Universidad del Aconcagua.

Facultad de Ciencias Sociales y Administrativas.

Licenciatura en Informática.

“Autenticación Biométrica por Huella Dactilar en Estadios.”

Autor:
Juan Pablo Butrón

Legajo:
16.677

Tutor:
Ing. Guillermo Sandez

Calificación

Índice de Contenidos

RESUMEN EJECUTIVO

A lo largo de este proyecto, se logró establecer el diseño de una solución tecnológica para implementar la autenticación biométrica en estadios de fútbol, y de esta manera complementar los actuales sistemas de control de acceso. Para ello se describió los inicios o bases teóricas de la identificación por huella dactilar, exponiendo todo el proceso de identificación de personas a través de las huellas dactilares utilizando tecnologías digitales. Teniendo en cuenta estos basamentos, se determinó cuáles deben ser los dispositivos de adquisición de huellas dactilares a ser utilizados y también cómo deben ser integrados a los controles. Luego se seleccionó tanto el hardware y software a ser desarrollado para sustentar la implementación de la totalidad del sistema, como así también las telecomunicaciones a ser requeridas. Respecto al software específico, se analizó de forma acabada su desarrollo estableciendo la descripción y plan del proyecto de software, especificaciones de requerimientos como así también los documentos de diseño. Finalmente se determinó conveniencias tanto económicas, culturales como tecnológicas para su realización, estableciendo la viabilidad del proyecto en su conjunto.

INTRODUCCION

El propósito del presente trabajo fue el de diseñar una solución integral para implementar la autenticación biométrica en estadios de fútbol, complementando así los actuales sistemas de ingreso basados en controles de acceso convencionales.

Nunca se ha realizado chequeo para comprobar la identidad de las personas que ingresan a los estadios de fútbol. Teniendo en cuenta esta situación se pretendió brindar una solución tecnológica que permitiera restringir el acceso a personas con “Prohibición de Concurrencia a Espectáculos Deportivos”.

La incorporación de tecnología biométrica al acceso permitirá la verificación de un individuo en forma automática, con velocidades de procesamiento y toma de decisiones acorde a las exigencias en los tiempos de respuesta. Contando con información previamente suministrada por el orden público se determinará si está habilitado para el ingreso al estadio y el sistema aprobará el acceso al mismo.

La cobertura del proyecto comprendió el estudio y análisis de la tecnología de identificación biométrica por huellas dactilares, comprobando la precisión o fiabilidad del sistema de autenticación. Respetando las exigencias en tiempos de respuesta, se diseñó una solución tecnológica en un sistema modelo de hardware y software aplicado; evaluando la viabilidad económica del proyecto.

Objetivo General

Diseñar una solución tecnológica integral para implementar la autenticación biométrica al ingreso en estadios, teniendo como premisas la exactitud y los tiempos de respuesta acordes a las exigencias del caso.

Objetivos Específicos

- Estudiar, analizar y describir la identificación por huella dactilar.
- Estudiar, analizar y seleccionar las diferentes tecnologías existentes en el mercado de la identificación biométrica de huellas dactilares.

- Estudiar, analizar y seleccionar el software y hardware de mercado requerido para integrar la autenticación biométrica con controles de acceso electromecánicos.
- Investigar la tecnología, tipo, seguridad y ancho de banda de las telecomunicaciones necesarias para realizar la implementación.
- Presentar un esquema de diseño del sistema.
- Describir los diversos factores que impactan el proyecto para determinar conveniencias económicas, culturales y tecnológicas de la solución planteada.

Justificación

El motivo de este trabajo se basó fundamentalmente en la premisa de brindar ayuda para resolver la inseguridad en eventos deportivos tales como partidos de fútbol. Contar con un sistema fiable de control de acceso a personas a los estadios de fútbol ayuda a brindar una solución a esta problemática y a aplicar leyes vigentes.

Los grandes avances en las tecnologías de autenticación biométrica y su seguridad relacionada permite la completa integración con el actual control de acceso a través de molinetes electromecánicos.

Las huellas dactilares durante muchos años han sido uno de los métodos más usados para el reconocimiento de personas; pero solamente en estos últimos años los sistemas de comprobación biométricos automatizados han estado disponibles. Los avances realizados por la industria, las necesidades de los gobiernos (migraciones, aduanas, pasos fronterizos), y las organizaciones de los estándares internacionales han conducido a grandes avances en reconocimiento de huellas dactilares, que prometen dispositivos cada vez más rápidos y de más alta calidad de adquisición para proporcionar una exactitud más alta y de mayor confiabilidad. Las huellas dactilares como método de identificación tienen una aceptación amplia entre el orden público, la comunidad de ciencia forense, y las personas en general por lo que continuarán siendo utilizadas en los sistemas de muchas empresas, gobiernos e instituciones, para los usos y aplicaciones que requieren una biometría confiable.

CAPÍTULO I - IDENTIFICACION POR HUELLA DACTILAR

1.1 Reseña histórica

El uso práctico de huellas dactilares como método de identificación de individuos ha sido utilizado desde finales del siglo XIX cuando Sir Francis Galton desarrolló un estudio de rigor científico con la aplicación de métodos estadísticos, a partir del cual demostró la imposibilidad de coincidencia entre dos huellas dactilares de forma absoluta. Dicho de otra manera: demostró de forma analítica la no existencia de dos huellas dactilares iguales y confirmó su exclusividad[1].

A finales de los años 60 la identificación por huella dactilar comienza su transición a la automatización, con la llegada de las computadoras, el subconjunto de los puntos estudiado por Galton fue utilizado para desarrollar la tecnología de reconocimiento automatizado de huellas dactilares.

En 1975, el FBI (Federal Bureau Investigation) fundó el desarrollo de escáneres de huella dactilar para clasificadores automatizados y tecnología de extracción de minucias o puntos característicos, lo cual condujo al desarrollo de un lector prototipo. Este primer lector usaba técnicas capacitivas para recoger las minucias[2]. En ese momento sólo los datos demográficos de los individuos, la clasificación de los datos de huellas dactilares y las minucias[3] eran almacenados a causa de que el costo de almacenamiento de las imágenes digitales de las huellas dactilares era prohibitivo.

Durante las siguientes décadas, el NIST (National Institude of Standards and Technology) se enfocó y condujo a desarrollos en los métodos automáticos para digitalizar las huellas dactilares en tinta y los efectos de compresión de imagen en la calidad de la imagen, la clasificación, extracción de minucias, y concordancia[4]. El trabajo del NIST condujo el desarrollo del algoritmo M40, el primer algoritmo operacional utilizado en el FBI para reducir la búsqueda de personas. Los resultados producidos por el algoritmo M40 fueron provistos a técnicos entrenados y especializados quienes evaluaron un grupo significantemente más pequeño de imágenes candidatas.

---

[1] TAPIADOR MATEOS, Marino y SIGUENZA PIZARRO, Juan A. Tecnologías biométricas aplicadas a la seguridad (Madrid, España, 2005).
[2] RATHA, Nalini y BOLLE, Ruud. Automatic Fingerprint Recognition Systems (New York, 2004).
[3] Minucias: discontinuidades locales en el patrón de la huella dactilar que corresponden esencialmente a las terminaciones y a las bifurcaciones de las líneas del canto de la huella dactilar.
[4] WAYMAN, James. Biometric Systems Technology, Design and Performance Evaluation (London, 2005).

La tecnología de huellas dactilares disponible continuó mejorando y para el año 1981, cinco sistemas automatizados de identificación por huella dactilar fueron desplegados. Varios sistemas estatales en los Estados Unidos y otros países habían implementado sus propios sistemas autónomos, desarrollados por un número de diferentes proveedores. Durante esta evolución, la comunicación y el intercambio de información entre sistemas fueron pasados por alto, significando que una huella digital recogida con un sistema no podía ser buscado en otro sistema. Estas prácticas llevaron a la necesidad y al desarrollo de estándares para huellas digitales.

Conforme a la necesidad de un sistema de identificación integrado en la comunidad de la justicia criminal de los Estados Unidos se volvió rápidamente evidente, la próxima fase en la automatización de huellas dactilares, la ésta ocurrió al finalizar la competencia de Sistemas Automatizados de Identificación de Huellas Dactilares (Automated Fingerprint Identification System, AFIS). La competencia identificó e investigó tres desafíos principales: 1: adquisición de huellas dactilares digitales, 2: extracción de características de crestas, y 3: concordancia de patrones de características de crestas[5]. Los sistemas modelo demostrados fueron evaluados en base a requerimientos de rendimientos específicos. La empresa Lockheed Martin fue seleccionada para construir el segmento AFIS del proyecto IAFIS del FBI. Los módulos principales de IAFIS estuvieron desarrollados y puestos en funcionamiento para 1999. A la par, también en este plazo, los productos comerciales de verificación de huellas dactilares comenzaron a aparecer para controles de acceso, para autenticación, y para beneficio de las funciones de verificación o autenticación.

1.2 Principales exponentes de la Dactiloscopia[6]

Francis Galton

Fue un explorador y hombre de ciencia inglés con un amplio espectro de intereses. No tuvo cátedras universitarias y realizó la mayoría de sus investigaciones por su cuenta. Sus múltiples contribuciones recibieron reconocimiento formal cuando, a la edad de 87 años, se le concedió el título de "Sir" o caballero del Reino Unido.

Galton fue el primero en proyectar una clasificación y división de los dibujos papilares, pero dejó sus estudios inconclusos, pues si bien anunció que las impresiones dactilares podían ser ordenadas al estilo de un diccionario, no determinó el método que se emplearía para ello; sin

[5] MALTONI, Davide y otros. Handbook of Fingerprint Recognition (New York, 2005).
[6] Dactiloscopia: Estudio de las impresiones digitales, utilizadas para la identificación de las personas.

embargo afirmó que eran un medio seguro para identificar a las personas, puesto que los dibujos eran inalterables y distintos en cada individuo.

Juan Vucetich

Nació en 1858 en territorio de la actual Croacia. Fue criminalista y creador del sistema dactiloscópico argentino. Murió en Buenos Aires – Argentina en 1925. Juan Vucetich creó un sistema de clasificación de los dibujos dactilares.

Juan Vucetich emigró hacia la Argentina, a los 24 años. En 1888, ingresó en la Policía de la Provincia de Buenos Aires. Hasta entonces, la técnica utilizada para la individualización de las personas era el método antropométrico, ideado por el francés Bertillon. El Bertillonage (deficiente e inseguro), basado en las medidas de ciertas partes del cuerpo humano y las particularidades fisonómicas, era utilizado como instrumento de las investigaciones por la policía de Francia desde 1882. La policía argentina consideró necesario instalar una oficina que se ocupara de las funciones relacionadas con la identificación de las personas.

Sabiendo que el método empleado, hasta la fecha, era el Bertillonage, Vucetich lo adoptó para instalar y organizar el Gabinete Técnico Policial que se le encargara. Pero al aproximarse al tema de las estrías papilares de los dedos, comenzó a dedicarse intensamente a su estudio. Hasta entonces no conocía absolutamente nada sobre impresiones dactilares, pero igualmente se dedicó a la tarea de obtener impresiones dactilares nítidas para hacer un análisis comparativo y buscar la manera de utilizarlas en el servicio de identificación.

El intenso estudio que efectuó, tomando como base lo ideado por Francis Galton, lo llevó a corroborar las ideas de aquél, es decir que los dibujos papilares podían ser clasificados por grupos. Al mismo tiempo que dirigía la Oficina de Identificación Antropométrica, Vucetich acumuló gran cantidad de impresiones dactilares. Y es así como a la par del Servicio Antropométrico, dio forma y organizó el servicio de identificación por medio de las impresiones dactilares, en 1891. Además inventó los elementos necesarios para captar lo más perfectamente posible los dibujos dactilares de los dedos de ambas manos y puso en práctica todo cuanto fue necesario para sistematizar el método.

En 1911 una ley nacional ordenó el enrolamiento general de los ciudadanos, utilizando el método “Vucetich” para individualizar y clasificar a las personas. Luego, Vicetich fue nombrado perito identificador y director del Registro Nacional de Identificación, que con algunas variantes, es hoy el Registro Nacional de las Personas (RENAPER) en la Argentina.

Henry Faulds

Henry Faulds fue un médico y misionero escocés pionero de la identificación de la personas a través de las huellas dactilares. Nació el 1 de junio de 1843 en la ciudad de Beith, Ayrshire, situada al norte de Escocia.

En 1880, Faulds publicó un ensayo sobre el comportamiento de las huellas dactilares, en el que observó que podrían ser utilizados para identificar, localizar y capturar a criminales, haciendo inclusive una propuesta a las autoridades locales. Poco tiempo después Sir Guillermo Herschel, funcionario británico que trabajaba en la India, publicó un estudio explicando la forma en que podían ser aprovechados ciertos signos biométricos, como las huellas dactilares y la firma para la identificación de personas.

En 1886, Faulds volvió a Gran Bretaña y ofreció su sistema de identificación personal a Scotland Yard de Escocia, que por cierto resultó rechazada. Dos años más adelante, sin embargo, Faulds entregó una nueva propuesta a la institución, comprobando que sus estudios habían sido anteriores a los efectuados por Herschel, el cual se difundió y constituyó el motivo de una batalla legal entre Faulds y Herschel que se prolongó hasta 1917, cuando Herschel confesó que Faulds había sido el primero para sugerir un uso forense para las huellas digitales. Faulds murió en 1930, sin reconocimiento a sus méritos científicos, y sin siquiera imaginar que el sistema que creó sería el utilizado en la identificación de personas en Estados Unidos e Inglaterra.

1.3 Caracterización y clasificación de las huellas dactilares

1.3.1 Características

Una huella dactilar usualmente aparece como una serie de líneas oscuras que representan los relieves, la porción saliente de las crestas, mientras los valles entre estas crestas aparecen como espacio en blanco y están en bajo relieve, la porción subyacente de las crestas de fricción.

La huella dactilar se manifiesta a partir del sexto mes del desarrollo del embrión como consecuencia de un proceso aleatorio, no genético, por lo que se puede afirmar que no existe ningún tipo de correlación entre gemelos idénticos o individuos de una misma familia. Son además invariantes con el tiempo: el dibujo papilar crece proporcionalmente según el desarrollo físico corporal, sin alterar el número, el grado de curvatura, ni la situación de las crestas presentes en la misma. Así, no se podrán modificar fisiológica, voluntaria o patológicamente, son, por tanto verdaderas características invariantes, particulares y unívocas propias del individuo, perfectamente válidas en procesos de identificación de personas.

De todas formas, existen diferentes sectores de la población que presentan claras dificultades para posibilitar una correcta adquisición y posterior identificación a partir de sus huellas dactilares. A continuación se detalla algunos colectivos sensibles a presentar este tipo de problemas:

- Colectivos étnicos: los dedos de los asiáticos tienen las crestas muy pequeñas y finas, hecho que dificulta en gran medida su adquisición. Este problema también se detecta en personas de edad avanzadas.
- Colectivos profesionales: la gente que trabaja con sus manos (albañiles, carpinteros, herreros, agricultores), pueden presentar callosidades que dificulten el proceso de adquisición, así como aquellos profesionales que manejan productos químicos de naturaleza corrosiva (cáustica o abrasiva).

La identificación por huella dactilar está basada principalmente en las **minucias**, o la ubicación y dirección de los finales y bifurcaciones (separaciones) de las crestas a lo largo su trayectoria (Figura 1.1).

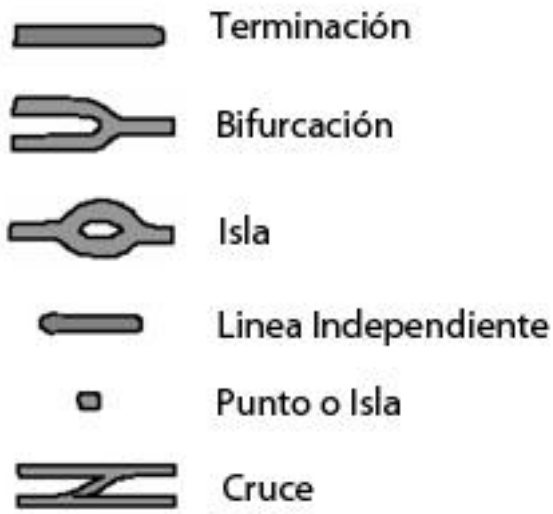
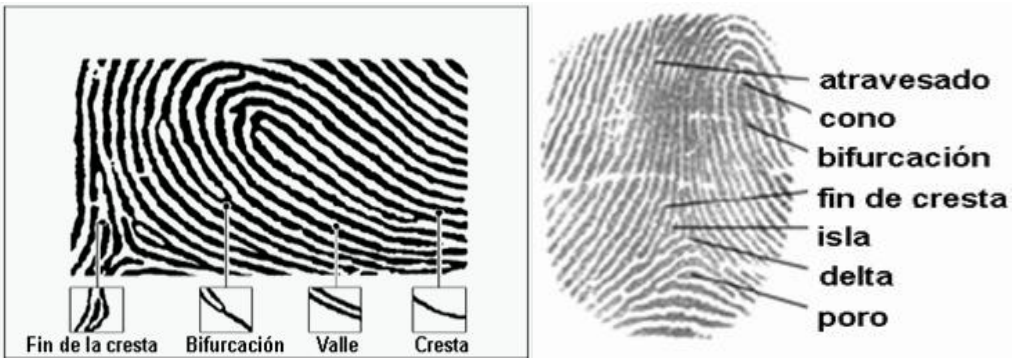


Figura 1.1. Tipos de minucias.

En la Figura 1.2 se presentan ejemplos de características de huellas dactilares: (a) cuatro tipos de minucias y (b) ejemplos de otras características algunas veces utilizadas durante la clasificación automática y procesos de extracción de minucias.



a) Minucias b) Otras características

Figura 1.2. (a) Cuatro tipos de minucias y (b) ejemplos de otras características

Siguiendo con el estudio morfológico de las huellas dactilares, se encuentran dos singularidades presentes en algunas huellas, en función de su tipología, denominadas Core (Núcleo) y Delta (Figura 1.3).

El Core responde al punto localizado en la zona nuclear de la huella, donde una de las crestas cambia bruscamente su dirección y describe un ángulo de 180º, retorna, por tanto, a la posición de origen. Este punto se utiliza como punto de referencia a partir del cual se cuentan el número de crestas a considerar en un análisis dactiloscópico concreto.

El Delta es un punto característico del dibujo papilar de algunas huellas que puede presentar forma de triángulo o de trípode, está formado por la aproximación o fusión de las crestas existentes en la zona frontera entre las zonas marginal, basilar y nuclear de la huella. Su importancia radica en que la zona donde se halla ubicada, así como en sus proximidades, aparecen muchos puntos característicos. Además, esta singularidad se utilizará para realizar una primera clasificación de las huellas dactilares.

Figura 1.3. Identificación de los puntos Core (Núcleo) y Delta sobre la huella dactilar

1.3.2 Clasificación
Henry

Todos los dactilogramas coinciden en el hecho de que las crestas papilares no describen formas aleatorias, sino que se agrupan hasta llegar a construir sistemas definidos por la uniformidad de su orientación y figura. Se puede distinguir con total claridad seis grupos o clases distintas de configuraciones dérmicas, según la denominada Clasificación de Henry.

Asimismo, estas clases pueden estar incluidas dentro de un sistema de clasificación superior, en función del número de deltas presentes en las huellas, se catalogarán así: *Adeltas*, si las huellas no presentan ningún delta (este grupo egloba aproximadamente el 20% del total de las huellas dactilares), Monodeltas, si presentan un único delta (aproximadamente 50% del total de huellas), o Bideltas, si presenta un total de dos deltas (aproximadamente 30% del total de huellas).

A continuación se detalla las seis clases propias de la clasificación de Henry (Figura 1.4), así como un conjunto de ejemplos de las morfologías correspondientes a cada una de ellas:

a) Arco: subtipo del Grupo Adelta
b) Arco Pronunciado: subtipo del Grupo Adelta
c) Bucle hacia la Derecha: subtipo del Grupo Monodelta
d) Bucle hacia la Izquierda: subtipo del Grupo Monodelta
e) Doble Bucle: subtipo del Grupo Bidelta
f) Remolino: subtipo del Grupo Bidelta

		
Arco	Arco Pronunciado	Bucle hacia la Derecha
		
Bucle hacia la izquierda	Doble Bucle	Remolino

Figura 1.4: clasificación de Henry de Huellas Dactilares

Vucetich

Vucetich ideó una clasificación básica de cuatro conformaciones las cuales llamó Arco A-1, Presilla interna I-2, Presilla externa E-2, y Verticilo V-4.

A continuación se detalla las cuatro clases propias de la clasificación Vucetich, así como un conjunto de ejemplos de las morfologías correspondientes a cada una de ellas

Arcos: Sus crestas van de un lugar a otro, sin regresar sobre sí mismas, son levemente arqueadas y carecen de deltas. Se clasifican como A-1 (Figura 1.5).

Figura 1.5: Arcos.

Presillas Internas: Cuenta con un delta, que es visto por el observador del lado derecho, las crestas papilares que forman el núcleo, nacen a la izquierda y van a correr hacia la derecha y dan

vueltas sobre sí mismas. El núcleo está formado por una horquilla, se les clasifica como I-2 (Figura 1.6).

Figura 1.6: Presillas internas

Presillas Externas: Cuenta con un delta, que es visto por el observador al lado izquierdo, las crestas papilares que forman el núcleo nacen a la derecha y van a correr hacia la izquierda y dan vueltas sobre sí mismos. Se les clasifica como E-3 (Figura 1.7).

Figura 1.7: Presillas externas

Verticilo: Su característica más importante es que cuenta con dos o más deltas, uno derecho y otro izquierdo, sus núcleos adoptan diversas formas, pero especialmente las circulares concéntricas y ovoides concéntricas. Se las clasifica como V-4 (Figura 1.8).

Figura 1.8: Verticilo

1.4 Dispositivos de Adquisición Electrónicos

En el mercado actual, existen una gran variedad de dispositivos de captura de huellas dactilares. Todos ellos obedecen a escaners del tipo *inkless*, es decir, dispositivos que posibilitan la adquisición de las huellas sin necesidad de calcar los dibujos papilares previamente entintados.

De acuerdo al método de captura, a continuación se describen distintos tipos de sensores existentes en la actualidad.

Ópticos Reflexivos

Esta técnica consiste en colocar el dedo sobre una superficie de cristal o un prisma que está iluminado por un diodo LED. Cuando las crestas de las huellas del dedo tocan la superficie, la luz es absorbida, mientras que entre dichas crestas se produce una reflexión total. La luz resultante y las zonas de oscuridad son registradas en un sensor de imagen.

La tecnología óptica utiliza un sensor de imagen CCD (Couple Charge Device o Dispositivo de Acoplamiento de Carga - Figura 1.9) como elemento responsable de la captación de la imagen una vez recorrido un pequeño juego de lentes. Este dispositivo electrónico está implementado mediante una matriz de fotosensores o elementos fotosensibles encargados de convertir la radiación luminosa en una tensión proporcional a la misma. Los parámetros que determinan la calidad del sensor CCD son la resolución o número de píxel que conforman la imagen generada por el CCD, el tamaño y el factor de ruido.

En la práctica existen algunas dificultades con esta técnica: las imágenes obtenidas con dedos húmedos y secos son muy diferentes y, además, el sistema es sensible al polvo y a la suciedad de la superficie. En este sistema si la piel está deteriorada o dañada, la huella no se reconoce correctamente. El reconocimiento de la huella dactilar de las personas mayores también es difícil de hacer ya que la piel no es lo suficientemente elástica. En algunas circunstancias esto puede producir un reconocimiento falso. Si la huella almacenada fue tomada con menos presión, se pueden producir aceptaciones falsas.

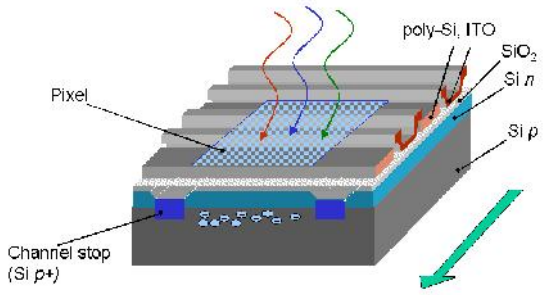


Figura 1.9: Versión simplificada en 3D de un sensor CCD

Capacitivos

El sensor es un circuito integrado de silicio cuya superficie está cubierta por un gran número de elementos transductores (o píxeles), con una resolución típica de 500 dpi. Cada elemento contiene dos electrodos metálicos adyacentes. La capacidad entre los electrodos, que forma un camino de realimentación para un amplificador inversor, se reduce cuando el dedo se aplica sobre dicha superficie: se reduce más cuando detecta crestas y menos cuando detecta el espacio entre ellas.

Esta tecnología utiliza un sensor de tipo electromagnético. El sistema detecta la diferencia de capacidades presentes entre la huella y el propio sensor. Cabe notar en este apartado, que las características eléctricas más importantes de la piel humana son la impedancia y la capacidad, siendo su modelo eléctrico equivalente, igual a una matriz de resistores y capacitores en paralelo. A continuación se muestra la implementación física del sensor descrito:

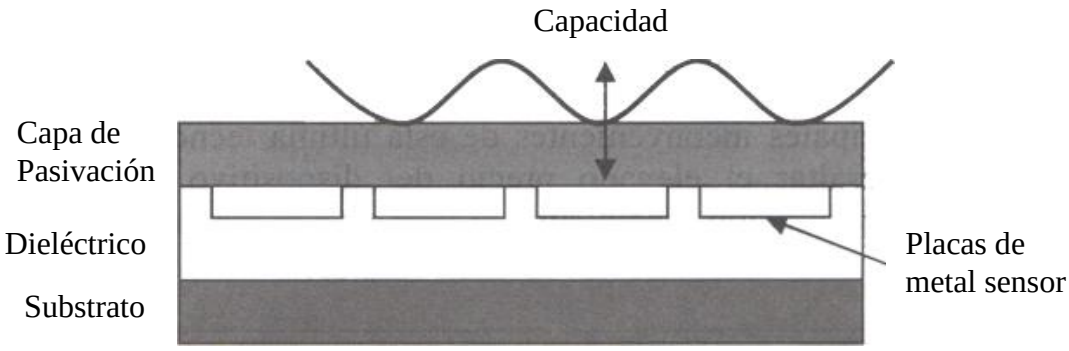


Figura 1.10. Arquitectura típica del sensor capacitivo

Cada metal sensor mide la capacidad existente entre él y la zona de la piel en contacto con la platina (crestas), y la traduce a niveles de gris. Cabe notar que el sudor humano presenta una muy elevada constante dieléctrica, hecho que producirá la saturación del sensor en una huella húmeda (adquisición demasiado negra), mientras que la excesiva sequedad de la misma provocará una captura difuminada (excesivamente blanca).

Este sensor es susceptible a las descargas electrostáticas. Estos sensores sólo trabajan con pieles sanas normales, ya que no son operativos cuando se utilizan sobre pieles con zonas duras, callos o cicatrices. La excesiva humedad, grasa o el polvo también pueden afectar a su funcionamiento. En este trabajo se ha seleccionado este tipo de sensor por adaptarse a las exigencias del caso.

Figura 1.11. Sensor capacitivo

Térmicos

Estos sensores están construidos con materiales termo-eléctricos capaces de crear corrientes a partir de diferencias de temperatura. En este caso se detecta el calor conducido por el dedo, el cual es mayor cuando hay una cresta que cuando hay un valle. Se ha desarrollado un componente de silicio con una matriz de píxeles denominado "FingerChip", es decir, "circuito integrado dedo", cada uno de los cuales está cubierto con una capa de material piroeléctrico en el que un cambio de temperatura se traduce en un cambio en la distribución de carga de su superficie. La imagen en escala de grises tiene la calidad adecuada incluso con el dedo desgastado, con suciedad, con grasa o con humedad. El sensor dispone de una capa protectora robusta y puede proporcionar una salida dinámica imprecisa.

De campo eléctrico

Estos dispositivos están formados por un anillo emisor de señal sinusoidal de baja potencia, bajo el cual se distribuye una matriz de pequeñas antenas receptoras. La amplitud de señal recibida por cada antena se modifica al producirse el contacto del dedo con el escáner, pudiendo a partir de esta información, diferenciarse el patrón de crestas y valles. La dermis de la piel es la capa causante de los cambios de amplitud en la señal.

Piezoeléctricos

La superficie de estos dispositivos es sensible a la presión ejercida durante el contacto dedo-sensor. Esta superficie está compuesta por un material elástico, de naturaleza piezoeléctrica, que proporciona las características topográficas del relieve de la huella dactilar al convertir las diferencias de presión en diferencias de tensión eléctrica. Presentan el inconveniente de no ser muy sensible a las pequeñas diferencias de relieve que pueden darse en el patrón de crestas y valles; sensibilidad que se ve aún más reducida por la cubierta protectora. Además, la imagen entregada por el sensor es binaria, lo que supone una pérdida muy significativa de información.

Ultrasónico

El sistema envía un barrido de ondas ultrasónicas (mayores de 20khz) que rebotan sobre la base de la huella. Esta tecnología se basa en la diferencia de impedancia acústica existente entre las crestas y los valles de la huella, lo que convierte en una tecnología más resistente que las anteriores,

a posibles ataques al sistema ya que realiza una lectura tridimensional de la huella producida por la presencia de partículas ajenas en la piel en la platina de escaneo.

Para cada nivel de superficie, las ondas ultrasonoras son reflectadas parcialmente y, por tanto, traspasadas también de forma parcial. Esta penetración de las ondas produce señales de retorno en sucesivas profundidades posibilitando de esta forma, la medida de la profundidad de los valles presentes entre crestas continuas de la huella. Debe notarse también que este sistema de adquisición, responde a un sistema de captación no invasivo, ya que trabaja con ondas de presión acústica, no electromagnética.

1.5 Reconocimiento de Huellas Dactilares

Las técnicas de reconocimiento de huellas se dividen en dos categorías: las técnicas analíticas basadas en las minucias, y las globales u holísticas basadas en la correlación. La principal características del primer sistema de reconocimiento radica en la difícil tarea de extracción de las minucias en imágenes de bajas calidad, mientras que el segundo sistema precisará de la implementación de algoritmos de alineación altamente exactos; es, por tanto, una técnica muy sensible a traslaciones y rotaciones de la huella durante el proceso de captura. Nótese que en el caso particular de las huellas dactilares, no existirá el problema de escala, ya que el proceso de captura de las mismas se realiza a la misma distancia, o sea sobre un papel o un escáner específico tipo inkless, y por tanto, siempre presentarán el mismo tamaño. También existen sistemas que combinan ambos métodos: extraen las minucias de las huellas y posteriormente, un fragmento de las mismas; una vez comparadas las minucias, pasan a realizar la comparación de estos fragmentos.

En este trabajo se analizará la técnica basada en minucias por ser la más amplia en su utilización y selección.

El proceso básico para la verificación e identificación de personas a partir de la huella dactilar es.

- Captura de la huella: este proceso es dependiente del dispositivo de captura, y permite almacenar la imagen de una o varias huellas dactilares para su posterior análisis.
- Creación del modelo: se extraen las minucias o puntos característicos de la huella presentes en la imagen adquirida y se almacenan en un archivo que se denomina patrón, modelo o planilla de la huella, necesario para la posterior comparación con la huella a reconocer.

- Comparación del modelo: en este proceso cabe distinguir si está realizando una tarea de verificación o identificación de huellas dactilares. En el primer caso se compara la planilla de referencia con la huella candidata una vez parametrizada, es decir una vez extraído el conjunto de minucias presentes en la misma. En el segundo caso se comparara la huella candidata parametrizada, con el total de plantillas presentes y almacenadas en la base de datos del sistema de identificación.
- Autenticación / Identificación: la autenticación (Figura 1.12) se llevara a cabo a partir del numero obtenido en el proceso anterior (normalmente entre 0 y 1), relativo al nivel de semejanza entre el modelo de referencia y el modelo candidato. Este número de semejanza se comparara con el umbral de seguridad establecido por el sistema; como resultado de dicha comparación se obtendrá la verificación o no del individuo candidato.

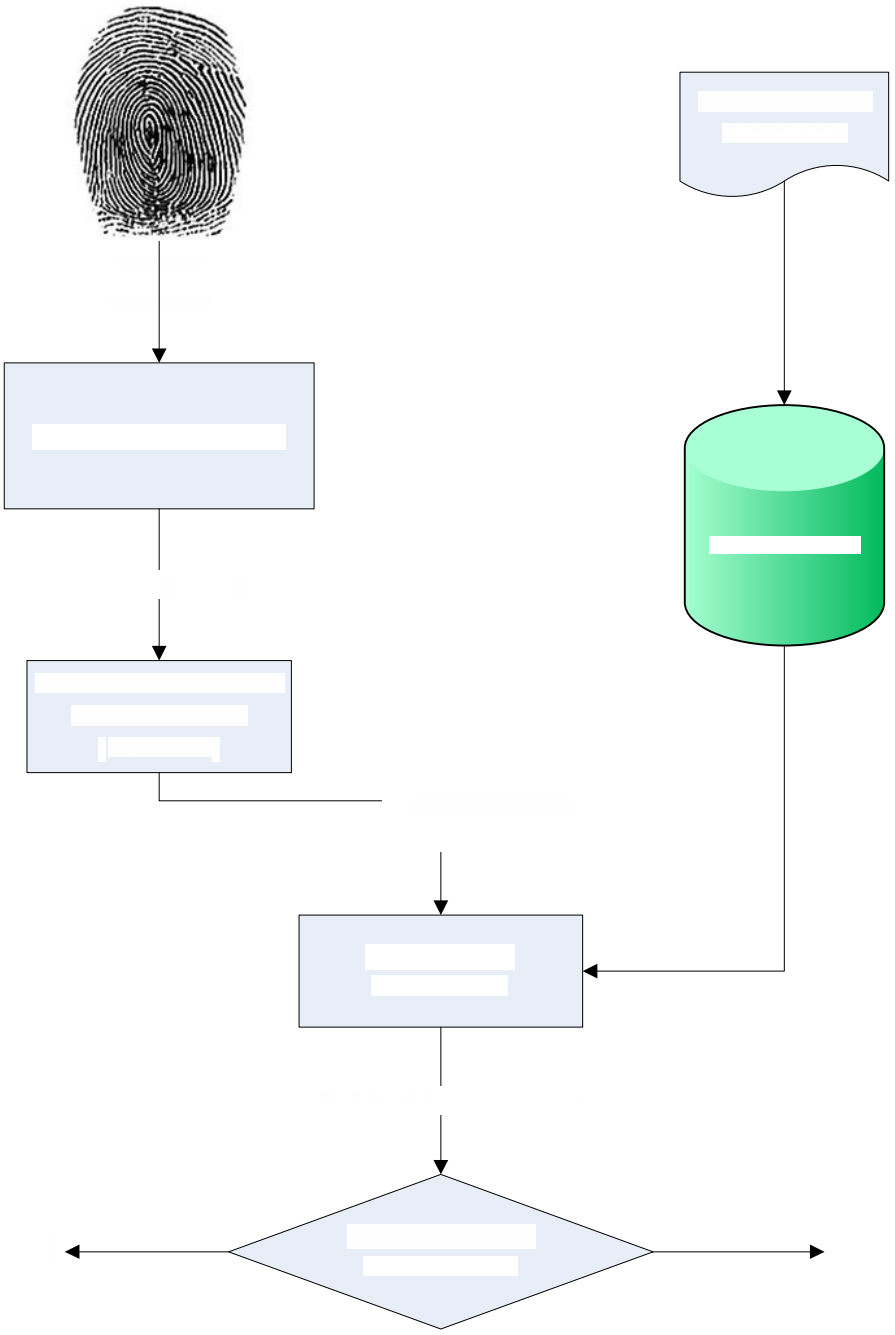


Figura 1.12. Sistema de autenticación de personas

El proceso de identificación (Figura 1.13) por su parte entregará como resultado, a las personas que presenten una plantilla con un mayor nivel de similitud con respecto a la entrada biométrica parametrizada.

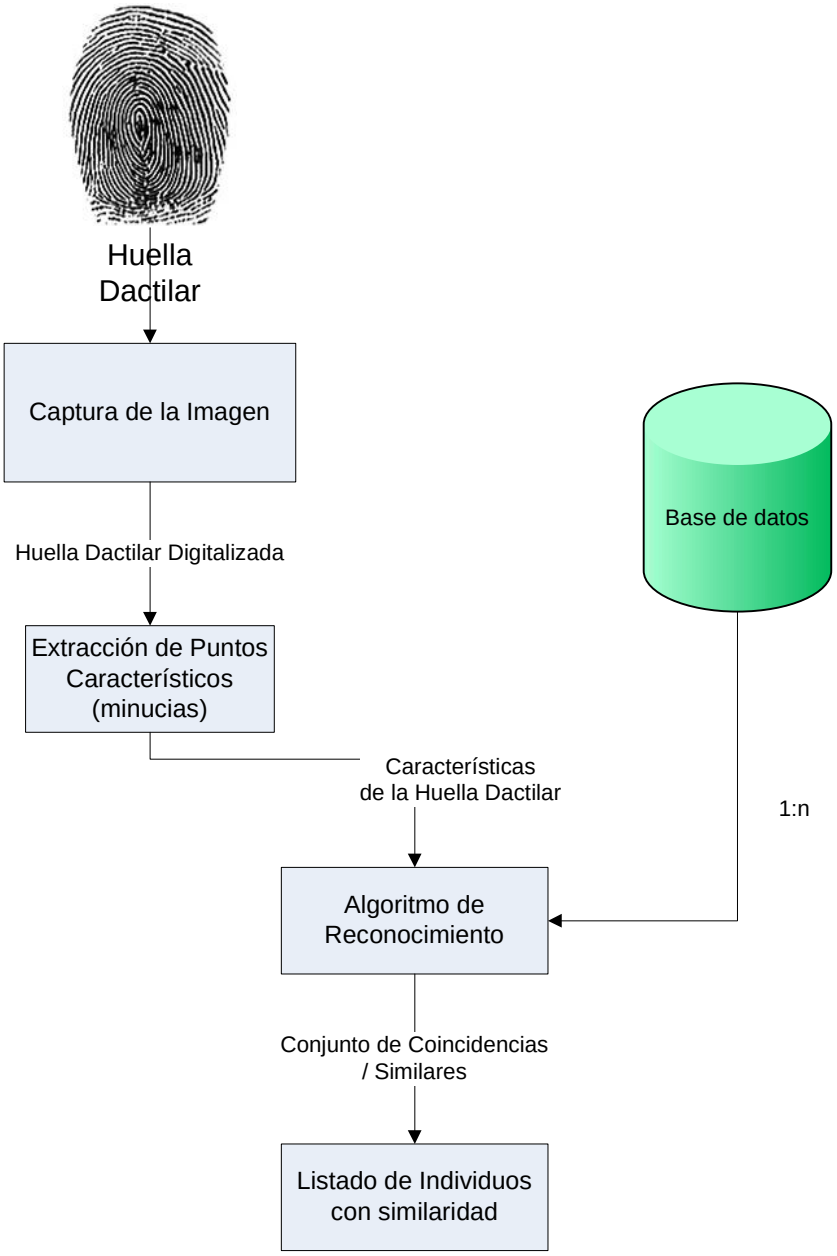


Figura 1.13. Sistema de identificación de personas

1.6. El proceso de Identificación

Este apartado se centrara en el estudio de las etapas que conforman el proceso completo de identificación de personas a través de la huella dactilar.

1.6.1 Captura o adquisición digital de la huella

Se debe distinguir dos métodos de adquisición directa de huellas dactilares: el método “off-line” y el método “on-line”.

El primero obtiene la huella digitalizada con una resolución espacial de 500dpi (dots per inch o puntos por pulgada) a 256 niveles de profundidad de gris (según recomendaciones del FBI), mediante el escaneo de un dispositivo impreso en papel obtenido con anterioridad, a partir de la operación tradicional de calcado del dedo entintado sobre papel. Esta metodología de funcionamiento requiere un costo de tiempo importante y es la que suele usarse en aplicaciones criminalistas. El segundo método, en cambio, se realiza en tiempo real, mediante el escaneo directo de la huella a través del uso de escáner del tipo inkless. Esta otra metodología es la que frecuentemente se utiliza en aplicaciones civiles.

El archivo resultante ocupa en ambos casos, entre 50 y 100 KBytes. El intervalo de áreas de captura de este tipo de sensores se encuentra entre los 12x18 a 13x20 mm aproximadamente (suficiente si se considera el tamaño medio estándar de una huellas que es de 8,4x12,7mm; la recomendación del FBI eleva a 1” cuadrada el área recomendable de captura).

Tras la captura de la huella, se realizará una valoración cualitativa de la misma, el resultado de la cual será: a) huella apta para ser procesada, b) huella recuperable mediante técnicas de pre-procesado digital de la imagen, c) huella inutilizable debido a la baja calidad en su adquisición.

1.6.2 Procesamiento de la Imagen

El problema fundamental cuando se realiza el pre-procesado de la imagen dactilar, consiste en discriminar de forma óptima si los píxeles evaluados, pertenecen a una cresta o no. Esta consideración se debe a la problemática inherente al proceso de captura: diferencias de brillo y contraste de la imagen, distintas presiones del dedo sobre el lector, valores distintos de humedad o calidad del lector.

A continuación se presenta el conjunto de pasos a realizar para adaptar la imagen capturada a los requerimientos propios del bloque extractor de minucias:

a) Mejora de la imagen para minimizar la información redundante presente en la imagen y extraer las crestas.
b) Binarización de la imagen para obtener la huella monocroma.
c) Valorización de la calidad de la huella.
d) Extracción de la región de interés de la huella.

Mejora de la Imagen

Esta etapa de mejora consiste en la aplicación de filtros lineales direccionales para mejorar la calidad de las imágenes originales, disminuyendo el ruido y acentuando los contornos o transiciones claro-oscuro o viceversa. Para la implementación de estos filtros, se requiriere de la

orientación local de las crestas próximas a cada píxel, extraída a partir del denominado *mapa o campo de orientación*. Dicho mapa de información adicional nos permitirá disponer de los ángulos tangentes de las crestas presentes en la imagen.

La aplicación de este filtrado específico sobre la imagen supondrá una mejora de la calidad de las crestas que presenten una dirección similar, y una reducción de los elementos espurios, caracterizados por presentar una orientación sensiblemente distinta.

Estimación del campo de Orientación

La determinación de este campo permitirá conocer la orientación de las crestas de la huella respecto a la horizontal. Recuérdese que, como se indica en el capítulo I punto 1.3.1, las crestas en una huella dactilar aparecen como una serie de líneas oscuras que representan los relieves, la porción saliente de las crestas, mientras los valles entre estas crestas aparecen como espacio en blanco y están en bajo relieve, la porción subyacente de las crestas de fricción. Para determinar la orientación de las crestas entonces, se divide la imagen en bloques de 15x15. Esta segmentación en lugar de píxeles hace que sea menos sensible a ruidos su determinación. Luego se calcula el gradiente, en *x* e *y* de cada píxel. A partir de la información del gradiente se puede estimar el ángulo de orientación aplicando el algoritmo de ajuste por mínimos cuadrados[7]. Puesto que en una huella no pueden existir grandes variaciones entre los ángulos de orientación de bloques vecinos, haciendo un promedio o filtrado paso bajo de la imagen, se consigue reorientar todos los segmentos.

Un ejemplo de estimación de campo de orientación se muestra en la Figura 1.14. En una imagen de una huella digital (Figura 1.14 A), se obtuvieron los vectores gradiente que se observan en la Figura 1.14 B, posteriormente se filtró la imagen usando el filtrado y se efectuó el mismo proceso observando que la orientación de los vectores varía (Figura 1.14 C). En la imagen filtrada los vectores gradiente siguen más estrechamente la trayectoria de las crestas y valles, lo que posiblemente facilitaría el proceso de detección de las minucias o puntos característicos de las huellas dactilares.

[7] Mínimos cuadrados es una técnica de análisis numérico encuadrada dentro de la optimización matemática, en la que, dados un conjunto de pares (o ternas, etc), se intenta encontrar la función que mejor se aproxime a los datos (un "mejor ajuste"), de acuerdo con el criterio de mínimo error cuadrático.

Figura 1.14. Estimación del campo de orientación

Binarización

El objeto de esta etapa es disminuir el margen de niveles de gris entre las crestas y los valles de la imagen, para facilitar el proceso de las etapas siguientes. Este procedimiento posibilita la conversión de la imagen a 256 niveles de gris (8 bits/píxel), en una imagen monocromática o bitono (1bits/pixel). El algoritmo denominado "Metodo de Otsu o Criterio del Discriminante" proporciona el cálculo automático del umbral que maximiza la separabilidad de los niveles de gris[8]. Dicho método está basado en el cálculo de la probabilidad de los niveles de intensidad.

Así, todos los píxeles que presenten un nivel de gris por debajo del umbral establecido tomarán el valor cero (negro), mientras que a los que se encuentren por encima se les asignará el valor un (blanco). En la Figura 1.15 se muestra la función de transferencia del proceso descrito.

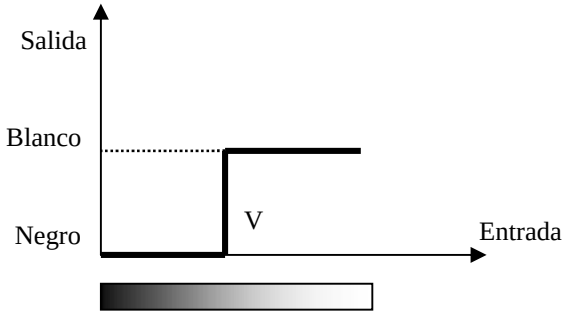


Figura 1.15. Función de transferencia del proceso de binarización

[8] NOBUYUKI, Otsu. A Threshold Selection Method from Grey-Level Histograms. IEEE Transactions Analysis and Machine Intelligence (EEUU, 1990).

Valoración de la calidad

Una vez obtenida la imagen perfectamente filtrada y binarizada, se podrá realizar de forma opcional, una comprobación automática del nivel de calidad de la misma, para rechazar las imágenes de pobre definición. Asimismo, el sistema o dispositivo podrá realizar una petición automática, solicitando una nueva entrada, en el caso de obtención de un resultado con un bajo nivel de calidad.

La calidad de una imagen para una captura dada, se calcula mediante la relación (S/N+S) donde N+S en la ubicación (i,j), obedece a la energía de la señal (en nuestro caso, una imagen 2D) estimada como sigue:

donde:

- (u,v) pertenecen a la región R (ejmplo: 8x8 píxeles).
- p(u,v) son los valores de los píxeles.
- p_{avg} es el nivel de gris promedio en la región R.

Extracción de la región de interés ROI

El procedimiento de extracción de la Región de Interés o ROI (Region of Interest) tiene como finalidad desestimar la información redundante relativa al fondo de la imagen (blanco perfecto), de esta forma se obtiene una importante reducción del tamaño del archivo final, con la consiguiente reducción del tiempo de proceso. Existen diferentes métodos para definir la ROI en una huella dactilar:

1. Se divide la imagen en bloques definidos de píxeles (ejemplo: 16x16). Posteriormente, se extraen todos los bloques de píxeles que presenten una mayor varianza del nivel de gris en la dirección normal a las crestas existentes. El contorno que definen dichos bloques obedecerá a la región de interés hallada (puede optarse por los contornos mas exteriores obtenidos, para conseguir una región resultante de tipo rectangular).
2. Se detecta el punto de referencia conocido como core (núcleo), y a partir de él, se define una región circular, tomando como centro de la misma, las coordenadas del punto core aislado; la región circular obtenido responderá a la nueva región de interés.

La figura 1.16 presenta un ejemplo práctico del preprocesado descrito sobre una huella de ejemplo.


Adquisición	Filtrado


Binarización	ROI

Figura 1.16. Ejemplo de preprocesado sobre una huella dactilar

1.6.3 Adelgazamiento (Thinning)

En esta etapa se realiza una reducción del grosor de las líneas mediante distintas técnicas hasta que todas presenten un grosor igual a un píxel, facilitando de esta manera el proceso de reconocimiento. La técnica utilizada en este estudio es la morfología matemática (MM), ya que responde a una potente herramienta de extracción de información a partir de las imágenes[9]. La MM obedece a una técnica no lineal de la imagen, basada en estructuras geométricas, desarrollada inicialmente por Matheron y Serra. Resultan de especial interés las siguientes operaciones morfológicas:

El operador morfológico de adelgazamiento o "morphological thinning" utilizado, responde a la substracción entre la imagen original I y el resultado de la operación morfológica hit-miss[10], normalmente con el elemento estructurante (EE) de la figura 1.17.

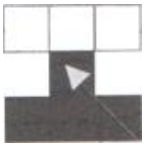


Figura 1.17. EE genérico de la transformación Thinning

[9] HARALICK, R.M.; STERNBERG, R.S. y ZHUANG , X. Image analysis using mathematical morphology. IEEE Trans. Pattern Analysis and machine intelligence (EEUU, 1987) Pág. 532-550

[10] El operador morfológico hit-miss tiene por objetivo buscar la coincidencia de la imagen original con un patrón determinado.

Esta operación elimina los pixeles que satisfacen el patrón que define el elemento estructurante (EE).

donde:

Bo, es el conjunto formado por los píxeles de B que pertenecen al objeto.

Bf, es el conjunto formado por los píxeles de B que pertenecen al fondo.

, son las funciones de erosión y dilatación morfológica respectivamente.

La operación morfológica *skeleton*, utilizada para la obtención de la imagen final adelgazada, responde a la iteración de la operación thinning utilizando una secuencia de elementos estructurantes generados a partir de la rotación sucesiva del patrón o EE genérico. Dependiendo del patrón y el paso utilizado, el operador podrá ser homotópico (preservará la topología de la imagen original) o no. Para el caso particular de las huellas, el elemento estructurante elegido, responderá a la secuencia morfológica de rotación mostrada en la figura 1.18, donde x representa cualquier valor (0 o 1). La figura 1.19 muestra el resultado de aplicar esta transformación sobre la imagen[11].

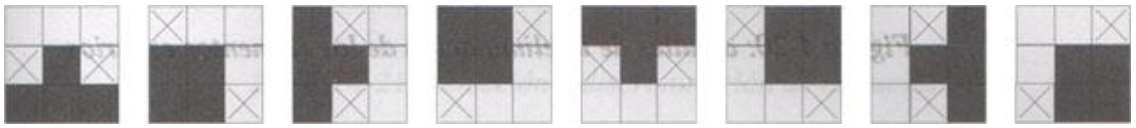


Figura 1.18. Patrones y pasos de rotación utilizados.

[11] ESPINOSA DURÓ, V.Fingerprint thinning algorith. IEEE AES Transaction aerospace and electronics systems (EEUU, 2003).

Preprocesada

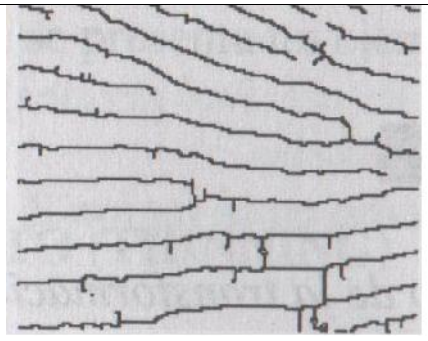
Adelgazada

Figura 1.19. Ejemplo de huella adelgazada.

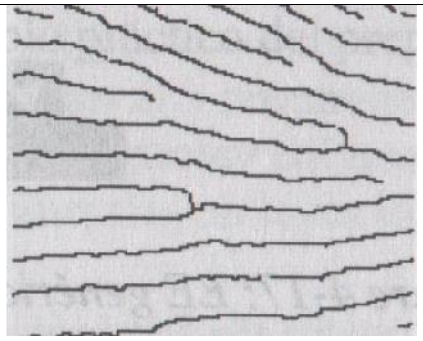
1.6.4 Depuración

Esta etapa consiste en la aplicación de algoritmos de limpieza o corte para eliminar las ramas indeseadas residuales perpendiculares a las crestas de la huella, que han surgido durante el proceso anterior de adelgazamiento, así como la unión de líneas rotas mediante un procedimiento de suavizado. La figura 1.20 muestra los resultados obtenidos. Este proceso se lleva a cabo mediante las siguientes sencillas reglas:

1. Eliminar las pequeñas líneas aisladas utilizando nuevamente el operador thinning con un elemento estructurante que se adapte a las nuevas necesidades.
2. Conectar las crestas rotas, es decir, unir todas las líneas que represente sus finalizaciones con dirección similar y que se hallen próximas entre sí.



Adelgazada



Depurada

Figura 1.20. Detalles de la eliminación de elementos espurios.

1.6.5 Extracción de características (minucias)

Esta etapa de extracción de características, o featured extraction, responderá a la etapa de obtención de la localización, orientación y tipo del conjunto de minucias presentes en la imagen adquirida, para elaborar los modelos de entrenamiento (plantillas) y test necesarios para la etapa de reconocimiento. El archivo resultante ocupa aproximadamente 300 bytes. De esta forma, sólo se almacenaran los datos que se corresponde con la disposición de las minucias evitando así guardar la imagen original de la huella.

Debido a que no será posible obtener siempre el mismo número de minucias en las fases de entrenamientos y test, deberá aplicarse un algoritmo de reconocimiento, o matching, capaz de comparar el vector de características candidato con la plantilla correspondiente.

El algoritmo proporciona dos salidas:

1. Un conjunto de minucias caracterizadas por su posición espacial y por su orientación respecto de la imagen de la huella.
2. La información local de las crestas presentes en la vecindad de cada minucia.

El algoritmo de extracción de minucias, responde a un sencillo algoritmo de reconocimiento de patrones basado en el análisis de los pixeles vecinos y los pixeles que conforman las líneas adelgazadas obtenidas en el proceso anterior. A continuación se detalla los criterios de detección de minucias y de clasificación de las mismas una vez localizadas (final de cresta y bifurcación de crestas). Sean (x,y) las coordenadas de un pixel presentes en una cresta adelgazada y N_0, N_1, … N_7, sus 8 vecinos. El píxel de coordenadas (x,y), será un final de cresta si se cumple la condición

=

(un único vecino), mientras que responderá a una bifurcación de cresta si obedece a la

expresión (tres o más vecinos). La figura 1.21 muestra un ejemplo de detección de estos dos tipos de minucias según este criterio. Este proceso se realiza sobre toda la imagen binaria aplicando ventanas de 3x3.

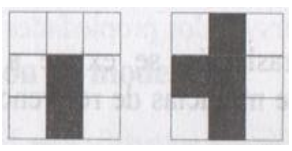


Figura 1.21. Detección y discriminación de minucias

1.6.6 Etapa de Reconocimiento

El algoritmo de reconocimiento de huellas dactilares o "matching" es un algoritmo de comparación robusto entre la entrada biométrica parametrizada o modelo de test, y el total de modelos de huella existentes en la base de datos del sistema, en función de la forma geométrica descrita por las posiciones de las minucias. En este sentido, será necesario realizar la tarea previa de estimar los parámetros necesarios de traslación y rotación, para alinear (hacer coincidir) el modelo de test con la plantilla, a partir de las minucias detectadas en la fase anterior. La parte final del algoritmo de reconocimiento determinará la mínima distancia euclídea[12] de las *n* comparaciones, siendo *n* igual al número de modelos que conforman la base de datos. El resultado de este cálculo, nos entregará la identidad de la persona a reconocer. A este procesado de datos se le denomina *minutiae pattern matching*[13].

Cuando dos imágenes de la huella dactilar de una misma persona son comparadas y una de estas imágenes está trasladada, todas las minucias de la huella dactilar se mueven en la misma dirección y la misma cantidad de píxeles. Esta etapa consiste en analizar la dirección y el número de píxeles que fue movida la imagen de entrada.

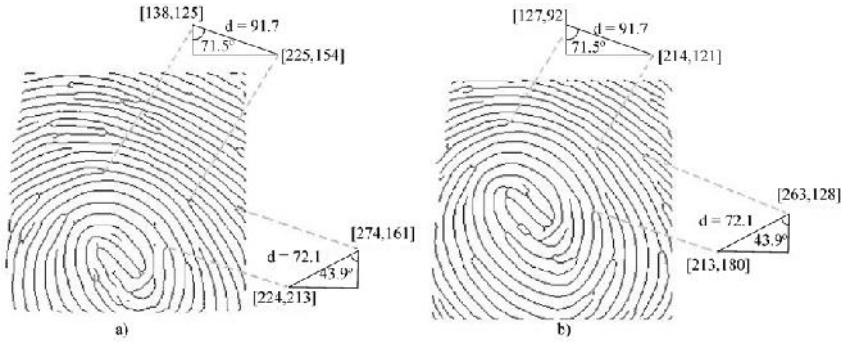


Figura 1.22 a) Imagen almacenada, b) Imagen de entrada

En la figura 1.22 la imagen de entrada se movió 11 píxeles a la izquierda y 33 píxeles hacia arriba con respecto a la imagen almacenada. Por lo tanto, todas las minucias de la imagen de entrada se movieron el mismo número de píxeles en la misma dirección.

Si dos imágenes de diferentes personas son comparadas y una de ellas está trasladada, el número de píxeles y la dirección cambian. En la figura 1.23 se presentan dos imágenes de diferentes personas; la primer minucia se movió 4 píxeles a la derecha y 5 hacia abajo, pero la segunda minucia se movió 10 píxeles a la derecha y 0 píxeles en el eje Y.

[12] En matemáticas, la distancia euclídea o euclidiana es la distancia "ordinaria" (que se mediría con una regla de acero) entre dos puntos de un espacio euclídeo, la cual se deduce a partir del teorema de Pitágoras.
[13] MALLAT, S. A wavelet tour of signal processing (EEUU Academic Press, 1999).

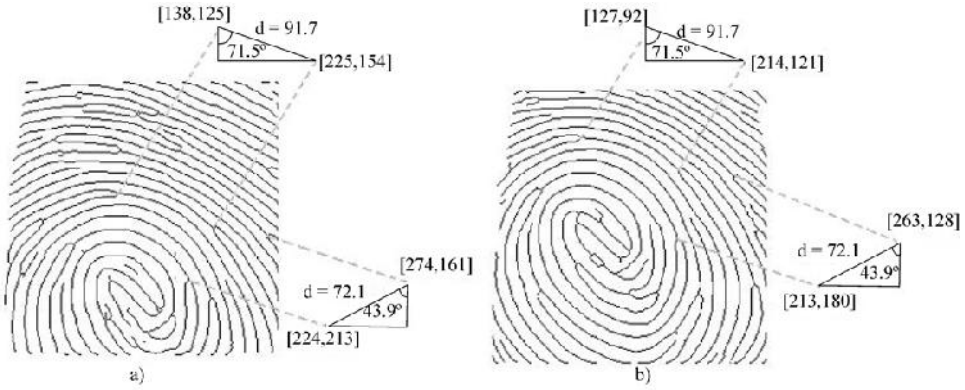


Figura 1.23 a) Imagen almacenada. b) Imagen de entrada

Algoritmo de alineamiento

La fase de alineamiento de imágenes, permitirá calcular los parámetros de rotación y traslación que conduzca al mayor nivel de correspondencia espacial, al ajustar la huella parametrizada con la plantilla. A continuación se detallan las etapas del algoritmo de alineamiento.

1. Seleccionar un par de *minucias de referencia* (una de cada imagen).
2. Determinar el número de pares de minucias que se corresponden.
3. Reiterar el proceso de selección, para cada una de los pares de combinaciones posibles de minucias de referencia que presentan características locales comunes.
4. El par de minucias de referencia final seleccionado es aquel que ha contabilizado un mayor número de pares de minucias que se corresponden y en consecuencia, el que ha estimado el mejor alineamiento.
5. Calcular los parámetros de rotación y traslación:
    a. El parámetro de rotación estimado, es la media de todos los valores individuales de rotación de todos los pares de minucias que se corresponden.
    b. El parámetro de traslación se extrae a partir de las coordenadas espaciales del par de minucias de referencia que ha supuesto el mejor alineamiento.
6. Aplicar los parámetros de rotación y traslación calculados a todas las minucias del modelo de test.

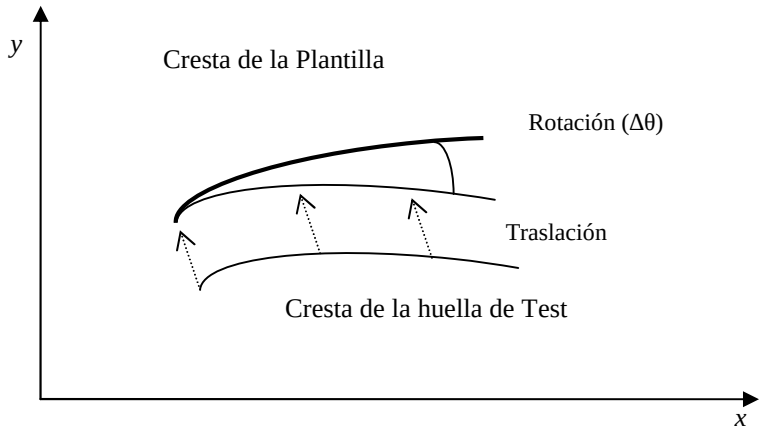


Figura 1.24. Detalle del proceso de alineamiento

Para ello, se aplican las siguientes ecuaciones:

donde:

- son los parámetros de rotación y traslación calculados en el punto 5.
- representa la minucia i-esima del patrón de prueba (coordenadas y ángulo de orientación de la cresta asociada).
- es la minucia de referencia.
- es la minucia final alineada.

Un detalle del proceso anterior descrito se muestra a continuación.

Cada imagen es dividida en bloques de NxN píxeles, y para cada bloque se calcula la orientación dominante marcada por el flujo de las crestas. El valor de la orientación de campo se acota en el rango [0º,+180º). Dadas las dos imágenes "Plantilla" y "Test" de (P_x x P_y) y (Tx x Ty) bloques respectivamente, el procesado de alineamiento trata de desplazar espacialmente la matriz "Plantilla" sobre la matriz "Test". Para cada posición relativa Plantilla-Test se identifica la zona solapada o región de interés (ROI), mencionada en puntos anteriores, entre ambas imágenes, y para cada par de bloques correspondientes en la ROI se calcula la diferencia entre las orientaciones de campo, tal y como muestran las ecuaciones (1) a (5).

(1)

(2)

(3)

(4)

(5)

Con el fin de hacer el algoritmo de alineamiento tolerante a las deformaciones no lineales existentes en las impresiones de las huellas dactilares, se dota al algoritmo de cierta elasticidad a la hora de calcular la diferencia de orientaciones entre dos bloques correspondidos en la ROI. Cada bloque de la imagen Plantilla es comparado no solamente con su bloque homólogo o correspondiente de la imagen Test, sino también con los bloques vecinos, considerando un nivel de vecindad K=2 centrado en el bloque correspondiente, tal y como queda reflejado en la ecuación (6). De esta forma, el algoritmo de alineamiento permite compensar las deformaciones no lineales intrínsecas al proceso de adquisición.

(6)

Para cada posición relativa Plantilla-Test objeto de estudio se calcula el valor medio de la diferencia de orientaciones de los bloques comprendidos en la ROI (7), así como su desviación estándar (8). Ambos parámetros se suman con el fin de obtener la función objetivo (9), capaz de cuantificar el nivel de correlación o alineamiento existente entre ambas imágenes en cada uno de los posibles alineamientos objeto de estudio.

(7)

(8)

(9)

El cómputo de la función objetivo se realiza sobre cada una de las posiciones relativas Plantilla-Test, con el consiguiente costo computacional puesto que el proceso de alineamiento se convierte en un procesado de fuerza bruta donde todos los posibles alineamientos son analizados y entre ellos el mejor alineamiento es seleccionado. Sin embargo, y con el fin de reducir el costo

computacional del algoritmo, sólo aquellas posiciones relativas en las que se obtenga un mínimo de bloques solapados, por encima de un cierto umbral $Umbral_{ROI}$ ($Umbral_{ROI}$ = 16x16 boques), son estudiadas (10).

=

(10)

Adicionalmente, y para dotar al algoritmo de cierto nivel de robustez frente a la posibilidad de obtener diferentes inclinaciones del dedo sobre el sensor durante el proceso de adquisición, el algoritmo es capaz de rotar la matriz de orientación de campo de la imagen Test. Dada una matriz de orientación, es posible calcular la nueva matriz resultante tras desplazar (X,Y) bloques y rotar la matriz original θ grados. Cada bloque (i,j) de la matriz original se convierte en un nuevo bloque (i',j') en la imagen rotada, tal y como muestra la ecuación (11). El nuevo valor de la orientación de campo en la imagen rotada se obtiene sumando el ángulo de rotación θ^o a la orientación del bloque original.

=

(11)

De esta forma, el sistema desarrollado permite alinear correctamente huellas que presentan solapamientos parciales e incluso inclinaciones distintas. Con todo ello, es fácil deducir que el tiempo de ejecución del algoritmo dependerá notablemente del tamaño de las matrices, así como del número de rotaciones distintas a probar en la fase de alineamiento. Al finalizar el proceso, el sistema obtiene como resultado el mejor alineamiento -aquel que minimiza la función objetivo cumpliendo con el requerimiento de presentar un área solapada superior a un cierto umbral- o por el contrario indica la no alineación si dichos requisitos no son satisfechos. En caso de alineamiento positivo se indican los parámetros espaciales (X,Y,θ) a aplicar sobre la imagen "Test" para alinear ésta con la "Plantilla".

Las deformaciones no lineales que se dan en las huellas dactilares hacen que dos modelos (modelo de Test-Plantilla), aún en el caso de pertenecer a una misma huella, no coincidan exactamente una vez alineados. De ahí la necesidad de diseñar un algoritmo elástico de comparación capaz de establecer correspondencia entre puntos dentro de unos ciertos límites de tolerancia.

Algoritmo de comparación de modelos

Cada vez que una huella accede al sistema, se extrae su patrón biométrico de minucias y se compara con cada una de las plantillas almacenadas en la base de datos. La comparación se realiza previa alineación de los dos modelos que se van a procesar, realizando anteriormente su conversión en dos cadenas de puntos ordenados según sus coordenadas polares. El resultado de la comparación vendrá dado por el valor que toma la función de coste después de comparar todas las parejas de minucias de las dos cadenas.

El algoritmo de comparación entre modelos de entrenamiento y test consta de dos partes. En la primera se ordenan las minucias de los dos modelos para formar sendas cadenas de puntos en coordenadas polares. La utilización de este sistema de coordenadas particular, se debe a que las deformaciones no lineales que aparecen en las huellas presentan siempre una zona en la que son consistentes, perdiéndose estas características a medida que los puntos se alejan de esta zona en las direcciones radiales. El punto de máxima consistencia es la minucia de referencia, que se tomara como centro de coordenadas polares del sistema (Figura 1.25). Una vez representadas las minucias en polares, se ordenan para formar las cadenas o vectores de características en orden creciente de sus coordenadas angular y radial. Las dos cadenas formadas constituirán los dos patrones a tratar por el algoritmo de comparación. En la segunda parte, el algoritmo efectúa la comparación de los dos vectores a partir de la distancia euclídea entre minucias, dando como resultado, la identidad de la persona que responde con el patrón que presenta una distancia euclídea menor con respecto del modelo de Test a evaluar.

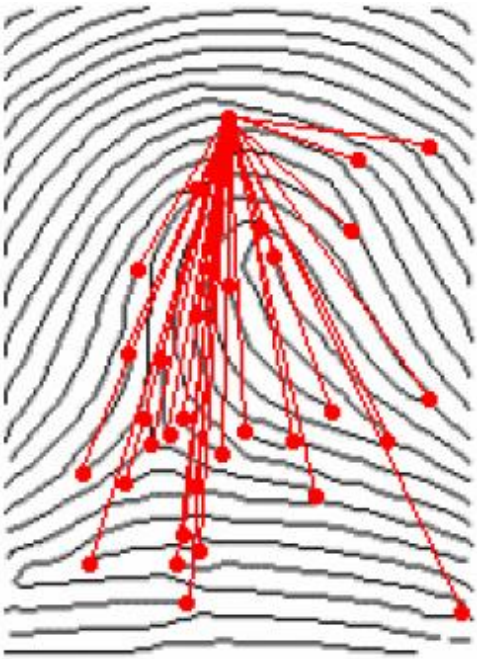


Figura 1.25. Imagen con la vectorización de todas las minucias respecto de la minucia de referencia.

1.7 Tasas de reconocimiento

Las prestaciones de un algoritmo de reconocimiento biométrico se evalúan atendiendo a los parámetros que a continuación se definen:

FRR (False Rejection Rate): tasa de rechazo erróneo, la probabilidad de que un usuario que está autorizado sea rechazado a la hora de intentar acceder al sistema. Si los usuarios son rechazados erróneamente con frecuencia, parecerá que el sistema no funciona correctamente y deberá ser revisado.

FAR (False Acceptance Rate): tasa de falso positivo, hace referencia a la probabilidad de que un usuario no autorizado sea aceptado. Este parámetro deberá ajustarse para evitar el fraude en los sistemas biométricos.

ERR (Equal Error Rate): el punto de cruce de las curvas FAR y FRR proporciona el valor umbral en el que las tasas son iguales y recibe el nombre ERR.

Las tasas FRR y FAR dependen de donde se fija el umbral (resultado de la etapa de cotejo, esto es, minucias emparejadas/minucias totales) de aceptación o rechazo. Un umbral alto dará lugar a un sistema con una tasa de falsa aceptación muy baja y posiblemente una tasa de falso rechazo elevada. Por el contrario, un umbral muy bajo conllevará una situación contraria con tasas bajas y altas de FRR y FAR, respectivamente. Las prestaciones del sistema suelen evaluarse en función del punto para el cual ambas tasas tienen el mismo valor (EER) tal y como se presenta en la Figura 1.26.

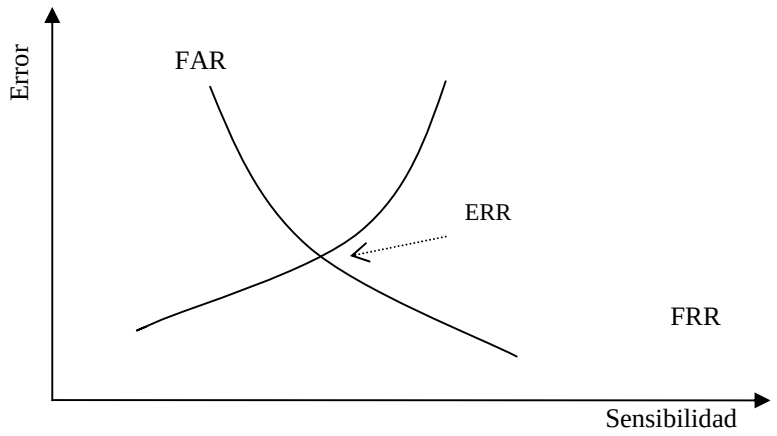


Figura 1.26.Donde se cruzan las dos líneas, FAR y FRR es el ERR.

1.8 Estándares Internacionales

El desarrollo de los estándares en tecnología de identificación biométrica por huellas dactilares cumple un rol fundamental para el avance e interoperación entre sistemas. Se requiere del arbitraje o guía de los estándares la gran variedad de algoritmos y sensores disponibles en el mercado.

La interoperabilidad es un aspecto crucial en las implementaciones, lo que significa que las imágenes obtenidas por un dispositivo deben ser capaces de ser interpretada por una computadora que utilice otro dispositivo. Los mayores esfuerzos de los estándares se enfocan en la estandarización del contenido, el significado y la representación de los formatos de datos para el intercambio de huellas dactilares e incluyen las normas ANSI/INCITS 381-2004 formato de intercambio de datos basado en imagines de dedos, ANSI/INCITS 377-2004 formato de intercambio de datos basado en patrones del dedo, ANSI-INCITS 378-2004 formato de las minucias del dedo para el intercambio de datos, ISO/IEC 19794-2 formato de minucias del dedo para intercambio de datos, ISO/IEC FCD 19794-3 formato de intercambio basado en patrones del dedo, y la ISO/IEC 19794-4 formato de intercambio basado en imágines de dedos.

A continuación se presenta un resumen de los estándares anteriormente mencionados, como así también otros que se destacan en el tema.

ANSI/INCITS 381-2004

Formato de intercambio de datos basado en imagines de dedos. Este estándar especifica un formato para el intercambio de los datos basados en imágenes para el reconocimiento de huellas dactilares y de la palma. Define el contenido, el formato, y las unidades de medida para tal información. Este estándar se piensa para esos usos de identificación y verificación que requieren el uso de los datos crudos o procesados de la imagen que contienen la información detallada del pixel.

ANSI/INCITS 377-2004

Formato de intercambio de datos basado en patrones del dedo. Este estándar especifica un formato para el intercambio de los datos para reconocimiento de huella dactilar basados en patrones. Describe la conversión de una imagen cruda de la huella dactilar a un patrón del dedo, recortado y muestreado seguido por la representación celular de la imagen del patrón del dedo para crear los datos del intercambio de los patrones del dedo.

ANSI/INCITS 378-2004

Formato de las minucias del dedo para el intercambio de datos. Este estándar define un método de representación de información de huellas dactilares usando el concepto de minucias.

Define la ubicación de las minucias en una huella dactilar, un formato de grabación para contener los datos de las minucias, y extensiones opcionales para contar crestas información de núcleo/delta.

ANSI/NIST ITL 1-2000

Formato de datos para el intercambio información de huellas dactilares, Faciales, cicatrices, marcas & tatuajes (Scar, Mark and Tatoo, SMT). Este estándar define el contenido, el formato, y las unidades de medida para el intercambio de la información de las imágenes de huellas dactilares, de la palma, faciales o ficha fotográfica, cicatriz, marca, y tatuaje (smt), que se puede utilizar en el proceso de la identificación de un sujeto. La información consiste en una variedad de ítems obligatorios y opcionales, incluyendo parámetros de escaneo, datos relacionados, descriptivos y de registro, información de huella dactilar digitalizada, e imágenes comprimidas o sin comprimir.

ISO/IEC 19794-2

Formato de minucias del dedo para intercambio de dato. Este estándar describe cómo los puntos de las minucias serán determinados, define los formatos de datos para contener los datos para el uso general y de tarjeta inteligente, y detalla la información de la conformidad. Las pautas y los valores para los parámetros de combinación y decisión se proporcionan como anexo informativo. El estándar define tres tipos de minucias, incluyendo los finales de cresta y la bifurcación. La estrategia adoptada de la determinación de las minucias se basa en los esqueletos derivados de una imagen digital.

ISO/IEC FCD 19794-3

Formato de intercambio basado en patrones del dedo. Este estándar de bosquejo especifica que una imagen de la huella dactilar está dividida en una grilla de células solapadas o no solapadas. En cada célula, el patrón del dedo será representado por una estructura de célula. Un método para obtener la estructura de la célula es descomponer cada uno de las células en una representación espectral de dos dimensiones tal como la Transformada Discreta de Fourier (Discrete Fourier Transform, DFT) de dos dimensiones. La descomposición produce los componentes espectrales, donde cada componente se puede caracterizar por una longitud de onda horizontales (x) y verticales (y), en dirección, amplitud, y fase.

ISO/IEC 19794- 4

Formato de intercambio basado en imagines de dedos. Este estándar especifica que la imagen deberá parecer haber sido capturada en una posición vertical y deberá esta aproximadamente centrada horizontalmente en el campo visual. La secuencia de la exploración y los datos registrados deberán parecer haber sido de izquierda a derecha, progresando de arriba a

bajo de la huella dactilar. El origen de los ejes, ubicación del pixel (0.0), es en la esquina superior de la mano izquierda de cada imagen con la posición de la coordenada x (horizontal) aumentando positivamente del origen al lado derecho de la imagen mientras que la posición de la coordenada y (vertical) aumenta positivamente del origen a la parte inferior de la imagen. También especifica que el encabezado debe ser de acuerdo a CBEFF.

ISO/IEC 19794-8

Esquema Datos del Patrón del Dedo. Este estándar esta prensado para ser utilizado para alcanzar interoperabilidad entre los sistemas de reconocimiento de huellas dactilares basados en minucias y en patrones. Se basa en las características comunes compartidas entre el patrón espectral y las minucias por medio de la codificación de las crestas de una forma que el esquema de crestas proporcione las bases para detectar minucias.

EFTS v7.1

Especificaciones de transmisión electrónica de huellas dactilares. Esta especificación cubre la transmisión electrónica de la información que implican las huellas dactilares al FBI del Sistema Automatizado Integrado de la Identificación de Huellas dactilares (IAFIS) basado en el estándar NIST ITL 1-2000 del ANSI. El propósito de este documento es especificar ciertos requisitos a los cuales las agencias deban adherir para comunicarse electrónicamente con el IAFIS.

EBTS v1.0

Especificaciones de transmisión electrónica de biometría. Esta especificación describe arreglos de las transacciones de las Especificaciones transmisión electrónica de huellas dactilares (EFTS) del FBI, que son necesarias para utilizar el sistema de identificación biométrica automatizada (ABIS) del Departamento de Defensa (DoD).

FBI- WSQ (Wavelet Scalar Quantization, WSO)

Compresión de imágenes de huellas dactilares por Cuantización de Ondeletas Escalares. Es una compresión con pérdida de información (Lossy) que es capaz de preservar los detalles de alta resolución de una imagen en escala de grises que son usualmente descartados por otros algoritmos de compresión del tipo Lossy. Alcanza un alto cociente de compresión, por medio 15:1 dependiendo de los parámetros.

IAFIS-IC-0110 (V3), 19 de diciembre de 1997.

“Servicios de información de la justicia criminal (CJIS) Especificación de compresión de imágenes en escala de grises de huellas dactilares WSO” del FBI.

JPEG2000 (Joint Photographic Experts Group 2000)

Compresión de imágenes de huellas dactilares del Grupo de Expertos de la Asociación Fotográfica 2000. Es un nuevo sistema de codificación de la imagen que utiliza técnicas avanzadas de compresión. Su arquitectura debe prestarse a una amplia gama de aplicaciones desde cámaras fotográficas digitales portables hasta avanzadas como la pre impresión (para las industrias de imprenta y publicación), diagnostico por imágenes en medicina y otro sectores clave.

NIST 800-76

Especificación biométrica de datos para la verificación de identidad personal. Contiene especificaciones para la adquisición, formateo, y almacenamiento de imágenes de huellas dactilares y patrones para tomar y dar formato imágenes faciales; y especificaciones para dispositivos biométricos sobre como tomar y leer imágenes digitales. La publicación especifica que las huellas dactilares sean almacenadas en la tarjeta como “patrones de minucias”, representaciones matemáticas de imágenes de huellas dactilares.

CAPITULO II – CONTROLES DE ACCESO A ESTADIOS

2.1 Situación actual

En la actualidad la violencia en espectáculos deportivos, en especial y particular los partidos de fútbol en la República Argentina, se presenta como un problema social creciente. Desde hace ya algunos años se está tratando de minimizar los efectos causados por esta problemática, aplicando controles para evitar situaciones violentas. Lo cierto es que no se sabe, en gran mayoría quién ingresa a un estadio de fútbol, ni cuál es su nombre, ni donde vive, en definitiva no se identifica a las personas. Cualquier individuo puede acceder a una entrada e ingresar a los establecimientos. No existe una herramienta tecnológica que les permita a las autoridades de seguridad ejercer el derecho de admisión en plenitud.

Quien tradicionalmente ejerce el control de acceso a los establecimientos es la fuerza policial. Verificando la posesión del boleto o ticket del espectador de forma manual se permite su ingreso (Figura 2.1).

Figura 2.1 Control de acceso tradicional.

Algunos establecimientos deportivos cuentan con controles de acceso automatizados en sus ingresos. Con molinetes y tarjetas de banda magnética se permite el paso, similares a los utilizados en estaciones de tren. Quien desee ingresar al establecimiento debe poseer un boleto que sirve de pase para la admisión al evento deportivo (Figura 2.2).

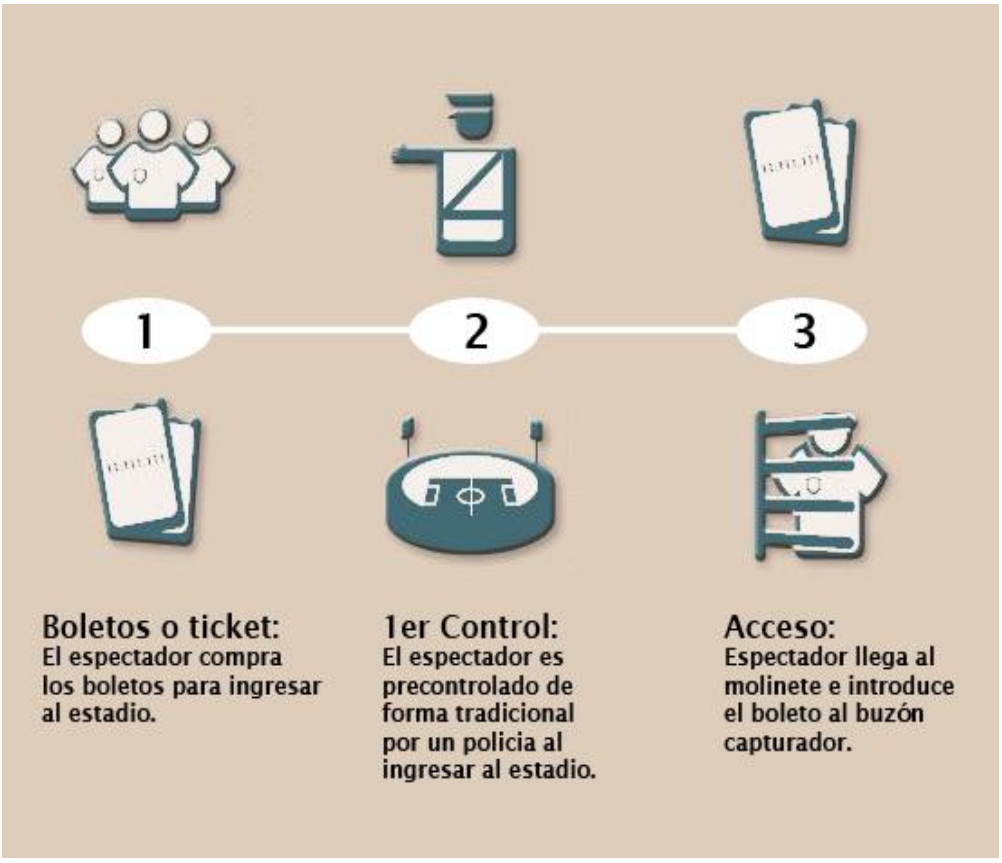


Figura 2.2. Control de acceso con molinete

A través de los controles descritos anteriormente, se logra establecer una verificación más rigurosa de las personas que ingresan, evitando fraudes y falsificación de entradas. Los mismos poseen suficiente espacio físico entre la valla de protección perimétrica exterior (1er control) y los molinetes de acceso al estadio. Permitiendo que el público pueda desplazarse libremente e ingrese cómodamente a los puntos de control o molinetes.

Las estimaciones de la FIFA (Federación Internacional de Fútbol Asociado) respecto al proceso de entrada o ingreso de las personas a los estadios se extiende sobre un período de una hora o más aproximadamente[14].

[14] FIFA. Estadios de fútbol. Recomendaciones técnicas y requisitos (Suiza, 2007).

2.2 Marco legal

El artículo 45 quater de la ley número 26.358 promulgada en el año 2008, establece un registro nacional de infractores a la ley del deporte. En el mismo se encuentran las personas procesadas con medidas cautelares de “Prohibición de Concurrencia” según el espectáculo deportivo de la especie que se trate. Como así también personas con condena a pena única o accesoria de inhabilitación especial para concurrir a espectáculos deportivos. La ley 24.192 establece el “Régimen Penal y Contravencional para la Prevención y Represión de la Violencia en Espectáculos Deportivos”.

Las leyes mencionadas anteriormente establecen el marco legal y sustento para implementar un sistema de control de acceso que prohíba la entrada a personas violentas.

CAPITULO III – SOLUCIÓN

La solución planteada en este trabajo, pretendió integrar los actuales controles de acceso con molinetes, incorporando en el funcionamiento de los mismos el chequeo biométrico por huella dactilar. Utilizando esta técnica de autenticación no se permitirá el paso de las personas que se encuentren alcanzadas por las leyes mencionadas en el capítulo anterior.

Para llevar adelante el diseño, en el siguiente capítulo se describió la selección de los dispositivos o equipos a ser integrados. Al momento de realizar este trabajo se desconoce cuáles son específicamente los dispositivos de control de acceso o molinetes utilizados en los estadios de fútbol, por lo que se describió y seleccionó tanto estos últimos como así también el dispositivo de captura de tarjetas a manera de ejemplo práctico. Teniendo en cuenta la premisa de rigurosos parámetros a cumplir, como así también que el control de acceso se realiza con tarjetas de banda magnética, se eligieron los mismos.

Una vez definidos y descriptos los dispositivos seleccionados, se puntualizó en la integración de los mismos, especificando la ubicación de los dispositivos con un diagrama interno del molinete. Luego se estableció el conexionado entre ellos mostrando diagramas de conectores.

Luego, un esquema de funcionamiento muestra el procedimiento o secuencia típica que deberá seguir un espectador al ingresar al establecimiento deportivo, y por último se establecen tiempos de accesos típicos de la solución planteada.

3.1 Dispositivos seleccionados.

Para seleccionar los dispositivos de autenticación biométrica, teniendo en cuenta lo desarrollado en el capítulo I punto 1.4 del presente trabajo, se elaboro un análisis respecto a las tecnologías disponibles. Para la selección tanto del dispositivo mencionado anteriormente como los molinetes de acceso, en todo momento se tuvo en cuenta el ambiente de trabajo y las exigencias respecto a las prestaciones, tiempos de respuesta y fiabilidad de los sistemas. El ingreso a espectáculos deportivos en estadios de fútbol, requiere rigurosos parámetros a cumplir.

3.1.1 Dispositivo de control biométrico.

El dispositivo de control biométrico seleccionado es el “Search Gate” de marca “3M Cogent Systems” (figura 3.1). El mismo es un avanzado dispositivo de control de acceso biométrico compatible con una amplia variedad de instalaciones. Utiliza el chip SecurASIC complementado con un algoritmo de búsqueda avanzado desarrollado por 3M Cogent que ha sido reconocido y evaluado por el NIST[15] obteniendo resultados destacables.

La elección del dispositivo de control biométrico se realizó luego de elaborar un análisis comparativo de las características más importantes a tener en cuenta en la selección de los mismos. A continuación se brinda un cuadro comparativo.

	Search Gate 	Verifier 300 LC 2.0 	MorphoAccess 120D 	Hamster 
Marca	3M Cogent	Crossmatch	Safran Morpho	Nitgen
Resolución	508 dpi	500 ppi ± 1%	500 dpi	500 dpi
Sensor dactilar	Capacitivo	Óptico	Óptico	Óptico
Base de Datos	1200 huellas	0 huellas	500 huellas	0 huellas
Tiempo respuesta	~ 1.5 seg.	-	< 1.5 seg.	-
Tasa Falso Rechazo	0.1 %-0.001% FRR	-	-	-
Tasa Falsa Aceptación	0.01 %-0.001% FAR	-	0.001% FAR	
Rango de humedad	10-90% sin-condensación	10-90% sin-condensado	10-90% sin-condensación	-
Rango Temperatura	0°C a 40º C	0°C a 40°C	-10° a 45°C	0°C a 40º C
Conexión	Ethernet / RS232 / RS485	USB 2.0	Ethernet / USB 2.0	USB 1.1

[15] NIST: Instituto Nacional de Estándares y Tecnología (NIST) de US.

Figura 3.1. Search Gate de 3M Cogent Systems

Por sus características este dispositivo provee un alto nivel de desempeño y precisión en ambientes hostiles con rangos de amplitudes térmicas y niveles de humedad exigentes. La selección de este dispositivo se realizó de acuerdo a su precisión, exactitud y tiempos de respuestas destacables respecto al resto de los dispositivos. Search-Gate puede almacenar hasta 1.200 huellas dactilares y es capaz de realizar búsquedas a velocidad de 500 huellas por segundo. Con capacidad Power-over-Ethernet (PoE)[16] y formatos Wiegand[17] personalizables, permite una instalación y configuración flexible.

Características Técnicas

- Sensor dactilar marca UPEK modelo TCS1, tecnología CMOS activo capacitivo, 508dpi de resolución.
- Método de enrolamiento de un solo dedo.
- Tiempo de extracción e identificación aproximado 1.5 segundos.
- Tasa de falso rechazo (FRR) 0.1 % - 0.001%.
- Tasa de falsa aceptación (FAR) 0.01 % - 0.001%.
- Nivel de seguridad configurable.
- Rotación dactilar permisible +/- 15º.
- Tamaño de huella dactilar 784 bytes.

[16] POE: Alimentación a través de Ethernet (Power over Ethernet, PoE) es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Permite que la alimentación eléctrica se suministre a un dispositivo de red usando el mismo cable que se utiliza para la conexión de red.
[17] Wiegand: Protocolo de comunicaciones que consta de dos partes fundamentales, una que describe el modo en que físicamente se transmite la información digital y la forma de interpretar numéricamente dicha información.

- Almacenamiento interno de 1.200 huellas dactilares.
- Interface I/O RS232 o RS485.
- Tasa de baudios 9600 –115 Kbps programable.
- Ethernet 10/100 Mbps.
- Wiegand I/O programable hasta 128 bits.
- Fuente de alimentación de 6 - 12V CC entrada estándar (12 - 48V CC jumper setup).
- Alimentación (PoE) completamente compatible con estándares 802.3af; 12~60V CC (jumper setting).
- Corriente en estado standby de 200 ma a 12V, en estado operacional de 280 ma a 12V.
- Temperatura de operación de 0 a 40º C.
- Dimensiones físicas de 137.7 x 79.7 x 57.9 mm.

3.1.2 Molinete

Como se menciono al iniciar el capítulo, al momento de realizar este trabajo se desconoce cuáles son los dispositivos de control de acceso utilizados por cada uno de los estadios de fútbol. En consecuencia en este punto se especifica los requerimientos técnicos que debe poseer el molinete.

Para realizar la integración con el lector biométrico el molinete debe poseer las siguientes especificaciones básicas:

- Placa de control con soporte contactos en seco (ver punto 3.1.3).
- Espacio físico para alojar lector biométrico.
- Señalización lumínica (Verde, Roja).

Debido a las exigentes condiciones de trabajo en las que se ve involucrado este tipo de molinete, el mismo debe poseer características especiales como son las de estar preparados para uso intensivo, tener gabinete y mecanismos reforzados, a prueba de polvo y derrames de líquidos, poseer sistema amortiguado, sentido de paso configurable para uno u otro lado, alta resistencia a golpes y vibraciones, alimentación en baja tensión y por último contar con indicadores de paso lumínicos.

En este trabajo, por ser una solución de diseño, se ha seleccionado el molinete marca “DCM”, y el modelo elegido es “MC400HD” (figura 3.2). El mismo está desarrollado por su fabricante para ser utilizado en instalaciones que requieran de un alto grado de seguridad y gran

resistencia mecánica. Ideal para ambientes de intenso tránsito como puede ser el ingreso a un estadio de fútbol.

Figura 3.2. Molinete marca DCM modelo MC400HD.

Información técnica.

- Acceso unidireccional con sentido configurable.
- Gabinete de chapa de acero inoxidable de 2mm de espesor con acabado satinado.
- Cono porta aspas de aluminio mecanizado.
- Tres aspas de 500 mm de largo de tubo de Acero inoxidable de 38mm de diámetro y 2mm de pared.
- Mecanismo con rotor siempre libre, rodamientos blindados, levas y trinquetes de acero.
- Amortiguador hidráulico industrial.
- Señalización de paso: Luz roja - Luz verde.
- Sensores de posición del brazo a contacto seco.
- Solenoide de 12 Vdc.
- Sistema Anti-pánico Autosuficiente (SAA).
- Peso 60 Kg.

3.1.3 Placa de Control

La función principal de la placa de control, es la de controlar la apertura o cierre del mecanismo que realiza el movimiento de las aspas del molinete. Por ello quien se encarga de interpretar la señal recibida por el lector biométrico de habilitación o no de paso, es la mencionada placa.

Los requisitos básicos que debe cumplir la placa de control son los siguientes:

- Entradas de habilitación de paso a contacto seco.
- Salidas de señal de paso, para indicación lumínica.
- Indicación sonora de habilitación.

En este trabajo, por ser una solución de diseño, se ha seleccionado la marca “DCM” (mismo fabricante del molinete) y el modelo elegido es la placa “PCA100” (figura 3.3). La misma es una placa electrónica controladora de molinetes para ser integrada en sistemas de control de acceso de personas.

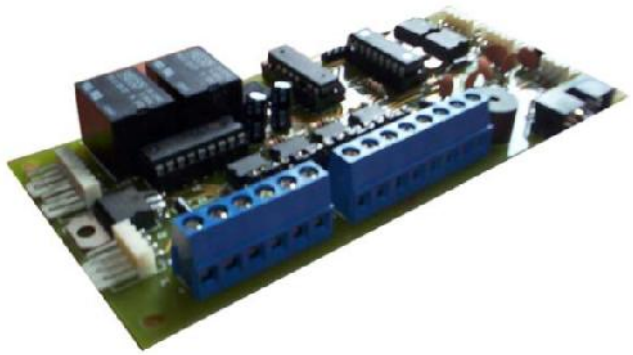


Figura 3.3. Placa de control PCA100 de DCM.

Características principales.

- Alimentación de 12V@ 3A.
- Control de molinetes uni o bidireccionales
- Control de molinetes con rotor siempre libre o siempre trabado.
- Entradas de habilitación de paso opto acopladas o a contacto seco.
- Salidas de señal de paso a colector abierto (Opcional a contacto seco).
- Entradas de manejo de pictogramas opto acopladas o a contacto seco y salidas a relay.

- Control de solenoides con transistores de potencia con protección.
- Indicación sonora de habilitación.

Funcionamiento de la placa controladora.

La placa PCA100 controla el paso del molinete luego de aplicada una señal de habilitación de entrada. La secuencia de funcionamiento para “motor siempre trabado” es la siguiente:

- Normalmente el mecanismo se encuentra trabado no permitiendo el paso de personas por el molinete.
- Al recibir una señal en la entrada de habilitación la placa de control emite una señal sonora y acciona el solenoide correspondiente permitiendo el paso en ese sentido.
- Al realizarse el paso de la persona los sensores detectan el giro de las aspas y la placa de control deshabilita al solenoide quedando el mecanismo nuevamente trabado.
- La placa de control posee un sistema de time-out que al no pasar una persona durante un tiempo de 30 segundos (aproximadamente) luego de recibir la señal de entrada se deshabilita el paso volviendo a su estado inicial.

3.1.4 Buzón captura de tarjetas

Como se indicó en el capítulo II, de acuerdo a la situación actual, algunos establecimientos deportivos cuentan con control de acceso a través de tarjetas de banda magnética que permite la validación del boleto al espectador. Por lo tanto es necesaria la incorporación de un dispositivo de captura de tarjetas, capaz de validar el boleto como así también permitir su devolución.

Los requisitos básicos que debe cumplir el buzón capturador de tarjetas son los siguientes:

- Salida de habilitación de paso a contacto seco.

En este trabajo, por ser una solución de diseño, se ha seleccionado la marca “DCM” (mismo fabricante del molinete) y el modelo elegido es el buzón de captura “BU200” (Figura 3.4).

Figura 3.4. Buzón BU200 de DCM.

Este buzón posee un sensor óptico en la boquilla, el cual cuando se obtura, el solenoide principal es accionado para la apertura del primer receptáculo del buzón. Si el sensor permanece un período de 15 a 30 segundos obturado, la placa controladora dejara de accionar al solenoide principal y esperara a que se retire la tarjeta para volver al estado inicial.

Una vez ingresada la tarjeta al primer receptáculo se espera el tiempo asignado por el Ajuste Principal (TM) para retornar la tarjeta. Si se detecta la señal de STORE, la tarjeta será direccionada al receptáculo inferior donde se almacenara sin esperar el tiempo establecido por el Ajuste Principal.

Principales Características

- Buzón de tarjetas con devolución.
- Control para Retorno de tarjetas rápida velocidad.
- Control para almacenamiento de tarjeta rápido.
- Componentes de gran confiabilidad.
- Posicionamiento de lector de proximidad en primer receptáculo.
- Alimentación de 12 a 13.5V 3Amp.

3.2 Integración de los dispositivos

3.2.1 Ubicación.

Diagrama interno y ubicación de los componentes del molinete MC400HD (figura 3.5)

Figura 3.5. Composición interna del molinete MC400HD.

Ubicación del dispositivo de control biométrico y buzón de tarjetas.

El dispositivo de control biométrico está compuesto por un armazón de plástico. En su interior posee un sensor de huella dactilar hubicado en la parte superior y una placa de circuitos integrados donde esta contenida toda la electrónica, conexionado y puertos. Para lograr una robusta integración, tanto el sensor de huella como la placa de circuitos se debe desmontar del armazón original y luego ensamblar en el denominado “cuerpo de puntera” del molinete MC400HD.

El buzón de tarjetas debe ser colocado en el interior de la denominada “Pata completa”, y su boquilla plástica de acceso en el denominado “cuerpo de puntera” del molinete, como muestra la figura 3.6.

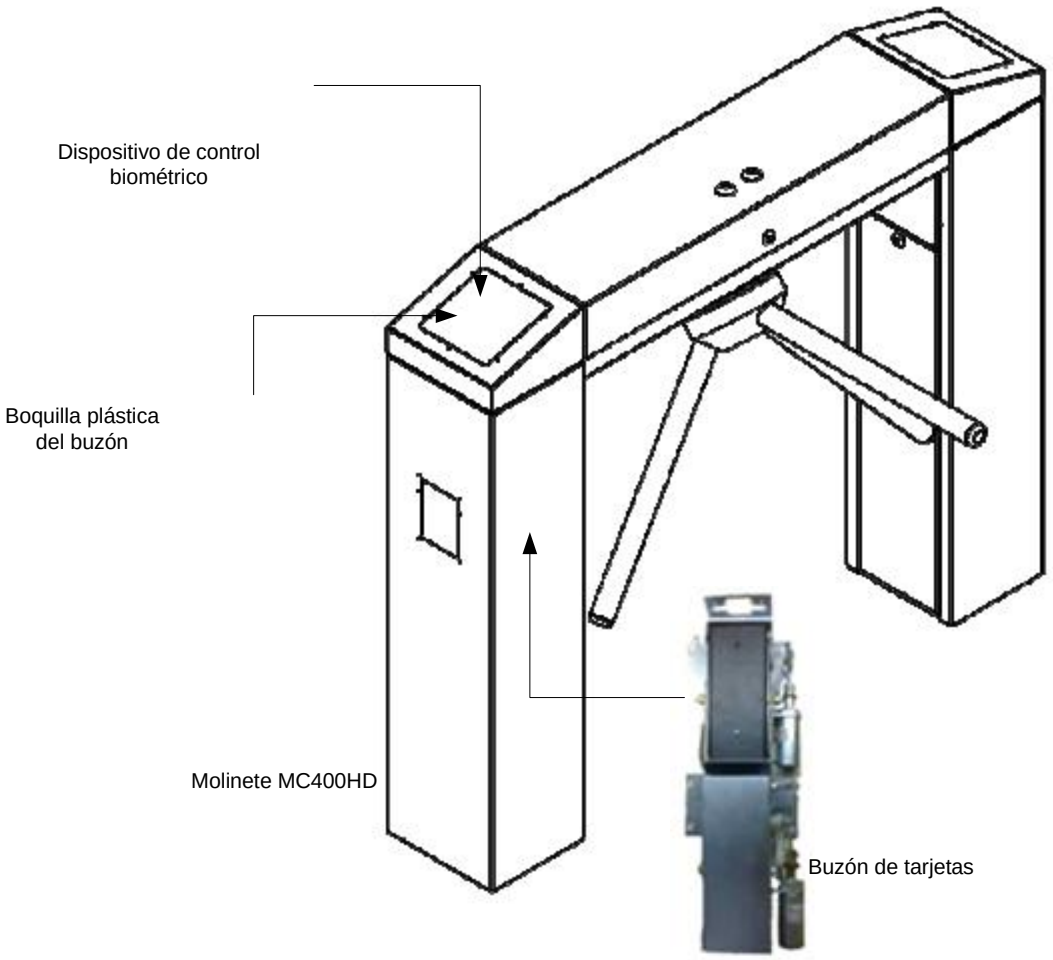


Figura 3.6. Ubicación del lector de huella dactilar y buzón de tarjeta.

3.2.2 Conexionado interno de los dispositivos
Lector Biométrico Search Gate

Para energizar el dispositivo de control biométrico, se puede utilizar una fuente de alimentación AC/DC, o como se ha establecido en este trabajo, se alimenta a través del puerto Ethernet. Utilizando la norma PoE de IEEE 802.3af se suministra energía al lector, por lo que se debe colocar un puente (jumper) en los pines 1 y 2 tanto de JP5 como P6 (figura 3.7).

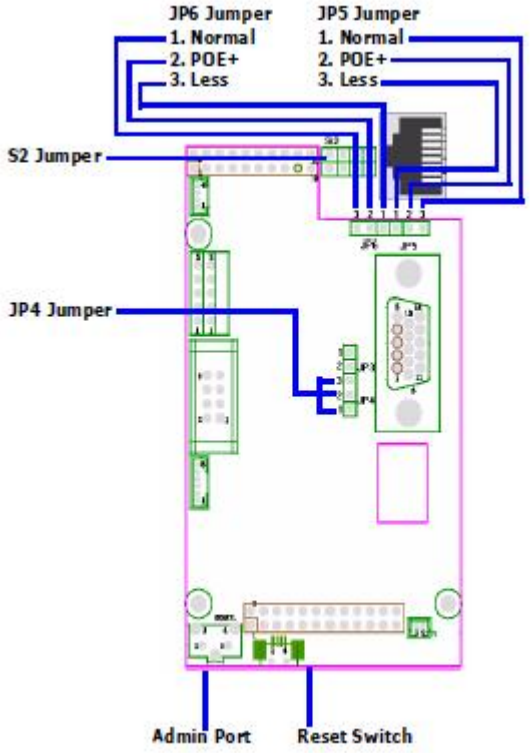


Figura 3.7. Diagrama SearchGate

La comunicación interna entre el lector biométrico y la placa de control del molinete debe realizarse a través de un conector del tipo DB-15 utilizando un relé (figura 3.8).

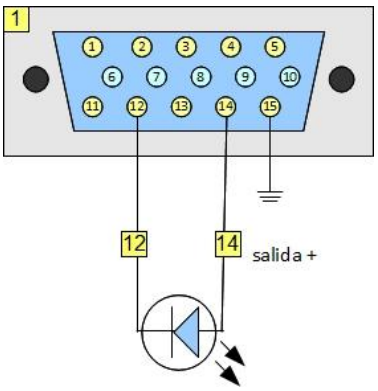
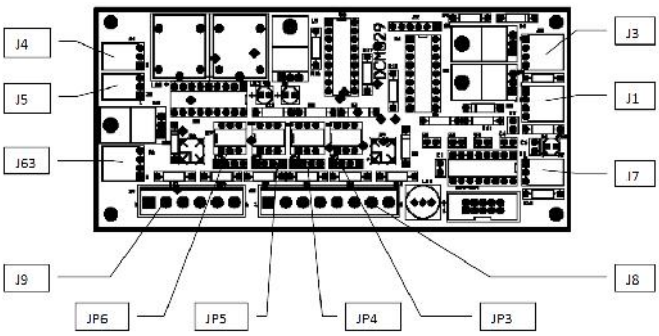


Figura 3.8 Pin Output DB-15 SearchGate

Placa de control PCA100

La distribución de conectores de la placa de control PCA100, es mostrada en el diagrama de conectores (figura 3.9) describiendo cada uno de ellos.



Nombre	Descripción
J1	Entrada Sensores de paso
J3	Salida Solenoides
J4	Salida Pictograma de Entrada
J5	Salida Pictograma de Salida
J6	Jumper Configuración Rotor SL / SC
J7	Sin uso
J8	Entradas
J9	Power / Salidas
JP3	Jumper Entrada Habilitación Salida
JP4	Jumper Entrada Habilitación Entrada
JP5	Jumper Habilitación Pictograma Entrada
JP6	Jumper Habilitación Pictograma Salida

Figura 3.9. Diagrama y descripción de conectores PCA100

Para energizar la placa de control se debe utilizar una fuente de alimentación AC/DC de 12V conectado al pin 1 (GND) y 2 (Positivo) de la bornera J9 (figura 3.10).

PIN	Descripción	Tipo	Valores
1	GND		
2	POWER	Sin protección	12Vdc@3A

Figura 3.10. Conexión bornera J9

En la bornera llamada J8 de la placa de control, deben ser conectados tanto las salidas del lector biométrico como del buzón de captura. Las señales recibidas de estos dispositivos deben ser por pulsos de 60ms. Luego, para utilizar entradas con contacto seco se debe colocar dos puentes (jumper), un entre los pines 1 y 2 y el otro entre los pines 3 y 4 de los conectores JP3 y JP4.

La salida al solenoide del molinete debe ser conexionada a los pines 1 y 2 a través del conector J3 de la placa de control (figura 3.11).

PIN	Descripción
1	12Vdc
2	Salida solenoide 1 (colector abierto 1A máx)
3	12Vdc
4	Salida solenoide 2 (colector abierto 1A máx)

Figura 3.11. Conexión bornera J3

Por último, para indicar de forma lumínica el acceso o no de la persona, se debe conexionar los semáforos como muestra la figura 3.12.

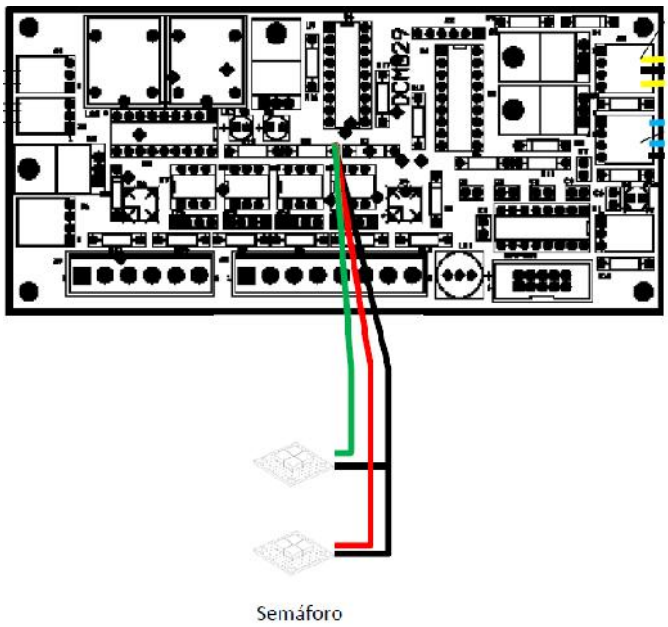


Figura 3.12. Conexionado de semáforo.

3.3 Esquema de funcionamiento

El procedimiento o secuencia típica (figura 3.13) que deberá seguir un espectador para ingresar a un establecimiento deportivo, comienza cuando éste “adquiere un boleto o ticket” para asistir al evento. Este boleto debe ser presentado en el “primer control de acceso”, el cual se realizará de forma manual por una autoridad policial. Éste validará que el espectador tenga el boleto correspondiente.

Luego de pasar el primer control, el espectador se debe dirigir al “control de acceso por molinetes”. Es aquí donde se controlará que pueda o no ingresar al estadio.

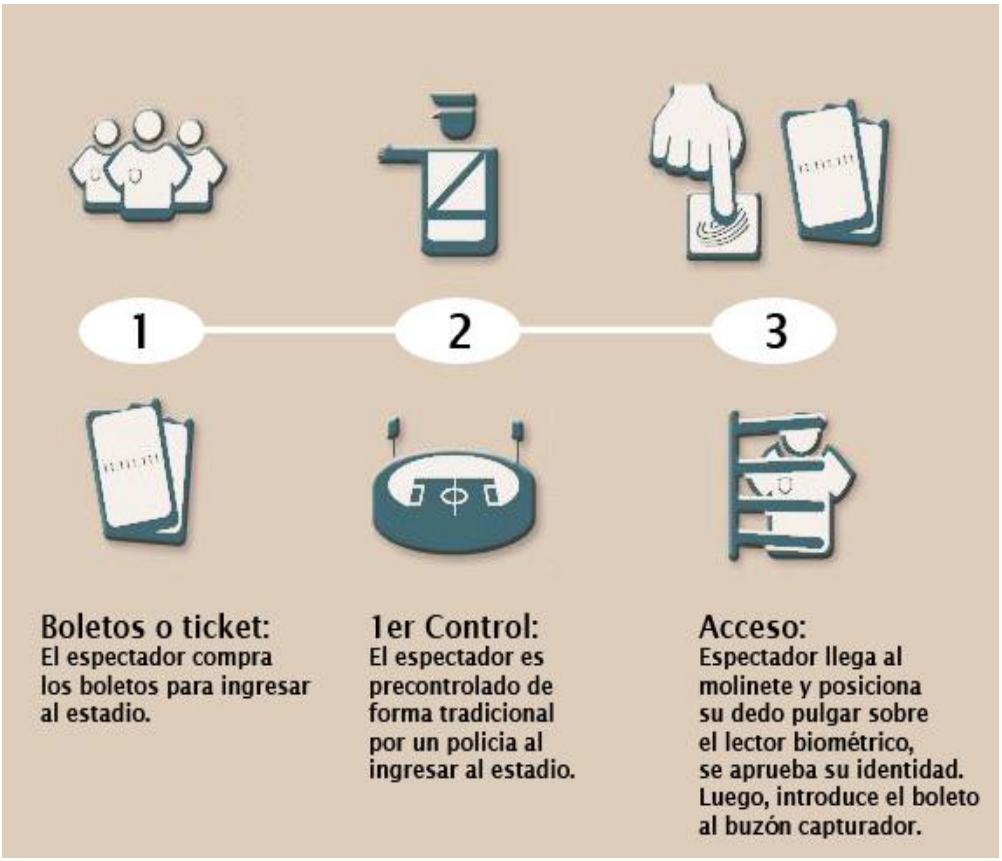


Figura 3.13. Secuencia típica

Para describir con mayor exactitud el tercer paso la figura anterior, se describirá detalladamente la secuencia o proceso de acceso. Luego se presenta un gráfico ilustrativo que describe el proceso mencionado (figura 3.14).

Secuencia o proceso de acceso

1º. El Espectador se presenta al acceso.

2º. Posa su dedo pulgar sobre el lector de huella dactilar ubicado en la parte superior del molinete.

3º. El dispositivo de control biométrico extrae puntos característicos (minucias) de la huella dactilar.

4º. El dispositivo de control biométrico chequea contra su base de datos interna, "lista negra"[18], los puntos característicos extraídos.

5º. En caso afirmativo (coincidencia) deniega el acceso indicando a la placa de control del molinete. Mediante luz indicadora de color rojo y doble pitido audible se le informa al

[18] Lista negra. Listado de huellas dactilar de las personas que se encuentran con prohibición de acceso a eventos deportivos.

Espectador. En esta etapa finaliza el proceso y se regresa al 2° paso. De lo contrario se prosigue al siguiente.

6º. En caso negativo (no coincidencia), se le informa al Espectador mediante luz indicadora de color verde y pitido audible.

7º. El Espectador introduce el boleto (tarjeta) en la boquilla del buzón. Validada ésta última se le permite el acceso indicando al controlador del molinete el destrabe del aspa. Mediante luz indicadora de color verde y pitido audible se le informa al Espectador.

8º. Tanto el dispositivo de control biométrico como el buzón de tarjetas quedan preparados para la siguiente rutina.

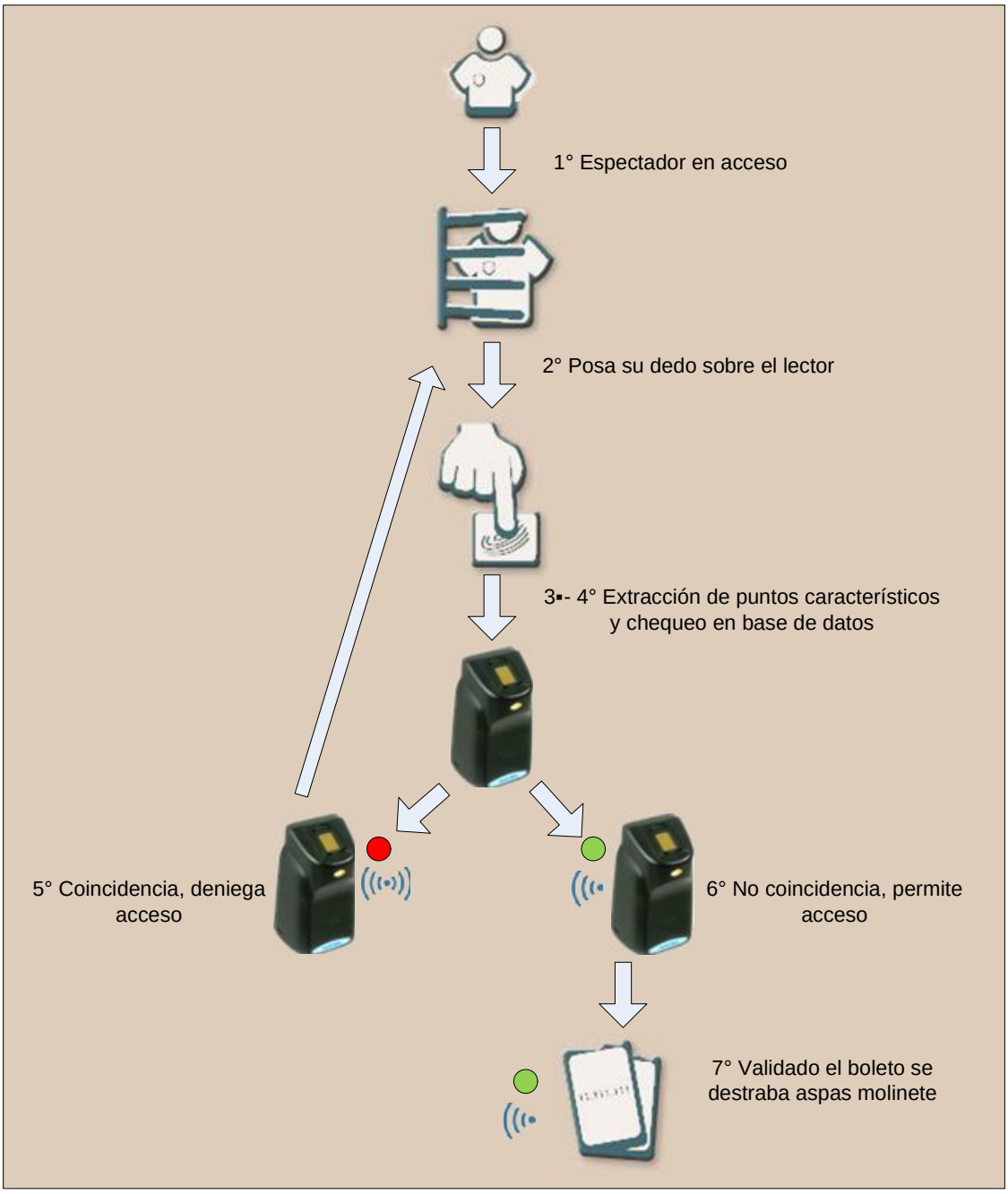


Figura 3.14. Secuencia de identificación típica

3.4 Tiempos de acceso

Como se ha mencionado en el capítulo anterior, según estimaciones de la FIFA, el tiempo que demoran las personas en ingresar al estadio es de una hora o más. Teniendo en cuenta esta afirmación se debe lograr, de acuerdo a la cantidad de personas que pueda albergar el estadio de

fútbol, un flujo de ingreso de personas que garanticen el orden y seguridad, ingresando en un tiempo aproximado de 1 hora - 1 ½ hora.

A continuación se presentan los tiempos estimados que llevará cumplir con cada uno de los pasos descritos en la secuencia de acceso o identificación típica:

1º. El Espectador se presenta al acceso. Tiempo estimado: 0,4 seg.

2º. Posa su dedo pulgar sobre el lector de huella dactilar. Tiempo estimado: 0,9 seg.

3º. Extracción de puntos característicos de la huella. Tiempo estimado: 0,75 seg.

4º. Chequeo contra base de datos interna. Tiempo estimado: 0,75 seg.

5º. Caso afirmativo (coincidencia) deniega el acceso, se regresa al 2° paso. De lo contrario se prosigue al siguiente. Tiempo estimado: 1 seg.

6º. Caso negativo (no coincidencia). Tiempo estimado: 0,8 seg.

7º. Introducción de boleto y validación. Tiempo estimado: 1,3 seg.

8º. Tanto el dispositivo de control biométrico como el buzón de tarjetas quedan preparados para la siguiente rutina. Tiempo estimado: 0,5 seg.

El tiempo de acceso estimado para la solución planteada con reconocimiento dactilar, es de 6 segundos por persona aproximadamente. Tiempo total que llevaría cumplir los pasos 1 hasta 7 detallados en la secuencia anterior. Esto indicaría que por cada molinete de acceso ingresarían aproximadamente diez (10) personas por cada 1 minuto de tiempo transcurrido, el equivalente a seiscientas (600) personas por cada 1 hora y por último novecientas (900) por un período de 1 ½ hora.

A modo de ejemplo, en este trabajo se tomará como caso de estudio el estadio del Club Deportivo Godoy Cruz Antonio Tomba, ubicado en la provincia de Mendoza, con capacidad para recibir un total de 14.000 espectadores.

Para lograr colmar su capacidad en los tiempos descritos anteriormente, es necesario que ingresen aproximadamente 155 personas por minuto a través de sus puertas de acceso. Esto indicaría que en 90 minutos se lograría la totalidad de su capacidad.

Siguiendo el establecimiento tomado como ejemplo, para lograr colmar su capacidad en los tiempos establecidos, se debería contar con una cantidad mínima de 24 molinetes de acceso con control biométrico distribuidos en las diferentes puertas de acceso. Esto garantizaría que los espectadores ingresen en aproximadamente 1 hora.

Debido a la criticidad de la solución, es recomendable prever un molinete adicional por cada una de las entradas de forma de backup, garantizando su funcionamiento a pleno.

Si se desea incrementar el flujo de personas en los ingresos y agilizar los tiempos de respuesta, sólo se deberá agregar más cantidad de molinetes con control biométrico. Si lo que se desea es aumentar la seguridad y disponibilidad, se deberán establecer grupos de molinetes trabajando con sistema redundante de servidores. Ante la caída de alguno de ellos, queda en funcionamiento el/los restantes.

Realizar chequeos aleatorios de las personas, esto es no validar la identificación en el control biométrico de alguna de ellas, lograría una mayor performance en tiempos de acceso. El aspecto negativo de esta modalidad, sería claramente reducir el nivel de seguridad o eficacia del sistema.

CAPITULO IV – COMPONENTES DE SOFTWARE Y HARDWARE TI

En este capítulo se describió todos los elementos de software a ser utilizados en el diseño de la solución planteada. Esto incluye licencias de sistema operativo de los servidores y estaciones de trabajo, bases de datos, y software específico requerido para la implementación.

Luego se continuó con el análisis del hardware de TI necesario, como ser el servidor y UPS a ser utilizados.

Realizado un estudio de mercado respecto al software existente desarrollado por la industria del sector, se concluyó que ninguno cumple con todos los requerimientos específicos y necesarios para implementar la solución planteada.

Esta última afirmación se basó en búsquedas de productos de software de control de acceso por la red de internet. Consultados proveedores del sector a nivel local y nacional no existe software que contemple todas las necesidades alcanzadas por el proyecto.

Por lo manifestado anteriormente, se debe desarrollar un software diseñado especialmente para el propósito requerido.

Su estructura debe estar compuesta por los siguientes módulos de software:

- Sincronización de base de datos con la central policial.
- Administración de roles y usuarios.
- Administración de controles de accesos, control de molinetes, auditoria de movimientos.
- Módulo especial de reportes.
- Adicionalmente podría diseñarse un módulo de auditoría en tiempo real de los accesos al estadio.

4.1 Software de base

El sistema operativo sugerido para el o los servidores es Microsoft® Windows Server 2008 R2 de 64 bits. Dada sus características de rendimiento, disminución en los tiempos de arranque, mejoras en la eficiencia de operaciones E/S para reducir potencia de procesamiento y mejoras generales en la velocidad de los dispositivos de almacenamiento; éste es ideal para cubrir las necesidades de la aplicación a ser soportada.

Para la o las estaciones de trabajo se sugiere utilizar Microsoft® Windows Professional 7 de 64 bits como software de base. Por sus características de rendimiento y versatilidad, es el producto seleccionado para soportar la terminal en el cual se realizará la gestión del sistema en su conjunto.

4.2 Análisis del Software específico

Respecto al software específico, como se mencionó anteriormente, no existe una solución que satisfaga en su totalidad las necesidades específicas de cada uno de los módulos mencionados. Es por esto que se debe realizar el desarrollo de una aplicación de software que integre todas las necesidades del proyecto.

En los puntos siguientes se brinda un análisis del software a ser desarrollado.

4.2.1 Descripción del proyecto de software

Objetivo

Implementar un sistema que permita la sincronización de base de datos con central policial, de las personas con derecho de admisión o denegación del ingreso a estadios de fútbol. Éste debe determinar la administración de molinetes de acceso con control biométrico y registrar cada evento por los puntos de acceso para luego realizar estadísticas o auditorias. El sistema debe permitir su ampliación de funciones de acuerdo a necesidades crecientes.

Entorno y Fundamentos

Descripción de la necesidad – Justificación

Debido que al momento de realizar este trabajo no se cuenta con una solución de software que satisfaga completamente con las necesidades específicas de la Institución Deportiva, surge la necesidad de desarrollar el mismo.

Descripción de la solución

El sistema debe permitir la administración de roles y usuarios, que facilite la administración de la autorización admitiendo especificar los recursos a los que podrán obtener acceso los usuarios del sistema. La administración de funciones deberá permitir tratar los grupos de usuarios como si fueran una unidad mediante la asignación de usuarios a funciones, como administrador, operadores, supervisores, etc.

Determinar el acceso o no de una persona y registrar cada movimiento es una función del módulo de control, el cual debe acceder a la base de datos y realizar las registraciones para luego realizar revisiones y auditorias.

El sistema debe ser fácilmente expandible y configurable sin afectar su rendimiento, haciéndolo especialmente apto para accesos de alto tránsito. Para ello debe ser flexible a la hora de permitir el alta, baja o modificación de los puestos de control o molinetes. Se debe facilitar la parametrización de los molinetes a ser administrados activando, suspendiento o desactivando funciones de control.

Entregables

- Descripción del proyecto
  - Objetivo.
  - Entorno y fundamentos.
  - Definición de entregables.
- Plan del proyecto
  - Metodología de desarrollo.
  - Equipo del proyecto.
  - Arquitectura y tecnología.
- Especificación de requerimientos de software
  - Casos de uso.
  - Requerimientos funcionales.
  - Requerimientos no funcionales.
  - Requerimientos ambientales.
- Plan de desarrollo
  - Información de la versión.
  - Estructura de trabajo y estimados.
- Documento de diseño
  - Información de la versión.
  - Arquitectura.
  - Persistencia (de datos del sistema).
- Plan de pruebas
  - Información de la versión.
  - Pruebas de integración y de sistema.
  - Pruebas de accesibilidad.
  - Pruebas de desempeño.
  - Pruebas de aceptación.

- Manual del operador en formato .doc
- Producto software terminado y aceptado.

4.2.2 Plan del proyecto de software
Metodología de desarrollo
Proceso de Administración del Proyecto[19]

El propósito de la Administración del Proyecto es establecer y llevar a cabo sistemáticamente las actividades que permitan cumplir con los objetivos de un proyecto de software en tiempo y forma esperados.

La Administración del Proyecto aplica conocimientos, habilidades, técnicas y herramientas, a cada una de las siguientes actividades del proyecto:

• **Planificación:** Conjunto de actividades cuya finalidad es obtener y mantener el *Plan del Proyecto* y el *Plan de Desarrollo* que regirán al proyecto específico, con base en la *Descripción del Proyecto*. Para la generación de este plan se deben realizar las siguientes tareas:

- Definir el Proceso Específico con base en la Descripción del Proyecto y el Proceso de Desarrollo y Mantenimiento de Software de la Institución Deportiva.
- Definir Ciclos y Actividades con base en la Descripción del Proyecto y en el Proceso Específico.
- Establecer el Equipo de Trabajo que realizará el proyecto.
- Definir el Plan de Manejo de Riesgos.
- Documentar el Plan del Proyecto.
- Documentar el Plan de Desarrollo.

• **Realización:** Consiste en llevar a cabo las actividades del Plan del Proyecto, de acuerdo a las siguientes tareas.

- Acordar las tareas del Equipo de Trabajo con el Responsable de Desarrollo y Mantenimiento de Software.
- Acordar la distribución de la información al Equipo de Trabajo.
- Revisar el cumplimiento del Plan de Capacitación.

[19] OKTABA, H.; ALQUICIRA ESQUIVEL, C.; SU RAMOS, A.; MARTINES, A.; QUINTANILLA, G.; RUVALCABA, M.; LOPEZ, M.; LOPEZ, F.; RIVERA, M.; OROZCO, M.; FERNANDEZ, Y.; FLORES, M. Modelo de Procesos para la Industria de Software MoProSoft Versión 1.3. NYCE. (México, 2005) Pág. 83.

- Recolectar los Reportes de Actividades, Reportes de Mediciones y Sugerencias de Mejora y productos de trabajo.
- Revisar los productos terminados durante el proyecto.
- Recibir y analizar las Solicitudes de Cambios de la Institución Deportiva.
- Realizar reuniones con el Equipo de Trabajo y con la Institución Deportiva para reportar el avance del proyecto y tomar acuerdos.

• **Evaluación y control:** Consiste en asegurar que se cumplan los Objetivos del proyecto. Se supervisa y evalúa el progreso para identificar desviaciones y realizar Acciones Correctivas, cuando sea necesario. Dentro de esta actividad se realizaran las siguientes tareas:
- Evaluar el cumplimiento del Plan del Proyecto y Plan de Desarrollo.
- Analizar y controlar los riesgos.
- Generar el Reporte de Seguimiento del proyecto.

Como resultado de estas actividades se tiene el Plan del Proyecto y el Plan de Desarrollo actualizados.

• Cierre: Consiste en entregar los productos de acuerdo a un Protocolo de Entrega y dar por concluido el ciclo o proyecto. Como resultado se tiene el Documento de Aceptación de la Institución Deportiva.

Se realizan las siguientes tareas:
- Formalizar la terminación del proyecto o de un ciclo.
- Generar el Reporte de Mediciones y Sugerencias de Mejora.

Objetivos

O1. Lograr los Objetivos del proyecto en tiempo mediante la coordinación y el manejo de los recursos del mismo.

O2. Mantener informada a la Dirección mediante la realización de reuniones de avance del proyecto.

O3. Atender las solicitudes de cambio de la Dirección mediante la recepción y análisis de las mismas.

Indicadores

I1 (O1). El Plan del Proyecto y el Plan de Desarrollo contemplan a los Objetivos establecidos en la Descripción del Proyecto y a las Metas Cuantitativas para el Proyecto.

I2 (O1). Las actividades del proyecto se realizan conforme a lo establecido en el Plan del Proyecto y en el Plan de Desarrollo.

I3 (O1). El tiempo y costo real están acordes con lo estimado.

I4 (O2). Las reuniones de avance del proyecto se realizan conforme a lo acordado con la Institución deportiva.

I5 (O3). El mecanismo de recepción y análisis se aplica a todas Solicitudes de Cambios.

Responsabilidad y autoridad

Responsable:

• Responsable de Administración del Proyecto Específico

Autoridad:

• Responsable de Gestión de Proyectos

Procesos relacionados:

Gestión de Negocio

Gestión de Procesos

Gestión de Proyectos

Desarrollo y Mantenimiento de Software

Roles involucrados y capacitación

Rol	**Abreviatura**	**Capacitación**
Responsable de Gestión de Proyectos	RGPY	Conocimiento sobre las actividades necesarias para llevar a cabo la gestión de proyectos.
Responsable de Administración del Proyecto Específico	RAPE	Capacidad de liderazgo con experiencia en la toma de decisiones, planificación estratégica, manejo de personal, delegación y supervisión, finanzas y desarrollo de software.
Cliente	CL	Interpretación del estándar de la especificación de requerimientos.
Responsable de Desarrollo y Mantenimiento de Software	RDM	Conocimiento y experiencia en el desarrollo y mantenimiento de software.
Equipo de Trabajo	ET	Conocimiento y experiencia de acuerdo a su rol.

Actividades

Rol	Descripción	
A1. Planificación (O1)		
RGPY RAPE RDM	A1.1.	Revisar con el Responsable de Gestión de Proyectos la Descripción del Proyecto.
RAPE CL	A1.2.	Definir conjuntamente con la Entidad Deportiva el Protocolo de Entrega de cada uno de los entregables especificados en la Descripción del Proyecto.
RAPE	A1.3.	Identificar el número de ciclos y las actividades específicas que deben llevarse a cabo para producir los entregables y sus componentes identificados en la Descripción del Proyecto. Identificar las actividades para llevar a cabo el Protocolo de Entrega. Documentar el resultado como Ciclos y Actividades.
RAPE	A1.4.	Identificar y documentar la relación y dependencia de cada una de las actividades.
RAPE RDM	A1.5.	Establecer el Tiempo Estimado para desarrollar cada actividad.
RAPE	A1.6.	Elaborar el Plan de Adquisiciones y Capacitación, definiendo las características y el calendario en cuanto a recursos humanos, materiales, equipo y herramientas, incluyendo la capacitación requerida para que el equipo de trabajo pueda desempeñar el proyecto
RGPY RAPE	A1.7.	Conformar el Equipo de Trabajo, asignando roles y responsabilidades basándose en la Descripción del Proyecto.
RAPE	A1.8.	Asignar fechas de inicio y fin a cada una de las actividades para generar el Calendario de trabajo tomando en cuenta los recursos asignados, la secuencia y dependencia de las actividades.
RAPE	A1.9.	Evaluar y documentar el Costo Estimado del proyecto.
RGPY RAPE RDM	A1.10.	Identificar, describir y evaluar los riesgos que pueden afectar el proyecto, que contemple riesgos relacionados con el equipo de trabajo incluyendo al Cliente y a los usuarios, riesgos con la tecnología o la metodología, riesgos con la organización del proyecto (costo, tiempo, alcance y recursos) o riesgos externos al proyecto. Identificar la probabilidad e impacto de cada riesgo estimando sus implicaciones en los objetivos del proyecto (análisis cuantitativo). Priorizar los efectos de los riesgos sobre los objetivos del proyecto (análisis cualitativo). Desarrollar procedimientos para reducir el impacto de los riesgos. Documentar en el Plan de Manejo de Riesgos o actualizarlo.
RAPE	A1.11.	Generar el Plan del Proyecto o actualizarlo antes de iniciar un nuevo ciclo.
RAPE RDM	A1.12.	Generar el Plan de Desarrollo en función del Plan del Proyecto o actualizarlo antes de iniciar un nuevo ciclo.
A2. Realización (O1, O2, O3)		
RAPE RDM	A2.1.	Acordar con el Responsable de Desarrollo y Mantenimiento del proyecto la asignación de tareas al Equipo de Trabajo incluyendo a los subcontratistas si hubiese.
A3. Evaluación y Control (O1)		
	A3.1	El nivel 1 de capacidad (realizado) no contempla actividades de Evaluación y Control.
A4. Cierre (O1)		
RAPE CL	A4.1.	Formalizar la terminación del ciclo o del proyecto de acuerdo al Protocolo de Entrega establecido en el Plan del Proyecto y obtener el Documento de Aceptación.

Diagrama de flujo de trabajo del proceso de Administración de Proyectos Específicos (figura 4.1).

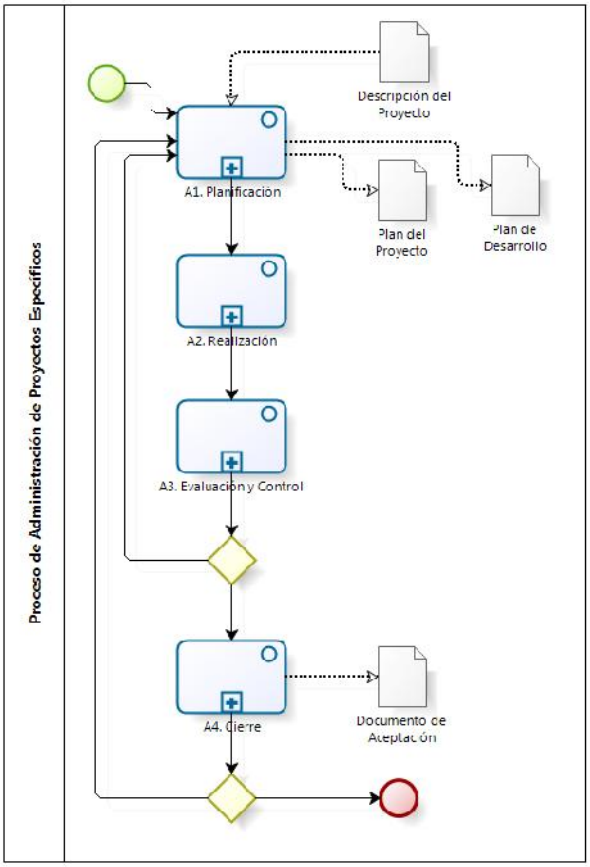
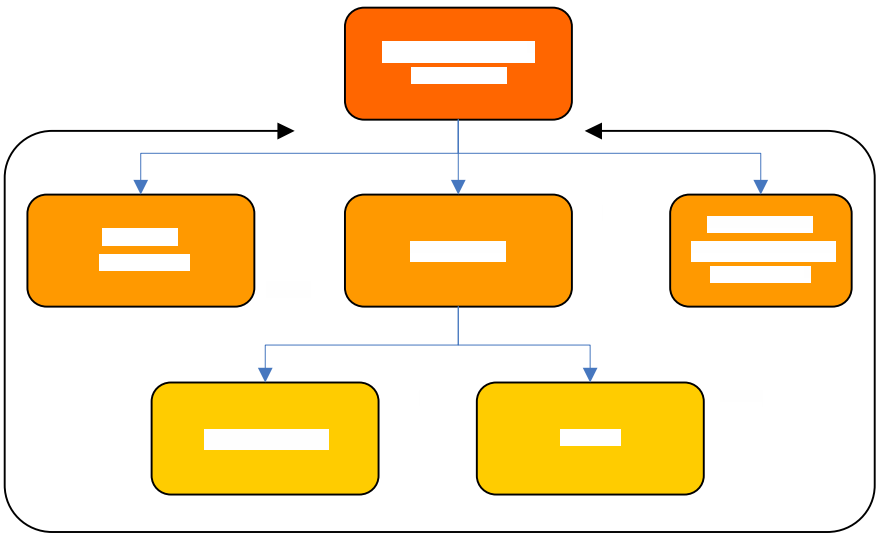


Figura 4.1: Diagrama de Flujo de Trabajo.

Equipo del proyecto
Equipo de trabajo (figura 4.2)

Se recomienda un equipo de desarrollo del producto, que trabaje según los roles reflejados en el siguiente Modelo de Equipo de Trabajo.



4.2 Equipo de trabajo

Descripción

Responsable de Desarrollo y Mantenimiento de Software: Es el responsable de la interacción con los promotores del proyecto y, en conjunto con otros integrantes del equipo, realiza el relevamiento necesario para determinar el alcance del sistema. Además debe efectuar el seguimiento diario de las tareas asignadas a cada uno de los integrantes del equipo de trabajo, y encargarse de llevar adelante la planificación del proyecto, trabajando directamente con el equipo. Es la persona que informa a la Institución Deportiva todas las cuestiones relativas a las tareas cotidianas, y quien implementa acciones para mejorar continuamente la gestión y los resultados obtenidos.

Analista Funcional: Realiza tareas de relevamiento, análisis y diseño de los sistemas informáticos y genera la documentación del sistema, tanto en lo referente al manual del usuario como en lo relativo a su diseño. En caso que corresponda, puede realizar los controles y la supervisión de la programación y el seguimiento del proyecto, además de analizar las pruebas del sistema que se está desarrollando.

Arquitecto: Valida la arquitectura contra los requerimientos pautados. Realiza el diseño técnico de los nuevos proyectos y aplicaciones pequeñas, y programa los módulos complejos. Supervisa a los programadores y testers que participan en el proyecto.

Analista de aseguramiento de calidad: El analista de aseguramiento de calidad garantiza que se cumplan los objetivos del proyecto. Supervisa y evalúa el progreso para identificar desviaciones

y realiza acciones correctivas cuando sean necesarias. Genera el reporte de seguimiento del proyecto.

Programador: Efectúa la codificación y documentación del sistema. Además realiza pruebas sobre sus códigos para eliminar o corregir deficiencias o errores.

Tester: Es el responsable de la ejecutar las tareas determinadas en el plan de pruebas del sistema y el plan de pruebas de integración, y de generar la documentación de respaldo de las tareas realizadas.

Arquitectura y tecnologías

Se indican a continuación las recomendaciones pertinentes para la construcción del producto software.

Conjunto de tecnologías:

- Proceso de desarrollo dirigido por metodologías ágiles, o por casos de uso, centrado en la arquitectura, iterativo e incremental.
- Programación orientada a objetos y en tres capas: Esto permite hacer los programas y módulos más fáciles de escribir, mantener y reutilizar. También ordena al sistema de forma que nunca se acceda a la base de datos en forma directa, sino a través de operaciones o transacciones de capas intermedias.
- Documentación y modelado en UML: Lenguaje Unificado de Modelado es el lenguaje de modelado de sistemas de software más conocido y utilizado en la actualidad; aún cuando todavía no es un estándar oficial, está apoyado en gran manera por el OMG (Object Management Group). Es un lenguaje gráfico para visualizar, especificar, construir y documentar un sistema de software. UML ofrece un estándar para describir un "plano" del sistema (modelo), incluyendo aspectos conceptuales tales como procesos de negocios y funciones del sistema, y aspectos concretos como expresiones de lenguajes de programación, esquemas de bases de datos y componentes de software reutilizables.

Herramientas de desarrollo

- Sistema Operativo: Microsoft Windows 7.
- Lenguaje de programación: Microsoft Visual C#
- Software de desarrollo: Visual Studio Professional 2012
- Base de datos: Oracle Database 11g
- Suite de oficina: Open Office

- Cliente de administración de la base de datos: SQL Developer 3.2.2
- Gestión de proyectos: Mioga, aplicación groupware para gestionar proyectos en Intranet.
- Modelado UML: ArgoUML, software editor UML gratuito.

4.2.3 Especificación de Requerimientos de Software (ERS)

Casos de Uso

Actores

Administrador

Operador

Público

Diagrama de casos de uso Figura 4.3

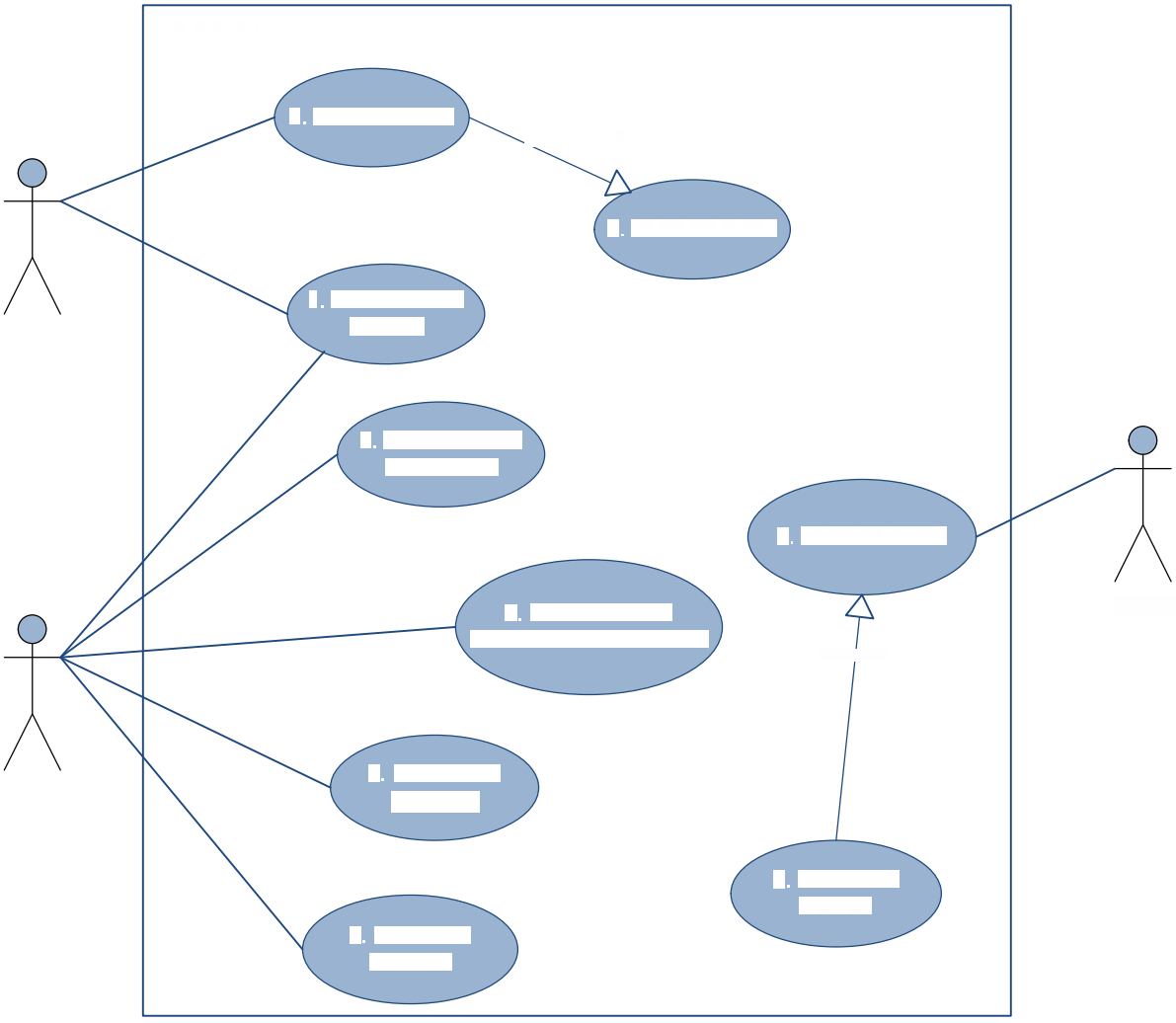


Figura 4.3 Casos de Uso

4.2.4 Documento de Diseño

Interfaz de Usuario

Mapa funcional

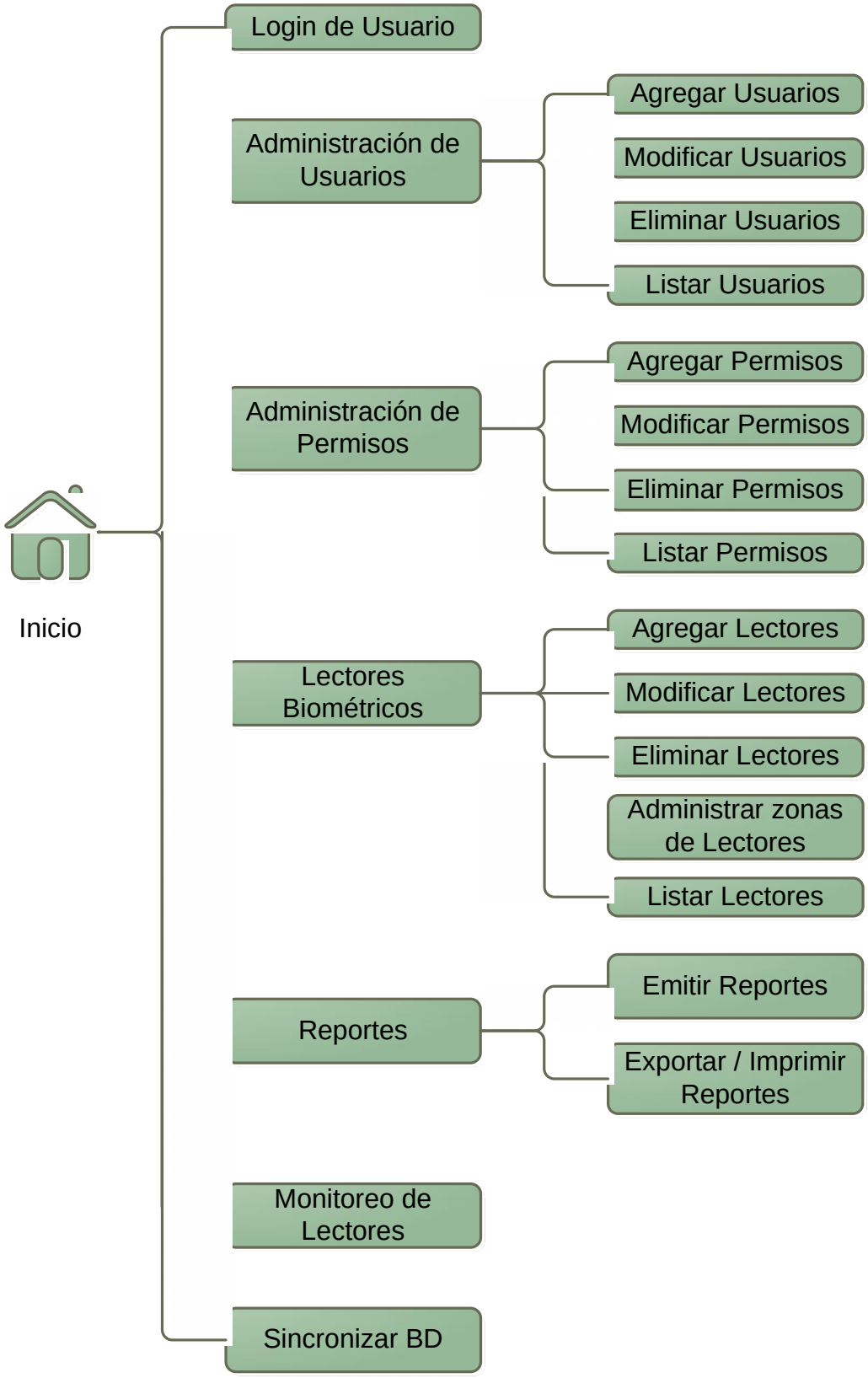


Figura 4.4 Mapa Funcional

Persistencia

Diagrama Entidad Relación (figura 4.5)

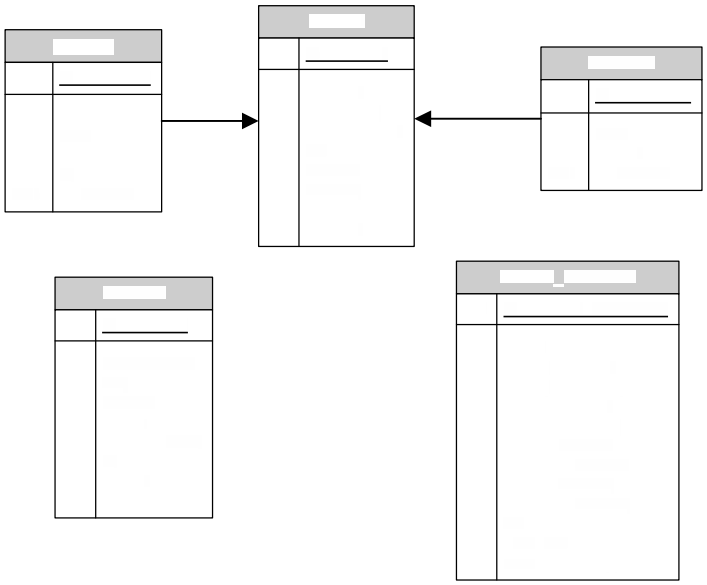


Figura 4.5 Diagrama entidad relación

Base de datos del Sistema (Figura 4.6)
Nombre de la base de datos: dbaccesoestadios

Ubicación: La base de datos debe estar alojada en el servidor de aplicación (ver punto "*4.4 Servidor*").

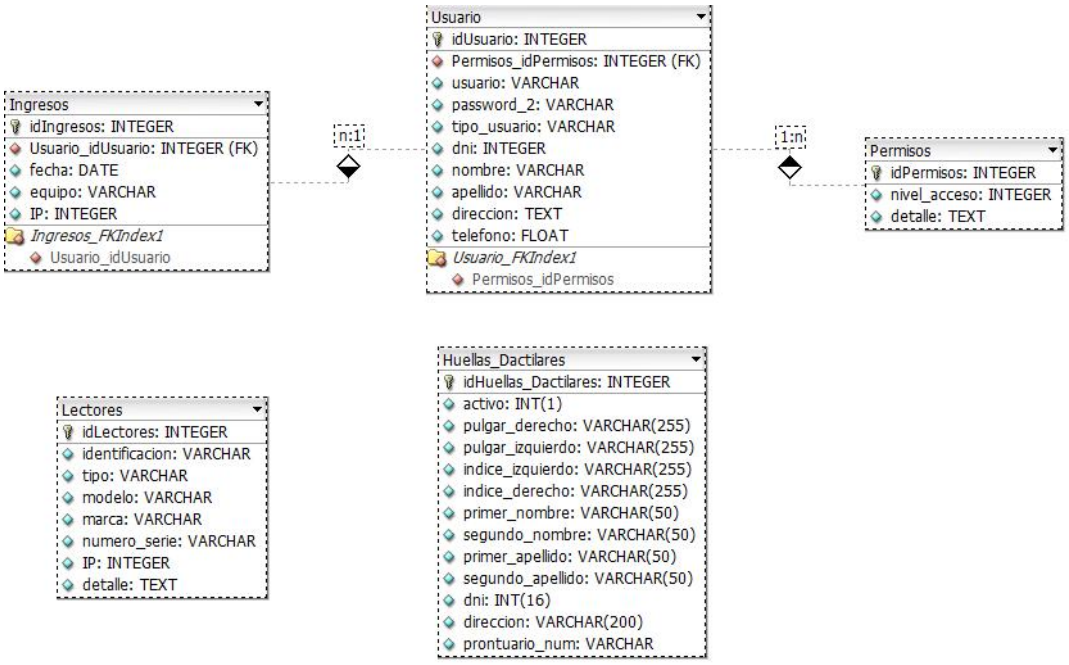


Figura 4.6 Diagrama Base Datos

4.3 Base de Datos

La base de datos del sistema debe mantener información centralizada y actualizada frecuentemente, de las personas que se encuentran alcanzadas por las leyes mencionadas en el capítulo III. La frecuencia de actualización debe realizarse de forma diaria (sugerida), o en su defecto semanal, sincronizando la información proveniente del sistema policial de identificación de huellas dactilares AFIS.

El sistema AFIS contiene las huellas decadactilares (diez dedos) de todas las personas que se encuentran con prohibición de acceso a espectáculos deportivos. El organismo de control actualiza de forma periódica quienes pueden o no acceder a los recintos. De esta manera, quien decide el acceso de una persona es la autoridad policial.

Para el caso planteado, la huella dactilar que debe contener la base de datos del sistema a ser desarrollado, debe ser del dígito pulgar derecho. En caso de no encontrarse se debe suplantar por el dígito pulgar izquierdo o el dedo índice de ambas manos. La sincronización se debe realizar de forma automática, o de existir algún error debe permitir la realización manual por el operador del sistema. A demás de las huellas dactilares, el sistema debe transmitir o sincronizar datos demográficos básicos referentes a las personas. Éstos deben ser: tanto primer y segundo nombre como apellido, DNI, dirección y por último número de prontuario.

En el aspecto técnico, el motor de base de datos debe ser de la marca Oracle, en correspondencia con el utilizado por el sistema AFIS. Las características de Oracle respecto a su seguridad y robustez hacen de éste, el ideal para ser utilizado por aplicaciones de alta estabilidad y escalabilidad. Soportando múltiples plataformas, Oracle es flexible y adaptable a las necesidades.

4.4 Servidor

La base de datos debe estar alojada en un servidor con características especiales. Debe poseer una capacidad adecuada para las exigencias tanto de procesamiento como almacenamiento de imágenes.

Luego de realizar un estudio de mercado de las tecnologías disponibles, el servidor que soporte tanto el sistema como la base de datos debe ser de marca IBM. El modelo System x3650 M3 (figura 4.7), cumple ampliamente con las exigencias planteadas en este trabajo. Creado para soportar la tecnología de procesadores Intel Xeon más reciente, dota al procesamiento extrema potencia. Integrado con los nuevos adaptadores RAID (array redundante de discos independientes) a 6 Gigabits por segundo (Gbps) y el doble de rendimiento de entrada/salida (E/S), ofrece una

arquitectura sólida ideal para aplicaciones de vital importancia. El soporte de memoria avanzada y la mayor capacidad de disco permiten hacer uso de mayores velocidades de procesamiento sin sacrificar tiempo de actividad.

Figura 4.7. Servidor IBM System x3650 M3

Principales características del servidor:

- Chasis de 2U (Unidades de rack).
- Soporta hasta dos procesadores Intel Xeon de la serie 5600 a 3,46 GHz de seis cores (3,60 GHz en la versión de cuatro cores) y velocidad de acceso a memoria de hasta 1333 MHz.
- Alto rendimiento con módulos RDIMM (Registered Dual Inline Memory Modules) de hasta 192 GB o módulos UDIMM de 48 GB; memoria Double Data Rate 3 (DDR-3) de nueva generación.
- Flexibilidad de almacenamiento interno gracias a las dieciséis unidades de disco duro (HDD) de 2,5" hot-swap Serial Attached SCSI (SAS)/Serial Advanced Technology Attachment (SATA) o Unidades de estado sólido (SSD) como máximo.

Para cubrir las necesidades del sistema y base de datos, la configuración sugerida es de dos procesadores Intel Xeon 5600, 32 Gb de memoria RAM DDR3 1333MHZ con 6 discos de 1Tb de almacenamiento cada uno.

Respecto a estos últimos se sugiere establecer un almacenamiento con estructura de discos en RAID[20] nivel 1 para soportar el sistema operativo. Utilizando dos discos, esta configuración otorga confiabilidad ante fallas en alguno de ellos. Para alojar la base de datos, se sugiere que se establezca una estructura de discos en RAID nivel 5 con los cuatro discos restantes, que permite

[20] RAID (Conjunto Redundante de Discos Independientes): sistema de almacenamiento que usa múltiples discos duros o SSD entre los que se distribuyen o replican los datos.

distribuir la información entre todos los discos miembros del conjunto. Los discos mencionados deben poseer características de “Hot-swap” o intercambiables en “caliente”.

Para añadir alta disponibilidad al servidor, éste debe contar con fuente de poder redundante, que permita su utilización indistinta ante fallos de alguna de ellas. Conectadas a un Sistema de Alimentación Ininterrumpida o UPS[21], lograría un alto nivel de autonomía. En este trabajo se seleccionó la reconocida marca APC por cumplir con una autonomía establecida de 50 minutos aproximadamente, con su modelo On-Line Smart-UPS RT 6000VA (figura 4.10), permitiendo alimentar a un servidor que consuma 700W.

Figura 4.8. UPS APC Smart-UPS RT 6000VA

[21] UPS: Dispositivo con baterías, que puede proporcionar energía eléctrica por un tiempo limitado y durante un corte eléctrico a todos los dispositivos que tenga conectados.

CAPITULO V – TELECOMUNICACIONES

5.1 Establecimientos deportivos

La conexión de todos los sistemas, estaciones de trabajo, servidores y dispositivos de control biométrico en los establecimientos deportivos, se debe realizar a través de conexiones de red tipo LAN Ethernet. El cableado estructurado debe cumplir con la norma ANSI/TIA/EIA-568-B.2-1 Categoría 6[22]. Esto facilitará el mantenimiento, instalación y actualizaciones del sistema, permitiendo el conexionado y agregado de puntos de control fácilmente. Los equipos activos (switches) deben ser de alta disponibilidad con un potente rendimiento de red y confiabilidad. Deben poseer control de tráfico de la red mediante funciones avanzadas y la velocidad de trabajo debe ser de 10/100 Mbps.

Luego de un estudio realizado, teniendo en cuenta el caso de estudio, a continuación se presenta un resumen de las características técnicas mínimas que debe poseer el/los equipos activos a ser utilizados en el diseño de la solución planteada.

- Velocidad de trabajo: 10/100 Mbps
- Cantidad de puertos: 28 o superior.
- Seguridad: soporte de listas de control de acceso (ACL[23], Access Control Lists) para impedir el acceso de usuarios no autorizados; LAN virtuales (VLAN[24]) para aislar servicios críticos del tráfico de los usuarios temporales; seguridad de puertos IEEE 802.1X[25], para limitar el acceso a determinados segmentos de la red.
- Alimentación por Ethernet: 24 puertos con soporte PoE.
- Compatibilidad con IP: compatibilidad nativa con IPv4.
- Administración remota: mediante el Protocolo simple de administración de redes (SNMP, Simple Network Management Protocol).

En este trabajo, por ser una solución de diseño, se ha seleccionado el equipo de marca Cisco modelo SG300-28P (figura 5.1) que cumple ampliamente con las características descritas anteriormente.

[22] ANSI/TIA/EIA-568-B.2-1 Categoría 6: Estándar de cables para Gigabit Ethernet.
[23] ACL: Permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.
[24] VLAN: Método de crear redes lógicamente independientes dentro de una misma red física.
[25] IEEE 802.1X : Norma del IEEE para el control de acceso a red basada en puertos.

Figura 5.1. Switch Cisco SG300-28P

Para obtener óptimos resultados y alta disponibilidad en los equipos de conectividad, éstos deben ser protegidos por UPS (Sistema de Alimentación Ininterrumpida). Los requisitos de disponibilidad descritos deben ser de un tiempo aproximado de 50 minutos de autonomía para alimentar dos equipos activos que consuman 200W en total. En este trabajo, por ser una solución de diseño, se ha seleccionado el equipo marca APC con su modelo Smart-UPS 1000VA (figura 5.2), el cual lograría los niveles de autonomía establecidos.

Figura 5.2. UPS APC Smart-UPS 1000VA

5.2 Enlace a central policial

Para conseguir que los datos se sincronicen entre el establecimiento deportivo y la central policial, debe existir un enlace de datos con una capacidad o ancho de banda adecuado. Debe soportar un tráfico de información donde viajarán imágenes de resolución media e información referente a datos filiatorios de las personas con prohibición de acceso a eventos deportivos. La velocidad de conexión sugerida del enlace es de 2 Mbps.

A los efectos de garantizar la seguridad de las comunicaciones, se sugiere la incorporación de un Router con capacidades avanzadas de encriptación de datos. El mismo debe poseer, de acuerdo a las características del enlace, dos interfaces del tipo Ethernet. También debe ser de alta velocidad de trabajo, disponibilidad y posibilidad de soportar VPN[26].

De acuerdo a las exigencias técnicas descritas anteriormente, se ha seleccionado el equipo Cisco 1941 (figura 5.3) de la serie 1900.

Los routers de servicios integrados de la serie Cisco 1900 ofrecen una amplia gama de características, entre las que se pueden destacar:

[26] VPN: Red privada virtual, es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada

- Conectividad ininterrumpida y alto rendimiento con servicios integrados que permite un excelente desenvolvimiento en ambientes WAN[27] de alta velocidad y confiabilidad.
- Diseño modular que ofrece una óptima flexibilidad de servicio.
- Excelente seguridad que incluye firewall, sistema de prevención de intrusiones y filtrado de contenidos para proteger contra ataques maliciosos y amenazas.
- Soporte para redes VPN que permite colaborar en forma segura mediante los métodos Group Encrypted Transport VPN (GETVPN), Dynamic Multipoint VPN (DMVPN), o Enhanced Easy VPN.
- La redundancia, incluidos diagnósticos y fuentes de alimentación de respaldo, aumenta la tolerancia a fallas y tiempo de disponibilidad.

Figura 5.3. Router Cisco 1941

El conexionado del router se debe realizar con los puertos Gigabit Ethernet del tipo RJ45. A traves de los puertos etiquetados con GE 0/1 y GE 0/0 en color amarillo, se debe conectar el enlace al proveedor de servicios WAN y el servidor del establecimiento deportivo respectivamente (figura 5.4).

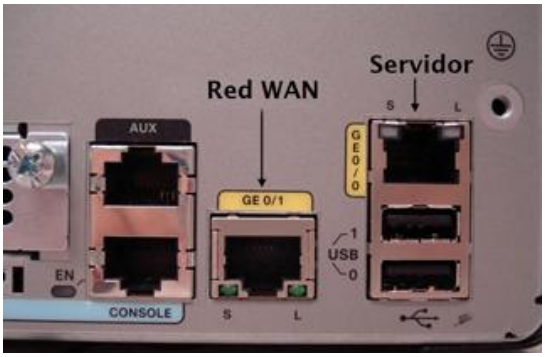


Figura 5.4. Conexionado Router Cisco 1941

[27] WAN: Red de área amplia de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km.

5.3 Esquema de Conexionado

A los efectos ilustrativos, a continuación se muestra un esquema de conexionado del sistema (figura 5.5).

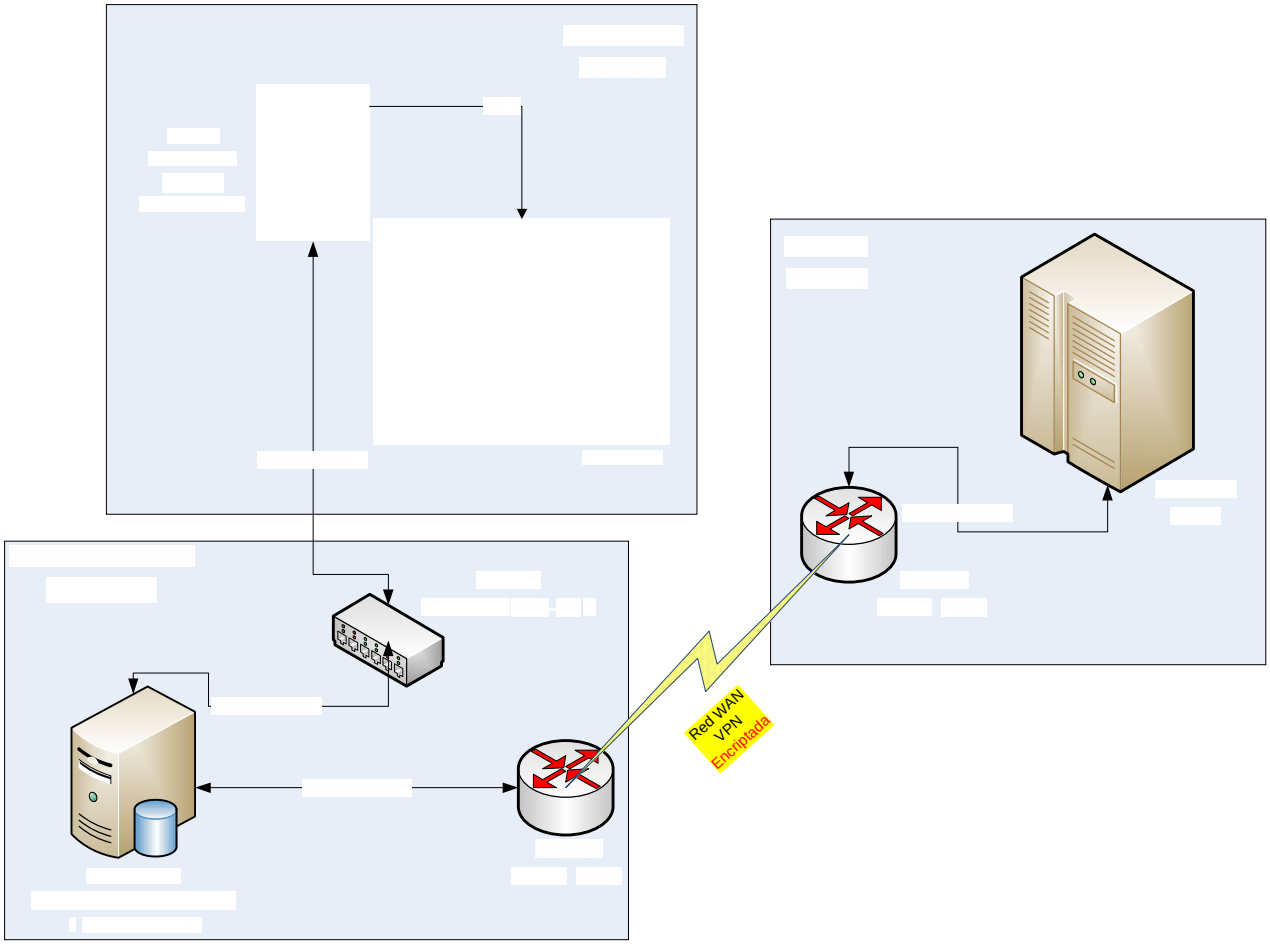


Figura 5.5. Esquema de conexionado.

CAPITULO VI – IMPACTO ECONÓMICO, CULTURAL Y TECNOLÓGICO

6.1 Análisis económico

Para realizar un análisis o conveniencia económica del proyecto, se tomó en cuenta todos los costos asociados a su implementación.

Por ello sumaron gastos que serán incurridos en equipamiento tecnológico o hardware, como ser el servidor que alojará el sistema. De acuerdo a la selección realizada, el costo del servidor IBM System x3650 M3 es de aproximadamente u$s 6.000 al momento de realizar este trabajo. Como se describió en capítulos anteriores, para lograr un alto nivel de autonomía en el servidor, se debe incorporar un Sistema de Alimentación Ininterrumpida (UPS) de la marca APC modelo On-Line Smart-UPS RT 6000VA, cuyo costo es de aproximadamente u$s3.700.

Respecto a la solución de conexión de todos los sistemas, estaciones de trabajo, servidores y dispositivos de control biométrico, se selecciono el Swtich marca Cisco modelo SG300-28P, cuyo costo es de u$s1.250 aproximadamente, alimentado por una UPS marca APC cuyo modelo Smart-UPS 1000VA cuesta alrededor de u$s 450. La cantidad necesaria de equipos de conexión dependerá de la totalidad de puntos de control biométricos a ser instalados.

En relación a los dispositivos de control biométricos, según la selección realizada el Search Gate de marca 3M Cogent System tiene un costo cercano a los u$s600. La cantidad a ser utilizada, como se mencionó en el párrafo anterior, dependerá de la cantidad de puntos de control.

Cabe aclarar que en este trabajo, no se analiza el costo de los molinetes, placa de control y buzón de tarjetas, ya que se da por cierto que el establecimiento deportivo posee estos dispositivos y el control biométrico será integrado a los mismos.

Para garantizar la seguridad y estabilidad de las comunicaciones entre la central policial y el establecimiento deportivo, se sugirió la incorporación del router marca Cisco modelo 1941 cuyo costo es de u$s250 aproximadamente. Respecto al servicio de conexión o enlace recién mencionado, éste posee un costo mensual de prestación, que al momento de realizar este trabajo se determina en aproximadamente u$s260 la conexión de 2Mbps.

Respecto al software relacionado al diseño de la solución planteada, se debe tener en cuenta el software de base seleccionado, que corresponde a Microsoft Windows Server 2008 R2 de 64 bits standard edition, tiene un costo de u$s1.200 aproximadamente. Para la estación de trabajo que

realizará la administración del sistema en su conjunto, se seleccionó Microsoft Windows Professional 7 como software de base con un costo de u$s270 aproximadamente.

El principal componente de software es el específico, que debe determinar el acceso o no de una persona y registrar cada movimiento. Esta función corresponde al módulo de control, el cual debe acceder a la base de datos y realizar las registraciones para luego realizar revisiones y auditorias.

Debe permitir la administración de roles y usuarios, facilitar la administración de la autorización. La administración de funciones deberá permitir tratar grupos de usuarios mediante la asignación de usuarios a funciones, como administrador, operadores, supervisores, etc.

Como se menciono en el capítulo IV, este software debe ser desarrollado por no existir en el mercado. El costo de desarrollo e implementación según los cálculos establecidos es de aproximadamente u$s15.000.

Por último, se deben tener en cuenta los gastos relacionados a la integración de los dispositivos de control, cableado estructurado incluyendo todos sus componentes, servicios de parametrización, instalación, configuración de todo el software relacionado, y el gerenciamiento de la totalidad proyecto; que asciende a u$s 20.000 aproximadamente.

A continuación se brinda una tabla a modo de resumen de los costos establecidos.

	Cantidad	Costo
Servidor IBM, System x3650 M3	1	u$s 6.000
UPS APC, On-Line Smart-UPS RT 6000VA	1	u$s 3.700
Switch Cisco, SG300-28P	2	u$s2.500
UPS APC, Smart-UPS 1000VA	1	u$s450
Control Biométrico 3M Cogent System, Search Gate	24	u$s14.400
Router Cisco, 1941	1	u$s250
Conexión de 1mbps (costo anual)	1	u$s3.120
Microsoft® Windows Server 2008 R2 de 64 bits	1	u$s1.200
Software específico	1	u$s15.000
Microsoft® Windows Professional 7	1	u$s270
Instalación, integración, cableado, configuración, parametrización y gerenciamiento del proyecto.	1	u$s20.000
Servicio de mantenimiento (costo anual)	1	u$s18.000
Costo total		u$s84.000

De acuerdo al análisis de costos realizado anteriormente, dada la envergadura del proyecto, y sus beneficios relacionados respecto a la seguridad en el ingreso, se logra determinar que los mencionados costos pueden ser cubiertos por las instituciones o establecimientos deportivos intervinientes. Gracias al beneficio social que conllevará este proyecto, los costos podrían ser cubiertos a través de financiamientos de organismos externos o entidades gubernamentales.

En este trabajo se determina que existe una conveniencia económica viable del proyecto.

6.2 Análisis socio cultural

El control de acceso permitiría dejar fuera de los establecimientos a quienes se encuentren con algún antecedente de causar problemas. Esto impactaría directamente en la disminución de los problemas descritos en el capítulo II y los ayudaría a mitigar.

Debido a la constante difusión en los medios de comunicación que día a día reflejan la violencia en los estadios de fútbol, los desmanes y destrozos ocurridos durante cada evento deportivo, como se dijo en el párrafo anterior, aplicar este método ayudaría a resolverlo.

En este trabajo se determina que existe una conveniencia socio-cultural aceptable del proyecto tratado.

6.3 Análisis tecnológico

En la actualidad, al momento de realizar este trabajo, se cuenta con una amplia gama de equipamiento tecnológico disponible en el mercado. Tanto el servidor que soporta la aplicación como así también los equipos de conectividad están disponible en el mercado local. La tecnología de adquisición y control biométrico se ha desarrollado ampliamente y se cuenta con una amplia oferta. El equipo biométrico seleccionado en este trabajo, está disponible y puede ser adquirido en el mercado local.

Respecto al enlace de datos requeridos para el proyecto, puede ser adquirido y es un servicio que proveedores locales se encuentran habilitados para prestar.

Dado los avances en el desarrollo de aplicaciones y la capacidad existente en el país de mano de obra calificada, confeccionar el software específico resulta viable o factible de realización. En el mercado local existen empresas dedicadas al desarrollo de software con amplia experiencia por lo que resulta factible su realización.

En este trabajo se determina que existe una conveniencia tecnológica plausible del proyecto.

CONCLUSIÓN

De acuerdo al propósito determinado al inicio de este trabajo, se ha logrado establecer el diseño de una solución tecnológica para implementar la autenticación biométrica en estadios de fútbol, complementando los actuales sistemas de control. Para ello se ha determinado cuáles deben ser los dispositivos de adquisición de huellas dactilares a ser utilizados y también como deben ser integrados a los controles actuales. Luego se ha seleccionado tanto el hardware y software a ser desarrollado para sustentar la implementación de la totalidad del sistema, como así también las telecomunicaciones a ser requeridas.

El marco legal le otorga legitimidad al proyecto, y el sustento para su realización se establece con la creciente violencia dentro de los espectáculos deportivos. Aplicando controles más rigurosos en los accesos no se permitiría ingresar a personas apremiantes.

Los análisis de impacto económico, cultural y tecnológico, determinan que el proyecto es viable en su totalidad, ya que los recursos económicos pueden ser afrontados por los establecimientos deportivos; culturalmente el impacto sería aceptable y la tecnología actual permite la realización del mismo.

Tomando una de las premisas del proyecto de establecer tiempos de acceso adecuado, se ha determinado con un caso ejemplo, que el proyecto es sustentable y viable, permitiendo el ingreso de las personas a los establecimientos deportivos en los tiempos establecidos por organismos internacionales.

BIBLIOGRAFÍA, FIGURAS Y GLOSARIO
Bibliografía

PICOUTO RAMOS, Fernando – LORENTE PÉREZ, Iñaki – GARCÍA, Jean Paul – RAMOS, Antonio Ángel. Hacking y Seguridad en Internet. Madrid, España, 2007.

TAPIADOR MATEOS, Marino y SIGUENZA PIZARRO, Juan A. Tecnologías biométricas aplicadas a la seguridad (Madrid, España, 2005).

GRAÑA ROMAY, Manuel. Estudio sobre el reconocimiento de huellas dactilares. Publicación en la Universidad de Guipúzcoa, España, 2007.

RATHA, Nalini y BOLLE, Ruud. Automatic Fingerprint Recognition Systems (New York, 2004).

WAYMAN, James. Biometric Systems Technology, Design and Performance Evaluation (London, 2005).

MALTONI, Davide y otros. Handbook of Fingerprint Recognition (New York, 2005).

NOBUYUKI, Otsu. A Threshold Selection Method from Grey-Level Histograms. IEEE Transactions Analysis and Machine Intelligence (EEUU, 1990).

HARALICK, R.M.; STERNBERG, R.S. y ZHUANG , X. Image analysis using mathematical morphology. IEEE Trans. Pattern Analysis and machine intelligence (EEUU, 1987) Pág. 532-550.

ESPINOSA DURÓ, V.Fingerprint thinning algorith. IEEE AES Transaction aerospace and electronics systems (EEUU, 2003).

MALLAT, S. A wavelet tour of signal processing (EEUU Academic Press, 1999).

OKTABA, H.; ALQUICIRA ESQUIVEL, C.; SU RAMOS, A.; MARTINES, A.; QUINTANILLA, G.; RUVALCABA, M.; LOPEZ, M.; LOPEZ, F.; RIVERA, M.; OROZCO, M.; FERNANDEZ, Y.; FLORES, M. Modelo de Procesos para la Industria de Software MoProSoft Versión 1.3. NYCE. (México, 2005).

https://secure.interpol.int/

http://www.afa.org.ar/

http://www.apc.com/

http://www.biometria.gov.ar/

http://www.cisco.com/

http://www.cogentsystems.com/

http://www.dcm.com.ar/

http://www.fifa.com/

http://www.ibm.com/

http://www.nist.gov/

http://www.seguridad-la.com/

http://www.uv.es/

http://www.wikipedia.org/

http://www.xelios.es/

Imágenes

Figura 1.2 (a): Cuatro tipos de minucias. *Fuente Revelado de huellas lofoscópicas en papel. http://www.monografias.com/trabajos57/huellas-lofoscopicas/huellas-lofoscopicas3.shtml*

Figura 1.2 (b): Ejemplos de otras características. *Fuente Revelado de huellas lofoscópicas en papel. http://www.monografias.com/trabajos57/huellas-lofoscopicas/huellas-lofoscopicas3.shtml*

Figura 1.4: Clasificación de Henry de Huellas Dactilares. *Fuente Marino Tapiador Mateos – Juan A. Siguenza Pizarro. Tecnologías biométricas aplicadas a la seguridad. Madrid, España, 2005.*

Figura 1.5: Arcos. *Fuente Revelado de huellas lofoscópicas en papel. http://www.monografias.com/trabajos57/huellas-lofoscopicas/huellas-lofoscopicas3.shtml*

Figura 1.6: Presillas internas. *Fuente Revelado de huellas lofoscópicas en papel. http://www.monografias.com/trabajos57/huellas-lofoscopicas/huellas-lofoscopicas3.shtml*

Figura 1.7: Presillas externas. *Fuente Revelado de huellas lofoscópicas en papel. http://www.monografias.com/trabajos57/huellas-lofoscopicas/huellas-lofoscopicas3.shtml*

Figura 1.8: Verticilo. *Fuente Revelado de huellas lofoscópicas en papel. http://www.monografias.com/trabajos57/huellas-lofoscopicas/huellas-lofoscopicas3.shtml*

Figura 1.9: Versión simplificada en 3D de un sensor CCD. *Fuente Dispositivos Sensores de Luz. https://proyectotelematica.wikispaces.com/d.08.03.04+Dispositivos+Sensores+de+Luz*

Figura 1.10: Arquitectura típica del sensor capacitivo. *Fuente Marino Tapiador Mateos – Juan A. Siguenza Pizarro. Tecnologías biométricas aplicadas a la seguridad. Madrid, España, 2005.*

Figura 1.11: Sensor capacitivo. *Fuente UPEK FIPS 201 Compliant Silicon Fingerprint Sensor. http://www.upek.com/*

Figura 1.14: Estimación del campo de orientación. *Fuente Marino Tapiador Mateos – Juan A. Siguenza Pizarro. Tecnologías biométricas aplicadas a la seguridad. Madrid, España, 2005.*

Figura 1.16: Ejemplo de preprocesado sobre una huella dactilar. *Fuente Marino Tapiador Mateos – Juan A. Siguenza Pizarro. Tecnologías biométricas aplicadas a la seguridad. Madrid, España, 2005.*

Figura 1.17: EE genérico de la transformación Thinning. *Fuente Marino Tapiador Mateos – Juan A. Siguenza Pizarro. Tecnologías biométricas aplicadas a la seguridad. Madrid, España, 2005.*

Figura 1.18: Patrones y pasos de rotación utilizados. *Fuente Marino Tapiador Mateos – Juan A. Siguenza Pizarro. Tecnologías biométricas aplicadas a la seguridad. Madrid, España, 2005.*

Figura 1.19: Ejemplo de huella adelgazada mediante la transformación descrita. *Fuente Marino Tapiador Mateos – Juan A. Siguenza Pizarro. Tecnologías biométricas aplicadas a la seguridad. Madrid, España, 2005.*

Figura 1.20: Detalles de la eliminación de elementos espurios. *Fuente Marino Tapiador Mateos – Juan A. Siguenza Pizarro. Tecnologías biométricas aplicadas a la seguridad. Madrid, España, 2005.*

Figura 1.21: Detección y discriminación de minucias. *Fuente Marino Tapiador Mateos – Juan A. Siguenza Pizarro. Tecnologías biométricas aplicadas a la seguridad. Madrid, España, 2005.*

Figura 1.22: a) Imagen almacenada, b) Imagen de entrada. *Fuente Gualberto Aguilar, Gabriel Sánchez, Karina Toscano, Mariko Nakano, Héctor Pérez. Reconocimiento de Huellas Dactilares Usando Características Locales. D.F. México, 2008.*

Figura 1.23: a) Imagen almacenada. b) Imagen de entrada. *Fuente Gualberto Aguilar, Gabriel Sánchez, Karina Toscano, Mariko Nakano, Héctor Pérez. Reconocimiento de Huellas Dactilares Usando Características Locales. D.F. México, 2008.*

Figura 1.25: Imagen con la vectorización de todas las minucias respecto de la minucia de referencia. *Fuente Baez Moyano, L. Martín. Extracción de características de Galton de Huellas Dactilares por procesamiento digital de la imagen. UTN FRC.*

Glosario de Términos

PIN: Personal Identification Number

AFIS: Automated Fingerprint Identification System

IAFIS: Integrated Automatic Fingerprint Identification System

CMOS: Complementary metal-oxide-semiconductor.