas las necesidades. Una compañía puede incluso decidir el uso de distintas técnicas en distintos ámbitos. Más aún, existen esquemas que utilizan de manera integrada más de una característica para la identificación. Por ejemplo, se integran el reconocimiento de rostros y huellas dactilares. La razón es que el reconocimiento de rostros es rápido pero no extremadamente confiable, mientras que la identificación mediante huellas dactilares es confiable pero no eficiente en consultas a bases de datos. Lo anterior, sugiere utilizar el reconocimiento de rostros para particionar la base de datos. Luego de esto comienza la identificación de la huella. Los resultados alcanzados por el sistema conjunto son mejores que los obtenidos por sus partes por separado. En efecto, las limitaciones de las alternativas por separado son soslayadas, logrando además, respuestas exactas con un tiempo de proceso adecuado. En la figura 1.5, se presenta un esquema de división de las características biométricas.

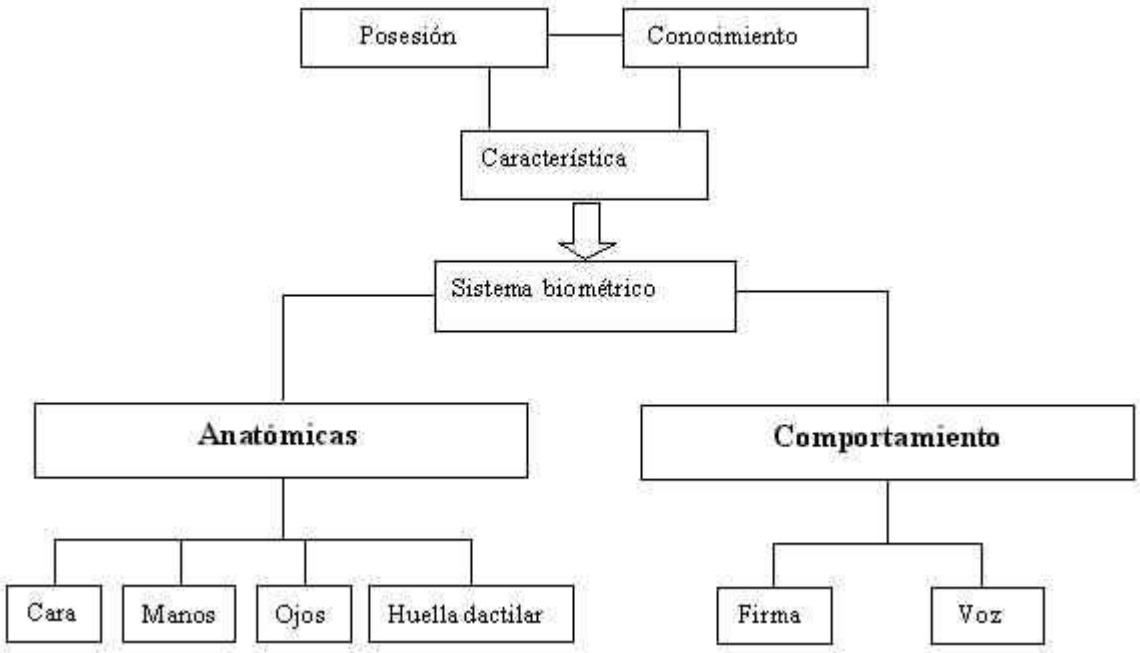


Figura 1.5.- División de las características biométricas para identificación personal.

Huellas Dactilares

Un indicador biométrico que satisface muchos requisitos, es la huella dactilar. Este indicador ha sido utilizado por los seres humanos para identificación personal, durante más de cien años. En la actualidad, las

huellas dactilares representan una de las tecnologías biométricas más maduras y son consideradas pruebas legítimas de evidencia criminal en cualquier corte del mundo.

Una huella dactilar es la representación de la morfología superficial de la epidermis de un dedo. Posee un conjunto de líneas que, en forma global, aparecen dispuestas en forma paralela (colinas o ridge lines y furrows). No obstante, estas líneas se intersectan y en ocasiones terminan en forma abrupta.

Los puntos donde las colinas terminan o se bifurcan, se conocen técnicamente como minucias. Otros puntos singulares de una huella dactilar son aquellos donde la curvatura de los ridges es máxima. Esos puntos reciben el nombre de cores y deltas. La característica más interesante que presentan tanto las minucias como los puntos singulares cores y deltas es que son únicos para cada individuo y permanecen inalterados a través de su vida. A pesar de esta variedad de minucias (han sido enumerados 18 tipos distintos de minucias), las más importantes son las terminaciones y bifurcaciones de ridges. Esto último, se debe a que las terminaciones de ridges representan aproximadamente el 60.6% de todas las minucias en una huella y las bifurcaciones el 17.9%.

Asimismo, varias de las minucias menos típicas se pueden expresar en función de las dos señaladas. Naturalmente, para poder identificar a una persona mediante las minucias de su huella, es necesario poder representar a estas últimas, para poder compararlas. La representación estándar consiste en asignar a cada minucia su posición espacial (x, y) y su dirección, que es tomada con respecto al eje ‘x’ en el sentido contrario a las manecillas del reloj. Esta representación se muestra en la figura 1.6, para una minucia de término y una de bifurcación de ridge.

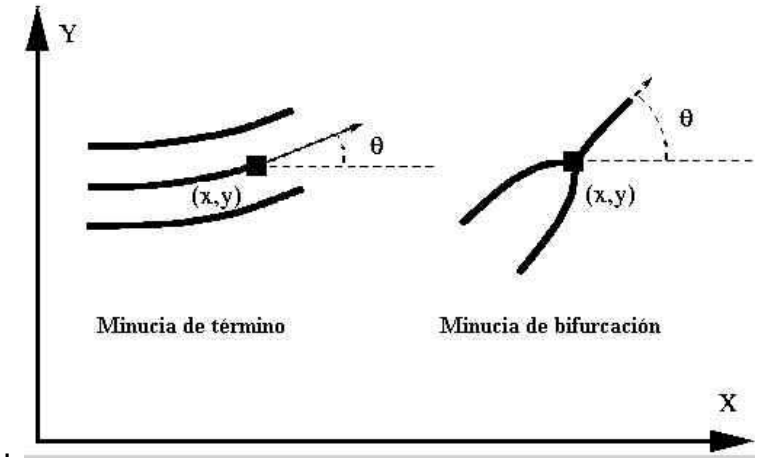


Figura 1.6.- Representación de minucias en términos de su posición y dirección.

Para reconocer una huella dactilar, se procede desde una escala gruesa a una fina. En primer lugar, se clasifica a la huella, es decir, se asigna a una clase previamente determinada, de acuerdo a la estructura global de los ridges. El objetivo de esta etapa es establecer una partición en la base de datos con huellas. En general, la distribución de las huellas en las distintas clases, es no uniforme, lo que obliga a sub-clasificar a la huella en estudio, es decir, generar un nuevo conjunto de clases a partir de las ya definidas. Luego se procede a la comparación a escala fina. Este proceso recibe el nombre de matching. El proceso consiste en comprobar si el conjunto de minucias de una huella coincide con el de otra.

Las principales dificultades en el proceso de matching son:

- En una imagen de calidad hay alrededor de 70 a 80 minucias en promedio, cantidad que contrasta abiertamente con las presentes en una imagen latente o parcial cuyo valor promedio es del orden de 20 a 30.
- Hay traslaciones, rotaciones y deformaciones no lineales de las imágenes que se heredan a las minucias.
- Aparecen minucias espurias, mientras otras verídicas desaparecen.
- La base de datos puede ser muy grande.
- No existe un método de comparación que entregue una coincidencia exacta entre las características de la imagen de entrada y las pertenecientes a la base de datos.

A la fecha, las técnicas propuestas que han obtenido mayor éxito en la labor de matching, se han basado en una comparación de índole geométrica de los vectores de características.

Reconocimiento Facial.

El reconocimiento de imágenes faciales, también denominado reconocimiento de caras, permite determinar la identidad de una persona al comparar una imagen de su cara con imágenes de referencia almacenadas en una base de datos en la que también se almacena la identidad de las personas asociadas a cada imagen de referencia. Esta comparación se realiza analizando elementos estructurales presentes en los rostros. El sistema de reconocimiento implantado puede ser, por el momento, comparar caras frontales en condiciones adecuadas.

Para probar el sistema de reconocimiento de rostros frontales se deberá seleccionar la imagen a analizarse desde algunas de las bases de datos. El sistema entregará las caras más parecidas al rostro seleccionado, indicando asimismo el grado de similitud o parecido.

Estos sistemas logran identificar a la persona en menos de dos segundos. Pese a ello, no son suficientemente rápidos en zonas con gran afluencia de gente. Por tanto, todavía hay mucho trabajo por delante.

Se necesitan sistemas con mucha memoria y gran tiempo de cómputo, dos características fundamentales para acortar los tiempos de ejecución.

La identificación de características faciales, ha recibido un fuerte impulso, gracias al cambio en la tecnología de vídeo multimedia. Esto ha propiciado un aumento de cámaras en los lugares de trabajo y en el hogar. El reconocimiento por características faciales es inherente a todos nosotros. Individuos específicos pueden distinguirse de una multitud sólo con verles el rostro. Por tanto, este tipo de identificación es considerada como la más natural dentro de los sistemas biométricos.

El reconocimiento facial se puede aplicar en el control de accesos a edificios públicos, cajeros automáticos, agencias del gobierno, laboratorios de investigación y también como clave secreta de acceso para el uso de computadores personales.

Este sistema se podría utilizar de la misma manera para tener bases de datos con la información de quién entra y quién sale de edificios emblemáticos. Los primeros programas de reconocimiento facial, fueron instalados en el Reino Unido. En 1997, la ciudad de Newham (250.000 habitantes) equipó sus calles con un sistema de vídeo-control conectado a un programa informático. Según la policía, la iniciativa permitió una disminución del 34% de la criminalidad.

Este sistema ya se ha utilizado en EEUU durante la última final de fútbol americano, conocida como Súper Bowl, donde las cámaras registraron las caras de cada uno de los espectadores, para cotejarlas con las de los criminales almacenadas en su base de datos.

El proceso de identificación facial se divide en dos tareas: «detección» y «reconocimiento». La primera comprende la localización de las caras que existen en una fotografía o en una secuencia de vídeo. La segunda tarea compara la imagen facial con caras previamente almacenadas en una base de datos. Se suele cotejar una serie de puntos clave, como la boca, nariz y ojos.

Conscientes de la creciente importancia de los sistemas de seguridad, los expertos pretenden crear una aplicación que permita realizar la identificación facial, mediante técnicas de aprendizaje estadístico. Para desarrollar esta tarea, se va a utilizar una de las herramientas de aprendizaje más potentes que existen en la actualidad, la Máquina de Vectores Soporte («Support Vector Machine», SVM), dada su versatilidad y prestaciones en la clasificación.

Para resolver el problema de la detección facial, diversos investigadores han usado otros métodos. Por ejemplo, las redes neuronales o

aproximaciones de máxima verosimilitud. Pero, analizando los resultados obtenidos, se puede comprobar que la máquina de vectores soporte es la que proporciona el menor error y la mejor generalización.

Este método permite discriminar dentro de un gran conjunto de alternativas aquellos rostros que no cumplen con ciertas condiciones en un proceso que es más rápido para concentrar los recursos de procesamiento en aquellos rostros potenciales.

Tarjetas Inteligentes

Las tarjetas inteligentes son dispositivos con las características físicas de las tarjetas de crédito, con un microprocesador incrustado que controla el acceso a la información que contiene.

Las tarjetas inteligentes se utilizan actualmente para almacenar información de todo tipo, en cualquier mercado (banca, salud, servicios, etc.), para control de accesos y seguridad (por su capacidad de encriptamiento, manejo de claves públicas y privadas, etc.), para pago electrónico (monederos electrónicos) y más.

Hasta ahora, la banda magnética de las tarjetas de crédito y de débito, ha sido la tecnología dominante en el mercado; con todo, en ellas sólo se puede almacenar una pequeña cantidad de información, de modo que la gran mayoría de los datos personales y de las operaciones de la tarjeta magnética, residen en servidores centrales de la compañía que las emite.

Con una tarjeta inteligente, toda la información necesaria para las transacciones está alojada en el microprocesador insertado, lo que significa que el tráfico de información a sistemas centrales es mucho menor con respecto al de las tarjetas de banda magnética, incrementándose así, el nivel de seguridad de las operaciones.

Con las tarjetas inteligentes, se puede operar desde un simple control de acceso del personal a una empresa o escuela, hasta complejas combinaciones, que pueden incluir la información personal del usuario, su historial clínico y algún sistema de cliente frecuente, incluyendo servicios financieros, como monedero electrónico o tarjetas de débito y de crédito.

Las tarjetas inteligentes cada vez son más utilizadas. Los niveles de seguridad y la capacidad de almacenamiento que manejan han llevado a los bancos y a otras Instituciones Financieras a reemplazar poco a poco sus tarjetas convencionales de banda magnética por tarjetas de chip. La posibilidad de almacenar y procesar información en este sofisticado y diminuto mecanismo facilita la realización de procesos y permite administrar la información de mejor manera.

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

con los cajeros automáticos. También para proporcionar un medio con el cual operar en puntos de venta específicos.

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

En la actualidad la utilización de la tarjeta magnética se ha generalizado de tal forma que, al año, se producen y utilizan una media de 1,400 millones de tarjetas magnéticas en el mundo.

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

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

La tarjeta inteligente surge ante las nuevas necesidades del mercado, las cuales no pueden ser satisfechas por la tarjeta de banda magnética.

Esta tecnología tiene su origen en la década del 70, cuando inventores de Alemania, Japón y Francia inscribieron las patentes originales. Debido a varios factores que se presentaron y de los cuales la inmadura tecnología de semiconductores tuvo un mayor peso, muchos trabajos sobre tarjetas inteligentes *(smart cards)* estuvieron en investigación y desarrollo hasta la primera mitad de los años 80.

Hasta el punto mencionado, la tecnología con chip aporta prácticamente lo mismo que la banda magnética.

Sin embargo, hay al menos tres aspectos en los que la potencialidad implícita en el chip otorga a esta última tecnología una clara ventaja de cara al futuro.

Seguridad.- El contenido de la banda magnética, por la tecnología que implica, puede ser leído y, aunque no es sencillo, puede ser manipulado por personas con conocimiento y medios adecuados. El chip, sin embargo, contiene una tecnología interna mucho más sofisticada, que hace que las posibilidades de manipulación física se reduzcan de forma muy sensible. Al mismo tiempo, por su capacidad interna, es capaz de soportar procesos criptográficos muy complejos (DES simple, triple DES, RSA). Más adelante, en este documento, se abundará sobre la seguridad en las tarjetas inteligentes.

Capacidad de almacenamiento de información.- La cantidad de información incorporable a una banda magnética es pequeña y, parcialmente

modificable, por lo que la relación entre el usuario de la tarjeta y el emisor es unidimensional: únicamente se actualiza cuando sé interactúa, a través de hardware sofisticado (ATMs). El chip, no obstante, une a su mayor capacidad de información, la capacidad de poder gestionar dicha información, con lo que se abren nuevas posibilidades para la relación usuario-emisor. Estas características diferenciales, motivan que la difusión de la tecnología chip aplicada en tarjetas de plástico sea altamente deseable. Esta difusión, pasa inevitablemente por la estandarización del producto. En el terreno estrictamente físico, la ubicación exacta del chip en la tarjeta de plástico y de los contactos a través de los que interactúa, está consensuada a nivel mundial. Esto, además de otros efectos intrínsecamente más importantes, ha tenido como efecto que su imagen se esté popularizando y sea cada vez más comúnmente reconocida. La parte exterior de todo el mecanismo que soporta su operatoria no es el chip, sino un conjunto de zonas de contacto, cada una de las cuales tiene funciones predeterminadas.

Flexibilidad.- La tecnología de Tarjetas Inteligentes es compatible con los principales tipos de sistemas operativos. También existe un entorno de programación que permite crear, almacenar o suprimir aplicaciones en las tarjetas, lo que significa que es posible hacer tarjetas “a medida”, seleccionando para la tarjeta las aplicaciones que se adapten a las circunstancias y necesidades de cada persona.

Aparición cronológica

1979: Primer prototipo de tarjeta de memoria.

1982: Primera tarjeta telefónica fabricada para France Telecom.

1988: Primera tarjeta DES bancaria fabricada para Carte Bancaire.

1993: Primera tarjeta GSM-SIM (Global System for Mobile Communication).

1996: Primera tarjeta RSA 1024 bits “cryptoprocessor”.

1997: Primera tarjeta de ICC Java powered.

2000: Primera tarjeta de ICC Windows 2000 powered.

2000: Primera tarjeta de ICC para SunRay Workstation.

Principales fabricantes

Gemplus (www.gemplus.com).

Schlumberger (www.slb.com).

Bull (www.bull.com).

Oberthur (www.oberthur.com).

Orga (www.orga.com)..

Solaic(www.winforms.phil.tu-bs.de/winforms/company/solaic/solaic.html).

De la Rue (www.delarue.com).

Descripción de una Tarjeta Inteligente.

Es muy frecuente denominar a todas las tarjetas que poseen contactos dorados o plateados sobre su superficie, como tarjetas inteligentes. Sin embargo, este término es bastante ambiguo y conviene hacer una clasificación correcta. ISO (International Standard Organization), prefiere usar el término “tarjeta de circuito integrado” (Integrated Circuit Card o ICC), para referirse a todas aquellas tarjetas que posean algún dispositivo electrónico, ver figura 1.7. Este circuito contiene elementos para realizar transmisión, almacenamiento y procesamiento de datos. La transferencia de datos puede llevarse a cabo a través de los contactos que se encuentran en la superficie de la tarjeta, o sin contactos, por medio de campos electromagnéticos. Estas tarjetas presentan diversas ventajas en comparación con las de bandas magnéticas:

Figura 1.7.- Tarjeta Inteligente

Son capaces de almacenar más información.

Pueden proteger la información que almacenan en sus memorias de posibles accesos no autorizados.

Poseen una mayor resistencia al deterioro de la información almacenada.

Ya que el acceso a la información se realiza a través de un puerto serie y es supervisado por el propio sistema operativo de la tarjeta, es posible escribir datos confidenciales que no puedan ser leídos por personas no autorizadas. En principio, las funciones de escritura, lectura y borrado de la memoria pueden ser controladas tanto por el hardware, como por el software o por ambos a la vez. Esto permite contar con una gran variedad de mecanismos de seguridad.

Siendo el chip integrado, el componente más importante, las tarjetas están clasificadas según el tipo de circuito y estas pueden ser:

Tarjeta Inteligente de Contacto:

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

Tarjetas Inteligentes Sincrónicas o Tarjetas de Memoria.

Los datos que se requieren para las aplicaciones con tarjetas de memoria, son almacenados en una EEPROM (Electrical Erasable Programable Read Only Memory).

Estas tarjetas son desechables, cargadas previamente con un monto o valor que va decreciendo a medida que se utiliza y una vez que se acaba el monto, se vuelve desechable.

Memoria Libre: Carece de mecanismos de protección para acceder a la información. Las funciones que desempeñan están optimizadas para aplicaciones particulares en las que no se requieren complejos mecanismos de seguridad. Se utilizan para el pago de peajes, teléfonos públicos, máquinas dispensadoras y espectáculos.

Memoria Protegida: Poseen un circuito de seguridad que proporciona un sistema para controlar los accesos a la memoria frente a usuarios no autorizados. Este sistema funciona mediante el empleo de un código de acceso que puede ser de 64 bits o más.

Tarjetas asincrónicas

Estas tarjetas poseen en su chip un microprocesador, de acuerdo con el diagrama de la figura 1.8, además cuenta con algunos elementos adicionales como son:

ROM enmascarada.

EEPROM.

RAM.

Puerto de Entrada/Salida

La ROM (Read Only Memory), enmascarada contiene el sistema operativo de la tarjeta y se graba durante el proceso de fabricación.

La EEPROM es la memoria no volátil del microprocesador y en ella se encuentran datos del usuario o de la aplicación, así como el código de las instrucciones que están bajo el control del sistema operativo. También puede contener información como el nombre del usuario, número de identificación personal o PIN (Personal Identification Number).

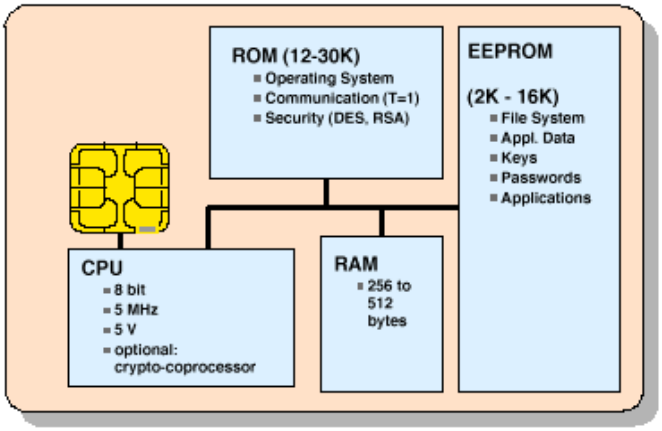


Figura 1.8.- Tarjeta Asincrónica

La RAM (Random Access Memory) es la memoria de trabajo del microprocesador. Al ser volátil se perderá toda la información contenida en ella al desconectar la alimentación.

El puerto de entrada y salida normalmente consiste en un simple registro, a través del cual, la información se transfiere bit a bit.

Las tarjetas con microprocesador son bastante flexibles puesto que pueden realizar múltiples funciones. En el caso más simple, sólo contienen datos referentes a una aplicación específica, esto hace que dicha tarjeta únicamente se pueda emplear para esa aplicación. Pese a esto, los sistemas operativos de las tarjetas más modernas hacen posible que se puedan integrar programas para distintas aplicaciones en una sola tarjeta. En este caso la ROM contiene sólo el sistema operativo con las instrucciones básicas, mientras que el programa específico de cada aplicación se graba en la EEPROM después de la fabricación de la tarjeta.

Tarjetas Inteligentes sin Contacto

Son similares a las de contacto, con respecto a lo que pueden hacer y a sus funciones, pero utilizan diferentes protocolos de transmisión en capa lógica y física. No utilizan contacto galvánico sino de interfaz inductiva. Poseen además del chip, una antena de la cual se valen para realizar transacciones, en la figura 1.9 se pueden apreciar las capas de una tarjeta sin contacto. Son ideales para las transacciones que tienen que realizarse rápidamente.

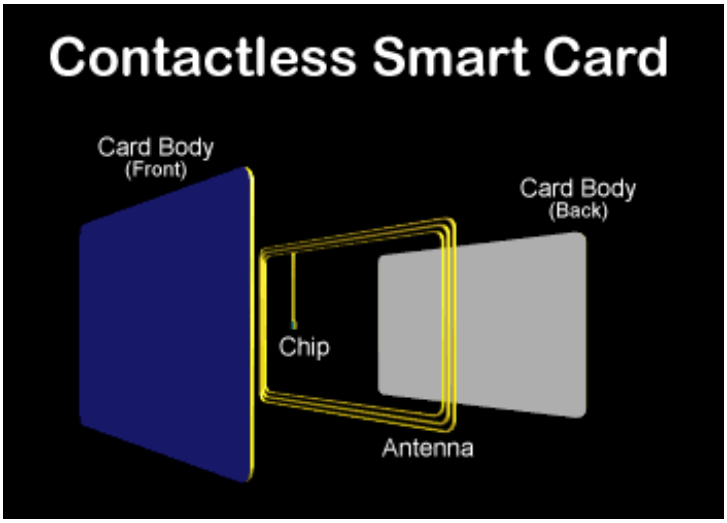


Figura 1.9.- Tarjeta Inteligente sin Contacto

Esta tecnología ofrece ventajas con respecto a la de las tarjetas de contacto. Cuando en una tarjeta de contactos se producen fallos de funcionamiento, casi siempre se deben al deterioro en la superficie de contacto o a la suciedad adherida a los mismos. Una de las ventajas de las tarjetas sin contacto, es que los problemas técnicos antes mencionados no ocurren debido, claro está, a que carecen de contactos. Otra de las ventajas es la de no tener que introducir la tarjeta en un lector. Esto es una gran ventaja en sistemas de control de accesos, donde se necesita abrir una puerta u otro mecanismo, puesto que la autorización de acceso puede ser operada sin que se tenga que sacar la tarjeta del bolsillo e introducirla en un terminal.

Este tipo de tarjetas se comunican por medio de radiofrecuencias. Según la proximidad necesaria entre tarjeta y lector, existen dos tipos:

- Tarjeta Cercana: debe estar a unos pocos milímetros del lector para que sea posible la comunicación.
- Tarjeta Lejana: la distancia varía entre centímetros y unos pocos metros.

Desde el punto de vista de cómo se alimentan, existen dos tipos:

- Uno en el cual la tarjeta incorpora junto al chip una batería que alimenta a los circuitos.
- Otro tipo que incorpora un hilo metálico incrustado (antena). Este hilo se somete a un campo electromagnético variable que a su vez induce una corriente eléctrica capaz de alimentar los circuitos de la tarjeta.

Seguridad

Existen en la actualidad empresas que han tomado la decisión de basar la seguridad de sus sistemas en las tarjetas inteligentes. La seguridad física de estas es muy alta. Sin el PIN (Personal Identification Number), estas tarjetas no se activan, impidiendo su uso por usuarios no autorizados.

Un problema de seguridad que hasta ahora ha quedado sin resolver, es el de la comunicación entre la tarjeta y el lector. Algunas tarjetas se utilizan sobre redes de comunicaciones como Internet en las que se pueden producir escuchas de información confidencial. Otro de los problemas es el de la autentificación, consistente en asegurar de forma fiable la identidad del interlocutor. La tarjeta tiene que estar segura de que el lector con el que trata o el expendedor de dinero electrónico del que extrae dinero, son de fiar y a su vez los lectores y los sistemas centrales de las aplicaciones financieras, tienen que asegurarse que están tratando con una tarjeta válida.

La criptografía busca resolver tres problemas básicos: confidencialidad, que la información no sea accesible a un usuario no autorizado; integridad, que la información no sea modificada sin autorización y autenticación, que se reconozca de forma fiable la identidad del interlocutor.

Para entender algunas de las aplicaciones de dinero electrónico en tarjetas inteligentes hay que entender también las técnicas criptográficas de demostración de identidad de conocimiento cero (Zero-knowledge proof identity ZKPI).

ZKPI es un protocolo criptográfico, que permite demostrar la identidad de un interlocutor sin que un espía obtenga información que le permita suplantarlo en el futuro. El problema de la identificación por nombre de usuario y clave (muy usada en los sistemas multiusuario), es que un espía que escuche una vez las comunicaciones, obtiene la información suficiente para suplantar al legítimo usuario. El protocolo ZPKI, obvia este problema impidiendo un ataque tan simple como escuchar las comunicaciones cuando se está ejecutando el protocolo de demostración de identidad.

La palabra “criptografía” deriva de “cripto” (oculto) y “grafos” (escritura) y su objetivo es garantizar la privacidad y autenticidad del mensaje y del emisor. En el bando contrario, el criptoanálisis persigue romper la privacidad del mensaje y suplantar al emisor.

La técnica de encriptado, se basa en un algoritmo de cifrado y una clave, de tal forma que se requieren ambos para generar, a partir del texto claro, el texto cifrado. Para descifrar se requieren un algoritmo de descifrado y una clave de descifrado.

Un protocolo criptográfico es aquel que utiliza técnicas criptográficas junto con las reglas de comunicación.

Estos protocolos se utilizan por temas tan diversos como asegurar una comunicación, reconocer al interlocutor, firmar contratos, etc.

La técnica más inmediata para obtener una clave, consiste en probar todas las claves posibles hasta descifrar la correcta. Esta técnica se conoce como “fuerza bruta”. Cuando un atacante conoce un mensaje en claro y cifrado, probará todas las claves posibles, comparando el resultado del descifrado con el texto claro, cuando coinciden ha obtenido la clave.

Cifrado simétrico

Se caracteriza por poseer un único algoritmo de cifrado/descifrado, aunque en la ejecución de ambas operaciones pueden existir pequeñas variaciones y por una única clave para cifrar y descifrar. Esto implica que la clave tiene que permanecer oculta y ser compartida por el emisor y el receptor, lo que significa que se debe distribuir en secreto y se necesita una clave para cada par de interlocutores.

Cifrado asimétrico (clave pública)

Se caracteriza por la existencia de dos claves independientes para cifrar y para descifrar. Esta independencia permite al receptor hacer pública la clave de cifrado, de tal forma que cualquier entidad que desee enviarle un mensaje pueda cifrarlo y enviarlo. La clave de descifrado permanece secreta, por lo que sólo el receptor legitimo puede descifrar el mensaje. Ni siquiera el emisor es capaz de descifrar el mensaje una vez cifrado.

Fortaleza de los algoritmos de cifrado

Dentro de los sistemas criptográficos hay que distinguir entre el algoritmo criptográfico y el protocolo criptográfico. Un algoritmo criptográfico es un mecanismo que permite convertir un texto claro (legible) en otro cifrado (ilegible). Un protocolo criptográfico es un protocolo en el que se utilizan algoritmos criptográficos.

La seguridad de un sistema con protección criptográfica puede venir de la debilidad de sus algoritmos o de sus protocolos, también puede producirse a través de sus claves. Un algoritmo es inseguro cuando existe un método más eficaz que la fuerza bruta para obtener la clave; no es necesario probar todas las claves posibles para obtenerla. Un protocolo es inseguro cuando siendo seguros sus algoritmos criptográficos, es posible debilitar alguna de sus propiedades criptográficas (autenticación, integridad y confidencialidad).

Cifrado Data Encryption Standard (DES)

Es uno de los sistemas criptográficos más utilizados en todo el mundo. Esto no significa que el algoritmo sea el menos vulnerable o el más eficiente, sino que su verdadera importancia reside en la aceptación que ha tenido en el mercado criptográfico, ya que fue uno de los primeros intentos por parte del gobierno de los Estados Unidos por implantar un estándar para transmitir datos digitales de una forma segura.

El DES se define como un algoritmo simétrico cifrador de bloques de 64 bits, es decir, el algoritmo cifra bloques de texto de 64 bits utilizando una clave de 56 bits, generando un bloque de texto cifrado de 64 bits.

Debido al carácter simétrico del algoritmo, se utiliza la misma clave para cifrar y descifrar, usándose también el mismo algoritmo para ambas funciones.

Cifrado RSA

RSA es uno de los algoritmos de clave pública más representativos. Sirve tanto para cifrar como para realizar firmas digitales. Es uno de los pocos algoritmos que se pueden implantar y comprender de una manera sencilla. Su nombre se debe a las iniciales de sus tres inventores, Ron Rivest, Adi Shamir y Leonard Adleman, los cuales crearon el algoritmo en el año de 1977.

La verdadera fortaleza del sistema radica en la dificultad de obtener la clave privada a partir de los datos públicos del sistema.

Aunque existen algoritmos que realizan la firma digital con técnicas de cifrado simétrico, éstos adolecen de la necesidad de enviar claves por separado.

Usos de las Tarjetas Inteligentes

Los usos más comunes de estas tarjetas son:

- Programas de Fidelización.
- Monederos Electrónicos.
- Aplicaciones en Grupos Cerrados.
- Tarjetas de asistencia Médica (Clínicas y Seguros).
- Documentos y Credenciales (Seguridad y Control de Acceso).
- Débito-Crédito.

Las tarjetas inteligentes presentan un costo por transacción que es menor que el de las tarjetas magnéticas convencionales. Esto es incluyendo los costos de la tarjeta, de las infraestructuras necesarias y de los elementos para realizar las transacciones.

Ofrecen prestaciones muy superiores a las de una tarjeta magnética tradicional. Esta ventaja se explica por las configuraciones múltiples que puede tener, lo que permite utilizarla en distintas aplicaciones.

Permiten realizar transacciones en entornos de comunicaciones móviles, en entornos de prepago y en nuevos entornos de comunicaciones. A estos entornos no puede acceder la tarjeta tradicional.

Las mejoras en seguridad y funcionamiento permiten reducir los riesgos y costos del usuario.

Están surgiendo nuevos servicios y aplicaciones que necesitan de esta tecnología, para los cuales las tarjetas de banda magnética no pueden brindar soluciones.

Las tarjetas inteligentes son elementos que sin lugar a dudas se convertirán en un algo cotidiano en nuestras vidas.

La incursión de esta tarjeta en el continente europeo es cada día más grande. La tarjeta inteligente está ganando terreno día a día sobre todo en Francia. En los Estados Unidos aún existe cierta resistencia pero poco a poco está ganando aceptación. No sería extraño pensar que en nuestro país, comiencen a aparecer nuevas aplicaciones y/o servicios, en los que la tarjeta inteligente se torne un elemento fundamental (como sucedió con las tarjetas telefónicas).

En un futuro próximo tal vez las computadoras de escritorio, cuenten con un lector de tarjetas inteligentes integrado, al igual que hoy en día los computadores personales cuentan con una disquetera y con un lector de CDs.

Se presenta la tabla 1.1 que es un resumen de comparación entre tecnologías para identificación con respecto a diversos parámetros de capacidades, costo y distancias.

Tabla 1.1.- Comparación de los diferentes sistemas de identificación.

Parámetros del sistema	**Código de barras**	**OCR**	**Reconocimiento de voz**	**Biometría**	**Tarjeta inteligente**	**Sistema RFID**
Cantidad promedio de datos(bytes)	1-100	1-100	-	-	16-64k	16-64k
Cantidad de datos	Bajo	Bajo	Alto	Alto	Muy alto	Muy alto
Capacidad de lectura en las máquinas	Buena	Buena	Costosa	Costosa	Buena	Buena
Capacidad de lectura por las personas	Limitada	Simple	Simple	Difícil	Imposible	Imposible
Susceptibilidad a la suciedad/humedad	Muy alta	Muy alta	-	-	Posible (contacto)	No influye
Bloqueo de línea de vista	Fallo total	Fallo total	-	Posible	-	No influye
Influencia de la dirección o posición	Baja	Baja	-	-	Unidireccional	No influye
Degradación por el uso	Limitado	Limitado	-	-	Al contacto	No influye
Costo de los lectores	Muy bajo	Medio	Muy alto	Muy alto	Bajo	Medio
Costo de operación	Bajo	Bajo	Ninguno	Ninguno	Medio	Ninguno
Modificaciones y copiado no autorizados	Poco probable	Poco probable	Posibles (audio y video)	Imposible	Imposible	Imposible
Velocidad de lectura	Baja(4s)	Baja(3s)	Muy baja(mas de 5s)	Muy baja(de 5 a 10s)	Baja(4s)	Muy Rápida(0.5s)
Distancia máxima entre el portador de datos y el lector	0-50cm	Menor a 1cm Scanner	0-50cm	Contacto directo	Contacto directo	0-5m microondas

1.2 Tecnología RFID.

Para retomar el propósito central del presente proyecto, introduzcámonos a la tecnología específica de RFID, sin perder de vista que el objetivo central, que es el de: “Realizar una investigación de sistemas basados en etiquetas RFID para la identificación vehicular”, con énfasis en aquellos aspectos que impactan en las características deseadas para el sistema.

En la actualidad, la tecnología más extendida para la identificación de objetos es la de los códigos de barras; sin embargo, éstos presentan algunas desventajas, como son la escasa cantidad de datos que pueden almacenar, la imposibilidad de ser modificados (reprogramados) y los alcances de una automatización. La mejora obvia que se sugirió y que constituye el origen de la tecnología RFID, consiste en usar chips de silicio que pudieran transferir los datos que almacena el vehículo al lector sin contacto físico (de forma equivalente a los lectores de infrarrojos utilizados para leer los códigos de barras).

Cada vez es más frecuente ver tarjetas identificadoras sin contacto con el sistema de lectura. Este tipo de sistemas se llaman abreviadamente RFID (siglas de **R**adio **F**requency **ID**entification, en español *Identificación por radiofrecuencia*). Estos dispositivos están sustituyendo poco a poco a las etiquetas de códigos de barras y a las tarjetas magnéticas en todas sus aplicaciones. Ver figura 1.10.

El sistema de RFID (Radio Frequency IDentification), es la tecnología inalámbrica que nos permite, la comunicación entre un lector y una etiqueta o Transponder. Estos sistemas permiten almacenar información en sus etiquetas, mediante comunicaciones de radiofrecuencia. Esta información puede ir desde 1 Bit hasta 514 KBytes dependiendo principalmente del sistema de almacenamiento que posea el transponder (o Tag).

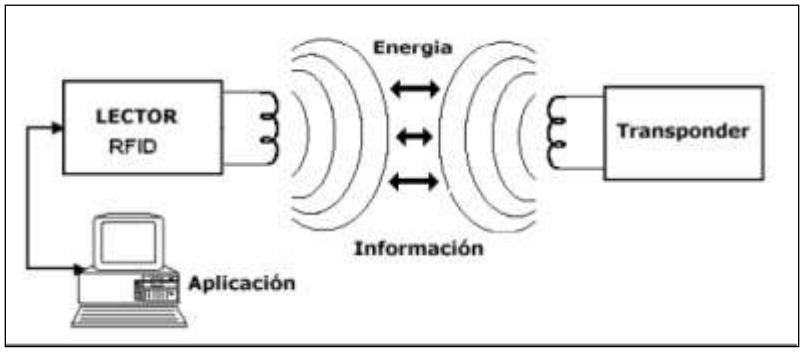


Figura 1.10.- Componentes de un Sistema RFID

1.2.1 Historia del RFID.

Los estudios que se realizaron sobre los campos magnéticos, los trabajos en la primera parte del siglo XIX relacionados con el electromagnetismo se deben a personajes como Maxwell, Hertz, Marconi y muchos más, que contribuyeron al estudio de las ondas de radio y el radar (ondas de radio que rebotan), contribuyeron a sentar las bases, entre otras, para el desarrollo de la RFID. Esta tecnología ha sido producto de pequeñas contribuciones y aportaciones de diversos científicos y técnicos.

Se ha sugerido que el primer dispositivo conocido, similar a RFID, pudo haber sido una herramienta de espionaje inventada por León Theremin para el gobierno soviético en 1945. El dispositivo de Theremin era un dispositivo de escucha secreto, pasivo, no una etiqueta de identificación, por lo que esta aplicación es dudosa. Según algunas fuentes, la tecnología usada en RFID, habría existido desde comienzos del año 1920, desarrollada por el MIT y usada extensivamente por los británicos en la Segunda Guerra Mundial.

Una tecnología similar, el transpondedor de IFF, fue inventada por los británicos en 1939 y fue utilizada de forma rutinaria por los aliados en la Segunda Guerra Mundial, para identificar los aeroplanos como amigos o enemigos. Se trata probablemente de la tecnología citada por la fuente anterior.

Otro trabajo temprano que trata el RFID, es el artículo de 1948 de Harry Stockman, titulado “Comunicación por medio de la energía reflejada” (Actas del IRE, pp. 1196-1204, octubre de 1948). Stockman predijo que “... el trabajo considerable de investigación y de desarrollo tiene que ser realizado antes de que los problemas básicos restantes en la comunicación de la energía reflejada se solucionen en un mundo en y antes de que el campo de aplicaciones útiles se explore.” Hicieron falta treinta años de avances en una multitud de diferentes campos, antes de que RFID se convirtiera en una realidad.

Los sistemas RFID en explotación comercial, no son del todo nuevos, aparecieron en los años 80 y a partir de entonces, han evolucionado incesantemente, lo que ha desarrollado a su vez la tecnología en estas aplicaciones. La tabla 1.2 se muestra un resume del avance de la tecnología RFID.

Tabla 1.2.- Resumen de la evolución de la tecnología RFID.

Década	Avances Tecnológicos
1940-1950	Se rediseña el radar para uso militar tomando gran relevancia en la ª Guerra Mundial. RFID, aparece en 1948.
1950-1960	Primeros experimentos con RFID en laboratorios.
1960-1970	Desarrollo de la tecnología RFID, primeros ensayos en algunos campos de la tecnología.
1970-1980	Explosión de la tecnología. Se realizan más pruebas. Primeras Aplicaciones.
1980-1990	Aparecen más aplicaciones para la tecnología.
1990-2000	RFID toma relevancia en el mundo cotidiano. Aparecen los estándares.

1.2.2 Descripción y Elementos de un Sistema de Radiofrecuencia.

RFID es un sistema de almacenamiento y recuperación de datos de manera remota, que usa dispositivos denominados etiquetas, transpondedores o tags RFID. El propósito fundamental de la tecnología RFID, es transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio frecuencia. Las tecnologías RFID se agrupan dentro de las denominadas Auto ID (Automatic Identification o Identificación Automática).

Una etiqueta RFID es un dispositivo pequeño, similar a una etiqueta, que puede ser adherida o incorporada a un producto, animal o persona. Contienen antenas para permitir recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID. Las pasivas no necesitan alimentación eléctrica interna, mientras que las activas sí lo requieren. Una de las ventajas del uso de radiofrecuencia (en lugar, por ejemplo, de infrarrojos) es que no se requiere visión directa entre emisor y receptor.

Un sistema RFID consta de los siguientes tres componentes:

A.- Etiqueta RFID o Transponder.

Compuesta por una antena, un transductor radio y un material encapsulado o chip. El propósito de la antena es permitirle al chip, el cual contiene la

información, transmitir la información de identificación de la etiqueta. Existen varios tipos de etiquetas.

Las etiquetas RFID pueden ser *activas*, *semi-pasivas* (o *semi-activas*) o *pasivas*.

Las etiquetas RFID pasivas, no tienen fuente de alimentación propia. La mínima corriente eléctrica inducida en la antena, por la señal de escaneo de radiofrecuencia (campo electromagnético) proporciona suficiente energía al circuito integrado CMOS de la etiqueta para poder transmitir una respuesta. Debido a las preocupaciones por la energía y el costo, la respuesta de una etiqueta pasiva RFID es necesariamente breve, normalmente apenas un número de identificación (ID). La falta de una fuente de alimentación propia hace que el dispositivo deba ser bastante pequeño. Existen productos disponibles en forma comercial, que pueden ser insertados bajo la piel. Las etiquetas pasivas, en la práctica tienen distancias de lectura que varían entre 10 milímetros, hasta cerca de 6 metros, dependiendo del tamaño de la antena de la etiqueta y de la potencia y frecuencia en la que opera el lector. En el presente año (2007), el dispositivo disponible comercialmente más pequeño de este tipo, mide 0.05 milímetros × 0.05 milímetros y es más fino que una hoja de papel; estos dispositivos son prácticamente invisibles.

Las etiquetas RFID semi-pasivas, son muy similares a las pasivas, salvo que incorporan, además, una pequeña batería. Esta batería permite al circuito integrado de la etiqueta estar constantemente alimentado. Además, elimina la necesidad de diseñar una antena para recoger potencia de una señal entrante. Por ello, las antenas pueden ser optimizadas para la señal de *backscattering* Las etiquetas RFID semi-pasivas responden más rápidamente, por lo que son más fuertes en la relación de lectura comparadas con las etiquetas pasivas.

Las etiquetas RFID activas, por otra parte, deben tener una fuente de energía y pueden tener rangos mayores y memorias más grandes que las etiquetas pasivas, así como la capacidad de poder almacenar información adicional enviada por el transmisor-receptor. Actualmente, las etiquetas activas más pequeñas tienen un tamaño aproximado de una moneda. Muchas etiquetas activas, tienen rangos prácticos de cien metros y una duración de batería de hasta varios años (5 a 10 aproximadamente).

Como las etiquetas pasivas son más baratas al fabricarse y no necesitan batería, la gran mayoría de las etiquetas RFID existentes en el mercado son del tipo pasivo. En el 2004, las etiquetas tenían un precio desde 0.4 dls, en grandes pedidos. El mercado universal de productos individuales con tecnología RFID, será comercialmente viable con volúmenes muy grandes, de 10,000 millones de unidades al año, llevando el costo de producción a menos de 0,05 dls según un fabricante. La demanda actual de chips de circuitos integrados con RFID, no está cerca de soportar ese costo. Los analistas de las compañías independientes de investigación como Gartner and Forrester Research convienen en que un nivel de precio de menos de

0.10 dls (con un volumen de producción de 1.000 millones de unidades), sólo se puede lograr en unos 6 u 8 años, lo que limita los planes a corto plazo, para una adopción extensa de las etiquetas de RFID pasivas. Otros analistas creen que esos precios serían alcanzables dentro de 10 a15 años.

A pesar de que las ventajas en cuanto al costo de las etiquetas pasivas con respecto a las activas son significativas, otros factores incluyendo exactitud y funcionamiento en ciertos ambientes como cerca del agua o metal y confiabilidad hacen que el uso de etiquetas activas sea muy común hoy en día.

El chip posee una memoria interna con una capacidad que depende del modelo y varía en una decena a millares de bytes. Existen diversos tipos de memoria:

- Sólo lectura: el código de identificación que contiene es único y es personalizado durante la fabricación de la etiqueta.
- De lectura y escritura: la información de identificación puede ser modificada por el lector.
- Anticolisión. Se trata de etiquetas especiales que permiten que un lector identifique varias al mismo tiempo (habitualmente las etiquetas deben entrar una a una en la zona de cobertura del lector).

B.- Lector de RFID o transceptor.

Compuesto por una antena, un transceptor y un decodificador. El lector envía periódicamente señales para ver si hay alguna etiqueta en sus inmediaciones. Cuando capta una señal de una etiqueta (la cual contiene la información de identificación de ésta), extrae la información y se la pasa al subsistema de procesamiento de datos.

C.- Subsistema de procesamiento de datos: proporciona los medios de proceso y almacenamiento de datos.

1.2.3 Funcionamiento Básico de un Sistema de Radiofrecuencia

El modo de funcionamiento de los sistemas RFID es simple. La etiqueta RFID, que contiene los datos de identificación del objeto al que se encuentra adherido, genera una señal de radiofrecuencia con dichos datos cuando se encuentra dentro de la zona de cobertura del Lector de RFID. Esta señal puede ser captada por un lector RFID, el cual se encarga de leer la información y pasársela, en formato digital, a la aplicación específica que utiliza RFID.

Todo sistema RFID se compone de un interrogador o sistema de base que lee y escribe datos en los dispositivos y un *"*transponder*"* o transmisor que responde al interrogador (antena lectora).

- El interrogador genera un campo de radiofrecuencia, normalmente conmutando una bobina a alta frecuencia. Las frecuencias usuales van desde 125 khz hasta la banda ISM de 2.4 Ghz, incluso más.
- El campo de radiofrecuencia (campo eléctrico) genera una corriente eléctrica sobre la bobina de recepción del dispositivo. Esta señal es rectificada y de esta manera se alimenta el circuito o Chip.
- Cuando la alimentación llega a ser suficiente el circuito transmite sus datos.
- El interrogador detecta los datos transmitidos por la tarjeta como una perturbación del propio nivel de la señal.

La señal recibida por el interrogador desde la tarjeta está a un nivel de -60 db por debajo de la portadora de transmisión. El rango de lectura para la mayoría de los casos está entre los 30 y 60 centímetros de distancia entre interrogador y tarjeta, para las aplicaciones en el comercio y la industria.

Podemos encontrar además, dos tipos de interrogadores diferentes:

- Sistemas con bobina simple, la misma bobina sirve para transmitir la energía y los datos. Son más simples y más baratos, pero tienen menos alcance.
- Sistemas interrogadores con dos bobinas, una para transmitir energía y otra para transmitir datos. Son más costosos, pero consiguen unas prestaciones mayores.

1.2.4 Características Tecnológicas Principales

Principios Físicos

Los sistemas de RFID se basan en el envío de información de una unidad móvil, que es el Tag o “transponder” a una unidad fija “lectora o interrogador”.

La trasmisión de información para unidades que están muy cerca una de otra, es por medio de inducción magnética y entre unidades más lejanas por ondas electromagnéticas.

Acoplamientos

La comunicación entre el Tag o “transponder” y la antena lectora, como ya se ha comentado, en función de la aplicación y la distancia entre ambos elementos, puede darse mediante los acoplamientos siguientes:

Close coupling.- Están diseñados para rangos de alcance entre 10 mm y un máximo de 1 cm. El transponder cuando se realiza la comunicación, suele estar en el centro de un aro que es la bobina del lector, o bien, en el centro de una bobina en forma de “U”. El funcionamiento de la bobinas del transponder y de lectores es el mismo que el de un transformador. El lector

representa las espigas primarias y el transponder las secundarias del transformador, es decir en un sistema de este tipo el transponder se inserta en el lector para producir el acoplamiento magnético entre bobinas, ver figura 1.11.

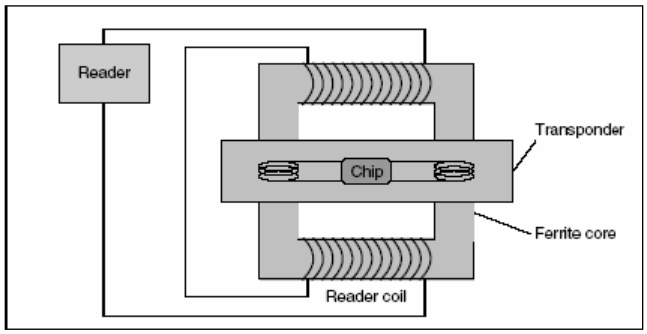


Figura 1.11.- Sistema Close Coupling.

A diferencia con los sistemas de acoplamiento inductivo y de microondas, la eficiencia de la energía trasmitida del lector al transponder es excelente, por eso suelen ser usados en sistemas que necesitan del uso de chips potentes, que consuman mucha energía, como por ejemplo microprocesadores.

Inductivo.- El acoplamiento inductivo opera prácticamente igual que los transformadores de núcleo de aire. Ver figura 1.12.

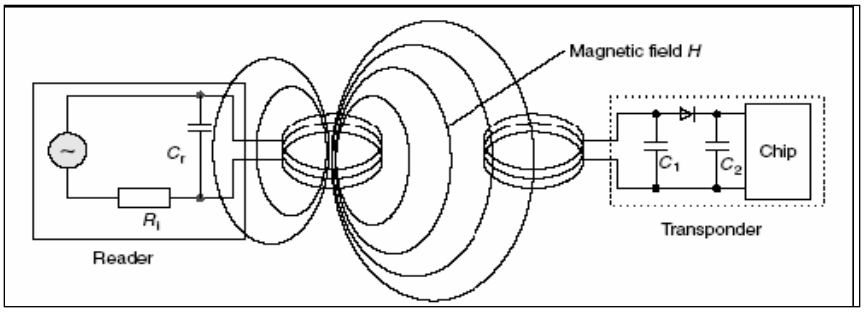


Figura 1.12.- Sistema de acoplamiento inductivo.

El campo creado por la antena del interrogador es la energía que aprovecha del transponder para su comunicación. Este campo está cerca de la antena del interrogador, lo que permite alcanzar una distancia cercana al diámetro de la antena. A distancias mayores la potencia necesaria sería muy elevada. La bobina del lector genera un fuerte campo electromagnético, que penetra la sección de la antena del transponder y en su zona cercana.

Las antenas de estos sistemas son realmente bobinas en los dos elementos. Estos sistemas son para lecturas menores a 1m.

“Backscatter”.- Este es un sistema de transferencia de información de larga distancia mayor a 1 m. Se basan en el uso de ondas electromagnéticas generalmente en el rango de UHF o microondas. Se conocen con este nombre debido a sus principios de operación.

Backscatter es la reflexión de ondas, partículas o señales que regresan en la dirección que fueron generadas o de dónde vienen.

La tecnología en RFID opera en 868 MHz en Europa y 915 en los Estados Unidos y en el rango de microondas en 2.5. GHz y 5.8. La ventaja es de trabajar en una longitud de onda corta lo que permite antenas de un tamaño menor y de gran eficiencia en el transponder.

Estos sistemas tienen un alcance típico de tres metros en transponders pasivos (sin batería) y de unos 15 m en transponders activos. El lector tiene un acoplador direccional para separar la señal transmitida de la señal recibida, mucho más débil, el interrogador detecta los datos transmitidos por la tarjeta como una perturbación del propio nivel de la señal. La señal recibida por el interrogador desde la tarjeta está a un nivel de unos -60 db por debajo de la portadora del propio sensor.

Inducción Magnética

Campo Magnético.- El físico danés Hans Christian Oersted, descubrió en 1820 que cuando una corriente eléctrica (I) fluye a través de un conductor, se forma un flujo magnético (B) alrededor del conductor.

La dirección de las líneas de flujo magnético es siempre a 90° con respecto a la dirección del flujo de la corriente eléctrica.

Cuando un conductor tiene una forma uniforme, la densidad de flujo o número de líneas de fuerza por unidad de área es uniforme a lo largo de la longitud del conductor y decrece uniformemente al incrementar la distancia desde el conductor. Esto se representa en la figura 1.13.

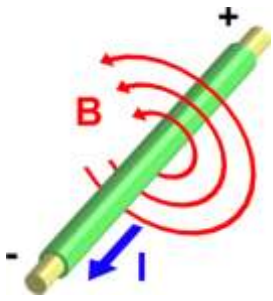


Figura 1.13.- Representación de Campo magnético.

André-Marie Amperé, demostró que el efecto magnético de la corriente en un alambre se puede intensificar enrollándolo en forma de una bobina.

La intensidad del flujo magnético es proporcional al número de vueltas.

Al introducir en la bobina un núcleo de hierro, se obtiene un poderoso electroimán

Fuerza Magnetizante[1] (figura 1.14)

La fuerza magnetizante es la necesaria para crear un flujo magnético en un material.

$$H = \frac{B}{\mu}$$

Figura 1.14.- Ecuación de la fuerza magnetizante.

La permeabilidad magnética[2] (figura 2.15), es la facilidad con la que un material puede ser magnetizado. Es la relación entre la densidad de flujo y la fuerza del campo magnetizante (B/H).

Un material tiene más de un valor de permeabilidad (pendiente de la curva B vs. H).

Sus unidades pueden ser Henry/m ó Gauss/Oersted.

$$\mu = \frac{B}{H}$$

Figura 1.15- Ecuación de la permeabilidad magnética.

B: Densidad de Flujo ó inducción magnética (en Gauss, Tesla ó Weber/m2). Ver figura 1.16.

1 Wb = 108 líneas de flujo.

1 Gauss = 10-4 Wb/m2.

1 Wb/m2 = 1 Tesla.

H Fuerza magnetizante ó intensidad (fuerza) del campo magnético (Oersted, Amper/m ó Amper/cm).

En la figura 1.16 se puede notar que las líneas de flujo magnético alrededor de los conductores en espiral son similares a las empleadas en las antenas transmisoras de los sistemas RFID y de acoplamiento inductivo

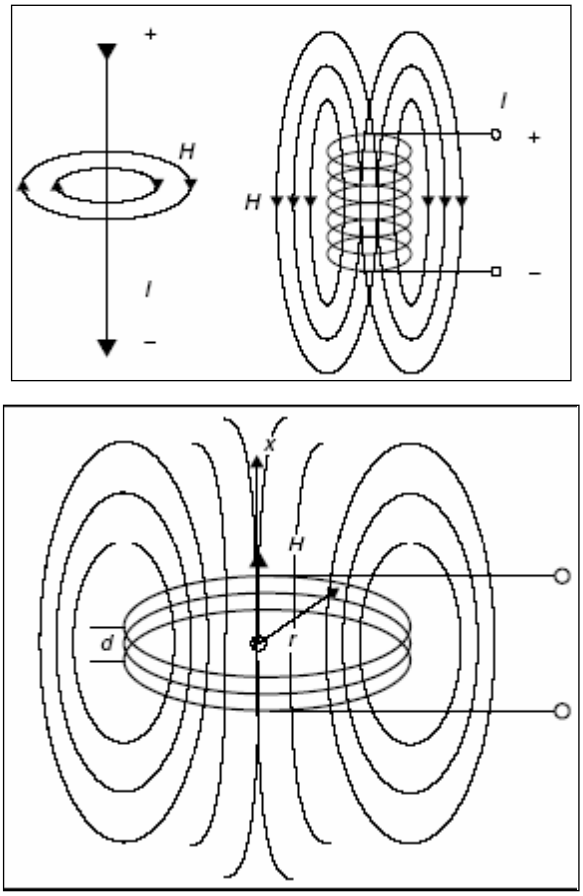


Figura 1.16.- Líneas de flujo magnético.

Densidad de Flujo o Inducción Magnética[3] (figura 1.17)

Es el número de líneas de fuerza por unidad de área.

$$B = \frac{\phi}{A} \qquad B=\mu H$$

Figura 1.17.- Densidad de flujo o Inducción magnética.

ϕ Flujo magnético.¨ **A** Área (m^2)

μ Permeabilidad (Gauss/Oersted ó Henry/m).

H Fuerza magnetizante.

En la figura 1.18, se puede apreciar la representación del flujo magnético

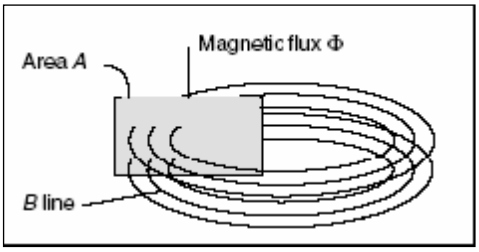


Figura 1.18.- Representación flujo magnético.

La inducción electromagnética, es el fenómeno que origina la producción de una fuerza electromotriz (f.e.m. o voltaje) en un medio o cuerpo expuesto a un campo magnético variable, o bien en un medio móvil respecto a un campo magnético estático. Es así que, cuando dicho cuerpo es un conductor, se produce una corriente inducida. Este fenómeno fue descubierto por Michael Faraday quién lo expresó indicando que la magnitud del voltaje inducido es proporcional a la variación del flujo magnético (Ley de Faraday).

Por otra parte, Heinrich Lenz, comprobó que la corriente debida a la f.e.m. inducida, se opone al cambio de flujo magnético, de forma tal que la corriente tiende a mantener el flujo. Esto es válido, tanto para el caso en que la intensidad del flujo varíe, o que el cuerpo conductor se mueva respecto a él.

En sistemas RFID inductivos, existe un acoplamiento magnético inductivo generado por la antena lectora y la antena del Tag o transponder, induciéndose en este segundo, un voltaje que se utiliza como alimentación para el chip en un proceso de almacenamiento de datos en memoria. Desde luego, las antenas tienen que estar en resonancia, en la frecuencia de operación del sistema RFID.

La inducción se produce por la proximidad de dos conductores en forma de espira y la corriente que atraviesa una de las espiras induce un flujo magnético en la otra espira y viceversa. La magnitud del flujo inducido depende de las dimensiones de ambos conductores, de la posición de un conductor respecto a lo otro y las propiedades magnéticas del medio. Dado

que existe influencia entre ambos, a este fenómeno se le llama “inductancia mutua”.

En la figura 1.19, se representa la inductancia mutua por dos espiras, donde L1 representa la antena lectora y L2 el Tag o transponder.

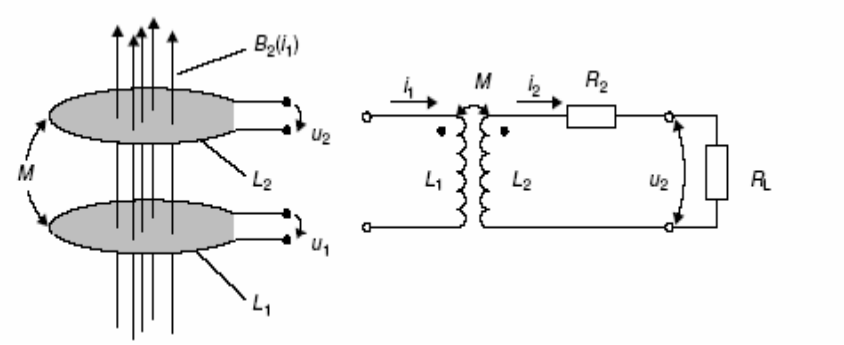


Figura 1.19.- Inductancia mutua.

El coeficiente de acoplamiento es un valor entre cero y uno que representa el grado de inducción creada entre dos espiras, donde el valor de “1” representa un acoplamiento total; es decir, las dos espiras están sometidas al mismo campo magnético.

Es por ello que en el diseño de un sistema RFID, el diámetro de antena es determinante ya que si es demasiado grande, se tendrá mayor alcance, pero el campo magnético cerca del centro de la espira será muy débil y si escogemos un radio pequeño nos encontramos un campo magnético que decrece rápidamente. En la práctica, en sistemas inductivos, el óptimo para el radio de la antena de inducción debe ser el doble del máximo alcance de lectura deseado.

Ondas Electromagnéticas

La radiación electromagnética, es una combinación de campos eléctricos y magnéticos oscilantes, que se propagan a través de espacio transportando energía de un lugar a otro. Su representación la podemos ver en la figura 1.20.

A diferencia de otros tipos de onda, como el sonido, que necesitan un medio material para propagarse, la radiación electromagnética se puede propagar en el vacío.

En el siglo XIX, se pensaba que existía una sustancia indetectable, llamada éter, que ocupaba el vacío y servía de medio de propagación de las ondas electromagnéticas.

El estudio teórico de la radiación electromagnética, se denomina electrodinámica y es un subcampo del electromagnetismo.

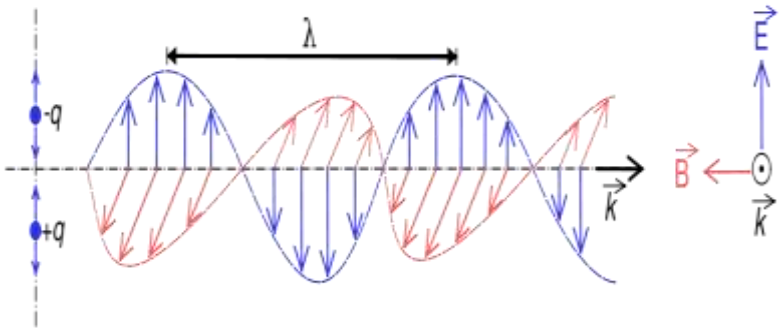


Figura 1.20.- Representación de las ondas electromagnéticas

Maxwell, reunió unas ecuaciones, (actualmente denominadas ecuaciones de Maxwell), de las que desarrolla que un campo eléctrico variable en el tiempo, genera un campo magnético y, recíprocamente, la variación temporal del campo magnético genera un campo eléctrico. Se puede visualizar la radiación electromagnética, como dos campos que se generan mutuamente, por lo que no necesitan de ningún medio material para propagarse. Las ecuaciones de Maxwell, también predicen la velocidad de propagación en el vacío (que se representa *c*, por la velocidad de la luz, con un valor de 299.792 km/s) y su dirección de propagación es perpendicular a las oscilaciones del campo eléctrico y magnético que, a su vez, son perpendiculares entre sí.

Atendiendo a su longitud de onda, la radiación electromagnética recibe diferentes nombres y varía desde los energéticos rayos gamma (con una longitud de onda del orden de picómetros), hasta las ondas de radio (longitudes de onda del orden de kilómetros), pasando por el espectro visible (cuya longitud de onda está en el rango de las décimas de micra). El rango completo de longitudes de onda es lo que se denomina el espectro electromagnético.

El espectro visible es un minúsculo intervalo que va desde la longitud de onda correspondiente al color violeta (aproximadamente 400 nanómetros), hasta la longitud de onda correspondiente al color rojo (aproximadamente 700 nm).

En telecomunicaciones, las ondas se clasifican mediante un convenio internacional de frecuencias, en función del empleo al que están destinadas, como se aprecia en la tabla 1.3:

Tabla 1.3.- Clasificación de las Ondas en Telecomunicaciones.

Sigla	Rango	Denominación	Empleo
VLF	10 kHz a 30 kHz	Muy baja frecuencia	Radio gran alcance
LF	30 kHz a 300 kHz	Baja frecuencia	Radio, navegación
MF	300 kHz a 3 MHz	Frecuencia media	Radio de onda media
HF	3 MHz a 30 MHz	Alta frecuencia	Radio de onda corta
VHF	30 MHz a 300 MHz	Muy alta frecuencia	TV, radio
UHF	300 MHz a 3 GHz	Ultra alta frecuencia	TV, radar
SHF	3 GHz a 30 GHz	Super alta frecuecia	Radar
EHF	30 GHz a 300 GHz	Extra alta frecuencia	Radar

Cuando un alambre o cualquier objeto conductor, tal como una antena, conduce corriente alterna, la radiación electromagnética se propaga en la misma frecuencia que la corriente.

De forma similar, cuando una radiación electromagnética incide en un conductor eléctrico, propicia que los electrones de su superficie oscilen, generándose de esta forma una corriente alterna cuya frecuencia es la misma que la de la radiación incidente. Este efecto se utiliza en las antenas, que pueden actuar como emisores o receptores de radiación electromagnética.

La radiación electromagnética, reacciona de manera desigual en función de su frecuencia y del material con el que entra en contacto. El nivel de penetración de la radiación electromagnética es inversamente proporcional a su frecuencia. Cuando la radiación electromagnética es de baja frecuencia, atraviesa limpiamente las barreras a su paso. Cuando la radiación electromagnética es de alta frecuencia, reacciona más con los materiales que tiene a su paso.

En función de la frecuencia, las ondas electromagnéticas pueden no atravesar medios conductores. Esta es la razón por la cual las transmisiones de radio, no funcionan bajo el mar y los teléfonos móviles se queden sin cobertura dentro de una caja de metal. Sin embargo, como la energía ni se crea ni se destruye, sino que se transforma, cuando una onda

electromagnética choca con un conductor, pueden suceder dos cosas. La primera es que se transformen en calor: Este efecto, tiene aplicación en los hornos de microondas. La segunda, es que se reflejen en la superficie del conductor (como en un espejo).

La energía transportada por las ondas electromagnéticas se almacena en los campos eléctrico y magnético de la onda.

La polarización de una onda electromagnética se determina por la dirección del campo eléctrico de la onda. Las líneas del campo eléctrico, se desplazan en paralelo o perpendicular a la superficie terrestre. Las transmisiones de energía entre dos antenas linealmente polarizadas es máximo, cuando las dos antenas están polarizadas en la misma dirección y mínima cuando forman un ángulo de 90° ó 270°

En los sistemas de RFID no podemos conocer cuál será la orientación entre la antena del Tag o transponder y la de la antena lectora. El problema se resuelve, usando polarización circular del lector de la antena; se trata de dos dipolos unidos en forma de cruz.

La comunicación por ondas electromagnéticas, entre el transponder o Tag y la antena lectora, es en sí una radiocomunicación y la elección de la antena es uno de los principales parámetros de diseño de un sistema de RFID.

Una antena isotrópica es una antena ideal que radia uniformemente en todas direcciones; se puede definir como ganancia[4], el factor de intensidad de radiación de una antena respecto a la intensidad de una antena isotrópica, representado en dBi, ver figura 1.21.

P (isotrópica)= P (antena) G (Ganancia)

Cuando el transponder se encuentran el rango de alcance del lector, este emite una onda electromagnética con una potencia efectiva de P_1G_1, el transponder recibe una potencia proporcional P_2 al campo E y a la distancia "r". La potencia Ps es la reflejada por la antena del transponder y la potencia P_3 es recibida por el lector a una distancia "r".

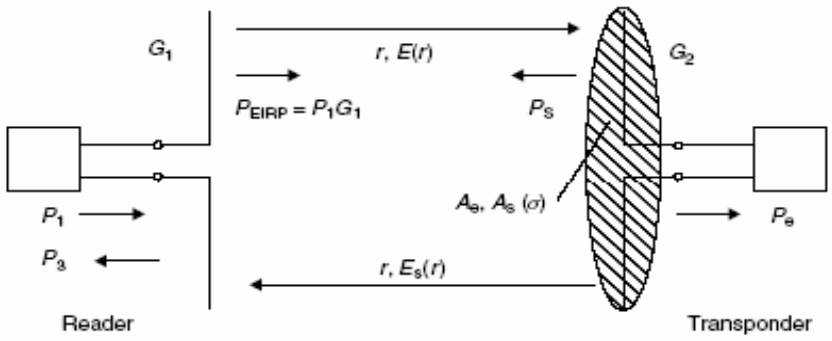


Figura 1.21.- Representación de la Potencia Isotrópica.

Códigos y Modulaciones

En la figura 1.22 se describe el sistema de comunicación digital; en forma semejante, la transferencia de datos entre lectores de etiqueta de un sistema RFID, requiere de tres bloques básicos de funcionamiento:

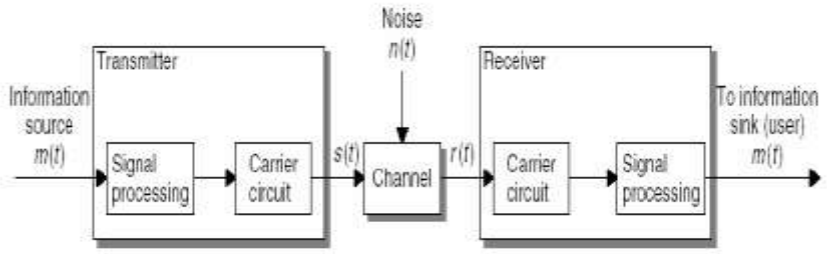


Figura 1.22.- Bloques de Funcionamiento de un Sistema RFID.

- El lector (Transmitter): codificación de señal (signal processing) y el modulador (carrier circuit).
- El medio de transmisión (Channel).
- En la etiqueta (Receiver): el demodulador (carrier circuit) y el decodificador de canal (signal processing).

Como puede observarse, la codificación forma parte de la forma en que “se comunican” los dispositivos. El sistema codificador de señal toma el mensaje a transmitir y su representación en forma de señal y la adecua óptimamente a las características del canal de transmisión. Este proceso implica proveer al mensaje con protección contra interferencias o colisiones y contra modificaciones intencionadas de ciertas características de la señal.

Existen distintas formas de codificación: código NRZ; código Manchester; código unipolar RZ; código DBP; código Miller; código Miller modificado; codificación diferencial; codificación pulso-pausa. Una descripción abreviada de estos métodos puede observarse en el “Estudio, diseño y simulación de un sistema de RFID basado en EPC”[5] de José María Ciudad Herrera y Eduardo Samá Casanovas; de la Universidad Politécnica de Cataluña, España.

Modulaciones

En telecomunicación, el término modulación engloba el conjunto de técnicas para transportar información sobre una onda portadora, típicamente una onda senoidal. Estas técnicas permiten un mejor aprovechamiento del canal de comunicación, lo que posibilita transmitir más información en forma simultánea, protegiéndola de posibles interferencias y ruidos.

Básicamente, la modulación consiste en hacer que un parámetro de la onda portadora cambie de valor de acuerdo con las variaciones de la señal moduladora, que es la información que queremos transmitir.

La tecnología RFID, está fuertemente implicada con los métodos analógicos de modulación. Podemos identificar la modulación de amplitud (AM), la modulación de frecuencia (FM) y la modulación de fase (PM), que son las principales variables de una onda electromagnética. Todo los demás métodos se derivan de alguno de ellos.

Las modulaciones usadas en RFID son:

- ASK (amplitude shift keying) (modulación por desplazamiento de amplitud).
- FSK (frecuency shift keying) (modulación por desplazamiento de frecuencia).
- PSK (phase shift keying) (modulación por desplazamiento de fase).

Amplitud Modulada.- Básicamente, la modulación consiste en hacer que un parámetro de la onda portadora, cambie de valor de acuerdo con las variaciones de la señal moduladora, que es la información que queremos transmitir.

Frecuencia Modulada (FM).- o Modulación de frecuencia, es el proceso de codificar información, la cual puede estar tanto en forma digital como analógica, en una onda portadora mediante la variación de su frecuencia instantánea, de acuerdo con la señal de entrada. El uso más típico de este tipo de modulación es la radiodifusión en FM.

La modulación de frecuencia, requiere un ancho de banda mayor que la modulación de amplitud para una señal modulante equivalente. No obstante, este hecho, propicia que la señal modulada en frecuencia, sea más resistente a las interferencias. La modulación de frecuencia, también es más robusta, ante fenómenos de desvanecimiento de amplitud de la señal recibida. Es por ello que la FM, fue elegida como la norma de modulación para las transmisiones radiofónicas de alta fidelidad.

Una señal modulada en frecuencia, puede ser también utilizada para transportar una señal estereofónica. Sin embargo, esto se hace mediante multiplexación de los canales izquierdo y derecho de la señal estéreo, antes del proceso de modulación de frecuencia.
De forma inversa, en el receptor se lleva a cabo la demultiplexación, después de la demodulación de la señal FM. Por lo tanto, el proceso estereofónico es totalmente ajeno a la modulación en frecuencia, propiamente dicho.

La utilización de la modulación de frecuencia para su uso en radio, fue descrita por primera vez en 1935, por Edwin Armstrong en un documento titulado “Método para reducir la perturbación de la señalización por radio mediante un Sistema de Modulación de Frecuencia”[6].

En la figura 1.23 se puede notar un caso particular simple de modulación de frecuencia, es la denominada modulación por desplazamiento de frecuencia (FSK)

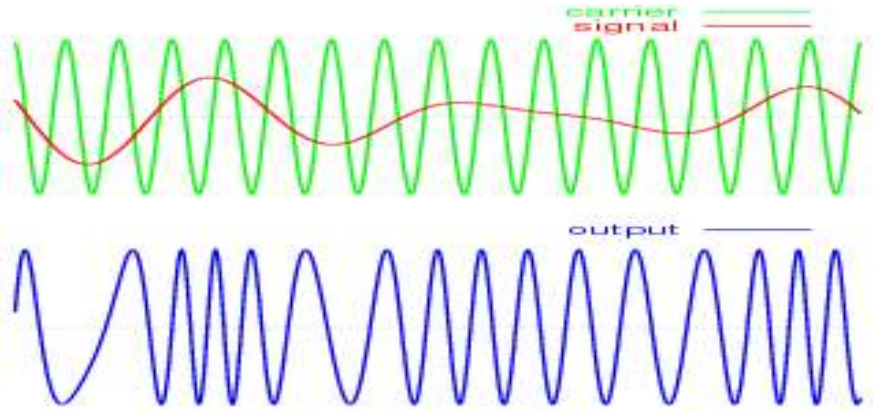


Figura 1.23.- Modulación por desplazamiento de frecuencia (FSK)

Modulación de Fase.- Es el caso de modulación, donde tanto las señales de transmisión como las señales de datos son analógicas. Es un tipo de modulación exponencial, al igual que la modulación de frecuencia. Se caracteriza porque la fase de la onda portadora varía directamente de acuerdo con la señal modulante, resultando una señal de modulación en fase.

La modulación de fase, no suele ser muy utilizada porque se requieren equipos de recepción más complejos que las señales moduladas en frecuencia. Además, puede presentar problemas de ambigüedad para determinar, por ejemplo, si una señal tiene una fase de 0º ó 180º

Por lo tanto, si variamos la fase de una portadora con amplitud constante, directamente proporcional a la amplitud de la señal modulante, con una velocidad igual a la frecuencia de la señal modulante, obtenemos la PM (Phase Modulation).

Para conseguir mayor alcance y más inmunidad al ruido eléctrico, se utilizan sistemas más sofisticados. En algunos casos se divide la frecuencia del reloj de recepción.

Frecuencias

Los sistemas RFID se clasifican, dependiendo del rango de frecuencias que usan. Existen cuatro tipos de sistemas: de frecuencia baja (entre 125 ó 134,2 kilohercios); de alta frecuencia (13,56 megahercios); UHF o de frecuencia ultra elevada (868 a 956 megahercios); y de microondas (2,45 gigahercios). Los sistemas UHF no pueden ser utilizados en todo el mundo, porque no existen regulaciones globales para su uso.

No hay ninguna corporación pública global, que gobierne las frecuencias usadas para RFID. En principio, cada país puede fijar sus propias reglas.

Las principales corporaciones que gobiernan la asignación de las frecuencias para RFID son:

- E.U.A.: FCC (Federal Communications Commission).
- Canadá: DOC (Departamento de la Comunicación).
- Europa: ERO, CEPT, ETSI y administraciones nacionales. Obsérvese que las administraciones nacionales tienen que ratificar el uso de una frecuencia específica, antes de que pueda ser utilizada en ese país.
- Japón: MPHPT (Ministry of Public Management, Home Affairs, Post and Telecommunication).
- China: Ministerio de la Industria de Información.
- Australia: Autoridad Australiana de la Comunicación (Australian Communication Authority).
- Nueva Zelanda: Ministerio de Desarrollo Económico de Nueva Zelanda (New Zealand Ministry of Economic Development.

Las etiquetas RFID de baja frecuencia (LF: 125 - 134 kHz y 140 - 148.5 kHz) y de alta frecuencia (HF: 13.56 MHz), se pueden utilizar de forma global, sin necesidad de licencia. La frecuencia ultra alta (UHF: 868 - 928 MHz), no puede ser utilizada de forma global, ya que no existe un único estándar global. En Norteamérica, la frecuencia ultra elevada se puede utilizar sin licencia para frecuencias entre 908 - 928 MHz, pero hay restricciones en la energía de transmisión. En Europa, la frecuencia ultra elevada, está bajo consideración para 865.6 - 867.6 MHz. Su uso es sin licencia, sólo para el rango de 869.40 - 869.65 MHz, pero existen restricciones en la energía de transmisión. El estándar UHF norteamericano (908-928 MHz), no es aceptado en Francia e Italia, ya que interfiere con sus bandas militares. En China y Japón no hay regulación para el uso de la frecuencia ultra elevada. Cada aplicación de frecuencia ultra elevada en estos países necesita de una licencia, que debe ser solicitada a las autoridades locales y puede ser revocada. En Australia y Nueva Zelanda, el rango es de 918 - 926 MHz para uso sin licencia, pero hay restricciones en la energía de transmisión.

Existen regulaciones adicionales, relacionadas con la salud y condiciones ambientales. Por ejemplo, en Europa, la regulación Waste Electrical and Electronic Equipment (“Equipos eléctricos y electrónicos inútiles”), no permite que se desechen las etiquetas RFID. Esto significa que las etiquetas RFID que estén en cajas de cartón, deben de ser retiradas, antes de deshacerse de ellas. Asimismo, existen regulaciones adicionales, relativas a la salud.

Seguridad - Encriptación

En algunos casos, el uso de los sistemas de identificación por radiofrecuencia, necesitará el uso de sistemas de seguridad para protegerlo de ataques.

Se pueden destacar algunos de estos requerimientos de seguridad: confidencialidad, integridad y autenticidad. Esto es, la lectura no autorizada del portador de la información o poder conseguir una réplica, modificar la información o carecer de elementos de autenticidad; colocar una portadora de información extraña en la zona de influencia del interrogador, con la intención de obtener un acceso no autorizado a un edificio o a una serie de servicios, sin tener que pagarlos; escuchar sin ser advertido, las comunicaciones de radio e introducir datos, imitando una portadora original.

No obstante lo anterior, hay sistemas que según su finalidad, como es el caso de la automatización industrial o el reconocimiento de herramientas o incluso el registro de un automóvil, no necesitan añadir costos adicionales por medidas de seguridad. Eventualmente, el requisito será el de autentificación del dispositivo para garantizar que es un elemento del sistema operado.

Al mismo tiempo, se ha de considerar que en caso de que los sistemas necesiten seguridad, omitirla por economía, puede suponer un gasto posterior más elevado, si alguien consiguiese acceso ilegal a servicios restringidos.

Existen diversos métodos para asegurar la información (encriptarla), sobre los cuales, se dispone de una basta bibliografía.

Algunos sistemas, utilizan encriptación de clave pública para conseguir mayor seguridad, ante posibles escuchas maliciosas.

Control de Errores

Los canales para transmitir señales con información útil o que requiere de interpretación exacta, tienen un riesgo elevado de pérdida de información durante la transmisión, si no se implantan métodos que eviten, en cierta medida, los errores.

El control de errores, se utiliza para reconocerlos en la trasmisión e iniciar medidas de corrección como por ejemplo, pedir la retransmisión de los bloques de datos erróneos. Las medidas más comunes de control de errores, son el control de paridad, la suma XOR (OR exclusiva), el LRC (Longitudinal Redundancy Check) y el CRC(Cyclic Redundancy Check).

El control de paridad es un método sencillo y común. Incorpora 1 bit de paridad en cada byte trasmitido, con un resultado de 9 bits enviados por cada byte de información. Definiendo previamente si se establece una paridad par o impar, para asegurar que el emisor y el receptor realicen el control adecuado.

Multiacceso

Por otro lado, podemos encontrar sistemas anticolisión que permiten leer varias tarjetas al mismo tiempo. En caso de que varias tarjetas estén en el rango de alcance del interrogador y dos o más quieran transmitir al mismo tiempo, se produce una colisión. El interrogador detecta la colisión y ordena parar la transmisión de las tarjetas durante un tiempo. Después, irán respondiendo cada una por separado, por medio de instrucciones derivadas de algoritmos bastante complejos.

La comunicación de la antena lectora hacia los Tags o transponders, se da a través de un flujo de datos, trasmitido a todos simultáneamente. Este tipo de comunicación, es la que se conoce como “broadcast”

A la comunicación desde muchas etiquetas que se encuentran en la zona de interrogación, hacia el lector se le llama de “multiacceso”. En este caso, la capacidad del canal que se tenga disponible debe dividirse entre los participantes (etiquetas), sin que sufran interferencias unos, por culpa de los otros.

Esta es la razón por la que se han desarrollado numerosos métodos, con el propósito de separar la señal de cada participante, de la de otros. Se identifican cuatro métodos diferentes: acceso múltiple por división de espacio (space división multiple Access SDMA); acceso múltiple por división de frecuencia (Frequency domain multiple accsess FDMA) acceso múltiple por división de tiempo (time domain multiple Access TDMA) y acceso múltiple por división de código (code división multiple Access)

Memoria

La mayor parte de los sistemas, tienen una memoria EEPROM (Electronic Erasable Programmable read-only memory), donde se almacenan datos. En algunos casos, llevan datos grabados de fábrica y en otros también hay datos que puede grabar el usuario.

Los chips de fabricantes que cumplen con la norma EPC contienen un campo de identificación del chip que su vez contiene cuatro partes: versión, fabricante, clase de objeto y número de serie.

Los demás campos de la memoria se graban con la información necesaria para la aplicación correspondiente. Los chips pueden tener la capacidad para almacenar hasta 128 kb.

1.3 Métodos de Evaluación y Decisión Multicriterio.

2.3.1 El Proceso de toma de decisiones.

“La toma de decisiones es un proceso de selección entre cursos alternativos de acción, basado en un conjunto de criterios, para alcanzar uno o más objetivos”[7]

Un proceso de toma de decisión comprende de manera general los siguientes pasos:

- Análisis de la situación:
- Identificación y formulación del problema;
- Identificación de aspectos relevantes que permitan evaluar las posibles soluciones.
- Identificación de las posibles soluciones;
- Aplicación de un modelo de decisión para obtener un resultado global y;
- Realización de análisis de sensibilidad.

La opinión de una sola persona en la toma de decisión puede tornarse insuficiente cuando se analizan problemas complejos, sobre todo aquellos cuya solución puede afectar a muchas otras personas. Debido a lo anterior se debe propiciar generar discusión e intercambio entre los actores, que por su experiencia y conocimiento pueden ayudar a estructurar el problema y a evaluar las posibles soluciones.

Para abordar una situación de un problema de toma de decisión en la que se presentan diversos objetivos o criterios que simultáneamente deben incorporarse, ha surgido la Metodología Multicriterio como Sistema de Ayuda a la Decisiones del ser humano.

1.3.2 Los Métodos de Evaluación y Decisión Multicriterio

Los métodos de evaluación y decisión multicriterio se utilizan especialmente para tomar decisiones frente a problemas que cobijan aspectos intangibles a evaluar por lo que en el proceso y en sus componentes, se pueden incorporar diversas metodologías.

Los métodos de evaluación y decisión multicriterio no consideran la posibilidad de encontrar una solución óptima. En función de las preferencias del agente decisor y de objetivos pre-definidos (usualmente conflictivos), el problema central de los métodos multicriterio consiste en seleccionar la o las mejores alternativas dentro de un conjunto de posibles soluciones a un problema.

Un criterio clasificador en la decisión multicriterio corresponde al número, que puede ser finito o infinito, de las alternativas a tener en cuenta en la decisión. Dependiendo de esta situación existen diferentes métodos. Cuando las funciones objetivo, toman un número infinito de valores distintos, que conducen a un número infinito de alternativas posibles del problema tenemos la necesidad de tomar una decisión multiobjetivo.

Aquellos problemas en los que las alternativas de decisión son finitas se denominan problemas de Decisión Multicriterio Discreta. Estos problemas

son los más comunes en la realidad y son los que se consideran en este apartado.

Los métodos de Decisión Multicriterio Discreta se utilizan para realizar una evaluación y decisión respecto de problemas que, por naturaleza o diseño, admiten un número finito de alternativas de solución, a través de:

- Un conjunto de alternativas estables, generalmente finito de soluciones (soluciones factibles que cumplen con las restricciones- posibles o previsibles); se asumen que cada una de ellas es perfectamente identificada, aunque no son necesariamente conocidas en forma exacta y completa todas sus consecuencias cuantitativas y cualitativas;
- Una familia de criterios de evaluación (atributos, objetivos deseados) que van a permitir evaluar cada una de las alternativas (analizar sus consecuencias), conforme a los pesos (o ponderaciones) asignados por el agente decisor y que reflejan la importancia (preferencia) relativa de cada criterio;
- Una matriz de decisión o de impactos que resumen la evaluación de cada alternativa de solución, conforme a cada criterio; una valoración (precisa o subjetiva) de cada una de las soluciones a la luz de cada uno de los criterios; la escala de medida de las evaluaciones puede ser cuantitativa o cualitativa y las medidas pueden expresarse en escalas cardinal (razón o intervalo), ordinal, nominal y probabilística;
- Una metodología o modelo de agregación de preferencias en una síntesis global; ordenación, clasificación, partición o jerarquización de dichos juicios para determinar la solución que globalmente recibe las mejores evaluaciones;
- Un proceso de toma de decisiones (contexto de análisis) en el cual se lleva a cabo una negociación consensual entre los actores o interesados (analista, experto, decisor y usuario).

A partir de esta estructura conceptual existen diversos métodos de evaluación y decisión multicriterio discretos como son:

- Ponderación Lineal (scoring),
- Utilidad multiatributo (MAUT),
- Relaciones de superación y
- Análisis Jerárquico (AHP- The Analytic Hierarchy Process-Proceso Analítico Jerárquico).

La diferencia entre los distintos métodos radica en la forma en que se deben de ponderar los atributos de lo deseado, como darle consistencia a

esta calificación y la forma de calificar, para cada parámetro, las distintas alternativas de solución que se tienen, por ejemplo.

1.3.3 El Proceso Analítico Jerárquico

El Proceso de Análisis Jerárquico (AHP, The Analytic Hierarchy Process) fue desarrollado por el matemático Thomas Saaty[8] y consiste en formalizar la comprensión intuitiva de problemas complejos mediante la construcción de un Modelo Jerárquico.

El propósito del método es permitir que el agente decisor pueda estructurar un problema multicriterio en forma visual, mediante la construcción de un Modelo Jerárquico que básicamente contiene tres niveles: meta u objetivo, criterios y alternativas.

Una vez construido el Modelo Jerárquico, se realizan comparaciones entre pares de dichos elementos (criterios-sub-criterios y alternativas) y se atribuyen valores numéricos a las preferencias señaladas por las personas, entregando una síntesis de las mismas mediante la agregación de esos juicios parciales.

El fundamento del proceso de Saaty descansa en el hecho que permite dar valores numéricos a los juicios dados por las personas, logrando medir cómo contribuye cada elemento de la jerarquía al nivel inmediatamente superior del cual se desprende.

Para estas comparaciones se utilizan escalas de razón en términos de preferencia, importancia o probabilidad, sobre la base de una escala numérica propuesta por el mismo Saaty, que va desde 1 hasta 9.

Una vez obtenido el resultado final, el AHP permite llevar a cabo el análisis de sensibilidad.

El AHP posee un software de apoyo y su aplicación comprende una variada gama de experiencias prácticas en campos muy diversos en diferentes países del mundo.

Actualmente existen en el mercado varios paquetes informáticos dedicados a la Decisión Multicriterio Discreta como lo son el AIM, ELECTRE, PROMCALC, MCView, entre otros.

Específicamente en el caso del AHP, se encuentran productos comerciales como: HIPRE 3+ INPRE, Expert Choice y Criterium® entre otros.

Muchos de ellos presentan interfaces amigables para el usuario y ofrecen completos resultados y análisis de sensibilidad. Algunos sitios permiten bajar de internet demostraciones gratuitas.

El Método fué desarrollado por el doctor en matemáticas Thomas Saaty, a fines de la década de los 80 para resolver el tratado de reducción de armamento estratégico entre los Estados Unidos y la otrora URSS.

El AHP, mediante la construcción de un modelo jerárquico, permite de una manera eficiente y gráfica organizar la información respecto de un problema, descomponerlo y analizarlo por partes, visualizar los efectos de cambios en los niveles y sintetizar.

El AHP se fundamenta en:

- La estructuración del modelo jerárquico (representación del problema mediante identificación de metas, criterios, sub-criterios y alternativas);
- Priorización de los elementos del modelo jerárquico;
- Comparaciones entre pares de elementos;
- Evaluación de los elementos mediante asignación de “pesos”;
- Ranking de las alternativas de acuerdo con los pesos dados;
- Síntesis;
- Análisis de Sensibilidad.

El AHP es una herramienta metodológica que ha sido aplicada en varios países para incorporar las preferencias de actores involucrados en un conflicto y/o proceso participativo de toma de decisión.

Dentro de las posibilidades de aplicaciones de la herramienta están entre otras:

- Formulación de políticas;
- Selección de equipos
- Priorización cartera de proyectos;
- Gestión Ambiental;
- Análisis costo beneficio; y
- Formulación de Estrategias de Mercado.

Algunas de las ventajas del AHP frente a otros métodos de Decisión Multicriterio son:

- Un sustento matemático;
- Permitir desglosar y analizar un problema por partes;
- Permitir medir criterios cuantitativos y cualitativos mediante una escala común;
- Incluir la participación de diferentes personas o grupos de interés y generar un consenso;
- Permitir verificar el índice de consistencia y hacer las correcciones, si es del caso;
- Generar una síntesis y dar la posibilidad de realizar análisis de sensibilidad; y

- Ser de fácil uso y permitir que su solución se pueda complementar con métodos matemáticos de optimización.

1.3.4 Base matemática del AHP

De acuerdo con el creador del método, el "AHP trata directamente con pares ordenados de prioridades de importancia, preferencia o probabilidad de pares de elementos en función de un atributo o criterio común representado en la jerarquía de decisión. Creemos que este es el método natural (pero refinado) que la gente siguió al tomar decisiones mucho antes que se desarrollaran funciones de utilidad y antes que se desarrollara formalmente el AHP"[9]

"El AHP hace posible la toma de decisiones grupal mediante el agregado de opiniones, de tal manera que satisfaga la relación recíproca al comparar dos elementos. Luego toma el promedio geométrico de las opiniones. Cuando el grupo consiste en expertos, cada uno elabora su propia jerarquía y el AHP combina los resultados por el promedio geométrico"[10]

Los axiomas del AHP son:

- Axioma No. 1 Referente a la condición de juicios recíprocos: La intensidad de preferencia de Ai/Aj es inversa a la preferencia de Aj/Ai.
- Axioma No. 2 Referente a la condición de homogeneidad de los elementos: Los elementos que se comparan son del mismo orden de magnitud.
- Axioma No. 3 Referente a la condición de estructura jerárquica o estructura dependiente de reaprovechamiento. Dependencia en los elementos de dos niveles consecutivos en la jerarquía y dentro de un mismo nivel.
- Axioma No. 4 Referente a condición de expectativas de orden de rango: Las expectativas deben estar representadas en la estructura en términos de criterios y alternativas.

En la figura 1.24 la matriz de relaciones paralelas entre ponderaciones, criterios y alternativas, de acuerdo con la descripción que da el Dr. Saaty[11]

Suponga que se tienen n piedras, A1,…,An con ponderaciones conocidas w1,…,wn, respectivamente y suponga que se forma una matriz de relaciones paralelas cuyas filas dan la relación de las ponderaciones de cada piedra con respecto a todas las otras. Por lo tanto se tiene la ecuación:

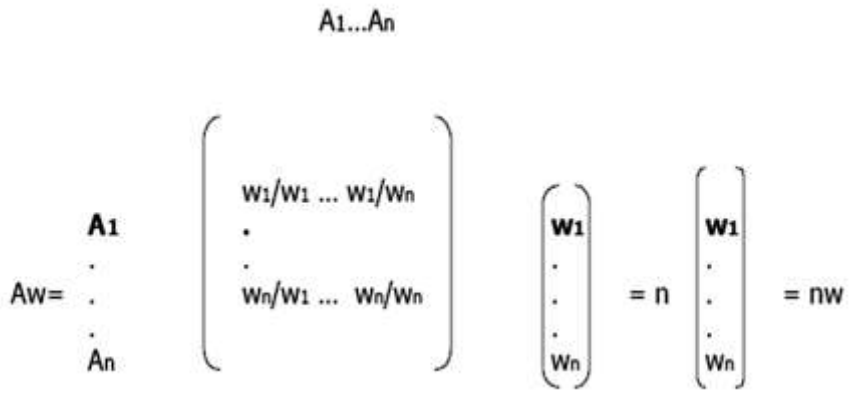


Figura 1.24 Matriz de relaciones paralelas

Donde A ha sido multiplicado a la derecha por el vector de ponderaciones w. El resultado de esta multiplicación es nw. Por lo tanto, para recobrar la escala de la matriz de relaciones, se debe resolver el problema Aw=nw o (A-nI)w=0. Este es un sistema homogéneo de ecuaciones. Tiene una solución no trivial si y sólo si el determinante de A-nI es nulo, o sea, n es un valor propio de A. Ahora A tiene rango unitario ya que cada fila es un múltiplo constante de la primera fila. Por lo tanto, todos sus valores propios excepto uno son cero. La suma de los valores propios de una matriz es igual a su traza, la suma de sus elementos diagonales y en este caso la traza de A es igual a n. Por lo tanto, n es un valor propio de A y uno tiene una solución no trivial. La solución consiste en entradas positivas y es única dentro de una constante multiplicativa.

Para hacer w único, uno puede normalizar sus entradas dividiendo por su suma.

Por lo tanto, dada la matriz de comparación, uno puede recobrar la escala. En este caso, la solución es cualquier columna de A normalizada. Note que en la A la propiedad recíproca aji=1/aij se aplica, por lo tanto, también aii=1. Otra propiedad de A es que es consistente: sus entradas satisfacen la condición ajk=aik/aij. Por lo tanto, toda la matriz puede ser construida de un conjunto de n elementos que forman una cadena a través de las filas y las columnas.

En el caso general, el valor preciso de wi/wj no se puede dar, sino sólo una estimación de él como juicio. Por el momento, se considera una estimación de estos valores por un experto que se supone perturba muy poco a los coeficientes. Esto significa perturbaciones pequeñas a los vectores propios. El problema ahora se convierte A´w´= λmaxw´ donde λax es el mayor valor propio de A´. Para simplificar la notación, se seguirá escribiendo Aw= λmaxw´, donde A es la matriz de pares ordenados. El problema es ahora qué tan buena es la estimación de w. Si w se obtiene resolviendo el problema, la matriz cuyas entradas son wi/wj es una matriz consistente. Es

una estimación consistente de la matriz A. A en sí misma no necesita ser consistente. De hecho, las entradas de A ni siquiera precisan ser transitivas; o sea, A1, puede preferirse a A2 y A2 a A3, pero A3 puede preferirse a A1. A es consistente si y sólo si λmax=n. Cambios pequeños en aij implican un cambio pequeño en λmax, la desviación de la última de n es una desviación de consistencia y puede ser representada por (λmax-n)/(n-1), lo que se denomina el índice de consistencia (C.I.).

Cuando la consistencia ha sido calculada, el resultado se compara con aquellos del mismo índice de una matriz recíproca aleatoria de una escala desde 1 hasta 9, con recíprocos forzados. Este índice se llama índice aleatorio (R.I).

En la tabla 1.4 se da el orden de la matriz (primera fila) y el valor promedio del R.I (segunda fila), denominada Relación de consistencias.

Tabla 1.4.- Relación de Consistencia

n	1	2	3	4	5	6	7	8	9	10
Índice Aleatorio De Consistencia :	0	0	0.52	0.89	1.11	1.25	1.35	1.40	1.45	1.49

La relación de C.I con el promedio R.I para la misma matriz de orden se llama relación de consistencia (C.R). Una relación de consistencia de 0.10 o menos es evidencia positiva para un juicio informado.

Las relaciones aji=1/aij y aii=1 se conservan en estas matrices para mejorar la consistencia. La razón de ello es que si la piedra No. 1 se estima que es k veces más pesada que la piedra No. 2, uno debería exigir que la piedra No. 2 se estime 1/k veces el peso de la primera. Si la relación de consistencia es muy pequeña, las estimaciones se aceptan; de lo contrario se intenta mejorar la consistencia mediante la obtención de información adicional. Lo que contribuye a la consistencia de un juicio es: La homogeneidad de los elementos de un grupo, o sea, no comparar un grano de arena con una montaña; la escasez de elementos en un grupo, porque un individuo no puede mantener en su mente simultáneamente las relaciones de muchos objetos y el conocimiento y cuidado del decisor sobre el problema en estudio.

1.3.5 Preparación y Organización para aplicar un AHP

Es importante llevar a cabo una seria y cuidadosa planeación por parte del grupo de trabajo encargado de la aplicación del mismo.

Aunque el problema a abordar sea diferente en cada caso particular, los aspectos que se presentan a continuación, deben tenerse en cuenta de manera general, por aquellos interesados en utilizar el AHP.

Definición de los Participantes

El equipo de trabajo es el responsable de identificar cuidadosamente los actores que deben participar en el proceso de toma de decisión. Deben quedar resueltas preguntas como: quiénes, cuántos, nivel de educación requerido, a quién representan, por qué deben formar parte del proceso, ya sea por su conocimiento de la situación problema o, porque representan a un grupo de interés, entre otros. Para este proyecto estará conformado por las personas directamente involucradas en coordinar la aplicación del AHP

Un actor será entendido como una persona natural o una persona que representa a una instancia, institución u organización, quienes están interesados o son afectados (directa o indirectamente) , por una actividad o aspecto de una situación en cuestión y por ende, tienen derecho a participar en decisiones relacionadas con la misma.

Teniendo en cuenta lo anterior, entre los participantes pueden estar: autoridades, técnicos, beneficiados o afectados, líderes de opinión, organizaciones, entre otros.

En algunos casos, la aplicación del AHP se puede llevar a cabo en diferentes etapas del proceso de toma de decisión. Cada resultado actuará como retroalimentación para la siguiente etapa. Esto puede implicar que los actores (directos, indirectos) puedan ir variando o incorporándose grupos nuevos a medida que así lo requieran las diferentes fases del proceso.

La institución coordinadora debe hacer posible que los actores identificados como relevantes en el proceso estén adecuadamente representados y actúen en igualdad de condiciones para expresar sus opiniones.

Entre más amplia sea la participación se requerirán mayores esfuerzos por parte del grupo coordinador, quien deberá identificar y utilizar las técnicas adecuadas para facilitar la aplicación del AHP, dependiendo de los grupos sociales con los que esté trabajando, los cuales seguramente presentarán distintos niveles de información y diferentes intereses. Por eso, es necesario estar de acuerdo sobre unos principios básicos claros. Estos principios ayudan a ordenar, comparar y compartir información.

Información requerida

Este es un elemento básico para la toma de decisión. Es necesario identificar la cantidad y calidad de información requerida para el proceso. Esta información puede ser de índole científica, técnica y la dada por la experiencia y conocimiento de los participantes. Puede darse el caso que en el proceso de aplicación del AHP surja la representación de los intereses de instancias, instituciones u organizaciones. Esta es tan importante como

la participación de personas con experiencia, conocimiento del problema en cuestión y por su reconocimiento social.

Muchas veces se presenta la necesidad, por parte de los participantes, de disponer de información nueva o complementaria de la que se dispone en la sesión. En ese caso se debe analizar la pertinencia de la misma, el tiempo, el proceso requerido para disponer de esa información adicional y poder continuar el proceso de toma de decisión.

Tiempo y otros recursos asociados con el proceso.

Es necesario establecer el tiempo con el cual se dispone para llevar a cabo el proceso de decisión. Esto afectará la elaboración y desarrollo del Plan de Trabajo: fechas, agenda, logística, materiales a utilizarse, número de participantes convocados, etc.

No se recomienda aplicar el AHP si se cuenta con escaso tiempo para tomar decisiones frente a problemas complejos, puesto que tratar de acelerar algunas etapas del mismo- por obtener resultados inmediatos, puede afectar negativamente la validez de los resultados.

Adicionalmente se requiere nombrar al facilitador para la aplicación del AHP. Éste debe tener la habilidad de guiar el proceso, animar y orientar a los participantes y hacer un buen uso del tiempo disponible, sin llegar a dominar o manipular la sesión.

El facilitador debe buscar que los participantes tengan una comprensión del método y su filosofía y así mismo lograr homogeneidad en el lenguaje para la definición del objetivo y la construcción y evaluación del modelo. Por ejemplo en lo concerniente a los términos a utilizar para que todos los participantes entiendan lo mismo y diferencien los conceptos: objetivo, criterio, sub-criterio y en el significado de los valores de la escala a utilizar para evaluar el modelo. Seguramente el facilitador deberá enfrentarse a “situaciones sorpresa”, como confrontación entre algunos miembros, falta de voluntad de algunos participantes para expresar su opinión o sus verdaderas preferencias, entre otros.

El grupo coordinador encargado de aplicar el AHP debe analizar y seleccionar previamente cuáles son las técnicas más adecuadas a desarrollar con los participantes para facilitar y fortalecer el desarrollo de la sesión. En algunos casos se pueden utilizar técnicas más familiares para el auditorio para la construcción del Modelo Jerárquico, por ejemplo en la pared con cartulinas, en el pizarrón y no directamente con la utilización del programa. En otros casos se podrá construir el modelo simultáneamente, en el computador y en la pared o en el pizarrón.

Cuando se aplique el AHP mediante la formación de grupos se debe ser cuidadoso en la organización de los mismos. Si hay dentro de un subgrupo muchos participantes con posiciones contrarias, pueden generarse conflictos durante toda la sesión. Debe tenerse en cuenta el tiempo

requerido y disponible para aplicar eficientemente el AHP. En algunos casos, los participantes pueden mostrarse cansados al final del día y no dar mayor atención a la evaluación del modelo, lo cual puede afectar la validez de los resultados.

1.3.6 Estructuración del modelo jerárquico.

Una de las partes más relevantes del AHP, consiste en la estructuración de la jerarquía del problema, etapa en la cual el grupo decisor involucrado debe lograr desglosar el problema en sus componentes relevantes (ver figura 1.25).

La jerarquía básica está conformado por: meta u objetivo general, criterios y alternativas.

Los pasos a seguir para la estructuración del modelo jerárquico son:

a. Identificación del Problema;
b. Definición del Objetivo;
c. Identificación de Criterios; e
d. Identificación de Alternativas.

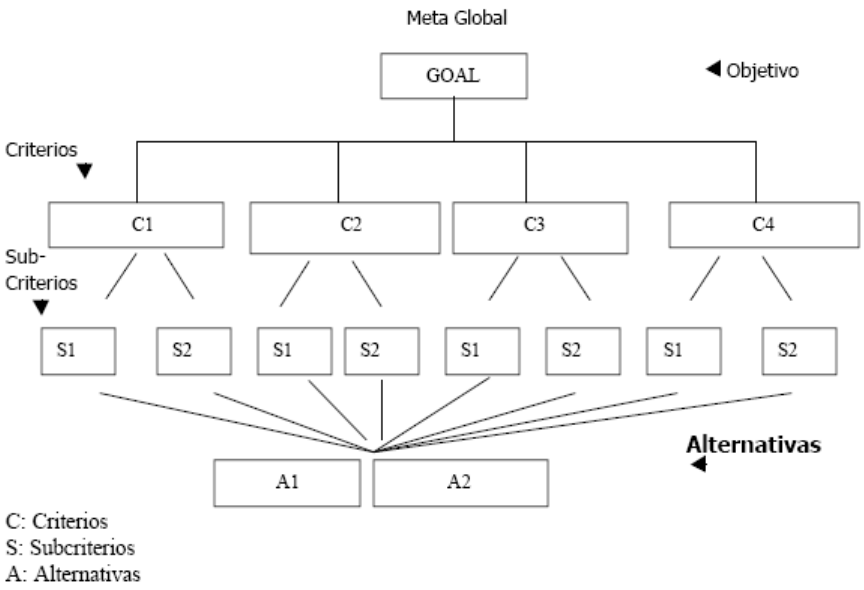


Figura 1.25.- Modelo Jerárquico