ESTADO DEL ARTE, DISEÑO Y PROGRAMACIÓN DE UNA APLICACIÓN QUE UTILICE TECNOLOGÍAS DE AUTENTICACIÓN

CARLOS MAURICIO GALVIS TRASLAVIÑA

UNIVERSIDAD SAN BUENAVENTURA
FACULTAD DE INGENIERÍA
INGENIERÍA DE SISTEMAS
BOGOTA D.C.
2007

ESTADO DEL ARTE, DISEÑO Y PROGRAMACIÓN DE UNA APLICACIÓN QUE UTILICE TECNOLOGÍAS DE AUTENTICACIÓN

CARLOS MAURICIO GALVIS TRASLAVIÑA

Proyecto de Grado para optar al título de Ingeniero de Sistemas

Asesor:
Ingeniero Emilio Barajas

UNIVERSIDAD SAN BUENAVENTURA
FACULTAD DE INGENIERÍA
INGENIERÍA DE SISTEMAS
BOGOTA D.C.
2007

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá D.C., __ de Noviembre de 2007

AGRADECIMIENTOS

Agradezco a todas las personas e instituciones que me apoyaron incondicionalmente en el desarrollo de este proyecto, así como aquellos que imponen barreras a la investigación al darme más argumentos para llevar a feliz término esta empresa.

CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

LISTA DE ANEXOS

INTRODUCCIÓN

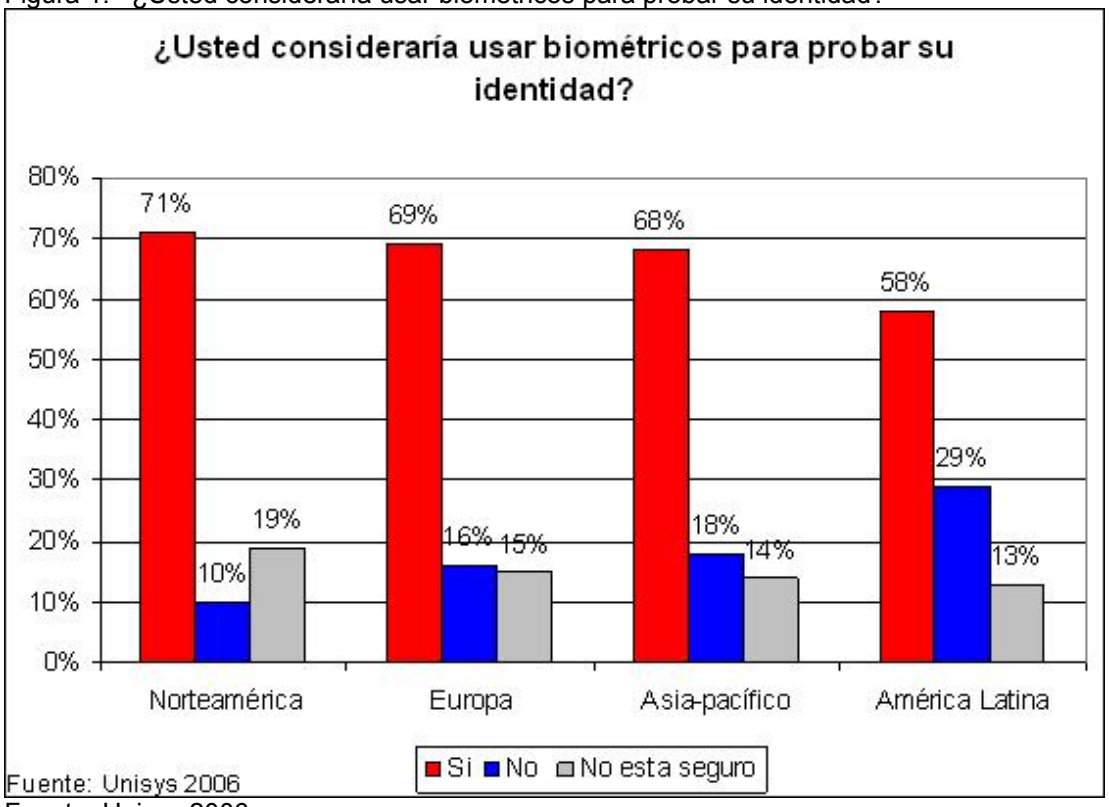
Desde que el hombre dejó de ser nómada y se estableció en un lugar, este se preocupó por brindar seguridad para él y su comunidad. En principio, la defensa era contra las fieras, con el paso del tiempo y el progreso de la humanidad se vio en la necesidad de defenderse de otros seres humanos, es por ello que se inventaron las fortalezas y los sistemas de control de acceso que aún hoy en día se utilizan y que se pueden dividir en tres grandes grupos, lo que se sabe (contraseñas), lo que se tiene (llaves, carné, entre otras.) y lo que se es (rasgos físicos).

A finales del siglo XX con la Guerra Fría y desde el 2001 con la Guerra anti-terrorista, el hombre se ha visto en la necesidad de mejorar los sistemas de control de acceso y aplicarlos en todas sus actividades, es así como actualmente todos requieren de un usuario y una contraseña para ingresar incluso en el computador doméstico y en el ámbito comercial se usan distintos dispositivos para validarse, como por ejemplo las tarjetas bancarias (crédito, débito) en los cajeros, el carné de la empresa para ingresar a ella, los documentos de identidad (cédula de ciudadanía, pasaporte) para desplazarse de un país o una región a otra.

Con todo esto se han desarrollado diversos dispositivos tales como Tarjetas con banda magnética, Tarjetas con códigos de barras, Tarjetas con microprocesadores y más recientemente se viene utilizando los rasgos físicos de las personas para validarse ante un dispositivo electrónico (tecnología biométrica).

Para el control de acceso a instalaciones se viene promoviendo el uso de tecnología biométrica, la cual es conocida y aceptada por la gran mayoría de las personas (ver Figura 1 página 2) aunque aún falta superar ciertos interrogantes en el ámbito usuario y vendedor como son: ¿Qué tipo de registro biométrico utilizar?, ¿Cuánto invertir en el cambio de tecnología?, ¿Qué nivel de fiabilidad debe tener el sistema? Así mismo en el ámbito tecnológico hay preguntas tales como: ¿Qué tipo de registro biométrico utilizar plantillas, imágenes o ambos?, ¿Dónde almacenar los datos en dispositivos de almacenamiento personal (tarjetas inteligentes, ópticas, entre otras.) o en bases de datos?, ¿El sistema debe usarse para identificación o para comprobación?

Figura 1. ¿Usted consideraría usar biométricos para probar su identidad?



Fuente: Unisys 2006

Con los registros biométricos aun no se han podido superar algunos inconvenientes en cuanto a la comparación y es así como no todos los rasgos pueden usarse para identificación cerrada.

1 PLANTEAMIENTO DEL PROBLEMA

1.1 ANTECEDENTES

En 1949 se inicia el uso del código de barras de manera comercial siendo actualmente uno de los sistemas con mayor difusión en el mundo y sobre el cual se han realizado múltiples modificaciones y su reglamentación se encuentra plenamente desarrollada, este tipo de tecnología se usa principalmente en el ámbito comercial para el control de inventarios y pago de mercancías así como en el manejo de cuentas (pago de servicios públicos).

En 1974 surge la banda magnética, este también se encuentra completamente regulado y su uso es masivo principalmente en el sector financiero (tarjetas crédito y debito). Hay otros sectores que lo utilizan como son los sistemas de pago de transporte masivo y control de acceso.

Aunque desde 1974 está disponible comercialmente tecnología biométrica (sistema de geometría de mano) su uso y reglamentación podría decirse que se inició en la década de los 90 (En 1997 se publica el primer estándar comercial de interoperatibilidad de biometría genérico) y después del 11 de septiembre de 2001 se ha convertido en el sistema a implementar, es así como la Unión Europea y Estados Unidos han creado comités especiales para implementar de la manera más expedita este sistema para la identificación de sus ciudadanos y los turistas que los visitan. EEUU empezó en el 2005 (con casi dos años de retraso) a utilizar este sistema para la identificación de los turistas e inmigrantes que llegan a su territorio.

Las perspectivas en el área de control de acceso, indican tendencias claras en el ámbito financiero, se piensa en dos posibles desarrollos: uno es el reemplazo de la banda magnética por la tarjeta con microprocesador y la otra es el uso de la biometría, en cualquiera de los casos la expectativa es que para el 2012 se haya migrado completamente a cualquiera de estas tecnologías, la decisión básicamente depende del costo de implementar cualquiera de ellas y su fiabilidad y universalidad, porque piensan usar la tecnología seleccionada incluso para acceder a sus servicios a través de Internet.

En el ámbito comercial (control inventarios) se está promoviendo la idea de migrar del código de barras a la tecnología RFID a través del uso del código ePC.

En el anexo A (página 104) se consigna un resumen a modo de línea de tiempo de la historia de las tecnologías de autenticación.

En Colombia las tecnologías tradicionales (código de barras, banda magnética, tecnología biométrica) han tenido el mismo desarrollo que en el resto del mundo, aunque hay tecnología que no tiene tan amplia difusión como son las tarjetas con microprocesador (sólo se usan en telefonía móvil y sistemas de transporte masivo).

En la Universidad de San Buenaventura, más específicamente en la facultad de ingeniería se han desarrollado los proyectos de grado : “Adopción de la tecnología de código de barras en el carnet de los empleados de la USB para el registro y control de jornandas Laborales”, “Diseño de un software para el registro de personal activo de la USB sede Bogotá”, “Software de registro para estudiantes y visitantes”, “Sistema de pago electrónico a través de Internet usando tarjetas inteligentes” y “Prototipo de un sistema de control acceso de personal mediante el uso de tarjetas inteligentes de tecnología RFID” de acuerdo a entrevistas realizadas a funcionarios de la Universidad, ninguno de estos proyectos se implantaron.

En la facultad de Administración de empresas se desarrollo un proyecto de grado titulado “Implementación de la tarjeta inteligente universitaria –TIU-“, que estudiaba la viabilidad de implementar un sistema de identificación de este tipo adicionando otros usos como el de las transacciones bancarias, debido a que la implementación se sugería fuera en asocio con una entidad bancaria, sin embargo al igual que los proyectos de la facultad de ingeniería este proyecto no se implantó.

Actualmente la universidad tiene implementado en el carne de empleados y estudiantes el código de barras 128, el cual no se está usando con ningun fin específico, y hace parte de un software aislado (no esta conectado con los otros sistemas y/o aplicaciones de la Universidad). De igual manera se utiliza la banda magnética de baja coercitividad (marrón) para el control de acceso a la rectoria, algunos auditorios y laboratorios, esta solución tecnologíca se maneja a través de un contratista.

Debido a la falta de información es difícil ver claramente la tendencia del mercado en Colombia, sin embargo instituciones financieras (Bancafé) ya han incursionado en el uso de tecnología biométrica, y en el ámbito gubernamental se espera que en el 2010 todos los colombianos tengan su documento de identidad con su respectivo registro biométrico de la huella dactilar.

Desde el punto de vista normativo se observa que el Instituto Colombiano de Normas Técnicas sólo ha producido normas en lo referente al uso del código de barras, la banda magnética y la tarjeta con microprocesador de contactos, es decir que la tecnología restante no cuenta con normas técnicas colombianas que las regulen.

Así mismo desde el punto de vista legal se observa que existen tres entes gubernamentales que regulan el uso de algunas de las tecnologías en Colombia como son: la Superintendencia de Industria y Comercio con el código de barras y solamente en lo concerniente a la fijación pública de precios, La Superintendencia Financiera con el código de barras y la banda magnética en las entidades financieras; La Superintendencia de Vigilancia y Seguridad Privada regula una modalidad de vigilancia denominada tecnológicos y lo único que tiene establecido es que las empresas de vigilancia que utilicen estos medios debe entregar copia del manual del dispositivo tecnológico a usar y del certificado de capacitación de las personas que lo usarán. Y otras normas establecen que los registros que estos sistemas generen pueden ser usados dentro de un proceso penal siempre y cuando no implique vulneración de la Constitución, ni de los tratados internacionales de derechos humanos suscritos por Colombia (se explicará de manera más clara y extensa en el marco legal y normativo).

Por todo lo anterior y teniendo en cuenta que en el ámbito mundial sólo existen dos estudios del estado del arte de las tecnologías de autenticación desarrollados por el Departamento de Defensa de Estados Unidos y Un instituto alemán para la Union Europea, donde se centran en las tecnologías biométricas y donde no se menciona cual es la situación de estas tecnologías en América; que ante Colciencias no existen grupos de investigación en esta área, es importante dar a conocer ante la comunidad académica el estado del arte de estas tecnologías y su aplicación en la vida cotidiana, para fomentar la creación de grupos de investigación, la normalización y legislación de estas tecnologías.

1.2 DESCRIPCIÓN Y FORMULACIÓN DEL PROBLEMA

En Colombia se están utilizando todas las tecnologías de autenticación existentes en el ámbito mundial, sin embargo es muy escasa o no existe bibliografía que presente cómo se realiza el diseño y programación de una aplicación que utilice tecnologías de autenticación, tampoco se conoce el estado del arte de las tecnologías de autenticación en Colombia y en el mundo.

¿Cuál es la tendencia y las limitaciones en las tecnologías de autenticación utilizadas en las aplicaciones desarrolladas para la industria nacional, y cómo diseñar y programar una aplicación que utilice tecnologías de autenticación?

1.3 JUSTIFICACIÓN

El interés creciente por parte de los gobiernos, la empresa privada y organismos supranacionales para implementar aplicaciones que garanticen la identidad de los usuarios que acceden a sus instalaciones y en especial a sus redes y la información que ellos manejan hacen que la academia y la industria inviertan en el desarrollo y estandarización de las tecnologías de autenticación que se usan actualmente, por lo que se requiere establecer cuál es la tendencia a corto, mediano y largo plazo en el uso de estas tecnologías, cuál es la normatividad y legislación vigente en Colombia.

1.4 OBJETIVOS

1.4.1 Objetivo General

Diseñar y programar una aplicación que utilice al menos una de las tecnologías de autenticación, basado en el estado del arte.

1.4.2 Objetivos Específicos

- Analizar el estado del arte de las tecnologías de autenticación en Colombia y en el mundo, así como determinar cuál es su tendencia.
- Analizar los requerimientos funcionales y no funcionales de la aplicación a desarrollar.

- Definir la tecnología de autenticación a utilizar en la aplicación.
- Caracterizar el modelo de red a implementar para el uso de aplicaciones que utilicen tecnologías de autenticación.
- Determinar las estratégias de prueba de la aplicación.

1.5 ALCANCES Y LIMITACIONES

1.5.1 Alcances

Se presentará el estado del arte y las tendencias en el ámbito nacional e internacional en el uso de las tecnologías de autenticación que sirvan como fuente de información y referente para futuras investigaciones en esta área del conocimiento.

Se desarrollará una aplicación para un hotel que implemente uno de los dispositivos de autentificación estudiados.

1.5.2 Limitaciones

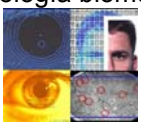
- Se presentará la información a partir de los desarrollos tecnológicos y la normativa y no desde la industria, teniendo en cuenta lo sensible de la información a tratar.

2 MARCO DE REFERENCIA

2.1 MARCO TEÓRICO - CONCEPTUAL

Las tecnologías de autenticación hacen referencia a herramientas desarrolladas por el hombre para particularizar a un individuo u objeto a partir de elementos considerados únicos, es así como se dividen en cuatro grandes grupos de acuerdo al elemento utilizado como son: el código de barras, la banda magnética, las tarjetas con circuito integrado y los biométricos (ver Tabla 1).

Tabla 1. Composición de tecnologías

Tecnología	Ventajas	Desventajas
Tarjeta de Proximidad 	No puede ser duplicada. La Tarjeta no tiene rozamiento. Bajo costo de mantenimiento.	Su costo es relativamente alto.
Código de Barras 	Es de las más conocidas y difundidas para el control en la cadena de producción No tiene rozamiento	No se puede rayar. Su vida útil es media. Puede ser clonada si no lleva código oculto.
Banda Magnética 	Es la más conocida y difundida, tiene un bajo costo, ampliamente usada en la banca y en el transporte masivo.	Es el medio de identificación más vulnerable de todos
Touch Memories / Llave electrónica 	Muy alto nivel de seguridad. Altamente resistentes al desgaste. Muy Confiable	Sensibles a la electricidad. Muy alto costo.
Tarjeta inteligente 	Durabilidad. Compatibilidad con múltiples dispositivos. Contiene circuito integrado que almacena mucha información	Transacciones más lentas. Costo alto. Sensible a la humedad.
Tecnología biométrica 	Muy alto nivel de seguridad. Muy confiable. Puede ser usada para múltiples funciones simultáneamente.	Alto costo de implementación Algunas tecnologías sólo soportan comparación 1 a 1 y tienen un alto nivel de error.

El código de barras es una tecnología desarrollada con el fin de facilitar la identificación de objetos (principalmente) o personas a partir de un código numérico o alfanumérico que se representa a través de unos símbolos, que dependiendo el tipo pueden ser barras o puntos, su nombre lo adquirió porque los primeros sistemas utilizaban barras para codificar esa información, actualmente existen otros códigos de barras que utilizan puntos distribuidos en un espacio específico y que representan esos códigos.

Las tarjetas con Circuito integrado son una tecnología desarrollada a partir de componentes electrónicos implantados en una tarjeta plástica y que dependiendo de la función que cumplan se pueden dividir en dos grandes grupos las tarjetas con memoria y las tarjetas con circuito integrado, estas a su vez se dividen en tarjetas de contacto y sin contacto, las tarjetas de contacto son aquellas que requieren entrar en contacto físico con el lector, para recibir o transmitir la información, mientras las que son sin contacto, a través de una radiofrecuencia transmiten la información de la tarjeta al lector y viceversa.

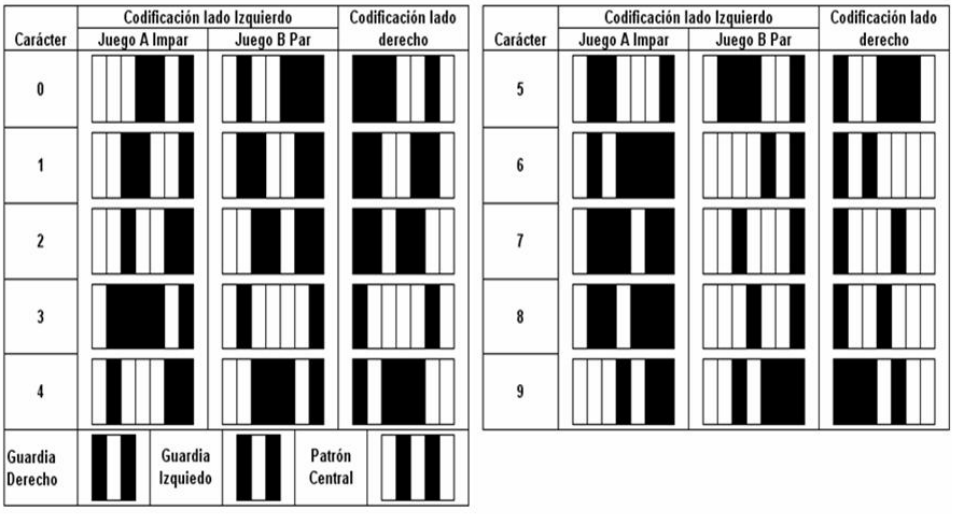
Las tarjetas con Banda Magnética son una tecnología usada principalmente en las entidades bancarias y en los sistemas de control de acceso y en otros países para el manejo de los tiquetes de transporte masivo, aéreos, entre otros. La banda magnética, como su nombre lo indica es una banda constituida con metales que al aplicárseles la fuerza de un campo magnético, cambian de posición, almacenando la información deseada.

La tecnología biométrica hace referencia al uso de métodos automatizados de autenticación de una persona, basados en sus características fisiológicas o conductuales, es así como dentro de las fisiológicas o morfológicas tenemos la huella dactilar, el iris, la retina, la geometría de la mano, y muchas otras, mientras que en las conductuales tenemos la voz, la firma, dentro de las más conocidas.

2.1.1 Códigos de barras Las distintas simbologías que existen actualmente se dividen en dos grandes grupos los de una dimensión (1D) o lineal y los de dos dimensiones (2D); los de una dimensión son los más ampliamente usados (principalmente en el área comercial para la identificación de los productos), mientras que los de dos dimensiones son utilizados en áreas que requieren alto grado de seguridad y almacenar una gran cantidad de información, entre ellos las aplicaciones más conocidas es en documentos de identificación y licencias de conducción (Ver anexo B).

Código EAN. Este código al igual que el código UPC(Unified Product Code) también tiene dos códigos básicos el EAN-8 y el EAN-13, su utilización depende del área disponible para impresión del código y el juego de caracteres es el mismo que para el código UPC (ver Tabla 2 página 10).

Tabla 2. Juego completo de caracteres para el código UPC y EAN.



Estel código fue diseñado para que incluso un sistema simple pueda leer el código por mitades. El escáner puede leer cualquier mitad primero, también una mitad puede ser leída de izquierda a derecha o de derecha a izquierda, es necesario para la lógica determinar que dato es de la mitad izquierda o de la derecha. Las dos mitades son imagen espejo la una de la otra, Hay dos barras de guardia, seguidas por seis caracteres y la barra central. El carácter (desde las barras de guardia) empiezan con un espacio y cada carácter está compuesto por dos espacios y dos barras, hay dos juegos de diez caracteres. Un juego es llamado paridad par y el otro es llamado paridad impar (ver Tabla 3 página 11).

El patrón central (01010) que es compartido por el lado derecho y lado izquierdo del símbolo, sirve para determinar la lógica de la dirección del rayo que cruza el símbolo, porque los escáneres no necesitan leer ambas mitades del símbolo en la misma pasada ni en la misma dirección). La longitud del patrón central sólo es de 4 módulos (más estrecha que los otros).

Tabla 3. Paridad de caracteres del lado izquierdo

PRIMER DÍGITO DEL CÓDIGO	PARIDAD PARA CODIFICAR CON					
	SEGUNDO DÍGITO DEL CÓDIGO	CARACTERES DEL CÓDIGO DEL FABRICANTE				
		1	2	3	4	5
0 (UPC-A)	Impar	Impar	Impar	Impar	Impar	Impar
1	Impar	Impar	Par	Impar	Par	Par
2	Impar	Impar	Par	Par	Impar	Par
3	Impar	Impar	Par	Par	Par	Impar
4	Impar	Par	Impar	Impar	Par	Par
5	Impar	Par	Par	Impar	Impar	Par
6	Impar	Par	Par	Par	Impar	Impar
7	Impar	Par	Impar	Par	Impar	Par
8	Impar	Par	Impar	Par	Par	Impar
9	Impar	Par	Par	Impar	Par	Impar

Código EAN-13. El código está compuesto por 13 dígitos y es ampliamente utilizado en todo el mundo (ver Tabla 4 página 11).

Tabla 4. Composición del Código EAN-13

CÓDIGO PAÍS	CÓDIGO EMPRESA	CÓDIGO PRODUCTO	DÍGITO DE CONTROL
770	1234	56789	7

Cálculo Dígito de Control (Factor de peso 31)
Los números pares se multiplican por 3 y los impares por 1, luego se suman los resultados de las multiplicaciones y se le restan al valor de la decena superior.

Ejemplo:

7	7	0	1	2	3	4	5	6	7	8	9
*	*	*	*	*	*	*	*	*	*	*	*
1	3	1	3	1	3	1	3	1	3	1	3
=	=	=	=	=	=	=	=	=	=	=	=
7	21	0	3	2	9	4	15	6	21	8	27

7+21+0+3+2+9+4+15+6+21+8+27=113
120-113=7

Para la codificación del código EAN-13 se utilizan treinta barras que representan los 13 dígitos, el guardia inicial, el guardia final y el patrón central.

Para la impresión del código hay unas dimensiones que se deben tener en cuenta (ver Tabla 5, Figura 2 página 12);

Tabla 5. Dimensiones del Código EAN-13

Factor de aumento	Modulo-X Ancho barra más estrecha	Ancho símbolo de 1ª a ultima barra	Margen claro		Símbolo	
			Izquierdo (11x Módulo-X)	derecho (7x Módulo-X)	Ancho	Altura
fm	mm	mm	mm	mm	mm	mm
.80	.264	25.08	2.90	1.85	29.83	20.73
.85	.281	26.64	3.09	1.97	31.70	22.02
.90	.297	28.21	3.27	2.08	33.56	23.32
.95	.314	29.78	3.44	2.19	35.43	24.61
1.00	.330	31.35	3.63	2.31	37.29	25.91
1.10	.363	32.92	3.81	2.42	41.02	27.21
1.20	.396	34.49	3.99	2.54	44.75	28.50
1.30	.429	36.06	4.17	2.65	48.48	29.80
1.40	.462	37.62	4.36	2.77	52.21	31.09
1.50	.495	39.19	4.53	2.88	55.94	32.39
1.60	.528	40.76	4.72	3.00	59.66	33.68
1.70	.561	42.33	4.90	3.12	63.39	34.98
1.80	.594	43.89	5.08	3.23	67.12	36.27
1.90	.627	45.47	5.26	3.35	70.85	37.57
2.00	.660	47.03	5.45	3.47	74.58	38.87

Figura 2. Tamaño Máximo y Mínimo del Código EAN-13

Para la impresión de los códigos de barras se debe tener presente que la combinación de colores sea la adecuada, por ello se ha establecido cuales son las posibilidades, las cuales se presentan a continuación (ver Tabla 6, Tabla 7).

Tabla 6. Espectrofotometría ACS.

ESPECTROFOTOMETRÍA ACS

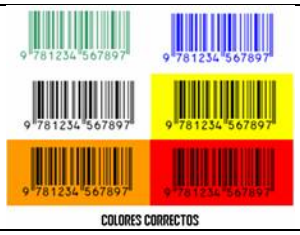
		Luminosidad	Eje Rojo-Verde	Eje Amarillo-Azul	Saturación	Tonalidad
Fondos Rojos	1	52.47	53.46	39.53	66.49	36.48
	2	60.67	56.29	52.64	77.07	43.08
	3	52.70	42.98	40.46	59.03	43.27

		Luminosidad	Eje Rojo-Verde	Eje Amarillo-Azul	Saturación	Tonalidad
Fondos Violeta	1	52.69	31.85	-31.65	44.90	315.18
	2	53.92	26.81	-27.49	38.40	314.28
	3	51.06	25 11	-35.89	43.80	304.98
Fondos Azul	1	60.99	-16.26	-38.97	42.23	347.36
	2	55.10	-27.21	-49.09	56.12	241.00
	3	55.76	-11.34	-47.82	49.15	256.66
Fondos Verde	1	57.59	-53.58	30.07	61.44	150.70
	2	53.96	-48.45	19.28	52.14	158.30
	3	55.38	-41.30	28.16	49.99	145.71
Fondos Amarillos	1	87.69	0.02	97.79	97.79	89.99
	2	91.45	7.95	98.07	98.39	85.37
	3	90.97	-2.15	104.68	104.70	91.18
Fondos Naranja	1	66.65	26.61	62.34	67.78	66.89
	2	72.30	29.45	69.51	75.49	67.04
	3	70.34	19.72	69.63	72.37	74.18
Símbolo Verde	1	57.34	-54.96	23.27	59.73	156.96
	2	53.20	-46.51	12.18	48.08	165.33
	3	53.38	-41.08	17.91	44.81	156.45
Símbolo Azul	1	31.51	26.20	-52.74	58.89	296.42
	2	28.01	8.13	-56.47	57.05	278.19
	3	28.26	22.22	-59.74	63.74	290.40
Símbolo marrón	1	42.07	5.80	20.39	21.20	74.11
	2	43.87	8.81	22.31	23.98	68.46
	3	43.25	4.43	23.04	23.47	79.12

1. Iluminación D65 10º 6500 oK 2. Iluminación A 10º Tungsteno 3. Iluminación CWF 10º Luz Día SE = 5

Fuente: ASOBANCARIA.Estándar del código de barras para las facturas recaudadas pr el sector financiero. Bogotá: ASOBANCARIA 1999 Pag 27

Tabla 7. Ejemplos de colores y contrastes de impresión.

Combinación Correcta de Colores		
 COLORES CORRECTOS	BARRAS	FONDO
	Negro	Blanco
	Azul	Blanco
	Verde	Blanco
	Negro	Amarillo
	Negro	Naranja
	Negro	Rojo
Combinación Incorrecta de Colores		
 COLORES INCORRECTOS	BARRAS	FONDO
	Amarillo	Blanco
	Rojo	Blanco
	Negro	Verde
	Negro	Marrón Oscuro
	Rojo	Oro
	Azul	Verde

2.1.2 Biometría. El término biometría viene del griego “bio” que significa vida y “metría” que significa medida o medición, de acuerdo al diccionario de la real academia de la lengua española biometría es el estudio mensurativo o estadístico de los fenómenos o procesos biológicos, sin embargo más recientemente y para el tema que nos concierne el significado de biometría es el conjunto de métodos automatizados que analizan determinadas características humanas para identificar o autentificar personas (ver Tabla 8 y Tabla 9 páginas 15 y 15 respectivamente).

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

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

- Universalidad: que tan común es encontrar este biométrico en los individuos.
- Singularidad: que tan único o diferenciable es la huella biométrica entre uno y otro individuo.
- Permanencia: que tanto perdura la huella biométrica en el tiempo de manera inalterable.
- Recolectable: qué tan fácil es la adquisición, medición y almacenamiento de la huella biométrica.
- Calidad: que tan preciso, veloz y robusto es el sistema en el manejo de la huella biométrica.
- Aceptabilidad: qué tanta aprobación tiene la tecnología entre el público.
- Fiabilidad: qué tan fácil es engañar al sistema de autenticación.

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

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

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

Tabla 8. Comparativo de las tecnologías biométricas más comunes.

Tecnología	Como Trabaja	Tamaño plantilla (bytes)	Fiabilidad	Facilidad De Uso	Posibles Incidencias	Costo	Aceptación Usuario
Huella digital	Captura y compara patrones de la huella digital	250- 1000	Muy alta	Alta	Ausencia de miembro	Bajo	Alta
Geometría de la mano	Mide y compara dimensiones de la mano	9	Baja	Alta	Edad, Ausencia de miembro	Bajo	Alta
Retina	Captura y compara los patrones de la retina	96	Baja	Baja	Gafas	Alto	Baja
Iris	Captura y compara los patrones del iris	512	Baja	Baja	Luz	Muy alto	Baja
Tecnología	Como Trabaja	Tamaño plantilla (bytes)	Fiabilidad	Facilidad De Uso	Posibles Incidencias	Costo	Aceptación Usuario
Geometría facial	Captura y compara patrones faciales	84 o 1300	Baja	Baja	Edad, Cabello, luz	Medio	Baja
Voz	Captura y compara cadencia, pitch, y tono de la voz	10000-20000	Alta	Media	Ruido, temperatura y meteorología	Alto	Media
Firma	Captura y compara ritmo, aceleración, y presión de la firma	1000 - 3000	Alta	Media	Edad, cambios, analfabetismo	Alto	Media

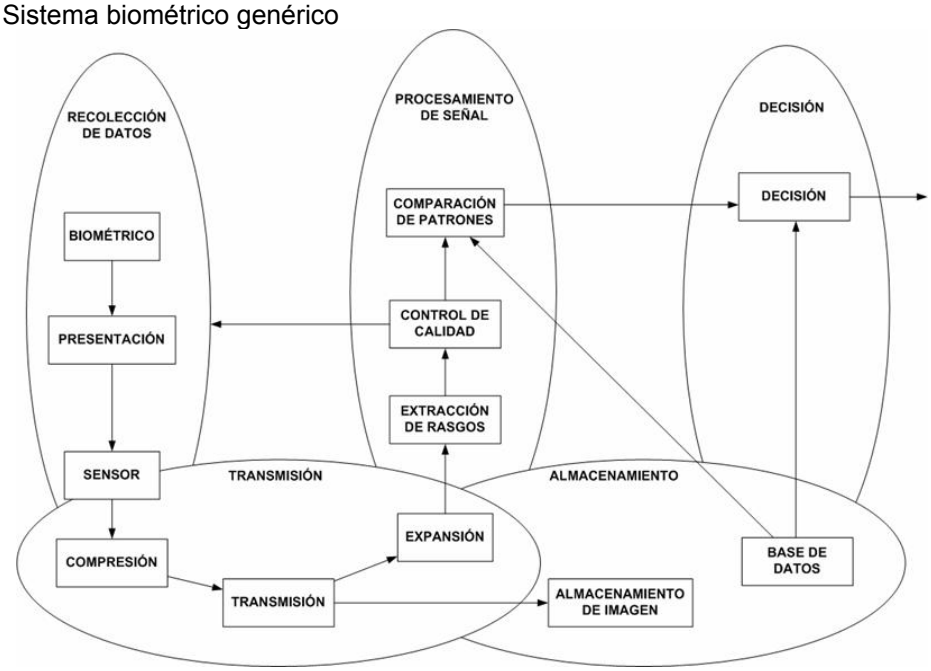
Tabla 9. Tecnología biométrica emergente y su madurez

Tecnología	**Como Trabaja**	**Madurez**
Escaneo de venas	Captura imágenes del patrón del flujo sanguíneo	Comercialmente disponible
Termografía Facial	Cámaras infrarrojas detectan patrones de calor creados por el flujo sanguíneo y emitido por la piel.	Su comercialización inicial falló por el alto costo
Comparación de ADN	Compara muestras de ADN con plantillas generadas como muestra	Muchos años para implementación

Tecnología	Como Trabaja	Madurez
Sensor de olor	Captura los químicos volátiles que los poros de la piel emiten	Muchos años para su comercialización
Medidor del pulso sanguíneo	Sensores infrarrojos medien el pulso de la sangre en el dedo	Experimental
Reconocimiento del patrón de la piel	Extrae distintos patrones ópticos por medidas de espectroscopia de la luz reflejada por la piel	Emergente
Identificación de la cama de la uña	Un interferómetro detecta las fases de cambio en la incidencia de luz en la uña del dedo; reconstruye distintas dimensiones de la cama de la uña y genera un mapa unidimensional	Emergente
Reconocimiento de movimiento	Captura una secuencia de imágenes para derivar y analizar las características de movimiento	Emergente: requiere desarrollo futuro
Reconocimiento de la forma de oreja	Está basada en la distinción de la forma de la oreja y la estructura del cartílago, proyectando parte del oído externo.	Todavía un tópico de investigación

En general un sistema biométrico se puede esquematizar de la siguiente manera (ver Figura 3 página 16):

Figura 3. Sistema biométrico genérico



Fuente: http://www.engr.sjsu.edu visitada 8 de Julio de 2006 02:56

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

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

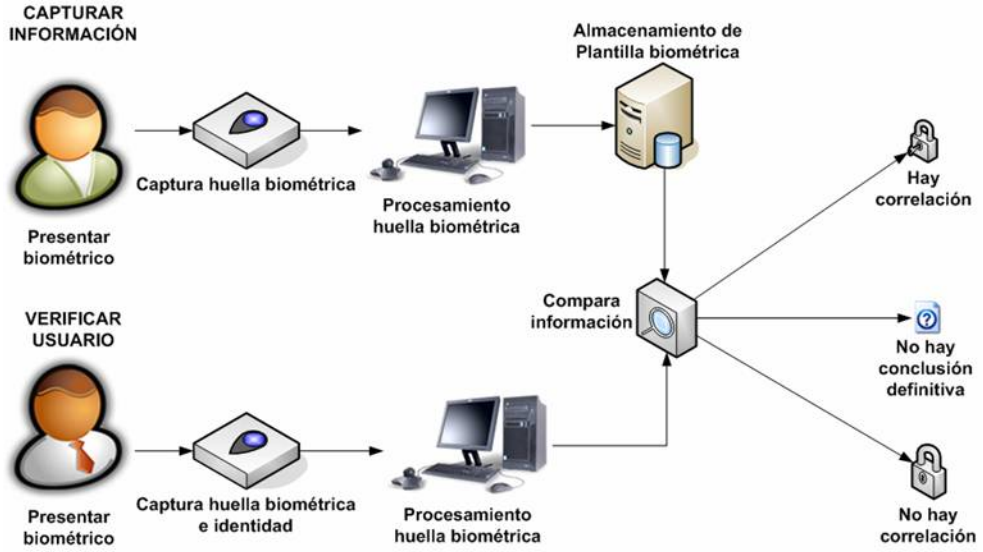
Verificación: Es una tarea de los sistemas biométricos que busca confirmar la identidad de un individuo que la reclama comparando una muestra biométrica con la plantilla biométrica previamente ingresada al sistema.

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

Partiendo de las definiciones anteriores se sabe que hay tres formas para comparar la muestra biométrica, la comparación uno a uno (Verificación), la comparación uno a muchos (Identificación cerrada) y la comparación uno a pocos que es una mezcla de los dos primeros (identificación abierta o watchlist).

Verificación: En el proceso de comparación uno a uno, el usuario presenta su(s) dato(s) biométrico(s) y este se compara con la plantilla biométrica almacenada en una base de datos o en un dispositivo portátil, verificando si hay o no coincidencia para esa identidad en la referencia establecida (ver Figura 4. Proceso de captura y verificación de usuario).

Figura 4. Proceso de captura y verificación de usuario



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

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

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

- Hay correlación: es decir que al comparar el dato biométrico capturado con la(s) plantilla(s) almacenada(s) la puntuación está dentro de los umbrales de coincidencia.
- No hay correlación: es decir que al comparar el dato biométrico capturado con la(s) plantilla(s) almacenada(s) la puntuación está fuera de los umbrales de coincidencia.

- Imposibilidad de alcanzar conclusión definitiva: es decir que hay falta de información para poder hacer una comparación adecuada.

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

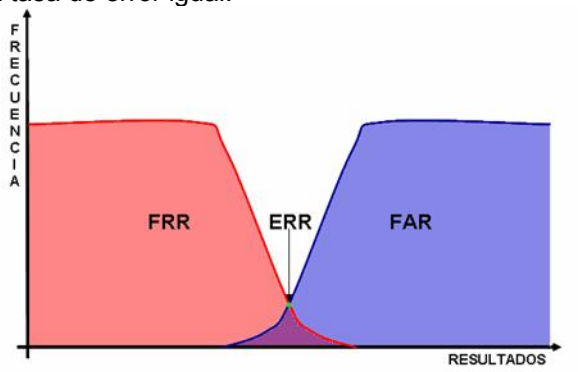
Los términos más comúnmente observados son los siguientes:

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

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

El punto de intersección entre la tasa de falsa aceptación y la tasa de falso rechazo se conoce como la tasa de error igual (EER - Equal Error Rate), algunas veces se llama tasa de error cruzada (CER – Crossover Error Rate).Es una estadística que muestra la actuación del biométrico, típicamente cuando opera en la tarea de verificación. En general entre más bajo sea el valor de la tasa de error igual, más alto es la precisión del sistema biométrico (ver Figura 5. Definición de la tasa de error igual.).

Figura 5. Definición de la tasa de error igual.



Otros términos utilizados son:

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

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

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

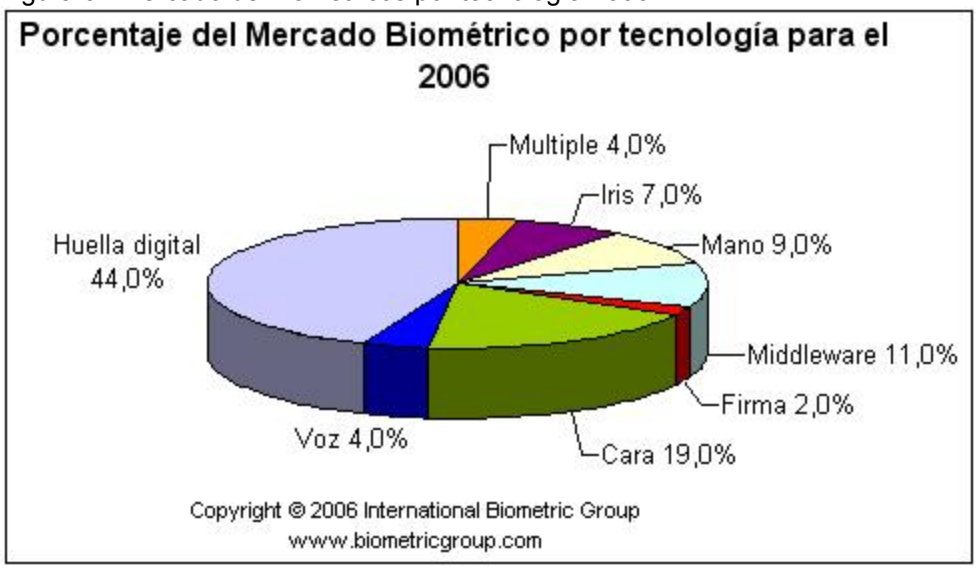
Error tipo I: este tipo de error ocurre en una prueba estadística cuando una reclamación valida es rechazada. Es decir cuando falla al rechazar una reclamación valida. Por ejemplo Claudia reclama ser Claudia, pero el sistema niega el reclamo de manera incorrecta.

Error Tipo 2: este tipo de error ocurre en una prueba estadística cuando una reclamación falsa es aceptada. Es decir cuando falla al aceptar una reclamación

falsa. Por ejemplo Erika reclama ser Sandra y el sistema acepta el reclamo de manera incorrecta.

Modalidades biométricas. Las tecnologías biométricas de mayor uso hoy y con más apoyo por las industrias comerciales son: la huella digital, el reconocimiento facial, la geometría de la mano, el iris, la voz, la firma (ver Figura 6).

Figura 6. Mercado de Biométricos por tecnología 2006



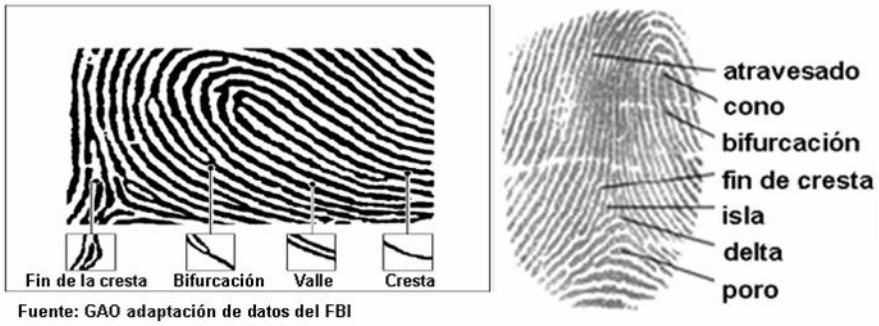
Fuente: www.biometricgroup.com visitada Mayo 20 de 2007 21:35

Reconocimiento de Huella digital. La comparación de la huella digital es una de las técnicas más antiguas y ampliamente utilizadas y aceptas en el ámbito global.

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

La huella digital aparece generalmente constituida por una serie de líneas oscuras que representan las crestas y una serie de espacios blancos que representan los valles. La identificación con huellas digitales está basada principalmente en las minucias (la ubicación y dirección de las terminaciones de crestas, bifurcaciones, deltas, valles y crestas, aunque existen muchas otras características de huellas digitales (verFigura 7. Características de Huellas digitales).

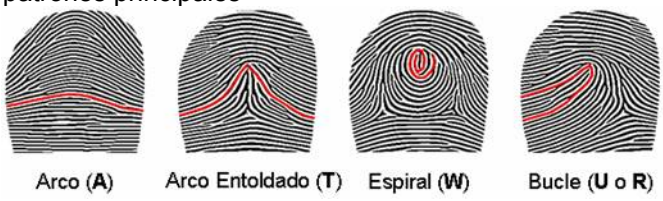
Figura 7. Características de Huellas digitales



Fuente: GAO adaptación de datos del FBI

Otra forma de distinguir las huellas digitales es por sus patrones, los cuales presentó Purkinje en su tesis doctoral (ver Figura 8).

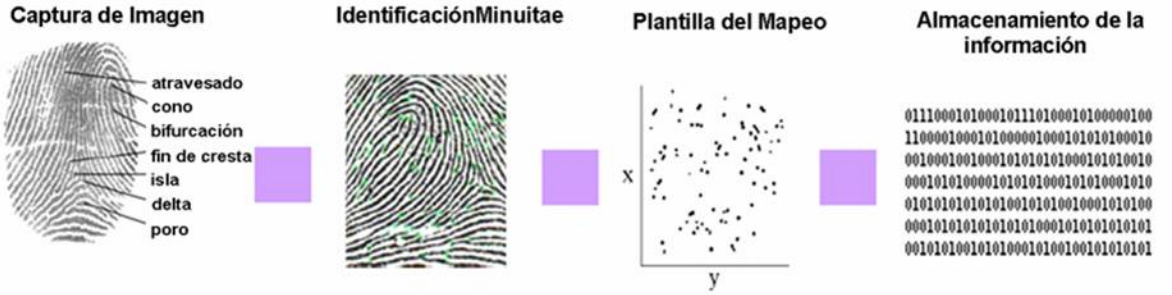
Figura 8. Los cuatro patrones principales



Fuente: KEOGH, Eamonn. The Science of Fingerprints. p-4

De manera general la forma de procesar una huella digital es la siguiente (ver Figura 9, página 22):

Figura 9. Proceso común de escaneo de la huella digital



Fuente: Ian Williams, Biometric Technology for DLID, An Introduction to the Science

Formato para guardar la imagen del dedo. Cada record debe pertenecer a un sólo individuo y debe contener una imagen guardada (consistente en una o más vistas) por cada uno o más dedos. Registros de imágenes sencillas para múltiples dedos (ver Figura 10 a Figura 12 y Tabla 10 a Tabla 16).

La organización del formato de registro es como sigue:

- Una sola longitud-fija (32-byte) general de encabezado de record que contiene la información acerca del registro global, incluyendo el número de imágenes de dedos representados y la longitud del registro global en bytes.
- Un sólo registro digital por cada dedo, vista, imagen multi-dedos consistente en:
- Un encabezado de longitud fija (14-byte) que contiene la información perteneciente a los datos para una imagen sencilla o multi-dedos;
- Datos de la vista de imagen comprimida o descomprimida para sencillo o multi-dedos.

Figura 10. Orden de escaneo de las líneas.

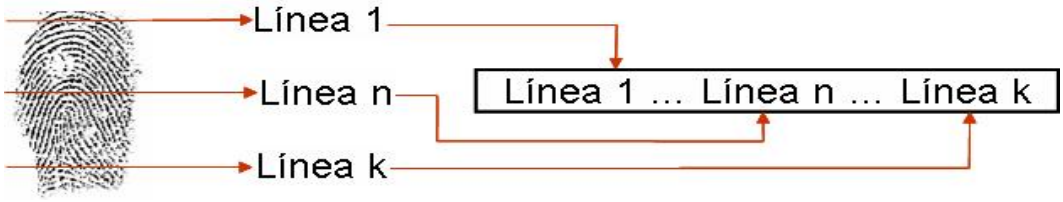


Figura 11. Diagrama que ilustra la representación celular del patrón de la huella.

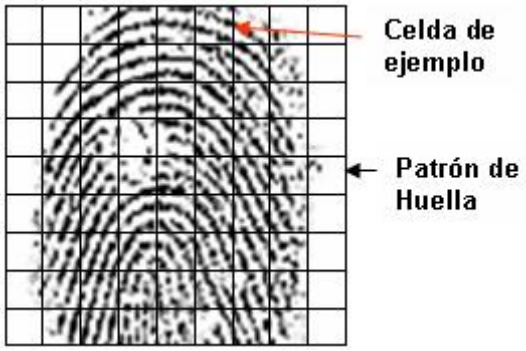


Figura 12. Representación celular del patrón de la huella

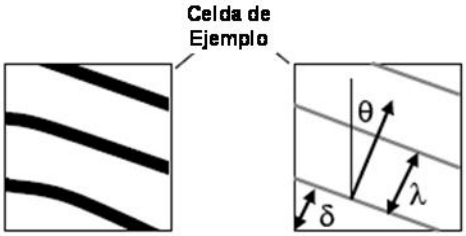


Tabla 10. Niveles de escena adquisición de imagen

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

Tabla 11. Encabezado de record general

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

Tabla 12. Código de algoritmo de compresión.

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

Tabla 13. Encabezado del record de imagen de dedo

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

Tabla 14. Código de posición de dedos, y dimensiones máximas

Posición de dedos	Código dedo	Máx. área imagen (mm^2)	Ancho (cm)	Longitud (mm)
Desconocido	0	1745	406	38.1
Pulgar derecho	1	1745	406	38.1
Índice derecho	2	1640	406	38.1
Corazón derecho	3	1640	406	38.1
Anular derecho	4	1640	406	38.1
Meñique derecho	5	1640	406	38.1
Pulgar izquierdo	6	1745	406	38.1
Índice izquierdo	7	1745	406	38.1
Corazón izquierdo	8	1640	406	38.1
Anular izquierdo	9	1640	406	38.1
Meñique izquierdo	10	1640	406	38.1
Derecha completa 4 dedos	13	6800	83.8	76.2
Izquierda completa 4 dedos	14	6800	83.8	76.2
Pulgares completa (2)	15	4800	50.8	76.2

Tabla 15. Tipos de impresión de dedo y palma.

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

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

Tabla 16. Ejemplo de almacenamiento de la huella digital.

Campo	Bytes	Valor	Notas
Identificador de formato	1-4	46 49 52 00	"FIR" – Record de Imagen de dedo
Número de versión	5-8	30 31 30 00	"010"
Longitud del record	9-14	00 00 00 03 93 b5	Una vista de dedo 32+1*(14+234,375)
Dispositivo ID	15-16	01 02	Vendedor proveedor
Nivel de adquisición de imagen	17-18	00 1F	Nivel 31
Número de dedos/palmas	19	01	
Unidad de escala	20	01	Píxel/pulgada

Campo	Bytes	Valor	Notas
Resolución Scan (horiz)	21-22	01 F4	500 píxel/pulgada
Resolución Scan (vert)	23-24	01 F4	500 píxel/pulgada
Resolución imagen (horiz)	25-26	01 F4	500 píxel/pulgada
Resolución imagen (vert)	27-28	01 F4	500 píxel/pulgada
Profundidad píxel	29	08	256 niveles de gris
Algoritmo de compresión imagen	30	00	No comprimido (no paquetes de bit)
Reservado	31-32	00 00	

2.1.3 Banda Magnética. Es una banda negra o marrón, que está hecha de finas partículas magnéticas en una resina. Las partículas pueden ser aplicadas directamente a la tarjeta o pueden ser hechas en forma de banda y después ser adherida a la tarjeta.

La banda magnética puede ser de baja coercitividad Lo-CO (banda marrón), hecha de oxido de hierro, o de alta coercitividad Hi-CO (banda negra) hecha de ferrita de bario. Estos materiales se mezclan con una resina para formar una mezcla espesa que se cubre con un sustrato. Una vez cubierta con el sustrato las partículas en la mezcla son alineadas para dar una buena señal en proporción al ruido (esto es equivalente a eliminar los estallidos y golpes que se oyen en viejas grabaciones). La banda se pasa con la mezcla espesa aún húmeda a través de un campo magnético para encuadrar todas las partículas.

La banda magnética en la tarjeta final puede ser codificada porque las partículas pueden ser magnetizadas en dirección sur o norte. Cambiando la dirección de codificación a lo largo de la banda permite escribir la información en la banda. Esta información puede ser leída y luego cambiada tan fácilmente como la primera codificación.

La densidad de partículas en la resina es uno de los factores de control de amplitud de señal. Entre más partículas haya, más alta será la amplitud de la señal. La densidad combinada con el grosor dan un método para controlar la amplitud. La importancia de la amplitud de la señal radica en la definición del diseño del lector de tarjetas. El estándar ISO/IEC 7811 define la amplitud de señal para las tarjetas que son usadas en un ambiente de intercambio (como las bancarias). La densidad de bits de información es seleccionada basada en los requerimientos del usuario. El estándar ISO/IEC 7811 establece los requerimientos de densidad de bits para las tarjetas en un ambiente de intercambio.

Cada carácter que es codificado en la banda está hecho de un número de bits, donde la polaridad de las partículas define cada bit. Los esquemas más comunes de codificación son F2F (Aiken BiPhase) y MFM (Modified Frequency Modulation).

La banda magnética tiene en su interior tres tracks o pistas (ver Tabla 17. Descripción de los Track de la Banda Magnética) la pista uno (1) o IATA, la pista dos (2) o ABA y la pista tres (3) o THRIFT

Tabla 17. Descripción de los Track de la Banda Magnética

Track no.	Densidad de grabación (bit por pulgada)	Configuración de carácter (incluyendo bit de paridad) (bit por carácter)	Información de contenido (incluyendo caracteres de control)
1	**210**	**7**	**79 caracteres alfanuméricos**
2	**75**	**5**	**40 caracteres numéricos**
3	**210**	**5**	**107 caracteres numéricos**

Track 1 (IATA). Con una densidad de grabación de 210 bit/pulgada, puede tener hasta 79 caracteres alfanuméricos; cada carácter compuesto por 7 bits, 6 bit de datos + 1 paridad (impares), ver Tabla 18. Composición Track 1.

Tabla 18. Composición Track 1

	< 76 CARACTERES ALFANUMÉRICOS >								
CI	CF	PAN	CS	NOMBRE	CS	ADD DATA	DIS DATA	CF	LRC

	DESCRIPCIÓN	**NO. CARACTERES**	**VALOR**
CI	CENTINELA INICIAL	1	05H
CF	CÓDIGO DE FORMATO	1	
PAN	NÚMERO CUENTA PRINCIPAL	19 DÍGITOS MÁX.	
CS	CAMPO SEPARADOR	1	3EH
NOMBRE	NOMBRE	26 MÁX.	
CS	CAMPO SEPARADOR	1	3EH
ADD DATA	FECHA DE VENCIMIENTO (AA/MM)	4	
	CÓDIGO DE SERVICIO	3	
DIS DATA	DATOS DISCRETOS PVKI	1	
	Y/O PVV O OFFSET	4	
	Y/O CVV O CVC	3	
CF	CENTINELA FINAL	1	1FH
LRC	CARÁCTER DE VERIFICACIÓN DE REDUNDANCIA LONGITUDINAL		

PVKI Pin Indicador de Verificación de llave PVV Pin verificador de valor
CVV Valor de verificación de Tarjeta CVC Código de validación de Tarjeta

Track 2 (ABA) Con una densidad de grabación de 75 bit/pulgada, puede tener hasta 40 caracteres alfanuméricos; cada carácter compuesto por 5 bits, 4 bit de datos + 1 paridad (impares), ver Tabla 19. Composición Track 2.

Tabla 19. Composición Track 2

	< 37 CARACTERES NUMÉRICOS >					
CI	PAN	CS	ADD DATA	DIS DATA	CF	LRC

	DESCRIPCIÓN	NO. CARACTERES	VALOR
CI	CENTINELA INICIAL	1	0BH
PAN	NÚMERO CUENTA PRINCIPAL	19 DÍGITOS MÁX.	
CS	CAMPO SEPARADOR	1	0DH
ADD DATA	FECHA DE VENCIMIENTO (AA/MM)	4	
	CÓDIGO DE SERVICIO	3	
DIS DATA	DATOS DISCRETOS PVKI	1	
	Y/O PVV O OFFSET	4	
	Y/O CVV O CVC	3	
CF	CENTINELA FINAL	1	0FH
LRC	CARÁCTER DE VERIFICACIÓN DE REDUNDANCIA LONGITUDINAL		

PVKI Pin Indicador de Verificación de llave PVV Pin verificador de valor
CVV Valor de verificación de Tarjeta CVC Código de validación de Tarjeta

Track 3 (THRIFT-TTS) Con una densidad de grabación de 210 bit/pulgada, puede tener hasta 107 caracteres alfanuméricos; cada carácter compuesto por 7 bits, 6 bit de datos + 1 paridad (impares) ver Tabla 20. Composición Track 3.

Tabla 20. Composición Track 3

	< 104 CARACTERES ALFANUMÉRICOS >						
CI	CF	PAN	CS	ADD DATA	DIS DATA	CF	LRC

	DESCRIPCIÓN	NO. CARACTERES	VALOR
CI	CENTINELA INICIAL	1	0BH
CF	CÓDIGO DE FORMATO	2 DÍGITOS	
PAN	NÚMERO CUENTA PRINCIPAL	19 DÍGITOS MÁX.	
CS	CAMPO SEPARADOR	1	0DH
ADD DATA	CÓDIGO DE PAÍS (OPCIONAL)	3	
	CÓDIGO DE MONEDA	3	
	EXPONENTE DE MONEDA	1	
	MONTO AUTORIZADO POR CICLO	4	
	MONTO REMANENTE DEL CICLO	4	
	INICIO DEL CICLO (FECHA VALIDA)	4	
	LONGITUD DEL CICLO	2	

	DESCRIPCIÓN	NO. CARACTERES	VALOR
ADD DATA	CUENTA DE INTENTOS	1	
	PIN DE CONTROL DE PARÁMETROS (OPCIONAL)	6	
	CONTROLES DE INTERCAMBIO	1	
	RESTRICCIONES DE SERVICIO PAN	2	
	RESTRICCIONES DE SERVICIO SAN -1	2	
	RESTRICCIONES DE SERVICIO SAN-2	2	
	FECHA DE EXPIRACIÓN (OPCIONAL)	4	
	NÚMERO DE SECUENCIA DE TARJETA	1	
	NÚMERO DE SEGURIDAD DE TARJETA (OPCIONAL)	9	
DIS DATA	NO. PRIMERA CUENTA SUBSIDIARIA (OPCIONAL)		
	NO. SEGUNDA CUENTA SUBSIDIARIA (OPCIONAL)		
	MARCADOR DE RELEVO	1	
	DÍGITO DE CONTROL CRIPTOGRÁFICO (OPCIONAL)	6	
	DATOS DISCRETOS		
CF	CENTINELA FINAL	1	0FH
LRC	CARÁCTER DE VERIFICACIÓN DE REDUNDANCIA LONGITUDINAL		

PVKI Pin Indicador de Verificación de llave PVV Pin verificador de valor
CVV Valor de verificación de Tarjeta CVC Código de validación de Tarjeta

Seguridad en la banda magnética. La seguridad utilizada en las bandas magnéticas es por lo general tecnología propietaria y costosa, dentro de las técnicas más comunmente utilizadas están: Marca de agua magnética (Watermark Magnetics ®), XSec, Holomagnéticos, XiShield, Jitter Enhancement, ValuGard, MagnePrint® entre otras.

2.1.4 Tarjeta con circuito integrado. Las tarjetas con circuito integrado también son llamadas tarjetas inteligentes o tarjetas con chip, sin embargo estos términos no son sinónimos y los distintos tipos de tarjeta se distinguen por el tipo de chip que tienen y la interfaz que usan para comunicarse con el lector.

Hay tres tipos de chips que están asociados con estas tarjetas: solo memoria, cableado lógico y microcontrolador.

Tarjetas con circuito integrado con chip de solo memoria. Estas tarjetas son como bandas magnéticas electrónicas y su objetivo es el suministrar una mayor seguridad que la tarjeta con banda magnética tradicional. Su ventaja sobre las tarjetas con banda magnética es su capacidad de memoria (hasta 16Kbits) y el menor costo que tiene el dispositivo lector/escritor de la tarjeta. Las tarjetas con chip de solo memoria simplemente almacenan datos. Estas tarjetas pueden tener una memoria que no se puede reescribir.

Las primeras versiones eran de solo lectura, baja capacidad (máximo 160 unidades de valor), tarjetas prepago con bajo nivel de seguridad. Versiones más modernas usan memorias de lectura/escritura y esquemas de conteo binario que permite que las tarjetas lleven más de 20000 unidades de valor. Muchas de estas tarjetas tienen esquemas avanzados de autenticación en el chip.

Tarjetas con circuito integrado cableado lógico. Contiene un maquina de estado basado en lógica que suministra encriptación y autenticación de acceso a la memoria y su contenido. Suministra un sistema de archivos estáticos que soporta múltiples aplicaciones, con acceso encriptado al contenido de la memoria opcional. El sistema de archivos y el juego de comandos solo pueden ser cambiados rediseñando la lógica del circuito integrado. Estas tarjetas incluyen variaciones como las I-Class o MIFARE.

Tarjeta con circuito integrado microcontrolador seguro. Estas tarjetas contienen un microcontrolador, un sistema operativo, una memoria lectura/escritura que puede ser actualizada muchas veces. Estas tarjetas contienen y ejecutan lógica y cálculos y almacenan datos de acuerdo con su sistema operativo. Todo lo que necesita la tarjeta para operar es una fuente de poder y un puerto de comunicación. Esta disponible en tarjetas de contacto, no contacto y de interfaz-dual. Este tipo de tarjetas son las que se conocen como tarjetas inteligentes.

Hay dos tipos básicos de interfaz de tarjetas con circuito integrado: las de contacto y las de no contacto. El que sea de contacto o no de contacto se refiere al suministro de corriente y bajo que esquema son transferidos los datos de la tarjeta al dispositivo lector y viceversa. Las tarjetas pueden tener los dos tipos de chips (llamadas hibridas) o que usan una chip de interfaz dual llamado tarjetas “combi”.

Tarjeta Inteligente de Contacto. Estas tarjetas requieren ser insertadas en un lector de tarjeta inteligente con una conexión directa a un micromódulo conductivo en la superficie de la tarjeta[1].

Tarjeta Inteligente de no contacto. Estas tarjetas deben estar ubicadas cerca del lector (generalmente no superior a 10 centímetros) para que se realice el intercambio de información. El intercambio de información se realiza con ondas

[1] Charles Cagliostro, Smart Cards Primer. (Diciembre 1999)

de radio frecuencia, esta comunicación se logra con una antena interna tanto en la tarjeta como en el lector.

Tarjeta Inteligente Híbrida. Estas tarjetas contienen dos chips en las tarjetas, una que soporta la interfaz de contacto y otra que soporta la interfaz de no contacto. Por lo general los chips contenidos en la tarjeta no están conectados entre sí.

Tarjeta Inteligente de interfaz dual. Estas tarjetas contienen un solo chip que soporta los dos tipos de interfaz, los de contacto y los de no contacto, permitiendo el acceso a la información por cualquiera de las dos vías.

Caracteristicas tarjeta con circuito integrado de contacto. La norma ISO7816 estableció las características que deben cumplir las tarjetas con circuito integrado, en cuanto a las características físicas de la tarjeta, dimensiones, ubicación de los contactos (ver Figura 13. Ubicación de los contactos, Figura 14. Asignación de contactos, Tabla 21. Asignación Contactos), definición de los protocolos de señales eléctricas y su transmisión.

Figura 13. Ubicación de los contactos

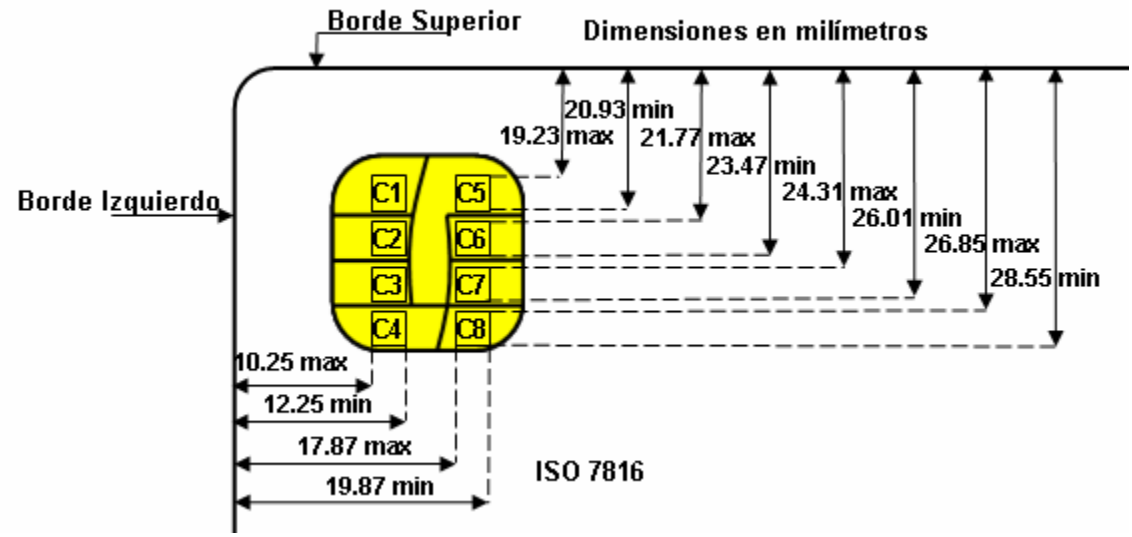


Figura 14. Asignación de contactos

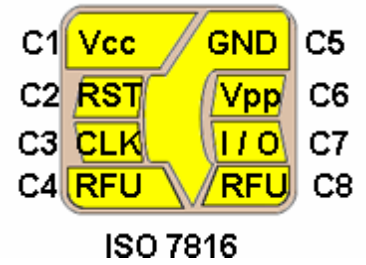


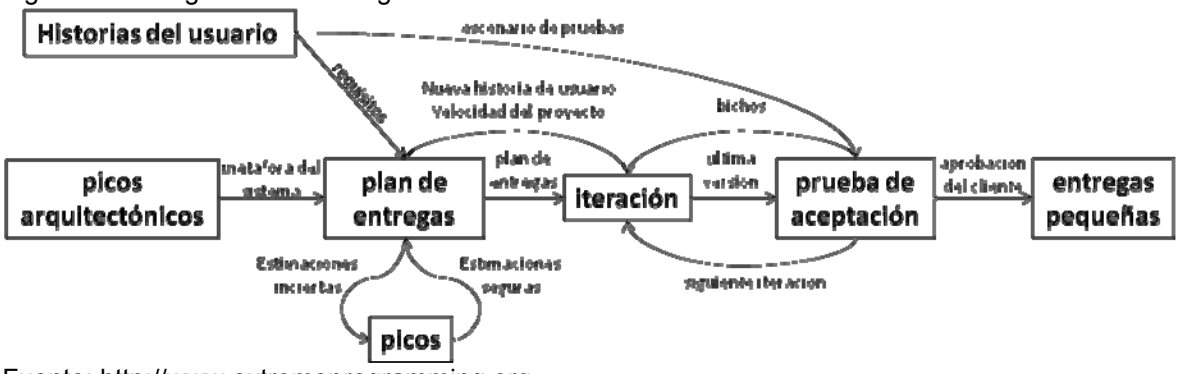
Tabla 21. Asignación Contactos

Contacto	Asignación	Descripción
C1	Vcc	Entrada de fuente de poder 5V (Opcional)
C2	Reset	Reinicializar la señal suministrada por el dispositivo de interfaz o en combinación con un restablecimiento interno del circuito (si es interno, es obligatorio el suministro de voltaje Vcc)
C3	Clock	Cronometro o señal de reloj (opcional)
C4	RFU	Reservado para uso futuro
C5	Gnd	Tierra (referencia de voltaje)
C6	Vpp	Voltaje de programación de entrada (Opcional)
C7	I/O	Entrada o Salida serial de los datos del circuito integrado en la tarjeta
C8	RFU	Reservado para uso futuro

2.1.5 Programación Extrema (eXtreme Programming – XP). La programación extrema se preocupa o centra su atención en las personas, tanto en la satisfacción del cliente, como en el trabajo mesurado y en equipo; es ideal para proyectos riesgosos con requerimientos dinámicos.

Al igual que en otras metodologías, XP tiene cuatro grandes etapas (planeación, diseño, codificación y pruebas) (ver Figura 15).

Figura 15. Diagrama Metodología XP



Fuente: http://www.extremeprogramming.org

Planeación. En ella se utilizan las historias del usuario (user stories) que son escritos hechos por usuario donde presentan las necesidades que observan debe suplir el sistema a ellos, éstas son escritas en terminología del cliente, sin sintaxis técnica, deben suministrar los suficientes detalles para planear los tiempos de entrega, las pruebas a realizarse y para determinar los riesgos.

Las user stories por lo general deben ocupar entre una y tres semanas en un "tiempo de desarrollo ideal", en caso de que el tiempo requerido sea mayor, la historia debe ser partida. [2]

Diseño. El diseño debe ser sencillo, para las sesiones de diseño se utilizan las tarjetas CRC (Clase, Responsabilidades, Colaboradores). Como siempre las cosas sencillas funcionan mejor que las complejas, en caso de encontrarse con código complejo, debe ser remplazado por código sencillo que es más económico, velos y fácil de remplazar.

Es importante definir los objetivos de manera clara y que sea entendible para todos los miembros del equipo, así como elegir un sistema de nombres que sea claro y entendible para todos los miembros del equipo y que puedan relacionar fácilmente sin necesidad de aprender lenguaje complejo y difícil de aprender sobre el sistema.

No se debe tener miedo de rehacer código, cuando se elimina redundancia, se eliminan funcionalidades no usadas y se rejuvenecen diseños obsoletos, se está refabricando.

Codificación. Siempre debe estar disponible el cliente, no sólo para ayudar al equipo de desarrollo, sino para ser parte de él. Hay que recordar que las user stories son escritas por el usuario con la ayuda de los desarrolladores, para permitir estimación de tiempos y asignarle prioridades, la ayuda del cliente asegura que la mayoría de los deseos de funcionalidad del sistema estén cubiertos por las historias.

Pruebas. Todo el código debe tener unidades de prueba y antes de ser entregado debe haber pasado por estas unidades, las pruebas no se hacen al final, se deben hacer a lo largo del desarrollo.

[2] http://www.extremeprogramming.org/rules/userstories.html Octubre 25 de 2006 23:50

Cuando se encuentre un bug (un incidente) se debe crear una prueba que evite que vuelva a aparecer. Un bug en producción requiere que se escriba una prueba de aceptación para protegese de él.

2.2 MARCO LEGAL O NORMATIVO

2.2.1 Jurisprudencia Colombiana.

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

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

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

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

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

Artículo 193 - Ofrecimiento, venta o compra de un instrumento apto para interceptar la comunicación privada entre personas. El que sin permiso de autoridad competente, ofrezca, venda o compre instrumentos aptos para

interceptar la comunicación privada entre personas, incurrirá en multa siempre que la conducta no constituya delito sancionado con pena mayor.

En este artículo se incluye el ofrecimiento a través de una página web de software que pueda servir como instrumento para interceptar una comunicación privada, como los sniffers de redes, software para ataques de fuerza bruta o contraseñas de acceso.

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

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

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

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

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

2.2.3 Estándares de la Organización Internacional de Estándares (ISO)

ISO/IEC 3166 Códigos para la representación de los nombres de los países y sus subdivisiones
parte 1: Código de países
parte 2: Códigos de subdivisión de países
parte 3: Códigos para el nombre formal usado por los países

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

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

ISO/IEC 7810 Tarjetas de Identificación - Características físicas

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

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

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

ISO/IEC 7816 Tarjetas de Identificación - Tarjetas con circuitos integrados

parte 1: Tarjetas con contactos - Características físicas
parte 2: Tarjetas con contactos - Dimensiones y localización de los contactos
parte 3: Tarjetas con contactos - Protocolos eléctricos
parte 4: Organización, seguridad y comandos de intercambio
parte 5: Registro de aplicación de proveedores
parte 6: elementos para intercambio de datos ínter industria
parte 7: comandos ínter industria para Lenguaje estructurado de consulta de tarjetas (SCQL)
parte 8: Comandos para operaciones seguras
parte 9: Comandos para administración de tarjetas
parte 10: Señales electrónicas y respuesta a restablecer para tarjetas síncronas
parte 11: Verificación personal a través de métodos biométricos
parte 12: Interfaz eléctrica USB y procedimientos de operación
parte 13: Comandos para administración de aplicación en un ambiente multi-aplicación
parte 15: Aplicación de información criptográfica

ISO/IEC 8484 Bandas magnéticas en libros de ahorros

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

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

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

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

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

ISO/IEC 9992 Tarjetas de transacción financiera - Mensajes entre tarjetas de circuito integrado y dispositivo receptor de tarjeta
parte 1: Concepto y estructura
parte 2: Funciones, mensajes (comandos y respuestas), elementos y estructura de datos

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

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

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

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

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

ISO/IEC 11694 Tarjetas de identificación - tarjetas con memoria óptica -- método de grabación lineal
parte 1: Características físicas
parte 2: Dimensiones y localización del área óptica accesible
parte 3: propiedades ópticas y características
parte 4: estructura lógica de datos
parte 5: formato de datos para el intercambio de información para aplicaciones usando ISO/IEC 11694-4, Anexo B
parte 6: Uso de biométricos en una tarjeta con memoria óptica

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

ISO/IEC 14496: Tecnología de información – Codificación de objetos audio-visuales
parte 1: Sistemas
parte 2: Visual
parte 3: Audio
parte 4: prueba de conformidad
parte 5: Referencia de Software
parte 6: Estructura de entrega de integración multimedia (DMIF)
parte 7: Referencia de software optimizado
parte 8: Transporte en redes IP
parte 9: Referencia de Hardware
parte 10: Codificación avanzada de video (AVC)
parte 11: Descripción de escena y motor de aplicación

parte 12: Formato ISO base de archivos de media
parte 13: Manejo de propiedad intelectual y Protección de extensiones
parte 14: Formato de archivo MPEG-4
parte 15: Formato de archivo AVC
parte 16: Extensión de formato de animación (AFX)
parte 17: Formato de subtitulo de texto de cronometro
parte 18: Compresión de formato de streaming (para fuentes de tipo abierto)
parte 19: Textura sintetizada de stream
parte 20: Representación de escena ligera (LASeR)
parte 21: Extensión de formato gráfico MPEG-J (GFX)
parte 22: Especificación de formato de fuente abierta (OFFS)
parte 23: Representación Simbólica de música (SMR)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ISO/IEC 19092 Servicios Financieros – Biométricos
parte 1: estructura de seguridad.

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

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

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

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

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

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

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

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

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

2.2.4 Estándares del Instituto Colombiano de Normas Técnicas (ICONTEC)

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

NTC1387 Sistema Internacional para la numeración de libros ISBN

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

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

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

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

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

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

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

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

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

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

NTC 3841 Codificación por barras. Terminología

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

NTC 3843 Codificación por barras. Especificaciones de simbología. Codabar

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

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

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

NTC-EN 796 Codificación por barras. Identificadores de simbología

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

2.2.5 Estándares de la Organización para el avance de estándares de información estructurada (OASIS)

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

2.2.6 Organización Internacional de Aviación Civil (ICAO)

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

Nota: no se están referenciado estándares de organizaciones nacionales de estandarización de otros países como NIST de Estados Unidos, porque son estándares que no se pueden exigir dentro de Colombia, porque ante la ley no tienen ningún valor; razón por la cuál se recomienda empezar a generar estándares y legislación en el ámbito nacional que proteja a los usuarios y regule a las empresas desarrolladoras y comercializados de éstas tecnologías.

3 METODOLOGÍA

3.1 ENFOQUE DE LA INVESTIGACIÓN

Empírico Analítico: orientado a la interpretación y transformación del mundo material.

3.2 LÍNEA DE INVESTIGACIÓN DE USB / SUB-LÍNEA DE FACULTAD / CAMPO TEMÁTICO DEL PROGRAMA

3.2.1 Línea de investigación. Tecnologías Actuales y Sociedad

3.2.2 Sublínea de investigación. Sistemas de Información y Comunicación

3.2.3 Campo temático del programa. Almacenamiento de Datos

3.3 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Para el presente proyecto de grado la recolección de información se realizó mediante la búsqueda en las páginas Web de las entidades supranacionales (entre otras ISO e ICAO) e internacionales (DoD y BioAPI) que manejan la información.

Mientras que para la recolección de información en las entidades nacionales (Ministerios, Superintendencias, entre otras.) se consultó en las páginas de las entidades y en otros casos se intercambió correspondencia con funcionarios de éstas para consulta de información específica que no se encontraba en las páginas de las entidades y que era pertinente para esta investigación.

3.4 POBLACIÓN Y MUESTRA

Para el desarrollo de este trabajo las estadísticas serán tomadas de las entidades oficiales nacionales, internacionales y supranacionales que hayan realizado este tipo de levantamiento de información.

3.5 HIPÓTESIS

La autenticación de la identidad de una persona y de productos a través de estas tecnologías hacen fiable la información manejada en el aplicativo, minimizando los errores de registros ingresados a las bases de datos.

3.6 VARIABLES

3.6.1 Variable independiente. Tecnología desarrollada para la autenticación de usuarios en las redes, aplicaciones e instalaciones.

3.6.2 Variable dependiente. Margen de error y fiabilidad de la Tecnología desarrollada para la autenticación de usuarios en las redes, aplicaciones e instalaciones.

3.6.3 Variable de control. Normatividad desarrollada, para la autenticación de usuarios en las redes, aplicaciones e instalaciones.

3.6.4 Variable cualitativa. Concepción de los usuarios sobre las características que deben cumplir las tecnologías de autenticación.

4 DESARROLLO INGENIERIL

Después de más de tres (3) años de investigación, y a través de entrevistas y/o consultas a inventores, autoridades en el tema, organismos reguladores y/o investigadores del área, comerciantes y usuarios o potenciales usuarios de las tecnologías, se logró condensar la información en tan sólo cuatro gigabites (4 GB) de documentos electrónicos en formato pdf, la mayoría de ellos en idioma ingles, francés y alemán, donde se encuentran más de ciento cincuenta (150) patentes, dos estados del arte, cada uno con más de ciento cincuenta (150) hojas, la mayoría de las normas, borradores y/o documentos producidos por organismos reconocidos en el área como ISO, ICONTEC, NIST, ASIS, GS1, ICAO, BioAPI; gran número (más de mil) de papers, libros, artículos y demás documentación generada por inventores e investigadores en el tema y otra documentación que por sus características sus autores clasificaron como confidencial, reservada o secreta.

Con toda esta información se logró establecer cuál era la necesidad primaria de los interesados en el tema (investigadores, autoridades, usuarios finales), que es: documentación confiable, actualizada y en español sobre todo en la parte teórica (su historia, tendencia, confiabilidad, modo de evaluación para determinar cuál se requiere y como usarla) y sobre la normatividad que las rige.

Ante esta necesidad y los requerimientos institucionales de desarrollar una aplicación con estas tecnologías y un documento sucinto, se produjó este trabajo y la aplicación que se presenta.

4.1 ANÁLISIS DE LA APLICACIÓN

Aplicando la metodología XP (Explicada en el marco teórico – conceptual) se procedió a recaudar la información necesaria para el desarrollo de la aplicación del hotel, a través de entrevistas, estableciendo así la situación actual y la solución propuesta para los requerimientos planteados por el adminstrador del hotel.

Teniendo en cuenta los servicios suministrados por el Hosting, se utilizará para el desarrollo de la aplicación a MySQL como motor de base de datos y a PHP como lenguaje de programación del sitio web.

Considerando los requerimientos del usuario final y teniendo en cuenta la gran cantidad de opciones de autenticación que se pueden usar (ver Tabla 1. Composición de tecnologías, página 8) se estableció de acuerdo a la facilidad de uso, aceptabilidad y costos utilizar el código de barras para el control de los productos que se comercializan en los ambientes del hotel y la tecnología biométrica para el manejo de los cargos a los huéspedes del hotel.

De los más de 60 codigos de barras que existen y se resumen en el anexo B, se seleccionó el código EAN-13, por ser el más ampliamente difundido en Colombia y por ende hay suministros y soporte técnico garantizado a corto y mediano plazo.

De las más de 30 tecnologías biométricas que se resumen en el anexo C, solo se consideraron las tecnologías biométricas más comunes (ver Tabla 8. Comparativo de las tecnologías biométricas más comunes., página 15) y su porcentaje de participación en el mercado (ver Figura 6. Mercado de Biométricos por tecnología 2006, página 21) y de ellas se seleccionó la huella digital como la mejor opción para el control de consumos, considerando su alta aceptabilidad, amplio desarrollo y su universalidad. Tambien se consideró que aunque esta tecnología se consideró inicialmente para ser implantada para control consumos a posteriori se puede utilizar tambien para el control de acceso a las habitaciones y la red del hotel, sin que esto implique grandes costos adicionales.

4.1.1 User Stories

En entrevista realizada al administrador del hotel se logró establecer las siguientes user stories que reflejan la situación actual y obtener los formatos utilizados para el manejo del hotel actualmente (ver anexo D – documentos hotel) y la solución propuesta para las necesidades manifestadas.

Situación Actual:

Reserva. El huésped llama e informa que desea realizar una reserva y se registra en el libro de reservas, llenando la información allí solicitada (Nombre, Número de Huéspedes, tipo de habitación, Número de noches, teléfono, e-mail, dirección, fecha de la reserva) y en caso de que requiera ser recogido (vuelo, procedencia,aerolínea, hora del vuelo), siempre se aceptan las reservas, teniendo en cuenta que en caso de que no haya cupo en el hotel, se tienen convenios con otros hoteles para hospedar al huésped en las mismas condiciones y precios ofrecidos por el hotel.

Check In. El huésped llega se registra en el hotel llenando la hoja de registro (nombre, pasaporte No., fecha de llegada, nacionalidad, profesión, fecha de salida, procedencia, destino, dirección, teléfono, ciudad, departamento, e-mail, fecha de nacimiento) y en caso de ser extranjero llena el libro del DAS que contiene la misma información que la hoja de registro, si tiene reserva se verifica y se le asigna la habitación reservada, en caso contrario se asignará la habitación de acuerdo a la disponibilidad y se entregarán hasta dos copias de la llave de la habitación.

Reporte al DAS. Diariamente de lunes a viernes a las 16:00 se debe enviar vía mail en archivo plano la información de los huéspedes extranjeros que hanrealizado check in o check out, el día Lunes se incluirán los movimientos del fin de semana (Sábado y Domingo), este archivo plano debe contener la siguiente información: código del hotel, código de la ciudad, tipo de documento, número del documento, código nacionalidad, primer apellido, segundo apellido, nombres, tipo de movimiento (llegada / salida) fecha de llegada y/o salida, país de procedencia, país de destino

Desayuno. Al llegar el huésped al restaurante el mesero le entrega el formato de desayuno para que escoja el tipo de desayuno que desea y diligencie el formato, una vez diligenciado y firmado, se entrega al cajero y éste informa al chef el pedido y carga a la habitación el pedido.

Restaurante y Bar. El huésped se identifica como tal y realiza su pedido, el barman o cajero llena el formato de pedido, una vez entregado el pedido y antes de que se retire el huésped del recinto se le hace firmar el recibo.

Registro de cargos bar y restaurante. Diariamente el barman y el cajero del restaurante entregarán al cierre del ambiente los comprobantes de pedidos para que sean cargados en la cuenta de la habitación, donde sólo se registrará el número del recibo, el concepto (bar/restaurante/minibar/teléfono/lavandería/otros) y el monto total del recibo, el recibo se anexará a la cuenta como comprobante.

Registro de cargos habitación. Diariamente las aseadoras entregarán al término del aseo de las habitaciones los comprobantes de consumos de minibar y los servicios de lavandería solicitados para que sean cargados en la cuenta de la habitación donde sólo se registrará el número del recibo, el concepto

(bar/restaurante/minibar/teléfono/lavandería/otros) y el monto total del recibo, el recibo se anexará a la cuenta como comprobante.

Check out. El huésped informa o llega a recepción para hacer entrega de la habitación, el botones procede a verificar la habitación, para realizar los cargos de minibar que procedan y de los elementos que hagan falta de la habitación (control remoto, dvd o cualquier otro elemento); el recepcionista verifica con el bar y el restaurante los consumos que han habido hasta el momento y no han sido reportados, carga los consumos y procede a hacer el check out, pedir las llaves y cobrar la cuenta.

Descripción de requerimientos de la solución propuesta:

Reserva. El huésped via telefónica o a través de la página web completa la información sobre la reserva que desea hacer, ingresando la información solicitada (Nombre, Número de Huéspedes, tipo de habitación, Número de noches, teléfono, e-mail, dirección, fecha de la reserva y en caso de que requiera ser recogido vuelo, procedencia, aerolínea, hora del vuelo)), siempre se aceptan las reservas, teniendo en cuenta que en caso de que no haya cupo en el hotel, se tienen convenios con otros hoteles para hospedar al huésped en las mismas condiciones y precios ofrecidos por el hotel.

Check In sin reserva. El huésped llega a la recepción e informa su intención de hospedarse en el hotel, si hay cupo se procede a solicitarle sus datos básicos (nombre, pasaporte No., nacionalidad, profesión, fecha de nacimiento, dirección, teléfono, ciudad, e-mail) si ya ha estado antes, se verifican sus datos, posteriormente se le solicita la información respecto a su estadía (fecha de salida, procedencia, destino), se preguntará quien es el responsable del pago – en caso de no ser él mismo, se le solicitan los datos del responsable de la cuenta (nombre, número de documento, dirección, teléfono, fax, e-mail) y en caso de ser extranjero llena el libro del DAS que contiene la misma información recogida previamente, se asignará la habitación de acuerdo a la disponibilidad y se entregarán hasta dos copias de la llave de la habitación.

Check In con reserva. El huésped llega a la recepción e informa de la reserva, se procede a solicitarle sus datos básicos (nombre, pasaporte No., nacionalidad, profesión, fecha de nacimiento, dirección, teléfono, ciudad, e-mail) si ya ha estado antes, se verifican sus datos, en caso contrario se completan, posteriormente se verifica la información respecto a su estadía (fecha de salida, procedencia, destino), se preguntará quien es el responsable del pago – en caso de no ser él

mismo, se le solicitan los datos del responsable de la cuenta (nombre, número de documento, dirección, teléfono, fax, e-mail) y en caso de ser extranjero llena el libro del DAS que contiene la misma información recogida previamente, se asignará la habitación y se entregarán hasta dos copias de la llave de la habitación.

Reporte al DAS. Diariamente de Lunes a Viernes a las 16:00 se debe enviar vía mail en archivo plano la información de los huéspedes extranjeros que han realizado check in o check out, el día Lunes se incluirán los movimientos del fin de semana (Sábado y Domingo), este archivo plano debe contener la siguiente información: código del hotel, código de la ciudad, tipo de documento, número del documento, código nacionalidad, primer apellido, segundo apellido, nombres, tipo de movimiento (llegada / salida) fecha de llegada y/o salida, país de procedencia, país de destino

Restaurante. El huésped realiza su pedido, el cajero solicita al huésped que se identifique, verifica y registra el pedido en la aplicación.

Bar. El huésped se identifica, realiza su pedido y el barman registra el pedido en la aplicación y despacha lo solicitado.

Registro de cargos habitación. Diariamente las aseadoras entregarán al término del aseo de las habitaciones los comprobantes de consumos de minibar y los servicios de lavandería solicitados para que sean cargados en la cuenta de la habitación por parte del personal de frontdesk donde se registrará la información contenida en el recibo y el concepto (minibar / lavandería), el recibo se anexará a la cuenta como comprobante.

Registro de telefonía. El personal de front desk verificará el pbx cada seis horas y registrará los consumos de las habitaciones, especificando el número marcado.

Check out. El huésped informa o llega a recepción para hacer entrega de la habitación, el botones procede a verificar la habitación, para realizar los cargos de minibar que procedan y de los elementos que hagan falta de la habitación (control remoto, dvd o cualquier otro elemento); el recepcionista verifica los consumos de telefonía que han habido hasta el momento y no han sido reportados, carga los consumos y procede a hacer el check out, pedir las llaves y cobrar la cuenta, generando la respectiva factura.

Gerencia y contabilidad. Estas dependencias diariamente ven el reporte de reservas, ocupación y consumos, que pueden solicitarlo para el día, el mes, un rango de fechas específico o un huésped específico.

4.2 DISEÑO PROPUESTO DE LA APLICACIÓN

Como se puede concluir de las user stories, actualmente no existe un sistema o una aplicación informática implementada para los procesos descritos, toda la documentación y procesos se llevan de manera manual y se almacenan en documentos impresos como se ven en el anexo D (Página 118).

A partir de las user stories de la solución propuesta se plantea el siguiente diseño (presentado en tarjetas CRC, modelo conceptual y lógico de la base de datos) para desarrollar la aplicación.

4.2.1 Tarjetas CRC (Clase, Responsabilidades, Colaboradores)

Nombre de Clase: Factura	
Superclase:	
Subclase:	
Responsabilidades	**Colaboradores**
Saber el monto total a pagar No. Factura Consumos (Ventas) Ocupación Descuento Productos Descuento Habitación Subtotal Iva Total	Ventas, Ocupación
Saber quién va a cancelar y en que forma Nombre Documento Dirección Telefono	Huésped

Nombre de Clase:	Ocupación
Superclase:	
Subclase:	
Responsabilidades	**Colaboradores**
Saber quien ocupa que habitación y por cuanto tiempo Fecha ingreso Fecha salida Procedencia Destino Habitación Huésped	Huésped, Habitación

Nombre de Clase:	Cliente
Superclase:	
Subclase:	Empresa, Huésped
Responsabilidades	**Colaboradores**
Tener los datos básicos de quien contrata los servicios Documento Nombre e-mail	

Nombre de Clase:	Empresa
Superclase:	Cliente
Subclase:	
Responsabilidades	**Colaboradores**
Conocer los datos básicos de los clientes corporativos Documento Nombre Dirección Teléfono e-mail Fax	

Nombre de Clase:	Huésped
Superclase:	Cliente
Subclase:	
Responsabilidades	**Colaboradores**
Conocer los datos básicos de los clientes no corporativos y de quienes usan directamente los servicios Documento Nombre Primer Apellido Segundo Apellido Tipo de documento Nacionalidad Profesión Estado Civil e-mail	

Nombre de Clase:	Habitación
Superclase:	
Subclase:	Bed & Breakfast, Standard, Apartamento
Responsabilidades	**Colaboradores**
Describir las habitaciones Nombre Número Precio capacidad	

Nombre de Clase:	Bed & Breakfast
Superclase:	Habitación
Subclase:	
Responsabilidades	**Colaboradores**
Describe la habitación Nombre Número Precio capacidad	

Nombre de Clase:	Standard
Superclase:	Habitación
Subclase:	
Responsabilidades	**Colaboradores**
Describe la habitación Nombre Número Precio capacidad	

Nombre de Clase:	Apartamento
Superclase:	Habitación
Subclase:	
Responsabilidades	**Colaboradores**
Describe la habitación Nombre Número Precio capacidad	

Nombre de Clase:	Producto
Superclase:	
Subclase:	Bebida, Comida, Lavanderia, Telefonia, Transporte, Otros
Responsabilidades	**Colaboradores**
Describir las habitaciones Nombre Valor de Comprar Valor de venta Unidad Descripción	

Nombre de Clase:	Bebida
Superclase:	Producto
Subclase:	
Responsabilidades	**Colaboradores**
Describir las habitaciones Nombre Valor de Comprar Valor de venta Unidad Descripción	

Nombre de Clase:	Comida
Superclase:	Producto
Subclase:	
Responsabilidades	**Colaboradores**
Describir las habitaciones Nombre Valor de Comprar Valor de venta Unidad Descripción	

Nombre de Clase:	Lavanderia
Superclase:	Producto
Subclase:	
Responsabilidades	**Colaboradores**
Describir las habitaciones Nombre Valor de Comprar Valor de venta Unidad Descripción	

Nombre de Clase:	Telefonia
Superclase:	Producto
Subclase:	
Responsabilidades	**Colaboradores**
Describir las habitaciones Nombre Valor de Comprar Valor de venta Unidad Descripción	

Nombre de Clase:	Transporte
Superclase:	Producto
Subclase:	
Responsabilidades	**Colaboradores**
Describir las habitaciones Nombre Valor de Comprar Valor de venta Unidad Descripción	

Nombre de Clase:	Otros
Superclase:	Producto
Subclase:	
Responsabilidades	**Colaboradores**
Describir las habitaciones Nombre Valor de Comprar Valor de venta Unidad Descripción	

Nombre de Clase:	Ventas
Superclase:	
Subclase:	
Responsabilidades	**Colaboradores**
Saber que productos se vendieron o suministraron y en que ambiente Fecha Producto Cantidad Valorcompra Cliente Iva pago	Huésped, Producto

Nombre de Clase:	Reserva
Superclase:	
Subclase:	
Responsabilidades	**Colaboradores**
Saber de requerimientos futuros para la ocupación de las habitaciones del hotel Fecha de arrivo Procedencia Vuelo Hora de arrivo Pick up Número de pasajeros Número de noches Huésped e-mail	Huésped, Aerolinea

Roles. De acuerdo con las user stories se lograron establecer los siguientes roles y permisos para los respectivos roles:

Roles de usuario	**No. De Identidades**	**Mecanismo de autenticación**
Administrador	1-5	Validación usuario y clave
Barman	1-10	Validación usuario y clave
Frontdesk	1-10	Validación usuario y clave
Maitre	1-10	Validación usuario y clave
DBA	1-10	Validación usuario y clave
Huésped	1000-100000	ninguno

	Roles de usuario					
Data	DBA	Barman	Huésped	FrontDesk	Administrador	Maitre
pais	**I L A B**		**L**	**L**		
departamento	**I L A B**		**L**	**L**		
ciudad	**I L A B**		**L**	**L**		
ambiente	**I L A B**			**L**		
empresa	**L**			**I L A**	**L**	
estadocivil	**I L A B**			**L**	**L**	
profesion	**I L A B**			**L**	**L**	
tipo_documento	**I L A B**			**L**		
aerolinea	**I L A B**		**L**	**L**	**L**	
tipo_hab	**I L A B**		**L**	**L**		
factura	**I L A B**			**I L A**	**L**	
producto	**I L A B**	**L**		**L**	**L**	**L**
acceso	**I L A B**	**L A**		**L A**	**L**	**L A**
habitacion	**I L A B**			**L**		
huésped	**L**			**I L A**	**L**	
ocupacion	**L**			**I L A**	**L**	
consumo	**L**	**I L A**		**I L A**	**L**	**I L A**
reserva	**L**		**I**	**I L A**	**L**	
detallefac	**L**			**I L A**	**L**	

I Insertar **L** Leer **A** Actualizar **B** Borrar

Componentes. la aplicación cuenta con trés componentes básicos que son:

- Web service
- Base de datos
- Web site

Relevancia. Los atributos que definen el comportamiento de los componentes previamente mencionados son:

- Permitir entrada/salida de archivos
- Utilizar criptografía
- Utilizar un protocolo de red
- Exponer a la interfaz de un web browser
- Utilizar HTTP
- Realizar operaciones aritméticas
- Utiliza autenticación con usuario y clave
- Construido con consultas SQL

Tablas principales. A continuación se muestra a manera de ejemplo el contenido que tendría las tablas principales de la base de datos de la aplicación

Factura

Id_factura	DescProd	Deschab	Formapago	Abono	IVA	Total
00001	0	0	1	0	16000	116000
00002	0	0	1	50000	32000	232000

Huésped

Numdoc	Email	Nombres	Primerapellido	Segundoapellido
73186236	cgalvis@gmail.net	Carlos Mauricio	Galvis	Traslaviña
28376797	auribe@presidencia.gov.co	Alvaro	Uribe	Velez

Id_tipodoc	nacionalidad	Id_profesion	Id_estado	Nit	Dirección	Telefono
1	11001	56	2	9872667	Tr 33 # 123 – 64	12137347
1	11001	49	1		Cr 7 # 10 – 23	16202471

Ocupación

Id_ocupacion	Habitacion	F_in	F_out	Numdoc	Procedencia	Destino
0001	1101	05-01-2007	05-08-2007	73186236	110001	050001
0002	402	06-15-2007	06-16-2007	28376797	050001	990001

Consumo

Id_consumo	Fecha	Id_producto	Cantidad	Valorcompra
00001	05-02-2007	9789990000016	2	1680
00002	05-02-2007	9781110000043	1	4956

Id_ocupacion	Id_ambiente	pago	Descripcion
0001	1	5	
0002	2	5	

Reserva

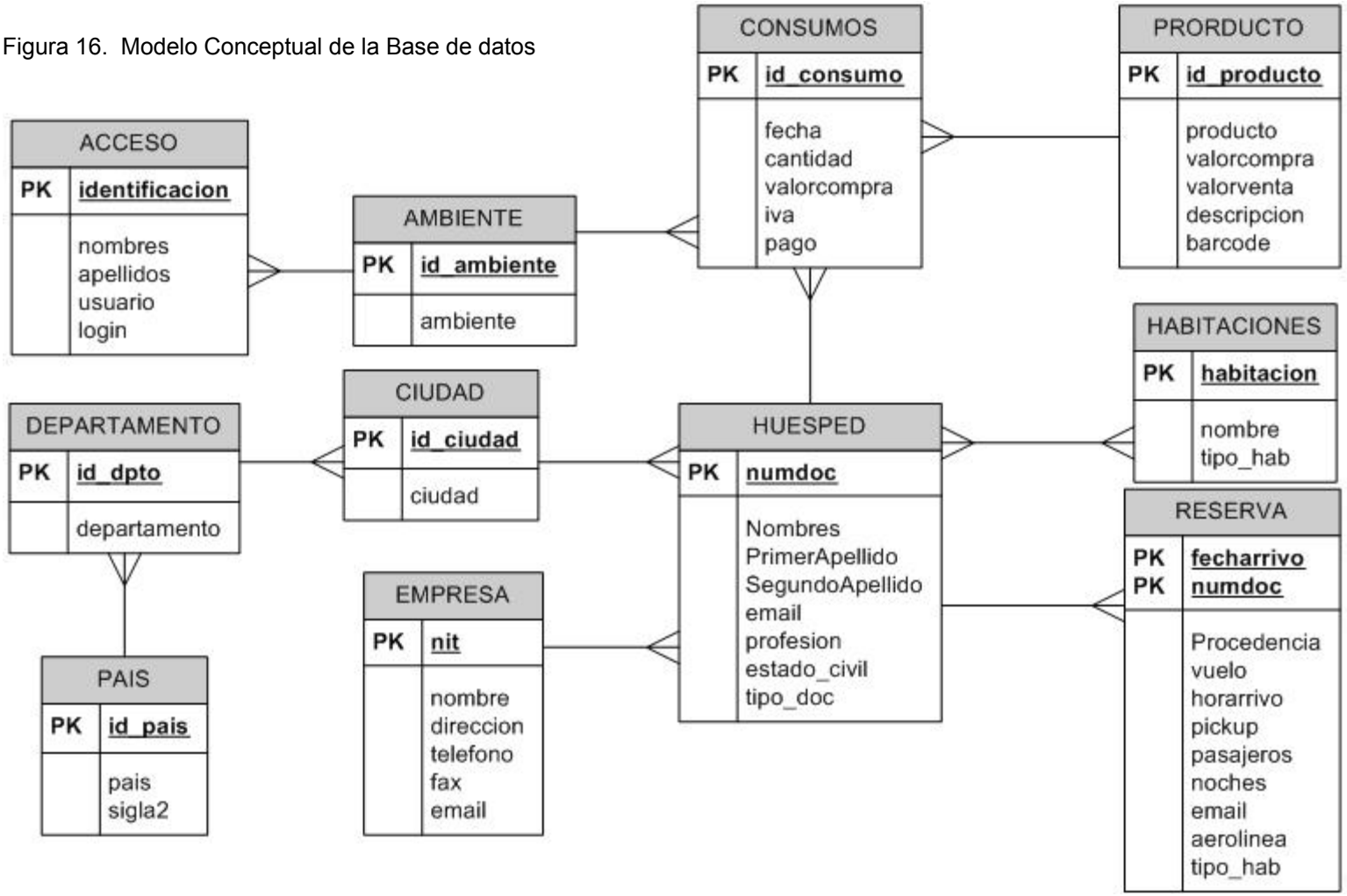
Fecharrivo	Numdoc	Id_aerolinea	Procedencia	Vuelo
06-15-2007	28376797	1	050001	AV456
07-21-2007	94872546			

Horarrivo	Pickup	Pasajeros	Noches	Tipo_hab
06:00	1	2	1	2
	0	1	5	3

En los numerales 4.2.2 hasta el 4.2.5 se presenta toda la información pertinente al Modelamiento y diseño de la base de datos de la aplicación, en concordancia con los requerimientos expuestos por el cliente en las user stories.

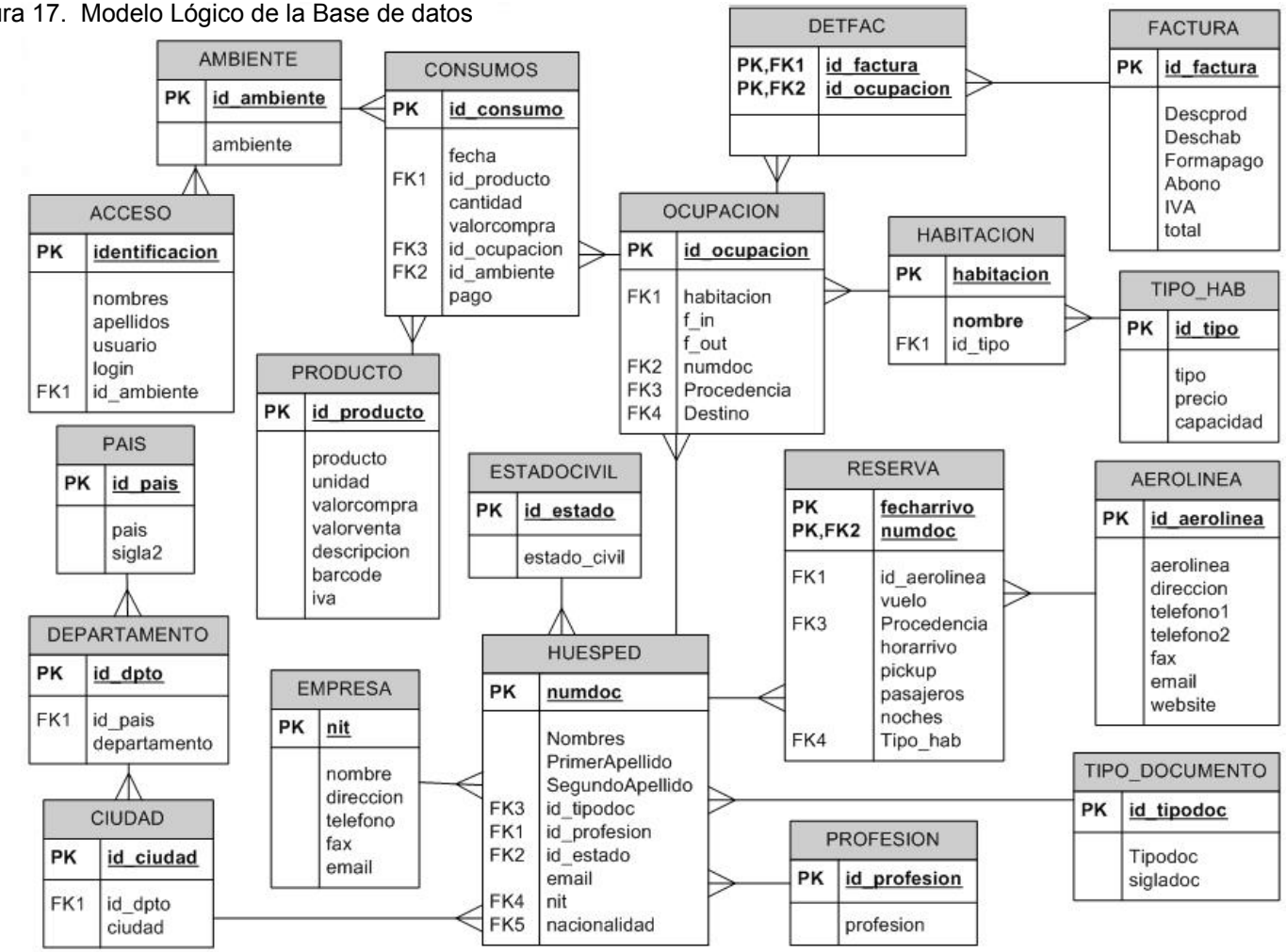
4.2.2 Modelo conceptual de la base de datos

Figura 16. Modelo Conceptual de la Base de datos



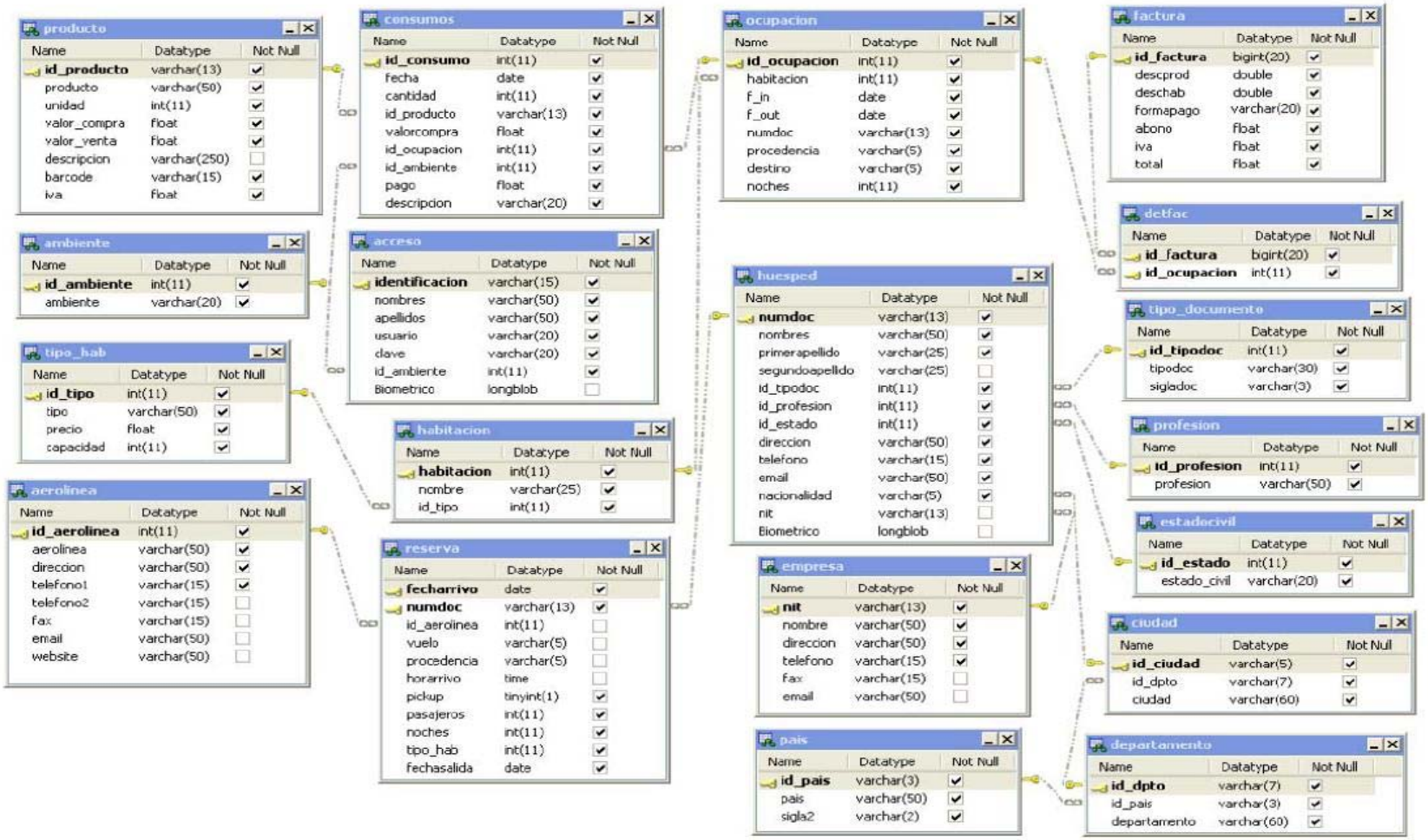
4.2.3 Modelo lógico de la base de datos

Figura 17. Modelo Lógico de la Base de datos



4.2.4 Diseño de la base de datos

Figura 18. Diseño de la Base de datos



4.2.5 Diccionario de datos de la base de datos

Tabla:	Pais							
Descripción:	Almacena El pais							
Atributo	**PK**	**FK**	**DF**	**CK**	**NULL**	**Tipo Dato**	**Long.**	**Observación**
Id_pais	X					Varchar	3	
pais						Varchar	50	
Sigla2						Varchar	2	
Descripción del atributo								
Id_pais	Número de identificación del país de acuerdo ISO3166							
pais	Nombre del país de acuerdo ISO 3166							
Sigla2	Sigla de dos (2) letras del país de acuerdo a ISO3166							

Tabla:	Departamento							
Descripción:	Almacena El departamento, estado o provincia de un país							
Atributo	**PK**	**FK**	**DF**	**CK**	**NULL**	**Tipo Dato**	**Long.**	**Observación**
Id_dpto	X					Varchar	7	
Id_pais		X				Varchar	3	Tabla Pais
Departamento						Varchar	50	
Descripción del atributo								
Id_dpto	Número de identificación del departamento de acuerdo ISO 3166							
Id_pais	Número de identificación del pais de acuerdo ISO 3166							
Departamento	Nombre del departamento de acuerdo ISO 3166							

Tabla:	Ciudad							
Descripción:	Almacena La ciudad de un país							
Atributo	**PK**	**FK**	**DF**	**CK**	**NULL**	**Tipo Dato**	**Long.**	**Observación**
Id_ciudad	X					Varchar	5	
Id_dpto		X				Varchar	7	Tabla Departamento
Ciudad						Varchar	60	
Descripción del atributo								
Id_ciudad	Número de identificación de la ciudad de acuerdo DAS							
Id_dpto	Número de identificación del departamento de acuerdo ISO 3166							
ciudad	Nombre de la ciudad de acuerdo DAS							

Tabla:	Ambiente							
Descripción:	Almacena los tipos de ambiente en que está distribuido el hotel							
Atributo	**PK**	**FK**	**DF**	**CK**	**NULL**	**Tipo Dato**	**Long.**	**Observación**
Id_ambiente	X					Int		Auto numérico
ambiente						Varchar	20	
Descripción del atributo								
Id_ambiente	Número de identificación del ambiente							
ambiente	Nombre del ambiente							

Tabla:	Empresa							
Descripción:	Almacena la información respecto a la empresa donde trabajan los huéspedes							
Atributo	**PK**	**FK**	**DF**	**CK**	**NULL**	**Tipo Dato**	**Long.**	**Observación**
Nit	X					Varchar	13	
Nombre						Varchar	50	
Direccion						Varchar	50	
Telefono						Int	10	(XXX)XXXXXXX
Fax					X	Int	10	(XXX)XXXXXXX
Email					X	Varchar	50	
Descripción del atributo								
Nit	Número de identificación Tributaria de la empresa							
Nombre	Nombre o razón social de la empresa							
Direccion	Dirección de correspondencia de la empresa							
Telefono	Teléfono de contacto de la empresa							
Fax	Fax de contacto de la empresa							
Email	e-mail de contacto de la empresa							

Tabla:	Estadocivil							
Descripción:	Almacena los distintos tipos de estado civil aceptados en Colombia							
Atributo	**PK**	**FK**	**DF**	**CK**	**NULL**	**Tipo Dato**	**Long.**	**Observación**
Id_estado	X					Int		Auto numérico
Estado_civil						Varchar	20	
Descripción del atributo								
Id_estado	Número de identificación del estado civil							
Estado_civil	Nombre del estado civil							

Tabla:	Profesion							
Descripción:	Almacena los distintos tipos de profesiones CIIU							
Atributo	**PK**	**FK**	**DF**	**CK**	**NULL**	**Tipo Dato**	**Long.**	**Observación**
Id_profesion	X					Int	5	
Profesion						Varchar	50	
Descripción del atributo								
Id_profesion	Número de identificación de la profesión del huésped de acuerdo a CIIU							
Profesion	Nombre de la profesión del huésped de acuerdo a CIUU							

Tabla:	Tipo_documento							
Descripción:	Almacena los tipos de documentos de identificación aceptados en Colombia							
Atributo	**PK**	**FK**	**DF**	**CK**	**NULL**	**Tipo Dato**	**Long.**	**Observación**
Id_tipodoc	X					Int		Auto numérico
Tipodoc						Varchar	20	
Sigladoc						Varchar	3	
Descripción del atributo								
Id_tipodoc	Número de identificación del tipo de documento							
Tipodoc	Nombre del tipo de documento							
Sigladoc	Sigla del tipo de documento							

Tabla:	Aerolinea							
Descripción:	Almacena el tipo de habitaciones							
Atributo	**PK**	**FK**	**DF**	**CK**	**NULL**	**Tipo Dato**	**Long.**	**Observación**
Id_aerolinea	X					Int		Auto numérico
Aerolínea						Varchar	50	
Direccion						Varchar	50	
Telefono1						Int	10	(XXX)XXXXXXX
Telefono2					X	Int	10	(XXX)XXXXXXX
Fax					X	Int	10	(XXX)XXXXXXX
Email					X	Varchar	50	
Website					X	Varchar	50	
Descripción del atributo								
Id_aerolinea	Número de identificación de la aerolínea							
Aerolínea	Nombre de la aerolínea							
Direccion	Dirección de la aerolínea							
Telefono1	Teléfono principal de la aerolínea							
Telefono2	Teléfono opcional de la aerolínea							
Fax	Fax de la aerolínea							
Email	e-mail de la aerolínea							
Website	Website de la aerolínea							

Tabla:	Tipo_hab							
Descripción:	Almacena el tipo de habitaciones							
Atributo	**PK**	**FK**	**DF**	**CK**	**NULL**	**Tipo Dato**	**Long.**	**Observación**
Id_tipo	X					Int		Auto numérico
Tipo						Varchar	50	
Precio				X		Double	10,2	Precio > 0
Capacidad				X		Int	2	Capacidad > 0
Descripción del atributo								
Id_tipo	Número de identificación del tipo de habitación							
Tipo	Nombre del tipo de habitación							
Precio	Precio de la noche en el tipo de habitación							
Capacidad	Capacidad máxima de huéspedes por habitación							

Tabla:	factura							
Descripción:	Almacena la información de la factura							
Atributo	**PK**	**FK**	**DF**	**CK**	**NULL**	**Tipo Dato**	**Long.**	**Observación**
Id_factura	X					Int		Auto numérico
Descprod			X			Double	2,2	Cero (0)
Deschab			X			Double	2,2	Cero (0)
Formapago						Varchar	20	
Abono			X			Double	10,2	Cero (0)
IVA						Double	10,2	Iva > 0
Total						Double	10,2	Total > 0

Descripción del atributo	
Id_factura	Número de identificación de la factura
Descprod	Descuento en el precio de los productos
Deschab	Descuento en el precio de la habitación
Formapago	Forma en que cancelará la habitación
Abono	Monto que abono al pago de la cuenta
IVA	Monto del IVA que debe cancelar
Total	Monto total a cancelar por el cliente

Tabla:	Producto							
Descripción:	Almacena la información respecto a los productos ofrecidos							
Atributo	**PK**	**FK**	**DF**	**CK**	**NULL**	**Tipo Dato**	**Long.**	**Observación**
Id_producto	X					Varchar	13	
Producto						Varchar	50	
Id_unidad		X				Int		Tabla Unidad
Valorcompra				X		Double	10,2	Cero (0)
Valorventa				X		Double	10,2	Cero (0)
Descripcion					X	Varchar	250	
IVA						Double	2,2	
Barcode						Varchar	15	
Descripción del atributo								
Id_producto	Número de identificación asignado al producto							
Producto	Nombre del producto							
Id_unidad	Unidad de medida del producto							
Valorcompra	Valor de compra del producto							
Valorventa	Valor de venta del producto							
Descripción	Breve descripción del producto							
IVA	Valor del iva que se le aplica al producto							
Barcode	Código de barras EAN-13 del producto							

Tabla:	Acceso							
Descripción:	Almacena los usuarios que tienen permisos en la base de datos							
Atributo	**PK**	**FK**	**U**	**CK**	**NULL**	**Tipo Dato**	**Long.**	**Observación**
Identificación	X					Varchar	15	
Nombres						Varchar	50	
Apellidos						Varchar	50	
Usuario			X			Varchar	20	
clave						Varchar	20	
Ambiente		X				Int		Tabla Ambiente
Biometrico					X	BLOB		
Descripción del atributo								
Identificación	Número del documento de identidad del empleado							
Nombres	Nombre(s) completo(s) del empleado							
Apellidos	Apellido(s) completo(s) del empleado							
Usuario	Usuario asignado al empleado							
clave	Clave asignada al empleado							
Ambiente	Rol asignado al empleado							
Biometrico	Plantilla Biométrica							

Tabla:	Habitacion							
Descripción:	Almacena las habitaciones que tiene el hotel							
Atributo	**PK**	**FK**	**DF**	**CK**	**NULL**	**Tipo Dato**	**Long.**	**Observación**
Habitación	X					Int		
Nombre						Varchar	20	
Id_tipo		X				Int		Tabla Tipo_hab
Descripción del atributo								
Habitación	Número de identificación de la habitación							
Nombre	Nombre de la habitación							
Id_tipo	Identificación del tipo de habitación que es							

Tabla:	huésped							
Descripción:	Almacena la información respecto al huésped que nos visita							
Atributo	**PK**	**FK**	**DF**	**CK**	**NULL**	**Tipo Dato**	**Long.**	**Observación**
Numdoc	X					Varchar	13	
Nombres						Varchar	50	
Primerapellido						Varchar	25	
Segundoapellido					X	Varchar	25	
Id_tipodoc		X				Int		Tabla Tipo_documento
Id_profesion		X				Int	5	Tabla profesion
Id_estado		X				Int		Tabla estado_civil
Direccion						Varchar	50	
Telefono						Int	10	(XXX)XXXXXXX
Email						Varchar	50	
Nit		X			X	Varchar	13	Tabla empresa
nacionalidad		X				Varchar	5	Tabla ciudad
Biometrico					X	BLOB		
Descripción del atributo								
Numdoc	Número del documento de identificación del huésped							
Nombres	Nombres completos del cliente (de acuerdo al documento de identidad)							
Primerapellido	Primer apellido del cliente (de acuerdo al documento de identidad)							
Segundoapellido	Segundo apellido del cliente (de acuerdo al documento de identidad)							
Id_tipodoc	Identificación del tipo de documento usado por el huésped							
Id_profesion	Identificación de la profesión que ejerce el huésped							
Id_estado	Identificación del estado civil del huésped							
Direccion	Dirección de contacto del huésped							
Telefono	Teléfono de contacto del huésped							
Email	e-mail de contacto del cliente							
Nit	Número de identificación de la empresa donde trabaja el cliente							
nacionalidad	Identificación de la ciudad de expedición documento de identificación							
Biométrico	Plantilla biométrica							

Tabla:	ocupacion							
Descripción:	Almacena la información de la ocupación del hotel por parte de los huéspedes							
Atributo	**PK**	**FK**	**DF**	**CK**	**NULL**	**Tipo Dato**	**Long.**	**Observación**
Id_ocupacion	X					Int		Auto numérico
Habitacion		X				Int		Tabla habtiacion
F_in						Date		(MM-DD-AAAA)
F_out						Date		(MM-DD-AAAA)
Numdoc		X				Varchar	13	Tabla huésped
Procedencia						Varchar	5	Tabla ciudad
Destino						Varchar	5	Tabla ciudad
Descripción del atributo								
Id_ocupacion	Número de identificación de la aerolínea							
Habitación	Nombre de la aerolínea							
F_in	Dirección de la aerolínea							
F_out	Teléfono principal de la aerolínea							
Numdoc	Fax de la aerolínea							
Procedencia	Ciudad de procedencia al llegar al hotel							
Destino	Ciudad de destino al salir del hotel							

Tabla:	Consumo							
Descripción:	Almacena la información respecto a los consumos del huésped							
Atributo	**PK**	**FK**	**DF**	**CK**	**NULL**	**Tipo Dato**	**Long.**	**Observación**
Id_consumo	X					Int		Auto numérico
Fecha			X			Date		(DD-MM-YYYY) now()
Id_producto		X				Varchar	13	Tabla Producto
Cantidad			X			Int	3	Uno (1)
Valorcompra						Double	10,2	valorcompra > 0
Id_ocupacion						Int		
Id_ambiente		X				Int		Tabla Ambiente
Pago						Double	10,2	Pago > 0
Descripción					X	Varchar	50	
Descripción del atributo								
Id_consumo	Número de identificación del consumo							
Fecha	Fecha en que se realizó el consumo							
Id_producto	Identificación del producto que consumió							
Cantidad	Cantidad de unidades que consumió del producto							
Valorcompra	Valor de venta del producto							
Id_ocupacion	Identificación del huésped que consumió el producto							
Id_categoria	Identificación del ambiente donde consumió el producto							
Pago	Valor total del consumo							
Descripción	Datos adicionales del consumo cuando aplique							

Tabla:	Reserva							
Descripción:	Almacena los datos de las reservas hechas por los clientes							
Atributo	**PK**	**FK**	**DF**	**CK**	**NULL**	**Tipo Dato**	**Long.**	**Observación**
Fecharrivo	X					Date		MM-DD-YYYY
Numdoc	X					Varchar	15	
Id_aerolinea		X			X	Int		Tabla aerolínea
Procedencia					X	Varchar	5	Tabla ciudad
Vuelo					X	Varchar	5	
Horarrivo					X	Date		HH:MM
Pickup						Bolean		
Pasajeros			X			Int		Uno (1)
Noches			X			Int		Uno (1)
Tipo_hab						Int		Tabla tipo_hab
Descripción del atributo								
Fecharrivo	Fecha en que llegará al hotel							
Numdoc	Número del documento de identificación del cliente							
Id_aerolinea	Identificación de la aerolínea por la que tiene el vuelo de arribo							
Procedencia	Ciudad de la que viene el vuelo							
Vuelo	Número de identificación del vuelo							
Horaarrivo	Hora en que llega el vuelo según itinerario							
Pickup	Si el huésped desea ser recogido en el aeropuerto							
Pasajeros	Número de personas que llegan incluyendo a quien hace la reserva							
Noches	Número de noches que esperan quedarse en el hotel							
Tipo_hab	El tipo de habitación sobre la que quiere hacer la reserva							

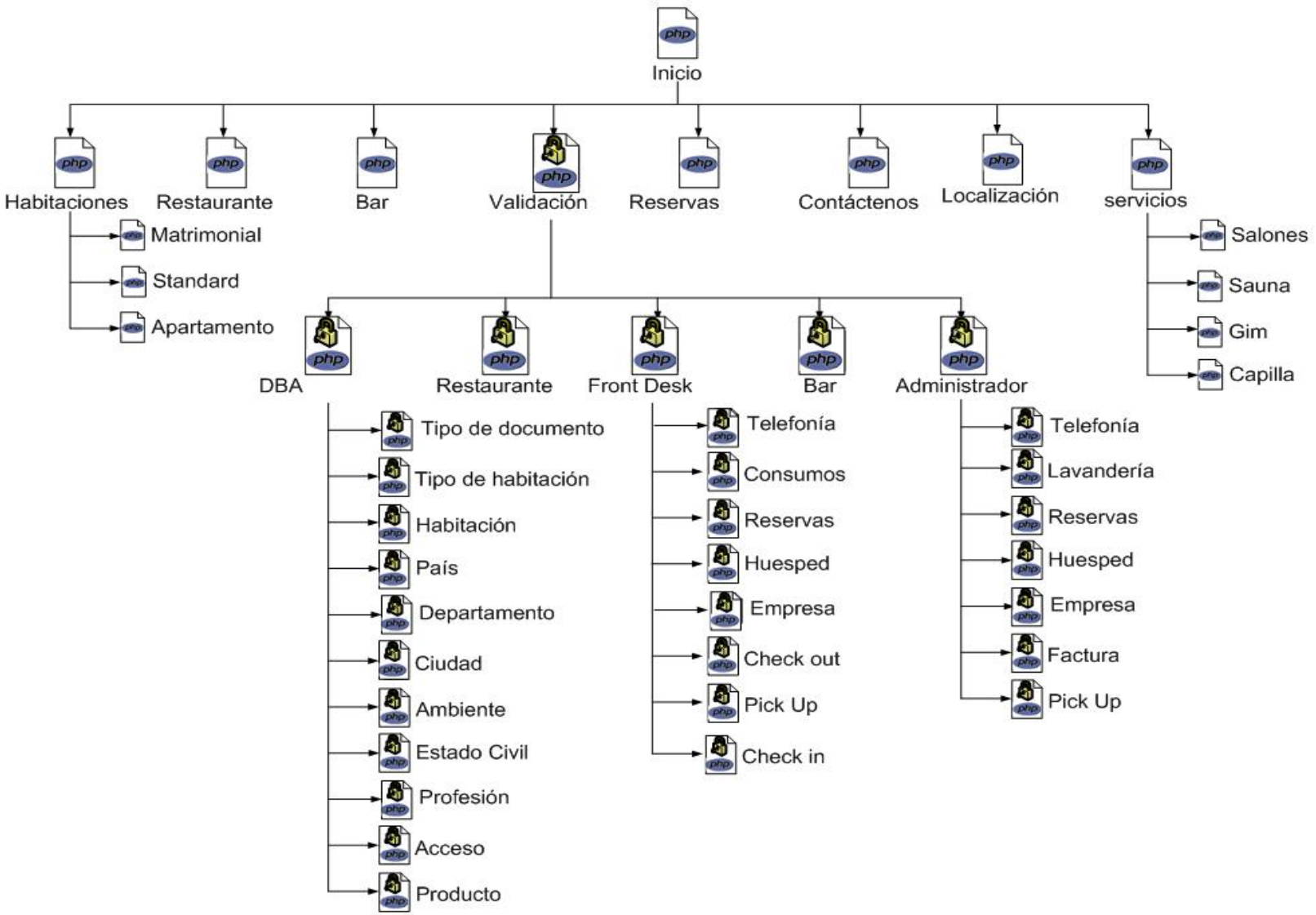
Tabla:	Detallefac							
Descripción:	Almacena la información que relaciona los detalles de las facturas							
Atributo	**PK**	**FK**	**DF**	**CK**	**NULL**	**Tipo Dato**	**Long.**	**Observación**
Id_factura	X	X				Int		Tabla Factura
Id_ocupacion	X	X				Int		Tabla Ocupacion
Descripción del atributo								
Id_factura	Número de identificación de la factura							
Id_ocupacion	Número de identificación de la ocupación de un huésped							

4.2.6 Mapa de navegación. La aplicación está dividida en dos partes principales que son:

- La publicidad y comercialización, donde se presentan los servicios del hotel y se permite que el huésped realice su reserva, esta parte no requiere de ninguna validación.

- La segunda parte está desarrollada para el uso interno del hotel y en ella se realizan todas las operaciones o transacciones contempladas en esta aplicación, para acceder a ella se requiere de la validación del usuario.

Figura 19. Mapa de navegación



4.3 PRUEBAS

Considerando los requerimientos de la aplicación y mediante el uso de herramientas de software como Risk Radar ®[3] y Threat Analysis and Modeling[4], se lograron identificar y hacer seguimiento a los siguientes riesgos y posibles ataques.

Riesgos

- Confidencialidad: Acceso No autorizado a la información
- Integridad: Ejecución ilegal de la aplicación
- Disponibilidad: Ejecución no efectiva de la aplicación por el personal autorizado

Ataques

- Ataque criptoanálisis: ataque que busca el reconocimiento de la información cifrada.
- Denegación de servicios: ataque que busca la degradación en el rendimiento de un sistema remoto y, eventualmente, su caída.
- Forzar el browser: ataque que busca acceder a una página restringida digitando directamente su URL.
- Ataque formato string: función comúnmente usada para la salida de datos con la familia de funciones printf que el programador llama la función sin especificar un formato string.
- Ataque de respuesta HTTP: el atacante captura la cookie de autenticación del usuario, usando software de monitoreo.
- Ataque de overflow / underflow: ataques que busca reescribir o permitir la ejecución de código arbitrario y potencialmente dañino. Underflows de enteros puede causar la denegación de servicios.
- Ataque de hombre en el medio: interceptación de mensajes entre el emisor y receptor.
- Ataque un-click: ataque que busca que el navegante de click en un link o ventana emergente que redirige la navegación a una página montada por el atacante.
- Fuerza bruta contra password: cuando se usan procesos automáticos de prueba y error para que un usuario no válido presente credenciales válidas de manera exitosa.

[3] Base de datos de administración de riesgos disponible en: < http://www.iceincusa.com/16CSP/content/software/tools/r_radar/risk_rad.htm> visitada 20 de Marzo de 2005 23:00

[4] Aplicación de Modelamiento de riesgos desarrollada por Microsoft disponible en: < http://msdn2.microsoft.com/es-ar/security/aa570412.aspx> visitada 25 de Agosto de 2006 20:45

- Ataque de repudiación: acción legítima o de otro tipo que busca de manera específica denegar una acción o transacción.
- Robo de sesiones: Es el acto de tomar el control de una sesión de un usuario, mientras el usuario legítimo está usando la aplicación con una sesión abierta.
- Inyecciones SQL: ataque que explota las vulnerabilidades de validaciones de entrada para correr comandos arbitrarios en la base de datos.

Por lo anterior se establecieron y se probaron las siguientes contramedidas, para minimizar, eliminar y/o transferir los riesgos y ataques identificados.

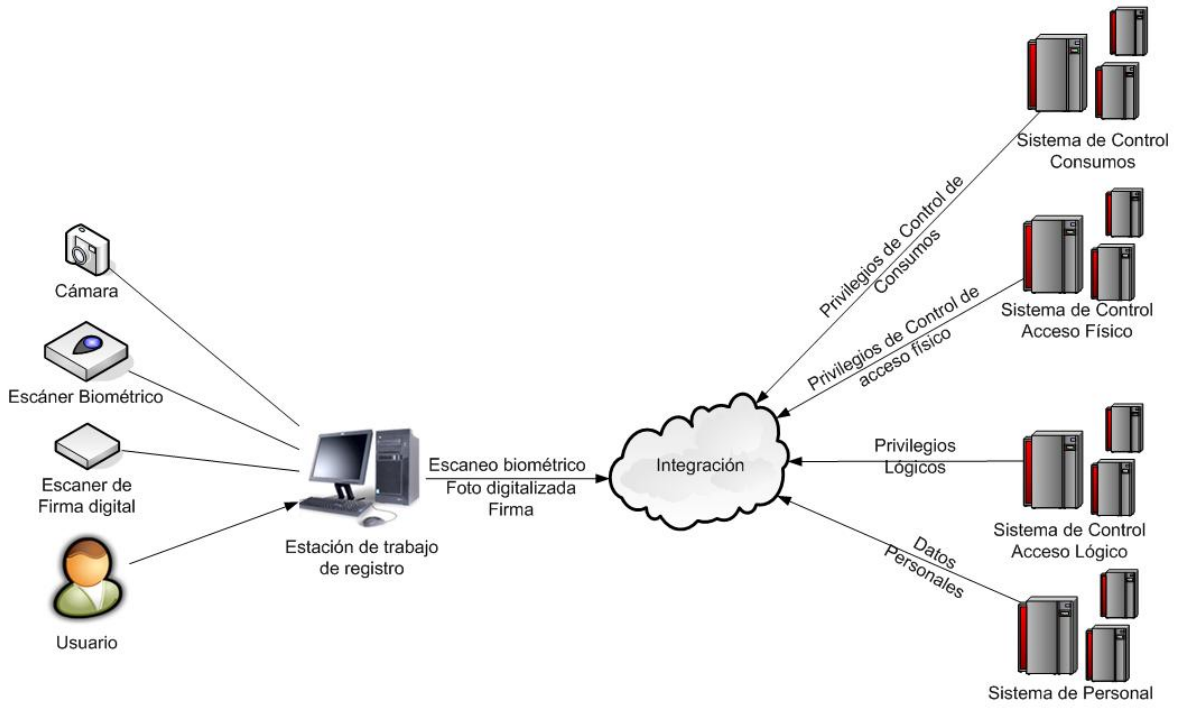
Contramedidas

- Usar crypto bien conocida
- Usar claves largas
- Asegurar almacenamiento de claves
- Guardar claves fuera del dominio de la aplicación
- Forzar requerimiento límite de tamaño
- Mostrar mensajes de error genéricos
- Implementar verificación para overflow / underflow
- Usar un canal de comunicación segura
- Autenticar al cliente y al servidor
- Forzar la complejidad de la clave
- Implementar políticas de bloqueo de cuentas
- Usar enunciados SQL parametrizados

4.4 ARQUITECTURA DE RED

El siguiente diagrama es un ejemplo conceptual de la arquitectura de la red que se requiere implementar para usar la aplicación, la existencia o no de ciertos componentes de la red, dependen de las necesidades específicas del usuario (ver Figura 20. Ejemplo conceptual de arquitectura de red, página 75).

Figura 20. Ejemplo conceptual de arquitectura de red



En la red se destaca la existencia al menos una estación de trabajo donde se registra el usuario con la(s) tecnología(s) que se haya(n) seleccionado de acuerdo al estudio de requerimientos, esta información se comparte entre los distintos sistemas y/o aplicaciones que la puedan requerir.

Los puertos usados para las tecnologías biometricas estan definidos dentro de los puertos registrados y solo estan establecidos dos hasta ahora ello son:

- Finger Image transfer protocol (fpitp) en el puerto 1045/ tcp y udp

- Biometrics server (bioserver) en el puerto 6946/ tcp y udp

Para las otras tecnologías no hay puertos establecidos, ellos usan tecnología TTL (Lógica Transistor-Transistor) y actualmente se pueden conectar mediante conectores RJ45, RS232, RS485, USB y PS/2.

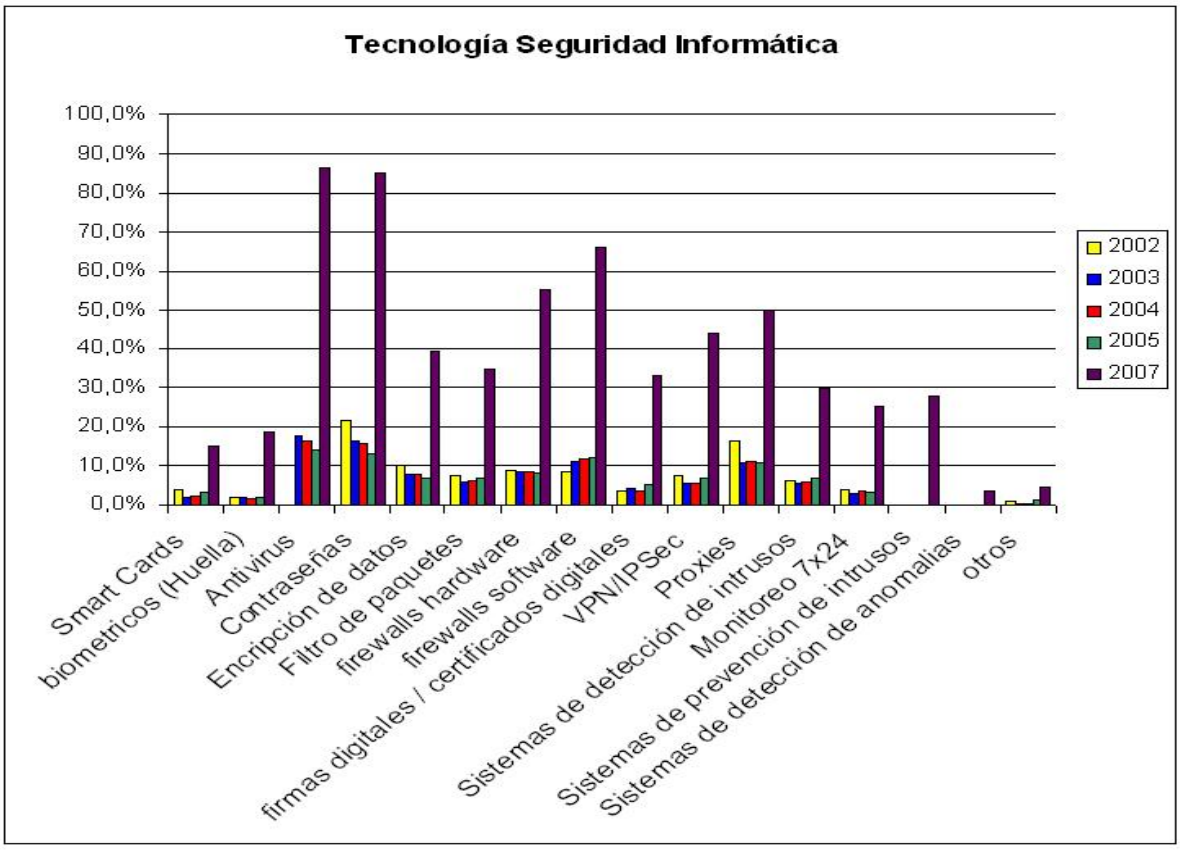
5 PRESENTACIÓN Y ANÁLISIS DE RESULTADOS

5.1 ESTADÍSTICAS

Al igual que en el resto del mundo, Colombia tampoco cuenta con estadísticas claras, precisas y confiables que muestren de manera certera la tendencia en el uso de tecnologías de autenticación, ni las consecuencias que esto genera, como lo refleja las siguientes estadisticas (únicas que existen en Colombia) sobre el uso de tecnologías de autenticación y que fueron generadas por la Asociación Colombiana de Ingenieros de Sistemas (ver Figura 21 y Figura 22).

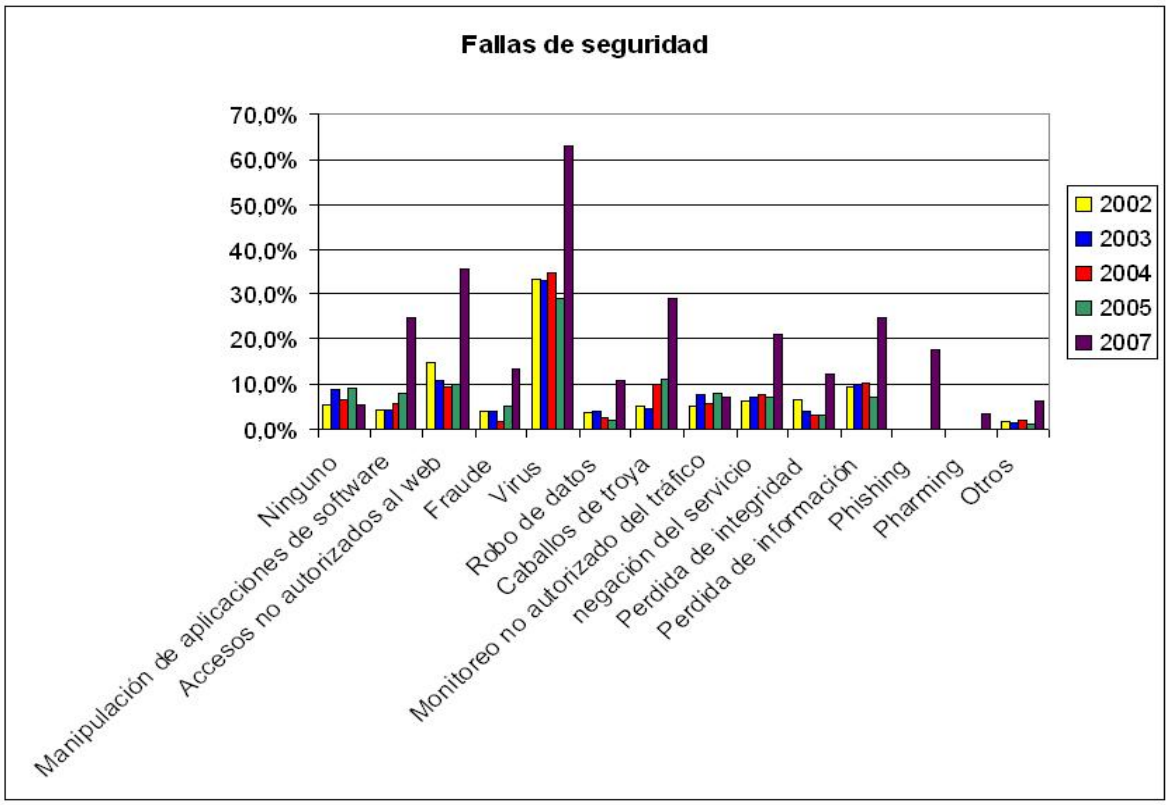
Estas estadísticas se sacan de una población limitada (personas que participan activamente en la lista de seguridad SEGURINFO) y tiene un error muestral estimado del 8%

Figura 21. Mecanismos de seguridad Informática usados en Colombia



Fuente: ACIS, V II Encuesta Nacional de Seguridad Informática

Figura 22. Fallas de seguridad informática en Colombia



Fuente: ACIS, VII Encuesta Nacional de Seguridad Informática

5.2 ESTADO DEL ARTE

Se publicaron fragmentos de la investigación en la página web www.monografias.com así:

- Introducción a los códigos de barras en el link http://www.monografias.com/trabajos42/codigo-de-barras/codigo-de-barras.shtml, publicación realizada el 27 de febrero de 2007 y con 2001 visitas hasta el 27 de agosto de 2007.

- Introducción a la tarjeta con banda magnética en el link http://www.monografias.com/trabajos43/banda-magnetica/banda-magnetica.shtml, publicación realizada el 20 de marzo de 2006 y con 1567 visitas hasta el 27 de agosto de 2007.

- Introducción a la biometría en el link http://www.monografias.com/trabajos43/biometria/biometria.shtml, publicación realizada el 4 de abril de 2007 y con 1896 visitas hasta el 27 de agosto de 2007.

- Introducción a la tarjeta con circuito integrado en el link http://www.monografias.com/trabajos43/tarjeta-circuito-integrado/tarjeta-circuito-integrado.shtml, publicación realizada el 9 de abril de 2007 y con 217 visitas hasta el 27 de agosto de 2007.

Se han recibido consultas de integrantes de la Universidad Industrial de Santander[5] en Bucaramanga, Universidad del Aconcagua en Argentina[6], ITAIPU[7] en Paraguay.

Se han recibido propuestas para realizar publicaciones por parte de la Asociación Argentina de Quimicos Cosméticos[8] en Argentina.

Actualmente hay un interés creciente por implementar sistemas que utilizan tecnologías de autenticación, sin embargo las fuentes de información son limitadas y por lo general se encuentran en otros idiomas diferentes al español, así mismo se observa que pese a que son tecnologías con más de 25 años en el mercado, su difusión y uso es aún desconocido para la mayoría de la población, pese a que utilicen alguna o todas las tecnologías a diario.

5.3 APLICACIÓN

La aplicación fue validada en hojas de estilo en cascada (CSS), accesibilidad de contenido (WAI-AA) y en links.

Las tecnologías de autenticación pueden ser aplicadas en cualquier tipo de aplicación o sistema de información, sin que estos tengan relación directa con el control de acceso a dependencias o sistemas de información.

[5] Ingeniero Bernardo Moreno C., e-mail bernardmore@gmail.com, 10 de Marzo de 2007 12:00 y Nicolas Rey e-mail nicrey8@hotmail.com, 16 de Abril de 2007 23:07
[6] Guillermo Quiroga, e-mail Guillermo.quiroga@hotmail.com, 27 de Agosto de 2007 15:08
[7] Licenciada Ada Benitez, e-mail adabenitez@gmail.com, 05 de Junio de 2007 13:53
[8] Daniel Inzerrilli, e-mail danielinze@yahoo.com.ar, 08 de Marzo de 2007 12:25

La selección de una u otra tecnología, para ser usada en una aplicación o sistema depende de las necesidades puntuales y aceptación del usuario final más que de las tendencias que pretenden imponer los desarrolladores o empresas que comercializan estos tipos de sistemas.

Para determinar de manera objetiva y precisa la tecnología, se debe realizar un levantamiento de información adecuado donde se establezca el motivo real por el cual se desea implementar este tipo de tecnologías y donde se informe al cliente las implicaciones que tiene en cuanto a la modificación en manuales de funciones, procedimientos e incluso cambios arquitectónicos para que la implantación del sistema cumpla con los objetivos para el cual fue planeado.

6 CONCLUSIONES

Las cuatro tecnologías estudiadas son viables a corto y mediano plazo, aunque a largo plazo algunas de ellas van a perder presencia comercial, como es el caso de la banda magnética en las entidades financieras, donde se está estudiando la posibilidad de reemplazarla con alguna de las otras tecnologías y el código de barras que ya está siendo remplazando por el código de producto electrónico (ePC), para facilitar el rastreo de los productos y reducir el uso de códigos en la identificación de estos a lo largo de la cadena de distribución.

Actualmente la industria está utilizando las tecnologías de autenticación como herramientas para identificar a las personas, en algunos casos para garantizar la identidad de sus empleados y en otras para reducir costos y dar un mejor servicio, es así como las grandes cadenas hoteleras ya han remplazado las llaves tradicionales por tarjetas RFID o con banda magnética para acceder a las habitaciones.

Aunque algunos autores sugieren o prevén que a mediano plazo algunas tecnologías (La tarjeta con banda magnética y el código de barras) tienen su vida útil contada, es claro que cada una de ellas ha ganado espacio en áreas específicas de la industria y aunque algunas efectivamente van a perder protagonismo, es poco probable que desaparezcan, porque incluso la brecha tecnológica que existe entre los países hace poco probable que esto suceda.

Para la implementación de las tecnologías de autenticación se requiere un estudio previo y particular de en donde y para que se va a implementar, porque no hay una solución absoluta para cada industria.

La implementación de alguna(s) de las tecnologías de autenticación implica el cambio de algunos procesos y en consecuencia se requiere modificar o elaborar nuevamente al menos los manuales de funciones y procedimientos de la entidad donde se usen éstas tecnologías.

En Colombia hay una falencia manifiesta en la regularización de este tipo de tecnologías, generando un conflicto entre abogados y desarrolladores, comerciantes y usuarios de estas técnologías, por lo que en algunos casos se ha

visto frenado el uso y desarrollo de estas tecnologías, ante el temor de estar violando los derechos humanos en algún modo.

En caso de utilizarse tecnologías de autenticación para el control de acceso, la selección debe estar sujeta a las recomendaciones que se obtengan del estudio de seguridad realizado a la entidad, por parte de un experto en seguridad, no solo física, sino también electrónica, de sistemas e industrial.

7 RECOMENDACIONES

7.1 RECOMENDACIONES EN EL ÁMBITO ACADÉMICO Y GUBERNAMENTAL

Considerando que las tecnologías de identificación en general tienen más de 25 años en el mercado, que su uso se ha masificado y está garantizado a corto, mediano y largo plazo, así mismo que fuera de Colombia ya existen gran cantidad de instituciones académicas y científicas que se están ocupando de estandarizar y realizar investigaciones sobre estas tecnologías, se debería plantear la necesidad de empezar a crear programas que satisfagan estos requerimientos en el ámbito nacional y que de esta manera Colombia no tenga que depender de organizaciones y/o empresas supranacionales o internacionales; se podría seguir el ejemplo de la Unión Europea que aunque reconoce la ventaja que le lleva Estados Unidos en la investigación y estandarización de estas tecnologías, ya ha generado directivas para convertirse en potencia por encima de Estados Unidos en un plazo no superior a diez (10) años.

7.2 RECOMENDACIONES PARA USUARIOS

En el desarrollo de aplicaciones y/o sistemas de información que interactúan con tecnologías de autenticación se recomienda que quienes vayan a hacer uso de estos recursos, realicen un estudio previo de la industria en que se encuentran, para saber cuál de la cuatro tecnologías es la más utilizada y/o se proyecta estandarizar, para implementarla.

En el caso de que se desee utilizar tecnología de autenticación para el control de personal, se recomienda usar más de una tecnología, de manera que en caso de que falle una se tenga la opción de utilizar la otra, así mismo se debe tener en cuenta los requerimientos jurídicos que implica el uso de la tecnología seleccionada, así como su aceptación entre los usuarios.

En el desarrollo de aplicaciones WML, se recomienda complementar con el uso de códigos de barras como beetag o shotcode, teniendo en cuenta que mediante la descarga de una aplicación gratuita en el dispositivo movil que tenga cámara fotográfica y acceso a Internet, se pude acceder más fácilmente a la página, al

tener tan solo que fotografiar el código y accederá al sitio sin necesidad de digitar la dirección.

7.3 RECOMENDACIONES PARA LA APLICACIÓN DEL HOTEL

Se podría desarrollar la página WML para el hotel en el que el usuario pueda realizar y consultar sus reservas, así como las ofertas ofrecidas por el mismo, esta aplicación debería contar ademas con un código de barras, para facilitar su acceso y que se puede agregar en la artes impresas del hotel.

Se podría desarrollar una aplicación para moviles que permita realizar la toma de pedidos en los distintos ambientes del hotel y para validar al huesped usar entonces la huella digital o la firma; así mismo otra aplicación que permita al conductor que recoge a los huéspedes en el aeropuerto consultar la información sobre los pasajeros que arriban.

BIBLIOGRAFÍA

BAGULEY, Philip. Como Gestionar Proyectos con éxito. España: Ediciones FOLIO, 1996. 251p.

BRAVO GARCIA, Ginés, GUTIERREZ RODRÍGUEZ, Abraham. PHP 5 a través de ejemplos. Madrid: Alfaomega, 2007. 552p.

CAMACHO ALVAREZ, Tobías Mauricio, CAMACHO LEGUIZAMON, Luís Fernando, MONROY CORREA, Henry. Adopción de la Tecnología de Código de Barras en el Carné de los Empleados de la USB Para El Registro y Control de Las Jornadas Laborales. 2000. Monografía.

DAZA ROJAS, Néstor Guillermo. Inteligencia Básica I. Cartagena: ENAP, 1994. 95p.

FAIRLEY, Richard. Ingeniería de Software. México: Editorial Mc Graw Hill, 1992. 390p.

FREUND, John E., SIMON, Gary A. Estadística Elemental. Octava Edición. México: Prentice Hall Hispanoamericana, S.A.2002. 566p.

INSTITUTO COLOMBIANO DE NORMAS TÈCNICAS. Normas Colombianas para la presentación de Tesis, trabahos de grado y otros trabajos de investigación. Segunda Actualización. Bogota D.C.: ICONTEC, 2004. 126p NTC 1486.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Norma Técnica Colombiana NTC-ISO 9000. Bogotá D.C.: ICONTEC, 2000. 42p.

JAN, Axelson. Serial Port Complete: programming and circuits for RS-232 and RS-485 links and networks. Madison, Wisconsin, USA: Lakeview Research, 2000.

JIMENEZ LOZANO, Álvaro. Código Nacional de Recursos Naturales Renovables y de Protección al Medio Ambiente. Colombia: Ediciones ECOE, 2004. 102p.

MORENO GUAUTA, Julie Stephani. Diseño de un software para el registro de personal activo de la USB seccional Bogotá.2003. Monografía.

MOSCOSO MONTAÑO, Jairo Alexander, ZORA HERNANDEZ, Faiber Alexander. Sistema de pago electrónico a través de Internet usando tarjetas inteligentes. 2001. monografía

OLARTE MEDINA, Julieth. Software de Registro para Estudiantes y Visitantes, 2001. Monografía.

POWELL, Thomas A. HTML 4 Manual de referencia. Primera Edición. España: Mc Graw Hill, 2001. 1157p.

RAMIREZ ROJAS, Luís Eduardo, ZAMBRANO MARQUEZ, Deider. Prototipo de un sistema de control de acceso de personal mediante el uso de tarjetas inteligentes de tecnología RFID. 2004. monografía.

SALAMANCA ALVAREZ, Manuel Mauricio, SANCHEZ SAAVEDRA, Victoria Alexandra, SANCHEZ BERNAL, Omar. Implementación de la tarjeta inteligente universitaria –TIU- .2000. Monografía.

SANDOVAL, Juan Domingo, BRITO, Ricardo, MAYOR, Juan Carlos. Tarjetas Inteligentes. España: Editorial Paraninfo, 1999. 212p.

WACKERLY, Dennis, MENDENHALL III, William, L. SCHEAFFER, Richard. Estadística matemática con aplicaciones. Sexta Edición. México: Thomson Editores, S.A., 2002. 853p.

ASOCIACIÓN BANCARIA Y DE ENTIDADES FINANCIERAS DE COLOMBIA. Estándar del código de barras para las facturas recaudadas por el sector financiero colombiano [Disk] ASOBANCARIA 1999. Computer disk; 3 ¼ mm. PDF format

BHATTACHARYYA, Saurav, SRIKANTHAN, T. Sección Dos, Biométricos por voz [DISK]. Nanyang Technological University 2003. Computer disk; 3 ¼ mm. PDF format.

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK. Study : "An investigation into the performance of facial recognition systems relative to their planned use in photo identification documents – BioP I" [DISK]. BSI 2004. Computer disk; 3 ¼ mm. PDF format

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Guía Para la Elaboración de Manuales de Procedimientos [DISK]. Bogotá D.C.: Departamento Administrativo de la Función Pública, 2001. 1 Computer disk; 3 ½ mm. DOC format.

DU, Yingzi, IVES, Robert W., ETTER, Delores M., WELCH, Thad B. Use of one-dimensional iris signatures to rank iris pattern similarities [DISK]. Optical Engineering 2006. Computer disk; 3 ¼ mm. PDF format

ESPINOSA DURÓ, Virginia. Evaluación de Sistemas de Reconocimiento Biométrico [DISK]. Barcelona: Escuela Universitaria Politécnica de Mataro, 2004. Computer disk; 3 ¼ mm. PDF format.

FAA. Guidance package Biometrics for Airport Access Control [DISK]. FAA 2005. Computer disk; 3 ¼ mm. PDF format

GALTON, Francis. Finger Prints [DISK]. Computer disk; 3 ¼ mm. PDF format

GILLELAND, Michael. Anatomy of Credit Card Numbers [DISK]. Merrian Park Software. Computer disk; 3 ¼ mm. PDF format

HOSOM, John-Paul.COLE, Ron, FANTY, Mark. Speech Recognition Using Neural networks at the Center for Spoken Language Understanding. Oregon Graduate Institute of Science and Technology. 1999.

ICAO. Annex I Use of Contactless Integrated Circuits in Machine Readable Travel Documents Version 4.0 [DISK]. ICAO 2004. Computer disk; 3 ¼ mm. PDF format

ICAO. MRTD Report. Volume 1 Number 1. ICAO 2006. Computer disk; 3 ¼ mm. PDF format

KEOGH, Eamonn. The Science of Fingerprints [Disk] Eamonn Keogh 2000 computer disk; 3 ¼ mm. PDF format

LAUFER, Berthold. History of the Finger--Print System. Volume 16 (2) Marzo/Abril 2000, pp 1-13.

MINISTERIO DE DEFENSA NACIONAL. Guía Manual de Procedimientos [DISK]. Bogotá D.C.: MDN, 2001. 1 Computer disk; 3 ½ mm. DOC format.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Recommended Security Controls for Federal Information Systems [DISK] NIST 2006. Computer disk; 3 ¼ mm. PDF format

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL. Biometrics "Foundation Documents" [DISK]. NSTC 2006. Computer disk; 3 ¼ mm. PDF format

ROMO, Marcelo. Boletín 4, Las tecnologías biométricas [DISK]. Ecuador: Universidad Internacional del Ecuador, 2003. Computer disk; 3 ¼ mm. PDF format.

SOFTWARE PROGRAM MANAGERS NETWORK. The program manager's guide to software acquisition best practice VERSION 2.31 [DISK]. Software Program Managers Network 1998. Computer disk; 3 ¼ mm. PDF format

STRANGIO, Christopher E. The RS232 Standard, A Tutorial with Signal Names and Definitions [DISK]. Lexington, Massachusetts: CAMI Research Inc, 2004. 1 Computer disk; 3 ¼ mm. DOC format.

THE BIOAPI CONSORTIUM. BioAPI Specification Version 1.1 [DISK]. The BioAPI Consortium 2001. Computer disk; 3 ¼ mm. PDF format

THE DEPARTMENT OF THE TREASURY. The Use of Technology to Combat Identity Theft. [DISK]. United States: The Department of Treasury, 2005. Computer disk; 3 ¼ mm. PDF format

TIBBO TECHNOLOGY. Tibbo Ethernet-to-Serial Devices: Hardware, Firmware, PC software. Tibbo Technology 2000-2004. Computer disk; 3 ¼ mm. PDF format.

TILTON, Cathy. Biometric Standards - An Overview [DISK]. DAON 2006. Computer disk; 3 ¼ mm. PDF format.

TWAIN, Mark. Life on the Mississippi [DISK]. Computer disk; 3 ¼ mm. PDF format

TWAIN, Mark. The Tragedy of Pudd'nhead Wilson [DISK]. Computer disk; 3 ¼ mm. PDF format

UNISYS. Research Global Study on the Public's Perceptions about Identity Management [DISK]. Unisys 2006. Computer disk; 3 ¼ mm. PDF format

U.S. GENERAL SERVICES ADMINISTRATION. Government smart card handbook. [DISK] GSA 2004. Computer disk; 3 ¼ mm. PDF format.

VILLALBA, Alejandro, ARTACHO, Juan Manuel, SANCHEZ, Diego, BERNUÉS, Emiliano. Autenticuz: Sistema de reconocimiento facial para control de acceso automático [DISK]. Zaragoza: Universidad de Zaragoza, 2004. Computer disk; 3 ¼ mm. PDF format.

VILLALÓN HUERTA, Antonio. El Sistema de Gestión de Seguridad de la Información [DISK] Grupo S2 2004. Computer disk; 3 ¼ mm. PDF format

YUN, Yau Wei. The '123' of Biometric Technology [DISK]. Laboratories for Information Technology Co-Chair, Biometrics Working Group of Security & Privacy Standards Technical Committee 2003. Computer disk; 3 ¼ mm. PDF format.

Disponible en Internet: <http://bellsouthpwp.net/l/a/laurergj/UPC/triviaqu.html> visitada 5 de Diciembre de 2006 23:39

Disponible en Internet: <www.bioapi.org> visitada 15 de Octubre de 2006 02:25

Disponible en Internet: < www.biometricgroup.com > visitada Mayo 20 de 2007 21:35

Disponible en Internet: < http://buscon.rae.es/draeI/> visitada 15 de Octubre de 2006 20:05

Disponible en Internet:
< www.biometrics.dod.mil/SiteComponents/References.aspx > visitada 10 de Octubre de 2006 19:53

Disponible en Internet: < http://www.biometrics.org/REPORTS/HAAPI20/> visitada 10 de Octubre de 2006 00:06

Disponible en Internet: < http://www.biometrics.org/research.htm > visitada 10 de Octubre de 2006 02:40

Disponible en Internet: < http://www.blackhat.com/html/bh-media-archives/bh-archives-2006.html#eu-06 > visitada 12 de Octubre de 2006 17:40

Disponible en Internet: < http://www.bsi.bund.de/index.htm> visitada 12 de Octubre de 2006 18:23

Disponible en Internet:
< http://www.biometricscatalog.org/document_area/default.aspx > visitada 8 de Octubre de 2006 19:22

Disponible en Internet:
<http://www.biometricssystem.com/biometricssysteminformation.php?icerik=Biometrics%20Fingerprint%20Recognition%20identification%20Verification%20Iris%20V

oice%20Face%20Hand%20Dermis%20Skin%20Smartcards%20Integrated%20Algorithms%20security%20technology%20cctv > visitada 8 de Octubre de 2006 14:50

Disponible en Internet:
< http://www.computersecurityfaq.com/security_websites.html> visitada 8 de Enero de 2007 05:30

Disponible en Internet:
< http://criminaljustice.state.ny.us/ojis/history/ph_cntrt.htm > visitada 8 de Diciembre de 2006 06:10

Disponible en Internet:
< http://www.cs.indiana.edu/~zmcmahon/biometrics-history.htm > visitada 8 de Diciembre de 2006 06:15

Disponible en Internet:
<http://www.ctst.com > visitada 8 de Octubre de 2006 21:18

Disponible en Internet: < www.defensetech.org/archives/cat_strategery.html > visitada 19 de Junio de 2007 08:00

Disponible en Internet:
<http://www.dinersclubus.com/dce_content/us/aboutdinersclub/companyhistory> visitada 8 de Julio de 2007 23:40

Disponible en Internet:
< http://www.engr.sjsu.edu/biometrics/publications_tech.html > visitada 8 de Julio de 2006 02:56

Disponible en Internet:
<http://es.wikipedia.org/wiki/Juan_Vucetich > visitada el 2 de Diciembre de 2006 06:00

Disponible en Internet: < http://Europa.eu.int/idabc/en/home > visitada 8 de Octubre de 2006 23:20

Disponible en Internet: <www.eurosmart.com> visitada 10 de Diciembre de 2006 22:08

Disponible en Internet: <www.freepantentsonline.com> visitada 1 de Diciembre de 2006 20:20

Disponible en Internet: < http://www.gaits.com/biometrics_signature.asp > visitada Mayo 20 de 2007 21:40

Disponible en Internet: < http://galton.org/books/finger-prints/ > visitada 16 de Junio de 2007 15:43

Disponible en Internet:
< http://www.geradts.com/anil/ij/vol_002_no_002/reviews/pb/page002.html > visitada 10 de Junio de 2007 12:21

Disponible en Internet: <www.gs1.org> visitada 1 de Noviembre de 2006 19:00

Disponible en Internet: <www.hardwarebook.net/cable/index.html> visitada 8 de Septiembre de 2006 18:30

Disponible en Internet: <www.hess-cr.com > visitada 3 de Septiembre de 2007 00:30

Disponible en Internet: <http://home3.americanexpress.com/corp/os/history.asp > visitada 8 de Julio de 2007 00:50

Disponible en Internet: <www.iaccolombia.org> visitada 5 de Diciembre de 2006 13:40

Disponible en Internet: <www.ibia.org> visitada 15 de Septiembre de 2006 19:21

Disponible en Internet: <http://www.icma.com/info/standards.htm> visitada 05 de Diciembre de 2006 07:15

Disponible en Internet: < http://www.identicard.com/news/index.htm > visitada 25 de Septiembre de 2006 17:30

Disponible en Internet: < http://www.identix.com/trends/standards.html > visitada 25 de Septiembre de 2006 18:10

Disponible en Internet: < http://www.idteck.com/technology/rfid.jsp > visitada 27 de Septiembre de 2006 20:26

Disponible en Internet: < http://www.idteck.com/technology/biometrics.jsp> visitada 27 de Septiembre de 2006 23:10

Disponible en Internet: < http://www.idtecktraining.com/index.asp> visitada 27 de Septiembre de 2006 23:20

Disponible en Internet: < http://www.idwholesaler.com/resources/technology.htm > visitada 15 de Marzo de 2007 00:54

Disponible en Internet: <http://www.iee.org/OnComms/Sector/Computing/Article_Display.cfm?ObjectID=BD50EE45-842E-4DB8-ABB84E72AFB45F14> visitada 20 de Diciembre de 2006 19:35

Disponible en Internet: < http://www.iriscan.com> visitada 26 de Noviembre de 2006 16:05

Disponible en Internet: < http://www.iscan.ca> visitada 27 de Septiembre de 2006 19:25

Disponible en Internet: < http://www.janes.com/transport/news/jar/jar030604_1_n.shtml > visitada 15 de Agosto de 2004 18:40

Disponible en Internet:
<http://www.janes.com/transport/news/jar/jar040922_1_n.shtml> visitada 10 de Enero de 2005 12:30

Disponible en Internet:
<http://www.kalysis.com/content/modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=5 > visitada 27 de Agosto de 2006 21:20

Disponible en Internet:
< http://www.magneprint.com/information/what_is_magneprint.asp > visitada 4 de Mayo de 2007 23:38

Disponible en Internet: < http://members.aol.com/SVG2254/West.htm > visitada 27 de Diciembre de 2006 14:20

Disponible en Internet: <www.municode.com> visitada 27 de Agosto de 2006 19:50

Disponible en Internet: <www.national.com> visitada 27 de Agosto de 2006 20:30

Disponible en Internet: < http://www.nist.gov/dads/ > visitada 20 de Agosto de 2006 21:45

Disponible en Internet:
< http://www.nlm.nih.gov/visibleproofs/galleries/cases/vucetich.html > visitada 20 de Diciembre de 2006 21:54

Disponible en Internet:
< http://www.nlm.nih.gov/visibleproofs/galleries/cases/vucetich.html > visitada 20 de Diciembre de 2006 23:45

Disponible en Internet: < http://perso.orange.fr/fingerchip/index.htm> visitada 10 de Diciembre de 2006 11:45

Disponible en Internet: < http://www.recoware.hu/angdata/histor.html > visitada 08 de Junio de 2007 19:30

Disponible en Internet:
< http://www.redwop.com/minutiae.asp?action=showArticle&ID=359 > visitada 16 de Junio de 2007 15:38

Disponible en Internet: <http://www.scafo.org> visitada 10 de Diciembre de 2006 10:30

Disponible en Internet: <http://scgwww.epfl.ch/courses/Biometrics-Lectures-2006-2007> visitada 18 de Octubre de 2006 23:00

Disponible en Internet: <www.silicon.fr> visitada 02 de Noviembre de 2006 22:30

Disponible en Internet: <www.smart.gov> visitada 03 de Noviembre de 2006 21:20

Disponible en Internet: < http://www.smartcardalliance.org/> visitada 02 de Diciembre de 2006 09:50

Disponible en Internet:
<http://www.telecarte.tm.fr/fr/Histoire_telecarte/tout_savoir_telecarte.htm#toutsavoir > visitada 18 de Junio de 2007 09:45

Disponible en Internet: < http://www.theiai.org/history/> visitada 03 de Enero de 2006 07:45

Disponible en Internet:
< http://www.tssi.co.uk/Products_x_Services/Document_Security/watermark.html > visitada 15 de Mayo de 2007 23:50

Disponible en Internet: <http://www.uc-council.org> visitada 5 de Diciembre de 2006 08:30

Disponible en Internet: <http://unstats.un.org/unsd/methods/m49/m49alpha.htm> visitada 1 de Octubre de 2006 22:23

Disponible en Internet: < http://usuarios.discapnet.es/ojo_oido/el_ojo_cuatro.htm > visitada Mayo 20 de 2007 21:54

Disponible en Internet: <http://v3.espacenet.com/ > visitada 20 de Junio de 2007 01:30

GLOSARIO

ACCESO: capacidad para hacer uso de cualquier fuente del sistema de información, de acuerdo con los privilegios otorgados

ACEPTABILIDAD: el nivel de aceptación que tiene entre usuarios. Es uno de los siete pilares o conceptos básicos de la biometría.

ÁCIDO DESOXIRRIBONUCLEICO: (ADN). Molécula gigante que contiene información genética y hereditaria. Está compuesto de dos cadenas polinucleotídicas que se disponen alrededor de un eje central formando una doble hélice, capaz de auto replicarse y codificar la síntesis del ácido ribonucleico (ARN). Lugar donde está depositada la información genética de un individuo.

ALMACENAMIENTO: capacidad de los dispositivos digitales para guardar bits.

ASOCIACIÓN AMERICANA DE BANQUEROS: (American Bankers Association - ABA). Desarrollaron el Track 2 para el código de barras, en donde se almacena información para transacciones de tarjetas de crédito.

ASOCIACIÓN EUROPEA DE NUMERACIÓN DE ARTÍCULOS: (European Article Numbering Association -EAN). Asociación sin ánimo de lucro creada en europa para el desarrollo de estándares en el ámbito de Europa para los códigos de barras.

ASOCIACIÓN FRANCESA PARA LA NORMALIZACIÓN: (Association Française pour la Normalisation - AFNOR). Organismo de estándares francés responsable por el desarrollo temprano de los estándares de las tarjetas inteligentes.

ASOCIACIÓN INTERNACIONAL DE FABRICANTES DE TARJETAS: (International Card Manufacturers Association - ICMA). Asociación que está globalmente enfocada en la tecnología de producción de tarjetas, tarjetas de banda magnética, tarjetas de no contacto, impresión de tarjetas y producción completa de tarjetas.

ASOCIACIÓN INTERNACIONAL DE TRANSPORTE ÁEREO: (International Air Transport Association - IATA). Asociación que define la codificación, posición y configuración de la primera pista de la banda magnética llamada Track 1.

APLICACIÓN DE JUEGO-ABIERTO: aplicación que determina los identificadores candidatos para un individuo/fuente recolectando uno o más ejemplos biométricos, buscando en la base de datos plantillas similares almacenadas.

APLICACIÓN DE JUEGO-CERRADO: aplicación que organiza las plantillas guardadas en la base de datos en orden de reducir la similaridad contra una muestra sometida.

ARCO: Un patrón de la huella digital donde las crestas de fricción entran de un lado, tiene un levantamiento en el centro, y sale en el lado opuesto. El patrón contendrá un punto delta no verdadero.

ÁREA DE IMAGEN DE LA HUELLA DIGITAL: el área de fricción de la piel en la superficie carnosa de un dedo localizado horizontalmente entre los dos bordes de la uña y verticalmente entre la primera juntura y la punta del dedo. Ella contiene un patrón único de curvaturas de fricción y valles de información comúnmente referido como “huella digital” o “huella dactilar”.

AMPLITUD DE LLAVE: (Amplitude shift keying - ASK). una forma de modulación que representa datos digitales como variaciones en la amplitud de la onda portadora.

BANDA MAGNÉTICA: un medio de almacenamiento magnético para un bajo volumen de datos.

BÁSICO: este es un tipo de imagen fundamental que especifica el formato del registro incluyendo la cabecera y datos de imagen.

BIOMÉTRICO: una característica medible, física o rasgo del comportamiento personal que reconoce o verifica la identidad reclamada por una persona viva.

BIFURCACIÓN: punto donde la cresta de la huella dactilar se divide o parte en dos crestas.

BINNING: proceso de análisis o clasificación de datos en orden de acelerar o mejorar la comparación biométrica.

BLOQUE GRANDE DE DATOS BINARIOS: (Binary Large OBject - BLOB). Típicamente un archivo de imagen o video, que tiene que ser manejado en una forma especial.

CALIDAD: qué tan preciso, veloz y robusto es el sistema en el manejo de la huella biométrica. Es uno de los siete pilares o conceptos básicos de la biometría.

CAPACIDAD: número total de unidades de datos (bits, bytes, palabras) que puede almacenar una memoria, banda magnética, entre otras.

CAPTURA: el proceso de tomar un ejemplo biométrico de un usuario final.

CAPTURA VIVA: el proceso de capturar un ejemplo biométrico por una interacción entre el usuario final y un sistema biométrico.

CARACTERÍSTICAS BIOMÉTRICAS CONDUCTUALES: características particulares de cada individuo relacionadas con su conducta (firma, forma de caminar, voz, entre otras.)

CARACTERÍSTICAS BIOMÉTRICAS BIOLÓGICAS: características particulares de cada individuo relacionadas con su aspecto físico (huella digital, geometría de la mano, iris, retina, entre otras.)

CELDA: una región rectangular definido por una división uniforme y no-solapada de la imagen.

CHIP: pequeño circuito integrado que realiza númerosas funciones en ordenadores y dispositivos electrónicos.

CICLO ANTICOLISIÓN: algoritmo usado para preparar un dialogo entre el dispositivo de acoplamiento de proximidad y una o más tarjetas de proximidad entre muchas dentro de su campo energizado.

CIRCUITO INTEGRADO: un tipo de circuito en el que todos sus componentes se encuentran integrados en un único chip semiconductor.

CODIFICADOR: circuito digital que convierte la información en un formato codificado.

CÓDIGO 128: código de barras lineal con alta compresión de datos y usado ampliamente, existen cuatro códigos más a partir de este que son los código 128A, 128B, 128C, EAN/UCC 128

CÓDIGO BIDIMENSIONAL: código de barras de alta densidad con la capacidad de almacenamiento de información y un alto nivel de seguridad.

CÓDIGO DE BARRAS: un sistema de código binario usando una serie numérica y barras de diferentes grosores o posiciones que pueden ser leídos por un equipo de reconocimiento óptico de caracteres (OCR).

CÓDIGO EAN: código lineal ampliamente usado en el área comercial para la identificación individual de productos, existen varias versiones para distintos usos como son código EAN/UCC 128, código EAN-13, EAN-14, EAN-8, EAN-5, EAN-2, EAN-18/NVE.

CÓDIGO ELECTRÓNICO DE PRODUCTO: (electronic Product Code - ePC). Código para la identificación física de objetos en un esquema univesal a través de etiquetas RFID.

CÓDIGO ITF-14: código lineal que es usado para marcar cajas y contenedores que contienen bienes con código EAN-13

CÓDIGO JAN: código lineal, que es la versión japonesa del código EAN-13

CÓDIGO LINEAL: código de barras de una dimensión, código de baja densidad en la capacidad de almacenamiento de información.

CÓDIGO UNIVERSAL DE PRODUCTO: (Universal Product Code - UPC). Estándar del símbolo de código de barras para venta de productos en Estados Unidos.

CÓDIGO UPC: código lineal usado por los Estados Unidos en el área comercial para la identificación individual de productos, existe el UPC-A y el UPC-E.

COERCITIVIDAD: fuerza electromagnética requerida para magnetizar o codificar una banda magnética.

COLECCIÓN AUTOMÁTICA DE TARIFIAS: (Automatic fare collection - AFC). (1) Sistemas de Colección de Tarifa automatizados, normalmente basado en la Banda magnética, tarjeta con chip o tecnología de RFID. (2) Colección de la tarifa automática, como en los esquemas de transporte publicó con tarjetas inteligentes de contacto o sin contacto inteligente.

COMPARACIÓN: proceso de comparar una referencia biométrica con una (s) referencia(s) almacenada(s) en orden de realizar una decisión de identificación o verificación.

COMPARACIÓN UNO A UNO: en el proceso de verificación, el usuario presenta su(s) dato(s) biométrico(s) y este se compara con la plantilla biométrica almacenada en una base de datos o en un dispositivo portátil, verificando si hay o no coincidencia para esa identidad en la referencia establecida.

COMPARACIÓN UNO A MUCHOS: en el proceso de identificación cerrada, el usuario presenta su(s) dato(s) biométrico(s) y el dato biométrico se compara contra la base de datos, donde se sabe que existe, buscando la identidad más probable del usuario.

COMPARACIÓN UNO A POCOS: es un proceso híbrido entre la verificación y la identificación, donde la persona no reclama una identidad específica, entonces se compara contra toda la base de datos para verificar si existe, una vez se verifica

que posiblemente existe, dentro de las coincidencias más probables, determina quién es el usuario. También es conocido como verificación abierta o watchlist.

CONO: punto de la línea de huella digital donde cambia de dirección de manera drástica

CONCEJO DE CÓDIGO UNIFICADO: (Unified Code Council - UCC). Organización que administra los estándares UPC y otros estándares de venta al detal.

CRESTA DE FRICCIÓN: las crestas presentes en la piel de los dedos y dedos de los pies, las palmas y plantas del pie, que hacen contacto con una superficie bajo un toque normal. En los dedos, el patrón único formado por las crestas de fricción genera una huella digital.

CRUDO: formato de archivo de imagen en donde la imagen es almacenada en el mismo formato en que él es almacenado en memoria de video, típicamente un ejemplo (para imagenes monocromáticas) por elemento de imagen o tres ejemplos (para imagenes a color) por elemento de imagen.

DATO BIOMÉTRICO: la información extraída de la muestra biométrica y usado para construir una plantilla de referencia (plantilla de datos) o para comparar contra una plantilla de referencia creada previamente (comparación de datos).

DECODIFICADOR: circuito digital que convierte la información codificada en un formato familiar o no codificado.

DETECCIÓN DE ERROR: proceso de detección de los bits, bytes o datos erróneos de un código.

EBGM: concordancia gráfica de manojos elásticos. Confía en el concepto que las imagenes de las caras reales tienen muchas características no lineales que no se rigen por los métodos de análisis lineal, como las variaciones en la iluminación (iluminación exterior vs. Iluminación interior), posición (de pie derecho vs. agachándose) y expresión (sonrisa vs. ceño fruncido).

EJEMPLO BIOMÉTRICO: información obtenida de un dispositivo biométrico, de manera directa o después de un proceso futuro.

EMISOR: entidad que expide la tarjeta.

ENGAÑO: (Spoofing). La habilidad de engañar un sensor biométrico en el reconocimiento de un usuario ilegítimo como un usuario legítimo o en fallar la identificación de alguien que se encuentre en la base de datos.

ENROLADO: un ser humano, ejemplo persona natural, asignado a MRTD por un estado usuario.

ENROLAR: proceso de recolectar ejemplos biométricos de una persona y la subsiguiente preparación y almacenamiento de la plantilla de referencia biométrica que representa la identidad de una persona.

ERROR TIPO I: un error que ocurre en una prueba estadística cuando un reclamo verdadero es rechazado (incorrectamente).

ERROR TIPO II: un error que ocurre en pruebas estadísticas cuando un falso reclamo no es rechazado (incorrectamente).

ESCRITURA: el proceso de almacenamiento de datos en memoria.

ESPECTROFOTOMETRÍA: método de análisis óptico más usado en las investigaciones biológicas, donde se compara la radiación absorbida o transmitida por una solución que contiene una cantidad desconocida de soluto, y una que contiene una cantidad conocida de la misma sustancia.

ESPECTROSCOPIA: técnica analítica experimental muy usada en física y química, que se basa en detectar la absorción de radiación electromagnética de ciertas energías y relacionar estas energías con los niveles de energía implicados en la transición cuántica.

ESPIRAL: patrón de huella digital donde las crestas son circulares o casi circulares, el patrón contendrá dos o más deltas.

ESQUELETO: la representación de un sólo píxel de ancho de una cresta o valle obtenido por operaciones sucesivas de adelgazamiento simétrico.

EXTRACCIÓN: proceso de convertir un ejemplo biométrico capturado en un dato biométrico que pueda ser comparado con una plantilla de referencia; algunas veces llamado caracterización

FRECUENCIA DE OPERATIVIDAD DE CAMPO: (Frequency of operating field - FC). Frecuencia del carrier.

FIABILIDAD: que es confiable, que tiene probabilidad de buen funcionamiento. Es uno de los siete pilares o conceptos básicos de la biometría.

FIRMA BIOMÉTRICA: (plantilla biométrica). La representación digital de una característica distintiva de un individuo.

FIRMA DINÁMICA: una modalidad biométrica que analiza las características dinámicas de la firma de un individuo, como la forma de la firma, velocidad de firmado, presión del lapicero al firmar, y movimientos en el aire del lapicero, para reconocimiento.

FINAL DE LA CRESTA: el punto de la minucia asignado a una posición donde la cresta de fricción termina o alternativamente empieza. Una final de la cresta es definida como la bifurcación del valle adyacente.

FISIOLOGÍA: ciencia que tiene por objeto el estudio de las funciones de los seres orgánicos. En biometría se refiere a las características físicas de una persona, tales como huella digital, geometría de la mano, características del iris, retina, entre otras.

FORMATO COMÚN DE INTERCAMBIO DE ARCHIVOS BIOMÉTRICOS: (Common Biometric Exchange Formats Framework - CBEFF). Formato estándar que es suministrado para abarcar cualquier tipo de biométrico.

FRONTAL: un tipo de Imagen facial básica que adhiere requerimientos adicionales apropiados para reconocimiento facial frontal y/o examen humano.

FRONTAL PARCIAL: un tipo de imagen que especifica imagenes faciales con un tamaño geométrico específico y posición del ojo basado en el ancho y alto de la imagen. Ésta es conveniente para minimizar los requisitos de almacenamiento para tareas de reconocimiento facial computarizado mientras le ofrece independencia de vendedor y capacidad de verificación humana.

FRONTAL TOTAL: un tipo de imagen facial que especifica imagenes frontales con suficiente resolución para examen humano, así como para el reconocimiento facial fiable por computador. Este tipo de imagen contiene toda la cabeza con todo el cabello en la mayoría de los casos, así como el cuello y los hombros.

FALLA DE ADQUISICIÓN: (Failure to Acquire - FTA). La falla del sistema biométrico para capturar y/o extraer información útil de un ejemplo biométrico.

FALLA PARA REGISTRO: (Failure to Enroll - FTE). Falla de un sistema biométrico para crear un registro de referencia adecuado para un usuario final.

GRADOS DE LIBERTAD: una medida estadística de cómo es único un dato biométrico. Técnicamente es el número de parámetros independientes estadísticamente contenidos en un dato biométrico.

GS1: (Global Registry). Es una organización global dedicada al diseño e implementación de estándares globales y soluciones para mejorar la eficiencia y

visibilidad en las cadenas globales de suministro y demanda y a través de sectores.

HISTÉRESIS: (1) Tendencia de un material a conservar una de sus propiedades, en ausencia del estímulo que la ha generado. (2) Fricción interna que tiene lugar en un material magnético sometido a un campo magnético variable.

HUELLA DIGITAL: es la impresión visible o moldeada que produce el contacto de las crestas papilares de un dedo en una superficie.

HUELLA DIGITAL DE LA PALMADA: huellas digitales tomadas presionando simultáneamente los cuatro dedos de una mano en un escáner de una tarjeta de huella digital, Palmada también es conocida como una impresión plana simultánea de cuatro dedos.

HUELLA DIGITAL LATENTE: una "imagen" de la huella digital dejada en la superficie que fue tocada por un individuo. La impresión transferida es dejada por la superficie de contacto con las crestas rígidas, usualmente causada por residuos aceitosos producidos por las glándulas sudoríparas en el dedo.

HUELLA DIGITAL RODADA: una imagen que incluye el dato de huella digital de borde de uña a borde de uña, obtenida "rodando" el dedo a través del sensor.

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

IDENTIFICACIÓN ABIERTA: es un proceso híbrido entre la verificación y la identificación, donde la persona no reclama una identidad específica, entonces se compara contra toda la base de datos para verificar si existe en la base de datos, una vez se verifica que posiblemente existe, dentro de las coincidencias más probables, determina quién es el usuario. También es conocido como comparación uno a pocos ó watchlist.

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

IDENTIFICACIÓN DE AMIGOS Y ENEMIGOS: (Identify Friend and Foe - IFF). Dispositivo que se utiliza para determinar la identidad de aeronaves especialmente mediante la transmisión de señales de radio.

IDENTIFICACIÓN POR RADIO FRECUENCIA: (Radio Frequency IDentification - RFID). Tecnología que usa transmisores de radio de bajo poder para leer datos almacenados en el transponder.

IDENTIFICADOR ÚNICO: (Unique IDentifier - UID). Número que es necesario para el algoritmo de anticolisión tipo A.

IMAGEN FACIAL: imagen electrónica basada en la representación del retrato de una persona.

IMPOSTOR: una persona que suministra un ejemplo biométrico y de manera intencional o inadvertida reclama la identidad de otra persona en un sistema biométrico.

IMPRESIÓN DE ESCANEO-VIVO: una imagen de huella digital que es producida por escaneo o graficación de un dedo vivo para generar una imagen de las crestas de fricción.

INFRARROJO: longitudes de onda situadas más allá del extremo rojo del espectro. Radiación electromagnética de mayor longitud de onda que la luz visible, pero menor que la de las microondas. Se encuentra entre 0.75 y 100 μm.

INSTITUTO NACIONAL AMERICANO DE ESTANDARIZACIÓN: (American National Standards Institute - ANSI). Principal organización encargada de promover el desarrollo de estándares tecnológicos en Estados Unidos.

INTERFAZ: mecanismo por el que los dos o más dispositivos electrónicos o sistemas se hacen compatibles operacionalmente entre sí, de manera que puedan funcionar adecuadamente juntos.

INTERFAZ DE PROGRAMACIÓN DE APLICACIONES: (Application Programming Interface - API). El método específico prescrito por un sistema operativo, aplicación o herramienta de terceros, por el cual un programador que escriba una aplicación puede realizar peticiones al sistema operativo.

INTERFAZ DE PROGRAMACIÓN DE LA APLICACIÓN BIOMÉTRICA: (Biometrics Application Programming Interface - BIOAPI). Especificación del API desarrollada por el consorcio BioAPI para servir a varias tecnologías biométricas.

IRIS: disco membranoso y coloreado, en cuyo centro está la pupila.

ISLA: cresta de la huella digital de muy corta extensión.

ENTRELAZADO 2 DE 5: (Interleaved 2-of-5 - ITF). Código de barras adoptado especialmente para materiales de empaquetado de baja calidad (cartón corrugado).

JPEG: (Joint Photographic Experts Group). Es un algoritmo diseñado para comprimir imagenes. JPEG es también el formato de fichero que utiliza este algoritmo. El formato de archivos JPEG se abrevia frecuentemente JPG debido a que algunos sistemas operativos sólo aceptan tres letras de extensión.

LASO: un patrón de huella digital en donde las crestas de fricción entran de cualquier lado, se curva grandemente y sale cerca del mismo sitio que entro. Este patrón contendrá un punto central y un delta.

LECTURA: el proceso de recuperar datos de una memoria, código de barras, entre otras.

LÍNEA TIPO: son las dos líneas más internas que empiezan en paralelo, diverge, y rodea o intenta rodear el área del patrón.

MINUTIAE: (Minucia). Características de crestas de fricción que se usan para individualizar una imagen de la huella digital. Las minucias son los puntos donde las crestas de fricción empiezan, terminan, o se dividen en dos o más crestas. En muchos sistemas de la huella digital, Minutiae (como opuesto a las imagenes) se compara para los propósitos del reconocimiento.

MÓDULO DE IDENTIDAD DEL SUSCRIPTOR: (Subscriber Identity Module - SIM). Módulo que contiene información del usuario, tal como su PIN, número de suscriptor, número telefónico y otra información clave.

MORFOLOGÍA: parte de la biología que trata de la forma de los seres orgánicos y de las modificaciones o transformaciones que experimenta. En biometría se refiere a las características físicas de una persona, tales como huella digital, geometría de la mano, características del iris, retina, entre otras.

MAQUINA LECTORA DE DOCUMENTOS DE VIAJE: (Machine Readable Travel document - MRTD). Máquina propuesta por la ICAO para que lea cualquier tipo de documento de identificación de viajeros y empleados de aeropuertos (pasaporte, visa, entre otras.).

MUESTRA BIOMÉTRICA: los datos desnudos capturados como un valor discreto inequívoco, único y lingüísticamente neutro que representa una característica biométrica de un enrolado como uno capturado por un sistema biométrico (por ejemplo la muestra biométrica puede incluir la imagen de la huella digital así como sus derivados para propósitos de autenticación).

MULTIALGORÍTMICO: usa múltiples algoritmos para procesar el mismo ejemplo biométrico.

MULTIINSTANCIA: usa múltiples instancias biométricas con una modalidad biométrica

MULTIMODAL: usa múltiples modalidades biométricas diferentes

MULTIPRESENTACIÓN: ésta técnica usa múltiples presentaciones de una instancia de una característica biométrica o una presentación simple que resulta en la captura de múltiples ejemplos

MULTISENSORIAL: usa múltiples sensores para medir la misma instancia biométrica

MULTITAREA: entorno de sistema operativo en el que la computadora parece ejecutar múltiples programas o tareas simultáneamente.

NUMERACIÓN EUROPEA DE ARTÍCULOS: (European Article Numbering - EAN). Código de barras europeo desarrollado para la identificación de artículos dentro de la cadena de distribución comercial.

NÚMERO DE AUTENTIFICACIÓN PERSONAL: (Personal Autentification Number - PAN). Número codificado en la tarjeta plástica que identifica al emisor y la cuenta particular del tarjeta habiente.

NÚMERO DE IDENTIFICACIÓN PERSONAL: (Personal Identification Number - PIN). Una clave o número secreto que se compone únicamente de dígitos decimales y que está asociado a una persona o usuario.

NÚMERO INTERNACIONAL ESTÁNDAR DEL LIBRO: (International Standard Book Number - ISBN). Es un identificador único para libros.

NÚMERO INTERNACIONAL NORMALIZADO DE PUBLICACIONES SERIADAS: (International Standard Serial Number - ISSN). Identificador único de publicaciones periódicas.

OASIS: (Organization for the Advancement of Structured Information Standards). Consorcio sin ánimo de lucro que orienta el desarrollo, la convergencia y la adopción de los estándares e-business.

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL: (International Civil Aviation Organization - ICAO). Organización encargada de establecer normas de carácter internacional para la aviación comercial.

PATRON: (Pattern). Algoritmo utilizado para el reconocimiento biométrico.

PERMANENCIA: qué tanto perdura la huella biométrica en el tiempo de manera inalterable. Es uno de los siete pilares o conceptos básicos de la biometría.

PÍXEL: componente individual de imagen, uno de una matriz n por m de elementos de imagen donde m es el número de columnas y n es el número de filas.

PLANTILLA DE INFORMACIÓN BIOMÉTRICA: un objeto de datos construidos en una tarjeta que contiene información requerida por el mundo externo para un proceso de verificación.

PR: el promedio o número de comparaciones necesarias - bajo el esquema binning - entre cada muestra y la base de datos, dividido por el tamaño de está última.

PRECISIÓN: una palabra para describir que tan bién funciona un sistema biométrico.

PULSACIÓN DINÁMICA: una modalidad biométrica que usa el patrón de un individuo para pulsar teclas como reconocimiento.

PUNTO CENTRAL: (Core Point). Es el "centro" de la huella digital. Es el punto más alto en la curva más interna de la cresta rígida de una huella digital. En un patrón espiral, el punto central se encuentra en la mitad de los círculos/espirales. En un patrón laso, el punto central se encuentra en la parte más profunda de la región donde se encuentre el laso más interno. Un punto central está definido técnicamente como el punto más profundo en la curva de cresta de fricción más interna. Puede existir ninguno, uno o muchos puntos centrales.

PUNTO DELTA: parte de un patrón de huella digital que luce similar a la letra griega delta (Δ). Es ese punto en una cresta o el punto más cercano al punto de divergencia de dos tipos de líneas, y localizada en o directamente en frente del punto de divergencia.

PUNTO DE MINUCIA: característica de la cresta de fricción que es usada para individualizar una imagen de huella digital. Las minucias son los puntos donde las crestas de fricción inician, terminan, o se dividen en dos o más crestas. En muchos sistemas de huella digital, la minucia (como opuesto a la imagen) es comparada para propósitos de reconocimiento.

RASGO: punto de referencia de punto(s) en la imagen facial como es usado en los algoritmos de reconocimiento facial, normalmente referido como un hito.

RASTREO DE DETECCIÓN DE ERROR: (Detection Error Tracking - DET). Detección de error de intercambio de datos biométricos.

RECOLECTABLE: qué tan fácil es la adquisición, medición y almacenamiento de la huella biométrica. Es uno de los siete pilares o conceptos básicos de la biometría.

RECONOCIMIENTO: término genérico usado en la descripción de sistemas biométricos. El término reconocimiento no implica de manera inherente la comprobación, lista de control o tarea de identificación.

RECONOCIMIENTO DE ADN: sistema biométrico invasivo que requiere de una muestra física y que su comparación actualmente no se puede realizar en tiempo real.

RECONOCIMIENTO DE DISCURSO: una tecnología que reconoce las palabras dichas, y no es una tecnología biométrica.

RECONOCIMIENTO DE IRIS: una modalidad biométrica que usa una imagen de la estructura física del iris de un individuo con propósitos de reconocimiento.

RECONOCIMIENTO DE LABIOS: tecnología biométrica conductual o fisiológica (depende del tipo de reconocimiento que se realice) no invasiva, que verifica la huella o el movimiento o la forma de los labios.

RECONOCIMIENTO DE LA GEOMETRÍA DE LA MANO: una modalidad biométrica que usa la estructura física de la mano de un individuo con propósitos de reconocimiento.

RECONOCIMIENTO DE LA HUELLA DIGITAL: una modalidad biométrica que usa la estructura física de la huella digital de un individuo con propósitos de reconocimiento.

RECONOCIMIENTO DE LA HUELLA PALMAR: una modalidad biométrica que usa la estructura física de la palma de la mano de un individuo impresa para propósitos de reconocimiento.

RECONOCIMIENTO DE OLOR: tecnología biométrica no invasiva basada en las características físicas de la composición química del olor del cuerpo.

RECONOCIMIENTO DE UÑA: tecnología biométrica emergente, que no ha sido muy estudiada y que consiste en el estudio de los rasgos particulares de la uña.

RECONOCIMIENTO DE VOZ: una modalidad biométrica que usa el discurso del individuo, una característica influenciada por la estructura física del tracto vocal del

individuo y características de comportamiento individual, con propósitos de reconocimiento.

RECONOCIMIENTO FACIAL: una modalidad biométrica que usa una imagen de la estructura física visible de la cara de un individuo para propósitos de reconocimiento.

RECONOCIMIENTO ÓPTICO DE CARACTERES: (Optical Character Recognition – OCR). Proceso de lectura de caracteres impresos en los documentos de papel con fuentes de tipo especiales, que pueden ser reconocidos y generan salidas en archivos de lectura de texto únicamente (Archivos ASCII planos).

REGISTRO DE IDENTIFICACIÓN BIOMÉTRICA: (Biometric Identification Record – BIR). Cualquier dato retornado a la aplicación, pueden ser datos crudos recién capturados por el dispositivo, datos intermedios en medio del procesamiento, o datos procesados listos para verificación/identificación.

RESULTADO DE SIMILITUD: un valor devuelto por un algoritmo biométrico que indica el grado de similitud o relación entre el ejemplo biométrico y la referencia.

RETINA: capa más interna de las tres capas del globo ocular y es el tejido fotorreceptor.

RUIDO: componentes indeseables en una señal que degrada la calidad de los datos o interfiere con señales deseadas procesadas por un sistema.

SEGMENTACIÓN: (1) Es el primer paso en la mejora de la imagen de huella digital, consiste en separar el fondo del resto de la imagen de la huella digital. (2) El proceso de separar la señal biométrica de interés de los datos totales adquiridos por el sistema (encontrar una huella digital individual de una impresión de la palmada).

SENSOR CAPACITIVO: genera una imagen de las crestas (crestas) y valles de la huella en la superficie de un circuito integrado de silicona.

SENSOR DE CAMPO ELÉCTRICO: se origina un campo entre el dedo y el semiconductor adyacente que simula la forma de los surcos y crestas de la superficie epidérmica. Se utiliza un amplificador under-pixel para medir la señal.

SENSOR ÓPTICO: dispositivo que se basa en una extracción de puntos de la imagen que se genera de la huella dactilar. Es el método más comúnmente utilizado.

SENSOR TÉRMICO: hay que arrastrar el dedo por el sensor, durante este movimiento del dedo el sensor mide la temperatura diferencial entre las crestas y

el aire retenido en los valles. Se realizan tomas sucesivas de la huella y el software reconstruye la imagen.

SIM CARD: tarjeta con módulo de identidad del suscriptor. Es una tarjeta electrónica removible que se inserta en un teléfono móvil GSM/GPRS/3G y que contiene el sistema operativo del celular y los programas que corren en él.

SINGULARIDAD: qué tan único o diferenciable es la huella biométrica entre uno y otro individuo. Es uno de los siete pilares o conceptos básicos de la biometría.

SISTEMA BIOMÉTRICO: un sistema automático capaz de:
1. capturar una muestra biométrica de un enrolado para un MRTD;
2. extraer los datos biométricos de una muestra biométrica;
3. comparar ese valor (es) de datos biométricos específico (s) con los contenidos en uno o más plantillas de referencia;
4. decidir qué tan bien coinciden ellos; e
5. indicar si una identificación o comprobación de identidad se han logrado o no.

SISTEMA BIOMÉTRICO MULTIMODAL: un sistema biométrico en donde dos o más componentes de modalidad (característica biométrica, tipo de sensor o algoritmo de extracción) ocurren en multiplicidad.

SISTEMA DE IDENTIFICACIÓN AUTOMÁTICA DE HUELLAS DIGITALES: (Automated Fingerprint Identification System - AFIS). Sistema biométrico altamente especializado que compara la imagen de una huella digital con la imagen contenida en una base de datos.

SISTEMA DE IDENTIFICACIÓN BIOMÉTRICA AUTOMÁTICA: (Automatic biometric identification system - ABIS). Sistema del Departamento de Defensa (DoD) desarrollado para mejorar la habilidad del gobierno de Estados Unidos para rastrear e identificar riesgos de seguridad nacional.

SISTEMA DE NUMERACIÓN EUROPEA DE ARTÍCULOS: (European Article Numbering System – EAN). Sistema desarrollado para estandarizar la numeración de los productos producidos en Europa y que se mueven en la cadena de distribución comercial.

SISTEMA INTEGRADO DE IDENTIFICACIÓN AUTOMÁTICA DE HUELLAS DIGITALES: (Integrated Automated Fingerprint Identification System). Base de datos nacional en línea corrida por el FBI que contiene las huellas digitales y la historia criminal de las personas.

TARJETA DE PROXIMIDAD: es un tipo de tarjeta con circuito integrado que utiliza las ondas de radio para transmitir información entre la tarjeta y el dispositivo lector a corta distancia.

TARJETA DE VECINDAD: es un tipo de tarjeta con circuito integrado que utiliza las ondas de radio para transmitir información entre la tarjeta y el dispositivo lector a una distancia mayor que la tarjeta de proximidad.

TARJETA INTELIGENTE: tarjeta con un circuito integrado empotrado que guarda información de los procesos.

TASA DE ACEPTACIÓN CIERTA: (True Accept Rate - TAR). Una estadística usada para indicar el número de veces que un sistema verifica un reclamo verdadero de identidad.

TASA DE BITS ERRADOS: (Bit error rate - BER). El número de coincidencias de pares de plantilla-muestras que el sistema ha puesto en las diferentes cajas, con respecto al número de pares evaluado.

TASA DE ERROR IGUAL: (Equal Error Rate -EER). Una estadística usada para verificar la actuación biométrica cuando trabaja en la tarea de verificación. El punto operativo en un sistema métrico donde la tasa de falsa aceptación (FAR) y la tasa de falso rechazo (FRR) son iguales.

TASA DE FALSA ACEPTACIÓN: (False Acceptance Rate - FAR). La probabilidad de que un sistema biométrico identifique incorrectamente un individuo o que falle para rechazar un impostor.

TASA DE FALSA ALARMA: (False Alarm Rate). Una estadística usada para medir la calidad del biométrico cuando opera en el modo de identificación abierta (watchlist ó comparación uno a pocos). La alarma suena incorrectamente cuando un individuo no está en el sistema, o la alarma suena con una identificación errónea de persona.

TASA DE FALSA ACEPTACIÓN: (False Acceptance Rate - FAR). La probabilidad de que un sistema biométrico identifique incorrectamente un individuo o que falle para rechazar un impostor.

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

TASA DE FALSA NO-COINCIDENCIA: (FNMR - False Non-Match Rate). Es parecida a la tasa de falso rechazo (FRR), con la diferencia de que la FRR incluye la tasa de falla para capturar el error (Failure to Acquire error rate).

TASA DE FALSO RECHAZO: (False Rejection Rate - FRR). La probabilidad de que un sistema biométrico rechace incorrectamente un individuo.

TASA DE RECHAZO CIERTA: (True Reject Rate). Una estadística usada para indicar el número de veces que un sistema verifica un reclamo falso de identidad.

TÉRMINO DE CRESTA: un punto de minucia en el final de la cresta de fricción.

TERMOGRAFÍA: método fotográfico que hace visible el calor irradiado por el cuerpo o una parte de él.

TRACK: pista de un dispositivo de almacenamiento.

TTM: duración del proceso de comparación desde la finalización de la captura, hasta la decisión del sistema.

TERCER ESTÁNDAR DE ECONOMÍA: (thrift Third Standard - TTS). Define la codificación, posición y configuración de la pista de la banda magnética llamada Track 3.

UMBRAL: un escenario de usuario para la operación de sistemas biométricos en la verificación o tarea de identificación abierta (watchlist). La aceptación o rechazo de datos biométricos es dependiente en la del resultado de concordancia por debajo o por encima del umbral. El umbral es ajustable así que el sistema biométrico puede ser más o menos estricto, dependiendo de los requerimientos de cualquier aplicación biométrica dada.

UNIVERSALIDAD: qué tan común es encontrar este rasgo biométrico en los individuos. Es uno de los siete pilares o conceptos básicos de la biometría.

VALLE: el área que rodea una cresta rígida, que no hace contacto con una superficie incidental durante un toque normal; el área del dedo entre dos crestas de fricción.

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

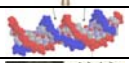
WATCHLIST: es un proceso híbrido entre la verificación y la identificación, donde la persona no reclama una identidad específica, entonces se compara contra toda la base de datos para verificar si existe en la misma, una vez se verifica que posiblemente existe, dentro de las coincidencias más probables, determina quién es el usuario; Es decir en este proceso se contesta a dos preguntas ¿Existe en la base de datos? y en caso afirmativo ¿Quién es? También es conocido como identificación abierta o comparación uno a pocos.

ANEXO A
Línea de tiempo - historia tecnología de autenticación

Tecnología	Fecha	Descripción
	6000 A.C.	Almacenamiento de huellas digitales, usado por asirios, babilónicos, japoneses y chinos.
	Siglo XIV	Chinos estampaban las huellas de manos y pies de los niños para identificarlos
	1686	Malpighi identificó diferencias en los patrones de huellas digitales
	1823	Purkine, identificó la naturaleza única de las huellas digitales
	1858	Hershel crea el primer registro de huellas palmares de empleados
	1870	Bertillon desarrolla el sistema de antropometría descriptiva
	28-oct-1880	Faulds publica el artículo “On the Skin-Furrows of the Hand”
	1882 -1890	La policía de Francia utiliza la técnica desarrollada por Bertillon
	8-sep-1888	Se publica artículo de Oberlin Smith en la revista Electrical World
	1883	Mark Twain publica el libro “life on the Mississippi”
	1-sep-1891	Se empieza a utilizar el método de Juan Vucetich en Argentina
	1892	Francis Galton publica el libro “Finger Prints”
	1892	Se identifica por primera vez por la huella digital a una asesina
	1894	Mark Twain publica el libro “The tragedy of Pudd’nhead Wilson”
	1896	La policía de Bengal implementa el sistema de huella digital
	1898	Invención de un grabador eléctrico sobre una tira de material flexible cubierta de polvo imantado
	1900	Scotland Yard adopta el sistema de huellas digitales de Henry
	1902	Denmark Hill en el Reino Unido es conectado con la escena del crimen
	1903	El departamento de policía de New York empieza los archivos de huellas digitales
	1903	Colapsa el sistema Bertillon
	1905-1908	Se implementa el sistema de huellas digitales en las Fuerzas Militares de EEUU
	1918	Locard establece 12 detalles Galton como mínimo para identificación positiva de una persona.
	18-dic-1934	Patentado lector óptico de código de barras clasificador de tarjetas

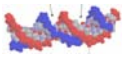
Tecnología	Fecha	Descripción
	Sep-1935	Se publica el artículo “A new Scientific Method of Identification”
	17-sep-1935	Patentado mejoras en o relacionadas con sistemas inalámbricos
	12-nov-1935	Patentada una máquina organizadora de tarjetas
	1936	Burch propone el concepto de los patrones de iris para reconocimiento
	1940	Un sistema activo llamado MKI es puesto en servicio
	1951	Se empieza a usar la tarjeta con banda magnética en bancos
	7-oct-1952	Patentado primer sistema de código de barras como un método y aparato clasificador
	1955	Se publica el artículo “The fundus Oculi in monozigotic twins: Report of six pairs of identical twins”
	Década 60s	IBM perfeccionó el método para adherir una banda magnética a la superficie de una tarjeta plástica
	Principio 60s	Se empieza a usar la tarjeta con banda magnética en el transporte público
	1960	Publicación modelo de los componentes fisiológicos de la producción del discurso acústico.
	1961	Aparece el primer escáner fijo de código de barras
	9-mar-1963	Publicación artículo “automatic Comparison of Finger-Ridge Patterns”
	1964-1965	Desarrollo del primer sistema semi-automático de reconocimiento facial.
	1965	Desarrollo del primer sistema de reconocimiento de firma
	1967	Se instalo el primer sistema de escáner en el ámbito comercial
	1968	Se desarrollo un sistema de identificación
	1969	El FBI impulsa la automatización del proceso de identificación de huellas digitales.
	1969	Pierce publica un artículo titulado “Whither Speech Recognition?”
	Sep-1969	NAFC crea el comité ad-hoc para la creación de un código único de producto
	25-nov-1969	Danna patenta un instrumento para identificar la firma
	Década 70s	Goldstein, Harmon y Lesk presentan los primeros resultados en la automatización del reconocimiento Facial
	1970	Se emite la norma ISO7811 para la banda magnética
	1970	Arimura Ichiro realiza aportes importantes al desarrollo de la tarjeta con circuito integrado
	1970	Perkell modela por primera vez componentes conductuales del discurso
	1971	The American Banking Association aprobó el uso de la banda magnética

Tecnología	Fecha	Descripción
	25-May-1971	Se patenta un sistema de identificación de la palma de la mano
	1972	BankAmericard Inc. adopta la banda magnética.
	7-nov-1972	Se patenta una tarjeta de información
	1973	Se funda el Uniform Code Council inc.
	16-ene-1973	Se patenta una impresora para tarjetas con banda magnética
	23-ene-1973	Se patenta un sistema y aparato transponder
	1974	El primer sistema de reconocimiento de la geometría de la mano estuvo disponible
	1974	Se realiza la primer venta usando un escáner UPC
	1975	FBI desarrollo un prototipo lector de huellas digitales
	1976	Se desarrolla primer prototipo de sistema de reconocimiento del hablante ¿?
	25-may-1976	Patentado un aparato para grabar la firma
	1977	Se funda European Article Numbering Association
	8-feb-1977	Roland Moreno patentó un sistema de transferencia de datos
	28-jun-1977	Namur patenta un arreglo de reconocimiento de hablante
	12-jul-1977	Se patenta un aparato para identificación personal
	25-abr-1978	Se patenta un método y circuito para decodificar
	22-ago-1978	Se patenta un aparato y método para identificar individuos a través de sus patrones vasculares de la retina
	Década 80s	NIST crea el grupo de discurso NIST
	8-jul-1980	Se patenta la tarjeta con microprocesador
	1983	James Bond utiliza tecnología de reconocimiento de iris
	20-sep-1983	Se patenta el algoritmo RSA
	1984	Telecom Francia lanza las telecartas
	1985	Flom y Safir proponen el concepto de que no hay dos iris iguales
	1987	Se expiden la norma ISO 7816 para tarjetas con circuito integrado
	3-feb-1987	Se patenta un sistema de reconocimiento de iris
	31-jul-1987	Se patenta un método para identificar una persona a partir de la geometría de la mano
	1988	El condado de Los Ángeles empieza a usar tecnología de reconocimiento facial
	28-jul-1988	Se crea el instituto colombiano de Codificación y Automatización Comercial IAC

Tecnología	Fecha	Descripción
	27-dic-1988	Se patenta un código de barras multilíneas y un método asociado de decodificación
	14-feb-1989	Se patenta un método y aparato para verificar la identidad de un individuo
	Principios 90	IBM desarrolla un sistema RFID que en frecuencia UHF y tiene un alcance de 7metros
	1990	Aparecen en Francia varias aplicaciones para la tarjeta inteligente
	Ene-1990	Kirby y Sirovich publican “Application of the Karhunen-loeve procedure for the characterization of human faces”
	1991	Aparece la tarjeta SIM con una capacidad de 3KB
	1991	Turk y Pentland publican “Eigenfaces for recognition”
	Oct-1992	Primera Reunión de Biometric Consortium
	3-nov-1992	Patente Colombiana para una “Unidad de Validación e Identificación”
	1993-1997	Corre el programa FacE REcognition Technology (FERET)
	1993	Se inician trabajos para probar y entregar un prototipo de unidad de reconocimiento de iris.
	31-ago-1993	Patentado método para decodificar símbolos de códigos de barras para escaneos parciales
	7-sep-1993	Patentado sistema para codificar y decodificar datos en una máquina lectora de formas gráficas
	1994	Lockheed Martin es seleccionado para construir el IAFIS del FBI
	1994	Sale al mercado RECOderm™
	1-mar-1994	Daugman patenta un sistema biométrico de identificación personal basado en el análisis del iris
	1995	OKI Electric Industry Ltd. Ofrece cajeros automáticos con reconocimiento de iris en Japón
	1997	Serge Humpich, crea una tarjeta maestra para retirar dinero de entidades financieras
	1997	Se presenta el proyecto HA-API
	1998	El FBI lanza Combined DNA Index System (CODIS)
	28-jul-1998	Se patenta una identificación biométrica de individuos usando patrones de venas subcutáneas
	1999	Se establece el centro de Auto-ID en el MIT
	1999	La ICAO inicia estudio de la aplicabilidad de los biométricos en MRTD
	Ene-2001	Se usa el sistema de reconocimiento facial en el Super Bowl en Tampa, Florida
	2000	Se da inicio a la prueba de reconocimiento facial del vendedor (FRVT)
	2001	Se publica un paper sobre el uso de patrones de venas subcutáneas

Tecnología	Fecha	Descripción
	2002	Se establece el comité de biométricos en la ISO
	1-feb-2002	Se crea el programa FEARID
	30-may-2002	Patente Colombiana para un “Sistema de Lectura de huellas dactilares”
	2003	Se establece European Biometrics Forum
	30-ene-2004	Se patente en Colombia un “dispositivo portátil que tiene capacidades de autentificación basadas en biometría”
	May-2004	Se da inicio al gran reto del reconocimiento facial (FRGC)
	2005	EAN internacional cambia su nombre a GS1
	2005	Expira la patente de Estados Unidos para el concepto de reconocimiento del iris
	2005	Iris on Move™ es anunciado en la Conferencia de Biometrics Consortium por parte de Sarnoff Corporation
	31-may-2005	Termina el programa FEARID
	31-ago-2006	Se asignan dos patentes a Fredy Mauricio Sanabria Higuera
	14-dic-2006	Se patenta un método y aparato para obtener información biométrica del iris de un sujeto en movimiento

Convenciones

 Adn

 Banda Magnética

 Biométricos

 Código de barras

 Firma

 Geometría de la mano

 Huella dactilar

 Huella palmar

 Iris

 Pulsaciones de tecla

 Reconocimiento facial

 Retina

 RFID

 Tarjeta con circuito integrado

 Vascular

 Voz

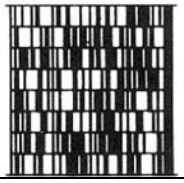
 Huella de la oreja

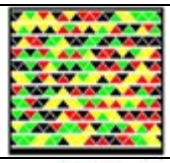
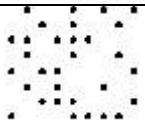
ANEXO B
Tabla de resumen código de barras

Nombre	Código	Longitud	Juego de caracteres	Dígito de control	Descripción
Código 128		variable	ASCII (128 caracteres)	Módulo 103	Tiene alta compresión de datos. Altamente usado
Código 128A		variable	A-Z, 0-9 y caracteres de control	Módulo 103	Tiene alta compresión de datos. Generalmente se remplaza por el EAN/UCC 128
Código 128B		variable	A-Z, a-z, 0-9	Módulo 103	Tiene alta compresión de datos. Generalmente se remplaza por el EAN/UCC 128
Código 128C		variable	Numérico 0-9	Módulo 103	Tiene alta compresión de datos. Generalmente se remplaza por el EAN/UCC 128
EAN/UCC 128		variable	ASCII (128 caracteres)	Módulo 103	Es una forma especial del código 128.
EAN-13		13	Numérico 0-9	Módulo 10	Es usado básicamente en supermercados para identificar productos en puntos de venta
EAN-8		8	numérico 0-9	Módulo 10	Es una versión corta del código EAN-13
EAN-5		5	Numérico 0-9	no	Código adicional para publicaciones
EAN-2		2	Numérico 0-9	no	Código adicional para publicaciones
JAN		13	Numérico 0-9	Módulo 10	Es la versión japonesa del EAN-13
EAN-Velocity		8	numérico 0-9	Módulo 10	EAN-Velocity es una forma especial de EAN-8. Es usado internamente por los distribuidores para marcar productos sin código de barras
EAN-14		14	numérico 0-9	Módulo 10	Es usado para bienes comercializados

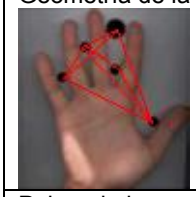
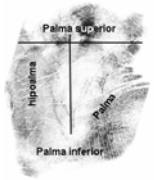
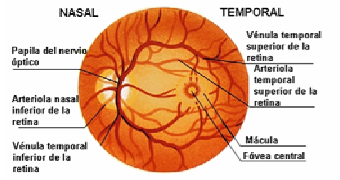
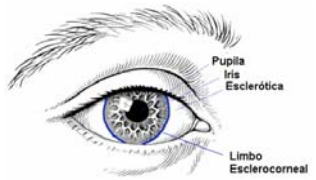
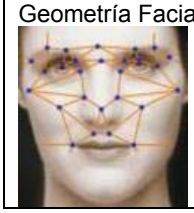
Nombre	Código	Longitud	Juego de caracteres	Dígito de control	Descripción
EAN-18/NVE		18	Numérico 0-9	Módulo 10	Es usado para mostrar el “Nummer der Versandeinheit”(NVE).
DUN-14		14	Numérico 0-9	Módulo 10	Número de Distribución de Unidad.
ISBN-10		13	Numérico 0-9	Módulo 11	International Standard Book Number. ISBN estándar hasta Diciembre 31/2005.
ISBN-13		13	Numérico 0-9	Módulo 10	International Standard Book Number. ISBN estándar desde Enero 1/2007.
ISBN-13 Dual		13	Numérico 0-9	Módulo 10	International Standard Book Number. ISBN de transición entre Enero 1/2006 Hasta Diciembre 31/2006
ISSN		8	Numérico 0-9	Módulo 11	International Standard Serial Number. ISSN es una identificación inequívoca de publicaciones periódicas
ISMN		10	Numérico 0-9	Módulo 10	Internationally Standard Music Number (ISMN)
SCC-14		14	Numérico 0-9	Módulo 10	Shipping Container Symbol (SCC)
ITF-14		14	Numérico 0-9	Módulo 10	Es usado para crear el SCC. Es usado para marcar cajas y contenedores que contienen bienes con código EAN-13
SSCC-18		18	Numérico 0-9	Módulo 10	Serial Shipping Container Code. SSCC es usado en la cadena de suministros para rastreo e identificación interna.
UPC-A		12	Numérico 0-9	Módulo 10	Es la versión estándar del código UPC

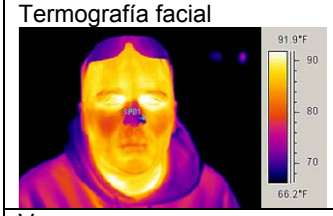
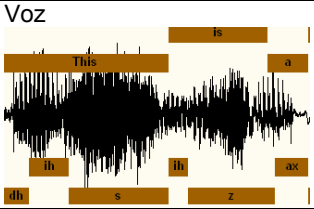
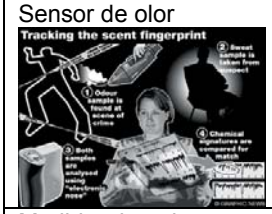
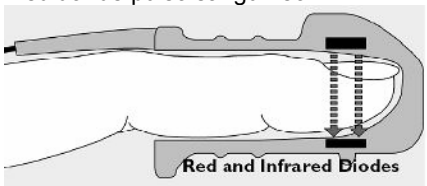
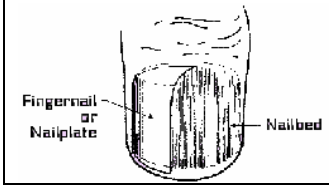
Nombre	Código	Longitud	Juego de caracteres	Dígito de control	Descripción
UPC-E		8	Numérico 0-9	Módulo 10	Es la versión corta del código UPC-A
Código 39		variable	A-Z, 0-9, 5 caracteres especiales	opcional Módulo 43	También conocido como código 3 de 9
Código 39 Extendido		variable	ASCII (127 caracteres)	opcional Módulo 43	También conocido como código 3 de 9 extendido
Código 93		variable	A-Z, 0-9, 5 caracteres especiales	Módulo 47	Similar al código 39 pero más compacto
Código 93 Extendido		variable	ASCII (127 caracteres)	Módulo 47	Similar al código 39 extendido pero más compacto
Código 2 de 5 estándar		variable	Numérico 0-9	opcional Módulo 10	También conocido como código industrial 2 de 5.
Código 2 de 5 entrelazado		variable	Numérico 0-9	opcional Módulo 10	También conocido como código 25 o código ITF
Codabar		variable	0-9, 6 caracteres especiales	opcional Módulo 16	Antiguo tipo de código de barras.
PZN		7	Numérico 0-9	Módulo 11	Pharmazentralnummer für medicine. Forma especial del código 39
LeitCode		14	Numérico 0-9	Módulo 10	Es usado por Deutschen Post/DHL.
IdentCode		12	numérico 0-9	Módulo 10	Es usado por Deutschen Post/DHL.
Plessey		variable	Numérico 0-9, caracteres A-F	-	Antiguo tipo de código de barras

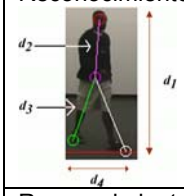
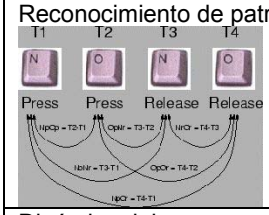
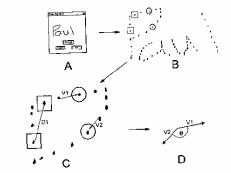
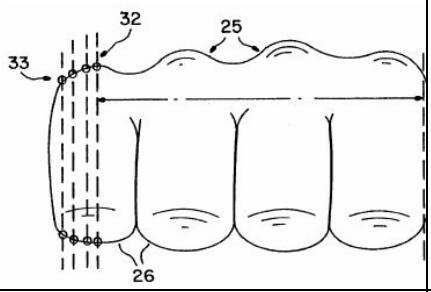
Nombre	Código	Longitud	Juego de caracteres	Dígito de control	Descripción
MSI Plessey		variable	Numérico 0-9	-	Modificación al código Plessey.
PostNet		Variable 5, 9 ó 11	Numérico 0-9	Módulo 10	Código usado para el manejo del correo especialmente usado por EEUU
Royal Mail		variable	A-Z, 0-9	-	Código usado por The Royal Mail 4 State Customer Code (RM4SCC)
Australia Post 4-state barcode		Variable	Caracteres alfanuméricos		Código Usado por el servicio de correo Australiano
RSS-14		14	Numérico 0-9		Codifica cualquier número de producto de 14 dígitos UCC/EAN
RSS-14 limitado		Variable 8, 12 ó 13	Numérico 0-9		Codifica número de producto UCC/EAN 8, 12 y 13 solamente
RSS-14 apilado		14	Numérico 0-9		Es una versión apilada verticalmente de RSS-14
RSS-14 expandido		variable			Codifica información complementaria, puede ser apilado.
Código 11 (USD-8)		Variable	Numérico 0-9, guión (-)	Módulo 11	Se utiliza para el etiquetado de los equipos de telecomunicaciones
Data Matrix		variable	ASCII	interno	Codifica de 1 a 2000 caracteres, es omnidireccional
PDF417		variable	ASCII	interno	Tiene 9 niveles de seguridad .Para control de documentos
Código Azteca		variable	ASCII	interno	Codifica de 12 a 3800 caracteres. Se utiliza en ambientes de control de acceso y seguridad
Maxicode		variable	ASCII	interno	arreglo de 866 hexágonos, con datos almacenados en forma binaria
Código 49		variable	ASCII	interno	Puede tener desde 2 hasta 18 renglones de alto. Creado para codificar objetos pequeños

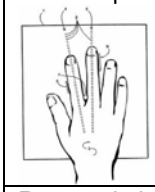
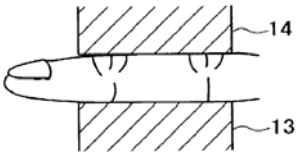
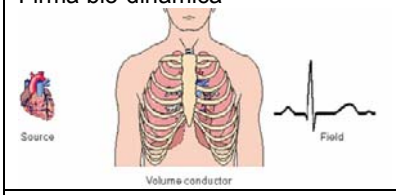
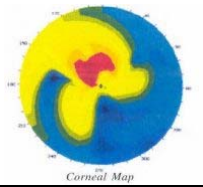
Nombre	Código	Longitud	Juego de caracteres	Dígito de control	Descripción
Código 16K		variable	ASCII	interno	Puede tener desde 2 hasta 18 renglones de alto. Creado para codificar objetos pequeños
Código QR		variable	ASCII	interno	Codifica hasta 7089 caracteres, es el más popular en el Japón, su nombre se basa en la frase “Quick Response”.
Código de barras a color de alta capacidad		Variable		Interno	Código de Barras propietario de Microsoft usado en sus productos de X-Box
3-DI		variable	ASCII	interno	Código Propietario desarrollado por Lynn Ltd.
Codigo de brras 3D (Bumpy)		variable			Cualquier código lineal que es empotrada en una superficie
Array Tag		Variable			Código propietario desarrollado por Dr. Warren D. Little de la Universidad de Victoria
Codidgo 1		variable	ASCII	interno	Hay 8 tamaños desde 1A (13 caracteres alfanumericos o 22 dígitos) hasta 1H(2218 caracteres alfanumericos o 3550 dígitos)
Código CP		Variable			Codigo propietario desarrollado por CP Tron, Inc
Data Glyphs		Variable		Interno	Código propietario desarrollado por Seros PARC
Datastrip		Variable		Interno	Conocido originalmente como Softstrip, desarrollado por Softstrip Systems y ahora propiedad de Dtastrip Inc.
Código de punto A					Tambien conocido como Codigo de puntos Philips

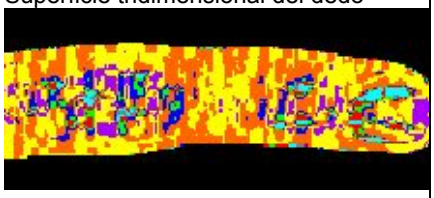
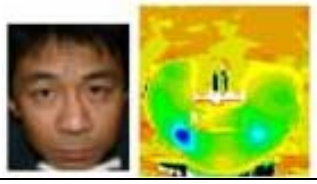
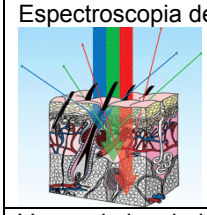
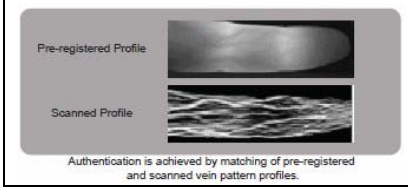
ANEXO C
Tabla de resumen tecnologías biométricas

Tecnología	Descripción	Inf. Disponible
Huella digital 	Para el manejo de la huella digital los algoritmos más usados son los de pattern y minutiae. Posibles incidencias: falta de miembro.	Patente US2530758 ISO/IEC 19794 Partes 2,3,4,8
Geometría de la mano 	Mide y compara dimensiones de la mano y dedos. Posibles incidencias: falta de miembro, edad.	Patente CH661428A5 ISO/IEC 19794 Partes 10, 12
Palma de la mano 	Al igual que la huella digital, se manejan las características que deja la huella palmar y se utilizan los mismos algoritmos de la huella digital. Posibles incidencias: falta de miembro, edad.	Patente US3581282 ISO/IEC 19794 Partes 2,3,4,8
Retina 	Esta es una tecnología considerada invasiva y consiste en el uso de rayos infrarrojos para captura y comparación de los patrones de la retina. Posibles incidencias: uso de gafas, falta de miembro.	Patente US4109237
Iris 	Captura y compara los patrones del iris Posibles incidencias: uso de gafas, falta de miembro.	Patente US4641349 US9409446 ISO/IEC 19794 Parte 6
Geometría Facial 	Captura y compara patrones faciales. Posibles incidencias: edad, cabello, luz.	ISO/IEC 19794 Partes 5, 12

Tecnología	Descripción	Inf. Disponible
Termografía facial 	Cámaras infrarrojas detectan patrones de calor creados por el flujo sanguíneo y emitido por la piel, mediante el uso de rayos infrarrojos. Posibles incidencias: cambios extremos en la temperatura ambiental.	Paper escrito por Diego A. Socolinsky, Lawrence B. Wolff, Joshua D. Neuheisel, Christopher K. Eveland.
Voz 	Hay tres formas de reconocer la voz que son la dependencia (se tiene un texto específico), texto aleatorio y la independencia del texto Posibles Incidencias: ruido, temperatura, cambios, edad.	Patente US4032711
Firma 	Se divide en dos grandes áreas: métodos estáticos (características de la firma que no cambian en el tiempo) y métodos dinámicos (características dinámicas en el proceso de la firma). Posibles incidencias: Edad, cambios, analfabetismo.	Patente US3480911, US3959769, US4035768 ISO/IEC 19794 Partes 7,11
Escaneo de venas 	Captura imágenes del patrón del flujo sanguíneo en el anverso de la mano. Posibles Incidencias: falta de miembro, edad.	Patente US5787185 ISO/IEC 19794 Parte 9
Sensor de olor 	Captura los químicos volátiles que los poros de la piel emiten, actualmente ya existen patentes de aparatos que detectan los olores y hacen comparaciones, pero no hay nada desarrollado sobre identificación de personas.	Paper escrito por Zahna Korotkaya, patentes de aparatos US6496742, US6018984, US6463786
Medidor de pulso sanguíneo 	Sensores infrarrojos miden el pulso de la sangre en el dedo. Posibles incidencias: falta de miembro, edad	Paper escrito por Lonnie C. Ludeman, Mario I. y Chacon M en 1996 para la conferencia internacional de aplicaciones y tecnologías en procesamiento de señales
Identificación de la cama de la uña 	Un interferómetro detecta las fases de cambio en la incidencia de luz en la uña del dedo; reconstruye distintas dimensiones de la cama de la uña y genera un mapa unidimensional. Posibles incidencias: falta de miembro, enfermedad.	Patente US5719950

Tecnología	Descripción	Inf. Disponible
Reconocimiento de movimiento 	Captura una secuencia de imágenes para obtener y analizar las características de movimiento de las personas. Posibles incidencias: enfermedad, condición de la superficie donde se marcha, velocidad de la marcha.	Actualmente hay dos universidades en USA, una en UK y otra en la India que están desarrollando esta tecnología
Reconocimiento de la forma de oreja 	Está basada en la distinción de la forma de la oreja y la estructura del cartílago, proyectando parte del oído externo. Tecnología usada en medicina forense. Posibles Incidencias: falta de miembro.	El programa FEARID de la Unión Europea estudió por 40 meses un procedimiento para la clasificación y comparación de huellas.
labios 	Tecnología biométrica que se divide en tres subcategorías que son huellas de los labios, movimiento de los labios y forma de los labios	Paper escrito por Zahna Korotkaya
Reconocimiento de patrones de tipeo 	Basada en la velocidad y fuerza de tipeo del teclado, los mejores resultados se han obtenido con los tiempos de presión de la tecla, aunque lo mejor es usar los tiempos de presión y los tiempos de latencia.	Patente US4805222
Dinámica del mouse 	Sistema biométrico de detección de intrusos basado en el análisis de la dinámica del mouse, se detectan diferencias de comportamiento.	Patente US2004221171
Forma de los nudillos 	Mediante el uso de una cámara de video se toma la imagen del perfil del contorno de los nudillos.	Patente US5594806
Arrugas del dedo 	Medición de las arrugas del dedo detrás de las juntas del dedo usando capacitancia electrostática	patente JP2001021309

Tecnología	Descripción	Inf. Disponible
Perfil de presión de la mano 	Método que verifica la identidad de la persona comparando una gran cantidad de medias de presión tomadas con un transducer cuando se presiona la mano contra ellos.	Patente WO03069540
Reconocimiento dinámico de asimiento 	Tecnología biométrica conductual que mide la presión que se ejerce sobre el mango del arma de acuerdo con la posición de la mano al tomar el arma.	Patente WO03098537, US6563940
Transmisión de sonido de los huesos 	Se envía un pulso sonoro a través del dedo, que es modificado por la carne y hueso, que es recibido por un micrófono y se convierte en información digital. Posibles incidencias: ausencia de miembros.	Patente US20030113001 y US7123752
Campo bioeléctrico 	Se detecta el campo bioeléctrico del cuerpo de las personas y se compara contra la plantilla en la base de datos.	Comercializado por William Olivadoti con sus modelos Biofinder II y Biofinder III
Firma bio-dinámica 	Basada en las señales bioeléctricas intrínsecas que se miden al contacto de dos dedos con el dispositivo lector.	Comercializado por Idesia como BDSTM Application Kit & BDSTM SDK, patentes WO2004012388, EP1525710, CA2494491 US7171680,
Seguimiento del movimiento del ojo 	Reconocimiento usando el movimiento de los ojos cuando sigue un objetivo en la pantalla de un computador, se requieren gafas especiales, que usan luz infrarroja, para medir los movimientos de los ojos. Posibles incidencias: falta de miembro, ceguera.	Desarrollado por el instituto de ciencias computacionales de la Universidad de Tecnología de Silesian en Polonia.
Topografía de la superficie de la cornea 	Se mide la refección de luz infrarroja sobre el centro de la cornea. Posibles incidencias: falta de miembro, gafas.	Patentes WO2004016161, EP1545291 y US2003253520

Tecnología	Descripción	Inf. Disponible
Superficie tridimensional del dedo 	Utiliza la curvatura de cada pequeña sección de la superficie del dedo, comenzando por una imagen normal. Posibles incidencias: falta de miembro.	Desarrollado por Damon L. Woodard en el laboratorio de investigación de visión de computadores, del departamento de ciencias de la computación e ingeniería de la Universidad de Notre Dame
Aproximación dinámica al reconocimiento facial 	Esta tecnología está basada en las características faciales dinámicas, donde se monitorea los movimientos de la cara durante una expresión y se obtiene un vector característico.	Proyecto en desarrollo, en el que participan la Universidad de Stony Brook y el Centro Estratégico de Seguridad de Puertos y Marítima de New York.
chip RFID biométrico basado en la uña del dedo 	El chip es capaz de detectar la capacitancia eléctrica de la uña y la carne bajo ella.	En desarrollo por FnBiometrics
Espectroscopia de la piel 	Se usa un diodo emisor de luz (LED) y fotodetectores de silicio para tomar las medidas basadas en las propiedades òpticas de la piel mediante la espectroscopia òptica de reflexión difusa.	Actualmente el centro para unificar biométricos y sensores de la Universidad del Estado de New York en Buffalo, está desarrollando estudios en el área.
Venas de los dedos  Authentication is achieved by matching of pre-registered and scanned vein pattern profiles.	Rayos infrarrojos próximos son transmitidos a través del dedo y parcialmente absorbidos por la hemoglobina en las venas para capturar un perfil único de patrón de venas.	Tecnología desarrollada por Hitachi, patente US7184576 ISO/IEC 19794 Parte 9

ANEXO D
Documentación Hotel

Registro Reservas

HOTEL RAMADA

RESERVAS

Hab	Nombre	Aerolinea	Procedencia	Vuelo	Fecha	Hora	Pick up	Noches	PX	e-mail	phone	address

Registro Consumos

HOTEL RAMADA

CONSUMOS

Ambiente: _____
Name/Nombre: _____
Room/Habitación _____ Date/Fecha _____

Cant.	Concepto	Charges
	SubTotal	
	Iva	
	Total	

Formato Pedido Desayuno

HOTEL RAMADA

BREAKFAST MENU

Name/Nombre: _____
Room/Habitación _____ Date/Fecha _____

_____ Toast, Juice, Coffee or Tea /
Tostada, Jugo, Café o Te

_____ Fried Eggs / Huevos Fritos
_____ Omelet / Omelet
_____ Scrambled / Revueltos

_____ with chesse / con queso
_____ with ham / con jamón

** comes with Toast, Juice, Cofee or Tea /
acompañados con Tostada, Jugo, Café o Te

_____ Pancakes
_____ Cereal
_____ Fruit Salad / Ensalada de Frutas

** comes with Toast, Juice, Cofee or Tea /
acompañados con Tostada, Jugo, Café o Te

Registro Lavandería

HOTEL RAMADA

LAVANDERÌA

Name/Nombre: _____
Room/Habitación _____ Date/Fecha _____

Cant.	Concepto	Charges
	Men Dress/Vestido de Paño	
	Party Dress/Vestido de Fiesta	
	Cocktail Dress/Vestido cocktail	
	Shirt/Camisa - Blusa	
	Pants/Pantalón	
	Skirt/Falda	
	T-shirt/Camiseta	
	Jacket/Chaqueta	
	Blazer/Blazer	
	Brassiere/Brassiere	
	Underwear/Panties-calzoncillos	
	Socks/Medias	
	Handkerchief/Pañuelo	
	SubTotal	
	Iva	
	Total	

Registro Libro del DAS

Habitación	Fecha	Nombre	Nacionalidad	Estado civil	Profesión	Procedencia	Permanencia	Hora	Px

Destino	Cédula	Lugar expedición	Pasaporte No.	Dirección	Teléfono	Firma

Registro Check in

PASSENGER
REGISTRATION FORM

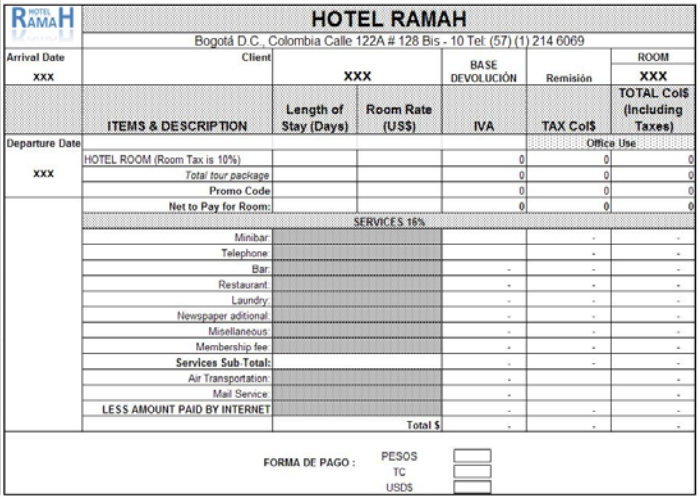
Name				Room N°	
Passport N° / CC		Place of Issue		Nationality	
Profession		City of departure		Destination	
Home Adress				Phone N°	
City		Country		E-mail	
Marital Status				Days you will stay	
Birth date: D M Y					
Name of the compang you work for:					
Arrival date: D M Y		Departure date: D M Y			

Day	Concept	Charges	Tax	Credits	Balance

Observaciones/Notes:

Recepcionist name:

Factura



HOTEL RAMAH

Bogotá D.C., Colombia Calle 122A # 128 Bis - 10 Tel: (57) (1) 214 6069

Arrival Date	Client			BASE DEVOLUCIÓN	Remisión	ROOM
xxx	xxx					xxx
	ITEMS & DESCRIPTION	Length of Stay (Days)	Room Rate (US$)	IVA	TAX Col$	TOTAL Col$ (Including Taxes)
Departure Date					Office Use	
xxx	HOTEL ROOM (Room Tax is 10%)			0	0	0
	Total tour package			0	0	0
	Promo Code			0	0	0
	Net to Pay for Room:			0	0	0
	SERVICES 16%					
	Minibar:				-	-
	Telephone:				-	-
	Bar:			-	-	-
	Restaurant:			-	-	-
	Laundry:			-	-	-
	Newspaper aditional:			-	-	-
	Misellaneous:			-	-	-
	Membership fee:			-	-	-
	Services Sub-Total:			-	-	-
	Air Transportation:			-		-
	Mail Service:			-		-
	LESS AMOUNT PAID BY INTERNET			-	-	-
			Total $	-	-	-

FORMA DE PAGO : PESOS ☐ TC ☐ USD$ ☐

Reporte DAS

Código Hotel	Código Ciudad	Tipo Documento	Número Documento	Código Nacionalidad	Primer apellido	Segundo Apellido	Nombres	Tipo de Movimiento	Fecha Entrada/Salida	País procedencia	País destino

ANEXO E
Manual del usuario

APLICATIVO HOTEL

MANUAL DEL USUARIO

TABLA DE CONTENIDO

INTRODUCCIÒN

El aplicativo para el hotel, es un aplicativo elaborado en MySQL y PHP, el cual permite sistematizar y apoyar los procesos relativos a la reserva y asignación de habitaciones, control de consumos, facturación de servicios de los huéspedes, generación de reportes para el DAS para el Hotel Ramah.

El presente manual hace referencia a la forma de navegación dentro de de la aplicación, describiendo los pasos que deberá seguir un usuario final del software para ingresar reservas, huéspedes, consumos, consultar la disponibilidad de habitaciones, cuenta del cliente, así como el proceso de generar reportes para el DAS.

El aplicativo puede utilizar código de barras EAN-13 para los productos comercializados y la huella digital para el control de huéspedes tanto en consumo como en el reemplazo eventual de la llave de la habitación.

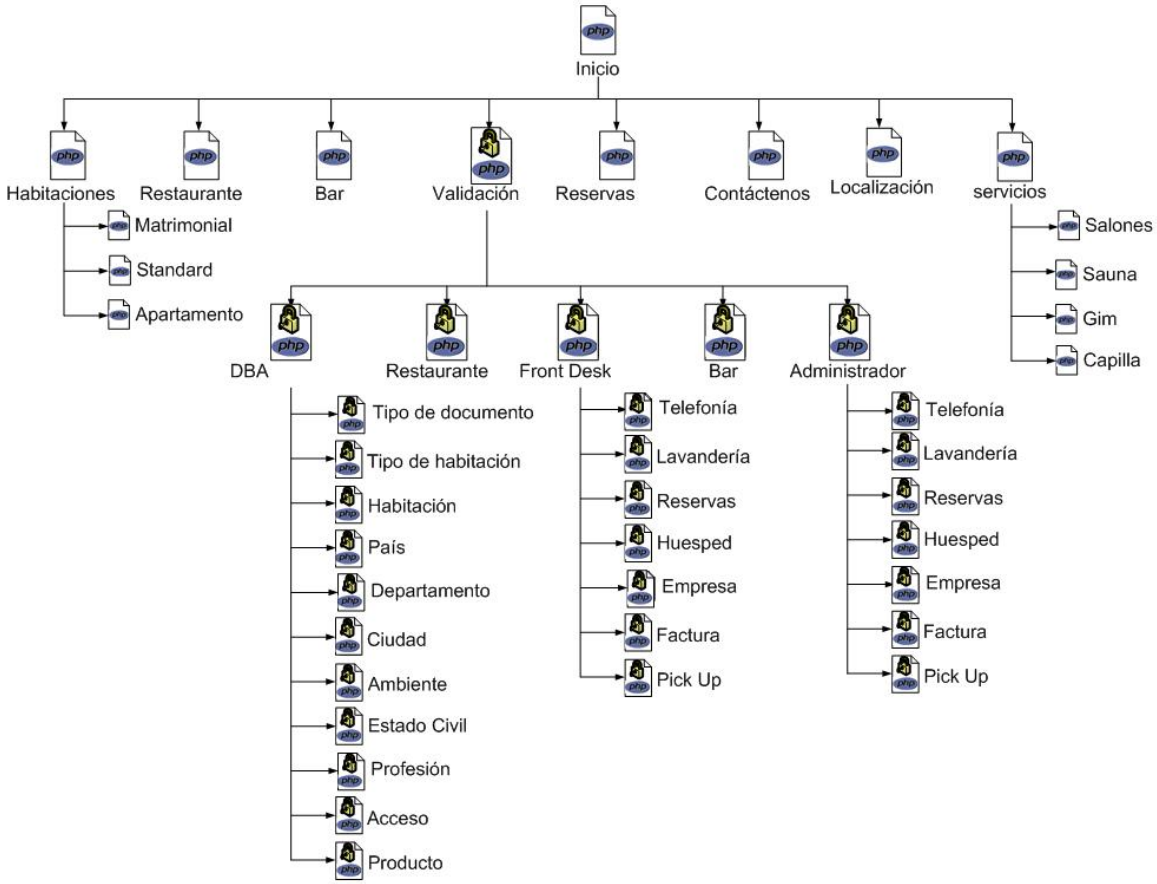
El manejo de usuarios se hace a partir de las áreas de trabajo (recepción, restaurante, bar, lavandería, administración).

1. ENTORNO GENERAL DEL APLICATIVO DEL HOTEL

El aplicativo posee un entorno de navegación para un ambiente web.

El aplicativo cuenta con un sitio web público en el que se ofrecen los servicios del hotel y el huésped puede interactuar con una página donde puede generar su reserva.

Hay una segunda parte que se puede acceder via internet y en la que se requiere la validación del usuario, esta segunda parte es la que acceden los empleados del hotel de acuerdo al rol que tengan.



MAPA DE NAVEGACÍÓN DE LA APLICACIÓN

El usuario Restaurante sólo tiene derecho a ingresar consumos de los clientes en el ambiente del Restaurante.

El usuario Bar sólo tiene derecho a ingresar consumos de los clientes en el ambiente del Bar.

El usuario Lavandería sólo tiene derecho a ingresar consumos de los clientes en el ambiente de la Lavandería (actualmente no habilitado).

El usuario Recepción sólo tiene derecho a ingresar consumos de los clientes en el minbar, lavandería, telefonía y Otros; generar las facturas, reportes del DAS; ingresar reservas, clientes, empresas; consultar la ocupación del hotel.

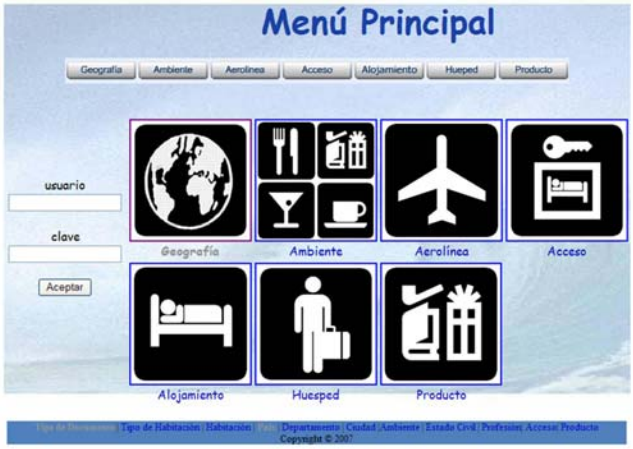
El usuario administrador tiene derecho a consultar todos los informes generados por la aplicación y la información que el usuario considere pertinente que le sea asignada.

2. FORMULARIOS

2.1 DBA

El administrador del sistema será el encargado de ingresar la información básica del aplicativo y manejar los permisos asignados a los empleados

2.1.1 Menú principal



MENÚ PRINCIPAL DBA

En el menú podrá acceder a los distintos formularios dando click en la imagen o en el nombre o en el botón o en el hipervínculo a pie de página.

En las imágenes principales y en los botones se agruparon algunas opciones:

- Geografia reúne las opciones que manejan la información de país, departamento y ciudad.
- Huesped que reúne las opciones tipo de documento, estado civil y profesión.
- Alojamiento que tiene las opciones tipo de habitación y habitaciones.
- Producto que tiene la opcion de insertar separda de la de borrar y actualizar, teniendo en cuenta que al crear un producto se le debe crear un código de barras y asignarle un ambiente donde se comercializará y estas características son inmodificables en el producto.

2.1.2 Opciones

En las distintas opciones se da la posibilidad de ingresar, modificar y eliminar la información que en ella se maneja.

Del menú la opción geografía, huésped y alojamiento presentan menús en la columna izquierda donde se muestran las distintas opciones de estas opciones

PÁGINA PAÍS

PÁGINA AMBIENTE

PÁGINA AEROLÍNEA

PÁGINA ACCESO

PÁGINA TIPO DE HABITACIÓN

PÁGINA PROFESIÓN

PÁGINA PRODUCTO

2.2 Administrador

Administradores donde se encuentra el personal del área de contabilidad y la gerencia del hotel y son quienes tienen acceso a ver la información generada por el sistema

MENÚ PRINICPAL ADMINISTRADOR

En el menú podrá acceder a los distintos informes dando click en la imagen o en el nombre o en el botón o en el hipervínculo a pie de página.

2.3 Front Desk

Es el personal que atiende la recepción del hotel y son los encargados de generar reservas, realizar los cargos de telefonía y lavandería, son los encargados de completar la información de los huéspedes que llegan al hotel, de las empresas que cancelan las cuentas de los huéspedes, de despachar los conductores que recogen en el aeropuerto a los huéspedes que soliciten este servicio.

2.3.1 Menú principal

MENÚ PRINICPAL ADMINISTRADOR

En el menú podrá acceder a los distintos formularios dando click en la imagen o en el nombre o en el botón o en el hipervínculo a pie de página.

2.3.2 Opciones

En las distintas opciones se da la posibilidad de ingresar, modificar y eliminar la información que en ella se maneja.

PÁGINA CARGOS

PÁGINA RESERVAS

PÁGINA HUESPED

PÁGINA EMPRESA

2.4 Bar y Restaurante

Aunque son roles diferentes la interfaz es la misma, pero presenta productos diferentes y de acuerdo al ambiente que se ésta trabajando, quienes atienden estos ambientes sólo tienen la opción de cargar los consumos y para ello es indispensable validar al cliente mediante la huella digital y los productos se cargan con la lectura del código de barras de los productos.

PÁGINA DE CONSUMOS