MONITOREO BIOMETRICO DEL TIEMPO - UCLA
GUIA PARA SU IMPLEMENTACION

YVAN D. GUTIERREZ TERAN

UNIVERSIDAD CENTRO OCCIDENTAL "LISANDRO ALVARADO"

Barquisimeto, 2010

MONITOREO BIOMETRICO DEL TIEMPO - UCLA
GUIA PARA SU IMPLEMENTACION

POR

YVAN D. GUTIERREZ TERAN

Trabajo de Ascenso presentado para optar a la categoría de titular en el escalafón del Personal Docente y de Investigación

UNIVERSIDAD CENTRO OCCIDENTAL "LISANDRO ALVARADO"

DECANATO DE CIENCIAS Y TECNOLOGIA

Barquisimeto, 2010

MONITOREO BIOMETRICO DEL TIEMPO - UCLA
GUIA PARA SU IMPLEMENTACION

YVAN D. GUTIERREZ TERAN

Trabajo de Ascenso Aprobado

_____ _____

_____

Barquisimeto, de Noviembre del 2010

A mi madre, **Juana María Terán** y a mi padre **Miguel Antonio Gutiérrez**, siempre los recordare y estarán en mi, en todo lo que haga, a dondequiera que vaya y dondequiera que esté, con todo mi amor su hijo

A mí querida y amada esposa, **Jamellys Mallanyn González Pérez**
y a mis cuatro amados hijos **Jamellyn Cristina, José Miguel, Yván Alejandro, Leonardo Alfonso y a mi nieta Valeria Valentina**

Cuyas vidas han sido, y siguen siendo para mí fuente de inspiración y guía constante.

Agradecimientos

Es difícil el poder escribir en pocas palabras nuestra gratitud hacia Dios, nuestras familias, nuestros amigos, y diversas instituciones por permitirnos y facilitar la consolidación de este proyecto. En base a esto solamente mencionaremos a algunas de las instancias (humanas e institucionales) que influyeron (creemos) más cercanamente en la escritura de este libro.

En primer lugar queremos agradecer a la empresa ZKSoftware Inc por motivarnos a escribir un libro que esperamos sirva para incrementar la calidad de la educación superior en nuestro país y en algunos de América Latina.

Enseguida queremos agradecer a la Universidad Centro Occidental Lisandro Alvarado por su apoyo para poder materializar diversas ideas en un medio físico.

Dentro de la Universidad Centro Occidental Lisandro Alvarado quisiéramos agradecer de manera muy especial al Vicerrector Administrativo, Licenciado Edgar Alvarado y al Licenciado Miranda por haber confiado en mi, tanto en el apoyo que me dieron en el proyecto actual como en el anterior, fuente inicial de motivación para escribir este libro.

Queremos agradecer a nuestra familia: Jamellys Mallanyn, José Miguel, Yván Alejandro, Leonardo Alfonso y Jamellyn Cristina (y a su primera hija y mi nieta Valeria Valentina). Estamos seguros que sin los sacrificios de ustedes (reconocemos que no les pedimos permiso) no hubiera sido posible terminar en tan corto tiempo este proyecto.

Al final, pero no al último, queremos agradecer a Dios su gran ayuda y apoyo para poder continuar haciendo cosas productivas y trascendentes. Para todos ellos muchas gracias.

Ing., MSc. Yván D. Gutiérrez Terán
Decanato de Ciencias & Tecnología
Departamento de Sistemas

INDICE GENERAL

INDICE DE FIGURAS

Prólogo

La Biometría le ha dado una nueva dimensión a la verificación individual de la identidad. Esta ha permitido la automatización del control y registro del tiempo de las personas sin mucha supervisión en el proceso, en donde esto antes no era posible, proveyendo niveles de exactitud y consistencia que simplemente no puede ser garantizado por los métodos tradicionales, confiando solamente en la interpretación humana. Sin embargo, la verificación biométrica no es infalible y su implementación requiere una comprensión de ambos, la tecnología y la interfaz humana con la tecnología, si se desea lograr el éxito. Se debe ponderar todos los aspectos del diseño biométrico del sistema, incluyendo la interfaz con el usuario, la parte técnica de la arquitectura, el medio ambiente en la cual va a ser utilizada y todos los procesos de trasfondo necesarios para una situación particular. Sólo entonces podemos estar seguros de una implementación exitosa de la tecnología.

Aunque la biometría puede ser vista por algunos como una tecnología nueva o emergente, de hecho ha existido un gran número de sistemas biométricos instalados alrededor del mundo durante la última década. El continuo desarrollo tecnológico en otras áreas como los microprocesadores y las comunicaciones, combinadas con una sociedad cada vez más globalizada, proveerán más oportunidades para integrar la verificación biométrica en otros procesos, para el beneficio de los administradores y usuarios.

Este libro provee una guía simple sobre la implementación de un sistema biométrico, las cosas que hay que tener en cuenta y de las que se debe cuidar, para asegurar una implementación exitosa. También provee de conocimientos básicos sobre el tema de la biometría para todos los que estén interesados en la verificación de la identidad, ya sea porque son potenciales usuarios finales de dicha tecnología o profesionales en el campo tales como asesores o integradores de sistemas. También proveerá una fuente valiosa de referencia al estudiante o investigador académico de biometría, especialmente el capitulo referente al desarrollo de un programa biométrico, en el cual encontrarán una gran cantidad de información práctica para echarlos a andar en su viaje particular de descubrimientos. Ciertamente, hay algo en este libro para todo el mundo, inclusive para la mas alta gerencia y directores de grandes empresas, en el capitulo tres sobre implementando la biometría, podrán encontrar información importante para la toma de decisiones en lo referente a la implementación de la biometría, evaluando aspectos tales como la seguridad, el medio ambiente, costos, entrenamientos, selección de equipos biométricos y muy especialmente el aspecto sicológico que representa todo esto a los usuarios finalmente.

El libro esta organizado como una serie de capítulos autocontenido, que quizás es mejor leído secuencialmente, aunque esto no es esencial. Un lector experimentado puede elegir ir directamente a un capítulo de interés.

Ing. Yván Darío Gutiérrez Terán

1. Orígenes de la Biometría

A continuación presentaremos el relato de un hombre, llamado Khasekem, el cual existió ya hace mucho tiempo y de quien se cree, fue el padre de la biometría, no como la conocemos hoy en día, pero si formo las bases para su creación, ello sucedió ya hace mas de 3000 años, en Egipto, donde todo comenzó. El joven Khasekem podía sentir el calor del camino arenoso del desierto escurrirse a través de sus sandalias, cuando caminaba bajo un sol matutino abrasador en las suaves e inclinadas colinas hacia el muelle en Aswán. Sus pensamientos lo regresaban a sus días de estudiante en Heliópolis en el bajo Egipto, donde se había alojado en la casa de su tío Sebékkhu. Sebékkhu era un hombre de mucha sabiduría y Khasekem estaba muy en deuda con su tío, no solo por su gran generosidad, sino también por su constante orientación durante todo su entrenamiento como escriba en Heliópolis.

Su primer trabajo oficial fue el de copiar algunos de los registros pertenecientes a la construcción de la gran pirámide de Khufú, la cual había sido terminada para el año del nacimiento de Khasekem. Por estos registros sabía que la pirámide tenia una altura de 288 codos[1] con una base de 452 codos cuadrado y requería algo mas de 2,5 millones de bloques de piedra, cada una de las cuales debía ser cortada en forma precisa e identificada respecto a su puesto exacto dentro de la construcción. También sabía que más de 1600 talentos de plata habían sido gastados en alimentos para la mano de obra, la cual había sido aproximadamente de unos 100.000 hombres, muchos de los cuales habían sido de las comunidades de agricultores de la zona y para ellos era un honor tener la oportunidad de trabajar en el proyecto durante el periodo de inundaciones, las cuales ocurrían a menudo por dos o más semanas. La comida y el refugio proveído como consecuencia de la construcción de la pirámide eran particularmente bienvenido en ese momento. Khasekem había notado que existían varias cosas interesantes acerca de la identificación individual y exacta de estas personas.

[1] El *codo real* egipcio, utilizado desde la dinastía III, tenía 52,3 cm.

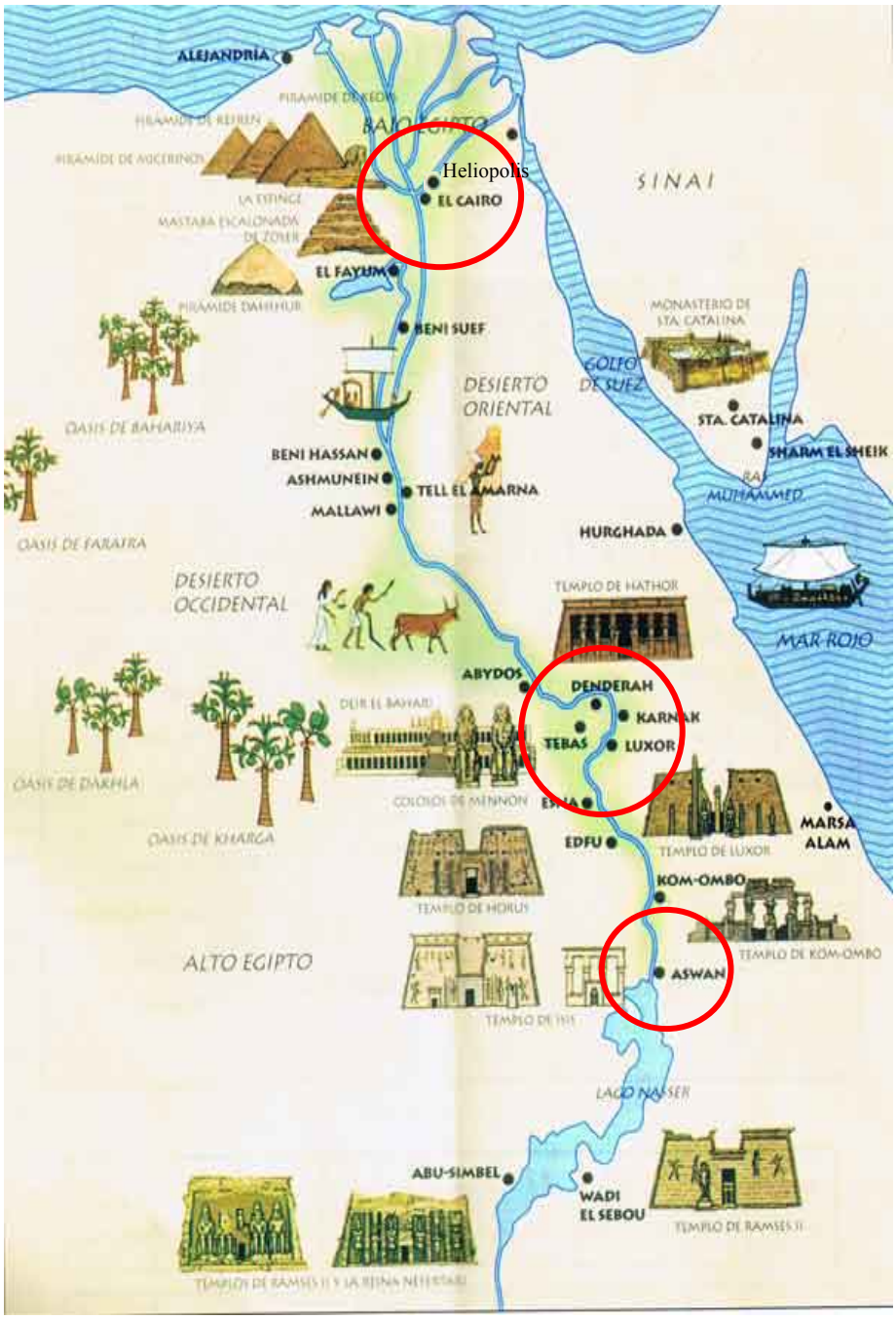


Figura 1.0 Mapa Histórico del viejo Egipto

Otros hombres, particularmente los experimentados picapedreros o canteros trabajarían en el proyecto a tiempo completo, muchos de ellos en canteras muy lejanas cómo Aswán. Esto constituía de alguna forma un desafío logístico, cuando las

provisiones eran recogidas y guardadas en varias áreas y luego transportadas al otro lado de la región a varios puntos donde existían atracaderos sobre el Nilo, de donde podían ser transportados por barco a Aswán. Todas las provisiones tenían que ser contabilizadas y transcritas en los registros centrales. Era el buen trabajo de Khasekem en comprender y copiar con exactitud estos registros, que le habían hecho ganar su posición como ayudante del administrador principal en Aswán cuyo nombre era Tafnékht.

El papel de Khasekem, fue el de administrar y proveer de alimentos a la fuerza de trabajo o mano de obra; un elemento clave en la ejecución y éxito del proyecto. Su sueño era que a través del trabajo duro y la diligencia en esta posición, podría un día ser presentado al gran faraón Khaefré, del cual se sabía que tomaba un interés directo sobre el proyecto y a menudo elogiaba el excelente trabajo de los hombres y su administración cuando estos colmaban su atención.

Figura 1.2 **Estrato social de los habitantes de Egipto**

Las embarcaciones que atracaban en Aswán, normalmente poseían una longitud de 100 codos y lucían magníficamente cuando se acercaban alrededor de la encorvadura del río justo al norte del asentamiento. Khasekem nunca se cansó de observar estos graciosos gigantes aproximarse al embarcadero y ver como en un frenesí de actividades, eran bajadas las velas y las sogas eran lanzadas a la orilla mientras los remeros y el piloto maniobraban hábilmente la embarcación hasta llevarlo a su posición. En su travesía hacia Aswán, traían trigo, cebada y otras provisiones para el almacén bajo la autoridad de Tafnékht, antes de ser cargados con

bloques de piedra listos para ser enviados de regreso al sitio de la pirámide en Gizeh. Khasekem tenía que asegurarse de que todas las provisiones fuesen correctas y bien contabilizadas antes de colocar el sello de Tafnékht en la documentación de retorno. Ésta fue una importante parte de su trabajo, pero la mayor parte de su tiempo, la pasó en la administración de las provisiones de suministros a la fuerza de trabajo.

A cada hombre le fue garantizado el equivalente al pago de 1,5 khárs al mes, formado principalmente de trigo con una proporción de cebada. La medida de un khár era tomada usando una vasija de hekát, usualmente con 16 hekáts se hacia 1 khár. El pago generalmente consistía en 20 hekáts de trigo más 4 hekáts de cebada por hombre, además, se hacia un convenio en donde a cada hombre le sería destinado al mes un día libre, el cual, no lo trabajaría para así poder recolectar sus provisiones del almacén, sujeto a la aprobación de Khasekem, en lo que se refiere a la identidad verdadera del hombre y el derecho legítimo a reclamar la concesión de ese día. Esto había sido antes un asunto algo controversial, ya que se había descubierto que algunos individuos habían tratado de reclamar una concesión dos veces en un mismo mes, alegando una o más identidades. Mientras que las penas por este comportamiento fraudulento eran bastante severas si eran descubiertas, el incentivo por hacerlo eran aún mas fuertes, ya que tales provisiones podían ser canjeadas por otros bienes y servicios entre la comunidad trabajadora. Además de esto, el hecho de mantener una mano de obra de alrededor de 700 hombres en la cantera, no era fácil notar al impostor. Estos acontecimientos eran infrecuentes, pero Tafnékht había dado instrucciones claras y estrictas en nombre del faraón de que tal comportamiento no sería tolerado.

Desde su permanencia en Aswán, Khasekem había estado desarrollando el sistema usado para identificar al personal que solicitaba su paga, por medio del cual, cada persona tenía un registro en el que se estipulaba su nombre, edad, lugar de origen y la ocupación precisa en el sitio de trabajo. Khasekem había estado sistemáticamente añadiendo más detalles a estos registros con el fin de identificar a cada persona con exactitud. Hizo esto notando las características físicas y a veces conductuales de cada persona e incluyéndolas como parte del registro. Por lo tanto, cuando un trabajador que solicitaba su paga se presentaba y daba su nombre, Khasekem podía hacer referencia al registro de esa persona leyendo las notas descriptivas antes tomadas. Por ejemplo, las notas de un registro se podrían leer de la siguiente manera: Nechutés, hijo de Asós, edad cuarenta, de tamaño mediano, el cutis cetrino, semblante alegre, cara larga con la nariz recta y una cicatriz en la mitad de su frente. El detalle dentro de estos registros le permitió a Khasekem verificar la identidad de cada trabajador con exactitud. En los casos en donde había pocas características particularmente distintivas, una medición anatómica sería hecha para complementar el registro. Se tomaría la distancia entre la punta de un pulgar extendido y el codo de su brazo, el cual podría medir alrededor de 1 codo (medida usada por los egipcios), de un hombre adulto de proporciones normales. Una vara de

medir marcada con divisiones se usaría para tomar y posteriormente verificar esta medida.

Veamos un día normal en la vida de Khasekem. Llegaba muy temprano en la mañana, generalmente calurosa y soleada, después de verificar que todo el personal estuviera presente y que el almacén era seguro, consultaba en sus registros para ver quién estaba programado para recopilar sus provisiones. Se había dispuesto atender 23 hombres ese día, por lo que ordeno realizar todos los preparativos así como también, le fuesen traídos todos los registros de estos hombres a su habitación, donde los trabajadores solicitantes se presentarían inicialmente en forma ordenada. Después de verificar que todos los registros estaban presentes y correctos, se daba instrucciones para que el primer hombre se le permitiese entrar y hacer su reclamo. Perábsen, un hombre corpulento con piel ennegrecida por la exposición persistente al sol, caminaba en la habitación a grandes pasos y después de hacer los saludos acostumbrados a Khasekem, anunciaba que era Perábsen de Dendára, que trabajaba con el séptimo equipo de mamposteros sobre la zona 9 de la cantera principal y se le había asignado ese día para recolectar su provisiones. Khasekem rápidamente localizaba el registro pertinente y leía los detalles relevantes de Perábsen, que indicaban entre otras cosas, que era un hombre de constitución robusta, de altura mediana, con una tez oscura y un rasguño leve en un ojo. Además, se notaba que Perábsen tenía una voz particularmente resonante y de una disposición ligeramente impetuosa. La descripción se adaptaba muy bien a sus rasgos, por tanto Khasekem, después de consultar el libro mayor principal para verificar cuando había sido la última vez en la que se le había otorgado provisiones, podía constatar que había sido en realidad un mes atrás, por tanto Khasekem, satisfecho de que todo estaba en orden, daba instrucciones para que a Perábsen se le proveyera con su cupo de provisiones.

El siguiente hombre entró y se presentó como Hárkhuf de Philáe, dedicado a la consignación especial de piedra caliza arreglada para las nuevas e importantes obras en Karnák. Khasekem observó que este hombre cojeaba marcadamente y también que le faltaba un dedo de su mano izquierda, presumiblemente el resultado de algún desafortunado accidente, por lo demás parecía, bien de salud y de espíritu. A él le pareció recordar haber notado previamente tales detalles y se preguntó si estos podían haber sido de este hombre, Hárkhuf. Al consultar el registro de Hárkhuf de Philáe, confirmó que éstos eran efectivamente los rasgos relacionado con este hombre, conjuntamente con otros detalles del cutis y las características faciales que no dejaron ninguna duda a Khasekem con respecto a la verdadera identidad del hombre que estaba frente a él. De nuevo, después de comprobar en el libro mayor principal, Khasekem dio instrucciones para concederle a Hárkhuf su concesión de comestibles y hacer el llamado a presentarse el próximo hombre. Durante todo el día y en una forma similar, los otros 21 hombres fueron presentándose siendo sus identidades verificadas por Khasekem. Después de que al último hombre se le había

proporcionado sus provisiones, el almacén quedaba oficialmente cerrado por ese día y un sello era colocado cuidadosamente sobre las puertas principales. Khasekem completaba las anotaciones en el libro mayor principal y daba instrucciones explícitas para que los registros de las personas chequeadas ese día fuesen regresados al depósito. Khasekem estaba satisfecho de que todo estaba bien y en perfecto orden, cerrando el libro mayor de transacciones por ese día. Ciertamente, así habían sido las cosas, ya que no había ningún ejemplo reciente de reclamos de identidad fraudulento, o la distracción de fondos de las previsiones del almacén; ahora que la administración, severa, pero justa de Khasekem, estaba bien y realmente en su lugar. Esto era de gran satisfacción para Khasekem el poder ver que con su proceso en forma cuidadosa se lograba el objetivo.

Figura 1.3 Khasekem en el viejo Egipto

Khasekem de hecho exitosamente utilizó la verificación biométrica de identidad para mejorar los procesos alrededor de su papel particular de trabajo. Él no tuvo los beneficios de los microprocesadores y la electrónica para ayudar a automatizar el proceso, pero los principios empleados fueron exactamente iguales en lo que respecta a la identificación y registró de una característica anatómica y/o conductual medible, que podía ser recordada posteriormente para verificar la identidad de una persona en particular. A decir verdad, Khasekem estuvo muy por encima de la mayoría de los practicantes de la biometría de hoy en día, en lo que respecta a que podía seleccionar cualquier número de características biométricas y

unirlas todas ellas como fuese necesario para suministrar un modelo de identidad adecuadamente preciso para cada individuo. También trabajó en el hecho de, cómo el continuo despliegue de tales métodos, actúan como un poderoso elemento disuasivo contra reclamos falsos de identidad, mientras proveía un registro exacto de quién estaba haciendo qué y dónde en relación a grandes proyectos civiles y asuntos importantes de estado.

Así pues, que las raíces de la tecnología biométrica a decir verdad, vienen de miles de años atrás. Ciertamente no es la idea novedosa que muchas personas creen que es hoy. Sólo estamos redescubriendo los principios los cuales, al igual que muchas otras cosas, nuestros antepasados en el valle del Nilo ya habían refinado y con éxito implementado dentro de esa civilización elegante y extraordinaria. La deuda que tenemos con el Egipto antiguo en muchas ramas de la ciencia es incalculable y la verificación biométrica representa simplemente un guijarro diminuto, en una playa enorme de conocimientos, con el entendimiento de que de ese período de la historia de la humanidad ése es nuestro legado.

2. Conocimientos Previos a la Implementación

La biometría se basa en la premisa de que cada individuo es único y posee rasgos físicos distintivos (rostro, huellas digitales, iris de los ojos, etc.) o de comportamientos (la voz, la manera de firmar, etc.), los cuales pueden ser utilizados para identificarla o validarla.

Los dispositivos capaces de realizar el proceso de identificación o validación son el tema de esta sección.

Desde sus primeras apariciones en el mercado, este tipo de dispositivos han tenido que sortear tres dificultades fundamentales:

1. Su elevado costo que impedía su despliegue masivo, de cientos o incluso de miles de unidades en las grandes corporaciones donde, cada empleado, debería poseer sus propios dispositivos de seguridad.
2. Su tamaño, demasiado grande para poder instalarlo normalmente en computadores de sobremesa, portátiles o en los pequeños dispositivos de mano tan de moda en la actualidad como teléfonos móviles, PDA´s,... etc.
3. Y por último, la poca sensibilidad mostrada por los grandes proveedores de redes hacia el uso y la necesidad de integración de este tipo de productos biométricos en sus infraestructuras de red.

Este panorama está cambiando drásticamente en estos últimos años como consecuencia del interés y de la necesidad creciente surgida en el mercado a la hora de exigir sistemas más seguros. (Mercado internacional)

La medición biométrica ha venido estudiándose desde tiempo atrás y es considerada en la actualidad el método ideal de identificación humana. Las identificación por medio de las huellas dactilares es una de las forma más representativa de la utilización de la biometría. Existen sin embargo otros dispositivos biométricos que procesan otras características humanas.

En el mundo interconectado del siglo XXI la identificación es insuficiente. Se necesitan sistemas aun más seguros. El control de accesos e intrusión... sean una realidad segura para empresas y consumidores. Ese paso se realizará por medio de los sistemas biométricos los únicos que permiten una AUTENTICACIÓN inequívoca e

individualizada. La presente seccion tiene como objetivo dar a conocer que es un dispositivo biométrico, su origen, conocer los diferentes dispositivos biométricos que existen en el mercado, su funcionamiento y finalmente su implementación. Otro enfoque importante del trabajo es saber cuando o porque se usarían tales dispositivos, tendencias, ventajas y desventajas de su uso.

2.1 ¿Qué es la Biometría?

La palabra biometría deriva de las palabras: bio (vida) y metría (medida).
La ciencia biométrica se define como el análisis estadístico de observaciones biológicas.
Así, un dispositivo biométrico es aquel que es capaz de capturar características biológicas de un individuo (rostro, huella dactilar, voz, etc.), compararlas, electrónicamente, contra una población de una o más de tales características y actuar según el resultado de la comparación.

2.2 ¿Porqué usar Biometría?

La biometría es fácil de usar, nada que recordar nada que cambiar nada que perder. Además proporciona un nivel más alto de seguridad, unívoca "firma" de una característica humana que no puede ser fácilmente adivinada o "hackeada". La Identificación y Autenticación biométrica (I&A) explota el hecho de que ciertas características biológicas son singulares e inalterables y son además, imposibles de perder, transferir u olvidar. Esto las hace más confiables, amigables y seguras que las contraseñas (passwords).

En el pasado el procesamiento de I&A biométrica era hecho manualmente por gente que física y mentalmente comparaba huellas dactilares contra tarjetas, rostros contra fotos de pasaportes y voces contra cintas grabadas. Hoy en día, dispositivos tales como escáneres, videocámaras, y micrófonos pueden, electrónicamente, capturar y entregar estas mismas características biométricas para automatizar procesos y comparaciones. Cada tecnología biométrica (huella dactilar, rostro, voz, etc.) tiene sus propias características, variedades y certezas.

El proceso de captura, extracción de esas características y variedades, el almacenamiento y la comparación es universalmente similar para todos los dispositivos biométricos. Pero no todo es perfecto en estos sistemas. Existe la posibilidad de que el sistema acepte o rechace indebidamente a un usuario. Existen algoritmos que permiten minimizar estos errores.

Los niveles de precisión biométricos pueden variar pero son siempre más confiables que el 100% de falsas aceptaciones experimentadas con las contraseñas prestadas o robadas.

2.3 Funcionamiento Básico del Dispositivo Biométrico

La figura siguiente, muestra el diagrama en bloques de un sistema biométrico general y describe brevemente su funcionamiento.

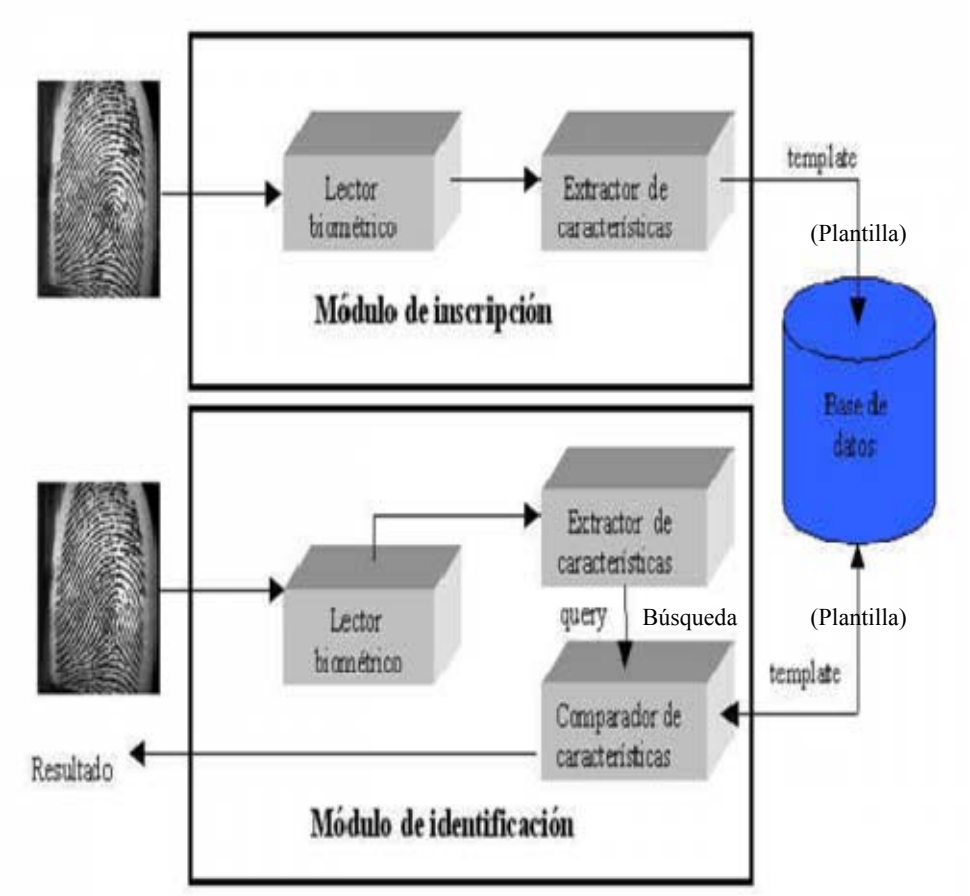


Figura 2.1 Módulos para el reconocimiento de Huellas dactilares

La mayoría de los sistemas biométricos funcionan de maneras muy similares y se puede resumir en dos pasos:

- El primer paso consiste en que la persona debe registrarse (“enroll” en inglés) en el sistema. Durante el proceso de registro, el sistema captura el rasgo característico de la persona, como por ejemplo la huella digital, y lo procesa para crear una representación electrónica llamada plantilla de referencia (“reference

template" en inglés.) La plantilla de referencia debe ser guardado en una base de datos, una tarjeta inteligente ("smart card" en inglés), o en algún otro lugar del cual será extraído en cualquier ocasión futura para el segundo paso.

A pesar de que es poco probable obtener dos tomas iguales aún del mismo individuo, a causa de diferencias ambientales y otras condiciones en el momento de la captura, el sistema aún debe poder funcionar correctamente. La mayoría de los algoritmos de comparación generan un ámbito para cada ensayo de comparación el cual es cotejado dentro de determinados umbrales antes de ser aceptados o rechazados. Cada proveedor de tecnología biométrica configura la/el falsa/o aceptación/rechazo de forma diferente. .

La figura siguiente muestra esta relación de compromiso.

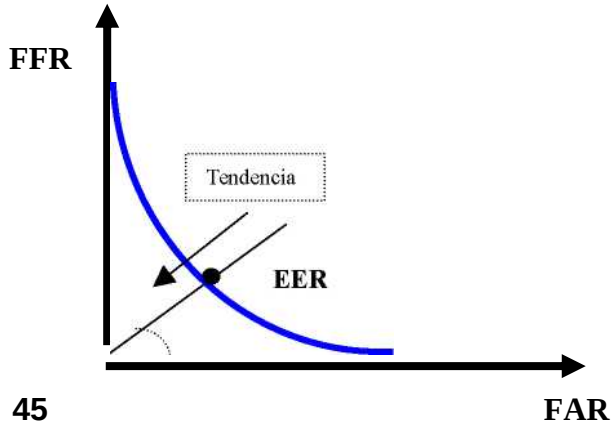


Fig. 2.2 Relación entre FAR, FRR y ERR

Para determinar las prestaciones de un sistema biométrico, nos remitiremos al análisis y valoración de los siguientes parámetros estándares

- FAR (False Acceptance Rate – Falsa Aceptación): Porcentaje de personas no autorizadas aceptadas por el sistema.
- FRR (False Reject Rate - Falso Rechazo): Porcentaje de personas autorizadas no aceptadas por el sistema.
- SR (Success Rate - Exito): Responde a una combinación de los dos factores anteriores que se utiliza como indicador de la resolución total del sistema.

$$SR = 1 - (FAR + FRR)$$

- ERR (Equal Error Rate – Error de igualdad): El FAR y el FRR responden a parámetros inversamente proporcionales, por tanto, variarán en función de las

condiciones prefijadas por el programa de identificación biométrica. Así, si por ejemplo debemos utilizar el programa en un entorno de máxima seguridad, intentaremos que el FAR sea el más pequeño posible, aunque esta acción signifique de forma implícita, el incremento drástico del factor FRR. Deberemos fijar un parámetro o umbral que nos permita igualar los dos factores, asegurando de esta manera el óptimo funcionamiento del sistema. Este umbral se denomina Equal Error Rate (ERR), y es el que determinará, finalmente, el poder de identificación del sistema.

Las tasas de errores son medidas de dos maneras, una por la cantidad de personas con permiso que son rechazadas (tasa de falso rechazo) y otro por la cantidad de personas sin permiso que son aceptadas (tasa de falsa aceptación o indebida). En este caso, es claro, que la mayor preocupación se centra con el segundo tipo, pero en implementaciones prácticas el primer problema genera mucha molestia.

Si el umbral es demasiado bajo, se vuelve demasiado fácil para una persona no autorizada ser aceptada por el sistema, en cambio si el umbral está demasiado alto, personas autorizadas pueden llegar a ser rechazadas.

- De acuerdo a la teoría tradicional en biometría, el segundo paso depende de si la función del sistema biométrico consiste en verificar la identidad de la persona o identificar a la persona.

  1. En el caso de verificación, la persona le informa al sistema cual es su identidad ya sea presentando una tarjeta de identificación o entrando alguna clave especial. El sistema captura el rasgo característico de la persona (la huella digital en nuestro ejemplo) y lo procesa para crear una representación electrónica llamada plantilla en vivo (“live template” en inglés.). Por último, el sistema compara la plantilla en vivo con la plantilla de referencia de la persona. Si ambos modelos parean la verificación es exitosa. De no serlos, la verificación es fallida.

  2. En caso de que la función del sistema biométrico sea identificación, la persona no le informa al sistema biométrico cual es su identidad. El sistema tan solo captura el rasgo característico de la persona y lo procesa para crear la plantilla en vivo. Luego el sistema procede a comparar la plantilla en vivo con un conjunto de modelos de referencia para determinar la identidad de la persona.

     Dependiendo de la función del sistema, este segundo paso puede ser:

     - **Identificación positiva**

La función de un sistema de identificación positiva consiste en probar que la identidad de la persona está registrada en el sistema. La persona hace una reclamación positiva de identidad al sistema biométrico, es decir, la persona alega que está registrada en el sistema. El sistema responde comparando automáticamente la plantilla en vivo con uno o varios modelos de referencia. Si la persona es identificada, el sistema biométrico le concede a la persona ciertos privilegios, de lo contrario los privilegios son negados.

- **Identificación negativa**

La función de un sistema biométrico de identificación negativa consiste en probar que la identidad de la persona no está registrada en el sistema biométrico. Un ejemplo puede ser un sistema que verifique que las personas que entran a un banco no se encuentren en una lista de delincuentes. La persona le hace una reclamación negativa de identidad al sistema biométrico, el cual responde comparando automáticamente la plantilla en vivo con uno o varios modelos de referencia. Si la identidad no está registrada, el sistema biométrico le concede ciertos privilegios a la persona como, por ejemplo, permitirle entrar al banco. Si el sistema reconoce a la persona, este le niega dichos privilegios y hasta quizás alerte si se debe tomar alguna acción más radical como intervenir la persona.

Tanto en verificación como en identificación, si la comparación es exitosa el sistema biométrico concede a la persona ciertos privilegios como, por ejemplo, acceso a un área restringida o acceso a su cuenta de banco. Cuando la comparación es fallida, los privilegios son negados.

2.4 Reconocimiento Facial

De todas las técnicas biométricas, el reconocimiento facial es quizás el más fascinante en concepto, especialmente para el laico que puede tender a desestimar lo que involucra la identificación fidedigna de personas por sus características faciales bajo condiciones operacionales del mundo real.

Al considerar los sistemas de reconocimiento faciales, sería útil poder subdividirlo en dos grupos primarios.

- En primer lugar, existen a lo que podríamos referirnos como grupos de escenas controladas, por medio del cual, el sujeto a ser examinado es colocado

en un ambiente conocido con una cantidad mínima de variaciones en la escena. Por ejemplo, en una situación típica de control de acceso, el sujeto ordinariamente estará de cara a la cámara a una distancia medianamente constante, produciendo cuadros sobre la imagen de proporciones generalmente similares.

- En segundo lugar, existen a lo que podríamos referirnos como grupos de escenas aleatorias, por medio del cual el sujeto a ser examinado, podría aparecer donde quiera dentro de la escena de la cámara, a diversas distancias de la cámara y en diversos grados del eje desde la posición directamente adelante. Esta situación podría ser encontrada, por ejemplo, con un sistema que este tratando de identificar la presencia de un individuo dentro de un grupo o multitud.

Estos dos grupos representan proposiciones muy diferentes para el diseñador de sistemas. Además de estos grupos primarios, está la pregunta de si requerimos la funcionabilidad de verificación (comparación uno-a-uno) o de identificación (comparación uno-a-muchos).

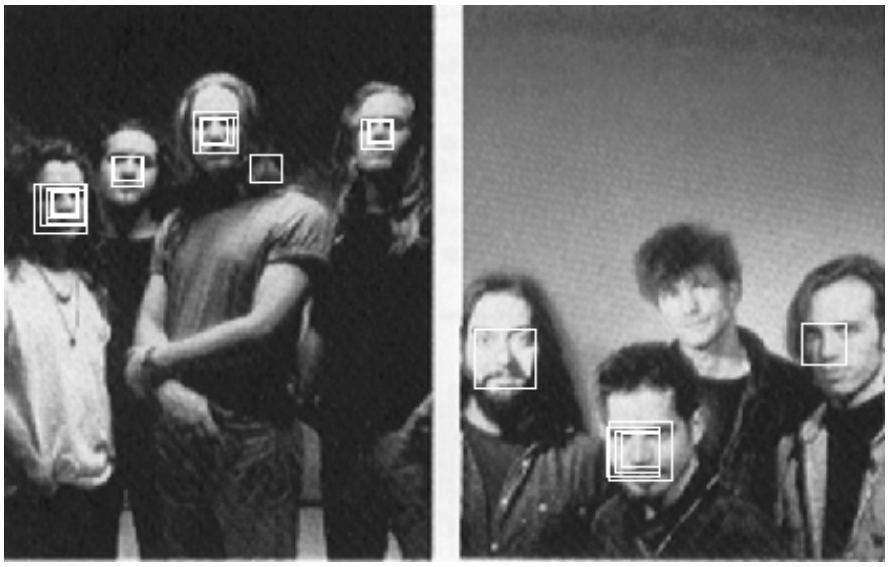


Figura 2.3 Grado de reconocimiento Facial y errores de captura

Consideremos un requerimiento sencillo de verificación de una escena, dentro de un medio ambiente controlado. Los sujetos individualmente a ser examinados, habrán sido previamente matriculados o registrados en el sistema y sus imágenes faciales captadas según un proceso predefinido y repetible. Al usar el sistema, este eficazmente exigirá una identidad evocando su imagen almacenada en la base de datos por ya sea la introducción de un PIN (número de identificación personal) o

quizás una tarjeta con código de barra o una acción basada en señales similares. El sistema ahora tiene que cotejar la imagen almacenada en la base de datos con la muestra en vivo capturada por la cámara. En primer lugar, para la muestra en vivo se debe confirmar que, una imagen facial este presente dentro de la escena y localizada en un espacio consecuentemente. En la mayoría de los casos esto será relativamente sencillo ya que el sistema puede detectar los bordes de la cabeza en contra de la escena del fondo y el sujeto después de todo estará relativamente estático. Sin embargo, si la escena está sujeta a cambios fuertes y aleatorios de la iluminación, entonces esto podría no ser tan fácil, ya que las variaciones de tonalidad dentro de la escala del gris de la imagen vista por la cámara puede tender a fluctuar bárbaramente, dificultando localizar el borde de la fuente fidedigna. Habiendo captado la imagen, el sistema típicamente puede dedicarse al principio de localizar y corresponder características dentro de una cuadricula. Por ejemplo: la posición relativa y real de los ojos, nariz, boca y orejas dentro de la cuadricula. Esto puede ser logrado, agrupando racimos de píxeles a fin de determinar los atributos grises a escala de un área dado. Esto ciertamente puede ser parte de un proceso inicial de refinamiento el cual produce un mapa binario de la imagen para la comparación con la plantilla almacenada. Con un proceso de pareo uno-a-uno, entonces podemos sumar el número de características de pareo y referenciarlo a un preajustado umbral del sistema a fin de lograr llegar a una simple conclusión determinando la equivalencia o no equivalencia para nuestro proceso de verificación de identidad.

Si operamos en el modo de identificación, debemos por su puesto explorar la base de datos de plantillas para encontrar uno que mas se parezca a la muestra en vivo presentada, de acuerdo a ciertos parámetros del umbral del sistema, o ciertamente concluir que ninguna muestra almacenada equivale para el grado requerido de precisión. En cualquier caso, tenemos la base para que los procesos de verificación de identidad biométrica sean de fácil manejo, sin-contacto, los cuales pueden ser de utilidad en un número variado de aplicaciones.

Figura 2.4 El reconocimiento Facial – ¿Es ésta la misma persona?

Ahora consideremos una situación aleatoria de una escena donde tenemos el deseo de identificar a un individuo que se encuentra dentro de un grupo. En primer lugar, debemos identificar y localizar dentro de la escena cualquier cosa que parezca ser una cara humana, del cual puede haber muchos ejemplos. Tenga presente que las caras individuales al variar la distancia desde la cámara, serán representadas como grupos de píxeles de tamaño diversos dentro de la escena global. También considere que las caras pueden estar enfocadas o encuadradas a la cámara, desde cualquier perfil (derecho o izquierdo), desenfocadas de la cámara o en cualquier parte de en medio, adicionalmente estarán en movimiento mientras están dentro de la escena global. Esto representa un reto y algunos sistemas estipularán que la imagen facial no debe pasar de un número de grados dado, fuera del eje de lo que directamente se sitúa delante, si es que este va a ser formalmente detectado. Habiendo localizado la imagen facial dentro de la escena, luego podemos tratar de corresponder o parear contra ya sea una sola muestra, si es que estamos buscando a un individuo específico, o contra una base de datos de individuos con quienes nosotros estamos interesados, en cualquier caso siempre tratando de parear dentro de los criterios predefinidos. En una situación así descrita, nuestra base de datos de plantillas necesitara contener información adecuada acerca del individuo, tales como si hemos formalmente pareado o correspondido a ellos ya sea en un aspecto de semiperfil o directamente enfrente o si hemos variado la resolución en relación a la escena. Este es un factor que debe ser considerado cuidadosamente por el diseñador. Puede ser que no tengamos información adecuada de la plantilla para ciertos individuos en los que estamos en particular interesados, pudiendo tener poca probabilidad de alistarse como voluntarios para ser registrados en nuestro sistema. También deberíamos entender que los individuos dados, pueden aparecer dentro de la escena por una enorme y variable cantidad de tiempo, proveyéndonos con una igualmente variable oportunidad de captar una buena calidad de imagen. En dos palabras, existen muchas variables las cuales pueden hacer que esta sea positiva o de otra manera esperar confiadamente detectar la presencia de un individuo en particular en tal situación.

Por supuesto, la funcionabilidad aleatorias de las escenas, por el cual los reclamos numerosos y algunas veces dudosos han sido hechos en los últimos tiempos por vendedores, es naturalmente atractivo a muchas aplicaciones de la ley y practicantes de la seguridad en general, ofreciendo la promesa de positivamente identificar a cualquier individuo como por ejemplo Jamellys González, en algún lugar abarrotado de personas en un supermercado, o que asiste a un partido de fútbol o que llega a la Terminal de un aeropuerto. En la práctica, puede que esto no sea tan fácil, el carácter aleatorio de la vida real es a menudo un poco más aleatorio para los sistemas automatizados, especialmente si como en el ejemplo anterior, Jamellys González está en la caja registradora de un supermercado y tiene un interés preestablecido en quedar de incógnito. Deberíamos recordar que el cerebro humano después de muchos miles de años de desarrollo, se ha vuelto bastante bueno en reconocer rápidamente personas familiares desde el interior de una escena algunas veces muy complicadas. Las

computadoras aun tienen que recorrer un largo camino para llegar a tal nivel de funcionabilidad y sofisticación. Sin embargo, dentro de la hermandad del reconocimiento facial, mucha investigación continúa siendo llevada a cabo, incluyendo el uso de redes neurales y otras técnicas a fin de proveer siempre mejores herramientas, pero, debemos ser realistas en lo que se refiere a la aplicación de esta tecnología en ambientes de todos los días, especialmente con relación a situaciones con escenas aleatorias. Además, nos gustaría ver que se haga más énfasis en la calidad de mediciones en la biometría de reconocimiento facial.

En cuanto al desempeño de estos equipos. El desempeño es el tiempo total que le toma a una persona usar el equipo. Para los fabricantes es difícil especificar el desempeño, dado que depende relativamente del usuario. Algunos fabricantes hablan de un "tiempo de verificación" del lector facial, pero ello solo es el tiempo que le toma al lector verificar la identidad después que el usuario ha colocado la parte de su cuerpo en la unidad. Muchos lectores biométricos verifican la identidad en menos de dos segundos. El desempeño incluye el tiempo de verificación más el tiempo que toma digitar el número de identificación y colocar la parte del cuerpo a ser leída.

En conclusión, el reconocimiento facial es una técnica biométrica muy interesante que sin lugar a dudas, continuara siendo desarrollada en años venideros. Sus aplicaciones quizás requieran un poco mas de intelecto, por parte del programador, que con otras biometrías y probablemente podría servir en una situación en la cual se solicite por encargo, la cual puede ser cuidadosamente diseñadas

2.5 Conclusiones

Los dispositivos presentados hasta aquí son los sistemas biométricos principales actualmente en uso y desarrollo, pero no son los únicos. Los investigadores examinan actualmente la viabilidad de sistemas basados en el análisis del ADN e incluso de los olores corporales.

La mayoría de las soluciones requieren asociar dispositivos de entrada de información externas a un software de soporte. Existen sistemas que utilizan un dispositivo de entrada de información externo que todos tienen: el teclado. En vez de sustituir el sistema de la conexión del usuario mediante nombre/contraseña, esta tecnología (dinámica, llamada de golpe de teclado) trabaja conjuntamente con la información de la conexión. Cuando usted pulsa su nombre y contraseña, el software mide su ritmo al pulsar y lo compara con su perfil.

No hay razón técnica por la que varios sistemas biométricos no podrían trabajar en conjunción para analizar muchas de nuestras características, pero cada sistema está asociado a un modelo que identifica al usuario.

Teniendo en cuenta las preocupaciones actuales por la seguridad, los sistemas biométricos parecieran ser inevitables. Pero de hecho sigue habiendo resistencia considerable a ellos. Los departamentos de administración de redes, por ejemplo, tienen que considerar la pérdida real que ocasiona el acceso desautorizado, así como el costo y las complicaciones de poner elementos de hardware en los escritorios de los usuarios y de mantener ese hardware. Para los usuarios caseros, el costo, la conveniencia, y la necesidad son consideraciones importantes. Los vendedores de accesorios biométricos tienen mucho que hacer antes de que sus sistemas lleguen a ser de uso común, pero seguramente en la segunda década del milenio se encontraran estos elementos en la mayoría de los sitios que requieran de acceso seguro.

Debe tenerse en cuenta sin embargo, que en los últimos tiempos han comenzado a surgir diversos grupos de protesta frente al avance del uso de los dispositivos biométricos. La principal queja se basa en el hecho de que la organización puede utilizar los datos obtenidos no solo para la identificación de la persona, sino también para ser vendida o utilizada por otras corporaciones, gobiernos o centros médicos. Una lectura de la retina inofensiva para el usuario puede ser utilizada para indicar si la persona tiene SIDA o toma drogas, por ejemplo.

Precisamente, para evitar el peligro de la centralización o venta no autorizada de la información, una alternativa comenzó a ser utilizada por las empresas. El uso de una "tarjeta inteligente" en conjunto con un dispositivo como el de lectura dactilar, permite almacenar los datos obtenidos en el chip del usuario en vez de ser guardados en la base de datos del sistema. La información del usuario es comparada luego con la guardada en la tarjeta, ofreciendo así una seguridad extra a la persona.

3. Implementando la Biometría

En el primer capítulo, se hizo referencia a los egipcios antiguos y de miles de años de principios biométricos y su uso. Cuando las personas piensan acerca de Egipto antiguo naturalmente piensan acerca de las pirámides, astronomía y quizás su mitología cautivadora. Sin embargo, los egipcios antiguos estaban claramente muy bien organizados y diestros en los requisitos más mundanos y cotidianos de la vida. Fueron constructores de buques, maestros, arquitectos, agricultores, fabricantes, escribas, administradores y si usted piensa sobre esto un poco mas, por definición también han debido haber sido administradores de proyecto y bastante buenos. Una cierta cantidad de los logros asombrosos de las civilizaciones antiguas todavía nos sorprenden hoy, a pesar de nuestra sociedad técnicamente adelantada.

Se menciona muy especialmente esto aquí, porque la implementación práctica de un proyecto biométrico, requiere una administración cuidadosa del proyecto, si este fuera a ser exitoso. Esto es especialmente cierto en la mayoría de los proyectos que puedan involucrar una mezcla de hardware y software, algún tipo de legado, de una colección variada de fuentes, a ser implementados algunas veces a través de ambientes múltiples. Además, hay una gran cantidad de asuntos relacionados con los usuarios que necesitan ser cuidadosamente considerados y manejados. Es fácil perderse y alejarse de la idea principal con debates alrededor de los tipos de dispositivos de punta que existen y de su actuación teórica con vista a los beneficios potenciales para su organización, pero al final de todo, alguien tiene que hacerse responsable por vincularlo completamente todo y obtener los resultados deseados dejando el proyecto en plena marcha. ¡La experiencia pasada sugiere que definitivamente podríamos hacer algo asi como una pequeña guía egipcia antigua de administración del proyecto en este sentido! En algunas ocasiones se ha visto situaciones de “demasiadas manos en la masa”, todos queriendo hacer de todo, conjuntamente con un concepto más bien débil de propiedad, ciertamente ha conducido a resultados por debajo de los óptimos, y si no de completo fracaso. Usualmente es fácil, retrospectivamente, identificar donde las cosas han salido mal en determinadas situaciones y cómo deberían haber sido quizás manejadas, pero no sería más facil sustituir cualquier dificultad dentro de un plan cuidadosamente construido y una comprensión sólida de los asuntos que lo envuelven. Por supuesto, esto se aplica a cualquier proyecto referido en proceso sustentado por la tecnología, pero éste es especialmente el caso con la Biometría.

En este capítulo por consiguiente se examinara una cierta cantidad de elementos inherentes a la implementación de un sistema biométrico. Aunque esto no representará una descripción detallada de cómo concebir y ejecutar un proyecto biométrico, este podría quizás resaltar una cierta cantidad de áreas dignas de especial consideración, por aquellos que contemplen tal iniciativa y puede proveer un armazón preliminar en el cual poder construir un plan de conformidad integral.

3.1 Estando claro en cuanto a los Requisitos

¿Suena obvio? Pero algunas veces hay una cierta tendencia a salirse de control con el uso de la tecnología y lo que ésta puede hacer, quizás olvidando durante el proceso lo que nosotros en realidad necesitamos que esta haga. El primer paso por consiguiente es pensar claramente acerca de por qué pensamos que con la adopción de la tecnología biométrica podría ser esto útil para nosotros, y exactamente cómo. Esto a menudo se plasmaría en identificar un proceso existente y luego considerar cómo este podría llegar a ser con la integración de la Biometría para complementar o realzar este proceso.

Por ejemplo, consideremos un escenario físico típico de control de acceso. Damos por supuesto por asentado que ya disponemos de un sistema de acceso de control integral que incluye toda la funcionabilidad que nosotros en realidad necesitamos para nuestra organización y un montón de informes de gestión que han estado cuidadosamente hechos a la medida y refinados con el paso del tiempo. Además, el equipo de empleados que maneja este sistema está muy familiarizado con el manejo de este y tienen un buen soporte y contrato de mantenimiento en el lugar con el proveedor, quien ha demostrado ser confiable y estable. En lo particular no quisiéramos descartar este sistema para implementar una solución biométrica ya que este sirve bastante bien a nuestros propósitos en todos los aspectos. Sería mucho más apropiado, si es posible, simplemente integrar la verificación biométrica de identidad en el sistema existente. Nuestro requerimiento en este caso seria por consiguiente muy sencillo. Andamos buscando una metodología biométrica que pueda interactuar con nuestro sistema existente al dar la apariencia de estar integrado invisiblemente en el procesamiento del sistema. En otras palabras, nuestro sistema existente ni sabe ni le importa si la biometría esta involucrada en el proceso de verificación de identidad del usuario, este solo necesita recibir el resultado, para el cuál responderá en la manera para la cual ha sido programado. En este ejemplo hipotético, estaríamos buscando un dispositivo biométrico que pudiese emular nuestros lectores existentes de fichas bien sea en un formato autónomo, o en conjunción con la presentación de una ficha (tarjeta de acceso). Podríamos quedar bastante impresionados con la gran variedad de escenarios en sistemas presentados como posibilidades por los vendedores, pero no deberíamos perder de vista nuestras razones y objetivos originales para considerar la tecnología en primer lugar. En este caso, la razón primaria sin duda habría sido que

no estamos lo suficientemente seguros de que la ficha presentada halla sido del individuo original. Quizás tuvimos un número de fichas ó visitas genéricas en circulación y/o nuestro procedimiento administrador de fichas haya cometido un error o desliz.

Un caso ligeramente diferente podría estar en el contexto de un centro de llamadas, por medio del cual desearíamos ofrecerles a nuestros clientes la automatización de las instalaciones, proveyéndolas de un nivel alto de confianza en el reconocimiento de la verdadera identidad de la persona que llama. Esto puede ser con el objeto de permitirle a la persona que llama acceder a información privada y personal con relación a un esquema de lealtad del cliente por ejemplo. En este caso, naturalmente necesitaríamos identificar exactamente qué información tenemos en mente, cómo es esta guardada y cómo utilizaríamos la identidad y verificación de resultado del usuario para recuperar y presentar esta información. Una vez mas, la dimensión del proceso tiene lugar externamente a los elementos biométricos de verificación de identidad y debemos considerar cómo integrar lo dos. Probablemente estaríamos buscando un motor de verificación y un proceso que lea procedimientos, que pueda interactuar como una sola pieza con nuestra tecnología existente y sea manipulado en una manera familiar, quizás por medio de un lenguaje de comandos por ejemplo. Sin duda que existirán cualquier cantidad de vendedores que podrían describir alguna funcionabilidad alternativa o adicional que su producto en particular puede proveer - pero éste no es el punto, se anda buscando cierto grado de funcionabilidad en grado específico que, si no está disponible a la mano, tendremos que proveerlo en base a las necesidades, hecho a la medida.

El punto que se quiere destacar aquí es que la funcionabilidad biométrica debería estar bajo consideración como un realce del proceso comercial - no a la inversa. Debemos estar claros acerca de nuestros requisitos y debemos comprender hasta qué grado puede la tecnología actual suministrarnos lo que tanto estamos buscando. Si permitimos ser convencidos por las diversas posibilidades ofrecidas, estamos corriendo el peligro de perder de vista los beneficios potenciales de la tecnología, para nuestra situación en particular. Esto no quiere decir que deberíamos estar ciegos a nuevas ideas que previamente no se nos pudieron haber ocurrido, pero si el hecho de mantener a la fuerza en todo momento las cosas en perspectiva y directamente relacionadas con nuestros requerimientos básicos. En casi todos los casos, estos requerimientos serán procesos conducidos. En otras palabras, hemos identificado el problema en si o el proceso organizativo en el que creemos se aprovecharía la verificación de la identidad personal ofrecida por la Biometría. El reto es integrar la tecnología biométrica en ese proceso, en la manera más eficiente. Habrá pocos sistemas que resuelvan las cosas usando la Biometría ó en aras de la Biometría. Éste es un punto importante que algunas veces se ha desenfocado cuando las personas se han dejado llevar, quedando fuera de control con los detalles técnicos y las posibilidades teóricas a la oferta. ¿El requerimiento es para implementar un sistema

biométrico, o es para realzar y afinar un proceso necesario dentro de su organización? Si de la anterior pregunta su respuesta es la última, entonces la tecnología biométrica es una poderosa herramienta para tener en su colección, pero no es un fin en sí. Nuestra recomendación es que los potenciales usuarios deberían intercambiar ideas y deberían documentar el requerimiento antes de que se pongan a buscar un dispositivo específico. Luego entonces, deberían escribir en letras grandes y en una hoja en blanco estos requerimientos y colocarlo en la oficina de proyecto donde será visto todos los días por los interesados. Debajo de esta, podría ser colocada una lista de objetivos del proyecto y los puntos más notables. Es obvio que deberíamos tener construido un plan de proyecto con una línea base de nuestros objetivos y medida de progreso hacia el fin deseado.

Existe, por supuesto, una posible variación en la anteriormente citada filosofía y esa es, donde el advenimiento de la tecnología biométrica sugiere un nuevo proceso o una función que simplemente no fue posible de antemano, abriendo así un nuevo compás de oportunidades. Sin embargo, los mismos principios tienen aplicación en lo referente a que cuidadosamente debemos pensar detenidamente en la oportunidad y los beneficios percibidos y entonces debemos averiguar exactamente cómo podría dar la tecnología el requerimiento que hemos identificado. Deberíamos estar probando el caso comercial para implementar el sistema que tenemos en mente en la manera exactamente igual que haríamos si estuviéramos considerando alguna otra mejora para nuestros procesos o sistemas operacionales

Para concluir, es importante que consideremos la tecnología biométrica como una metodología disponible para soportar pertinentemente procesos de identidad personal. No debería terminar siendo la solución proverbial, en búsqueda de resolver un problema. Una forma de asegurar que conservemos nuestro pensamiento claro y entremos con buen pie, es absolutamente entender y aclarar los requerimientos arriba mencionados y entonces no ser influenciados por estos.

3.2 Estando claro en cuanto a los Usuarios

Éste es un área al que vale la pena invertir un poco de tiempo. Si nos ponemos a pensar un poco, las personas son mecanismos más bien complicados y necesariamente no piensan o reaccionan en igual forma a una misma situación dada. Vienen en todas las formas y tamaños - los doctores, los jugadores de fútbol, los políticos, los artistas, los obreros de la construcción, los músicos, los carniceros, los panaderos, los fabricantes de zapatos y un montón de gente más. También tienen diferentes intelectos y aptitudes en ciertas áreas. Algunos tienen ciertos prejuicios técnicos bien definidos, algunos son artísticas y algunos tienen habilidades lingüísticas naturales, etcétera. Es difícil dictar leyes para tan compleja y variada

especie, cuya comprensión, puntos de vista y lógica, serán tan diferentes de un individuo a otro. De modo semejante, su actitud y postura hacia un proceso que están obligados a seguir dentro de una situación de verificación y registro de todos los días, pueden ser igualmente variadas. En el contexto del uso de dispositivos biométricos, la percepción y actitud del individuo tienen también buena probabilidad de ser influenciadas por situaciones dentro de la cual la tecnología está siendo utilizada. Por ejemplo, un prisionero o una visita en la prisión al cual se le obliga el uso de un sistema biométrico dentro de un medio ambiente restringido, podría tener un punto de vista ligeramente diferente del cliente que se le solicita usar el mismo dispositivo Biométrico para verificar su identidad y poderle ofrecer la venta de algo mercadeado por Internet, recibiendo un beneficio por el uso de la tecnología. Este último usuario de nuevo podría tener un punto de vista diferente del cliente molesto por un producto, deseando reclamar y se le solicita la verificación biométrica para recibir tal beneficio. Entonces hay usuarios físicos y lógicos para el control de acceso, usuarios que registran tiempo y asistencia, usuarios para sistemas de votaciones, usuarios de las máquinas de cajero automático y un montón de otros quienes tendrán algún tipo de relación personal entre la tecnología y la situación dentro de la cual es implementada.

Anteriormente en el libro, se discutió cómo podría tener el usuario una influencia dramática sobre la eficiencia en los sistemas, según varios parámetros que podrían moldear su actitud hacia el proceso completo y la manera en la que ellos interactúan con el dispositivo bajo condiciones operacionales en tiempo real. Una cierta cantidad de esta variabilidad puede ser anticipadamente manejada por adelantado si nos tomamos un poco de tiempo en realmente comprender nuestros usuarios base y cual es su percepción del proceso que estamos introduciendo. Quizás el primer paso aquí es comprender el proceso actual y cómo los usuarios interactúan con este. Por ejemplo, consideremos un sistema de registro del tiempo y asistencia donde los usuarios lleven una tarjeta codificada la cual puedan introducir en terminales colocados estratégicamente a todo lo largo de la instalación cuando estén entrando o saliendo de su lugar de trabajo. Supongamos aun mas que los terminales existentes requieren una cierta cantidad de interacción con el usuario para escoger opciones tales como si están llegando, saliendo, código del usuario y otros detalles específicos de la organización. En tal situación, si creemos que incorporando la verificación biométrica va a proveer beneficios, es probablemente porque queremos un más alto nivel de confianza en lo que se refiere a la identidad verdadera del individuo que introduce la información en la Terminal. En otras palabras, tenemos una sospecha furtiva que Leonardo Alfonso ocasionalmente introduce la tarjeta en el sistema por José Miguel, mientras José está realmente en algún club trabajando diligentemente en un par de cervezas en lugar de estar en la oficina trabajando. Sin duda que José devuelve el cumplido de vez en cuando. Ahora, usted y yo podemos ver la introducción de la biometría en esta situación, como una metodología útil para ayudar aumentar la eficiencia en el lugar de trabajo. José y Leonardo quizás puedan necesitar un poco más de persuasión, antes de tener nuestra forma de pensar. ¡Está

bien! ¿Éste es un caso extremo - pero usted entiende la idea? Podría ser que no toda la fuerza laboral, inmediatamente compartan el entusiasmo del gerente quien está tratando de introducir la verificación biométrica de identidad en la organización. Si sabemos esto por adelantado, podemos tomar medidas para asegurar que la buena comunicación deja tales puntos de vista a ser tomadas en consideración y responder cualquier preocupación que pueda existir. Incluso si no hemos pensado acerca de estos detalles, podemos estar a punto de experimentar en cierto tiempo cosas interesantes, cuando tratemos de implementar el sistema. ¿Pero cómo descubrimos realmente cual es la percepción subyacente entre la fuerza laboral? La respuesta corta es, estando próximos a ellos y probando conjuntamente las cosas buenas y malas, para tener un punto de vista consecuentemente. La mayoría de las organizaciones poseen estructuras jerárquicas la cual les permite que la información tenga un efecto cascada en ambas direcciones siempre y cuando sea esta procedente, de manera que no debería ser demasiado difícil de lograr la comunicación. Los gerentes de secciones o los jefes de equipo probablemente tendrán una comprensión razonable del personal que trabajan en su área particular y también la mejor forma de comunicarse con ellos en relación a los nuevos procesos propuestos.

¿Pero qué pasaría si estuviésemos tratando con el público en general? En tal caso, se aplica los mismos principios, pero el mecanismo para recopilar puntos de vista y diseminar información claramente será un poco diferente. En la mayoría de los casos pudiese ser útil algún tipo de estudio del mercado al consumidor, quizás por medio de una encuesta dirigida a sectores específicos de usuarios. Se podría establecer una demostración de los equipos en las instalaciones donde los individuos interesados podrían venir y ver la tecnología funcionando, pudiendo expresar sus puntos de vista consecuentemente – si registrara metódicamente tales puntos de vista, estas podrían ilustrar y ser muy útil mas adelante para todo el proyecto. En cualquier encuesta a usuarios por supuesto será importante dejar claro las cosas, esbozando los beneficios esperados del sistema propuesto y exactamente cómo trabajara en la práctica. También se podría ofrecer algún cuestionario con preguntas de múltiple escogencia para medir la reacción del usuario a las diferentes metodologías biométricas en estudio y también informarles a los usuarios cómo podrían ser las plantillas administradas. Podríamos quedar sorprendidos por la cantidad de interés que los usuarios expresaran acerca de la tecnología. Habiendo recolectado de los usuarios una cantidad útil de datos de retroalimentación, entonces tenemos que estar claros en cómo vamos a usarlos. Un primer acercamiento objetivo y estructurado, será necesario si debemos extraer información significativa sin prejuicio. Además, deberíamos considerar cuidadosamente lo que ésta información nos está diciendo, aunque no sea lo que fue esperado o lo que en particular quisimos oír.

¿Pero por qué atravesar por todo este problema? ¿Por qué no simplemente implementamos el sistema y manejamos cualquier problema como vayan estos saliendo? Bien, es importante obtener la buena disposición del usuario y su

colaboración al implementar cualquier nuevo sistema o proceso, pero especialmente con la biometría ya que es un área que requiere interacción directa del usuario con el sistema en una manera muy personal. En este contexto, mientras más usted conozca sus usuarios, mejor esto será, este conocimiento lo ayudara a formarse un criterio acerca de varios diseños de sistemas y factores relacionados con proyectos globales, escogiendo la metodología biométrica mas apropiada para ajustar a la medida el medio ambiente y así obtener los mejores resultados. Podría usted argumentar que en una situación donde los usuarios están obligados a usar el sistema de cualquier manera, ese tipo de cosas es poco importante (así como por ejemplo en los sistemas de beneficios sociales). Sostendría la opinión de que es todavía importante saber cómo las personas van a reaccionar y a la vez entregaría un mensaje fuertemente psicológico a los usuarios, alrededor de la importancia que usted pone en la verificación de la identidad. Además, este le ayudará a pensar claramente acerca de un sistema óptimo y diseño del proceso para su situación particular y base de usuarios.

Para concluir, si estamos considerando la implementación de cualquier sistema biométrico o estamos en vías de obtener alguno, una de las primeras tareas claves debería ser un análisis de la base de datos de usuario potenciales, combinada con alguna forma de iniciativa para captar su manera de pensar y su respuesta para tal propuesta. Usando nuestra analogía del automóvil, el diseñar un sistema biométrico sin comprender a los usuarios es un poco como diseñar un automóvil sin conocer la suerte de terreno en el que será conducido - es posible, pero usted probablemente lo haría mejor si usted tuviera esta información.

3.3 Estando claro en cuanto al medio ambiente

Si comprender a los usuarios es importante, así también se debe comprender el medio ambiente en el cual el sistema propuesto debe ser usado. Esto ciertamente afectará la manera en que usted utilice los componentes que interconectan con el usuario, y ciertamente puede afectar su elección de metodología biométrica. Hay quizás dos formas ó vías a considerar en este sentido. En primer lugar, está el efecto que el medio ambiente puede tener en la infraestructura y componentes técnicos y su habilidad para funcionar en forma creíble. En segundo lugar, también está el efecto que el medio ambiente tiene en los usuarios, desde una perspectiva práctica y psicológica.

Consideremos por un momento los dispositivos lectores biométricos y cómo pueden ser afectados por el medio ambiente. Si pensáramos en utilizar un dispositivo de verificación de voz sin protección, probablemente pensaríamos dos veces antes de instalarlo a la intemperie, frente a los elementos, donde podrían estar sujeto al calor extremo, la humedad, la lluvia, la escarcha, etcétera, ni qué decir de los niveles

variables de ruido ambiental del tráfico y otros factores de todos los días. A nosotros tampoco nos gustaría instalarlos en un lugar escondido, rinconero dentro de una iglesia construida con piedra donde la acústica es propensa a formar eco. ¿Qué hay acerca de los lectores de huella digital? Muy bien para el control de acceso de la PC dentro de un medio ambiente limpio y controlado de una oficina, pero los utilizaríamos en el piso de una tienda con mucho movimiento de venta de acero o venta de aceites, donde las superficies ópticas podrían contaminarse en unos pocos minutos, posiblemente no. Éstos son ejemplos obvios de cómo necesitamos considerar nuestra aplicación en el contexto de su medio ambiente operacional. Hay más situaciones sutiles a considerar. Por ejemplo, si estuviéramos diseñando un sistema donde un número relativamente tremendo de usuarios están supuestos a atravesar por torniquetes, habiendo tenido su identidad verificada, en ese entonces necesitaríamos considerar una metodología la cual fuese ambas rápida y fácil de usar con un mínimo de interacción por parte del usuario con el proceso. Quizás una tarjeta inteligente ó magnética y ya sea un lector de huella digital o un lector de geometría de la mano podría hallarse en disposición en el lugar en este caso, a medida que podamos usar la tarjeta para bien sea cargar ó llamar a la plantilla biométrica con simplemente el usuario colocando su dedo o mano sobre el dispositivo para un rápido resultado de sí/no será aceptado. Esto podría acompañarse de un indicador visual obvio, incitando al usuario a proceder o esperar según sea el caso.

En definitiva, necesitamos considerar el medio ambiente donde nuestro sistema va a ser utilizado y qué efectos puede tener este en los dispositivos biométricos y cómo las personas interactúan con el. Deberíamos tener la intención de hacer el proceso tan invisible como sea posible, para que los usuarios no estén sufriendo una inconveniencia por colas innecesarias, causadas por una mala planificación ó funcionamiento defectuoso del sistema. No hay ni que decirlo, nuestra elección de metodología biométrica es importante en este contexto y debería reflejar las actividades de los usuarios en esta situación. Si están en un lugar público como un aeropuerto o una estación de autobuses, necesitaremos hacer las cosas tan rápidas y fáciles para ellos como sea posible. Si se está en una situación más relajada, quizás en un medio ambiente de oficina, en ese entonces podemos tener un poco más de flexibilidad en nuestra elección de dispositivos y cómo los utilizamos. La interacción entre los dispositivos y el servidor donde se procesa el sistema es también importante, especialmente si estamos tratando con un gran número de usuarios a través de puntos múltiples de verificación, creando un alto nivel de uso concurrente. Dependiendo de cómo hemos diseñado nuestro sistema, donde las plantillas biométricas han sido guardadas y donde el proceso de comparación tiene lugar, esto podría ser significativo. Si hemos elegido almacenar todas las plantillas en una base de datos central, y el proceso de comparación es también emprendido en una máquina servidora central, entonces habrá una buena cantidad de tráfico en la red a las horas pico, cuando los paquetes de información vuelen de acá para allá para comunicarse entre el usuario y los servidores. Si todo esto está siendo usado en una red existente,

con usuarios realizando otras actividades, es probable que también sea para ellos de tiempo crítico para otras actividades en el sitio, conduciendo a una degradación del rendimiento de la red en general. En tal situación, podría conducir a un retraso en el punto de verificación, no siendo del agrado de los usuarios, especialmente si hay una cola formada detrás de ellos.

Otro factor a tener en mente es el medio ambiente eléctrico. ¿Qué tan limpio y estable es el suministro de fuerza eléctrica en su medio ambiente propuesto? ¿Existen suficientemente tomas eléctricas cerca de su servidor? ¿Y qué hay acerca del equipo biométrico en cada punto de verificación? ¿Dispone usted de fuentes alternas de corriente como UPS dedicados y que hayan sido puestos a prueba consecuentemente? Se sabe de cosas extrañas que les han ocurrido a los equipos de procesamiento de datos cuando han sido conectadas a fuentes de poder dudosas. A veces esto se manifiesta en una manera obvia cuando de repente líneas sobrecargadas o excesivamente ruidosas pueden bombardear los componentes eléctricos en su sistema y lo pueden detener. Otras veces los efectos son más sutiles y podrían conducir a la corrupción aleatoria de datos o la ruptura abrupta del software. Por supuesto, cada gerente de sistemas o de redes piensa que esto nunca les ocurrirá y en todo caso, los componentes electrónicos de hoy en día son tan resistentes y buenos que para que preocuparnos por ello, ¿Será verdad esto? Además, en cualquier edificio público obviamente se habrá estado ocupado en asegurar la regulación y estabilidad del suministro eléctrico, ¿Que opina usted? Nadie debe ser tan ingenuo para creerse todo esto. Aunque el diseño original de la infraestructura eléctrica fuera satisfactorio cuándo se construyó el edificio, es probable que toda clase de alteraciones y toda clase de modificaciones pudieron haber sido emprendidas desde entonces por una colección variada de contratistas, bien sea para acomodar equipo adicional en el sitio o por cualquier otro motivo. Estos contratistas pudieron haber tenido diferentes puntos de vista alrededor de la mejor práctica e interpretación de estándares eléctricos. Al considerar el medio ambiente desde este punto de vista, el mejor consejo que uno puede dar, es tomar todo tipo de precaución para proteger la infraestructura de su sistema de los caprichos del medio ambiente inmediato. Use fuentes de alimentación regulada y protección contra picos y sobrecargas, ponga particular atención en la calidad y determinación del recorrido de todos los cables y asegúrese de que los componentes críticos de su sistema son también físicamente seguros. Esto es naturalmente importante con cualquier sistema, pero en particular sí es uno con el cual el público está supuesto a interactuar.

La otra cuestión en la que hay que pensar con respecto al medio ambiente es, el efecto práctico y psicológico que puede tener en los usuarios. Si usted está considerando la implementación de un pequeño sistema, dentro de su propia organización, donde los usuarios están positivamente obligados a usarla, usted podría quizás no querer considerar este aspecto en particular, como algo importante, aunque incluso en esta situación, un poco de previsión puede traer beneficios. Si usted está

implementando un sistema en un lugar público donde su uso es optativo (aunque a usted le gustaría alentar a las personas a usar el sistema), entonces este factor se vuelve de suma importancia ciertamente. La mayoría de las grandes tiendas por departamento y los supermercados, han gastado mucho esfuerzo y dinero en comprender el medio ambiente, para proveer la mejor experiencia a sus clientes. Se han dado cuenta de que el ambiente en general, además de la percepción por parte del usuario de tener una experiencia de compra fácil, encontrando todo a la mano y en aire acondicionado, hace una gran diferencia al seducir a las personas a comprar en sus tiendas. Principios similares tienen aplicación aquí, si usted tiene el deseo de atraer a las personas a su sistema, cuales son los beneficios que usted está mostrando para eso. Usted fácilmente los puede espantar si da la apariencia de estar tan demasiado técnico o complicado o si el procedimiento operacional es cualquier cosa menos que claro como el cristal. En un sentido más sutil, la mera apariencia de los puntos de verificación es también importante. Si tal parece ser que las cosas han sido realizadas con un presupuesto muy bajo y colocado con dificultad en un lugar muy inapropiado, entonces las personas no lo tomarán en serio. De modo semejante, si toda la operación tiene un aire de ultra alta seguridad, entonces probablemente no dará la apariencia de ser tan atractivo para la gran mayoría de las personas., seguramente seria mejor hacer los puntos de verificación atractivos y resaltantes a fin de que las personas naturalmente emigren hacia ellos. Hay mucho que puede ser logrado en este contexto dándole a todo el proyecto una identidad, con un logotipo adecuado e inmediatamente identificable y con una combinación de colores la cual puede ser reflejada en material promocional puesto en el sitio, permitiendo a los usuarios y prospectos de usuarios, rápidamente comprender lo que está ocurriendo y donde. Muchas pruebas públicas de biometrías emprendidas en la última década han perdido este punto de vista completamente. A veces incluso, ha sido difícil localizar los puntos de verificación de prueba, e incluso aun más duro, en encontrar alguien que pueda asesorarnos en la forma correcta del uso del equipo o dar respuestas a dudas sobre todo el proyecto. Por lo que respecta a un medio ambiente atractivo y hospitalario - esto parece algunas veces ser el último punto en la agenda del día. Es una lástima, como se pierde tan valiosa oportunidad de explorar una parte de los elementos más sutiles de la psicología del usuario, en lo que respecta al tema de verificación biométrica de identidad y su implementación en lugares públicos.

Siempre que el medio ambiente sea el correcto, conjuntamente con procedimientos operacionales confortables e intuitivos, es tanto una parte del diseño del sistemas como el configurar el protocolo de comunicación entre dispositivos o diseñar la interfaz con el usuario. Por otro lado se puede también, como se menciono anteriormente, tener un efecto significativo en el logro de la eficiencia del sistema. El reconocimiento de estos puntos y cómo incorporarlos en su proyecto le puede ayudar en la distribución e implementación de un mejor sistema, que a su vez tendrá una mejor oportunidad de aceptación del usuario y éxito.

3.4 Conjugando todos los factores para crear el sistema

Cuidadosamente habiendo considerado los objetivos y requisito originales, el perfil de los usuarios y el medio ambiente en el cual el sistema va a ser utilizado, entonces podemos desviar nuestra atención en cómo va nuestro sistema a ser físicamente configurado y utilizado en el sitio.

Quizás la primera cosa, es comprender la arquitectura del sistema y asegurar que ésta es óptima para los requisitos particulares que tenemos en mente. Si los componentes del sistema deben ser provistos en su totalidad por terceras personas, entonces nosotros necesitamos preguntarles cuidadosamente acerca del montaje e instalación estándar recomendado para los equipos, ya que pudiese no ser en nuestro caso particular el más adecuado. Muchas de esas preguntas, se centraran alrededor del tipo de metodología para la administración de las plantillas, el número y el lugar de puntos de verificación, la funcionabilidad de la administración del sistema y por supuesto el medio ambiente técnico dentro del cual estamos trabajando. Nuestra elección sobre el dispositivo de captura también será importante en este contexto. Por ejemplo, si la función de comparación de plantilla y huella puede ser realizada dentro del dispositivo mismo y adicionalmente estamos cargando la plantilla del usuario en una ficha tal como una tarjeta con un integrado en el, entonces nuestra preocupación en su mayor parte estará dirigida a la recolección fidedigna de los datos de las transacciones y las funciones administrativas en los lugares físicos designados. Alternativamente, si estamos tratando de bajar a disco una plantilla desde una base de datos central, para su comparación, o si el proceso de comparación y cotejo es emprendido en una unidad de proceso por separado, entonces nos preocuparemos mucho más por la función de la red y lo referente a la seguridad.

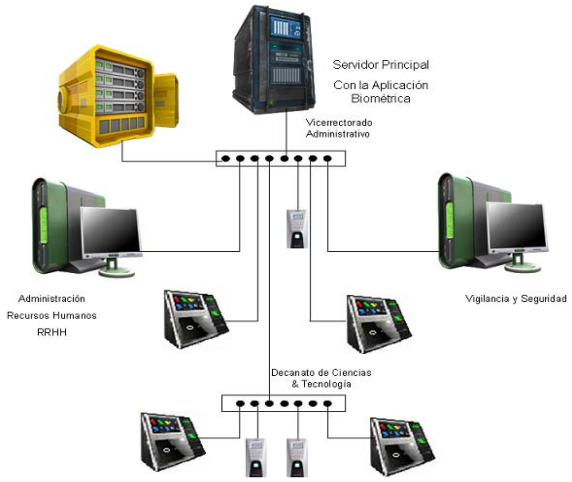


Figura 3.1 La posible infraestructura de un Sistema Centralizado

Si debiéramos asumir una arquitectura como la delineada en la Figura 3.1 con un servidor central dedicado al proceso de comparación y cotejo de huella y plantilla y manteniendo la base de datos de plantillasen otro servidor, entonces obviamente la eficiencia de este servidor debe ser escogido muy por encima de la tarea encomendada, con algunas capacidades de sobra en términos del procesador central y de almacenamiento de datos. Además, debemos considerar su flexibilidad ó maleabilidad. En esta arquitectura, si este servidor se desconecta o apaga repentinamente, entonces también lo hará nuestro sistema por lo que ninguna recuperación de plantillas o proceso de cotejo y comparación puede ser emprendido. En tal caso, casi ciertamente pensaríamos en un servidor secundario paralelo que automáticamente pueda cambiarse electrónicamente si el servidor primario deja de operar por cualquier razón (probablemente en un lugar físico diferente). Con el ejemplo dado en Figura 3.1 también le estaríamos poniendo una particular atención a la red y a la flexibilidad que todo debe tener, incluyendo cualquier concentrador y/o enrutador de datos así como también por supuesto, de la disponibilidad de ancho de banda. Sobre este último punto, se podría decir que es algo más complicado de lo que parece, ya que si toda nuestra infraestructura biométrica va a descansar sobre una red ya existente, posiblemente el ancho de banda se vea comprometido para toda la red. La administración de estaciones de trabajo, la cual podría incorporar la funcionabilidad de la matriculación de usuarios así como también mayor generación de tareas de reportes, también tendría que ser configurados con el propósito de robustecer la calidad y eficiencia. El hábito popular de poner a trabajar cualquier vieja PC que funcione y esparcirlas por todos lados, no tiene probabilidad de producir resultados óptimos en este caso.

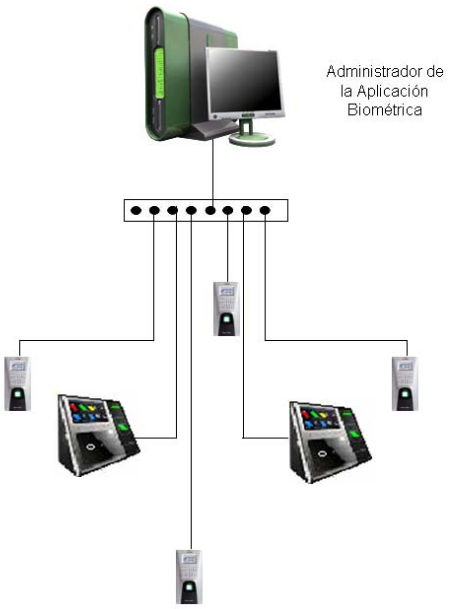


Figura 3.2 La infraestructura de un sistema simple

Por supuesto, podemos tener un requisito arquitectónico mucho más simple por medio del cual la mayor parte del procesamiento es emprendida en el punto de verificación, dentro de los dispositivos mismos y solo necesitamos el poder adicional de computación simplemente para propósitos de administración y de matriculación del usuario.

El diagrama mostrado arriba en la figura 3.2, describe simplemente tal sistema, por medio del cual el proceso de verificación es manejado por los dispositivos mismos sin hacer referencia a una base de datos central. En este caso podemos estar ligeramente menos preocupados acerca de la eficiencia global de la red, pero todavía nos preocuparemos por la flexibilidad de la red y también por la administración de las PC, las cuales mantendrán el historial de las transacciones realizadas. Ciertamente tendremos el deseo de implementar algunos procedimientos rigurosos de respaldo de datos en esta PC y podemos decidir tener ya sea una imagen en espejo de la unidad de disco duro, o quizás un respaldo de toda la computadora.

Brevemente hemos cubierto el tema de la arquitectura del sistema, para ilustrar el punto, de que éste es un tema que debería ser considerado con algún grado de mayor profundidad, como preludio al diseño de sistemas más detallados. Esto en particular será el caso, si estamos considerando un sistema en el dominio público, en el cual se estarán ofreciendo servicios a un gran número de usuarios con soporte mínimo de la administración y donde la fiabilidad será un asunto principal. Si estamos contemplando el uso de una red existente, se deduce que deberíamos comenzar con una buena comprensión de la arquitectura de la red, conjuntamente con la relación de eficiencia y una medición de la capacidad. Entonces podremos decidir si la red existente necesita ser mejorada antes de implementar nuestro sistema biométrico.

Permítanos ahora fijar la atención en alguno que otro de los componentes más obvios del sistema, comenzando con el dispositivo de verificación mismo. Probablemente hemos pensado fuertemente y por mucho tiempo acerca de la elección del dispositivo de verificación y finalmente hemos escogido el que creemos mejor reúne nuestros objetivos particulares para este sistema. Sin embargo, este podría o no servir directamente a nuestros propósitos. Podemos tener el deseo de integrar un lector de tarjetas u otros componentes para obtener la funcionabilidad que necesitamos. De hecho véase la figura 3.3, el dispositivo de verificación puede ser considerado como una colección de entidades incluyendo el dispositivo biométrico de captura, la interfaz de usuario, el suministro de energía, cualquier interface local adicional como relejs de salidas o anunciadores, cualquier dispositivos sinérgicos como lectores de tarjetas o teclados pequeños y por supuesto cualquier dispositivos controlador del volumen de personas como un torniquete. Estas entidades pueden ser

integradas en un solo equipo de reconocimiento, quizá dentro de una estructura adecuada, para proveerle una interfaz atractiva y lógica al usuario.

Figura 3.3 Componentes principales del dispositivo de verificación

Es importante que esta colección de entidades luzca y funcione como un todo desde el punto de vista del usuario y que estén ensambladas en una manera ergonómica que haga su uso intuitivo y obvio. Es también importante que cada uno de los componentes sean lo suficientemente robustos para tomar el nivel de uso que tenemos pensado para este sistema. Esto es especialmente importante en lo concerniente a los teclados pequeños y los lectores de tarjetas, aquí es digno de usar los mejores componentes disponibles en este contexto. La estética del diseño de los componentes en forma individuales podría o no ser un área en el que usted pudiese tener alguna influencia directa. Si usted lo hace, es digno de ponerle atención a la consistencia en el acabado para que todo se vea tan homogéneo como sea posible. Otra área al que prestarle atención es el suministro de energía eléctrica. Éste debería ser un suministro regulado y filtrado, preferentemente con respaldo de batería donde sea pertinente. La unidad debería ser atractivamente presentada y de diseño ergonómico, en buen estado, permitiendo el mantenimiento y uso fácil de los componentes, que idealmente debería ser reemplazado en el sitio, sin tener que desmantelar el sistema. Sería útil desde el punto de vista de la ingeniería, incluir un panel donde el técnico o ingeniero comisionado, pueda anotar el número del lector o dirección del nodo u otros detalles pertinentes. Habiendo diseñado ya todo, vale la pena documentar su construcción en algún grado de detalle. Usted nunca sabe cuándo puede necesitar construir unidades adicionales y si serán el mismo equipo o grupo de trabajo construyéndolas.

En el otro extremo por así decirlo, la administración de los PCs y el servidor de base de datos, deberían estar diseñados para el propósito y documentados

consecuentemente.(donde sea pertinente). Comencemos con el servidor. La discusión con el vendedor de dispositivos, asociado con una pequeña experimentación y cálculo debería determinar el poder de procesamiento y los requisitos de memoria en este sentido. Dondequiera sea posible la normalización para estandarizar los componentes de los fabricantes principales, de manera de facilitar el reemplazo de partes, debería volverse costumbre. Acerca de los requisitos del disco duro, deberíamos tener presente que este componente va a recibir una real paliza en cualquier diseño de sistema que implique recuperar plantillas y escribir transacciones en tiempo real para la base de datos. La regla general es simple, escoja el mejor componente de calidad disponible y por razone de seguridad haga un disco espejo dentro del servidor. Aunque la velocidad de acceso del disco no es crítica, puede ser considerado un factor importante dentro de un sistema grande, presentando a múltiples lectores y un número grande de usuarios concurrentes. La interfaz de la red también debería ser considerada cuidadosamente. Desvié del presupuesto cierta cantidad para cambiar las tarjetas y conectores de red e instale sólo componentes de fabricantes líderes en el mercado, asegurando con ello que se dispondrá de reemplazos para cada componente en el sitio. El servidor mismo naturalmente debería estar situado en un medio ambiente físicamente seguro y limpio con la temperatura controlada si es posible. El gabinete interno del servidor, adicionalmente debería poseer un enfriamiento adecuado, con electro-ventiladores guardados de reserva y conservados en el sitio. El acceso al servidor es un asunto que usted debería considerar cuidadosamente. Si esto depende del modelo de seguridad del sistema operativo, entonces cerciórese de que la clave secreta sea mantenida segura dentro de la oficina y que el equipo de ingenieros ó técnicos se encuentren apropiadamente entrenados desde el punto de vista de la seguridad. Por supuesto, usted podría estar usando un dispositivo biométrico para el acceso seguro al servidor, en cuyo caso asegúrese de que al menos dos ingenieros estén registrados en el sistema en cualquier punto de la red, además de una persona de cierta jerarquía del departamento administrativo. Si un segundo servidor de relevo es incorporado en el sistema global, entonces este debería estar situado en un lugar físico diferente, con todas las mismas reglas de seguridad aplicadas. Su administrador de red local, podrán mantener los dos en sincronización según sea el caso.

En cuanto a la administración de los PCs, desde el punto de vista de la eficiencia estas podría ser más simples en sus especificaciones, pero deberían ser especificados y construidos con la misma cautela y atención a los detalles. De nuevo, no estaría nada mal conservar algunos componentes guardados como reserva en el sitio de trabajo, aunque usted esté subcontratando el apoyo y el mantenimiento del sistema, a usted posiblemente le podría gustar solicitar esto dentro del contrato. Los detalles más finos de la red, incluyendo protocolos, cableado estándares y componentes auxiliares que dejaremos fuera del alcance de este libro, pero basta decir que usted debería tener todos los detalles de éste por escrito, conjuntamente con diagramas de la instalación, firmados por el ingeniero comisionado. Esto debería

acompañarse de un inventario completo del sistema, detallando cada componente y su configuración y especificación precisa. Esta información debería ser mantenida por duplicado, ambos, en y fuera del sitio para utilización futura. Es sorprendente cuántos sistemas son instalados sin esta disciplina la cual es, en opinión del autor, un requisito fundamental para cualquier sistema operacional. Si un proveedor esta renuente o es incapaz de cumplir con este requisito, entonces trate con alguien más que si lo haga. Si usted llegase a tener serio problema en el sitio con cualquier elemento del sistema, o se llegase a enemistar con su proveedor original, usted necesitará esta información.

El actual diseño del sistema en términos de topografía estará íntimamente asociado a las condiciones en el sitio. Naturalmente querremos configurar varios de nuestro edificio en la manera más eficiente para proveer el mejor y más confiable rendimiento global. Ya hemos discutido en una anterior sección algunas de las opciones para la administración de las plantillas y el efecto en el rendimiento global. Dependiendo del dispositivo biométrico que usted haya escogido, usted puede no tener oportunidad de variar este parámetro. Generalmente hablando, **MIENTRAS MÁS PROCESAMIENTO PUEDA SER EMPRENDIDO LOCALMENTE EN EL PUNTO DE VERIFICACIÓN, MEJOR SERÁ**. Por lo tanto si la plantilla o bien puede ser almacenada en el equipo o por el contrario esta puede ser proveída localmente a través del usuario (por ejemplo, el usuario podría llevar consigo una tarjeta con chip electrónico para el almacenamiento de datos y huella en el – Tecnología de tarjetas MIFARE ó HID) y el dispositivo biométrico pueda realizar el apareamiento ó comparación, entonces dispondremos de un sistema eficiente desde la perspectiva de la red como un todo, lo que quedaría por comunicar al servidor seria tan solo, el resultado de las transacciones y por lo tanto, podemos balancear mucho mejor nuestro diseño global del sistemas, consecuentemente.

Puede ser que el dispositivo biométrico pueda realizar la función de comparación localmente pero tenemos el deseo de almacenar las plantillas del usuario en una base de datos central. En este caso tendremos una discusión de tres puntos; a través de la red como la primera, por medio de la cual enviamos una petición al servidor y remitirnos la plantilla del usuario que requiere una identidad en el punto de verificación. En segundo lugar, el servidor devuelve la plantilla solicitada a lo largo de la línea y en tercer lugar, después de que el proceso de comparación haya sido iniciado, el resultado es devuelto al servidor para ser escrito en la base de datos de transacciones.

En situaciones en donde la comparación sea realizada ya al final en el servidor, las cosas son ligeramente diferentes. Ya que esta vez como un primer punto, estamos enviando la referencia del usuario y los datos biométricos en vivo a través de la red y recibiendo el resultado de regreso del servidor en el segundo. En teoría esto puede ser un poco más rápido si las plantillas de referencia se quedan en el servidor donde pueden ser accesadas rápidamente por un eficiente motor de base de datos y

comparadas, usando un rendimiento mas alto ofrecido por el servidor, pero en realidad mucho depende de los componentes implicados. La topografía final del sistema y la metodología operacional que usted escoja, sin lugar a dudas, será el producto de los componentes escogidos y de las condiciones reinantes en el sitio, incluyendo el número de usuarios esperados y de la velocidad requerida para una transacción. En la mayoría de los casos, usted tendrá algunas variables con las que hacer malabares para proveer la mejor componenda. Un aspecto que no debería estar comprometido sin embargo es la calidad de los componentes individuales escogidos. El eslabón más débil será el punto de ruptura bajo gran estrés.

Hasta ahora hemos discutido una parte de los puntos a considerar cuándo diseñamos un sistema biométrico. Naturalmente, hay mucho más detalle de que ocuparse de los que aquí se ha cubierto, pero esperamos haber puesto en escena y dado algunos indicadores a este respecto. Usted podría ciertamente considerar extraño el hecho de que hayamos cubierto una parte de redes y comunicaciones en un libro que se trata primordialmente de biometría. Pero el dispositivo biométrico mismo representa sólo un componente dentro de un sistema global y nosotros debemos considerar el sistema como un todo, si queremos comprender cómo el diseño global nos dará los beneficios que estamos buscando. Esto nos conduce elegantemente hacia la instalación.

3.5 Asuntos referentes a la Instalación

No es mi intención aquí ahondar en enorme detalle acerca de la instalación y ciertamente, deliberé sobre si este punto debería estar cubierto del todo en el libro. Al mirar retrospectivamente hacia sistemas biométricos que he visto implementados, conjuntamente con razones para su éxito relativo o fracaso, me convence, sin embargo, que el tema debería ser abordado, tan sólo para alojar la frase “Asuntos referentes a la instalación” firmemente en la conciencia del lector.

Cuando una institución esta considerando un nuevo sistema operacional de tecnología de la información, típicamente pondrá una gran cantidad de atención a su diseño e implementación, usualmente involucrando a los especialistas de tecnología de la información mas antiguos y de alto rango a manejar el proyecto hasta el final para su implementación y más allá. Con los sistemas biométricos esto no siempre ha sido el caso, con proyectos a menudo conducidos por el departamento de seguridad y a veces manejando presupuestos de forma poco realista y limitados. Esto a su vez, asociado con la relativa infancia de la industria biométrica, a menudo ha conducido a que las instalaciones hayan sido llevada a cabo por pequeñas empresas particulares del sector de seguridad, cuya comprensión mas amplia del panorama de sistemas de redes de tecnología de la información y las costumbres mejor asociadas podrían ser menos que optimas. Ésta no es necesariamente su culpa, pueden que sean expertos

indiscutibles en poner una cerca eléctrica de seguridad o instalar una alarma, pero ligeramente fuera de su entorno de conocimientos y profundidad en lo que respecta en los puntos más finos de un complejo enlace en red de un sistema biométrico. En el otro extremo de la escala se tiene la situación en donde las grandes compañías asesoras, le son pagadas vastas sumas de dinero por manejar el proyecto en su totalidad, incluyendo la instalación que puede o no ser subcontratada externamente por un tercero. Sin embargo, este panorama probablemente sólo sería aplicable a sistemas más grandes, o donde hay experticia interna pequeña. Afortunadamente hay un terreno intermedio, donde podemos encontrar compañías profesionales que tienen experiencia en biometría y en sistemas de tecnología de la información, capaces de diseñar sistemas inteligentemente e instalar en el sitio los equipos y periféricos, utilizando para ello a competentes ingenieros experimentados. No hay ni que decirlo, vale la pena salir a buscar este tipo de compañías. Sin embargo la experiencia de los especialistas en este tipo de proyectos, apunta hacia la escogencia de un pequeño equipo de trabajo interno en la organización, dedicado a manejar el proyecto con asistencia de una compañía especialista, con una trayectoria probada en biometría. El equipo interno sin duda incluiría al patrocinador del proyecto del área de negocio en si, y ciertamente incluiría a uno de los especialista mas antiguos y de alto rango de tecnología de la información y de redes, como administrador del proyecto, que pueda negociar con terceros según sea el caso, para asegurar que la solución escogida sea arquitectónicamente sensible dentro de su medio ambiente e instalado según el uso habitual y costumbres. Esto puede aumentar un poco el costo global del proyecto en términos de utilizar recursos humanos internos costosos, pero a largo plazo valdrá la pena.

Haber hecho el citado punto anteriormente, nos permitió resaltar una parte de las áreas que, mientras aparentemente parecen obvias, no obstante han contribuido a los fracasos más significativos en el pasado. Uno de los más favoritos entre estos probablemente sea el cableado. En cualquier situación donde estemos interconectando componentes electrónicos, bien sea una impresora serial conectada a una computadora, o dispositivos múltiples en una red, existirá una especificación óptima de cableado según la metodología, distancia cubierta y así sucesivamente. Desafortunadamente, el tipo óptimo de cable no es siempre usado. Si, un viernes por la tarde, José Miguel llama a su compañero de labores Leonardo Alfonso y le pide una cierta longitud de cable par trenzado de ocho hilos, blindados y de un tipo de referencia particular, si Leonardo contesta que él no tiene ninguno, pero ha encontrado simplemente uno de cuatro hilos lo suficiente largo para ir del punto A al B, a menudo quedará instalado de inmediato. ¿Es ésta una exageración? Especialistas en el campo eléctrico y electrónico, han descubierto sistemas principales en edificios prestigiosos, instalados por nombres de compañías prestigiosas en la industria con simplemente este tipo de error. Veamos el siguiente caso particular, dónde en las oficinas principales de una gran multinacional, habían estado experimentando corrupción en la data del sistema operacional primario. Componentes claves habían

sido intercambiados, terminales sustituidos por nuevos, y un mantenimiento muy caro había sido emprendido por un período de dos años, por una organización muy conocida en soporte de tecnología de la información, todo para nada. Al desmantelar el sistema en sus componentes básicos, el especialista contratado fue inmediatamente golpeado por un cableado sucio y la discrepancia en los tipos de cable entre componentes (ninguno de los cuales estaba en lo correcto). Después de quitarle el viejo cableado y recablearlo con la especificación correcta de cables, el sistema corrió perfectamente. No es solamente cuestión del tipo correcto de cable, sino la manera en la que son terminados y encaminados. Las terminaciones pobres pueden causar toda clase de problemas en una red. Algunos dispositivos utilizan conexiones físicas directas como bloques terminales del tipo con tornillos, mientras otros utilizan distribuciones especiales de enchufes y conectores. En el anterior caso, una cierta cantidad de paciencia y una cierta cantidad de atención a los detalles son requeridas para hacer una conexión segura, aun en este último caso, a veces, son requeridas herramientas especiales, que si no están disponibles, pueden conducir a ciertos compromisos para ser obtenidas o fabricadas. Un buen ingeniero supuestamente debería llevar un buen juego de herramientas, de buena calidad, además de una selección de accesorios para todo tipo de problema que se le presente. Podría ser buena idea examinar el juego de herramientas del próximo ingeniero que llegue a su empresa.

El enrutamiento de los cables, a veces también puede ser un asunto importante. Cada ingeniero electricista ha sido instruido en cómo operar los cables de datos en paralelo con el distribuidor primario de corriente alterna del edificio, cómo evitar colocar estrés innecesario en los cables durante la instalación, cómo asegurar que los elementos no toman su cuota prematuramente etcétera. En honor a la verdad, en la práctica la teoría no es siempre fácil de seguir, debido a complicaciones en el sitio, pero a veces el modo en el que los cables son ordenados todavía deja mucho que pensar. Existió un ingeniero, que amarro un montón de cables de datos directamente a un cable de 415 VAC, y lo llevo serpenteando desde la punta hasta el sótano de un edificio, porque le economizaba la instalación de tuberías y bandejas de conducción de cables (la calidad subestándar). Entonces hay esos que les gusta usar cables de datos como cordeles, o los echan a andar desnudos en ductos de servicio entre edificios etcétera. ¿Cuál es la respuesta? Pídale a su compañía de instalación, el plan topográfico del cableado, incluyendo especificaciones de cable y conductos, y pida inspeccionar la instalación al momento de poner en servicio el sistema antes de la entrega final. No tema gatear usted mismo con una antorcha en ductos de servicio si fuera necesario.

Otra área favorita es la del suministro eléctrico. Esto es en particular importante para los accesorios periféricos del sistema, como dispositivos biométricos, lectores de tarjetas etcétera. A veces los fabricantes suministraran una rudimentaria fuente eléctrica de algún tipo con el dispositivo (a menudo una pequeña caja para

pegar en una toma de corriente en la pared). Estos a menudo no poseen marca y son hechos en diversas partes del mundo para así hacer bajar los costos. Son también a menudo muy variable en su calidad de manufactura. Es entretenido a veces medir la salida de tales fuentes de poder, bajo carga y de esta manera, ver si se acercan al nivel indicado. Muchos dispositivos biométricos y accesorios periféricos sinérgicos pueden ser medianamente tolerantes de tener una cantidad muy pequeña de voltaje extra o de corriente alimentándolos, con tal de que sea estable. Lo que si no les gusta es el voltaje insuficiente o poca corriente, o enormes saltos y variables en el suministro, síntomas de que alguna fuente de poder se deleita en suministrarlo. Hablando sin rodeos, no debe existir ningún lugar para tales componentes dentro de una instalación de buena calidad. Hay muchísimas compañías que fabrican de buena calidad, correctamente reguladas y protegidas fuentes de poder, diseñadas para operar en el sitio 24 horas al día. Ciertamente cuestan un poco más, pero algunos miles de bolívares no van probablemente a meter a su organismo a la fuerza en bancarrota y la cantidad de dolores de cabeza que pueden ser salvados usando suministros de energía de buena calidad, les da extra valor el gasto adicional.

Puede parecer un poco pedante el poner atención a las áreas arriba delineadas, pero es sorprendente, simplemente cuánto pueden afectar el rendimiento de un sistema instalado. Muchas veces el equipo ha sido devuelto al fabricante en perfecto estado porque han sido percibidos como defectuoso en el sitio de trabajo, cuando en realidad ha sido la calidad de la instalación y de los artículos de consumo de la instalación que han causado el problema. Como usted puede apreciar, no se requiere demasiados de tales ocurrencias para so pesar el costo adicional leve de materiales de instalación de buena calidad y practica. Si usted estuviera comprando el nuevo Ferrari de fábrica, usted probablemente no le pediría a la fábrica que le suministrara cauchos de segunda mano, aceite recalentado en el motor y una batería de motocicleta – esta bien usted podría, pero el rendimiento, seguridad funcional y fiabilidad no pueden ser lo que usted esperó. Lo mismo es cierto para los sistemas biométricos. Asegure que los artículos de consumo en la instalación y los accesorios periféricos del sistema son de buena calidad y correctamente instalado y el sistema tendrá una buena probabilidad de actuar como se ha esperado. Si los ingenieros que realizan la instalación tienen permiso de escatimar gastos en esto, entonces tenga cuidado con problema que podrían ocurrir.

Hay asuntos medioambientales adicionales a este respecto, especialmente alrededor del lugar donde serán colocados los componentes del sistema. Si usted está utilizando un servidor de base de datos por ejemplo, este debería estar en un medio ambiente limpio (de ambas perspectiva física y eléctrica) y seguro y no pegado en el piso bajo el escritorio de alguien en una oficina compartida. Es también una buena idea el no situar accesorios periféricos y terminales adyacentes a maquinaria eléctrica pesada o tenerlos compartiendo la misma toma de corriente. Esto me recuerda de una sala de control que visité en una ocasión donde un encargado de seguridad había

traído una multitoma para ser conectada en el enchufe principal, a fin de poder conectar su caldero eléctrico y poder prepararse una buena taza de café en las mañanas. Desafortunadamente, no quedaba bien ajustada al enchufe en la pared y usualmente requería una cierta cantidad de meneo en el enchufe y a veces hasta una buena patada para establecer contacto y poder tener así tan importante encuentro ceremonial con el café. El acceso principal y la computadora del sistema de control ambiental, conjuntamente con la interfaz maestra de la red estaban también conectados a esta multitoma maestra, y fue extraño que cada persona en la mañana se quejara del funcionamiento errático de este sistema. Sí, por supuesto que los componentes deberían haber estado conectados a una fuente dedicada o UPS, preferentemente en una línea de voltaje separada, pero esto obviamente no se les ocurrió a los ingenieros que realizaron la instalación.

El lugar donde serán colocados los lectores biométricos o terminales también puede ser importante en su particular sistema. Si usted tiene que colocar los lectores en un semi-entorno exterior, asegure que no solo ellos están protegidos de los elementos, sino también termostaticamente controlado su temperatura. Naturalmente, usted no querrá situarlos en un medio ambiente abrasivo en donde la superficie del control de mando se averiará, o donde se contaminarán rápidamente, ya que esto tendría un efecto negativo en la percepción del usuario. Usted también debería permitir suficiente espacio físico al rededor de ellos para que los usuarios se encuentren a gusto con el medio ambiente operacional, y recuérdese de pensar acerca del acceso al equipo biométrico con propósitos de mantenimiento.

Para concluir, hemos hecho referencia a una parte de los asuntos más obvios alrededor de la instalación de sistemas que, aunque aplicadas a los sistemas en general, no son menos importantes para los sistemas biométricos. Habiendo invertido una gran cantidad de tiempo y una gran cantidad de esfuerzo en diseñar su sistema biométrico y procesos de asistencia, bien vale la pena poner una pequeña atención adicional a los detalles para bien de su instalación. No asuma que usted pueda subcontratar y olvidar este elemento del proyecto - es de fundamental importancia para el éxito inicial y la fiabilidad en curso del sistema como un todo.

3.6 Entrenando a los usuarios

Ésta es otra área crucialmente importante que significativamente puede afectar el rendimiento inicialmente realizado de su sistema biométrico, así como también la percepción del usuario y la aceptación de ella.

Si usted está introduciendo verificación biométrica de la identidad como un realce de un proceso existente, entonces la manera en la que este proceso esta cambiando, la razón del por que esta cambiando y lo que los usuarios tienen que

hacer diferentemente, todos estos argumentos son los que necesitan ser comunicados apropiadamente y en una manera oportuna a los futuros usuarios. Si todo el concepto es nuevo y no probado, entonces esta comunicación tiene ciertamente mucha importancia. Necesitamos asegurar que todos los usuarios se encuentran a gusto con los procesos que estarán obligados a seguir, y que han tenido la oportunidad de hacer cualquier tipo de pregunta que se les halla ocurrido, sin importa qué tipo de preguntas o que tan poco realistas pueden parecer ser. Esto es importante, naturalmente algunos individuos inicialmente pueden ver a la biometría como una invasión de la vida privada, especialmente si creen que las imágenes reales de su parámetro biométrico están siendo almacenadas en una base de datos en alguna parte con algún propósito oscuro. Probablemente una buena manera de tratar esto inicialmente sea a través de una serie de talleres donde la propuesta global del sistema pueda ser presentada y cuestionada e incluso desafiada consecuentemente por futuros usuarios. En este punto, las preguntas fundamentales acerca de cómo el dispositivo biométrico propuesto actualmente trabaja, administración de plantillas y su almacenamiento aparte de otros asuntos de interés los cuales pueden aquí ser tratados. Además, la organización puede explicar su justificación razonada del porque ir en esta dirección, cuales son los beneficios esperados y para quién.

Luego de haber emprendido un programa exitoso de mercadeo y comunicación, para abrirle el camino a la introducción del sistema, nosotros ahora podemos fijar la atención en el entrenamiento de los usuarios. Dependiendo del número esperado de usuarios, podría ser necesario ser emprendido en fases. Dentro de una organización, de una sola oficina, de tamaño mediana de quizás 100 - 200 individuos, ésta no será una tarea demasiado difícil ya que los podemos dividir en partes, en grupitos dóciles y probablemente podamos completar el ejercicio en uno o dos semanas. Con una organización mucho mas grande, con quizás miles de individuos trabajando desde múltiples lugares, obviamente se tendrá una tarea más complicada que realizar, complicada por el hecho de que las primeras personas a ser adiestradas pueden llegar a olvidar una cierta cantidad de lo que han aprendido si rápidamente no tienen chance de practicarlo en un sistema en vivo. Esto puede ser manejado de la siguiente forma, manteniendo un subsistema trabajando fuera de línea, quizás en un área poco crítica, con un equipo sencillo, quizás con un número de funciones mas reducido del que realmente este poseerá, pero del mismo tipo, tamaño y forma del que se usara a diario en el lugar. Si estamos introduciendo un sistema público como puede ser el caso con una agencia de beneficios o una organización comercial, entonces esto se convierte en algo parecido a una campaña militar, ya que se tendrá que emprender mucha coordinación y planificación. De hecho, mientras más grande sea el número de futuros usuarios, será más probable que deban estar dentro del dominio público, más complejo estas tareas llegaran a ser con más superposición de actividades entre la comunicación, entrenamiento y las fases de implementación.

Otro aspecto importante sobre esto, es la coordinación entre los técnicos o ingenieros de diseño del sistema y el equipo de implementación, los ingenieros de proceso y comunicación y el equipo que entrenara a los usuarios. No es bueno si teniendo el sistema implementado los usuarios no saben cómo usarlo. De modo semejante, no tendría ningún sentido entrenar a usuarios en un sistema que no está ni cerca de ser implementado. Dónde esto puede complicarse un poco es en el contexto de un sistema más grande, el cual se encuentra disperso a través de varios lugares con números grandes de futuros usuarios. En tal caso casi ciertamente estaremos considerando algún tipo de implementación organizado en fases, por lo que esto será demasiado más fácil de manejar que una estrategia de un rápido "Big Bang" explosivo. Además, facilita la experimentación y refinamiento conforme el sistema gradualmente progresa hacia el uso completo.

Éste podría ser un aspecto de la implementación de sistemas biométricos que usted previamente no había considerado en profundidad. Con cualquier sistema significativo, éste es un elemento que debería estar incorporado y presupuestado desde el principio. Esta claro al observar el diagrama en la Figura 3.4 que debería haber otras unidades involucradas de la organización aparte del equipo de implementación técnica o del equipo de administración del proyecto, si es que vamos a lograr una alta calidad e implementación confiable del sistema basado en la biometría.

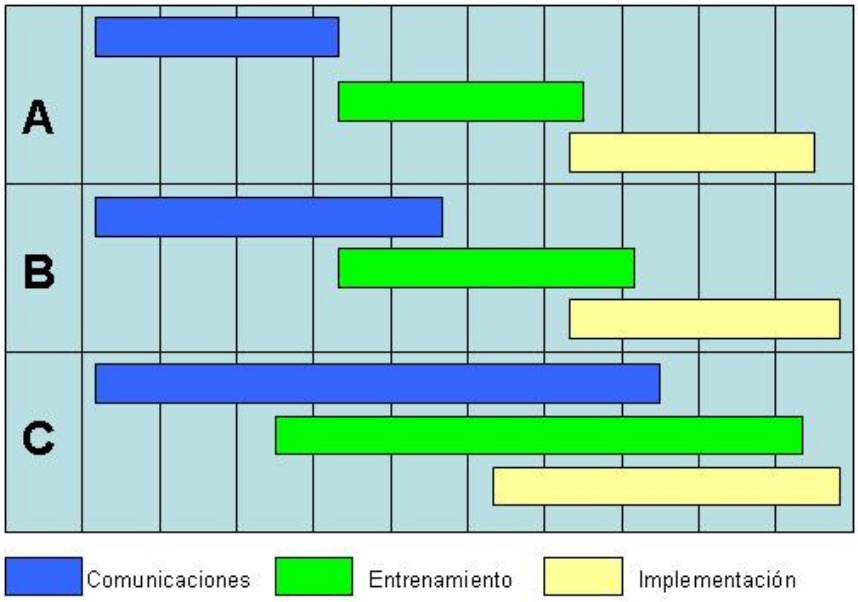


Figura 3.4 Programando la introducción del sistema

En el diagrama mostrado arriba, A.- representa una organización mediana contenida en un sitio, B.- representa una organización más grande distribuida a través

de múltiples sitios y C.- dibuja un sistema en el dominio público distribuido a través de múltiples sitios. A medida que la complejidad de la instalación se incrementa, hay una superposición creciente de la comunicación, los requisitos de entrenamiento y de la implementación con el paso del tiempo, con significativamente más esfuerzo requerido para la comunicación y las tareas relacionadas con el entrenamiento. Este en particular será el caso en dónde la implementación es puesta en fases. Claramente éste es un aspecto que requiere consideración ponderada y planificada.

Consideremos ahora el requisito de entrenamiento actual. Si deseáramos conocer que tan aproximadamente el rendimiento del equipo escogido es teóricamente capaz, entonces la calidad de la plantilla de referencia y la calidad de la muestra tomada en vivo en contra de la cual es comparada, tienen mucha importancia ciertamente. Nuestros usuarios por consiguiente necesitan ser correctamente matriculados en el sistema y también ser capaces de ofrecer una buena calidad de muestra en vivo, para la subsiguiente comparación. Es poco probable que estén capacitados de responsabilizarse por estas demandas si no saben nada acerca del proceso biométrico de verificación y cómo este trabaja. La primera cosa entonces es proveer algún entrenamiento fundamental que cubra este terreno, antes de seguir adelante hacia la utilización real del dispositivo biométrico, dejarlos practicar fuera del medio ambiente en vivo.

La metodología biométrica escogida naturalmente tendrá algún impacto en esto. Si estuviéramos utilizando los lectores de huella digital por ejemplo, entonces los usuarios necesitarían comprender cómo colocar sus dedos correctamente en la superficie del explorado biométrico con el fin de proporcionar una buena calidad en la toma de la muestra, en una manera coherente. Con la geometría de la mano, la tarea es hecha un poco más fácil por la provisión de pines que sirven como guías, alrededor de los cuales los dedos son ubicados, con tal que los usuarios tengan manos de tamaño para adultos comunes. Con el escudriñador de iris, los usuarios deben enfocar la imagen de su ojo, alineándola con el dispositivo de la cámara fotográfica. Con el explorador de retina se requiere que los usuarios se enfoquen en un punto dado, etcétera. Con la verificación de voz quizá en algunas instancias, este presente un poco más de desafío y reto, ya que los usuarios necesitarán comprender la operación correcta del dispositivo transductor así como también hacer un esfuerzo consciente hacia la consistencia de la enunciación. En cada uno de estos casos los individuos que están transmitiendo el entrenamiento, debe por supuesto, tener una comprensión minuciosa de la situación mismas y deberían haberse tomado su tiempo en familiarizarse completamente con el dispositivo en cuestión y de su operación. El fabricante del dispositivo o en su defecto, el integrador o vendedor, debería poder ayudar a este respecto, proveyendo entrenamiento para los entrenadores, conjuntamente con toda la documentación apropiada.

Hemos estado discutiendo el dispositivo biométrico en si y la necesidad de poner a los usuarios a familiarizarse con ambos el concepto y la realidad de su operación, pero por supuesto que hay otro elemento a considerar y ese es el proceso operacional mismo. Esta podría variar significativamente de una aplicación a otra, a merced del grado para el cual el usuario está obligado a interactuar con el programa o alguna otra forma de interfaz de usuario. Tomemos la verificación de voz por ejemplo. En teoría esto debería ser muy fácil, como el usuario puede reaccionar a los indicadores de voz programados en el sistema según el caso. En la práctica puede depender de la fortaleza de las rutinas que manejan el error en programación, asociadas con la forma que el elemento biométrico interactúa con el núcleo del proceso. En un sistema de control de acceso físico sencillo, una simple pantalla de cristal líquido o dispositivo equivalente puede ser suficiente como para comunicarle el estatus operacional al usuario con indicadores de lenguaje claro para cada etapa del proceso, y el resultado final de verificación y algunas otras instrucciones. Con un sistema controlando acceso a una computadora, a una red o incluso una específica funcionabilidad dentro del programa de computadora, esto no puede ser realmente tan fácil y probablemente necesitará mucha más documentación y explicación. Entonces hay aplicaciones hechas a la medida donde el proceso biométrico es integrado en algo diferente, el cual tiene valor para el usuario. Este puede ser el caso por ejemplo dentro de un sistema relacionado con la banca, o quizás un programa de fidelidad del cliente por medio del cual el usuario puede tener el deseo de ganar acceso a la información personal. Tal sistema sin duda incorporará un sistema lógico de mensajes para guiar al usuario a través del proceso, pero esto necesita ser comprendido y aprendido para el uso futuro del sistema. Usted puede lograr esto en línea con una parte de sus usuarios, pero es probable que una proporción significativa de ellos escoja que todo deba ser explicado y demostrado por un representante preocupado y competente de la organización. Si sus usuarios son integrantes del público en general, entonces usted ciertamente tendrá el deseo de hacer disponible algún material de referencia impreso que ellos puedan mantener para referencia futura. Este mismo material, útilmente puede formar parte del entrenamiento en el sitio para promocionar consistencia de acercamiento.

Inclusive con una mirada superficial de los puntos citados anteriormente, debería servir para resaltar el hecho de que el entrenamiento del usuario es en verdad realmente importante. Por supuesto que lo es para cualquier nuevo sistema o procesos en fase de introducción, pero en particular así lo es para un sistema biométrico, que puede ser un poco intimidante a los nuevos usuarios si no tienen experiencia previa de interactuar con tales dispositivos. También debería ser aparente que éste es un elemento que tendremos que presupuestar dentro de nuestro proyecto global. Necesitaremos proveer a los individuos competentes como entrenadores, cada uno de los cuales necesita pasar un programa de entrenamiento, con el fin de imprimirles velocidad en el manejo del sistema como un todo y en particular con los controles frontales del dispositivo biométrico. Todo el ejercicio de entrenamiento

adicionalmente necesita ser soportado con documentación y otros materiales como sea necesario para lograr el objetivo. Los entrenadores mismos por supuesto necesitarán información técnica y operacional completa, que tenga relación con el dispositivo biométrico en cuestión, así como también quizás un entrenamiento manual para delinear la operación del sistema y los beneficios respectivos. Los usuarios en la mayoría de los casos probablemente sacarían provecho de algún tipo de hoja suelta que esboce el propósito del sistema y cómo ellos, como usuarios, deberían interactuar con él, además de información de contacto para cuándo ellos experimenten dificultades o tengan alguna pregunta referente al sistema en conjunto. Esto puede tomar la forma de una hoja laminada simple, o quizá un folleto pequeño.

Ya hemos mencionado la importancia de medir el tiempo en relación a la comunicación, entrenamiento e implementación, pero dentro del área de entrenamiento propiamente habrá asuntos relacionados con el tiempo de los que ocuparse, dependiendo del tamaño y naturaleza exacta del sistema que usted tiene en mente. Esto cuesta obviamente menos esfuerzo en un sistema cerrado, donde usted sabe quiénes son sus usuarios y donde están y usted simplemente puede formular un programa de instrucciones consecuentemente. Sin embargo, usted no tendrá el deseo de entrenarlos más allá del avance de la implementación en vivo, ya que es importante que puedan practicar sus habilidades recién descubiertas en el medio ambiente natural tan pronto como sea posible. En un sistema público más amplio, esto probablemente será un poco más fácil, al menos una vez que el sistema haya sido implementado, el entrenamiento de usuarios estará en curso.

3.7 Manejando el sistema

He aquí un área en donde existe un tremendo campo de acción y en donde el sistema puede recibir un valor agregado, así como también puede ser limitado su potencial. Hay varios factores que entran en juego en este contexto, comenzando quizás con la administración de los componentes del sistema físico.

Empecemos en la sección de entrada con el dispositivo biométrico mismo. Asumiremos que ha sido correcta y seguramente instalado en el lugar apropiado. Muchos dispositivos biométricos tienen una superficie óptica o especial que es la llave de como funcionan. Por ejemplo, un lector de huella digital puede tener una superficie óptica de exploración, un dispositivo de exploración del iris tendrá una superficie a través de la cual la cámara fotográfica operara, y el dispositivo de geometría de la mano tiene una superficie reflectora que auxilia al proceso de captura de imagen. Sobra decir que estas superficies deberían ser mantenidas limpias, utilizando una tela suave, algo semejante a lo que se utiliza para limpiar lentes de la cámara fotográfica por ejemplo. Sin embargo, se necesitará tomar una decisión en lo que respecta a cada cuánto tiempo esta limpieza debería ser emprendida, y con

naturalidad esto dependerá del medio ambiente y del número de usuarios. Aunque los dispositivos mismos pueden funcionar realmente bien con una superficie ligeramente sucios, podría ser bastante chocante para los usuarios y demás personas ver tal suciedad, esto también debería ser tomado en consideración al implementar el itinerario de mantenimiento. Aprovechando que aun estamos en el tema de superficies ópticas, también deberían ser revisados en busca de abrasiones y otros daños menores que puedan afectar la operación del dispositivo. Si este es el caso, entonces un reemplazo debería ser realizado.

Mientras nos encontramos ocupados con nuestro horario de limpieza, es una buena oportunidad para comprobar la operación global del dispositivo biométrico. Si hay un teclado pequeño o un lector de tarjetas involucrado, asegúrese de revisar a fondo esto también, conjuntamente con la operación de cualquier interfaz de usuario tales como un panel LCD o una pantalla de diodos emisores de luz (LED). En su mayor parte, nos encontraremos con que los dispositivos modernos son medianamente fuertes y confiables, pero ciertos elementos pueden perder calidad con el paso del tiempo o pueden fallar completamente, perjudicando la confianza del usuario en el proceso, por lo tanto un mantenimiento regular y limpieza por completo son esenciales. No hay duda de que usted registrará tales chequeos en un libro de registro que indique los avances y fallas acerca del sistema.

Pasando a otro punto, asumiremos que la red misma está funcionando aunque un chequeo visual de cualquier componente de la interfaz, enrutador, conectores, cables y algo que se le parezca no estaría mal (usted pronto se enterará si no lo es). De regreso al servidor (donde sea pertinente), no dude en chequear que el medio ambiente mismo está siendo mantenido y que el servidor es como debe ser. Usted ya podría empezar a manejar los respaldos periódicos de datos, así usted sabrá que las cosas están trabajando bien en términos generales. Puede haber mantenimiento del software a considerar; Por ejemplo, usted periódicamente puede empacar la base de datos, o de-fragmentar sus unidades de disco duro. En la terminal de administración, usted debería estar revisando que este, está operando correctamente y que los componentes de la unidad de representación visual y periféricos, como los teclados y los ratones están limpios y funcionando correctamente.

Si todo el hardware está en buenas condiciones y funcionando correctamente, entonces podemos fijar la atención en los asuntos relacionados con el software. Es de preocupación primordial en este contexto la administración de la base de datos de los usuarios y las plantillas biométricas asociadas. Debemos asegurar por ejemplo que si un usuario deja la organización, o es transferido permanentemente a otra oficina, en ese entonces deberíamos quitar los datos de la plantilla biométrica del sistema para ese individuo (usted puede elegir retener registros históricos en su departamento de personal, pero ese es un asunto diferente). De modo semejante, un nuevo empleado necesitará estar matriculado en el sistema, sin demora y haber consecuentemente

configurado los derechos de acceso etcétera. También puede haber momentos en donde usted necesita rematricular a un individuo, si la plantilla original fuera sub-óptima, causando problemas operacionales. Si su base de datos incluye imágenes fotográficas de usuarios, entonces obviamente usted necesitará ocuparse de que la imagen este siempre en sincronía con la plantilla y otros datos. Además de la plantilla del usuario, hay con la mayoría de los sistemas, otros parámetros que pueden ser configurados para cada equipo biométrico individualmente, el más notable es el umbral de aceptación para el proceso de verificación mismo. Además, su sistema puede tener previstos el acceso y usos horarios por zonas, independientemente para cada usuario.

Ordinariamente, usted probablemente colocará el umbral de comparación al mismo nivel para todo el mundo, cuando el sistema es por primera vez puesto en servicio. Al poco tiempo usted sin duda se dará cuenta de que éste no es el ideal, ya que algunos usuarios pueden luchar contra el valor fijado que parece excelente para la mayoría. Con un sistema que continuamente rectifica la plantilla almacenada con cada transacción exitosa, también habrá campo para ajustar el umbral al cabo de un tiempo, para así aminorar la posibilidad de aceptaciones falsas. En cualquier caso esto significará explorar dentro del sistema y realizar cambios a los individuos en cuestión. Hay varios puntos que vale la pena notar aquí. En primer lugar, cualquier cambio que usted hace, para ajustar el umbral debería ser pequeño. Es mejor poner a punto este ajuste incrementalmente con el paso del tiempo para un usuario, que hacer cambios drásticos que pueden resultar en innecesarias aceptaciones falsas o falsos rechazos. En segundo lugar, la perspicacia en usted probablemente entrará en sospecha si un usuario en particular siempre acude a usted pidiéndole que aminore el umbral para el o ellos. Si este es el caso, vaya con el usuario al lector más cercano y obsérvelo como hace uso del equipo, puede ser que la inconsistencia del usuario sea el problema principal y que un poco de entrenamiento adicional curará esto sin aminorar el umbral a niveles dudosos.

Con respeto a los niveles de acceso y los usos horarios, usted puede suponer que colocará estos una vez y se olvidará de ellos. En realidad, es realmente posible que cierto empleado cambie su lugar y hábitos funcionales de vez en cuando y que estos parámetros necesitarán ser ajustados de nuevo consecuentemente. Cierta cautela debería ser tomada a este respecto, especialmente cuando podría en algunos casos necesitarse un periodo de transición, donde el usuario tiene derechos de acceso para una gran variedad de puntos. Si su sistema presenta un completo rastro de auditoría, usted podrá fácilmente monitorear esto. Si su sistema no lo hace, puede haber un campo definible por el usuario que usted pueda poner a trabajar para notar tales cambios. Si todo lo demás fracasa, un cuaderno de bitácora debería usarse para poner allí las alteraciones, a los ajustes del sistema. Si el terminal de la administración está en la red principal y usted también tiene acceso a los registros del personal, a usted le puede gustar establecer algún tipo de notificación automática cuando los empleados

cambian de departamentos, para así revisar los trasfondos en busca de tales individuos.

La mayoría de programas de sistemas biométricos, presentará reportes del sistema con algún tipo de descripción. En algunos casos, estos pueden consistir en algunos rudimentarios reportes de transacciones fijos, mientras que en los sistemas más sofisticados le pueden dejar manipular la base de datos, para así configurar sus propios reportes hechos a la medida. Otra opción seria, si la base de datos está en un formato conocido, es utilizar un paquete construido especialmente para generar reportes como Crystal Reports, Report Smith, o similares para producir sus reportes. En cualquier caso, usted necesitará estar claro acerca de que necesita de sus reportes, para quién es el beneficio y cada cuánto usted necesita manejarlos. Por ejemplo, el sistema sin duda será capaz de producir un informe de todas las transacciones para usted, pero esto es probablemente de poco valor. Es más probable que usted querrá saber simplemente las excepciones donde el proceso de verificación ha fracasado, o quizás las transacciones para un individuo o grupo de individuos, y casi ciertamente usted tendrán el deseo de filtrar esta información por un rango de fechas. Si el programa estándar que usted esta usando no tiene previsto esto, entonces será mejor ser servido por uno de los paquetes especialista en reportes nombrados anteriormente. También habrá reportes que no tengan que ver con transacciones, pero que usted puede desear producir periódicamente, como listas de usuarios o listas por grupos de usuarios. Si su sistema está usando tarjetas o fichas inteligentes o magnéticas, pudiese querer tener información relacionada a los usuarios, como el número de la tarjeta, la fecha de inicio y la fecha de renovación, todo esto con el deseo de producir reportes con el fin de administrar el reabastecimiento de tarjetas o fichas. También hay información relacionada con la administración del sistema en si, como pistas de auditoría o las fallas del sistema automáticamente puestas en bitácora etcétera.

Al configurar sus reportes, usted debería tener en mente cómo usted va a analizar la información resultante. Con informes de transacción por ejemplo, usted puede querer establecer patrones alrededor de puntos específicos de verificación, usuarios u hora del día, la cual podría ayudarle a comprender asuntos y quizás anticipar problemas y sus soluciones, consecuentemente. Usted también puede querer usar tales reportes para analizar las transacciones de un usuario en particular durante un período de tiempo y comprender cómo su rendimiento es afectado por trastornos fisiológicos o cambios de conducta en este contexto. Ciertamente, ésta debería ser una parte integral del manejo y entonación del sistema consecuentemente.

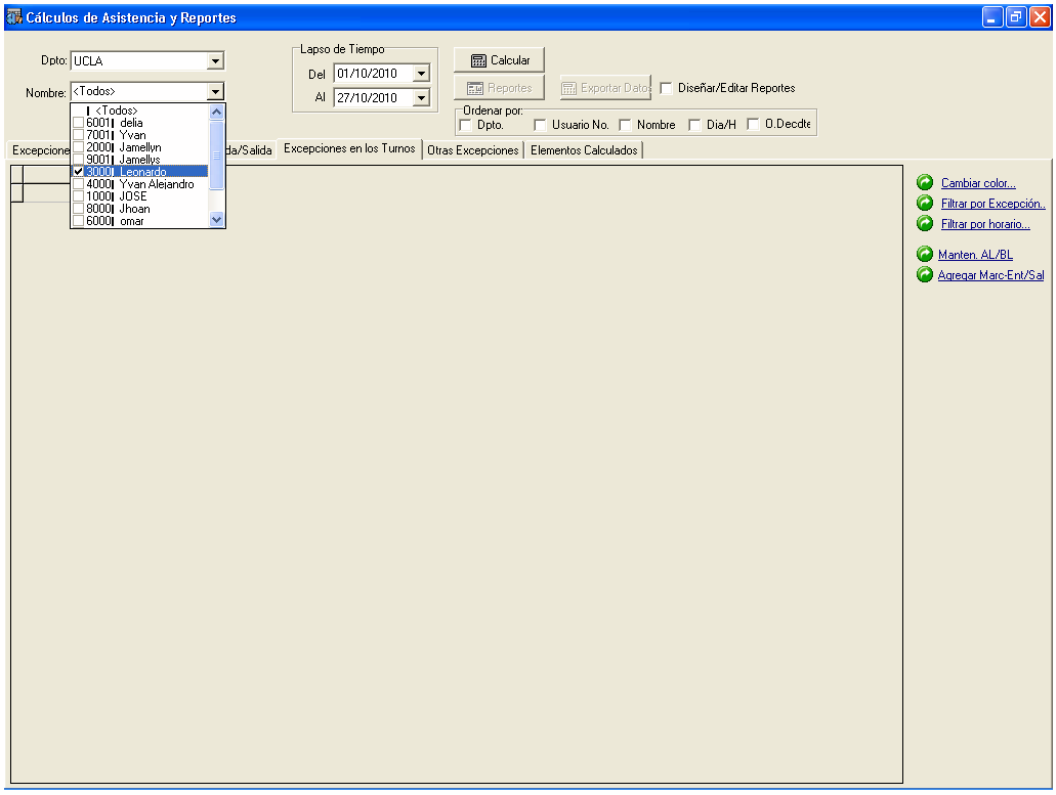


Figura 3.5 Una metodología de presentar reportes simple pero intuitivo

Estos reportes también le pueden ayudar a comprender el rendimiento general del sistema y, si usted tiene varios lectores biométricos en su sistema, quizá pueda identificar cuando un lector biométrico en particular está actuando por debajo del estándar, o quizá dónde hay un problema de conectividad en la red. Ciertamente, una funcionabilidad poderosa de los reportes es ser considerado un activo dentro de cualquier sistema biométrico. Su valor real sin embargo dependerá muchísimo de qué tan preparado usted esta para invertir algún tiempo pensando detenidamente en los reportes, su propósito preciso, su frecuencia y cómo utiliza usted los datos que ellos proveen. Ciertamente deberían ser considerados como parte del proceso de administración del sistema.

Un ejemplo de usar reportes positivamente puede estar en la interpretación de los rechazos falsos (personas que fueron rechazadas por el equipo biométrico por no poder verificar su identidad) y de los errores de falsa aceptación (personas que fueron aceptadas por los equipos biométricos, como resultado de un error en la verificación de la identidad), dentro de las transacciones de todos los días. Si Dios quiere, estos serán pocos y lejos el uno del otro, pero si usted se encuentra algún tipo de instancia, entonces rápidamente debería ocuparse de ellas, con los individuos afectados (en el

caso de falsa aceptación, usted puede ser que identifique o no al impostor, pero al menos conocerá la identidad que ha sido comprometida). Puede ser que el umbral esté colocado en un nivel impropio o que la plantilla de referencia es de mala calidad y el usuario en cuestión debería ser rematriculado en el sistema. En uno u otro caso, algún ajuste al sistema y la administración relacionada pueden ser necesarios. Si usted repentinamente comienza a experimentar simplemente un aumento en el número de errores en un punto de verificación, entonces éste señalaría hacia una falla con ese dispositivo en particular, necesitando un chequeo no programado de mantenimiento. Éstos son ejemplos obvios de cómo sus reportes le pueden ayudar a entrar en la administración cotidiana de su sistema biométrico.

3.8 Ocupándose de las excepciones

Hasta en los mejor sistemas planificados, aun allí todavía habrá excepciones, ya sea con usuarios, lectores biométricos, las condiciones medioambientales, las influencias externas en la red por fuerzas mayores y otras ocurrencias. La manera en la que nos ocupamos de las excepciones pueden hacer una diferencia significativa, en cómo es el sistema percibido por los usuarios, y ciertamente en algunos casos usuarios potenciales.

Consideremos por un momento a un solo usuario, que por alguna razón justamente da la apariencia de no poder hacer que el sistema trabaje para si mismo. Puede haber una tentación de parte del administrador de sistemas en pensar acerca de esta persona como un caso perdido, que sólo no comprende la tecnología o quizás no escucha instrucciones. Éste sería un error garrafal. Si a un usuario le está costando trabajo ser reconocido por el sistema, habrá una razón para ello, y a menudo una muy buena. Esta puede ser una característica física del individuo que dificulta interactuar con el lector biométrico de la manera usual. Por ejemplo, una persona de edad puede tener temporadas recurrentes de artritis en sus manos, dificultando utilizar un lector de geometría de la mano. Alguien más puede tener en particular huellas digitales débiles, dificultando captar una buena muestra para la comparación. Quizás alguien usando un dispositivo de exploración de retina tiene tan pobre alcance visual que cuando le quitan sus lentes, encuentra difícil el tener en la mira el blanco y seguir correctamente alineado con el dispositivo. Pueden haber muchísimas otras razones legítimas por qué ciertos individuos tienen tropiezos con una tecnología en particular que no son experimentadas por la mayor parte de los usuarios.

Cualquier sea la situación, es importante no volverse impaciente, o de alguna otra manera menospreciar al usuario - muy probablemente el error está en el sistema al no poder acomodar suficientemente un amplio rango de sujetos. Por supuesto, los usuarios mismos pueden estarse volviendo impacientes si no comprenden por qué no parecen las cosas estar trabajando para ellos. Lo que importa es comprender por qué

existe el problema y poder rápidamente remediarlo. Si el dispositivo que usted está usando posee características de ajuste del umbral de apareamiento individualmente regulable para cada usuario, entonces usted probablemente podrá encontrar un ajuste que trabaje para este usuario. Ciertamente, con algunos sistemas usted puede reducir este ajuste hasta tal punto que aceptara virtualmente cualquier muestra. Naturalmente esto compromete la seguridad en algo, pero si el usuario no sabe esto, puede ser una componenda aceptable, al menos en el corto plazo, mientras usted considera otras medidas. Si este tipo de situación es manejada correctamente, con cortesía, comprensión y un deseo genuino de ayudar al usuario, en ese entonces dará la imagen de que todo el sistema y su administración van por buen camino. El usuario bien atendido se convertirá en un buen embajador para el sistema - un punto importante si usted está tratando con el público en general. Por otra parte, si el usuario es obligado a sentirse que es una molestia y en cierta forma "diferente" de la norma, entonces esto tendrá un efecto opuesto. Distanciar a un usuario causará dificultades, aún cuando usted le tenga cautivo. Si usted está tratando con el público, le podría hacer perder clientes. Cualesquiera de tales problemas relacionados con usuarios usted por lo tanto debería verlo como una bendición, ya que ellos representan la oportunidad de mostrar simplemente qué tan bueno es usted para manejar tales asuntos, y qué tan importante el bienestar de sus usuarios es para la organización.

No todas las excepciones están relacionadas con los usuarios. Usted puede tener un dispositivo perjudicial en la red que parece trabajar intermitentemente, causando retrasos innecesarios en el proceso de transacciones. Tal falla puede o no puede ser fácil de rastrear, pero debemos ocuparnos de ella prontamente. ¡En muchos casos puede ser apropiado hacer un intercambio del dispositivo ofensivo y tratar con la unidad perjudicial fuera de línea, suponiendo por supuesto que usted tuvo la visión anticipada de mantener un dispositivo guardado de reserva en el sitio por simplemente tales emergencias! Lo que importa por supuesto será el no crear inconveniencia a sus usuarios por no más tiempo del necesario. Si usted no tiene un dispositivo de reemplazo, entonces puede ser mejor echar mano de un proceso manual en esa área en particular, hasta que el sistema este completamente operacional otra vez. Quizás usted este pensando, ah sí, pero una falla se puede desarrollar dentro de la infraestructura de la red misma, la cual es percibida incorrectamente como una falla del dispositivo. Esto es posible por supuesto, pero quizás menos probable si la red fuera bien diseñada y configurada inicialmente y fuesen usadas herramientas de monitoreo para observar capacidad y rendimiento en la red. En una situación realmente crítica, usted puede elegir incorporar alguna elasticidad en forma de rutas duplicadas o alternativas que puedan ser intercambiadas automáticamente cuando el rendimiento descienda por debajo de un cierto umbral. También hay fallas relacionadas con el software anfitrión. Naturalmente usted esperaría que cualquier software serio debería estar libre de errores, pero es difícil probar para cada escenario, y ciertas relaciones entre el software interno y el BIOS del sistema pueden trabajar ligeramente diferentes y producir efectos diferentes, bajo ciertas condiciones

operacionales. Esto es una falla, que será a veces difícil prender con un alfiler para identificarlo y eliminarlo enteramente. Sin embargo, la experimentación persistente del sistema antes de ponerla en funcionamiento, debería haber identificado algunos problemas principales a este respecto.

A veces las fallas naturalmente pueden caer fuera de su control inmediato. Se debe prestar atención a los saltos de energía en los transformadores, aunque esto sea menos probable en situaciones contemporáneas y usted sin duda tendrá un sistema de suministro continuo de energía eléctrica o UPS en el lugar, el cual mantendrá encendido el sistema por un cierto período de tiempo en tal caso. Para ocuparse de las excepciones eficientemente, usted debe tener un proceso adecuado para hacer eso. Parte de esto está en reconocer los tipos de errores que concebiblemente podrían ocurrir y poder tener un plan de contingencia en el lugar para asegurar la continuidad del negocio. Parte de esto también es tener a la mano el recurso correcto para manejar la situación. Si usted subcontrata cualquier de esto, tenga la seguridad de que su contrato incluya acuerdos del nivel de servicio como corresponde.

Para concluir, siempre habrá excepciones, ya sean usuarios, sistemas o el proceso que se trata. Cómo son ellos manejados y por consiguiente el impacto que tienen en todo el sistema, será indicativo de la cantidad de horas dedicadas a pensar y planificar el sistema de antemano. Un buen diseño y un sistema manejado profesionalmente se distinguirán a este respecto. Esto a su vez creará una percepción positiva entre usuarios, conduciendo a un sistema más coherente y de alto rendimiento. Una respuesta pobremente administrada para las excepciones, por otro lado, casi ciertamente tendrá un impacto negativo en la percepción del usuario, que, como ya hemos discutido, adversamente puede afectar el rendimiento global.

3.9 conclusiones de la Implementación

En este capítulo, hemos discutido una parte de los asuntos principales alrededor de la implementación de un sistema biométrico típico. Dependiendo de la escala y naturaleza precisa del sistema en cuestión, esto puede ser considerado como una visión general o quizás como la punta del iceberg. Una cosa es definitiva, el sistema no se instalará y manejará a sí mismo, y por eso necesitamos algún grado de planificación, experticia en la instalación y subsiguiente administración del sistema. El esfuerzo y recursos que le asignemos a esto tendrán un impacto en el éxito inicial y la subsiguiente fácil ejecución del sistema en conjunto.

Es recomendado por consiguiente que veamos la implementación del sistema como un verdadero proyecto y tratemos esto como lo haríamos con algún otro proyecto comercial orientado a la tecnología de la información. Si bien puede haber diversos grados de colaboración con entidades externas como fabricantes del

dispositivo y los integradores de sistemas, es todavía importante manejar absolutamente todo eficientemente y con objetivos claros e inmediatos en el lugar. En el mayor numero de los casos, creo que esto es mejor emprendido por la mismas organización, quien después de todo estará usando y viviendo con el resultado final. En cuanto a esto podría ser designado un Administrador general de Programas quien pueda unir a las diversas entidades y mantener la imagen completa de la estructura en cualquier momento. Esto será importante, como en cualquier sistema de tamaño considerable habrá mucha gente perdida que coordinar, una vez que la implementación comience de verdad. Por ejemplo, la entrega y prueba de cada uno de los dispositivos de captura biométrica, obviamente necesitarán ser emprendidas un buen tiempo antes de que sean finalmente instaladas in situ y conectadas a la red. A su vez, la red misma obviamente necesita estar en el lugar antes de que podamos comenzar a conectar cosas a ella. Éstos son ejemplos obvios donde una secuencia lógica de acontecimientos necesita tener lugar para instalar y habilitar el hardware y software que forman el núcleo de nuestro sistema. Sin embargo, hay factores adicionales como la comunicación y entrenamiento que son igualmente importantes y deben estar cuidadosamente planificadas para coincidir con la fase pertinente de la instalación de sistemas.

Si estamos de acuerdo con lo puntos antedicho, se hará evidente que hay diversas personas que necesitan interactuar con nuestro plan de proyecto, algunos de los cuales vienen realmente de disciplinas y con niveles de conocimientos diferentes. Si esto no está cuidadosamente planificado y orquestado entonces mucho tiempo podría ser desperdiciado en mal entendidos, conduciendo a una aproximación más bien fragmentada de la implementación. Esto es precisamente el porqué un Administrador general del Programa o Director de Programa, debería ser destinado a manejar el proyecto y resolver algunos asuntos que surjan allí adentro. Además, este individuo debería ser un experimentado y experto administrador de proyectos con una trayectoria de asignación y control de trabajos a los programadores comerciales. ¿Suena obvio no es verdad? Pero tristemente no siempre ha sido el caso, con algunas implementaciones de sistemas ejecutadas por gerentes de compra, gerentes de seguridad o quienquiera que parezca haber estado cerca en el momento.

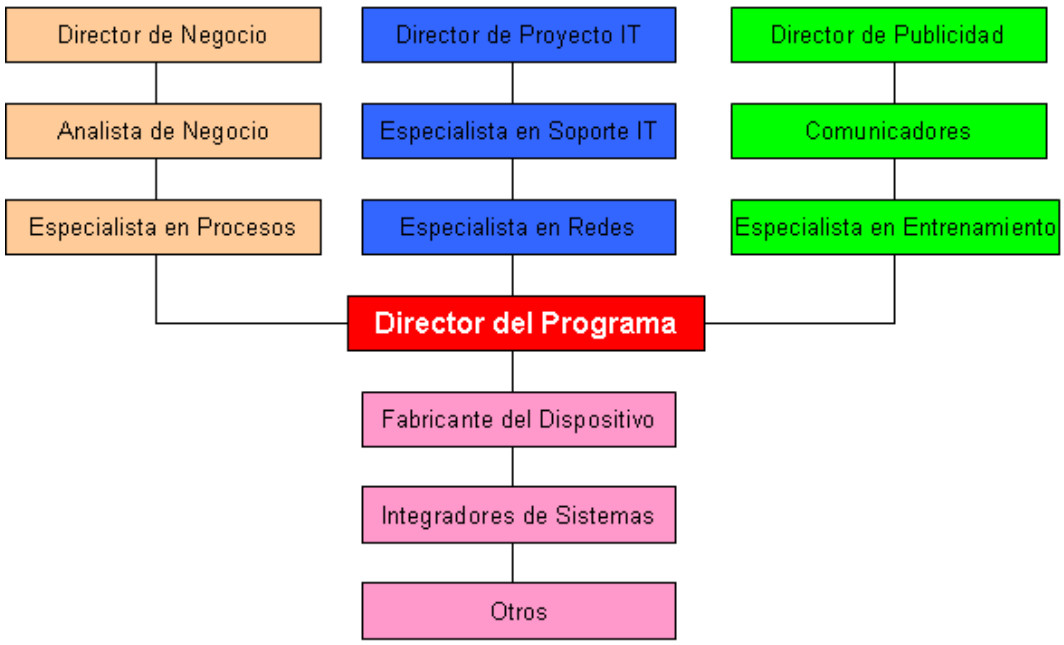


Figura 3.6 Posible estructura del proyecto para su implementación

El ejemplo en la Figura 3.6 representa una posible estructura del proyecto con la cual implementar un sistema biométrico típico. Naturalmente más bien depende de la escala y en algunas instancias nada de eso sería requerido, aunque en otros casos éste podría ser apreciado muchísimo como un armazón del esqueleto. El punto importante es que debería haber alguna estructura en el lugar, con el fin de poder implementar el sistema apropiadamente y por consiguiente darse cuenta de los beneficios por adelantado.

4. El Desarrollo de un Programa Biométrico

Es curioso que en los años formativos de lo que llamaremos la industria de la biometría, hubo mucho énfasis en el dispositivo de captura mismo, o a veces en los dispositivos integrados de este, pero relativamente poco en el software. Quizás esto ocurrió en forma natural, ya que muchos estaban preocupados en probar que el concepto realmente podría trabajar y que su dispositivo en particular era un competidor líder. Hoy en día, existen un montón de productos biométricos dirigidos a funciones de control de acceso de estaciones de trabajo y redes, que naturalmente presentan alguna especie de integración con el software del sistema operativo. Sin embargo, la alta calidad de los innovadores programas de aplicación que presenta la tecnología biométrica (o el potencial a integrarse a ella) es todavía relativamente muy delgada, casi en el suelo. Esto puede parecer sorprendente para algunas personas, cuando usted considera la gran cantidad de empresas profesionales productoras de software a través del globo y el hecho de que los dispositivos biométricos son a menudo percibidos (y de hecho público) como representantes de una excitante, tecnología de vanguardia, dentro de la arena más ancha de la informática.

¿Y entonces como queda usted con todo esto, si esta planeando implementar un sistema biométrico? Naturalmente dependerá de la naturaleza del sistema que usted tenga en mente y de si existen en el mercado un paquete de software que pueda reunir todos los requerimientos. Si este requerimiento es uno relativamente fácil, como el control básico de acceso físico o el registro del tiempo, entonces usted bien puede encontrar algo adecuado que usted pueda tomar de un vendedor e implementarlo directamente. Si el requerimiento es más específico en configuración o implica una integración con su infraestructura existente de sistemas, entonces las cosas son un poco mas diferentes, ya que indudablemente habrá una cierta cantidad de desarrollo requerido. La pregunta es, ¿Quien emprende y maneja este desarrollo?

Existen varias formas mas adelante en cuanto a esto, incluyendo A.- la total contratación de terceros para servicios, por medio del cual usted solo transmite el proyecto en su conjunto a otra compañía, B.- El desarrollo en conjunto, utilizando los servicios de una empresa productora de software en la que se confía, o quizás C.- un proyecto de desarrollo interno, por medio del cual su propio equipo IT (Tecnología de

la Informática), desarrollarán y probarán la solución propuesta. Los méritos relativos de estos acercamientos naturalmente dependerán de la escala del sistema, los recursos internos y varios otros factores, pero en cualquier caso habrá que entender, qué tan modernos los dispositivos biométricos son para interactuar con los sistemas anfitriones y cómo los podríamos tomar en cuenta en términos de desarrollo de software. En este capítulo por consiguiente le echaremos un vistazo a una parte de los asuntos alrededor del desarrollo aplicativo, para sistemas que utilizan la tecnología biométrica. Esto quizás puede ayudar al lector a alcanzar conclusiones en lo que se refiere a, ya sea, si esto es algo que fácilmente podría ser emprendido en forma interna, o de alguna otra manera.

4.1 Escogiendo las herramientas de desarrollo

La elección de las herramientas de desarrollo, es un área que requerirá alguna consideración. Esto especialmente será el caso si su aplicación biométrica necesita integrarse con otras aplicaciones, quizás compartiendo bases de datos o procedimientos existentes y usted tiene el deseo de obtener el mejor rendimiento del sistema. En áreas tales como el acceso a datos por ejemplo, sus herramientas de desarrollo incluye programas controladores nativos para el núcleo de la base de datos, ¿o usted tiene que confiar en algún estrato de interpretación? ¿En qué lenguaje fue escrita su aplicación actual y puede usted fácilmente interactúa con ellas, aunque su medio ambiente preferido de desarrollo sea de otra fuente? A veces esto es perfectamente posible, y a veces está lleno de dificultades.

Si estamos considerando una aplicación autosostenible, entonces obviamente las cosas son más fáciles, ya que no necesitamos pensar acerca de la interfase y sus dependencias, pero incluso aquí tendremos que pensar acerca de la plataforma en la cual el sistema será utilizado. ¿Se ejecutara este bajo UNIX AIX, Windows, 0S2, Linux, o quizá algún otro sistema? Necesitamos asegurar que las herramientas de desarrollo que nosotros usamos sirvan para la plataforma de implementación. En muchos casos probablemente podamos asumir el uso de Windows en alguna de sus versiones de escritorio, y probablemente pudiésemos pensar en utilizar algo así como Windows 2008 Server, para una situación de oficina cuyo rango sea de mediano alcance. Asumamos este último, a ser el caso para nuestras discusiones dentro de este capítulo, esto nos ayudará a enfocar nuestra manera de pensar. Está bien, entonces tenemos un medio ambiente de Windows de 32 bits en nuestra organización teórica. ¿Cuáles son los otros parámetros que deberíamos considerar cuándo estamos escogiendo nuestras herramientas de desarrollo? Bien, probablemente estaremos dependiendo de una base de datos, por dos cosas; para los detalles del usuario y también para almacenar las transacciones de autenticación, de tal manera que una buena interacción con las bases de datos debería estar en nuestra lista. Podemos desear mostrar información de gráficas en forma de fotos del usuario, despliegues

animados y quizás las imágenes de la biometría escogida en sí, como huellas digitales o iris por ejemplo, así es que los gráficos deberían estar bien sustentados también. Naturalmente tendremos el deseo de desarrollar una atractiva e intuitiva interfaz de usuario que sea familiar en apariencia y sentido, para aquellos quienes los estarán usando, así una herramienta que se integre como una sola pieza con la API de Windows y los diversos diálogos que serán requeridos. En el caso de una aplicación autosostenible como estamos considerando, muchos desarrolladores naturalmente gravitarán hacia los medios ambientes populares de desarrollo de Windows como C + +, Delphi y Visual Basic, todo ellos podrían ser adecuados. Otros pueden estar inclinados hacia Java como la promesa de portabilidad a través de plataformas, aunque algunos pueden tener algunos puntos de vista alrededor del rendimiento relativo en cuanto a estos.

Sin embargo, antes de que una elección final sea hecha, deberíamos considerar cuál dispositivo biométrico va a ser usado y lo que está disponible a título de un juego de desarrollo de software (SDK-Software Development Kit) para soportarlo. Algunos fabricantes de dispositivo pueden suministrar un DLL o dos, con algunas llamadas de función medianamente de bajo nivel para las funciones primarias, pero todavía le pueden dejar una buena cantidad de trabajo que hacer al desarrollador, en la forma de integración y comunicaciones. Otros vendedores pueden encapsular amablemente todo en un control OCX o un equivalente tal como un componente de Delphi o un paquete, con un mínimo de funciones relativamente de alto nivel con el que el desarrollador debe trabajar. Si controles como esto son suministrados, entonces naturalmente usted tendrá el deseo de asegurar que su ambiente de desarrollo puede hacer el mejor uso de ellos. Otra consideración aquí es el de las comunicación físicas con el dispositivo, la cual puede ser vía una conexión serial RS232 o RS485, o quizás cada vez mas común, a través de una conexión USB. Si el fabricante del dispositivo no ha encapsulado esto dentro de su propio SDK, entonces el desarrollador debe considerar usar una biblioteca de comunicación – este puede ser otro factor que podría influenciar la decisión de cual herramienta se desbeberá usar. Para el desarrollo general de aplicaciones autosostenible para el entorno de Microsoft Windows, las herramientas populares como Visual C + +, el Builder C + + o Delphi parecería ofrecer un balance entre la estabilidad de poder y la flexibilidad de interacción con los SDKs suministrados por los vendedores de dispositivos biométricos.

Regresemos por un momento a las aplicaciones más complicadas donde haya un requisito de interactuar con otras aplicaciones. Algunas de estas pueden ser aplicaciones heredadas del pasado, que se escribieron en un lenguaje menos familiar o quizás podría estar en ejecución, relativamente aisladas de las aplicaciones de la oficina en general, quizás en una máquina de rango medio. En tal caso, necesitaremos comprender cómo éstos estaban escritos y cómo podemos interactuar con ellos. Puede ser que podamos utilizar el lenguaje de programación nativo para hacer llamadas

directamente a la DLLs del fabricante biométrico, para proveer la funcionabilidad de autenticación. Por otra parte, esto puede ser más complicado si ya hay un nido entrelazado de interfaces entre módulos diferentes o inclusive diferentes programas corriendo en segundo plano. Aquí es donde un pequeño análisis por adelantado es requerido para comprender exactamente cómo una aplicación particular es configurada y en operación, a fin de que podamos averiguar la mejor forma de integrar la funcionabilidad biométrica en ella y que será requerido para hacer esto. Si implica diferentes lenguajes de programación y un conjunto de habilidades, en ese caso entonces deberíamos nombrar a un administrador de proyecto para coordinar esta actividad. Por supuesto, podría no ser un problema del todo, pudiéndonos encontrar con que un programador competente de C + + pueda programar todas las interfases y lógicas necesarias con la aplicación, mientras que en una forma limpia integra la funcionabilidad biométrica necesaria. Este es todo el punto de esta sección, enfatizar la necesidad de comprender nuestros objetivos y los detalles arquitectónicos de nuestra infraestructura existente, para que pudiéramos escoger las herramientas de desarrollo de aplicaciones más apropiadas y a la mano en nuestro trabajo.

¿Así es que cuales son las herramientas que tienen probabilidad de ser las mas adecuadas a este respecto? En muchos casos usted ya tendrá su metodología interna preferida y si este reunirá todos los requisitos o no, entonces podría tener cierto sentido el querer usarlos y ya que usted estará familiarizado con su operación entonces seria pequeña la curva de aprendizaje que tendría que tener, excepto quizás con varias llamadas específicas a funciones biométricas. Si usted tiene plena libertad, entonces las herramientas que tienen buena conectividad y funcionabilidad con la base de datos serían útiles. Los ejemplos populares para el ambiente Windows incluirían a la ediciones empresariales (Enterprise) de Borland C + +, Builder y Microsoft Visual C + +, Borland Delphi es también una muy versátil herramienta a este respecto y bien adecuado para el desarrollo de estilos iterativos RAD. Si usted está construyendo su base de datos, posiblemente utilizando algo así como Oracle o SQL Server, entonces seria pertinente asegurar que usted tiene los manejadores de alto rendimiento nativos para la versión correcta de su metodología escogida de base de datos. Entrar con buen pie y con las herramientas correctas de desarrollo es sumamente importante si queremos tener el mejor rendimiento y funcionabilidad en nuestra nueva aplicación biométrica. Uno puede evocar varias grandes aplicaciones corporativas en el mundo de la tecnología de la información que se han convertido en un asunto deprimente, de bajo rendimiento y pobre estabilidad, mayormente porque fueron hechas en primer lugar con herramientas poco óptimas y no habían sido bien pensadas desde una perspectiva arquitectónica. Si usted ha heredado un sistema viejo y su infraestructura con la que usted tiene que trabajar, entonces al menos gaste algún tiempo pensando acerca de estos asuntos e intente lograr la más completa y mejor solución.

4.2 La Interfaz Gráfica e intuitiva del Usuario

El lector al principio puede extrañar el hecho de que incluyéramos una sección meramente sobre la GUI, o Interfaz Gráfica del Usuario, pero ésta es una consideración de suma importancia, especialmente cuando estamos ocupándonos de las tecnologías y metodologías que serán nuevas para muchos usuarios y operadores del sistema. Presentar estas nuevas ideas en una manera amigable y familiar nos hará avanzar mucho, asegurando que los usuarios rápidamente capten los principios envueltos y disfruten su uso, volviéndose diestros en el manejo y uso del software.

Quizás el primer punto a notar aquí es la importancia de conservar las cosas simples. Si la interfaz es desordenada y no intuitiva, los usuarios lucharán por encontrar el camino y rápidamente llegarán a la conclusión de que éste es un pobre pedazo de software. Esto podría ser desastroso en el contexto del programa para registrar usuarios, donde es tan importante que el administrador adquiera confianza y destreza en capturar una buena calidad de información biométrica de la plantilla. Trae beneficios por consiguiente el hacer las cosas fáciles para ambos el administrador y los usuarios en general. Mientras conservamos las cosas simples e intuitivas, vamos también a tratar de hacer atractivos la interfase. Hay cantidades de cosas que podemos hacer a este respecto, para asegurar que cada pantalla que vea el usuario este elegantemente diseñada y sea agradable a los ojos. Parte de esto está en asegurar que las proporciones relativas de objetos como los campos de datos y las etiquetas están bien simétricos y alineados propiamente en la pantalla. Otro factor es el uso inteligente del color. Los usuarios no desean ser distraídos por extrañas combinaciones de colores, simplemente con el objetivo de ser diferentes, mantengamos los experimentos y pruebas en forma convencional, tal cual todo el mundo está familiarizado. Mientras todavía estamos en el tema de familiarizarnos con el entorno GUI, también deberíamos asegurar que los objetos como las opciones del menú funcionan en la manera esperada. Por ejemplo, si el usuario escoge “Archivo” desde el menú principal, presentémosle las opciones que él normalmente esperaría encontrar en una aplicación tradicional de Windows (asumiendo que estamos desarrollando en una plataforma de Windows). De modo semejante, aseguremos que usamos los diálogos estándar de Windows para imprimir y para el mantenimiento de archivos. Aun mientras todo esto suena bastante obvio, todavía uno se encuentra con aplicaciones que son muy pobres a este respecto. De vez en cuando se encuentra con usuarios escudriñando a lo largo y ancho de la estructura de un menú en una aplicación, buscando funciones que deberían ser obvias, aún después de que esta a sido usada por muchos meses. Esta metodología no seria de gran ayuda a su aplicación biométrica, donde estamos ya tratando de involucrar al usuario en los nuevos procesos y conceptos. Lo último que queremos hacer es dificultar las funciones de todos los días de las personas que laboran en una empresa. Hay áreas

por supuesto en dónde tendremos que desviarnos de la norma, debido a la naturaleza inusual de nuestra aplicación biométrica y la funcionabilidad requerida en esta. Un ejemplo de esto es la botonera de la barra del menú, para el cuál usted puede tener que diseñar algunos separadores obvios, pero otra vez estos deberían ser mantenidos relativamente simples y obvios en lo que se refiere a su propósito. Una interfaz simple, clara y atractiva es por consiguiente lo que deberíamos estar esperando proveer. Podemos apartar la complejidad del programa de la escena, enterradas en el código donde deberían estar.

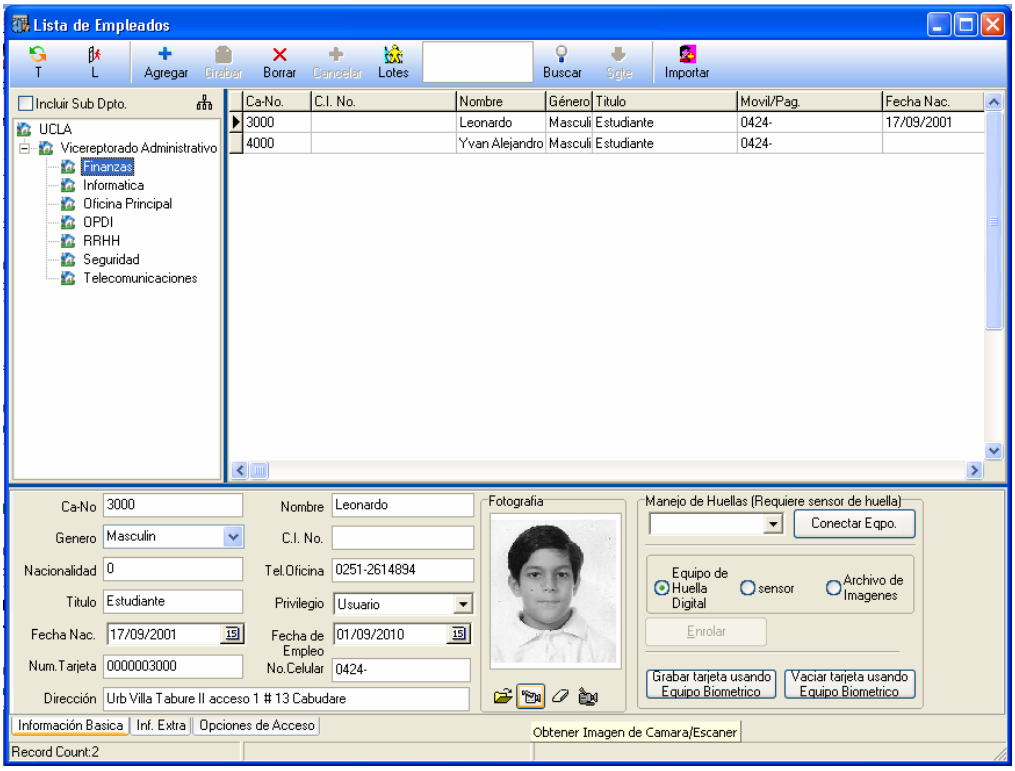
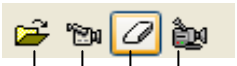


Figura 4.1 Ejemplo de una interfaz de usuario dentro de una aplicación biométrica

En el ejemplo de la figura 4,1, se observa de verdad bastante funcionabilidad disponible desde el interior de esta pantalla, y todavía no parece demasiada complicada a primera vista, un nuevo usuario debería rápidamente entender lo que está ocurriendo y cómo interactuar con el programa. Note también en este ejemplo el uso de un diálogo tabulado en la parte inferior, eficazmente propagando las funciones relacionadas a través de tres "páginas" o pantallas para no desordenar la interfaz del usuario o sumar complicación innecesaria. Esto puede trabaja bien solo cuando usted tiene varias funciones relacionadas, deseando agruparlas en una manera lógica y también intuitivas para el usuario. Usted también puede decidir agrupar objetos relacionados en la misma pantalla con el uso de cajas o marcos. Por ejemplo, en la Figura 4.1 usted notará que en el recuadro relacionado con la fotografía, se utilizaron

un grupo de iconos para describir las operaciones que se pueden realizar en el y eficazmente separándolos fuera de otras funciones. Estos iconos están agrupados de manera tal que cuando utilizamos el apuntador del Mouse y lo posamos sobre uno de estos iconos, este quedara resaltado en un marco de color, inmediatamente nos mostrara cual es su función y de dar clic sobre el, ejecutara la acción programada.



Un usuario novato debería no encontrar ninguna dificultad en comprender cómo obtener una imagen desde un archivo, cámara o escáner, pudiendo seleccionar la fuente de donde desea extraer la imagen o simplemente limpiar el recuadro para no mostrar ninguna imagen del todo. Note también, que si bien hay una cantidad medianamente significativa de código involucrado en realizar todas estas actividades referentes a la foto del empleado, esto está eficazmente escondido del usuario, quien sólo tiene que dar un clic sobre un solo botón o icono para obtener lo que desea.

El mismo procedimiento puede ser usado y recibido con aprecio con respecto a las tareas relacionadas a la biometría, la matriculación o enrolamiento de usuarios y la subsiguiente verificación. Si esto se hace fácil e intuitivo como sea posible, entonces el administrador de sistemas será capaz de emprender la tarea rápidamente y confiadamente de un usuario al siguiente.

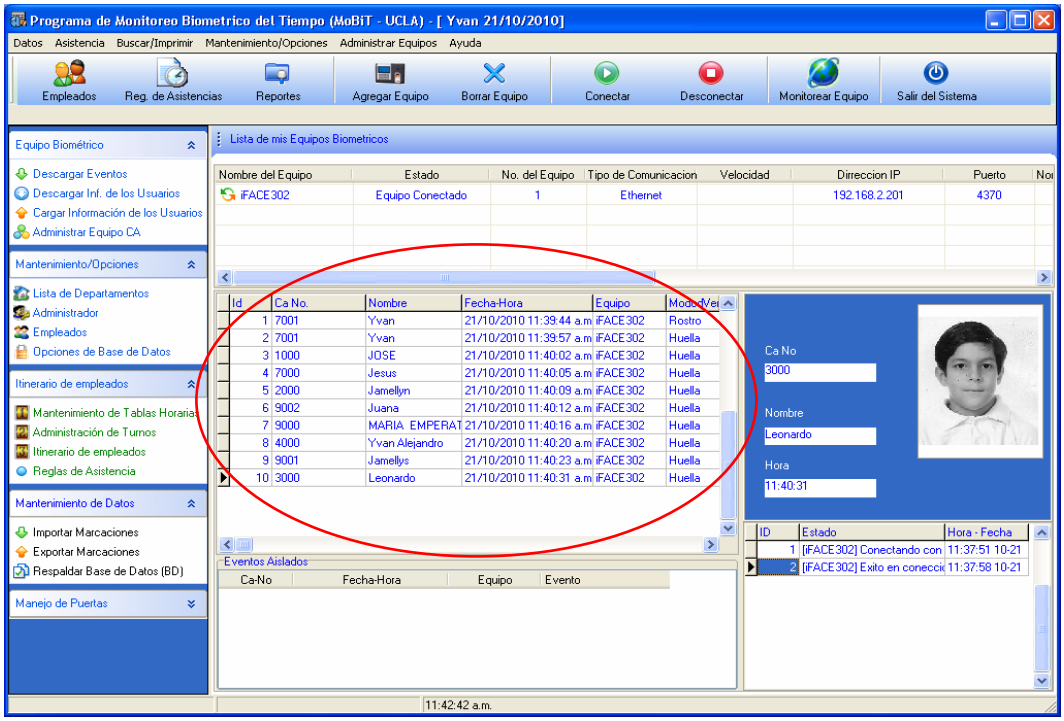


Figura 4.2 Transacciones en tiempo Real

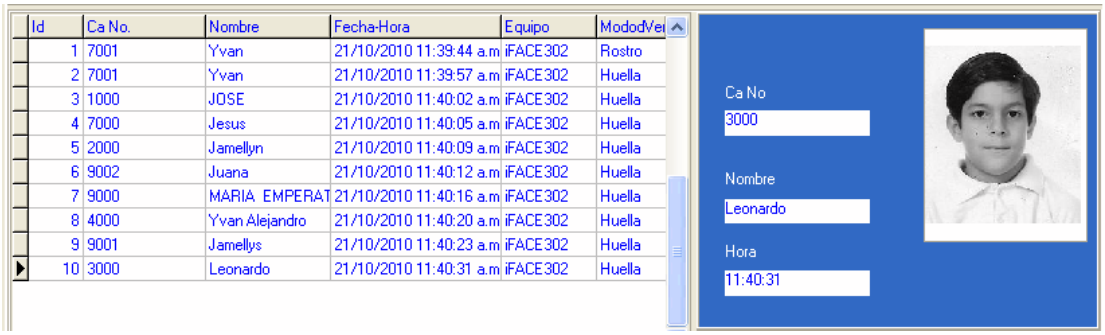


Figura 4.3 Transacciones en tiempo Real – Detalle Ampliado

Un área en donde hay mucho terreno para practicar la Interfaz Gráfica intuitiva del Usuario, es en el monitoreo de las transacciones, donde deberíamos tener como meta presentarle la información al administrador en una manera clara e inequívoca para que le permita a el ver, en tiempo real, exactamente lo que está ocurriendo a todo lo largo del sistema. Esto será en particular importante en situaciones donde haya lectores múltiples o puntos de verificación a todo lo largo de las instalaciones físicas de la empresa. Si los datos de estas transacción además pueden incluir una "puntuación" relativa de qué tan cerca la plantillas almacenada en el equipo biométrico o en una tarjeta y la plantilla leída en vivo coincidieron, lo cual indica un porcentaje de correspondencia entre ellas, e incluso mucho mejor ya que dejará al administrador monitorear a los individuos que puedan estar teniendo dificultades al usar el sistema por una razón u otra.

Además para poder monitorear los datos de las transacciones en tiempo real, seria pertinente en la mayoría de los sistemas dotar al administrador con algún tipo de generador de reportes funcional. Esto pudiese ser llevado a cabo por la utilización de una herramienta estándar de generación de reportes, como Crystal Reports o Report Smith, que deja al usuario configurar y manejar sus propios informes personalizados usando para ello la arquitectura estándar de base de datos. Esto puede satisfacer al "usuario avanzado" muy bien, especialmente si tienen experiencia previa en la herramienta escogida y saben cómo encontrar el camino alrededor. Sin embargo, éste puede ser realmente un área complicada para alguien que podría no ser en particular diestro en la metodología de base de datos y tecnología de la información. Su administrador del sistema biométrico puede ser tal individuo y por consiguiente, si podemos facilitar las cosas suministrándole una función simplificada de la generación de reportes, entonces esto podría valer la pena.

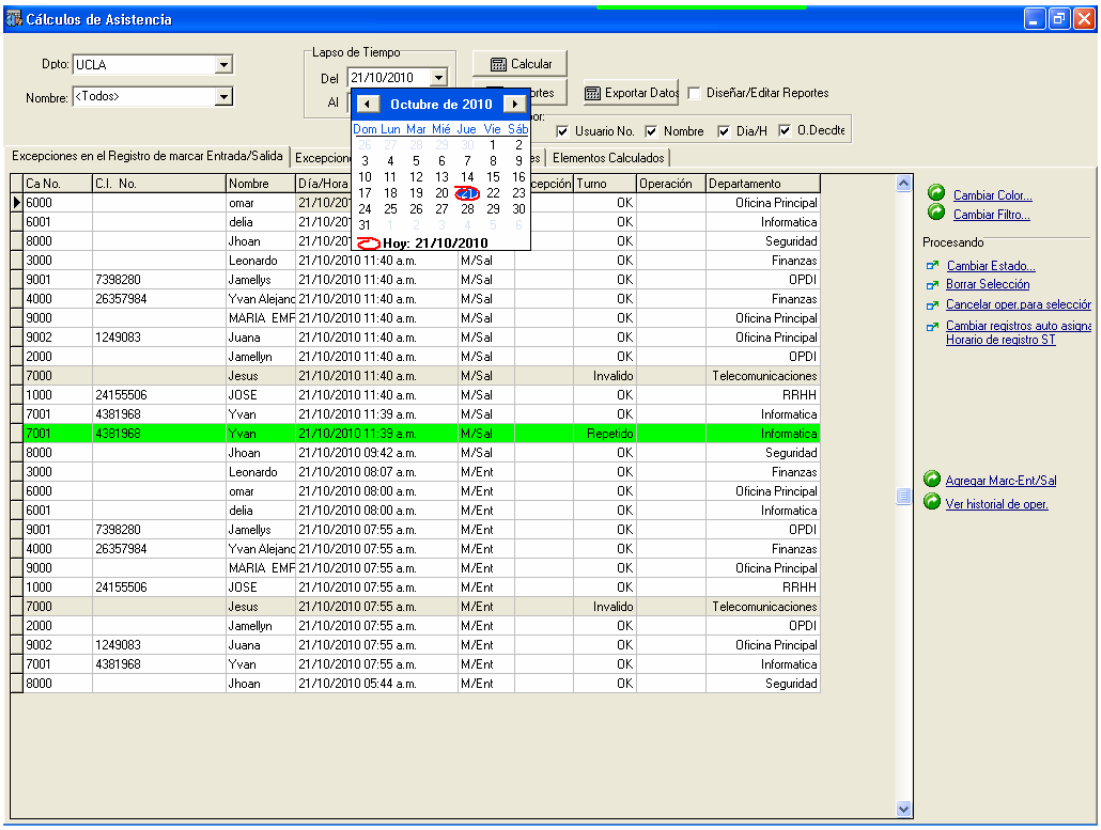


Figura 4.4 Un motor de reportes intuitivo

Una ventana de diálogo tan simple como la que se presenta en la Figura 4.4, le permite al administrador fácil y rápidamente producir reportes contra datos históricos, con simplemente algunos clicks del ratón. En este ejemplo, los reportes pueden ser rápidamente producidos por el usuario, por la verificación de resultados, por rango de fecha o por cualquier combinación de estos y otros parámetros. Esto es algo bastante poderoso, pero no agobia al administrador con tareas como tener que construir búsquedas SQL en la base de datos o tener que correr archivos especiales de comando para obtener los datos deseados. Por supuesto, no hay motivo por qué una herramienta de reportes más poderosa, adicionalmente no pueda ser usada donde esto sea garantizado, y siempre y cuando su base de datos esté en algún formato conocido, entonces no habrá dudas de que esto vaya a ser una materia relativamente fácil de organizar, para sus gerentes de soporte de redes o de tecnología de la información.

La sección de configuración en su aplicación debería ser igualmente abierta y fácilmente comprendida por un administrador con habilidades comunes en la tecnología de la información. Una vez más, debería ser posible esconder mucha de la complejidad detrás de una Interfaz Gráfica del Usuario, dejando al administrador con

sólo aquellas opciones relacionadas con las operaciones cotidianas de alto nivel del sistema.

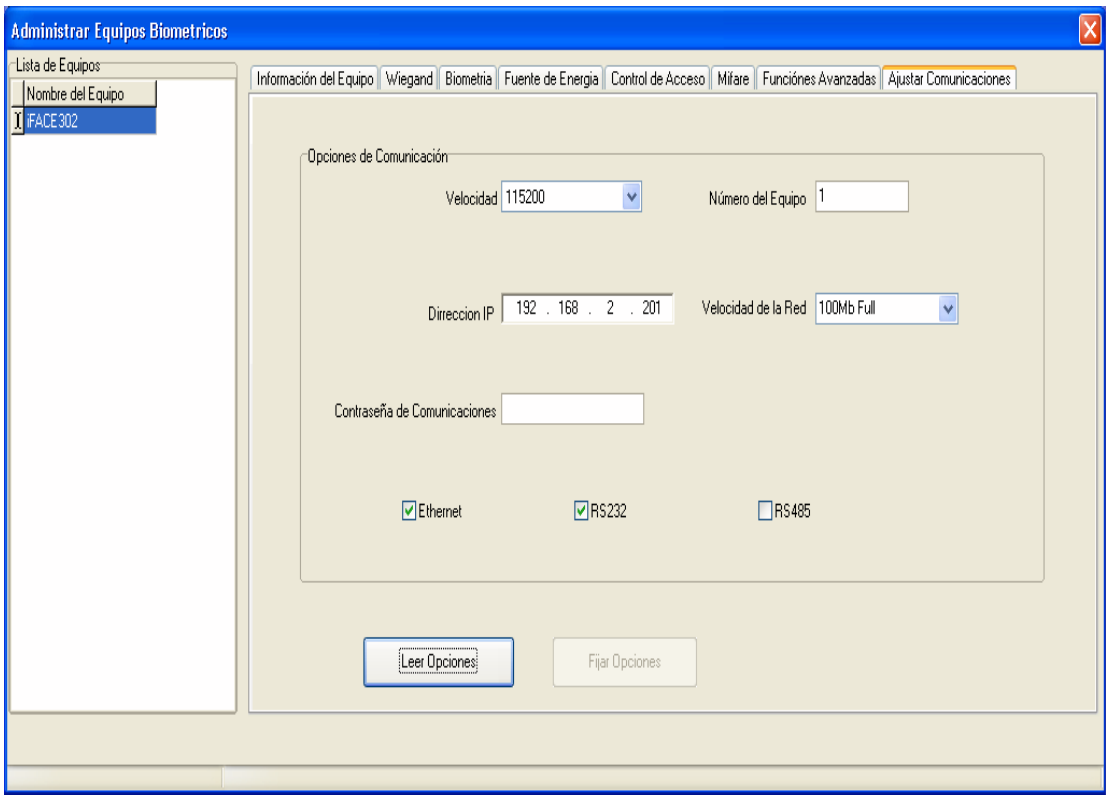


Figura 4.5 Estableciendo los parámetros básicos de operación

Un ejemplo de esto puede ser con respecto a la conexión entre el dispositivo biométrico y la computadora, donde la habilidad para rápidamente seleccionar y probar la conexión física sin meterse en demasiados detalles de bajo nivel, sería de gran valor. Adicionalmente podríamos incluir la habilidad para ajustar algunos parámetros regulables y específicos en el dispositivo en una misma pantalla (como el valor del umbral de correspondencia para la comparación entre la plantilla almacenada y la plantilla en vivo).

Dentro de una aplicación típica por supuesto habrá muchas pantallas y funciones con detalles visuales y de programación, como esos descritos en las anteriormente citadas ilustraciones, pero los principios esbozados arriba nos servirían bien en la mayoría de los casos. Cuando estamos realzando una aplicación existente para proveer funcionabilidad biométrica adicional, entonces la situación quizás será un poco diferente ya que tendremos que entremezclarnos bien con el diseño existente y lógica operacional tanto como sea posible. Pero incluso en tal caso, todavía podríamos ser guiados por el simple e intuitivo GUI.

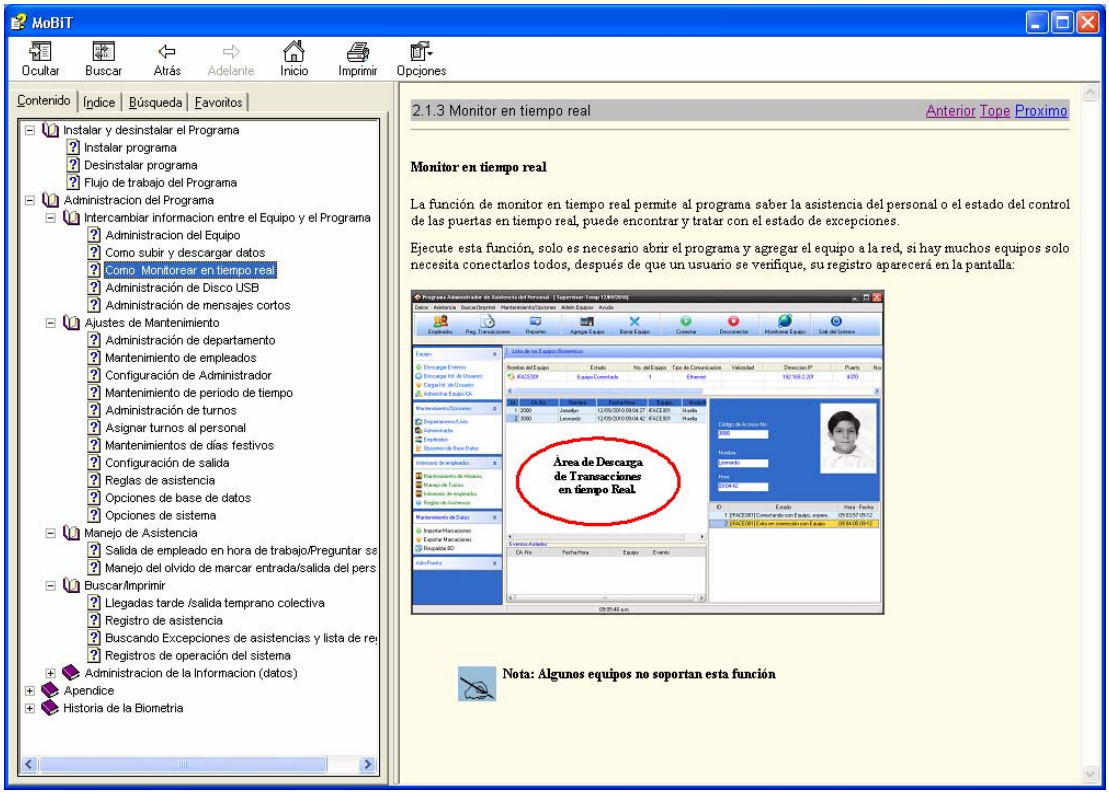


Figura 4.6 La tan deseada Ayuda

Otra área digna de nuestra atención es el archivo de ayuda. Esto puede ser percibido tanto como una bendición como un maleficio, dependiendo de la cantidad de consideración que le damos a esto dentro de nuestro diseño global. Estoy seguro de que todos nosotros hemos experimentado una especie de sentimiento vacío al ver un archivo pobre de ayuda que, aun mientras conteniendo muchos miles de palabras, no parece cubrir las áreas que probablemente parecen ser las mas útiles y necesitadas en un momento dado. Similarmente, el tipo de archivo de ayuda que lo lleva por una interminable cadena de enlaces a otras secciones, hasta que usted se encuentra verdaderamente perdido, eso también es de poco valor real. Lo que necesitamos es algo que sea conciso y vaya directamente al grano, mientras todavía permanece fácil y rápidamente navegable, incluso para un usuario novato. ¿Cuántos archivos de ayuda ha visto usted recientemente en aplicaciones, que representan a la mayoría y que caen en esta categoría? Posiblemente no muchas ya que esta es un área dónde incluso los nombres de grandes grupos familiares en la industria de la Programación, a menudo los pone en tal desorden que da vergüenza, ya que el archivo de ayuda representa un área donde una aplicación realmente puede brillar y puede ser percibida por el usuario como una aplicación de calidad. Aseguremos por consiguiente que nuestro archivo de

ayuda para la aplicación biométrica, permanezca brillante e intuitiva y que realiza la función para la cual fue siempre pretendida, o sea para guiar al usuario en la operación correcta del software y no para actuar como medio publicitario de medio tiempo.

Para concluir, la manera en que presentamos la información al usuario y al administrador de sistemas, es una parte importante de nuestra aplicación biométrica. Esto debería ser considerado con un poco mas de detalle y la Interfaz Gráfica del Usuario diseñada por alguien que tenga experiencia en este campo y comprenda cómo los usuarios interactúan con las computadoras. Si existe un premio en alguna parte para el paquete de software profesional mas fácilmente comprendido, lógicamente funcional y bellamente presentado, entonces nuestra aplicación biométrica debería ser una competidor sólido para ello (como estoy seguro debería serlo). Si no lo es, entonces es hora de volver al tablero de dibujo.

4.3 Comunicaciones de la PC

En muchos casos, cuando utilizamos un SDK (juego de desarrollo del software) de uno de los principales vendedores biométricos, este incluirá la funcionabilidad necesaria de comunicaciones para lograr enlazarse con el dispositivo biométrico por los puertos seriales de la computadora (o a veces usando la red y el protocolo Tcp/Ip). En este caso, el desarrollador no tendrá que preocuparse por los detalles de lo que está ocurriendo entre bastidores para lograr esto. En otros casos, el desarrollador puede estar interactuando con el dispositivo a un más bajo nivel y puede necesitar implementar el código para comunicarse con la PC, usando para ello los puertos seriales o el de la red. Esto puede ser simplificado por la provisión de una biblioteca de comunicación robusta, diseñada para el ambiente escogido de desarrollo y hay ciertamente algunos buenos ejemplos de tales herramientas disponibles para la comunidad de programadores. En uno u otro caso, quizás sería útil el recordarnos de los principios y conceptos básicos de la comunicación Tcp/Ip, sólo como punto de partida, para entender que será requerido en este contexto y los tipos de errores que podrían ocurrir. Se menciona la comunicación Tcp/Ip, ya que es la mas utilizada y permite mayores rango de comunicación, pudiendo estar el equipo biométrico en un lugar y la computadora con la aplicación en otro lugar muy lejos una de otra, ya que se utiliza o bien la Internet o la intranet para ello, por otro lado la comunicación serial RS232, solo sirve cuando el equipo biométrico se encuentra relativamente muy cerca de la aplicación en el PC, igualmente pasa con la comunicación RS485, aunque esta ultima permite mayores distancias, igualmente es para una comunicación local y de corto alcance. Por eso escogeremos la comunicación Tcp/Ip tanto en este libro como en el proyecto completo MoBiT-UCLA, por lo que quisiéramos mencionar algunas cosas referente a este protocolo de comunicaciones a través de un ejemplo.

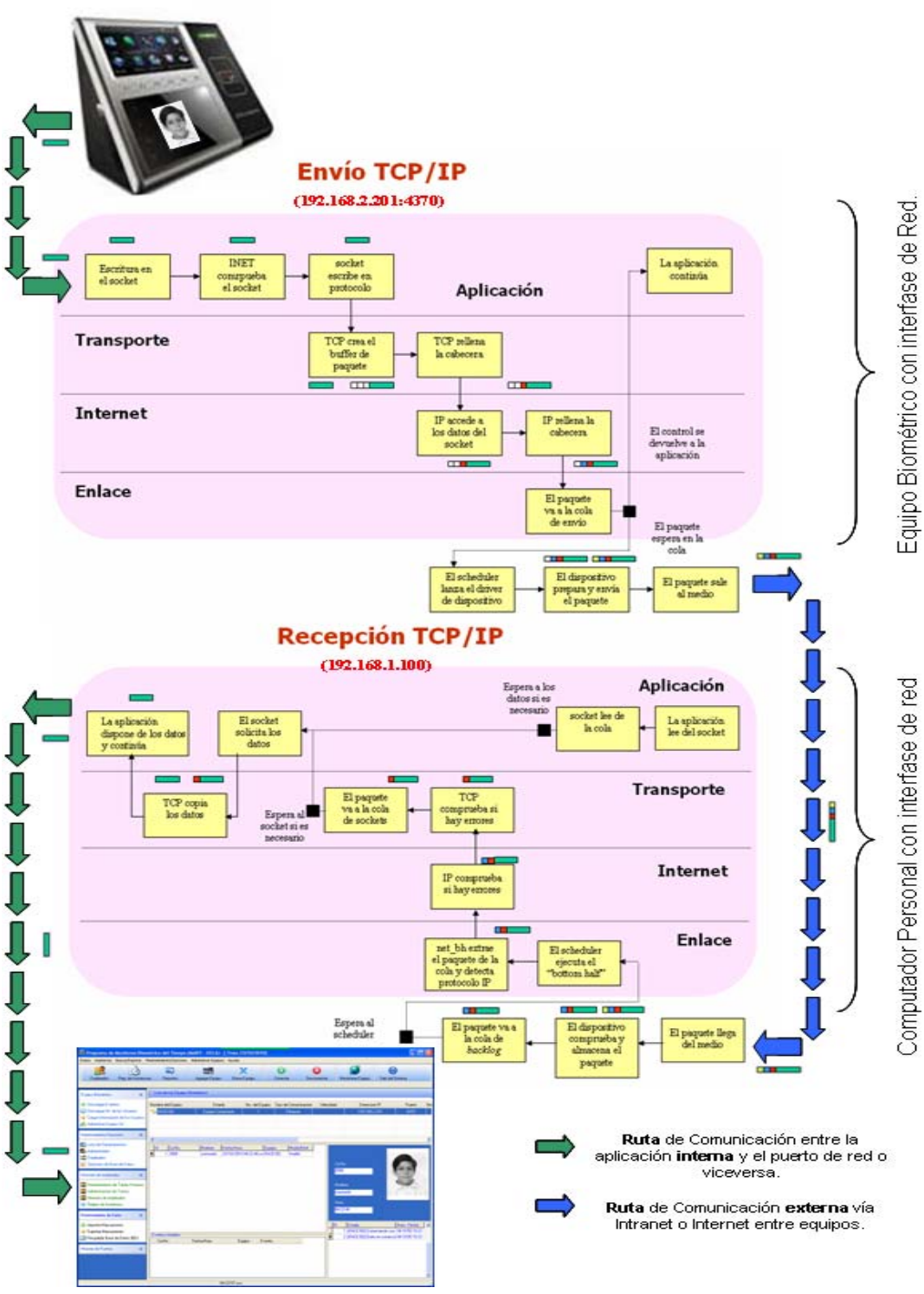


Figura 4.7 Comunicación entre Equipo Biométrico y PC usando TCP/IP

Dentro del mundo globalizado de desarrollo de software, el programar comunicaciones a menudo ha sido considerado como algo oscuro y del mas allá, con muchos practicantes de dicha disciplina pasando horas retozando con el código de una determinada aplicación en sus esfuerzos para iniciar o restaurar las comunicaciones. En realidad, la situación no es tan mala del todo, pero en particular a menudo no está bien documentado, incluso dentro de los ambientes de desarrollo basados en el popular Windows el cual constituye uno de los mejores negocios internacionales en el campo de desarrollo de herramientas (toolkit). Aunque reconociendo el desarrollo para otros sistemas operativos, basaremos nuestra discusión alrededor del ambiente Windows, ya que éste le será familiar a la mayor parte de lectores. Las herramientas disponibles dentro del mismo sistema operativo Windows dejan al usuario configurar los puertos de comunicación en la PC con un nivel razonable de detalle, aunque esta funcionabilidad puede permanecer poco familiar para muchos usuarios, quienes se sentirán dudosos de alguna terminología repetida una y otra vez.

De modo semejante, pocos desarrolladores habrán tenido ocasión de ver esta área a fondo ya que la mayor parte de ellos, solo se han preocupados por aplicaciones de oficina.

Nuestro experimento:

Estableceremos primeramente y en forma **ficticia** una conexión TCP/IP entre un terminal como aplicación cliente y nuestro equipo biométrico iFACE-302 (véase la figura 4.7), como servidor que intercambiarán información usando para ello simples comandos. Decimos ficticiamente porque el servidor, o sea, el iFACE-302 nunca responderá al cliente, porque el cliente no esta haciendo uso de las llamadas especiales de funciones del SDK, apropiados para hacer esta llamada, aunque la conexión realmente si se establece, no hay intercambio de información, pero la idea es valida igualmente. Luego mas adelante crearemos un programa usando visual Basic de Microsoft, para mostrar ya no ficticiamente sino en forma real como se establece una comunicación entre ellas, mostrando el uso de llamadas a DLLs en el paquete SDK para visual Basic y finalmente mostrar una aplicación funcionando en tiempo real para el monitoreo de transacciones.

Ejecutamos entonces el servidor en el host 192.168.2.201, utilizando el puerto 4370 y usamos el comando Telnet o hypertrm (este último es el Hyper Terminal de Microsoft), para actuar como cliente desde el host 192.168.1.100 (el texto en cursiva es introducido por nosotros y el texto en negrita es la respuesta del servidor):

telnet 192.168.2.201 4370
Trying 192.168.1.100... . ←- Tratando

Connected to 192.168.2.201. ←- Conectado a
Escape character is '^]'. . ←- Carácter Escape es
Bienvenido…
salir. ←- Intercambio de Información
Adios…
Connection closed by foreign host. ←-- Conexión cerrada por anfitrión foráneo
>_ ←-- Cursor - Símbolo del sistema

Esto es todo. Ahora procederemos a analizar cómo se ha llevado a cabo esta comunicación a distintos niveles de abstracción.

Nivel de aplicación

A "nivel de aplicación" (lo que "ven" los programas), la comunicación se ha desarrollado de la siguiente manera:

1. El cliente se conecta al servidor.
2. El servidor envía el mensaje "**Bienvenido**.".
3. El cliente envía el comando "salir".
4. El servidor responde con el mensaje "**Adios**.".
5. El servidor cierra la conexión.
6. El cliente cierra la conexión.

Esto es prácticamente lo mismo que podemos observar de la salida del comando telnet utilizado, lo cual no es casual; intencionalmente a este nivel se ocultan todos los detalles de implementación, que aparecerán cuando analicemos los niveles inferiores.

Nivel de transporte

El protocolo utilizado a "nivel de transporte" es TCP. Este protocolo es el encargado de establecer la conexión y dividir la información en paquetes, garantizando que los mismos son entregados correctamente (sin pérdidas y en el orden apropiado).

Cabe resaltar aquí que el otro protocolo de transporte de TCP/IP, UDP no garantiza ni el arribo de todos los paquetes enviados, ni el orden en que estos llegan a destino. Por esto es mucho más simple, no incluyendo algunas de las características de TCP como números de secuencia y asentimientos.

A continuación analizaremos algunos aspectos del protocolo TCP.

Puertos y direcciones

El protocolo TCP se basa en direcciones IP para identificar los equipos (hosts) desde donde provienen y hacia donde se envían los paquetes.

Los puertos (ports) son valores numéricos (entre 0 y 65535) que se utilizan para identificar a los procesos que se están comunicando. En cada extremo, cada proceso interviniente en la comunicación utiliza un puerto único para enviar y recibir datos.

En conjunción, dos pares de puertos y direcciones IP identifican unívocamente a dos procesos en una red TCP/IP.

Números de secuencia

TCP garantiza que la información es recibida en orden. Para ello, cada paquete enviado tiene un número de secuencia. Cada uno de los dos procesos involucrados mantiene su propia secuencia, que se inicia con un valor aleatorio y luego va incrementándose según la cantidad de bytes enviados.

Por ejemplo, si un paquete tiene número de secuencia x y contiene k bytes de datos, el número de secuencia del siguiente paquete emitido será x + k. (Sí, el número de secuencia va contando la cantidad de bytes enviados por cada host.)

Paquetes y acuses de recibo

TCP también asegura que toda la información emitida es recibida. Para ello, por cada paquete emitido, debe recibirse un asentimiento (en inglés “acknowledgement“, abreviado ACK). Si pasado determinado tiempo no se recibe el ACK correspondiente, la información será retransmitida.

El ACK hace referencia al número de secuencia (que ha su vez involucra la cantidad de bytes enviados). Por ejemplo, para comunicar que se ha recibido correctamente el paquete cuyo número de secuencia es x, que contiene k bytes, se enviará un ACK con el valor x + k (que coincide con el próximo número de secuencia a utilizar por parte del emisor del paquete en cuestión). Si el número de secuencia inicial es x, un valor de ACK t significa que el receptor ha recibido correctamente los primeros t-x bytes (en este sentido, el ACK es acumulativo).

El ACK no es un paquete especial, sino un campo dentro de un paquete TCP normal. Por esto, puede ocurrir que se envíe un paquete a solo efecto de asentir una determinada cantidad de bytes, o como parte de un paquete de otro tipo (por ejemplo, aprovechando el envío de nuevos datos, para comunicar la recepción de datos anteriores). De hecho, aunque ya se haya enviado un paquete exclusivamente de ACK con un valor t, si luego se envía un paquete de datos, puede repetirse en él el ACK

con el mismo valor t, sin que esto confunda al emisor de los datos que se están asintiendo. (Por simplicidad, en nuestro ejemplo hemos eliminado esta información redundante).

Otros campos de un paquete TCP

El protocolo TCP incorpora mecanismos tales como control de integridad de los datos (checksum), prevención de congestiones, entre otros, que no serán mencionados aquí por la simplicidad del ejercicio.

Inicio y fin de la conexión

Para dar comienzo a la conexión, el cliente envía un paquete SYN al puerto e IP en donde "escucha" el servidor, con un número de secuencia inicial aleatorio. Este último, responde con otro paquete SYN, con un número de secuencia inicial aleatorio y un ACK con el número de secuencia del paquete SYN recibido, más uno. El cliente envía un paquete con el ACK del SYN recibido, y una vez hecho esto la conexión se encuentra establecida y puede darse comienzo a la transmisión de datos (iniciada por cualquiera de las partes, según el protocolo de aplicación que utilicen).

La razón por la cual se intercambian números de secuencia aleatorios es para evitar que se confunda el inicio de dos conexiones diferentes y algunos ataques que se basan en falsear el comienzo de una conexión (spoofing).

La siguiente figura ilustra el establecimiento de una conexión TCP, llamada "negociación de tres pasos" o "3-way handshake":

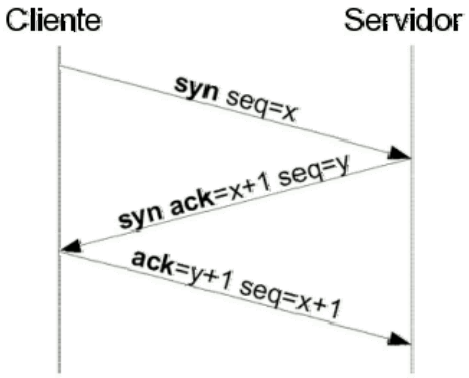


Figura 4.8 Comunicaciones - Establecimiento de una conexión TCP

Para finalizar la conexión, uno de los dos procesos envía un paquete FIN, a lo que el otro responderá con un ACK. A su vez, el otro proceso puede enviar un paquete FIN (recibiendo también un ACK) y la conexión quedará cerrada definitivamente.

Nótese que el segundo proceso puede no enviar el paquete FIN. Esto significa que ese extremo de la conexión no se cerrará, pudiendo aún enviar datos a través de la misma. De lo contrario, en caso de desear terminar la conexión, puede combinar el ACK y el FIN en un solo paquete (esta es la situación más común).

La siguiente figura ilustra la forma general de terminación de una conexión TCP:

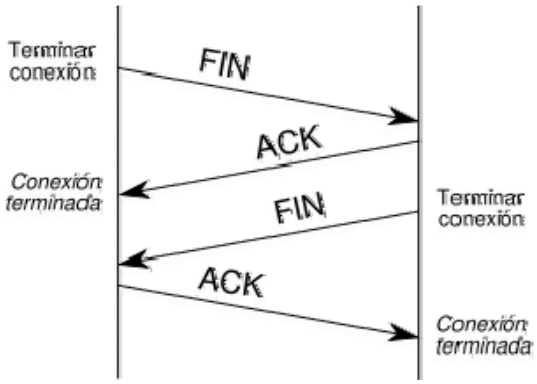


Figura 4.9 Forma general de terminación de una conexión TCP

Análisis a nivel de transporte

Habiendo revisado los conceptos más relevantes, analizaremos ahora la conexión realizada desde el punto de vista del protocolo TCP. Supondremos que el puerto utilizado por el cliente es **4683** (el del servidor, recordemos, es **4370**).

La siguiente figura muestra una visión simplificada de esta conexión:

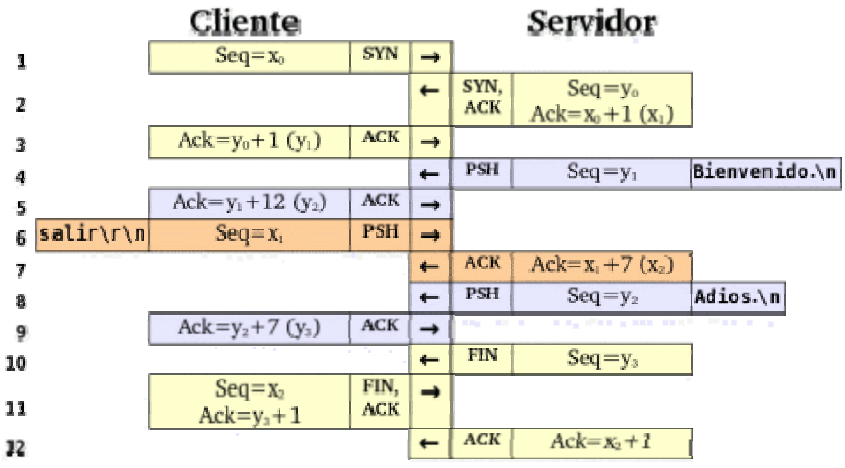


Figura 4.10 Visión simplificada de esta conexión

Veamos qué función cumple cada paquete:

1. El cliente envía un SYN al servidor, con número de secuencia x0.
2. El servidor responde con un paquete SYN, con número de secuencia y0 y un ACK con x0+1 (en adelante, x1).
3. El cliente envía un paquete ACK del SYN que acaba de recibir, con valor y0+1 (en adelante, y1). (A partir de este momento la conexión se encuentra establecida y puede comenzar el intercambio de datos entre las aplicaciones.)
4. El servidor envía un paquete PSH ("push") conteniendo la cadena "Bienvenido.\n" (12 bytes), con número se secuencia y1. (El caracter "\n", newline, representa el fin de línea.)
5. El cliente envía un ACK por la correcta recepción del paquete anterior. El número de ACK es y1+12 (que llamaremos y2 y será el próximo número de secuencia utilizado por el servidor).
6. El cliente envía la cadena "salir\r\n", con número de secuencia x1. (Los caracteres "\r\n" representan el fin de línea. Ver nota al final de la sección.)
7. El servidor envía el ACK correspondiente, con el valor x1 más la longitud de "salir\r\n" (7), que llamaremos x3.
8. El servidor envía la cadena "Adios.\n" (7 bytes), con número de secuencia y2.
9. El cliente envía el ACK con el valor y2+7 (en adelante, y3).
10. El servidor cierra su lado de la conexión enviando un paquete FIN, con secuencia y3.
11. El cliente, que también cierra su conexión, envía un paquete FIN con secuencia x3, con el ACK del paquete anterior (y3+1).
12. El servidor envía el ACK del anterior paquete FIN (con valor x3+1), con lo cual la conexión finaliza.

Nota: En el ejemplo de la figura 4.10 podemos ver un error en el diseño del protocolo de aplicación, ya que el servidor representa los fines de línea con el caracter "\n" ("newline", código ASCII 10), en tanto que el cliente está usando los caracteres "\r\n" ("newline" y "carriage return", códigos ASCII 10 y 13, respectivamente). Esta última es la forma de representación más utilizada en aplicaciones TCP/IP.

Nivel de red (protocolo IP)

Antes de realizar el análisis a "nivel de red" (protocolo IP) vamos a suponer que tenemos la siguiente topología (ver figura 4.11):

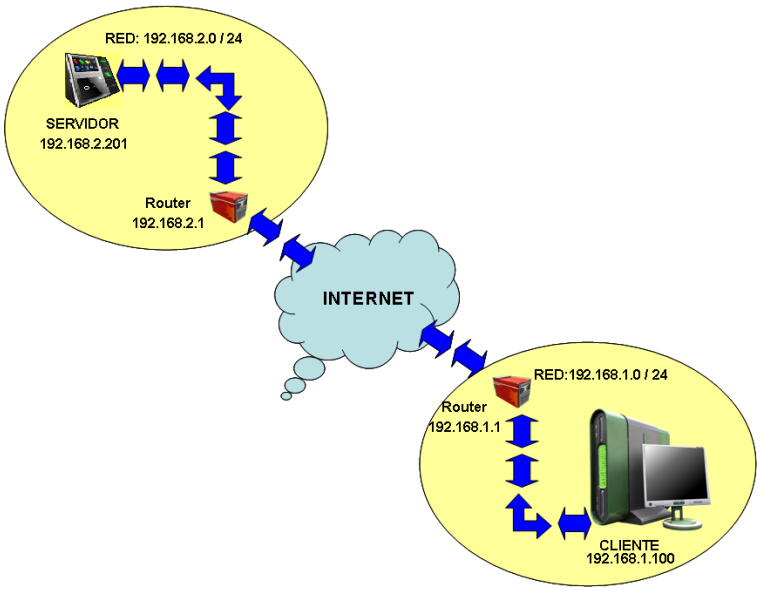


Figura 4.11 Topología de conexión entre equipo biométrico y PC

El cliente se ejecuta en el host cuya dirección IP es 192.168.1.100. El mismo está conectado a la red local 192.168.1.0/24 y su gateway ("router", "enrutador" o "puerta de enlace") es el host 192.168.1.0

La dirección de red local está compuesta por la dirección de red propiamente dicha, 192.168.0.0, y la máscara de red, 24 (que también puede ser representada como 255.255.255.0). Esto significa que los primeros 24 bits de cualquier dirección serán interpretados como identificador de la red, en tanto que los últimos 8 identificarán a cada host (recordemos que, aunque la notación usual es escribir las direcciones IP como cuatro números decimales separados por puntos, en realidad se componen de 32 bits).

Por ejemplo, en el contexto de esta red, la dirección 192.168.1.45 será considerada una dirección local (por coincidir los primeros 24 bits con los de la dirección de red). Esto significa que cualquier paquete destinado a dicha dirección IP, será entregado "localmente" (o sea, directamente a través del protocolo de enlace, como veremos más adelante).

En el caso de una dirección de destino "no-local", los paquetes serán entregados al gateway 192.168.1.1 (usando el protocolo de enlace), quien será luego el encargado de entregar el paquete al host de destino (si este perteneciera a alguna red local a la que dicho gateway esté conectado), o reenviarlo a través de otro gateway (en caso contrario).

De la misma manera el servidor, cuya dirección IP es 192.168.2.201, pertenece a la red 192.168.2.0/24, cuyo Gateway es 192.168.2.1

Análisis a nivel de red

A nivel IP no hay demasiado que agregar. Aquí se realiza el "ruteo" (o "encaminamiento") de los paquetes provenientes de la capa de transporte (que en este nivel se denominan "datagramas") desde la dirección IP de origen hasta la de destino (alternando estos roles 192.168.2.201 y 192.168.1.100 según sea el emisor el servidor o el cliente, respectivamente).

Un campo interesante que se añade es el TTL ("tiempo de vida" o "time to live"), que tiene un valor inicial en el host que produce el paquete (generalmente 64) y luego es decrementado por cada Gateway por el que pasa. Si un Gateway recibe un paquete con el campo TTL en cero, el mismo es descartado y se genera un paquete del protocolo ICMP (usado para control y mensajes de error) dirigido a su emisor, indicando que dicho paquete ha excedido la cantidad máxima de saltos. Esta medida es implementada para evitar que, quizás por un error de ruteo, un paquete quede indefinidamente "dando vueltas" por la red.

En este ejemplo supondremos que el enrutamiento de paquetes es simple (estático), para facilitar las explicaciones. Existen casos complejos en donde se utiliza enrutamiento dinámico, en los cuales paquetes pertenecientes a la misma comunicación pueden enviarse por caminos distintos, alterando inclusive el orden en que llegan al destino (y hasta pudiendo producirse pérdidas).

Debemos tener en cuenta que estamos usando el llamado IPv4 (IP versión 4), ya que también existe el IPv6 (IP versión 6), cuya aplicación se está difundiendo rápidamente en Internet y que soluciona muchos inconvenientes que presenta el anterior.

Nivel de enlace

El "nivel de enlace" es el nivel más cercano al "nivel físico" y es totalmente independiente del protocolo TCP/IP. Existen gran variedad de tecnologías de este tipo; siendo las más comunes Ethernet, WiFi, PPP, Frame Relay, ATM, entre otras.
Supondremos el caso más común: una red Ethernet. Este protocolo se basa en el uso de direcciones de 6 bytes (48 bits), que no son "ruteables" (aquí no existen gateways), por lo cual se utiliza en redes de área local (LANs). Cada dispositivo Ethernet tiene asociada una dirección única (asignada por el fabricante del mismo), la que usualmente se denomina MAC Address.

Resolución de direcciones

Supongamos que el host 192.168.1.100 quiere enviar un paquete IP al host 192.168.1.33 Como ambos están en la misma red local (los primeros 24 bits de sus direcciones coinciden), lo único que debe hacer es averiguar cuál es la dirección Ethernet de este último. Para ello, se utiliza el protocolo ARP ("Address Resolution Protocol").

El funcionamiento es muy simple. El host 192.168.1.100 envía un paquete (en terminología de Ethernet se denomina "frame") a la dirección ff:ff:ff:ff:ff:ff (las direcciones Ethernet se denotan con seis bytes en hexadecimal separados por dos puntos), que es la dirección de broadcast (que llega a todos los hosts de la red) preguntando quién tiene la dirección IP 192.168.1.33. Dicha solicitud ARP tiene como origen la dirección Ethernet del emisor (supongamos, 00:30:b8:80:dd:11).
El poseedor de esa dirección IP le responderá con otro frame con su dirección Ethernet como origen (supongamos, 01:4e:bb:a1:01:8b). De ahora en más, cada vez que el host 192.168.1.100 quiera enviar un paquete IP al host 192.168.1.33, enviará un frame Ethernet proveniente de la dirección 00:30:b8:80:dd:11 a la dirección 01:4e:bb:a1:01:8b, conteniendo el paquete original. (La información sobre las direcciones ARP se almacenan en cada host en una tabla que tiene una duración de algunos minutos.)

Fragmentación
Puede ocurrir que el tamaño de los paquetes producidos por la capa de red (IP, en nuestro caso) sean de un tamaño mayor al máximo que puede transmitir el medio físico utilizado (MTU o "unidad máxima de transferencia". Por esto, puede ocurrir que los paquetes se fragmenten, para acomodarse a esta limitación.

Esta situación puede volver a presentarse a lo largo del camino "físico" que recorra la información, siendo responsabilidad de cada gateway el fragmentar y reensamblar los paquetes para preservar los datos.

Análisis a nivel de enlace

Volviendo ahora a nuestro experimento, el host donde se ejecuta la aplicación cliente (192.168.1.100) debe enviar paquetes IP al host en donde se ejecuta el servidor (192.168.2.201). Claramente, éste último no pertenece a su red local, por lo cual deberá enviarlo a través del gateway.

Para ello, usando el protocolo ARP averigua la dirección Ethernet del gateway (cuya dirección IP, recordemos, es 192.168.2.1), que supondremos es 00:01:02:ed:41:61. Una vez hecho esto, envía un frame Ethernet (con origen 00:30:b8:80:dd:11 y destino

00:01:02:ed:41:61), conteniendo el paquete IP cuyo origen es 192.168.1.100 y con destino a 192.168.2.201.
El gateway recibirá el frame (puesto que la dirección Ethernet de destino es la suya) y dentro de él encontrará un paquete IP dirigido a 192.168.2.201. Decrementará el campo TTL y, en base a las reglas definidas en su "tabla de enrutamiento" (o "tabla de ruteo"), lo reenviará hacia el gateway correspondiente (usando el protocolo asociado al medio físico mediante el cual esté conectado con éste).

Una situación similar se presenta considerando los paquetes emitidos por el host 192.168.2.201 hacia 192.168.1.100

De esta manera, el mismo paquete IP va atravesando distintos gateways a través de distintos medios físicos (que involucran diferentes protocolos de enlace), hasta llegar al host de destino. Por ejemplo, el paquete original puede llegar al primer gateway a través de un frame Ethernet, ser enviado por este al gateway del proveedor de Internet a través de un paquete PPP, atravesar una red ATM en Internet, luego llegar por un enlace Frame Relay al gateway de la red de destino, y ser entregado en otro frame Ethernet al host de destino.

El camino de la información a través de los distintos niveles

La figura 4.12 ilustra un ejemplo del camino que sigue la información desde la aplicación que la produce, a través de los distintos niveles o capas de cada protocolo.

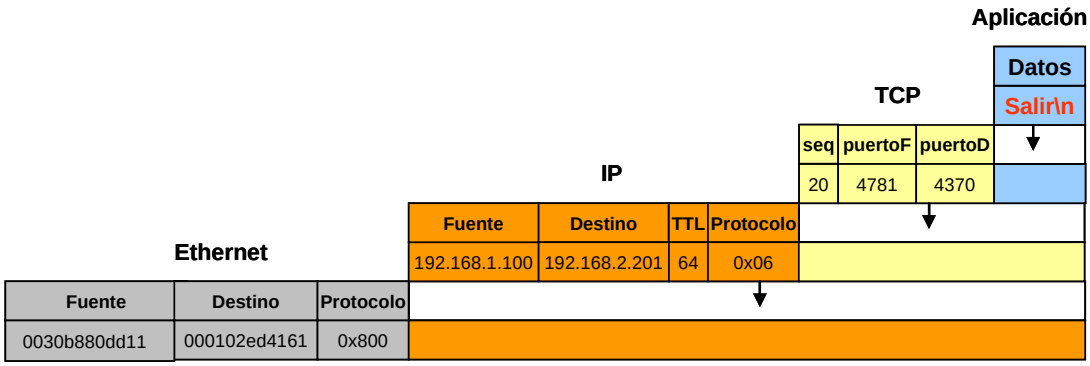


Figura 4.12 Camino que sigue la información desde la aplicación a través de los diferentes protocolos

Nota: Este ejemplo es una simplificación de la realidad. Se han omitido muchos otros datos que forman parte de cada protocolo (controles de error, delimitadores, indicadores de longitud, etc.), que no son relevantes en el contexto de este ejemplo.

1. Nivel de aplicación: La aplicación (en este caso, el programa cliente), escribe la cadena "salir\n".

2. Nivel de transporte: En la capa TCP forma un paquete agregando el número de secuencia (20), puerto de origen (4781) y puerto de destino (4370).
3. Nivel de red: En la capa IP se forma un paquete (datagrama) añadiendo la dirección IP origen (192.168.1.100), destino (192.168.2.201), el TTL (64) y un valor que identifica el protocolo del paquete encapsulado (0×06, valor hexadecimal que representa al protocolo TCP).
4. Nivel de enlace: En la capa Ethernet se forma un nuevo paquete (frame) agregando las direcciones Ethernet de origen (00:30:b8:80:dd:11) y destino (00:01:02:ed:41:61, la dirección del gateway, cuya IP es 192.168.1.1). Se añade además el identificador del tipo de protocolo del paquete contenido (el valor 0×800 corresponde al protocolo IP).
5. Nivel físico: El frame formado es enviado a través del medio físico que vincula los hosts de la red local (típicamente, cable de par trenzado).

Como puede apreciarse, tanto el protocolo IP como Ethernet "encapsulan" a otros protocolos. Esto permite realizar distintas combinaciones, creando "túneles" (como en el caso del ampliamente difundido y utilizado PPPoE).

Software, modelo conceptual y hardware

El siguiente diagrama, en la figura 4.13, muestra la relación entre cada uno de los componentes lógicos analizados, su implementación y la división entre hardware y software.

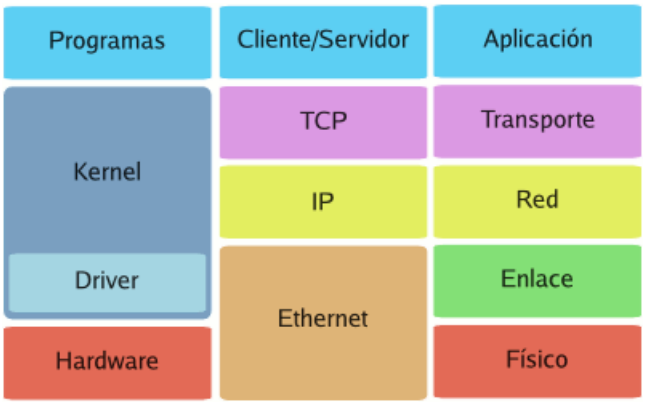


Figura 4.13 Relación entre cada uno de los componentes lógicos

Para finalizar

En este ejemplo hemos recorrido cada uno de los principales componentes del protocolo TCP/IP y analizado su función a través de un ejemplo concreto (aunque simple). Deliberadamente, hemos omitido algunos puntos importantes, como el

sistema DNS (que posibilita la utilización de nombres en vez de direcciones IP), la asignación automática de direcciones IP (a través del protocolo DHCP), y algunos detalles sobre direccionamiento y enrutamiento IP.

Habiendo introducido los datos en la PC, ahora tenemos que reconocerlo dentro de nuestro programa de aplicaciones. Asumiendo que este se ha escrito usando uno de los ambientes mas populares de desarrollo visual, tal como Visual C + + o Delphi, hay, como anteriormente fue citado, disponibles diversas bibliotecas con conectores de comunicación, que pueden manejar la interfaz entre nuestra aplicación y el puerto de comunicaciones Tcp/Ip. La metodología basada en eventos usualmente confiará en un factor provocante, el cual es activado cada vez que los datos arriban al puerto designado de comunicación. En el momento de la activación de este detonador, necesitaremos ver el paquete de datos entrante para averiguar quien ha enviado el mensaje y lo que el mensaje nos está diciendo (un dispositivo biométrico en alguna parte del sistema sin duda) (probablemente los detalles de una transacción de autenticación). Nuestro código, en la aplicación, necesitará extraer de este paquete de información los detalles apropiados y asegurar que la respuesta correcta es generada dentro del programa, mostrar información para escribir en un registro de la base de datos o cualquier cosa que sea apropiado. El paquete de datos por supuesto puede estar encriptada de algún modo, por el interés de la seguridad de la información y puede incluir una metodología avanzada de detección de errores con relación a la integridad de los datos, todo lo cual necesitará ser acomodado por nuestra aplicación, con rutinas de control de errores incorporado donde sea necesario. Naturalmente esta comunicación no es en una sola vía y nosotros sin duda estaremos generando una cantidad igual de tráfico en las comunicaciones de regreso al dispositivo biométrico o dispositivos en la red. Adicionalmente podemos estar haciendo un escrutinio de la red con el fin de asegurarnos que todos los dispositivos están presentes y trabajando correctamente.

Para concluir, la comunicación de datos entre el PC anfitrión y nuestro dispositivo biométrico, o la red de dispositivos, puede ser un área en el cual no necesitamos involucrarnos demasiado, si estamos usando las llamadas de función suministradas como cortesía de los vendedores biométricos, SDK. Sin embargo, una comprensión de lo que está ocurriendo a este respecto, será útil para comprender cualquier mensaje externo de error que pueden ser generados. Si se necesita en realidad llegar hasta un nivel bajo de programación en comunicaciones, entonces el desarrollador debería tener experiencia en este campo o rápidamente debería poder obtenerlas, acelerar y así obtener los conocimientos necesarios para poder abordar esta área. En la mayoría de los casos, usar una de las bibliotecas probadas disponibles de comunicación será más oportuno, ya que la curva de aprendizaje no será demasiada pronunciada y la funcionabilidad probablemente será más que adecuada para encontrar nuestros requisitos.

4.4 Interactuando con los dispositivos biométricos

En la última sección fue mencionado el SDKs, el cual es suministrado por la mayoría de vendedores biométricos de dispositivos. Esto es algo muy significativo ya que les permite a los diseñadores externos de software, desarrollar aplicaciones, o realzar la existente para proveer funcionabilidad biométrica vía el dispositivo escogido. Típicamente, el SDK consistirá en una o varias DLL (biblioteca dinámica de enlace) conteniendo varias funciones que pueden ser llamadas desde la aplicación anfitriona. El desarrollador naturalmente debe estar familiarizado con el modelo DLL y cómo usar esta funcionabilidad desde adentro del ambiente de desarrollo escogido. Algunos vendedores biométricos irán un paso más adelante y proveerán un control OCX o quizás un componente dedicado para ser usado dentro de la herramienta de desarrollo tal como el producto popular Delphi de Borland. Esto hace la vida incluso más fácil para el desarrollador, ya que el componente eficazmente encapsulara la funcionabilidad requerida para interconectar al dispositivo biométrico, haciendo fácil su inicialización y configuración. Varias de las funciones operacionales del dispositivo tales como enrolar (matricular) plantillas de usuarios o su comparación, serán realizadas vía la llamada a una función DLL provista como parte del OCX o componente cuando sea registrado dentro del ambiente de desarrollo escogido. Esto deja al desarrollador pasar menos tiempo preocupándose por la interfase del dispositivo y más tiempo concentrándose en los aspectos operacionales del software que se esta desarrollando.

Así como el acabado del software puede ser de calidad variable, así lo puede ser con el SDKs, especialmente acerca de su documentación y estabilidad global. A veces uno puede encontrarse con que el SDK está bien para un ambiente en particular (usualmente el favorecido por el vendedor) de desarrollo pero puede ser un poco más impreciso en su soporte para ambientes de desarrollo alternativos. Esto es digno de establecer por adelantado por medio de la discusión con el propio equipo de desarrollo de software del vendedor. Puede ser que estén encantados de cooperar en cualquier ajuste fino requerido para adecuar el SDK al uso con su herramienta preferida de desarrollo, para ampliar su interés global. Éste puede ser un punto a considerar para aquellos que están pensando por ejemplo en Linux.

Otro asunto que ha estado en las mentes de desarrolladores independientes de software al considerar la biometría es que cada vendedor parece tener su propio conjunto de reglas acerca de la interfaz del dispositivo y las necesarias llamadas a funciones. Esto fue reconocido hace algún tiempo por la industria biométrica y una iniciativa denominada BioAPI fue iniciada por un consorcio de partes interesadas incluyendo casas matrices tales como Intel, Unisys y Compaq así como también un montón de los principales vendedores biométricos de la industria. El consorcio BioAPI anunció en abril de 1998 su intención de desarrollar un estándar biométrico

común de API. Durante todo el resto de 1998 y 1999 otras iniciativas de API (BAPI y HA-API) fueron incorporadas a la mezcla global, produciendo un borrador a finales de 1999. Para cuando usted lea este libro, la segunda edición del estándar BioAPI posiblemente habrá sido expedida y adoptada por la mayor parte de vendedores biométricos. Esto facilitará mucho las cosas para los desarrolladores de software ya que podrán familiarizarse con un set estándar de llamadas a funciones, permitiendo que sea un proceso simple el adaptar diferentes dispositivos biométricos a sus aplicaciones. Desde la perspectiva de un usuario final, esto puede significar que no son totalmente dependientes de un solo vendedor y quizás pueden incorporar dispositivos de más de una fuente – lo cual seria un estado más deseable. Al momento de escribir, el documento en borrador de las BioAPI tenía unas 107 páginas, representando un esfuerzo considerable de parte de los integrantes del consorcio. . Los SDKs futuros de los principales vendedores biométricos, esperanzadamente serán condescendiente BioAPI con respecto a sus diversas llamadas a funciones, haciendo menor la curva de aprendizaje para el desarrollador de aplicaciones.

Pero qué en verdad ocurre en la práctica y qué tan difícil es para el desarrollador común, incorporar metodología biométrica en una aplicación. Mucho depende del ambiente de desarrollo utilizado. Puede ser cuestión de solo inicializar y luego llamar a las funciones dentro del propio DLL del vendedor biométrico, o en algunas instancias puede ser posible encapsular la funcionabilidad biométrica dentro de un módulo, haciéndola más fácil referirse desde cualquier otra parte del programa.

A continuación vamos a presentar el código fuente y la interfase final de un programa realizado en un ambiente de desarrollo de Visual Basic, como se deja ver en la siguiente lamina (ver figura 4.14), el ambiente visual que ofrece la corporación Microsoft, es cómoda e intuitiva, ayudando al desarrollador a tomar control de las múltiples variables en juego en el desarrollo de una aplicación biométrica, permitiendo y mostrando el uso de varias herramientas como ayuda al programador. Primero se mostrara el ambiente de programación, luego el programa mismo, mostrando las llamadas a funciones dentro de una DLL provista por el fabricante del equipo biométrico llamada zkemkeeper.dll, la cual incluye entre otras funciones a OnAttTransactionEx, OnAlarm y OnDoor. Estas tres funciones le permitirán a la aplicación conectarse al dispositivo biométrico y obtener de el, en tiempo real, cualquier transacción que sea realizada incluyendo alarmas por dejar la puerta abierta o por error en la transmisión de datos del usuario, al final se muestra la aplicación en plena ejecución mostrado los datos de los usuarios que se registran en el equipo (ver la figura 4.15).

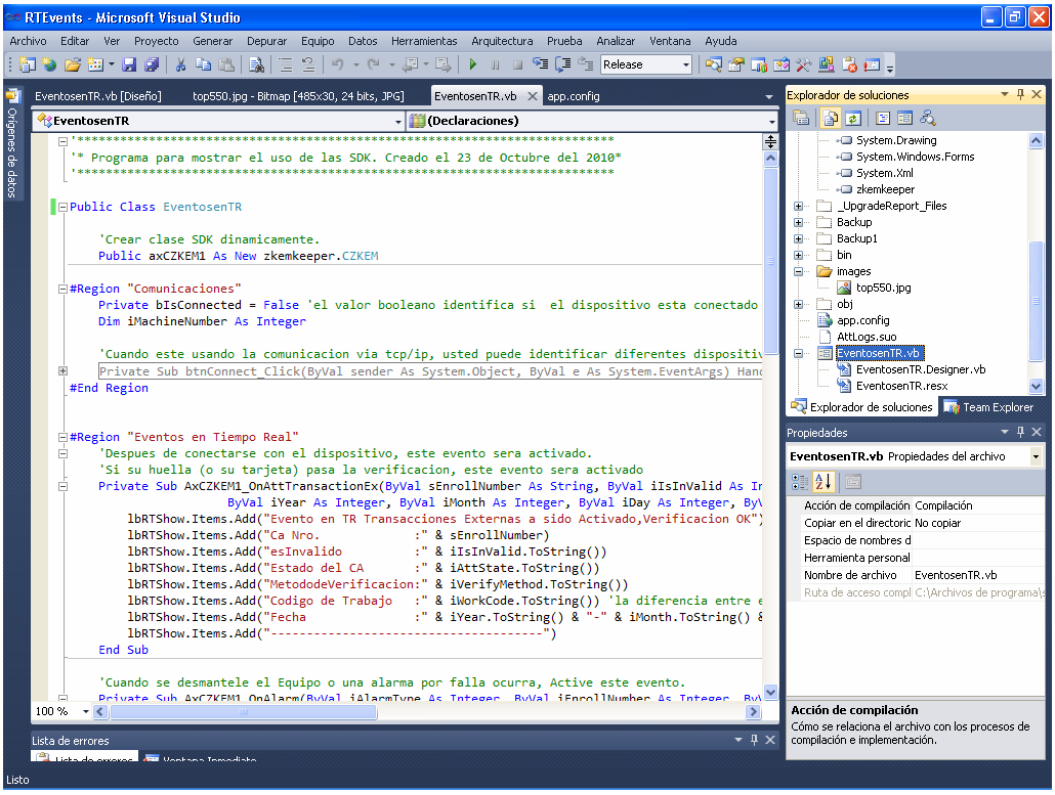


Figura 4.14 Ambiente de programación Visual – Microsoft Visual Estudio 2010

CODIGO FUENTE COMPLETO:

```
'*********************************************************************************************
'* Programa para mostrar EL uso de las SDK en Visual Basic 2010. Creado el 23/10/2010        *
'*********************************************************************************************

Public Class RTEvents

    'Crear clase SDK dinamicamente.
    Public axCZKEM1 As New zkemkeeper.CZKEM

#Region "Comunicaciones"
    Private bIsConnected = False 'el valor booleano identifica si  el dispositivo esta
conectado

    'Cuando este usando la comunicacion via tcp/ip, usted puede identificar diferentes
dispositivos por su direccion IP.
    Private Sub btnConnect_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles btnConnect.Click
        If txtIP.Text.Trim() = "" Or txtPort.Text.Trim() = "" Then
            MsgBox("IP no pede quedar vacio", MsgBoxStyle.Exclamation, "Error")
            Return
        End If
        Dim idwErrorCode As Integer
        Cursor = Cursors.WaitCursor
        If btnConnect.Text = "Desconectar" Then
```

```
            axCZKEM1.Disconnect()
            RemoveHandler axCZKEM1.OnAttTransactionEx, AddressOf  AxCZKEM1_OnAttTransactionEx
            RemoveHandler axCZKEM1.OnAlarm, AddressOf AxCZKEM1_OnAlarm
            RemoveHandler axCZKEM1.OnDoor, AddressOf AxCZKEM1_OnDoor
            bIsConnected = False
            btnConnect.Text = "Conectar"
            lblState.Text = "Estado Actual:Desconectado"
            Cursor = Cursors.Default
            Return
        End If

        bIsConnected = AxCZKEM1.Connect_Net(txtIP.Text.Trim(),
Convert.ToInt32(txtPort.Text.Trim()))
        If bIsConnected = True Then
            btnConnect.Text = "Desconectar"
            btnConnect.Refresh()
            lblState.Text = "Estado Actual:Conectado"
            iMachineNumber = 1 'En realidad, cuando usted esta usando la comunicacion via
tcp/ip, este parametro sera ignorado, cualquier valor entero estara bien.Aqui se uso 1.
            If axCZKEM1.RegEvent(iMachineNumber, 65535) = True Then 'Aqui usted puede Regis-
trar los eventos en tiempo real que usted quiere que sean activadazos (el parámetro 65535
significa todoslos registros)
                AddHandler axCZKEM1.OnAttTransactionEx, AddressOf AxCZKEM1_OnAttTransactionEx
                AddHandler axCZKEM1.OnAlarm, AddressOf AxCZKEM1_OnAlarm
                AddHandler axCZKEM1.OnDoor, AddressOf AxCZKEM1_OnDoor
            End If
        Else
            AxCZKEM1.GetLastError(idwErrorCode)
            MsgBox("Imposible conectarse al dispositivo,CodigodeError=" & idwErrorCode,
MsgBoxStyle.Exclamation, "Error")
        End If
        Cursor = Cursors.Default
    End Sub
#End Region


#Region "Eventos en Tiempo Real"
    'Despues de conectarse con el dispositivo, este evento sera activado.
    'Si su huella (o su tarjeta) pasa la verificacion, este evento sera activado
    Private Sub AxCZKEM1_OnAttTransactionEx(ByVal sEnrollNumber As String, ByVal iIsInValid As
Integer, ByVal iAttState As Integer, ByVal iVerifyMethod As Integer, _
                    ByVal iYear As Integer, ByVal iMonth As Integer, ByVal iDay As Integer,
ByVal iHour As Integer, ByVal iMinute As Integer, ByVal iSecond As Integer, ByVal iWorkCode As
Integer)
        lbRTShow.Items.Add("Evento en TR Transacciones Externas a sido Activado,Verificacion
OK")
        lbRTShow.Items.Add("Ca Nro.     :" & sEnrollNumber)
        lbRTShow.Items.Add("esInvalido :" & iIsInValid.ToString())
        lbRTShow.Items.Add("Estado del CA :" & iAttState.ToString())
        lbRTShow.Items.Add("MetododeVerificacion:" & iVerifyMethod.ToString())
        lbRTShow.Items.Add("Codigo de Trabajo   :" & iWorkCode.ToString()) 'La diferencia
entre el evento OnAttTransaction y OnAttTransactionEx
        lbRTShow.Items.Add("Fecha      :" & iYear.ToString() & "-" & iMonth.ToString() & "-" &
iDay.ToString() & " " & iHour.ToString() & ":" & iMinute.ToString() & ":" &
iSecond.ToString())
        lbRTShow.Items.Add("-------------------------------------")
    End Sub

    '/Cuando se desmantele el Equipo o una alarma por falla ocurra, Active este evento.
    Private Sub AxCZKEM1_OnAlarm(ByVal iAlarmType As Integer, ByVal iEnrollNumber As Integer,
ByVal iVerified As Integer)
        lbRTShow.Items.Add("Evento en Tiempo Real, Alarma ha sido Activada...")
        lbRTShow.Items.Add("...TipodeAlarma=" & iAlarmType.ToString())
```

```
        lbRTShow.Items.Add("...NumeroMatricula=" & iEnrollNumber.ToString())
        lbRTShow.Items.Add("...verificado=" & iVerified.ToString())
    End Sub
    'Evento de puerta Abierta
    Private Sub AxCZKEM1_OnDoor(ByVal iEventType As Integer)
        lbRTShow.Items.Add("Evento en Tiempo Real, Puerta ha sido Activada...")
        lbRTShow.Items.Add("...TipodeEvento=" & iEventType.ToString())
    End Sub
#End Region

    Private Sub RTEvents_Load(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles MyBase.Load

    End Sub

    Private Sub AxCZKEM1_OnAttTransactionEx()
        Throw New NotImplementedException
    End Sub

    Private Sub txtIP_TextChanged(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles txtIP.TextChanged
    End Sub
End Class
```

EXPLICACION DE FUNCIONES SEGÚN EL MANUAL DEL SDK PARA VISUAL BASIC:

OnAlarm :

OnAlarm (LONG AlarmType,LONG EnrollNumber,LONG Verified)
This event is triggered when the device reports an alarm.
[Return Value]
Alarm Type: Type of an alarm. 55: Tamper alarm. 58: False alarm. 32: Threatened alarm.
34: Anti-pass back alarm.
EnrollNumber: User ID. The value is 0 when a tamper alarm, false alarm, or threatened alarm is given. The value is the user ID when other threatened alarm or anti-pass back alarm is given.
Verified: Whether to verify The value is 0 when a tamper alarm, false alarm, or threatened alarm is given. The value is 1 when other alarms are given.

OnDoor :

OnDoor (LONG EventType)
This event is triggered when the device opens the door.
[Return Value]
EventType: Open door type
4: The door is not closed. 53: Exit button. 5: The door is closed. 1: The door is opened unexpectedly.

OnAttTransactionEx :

OnAttTransactionEx (BSTR EnrollNumber,LONG IsInValid,LONG AttState, LONG VerifyMethod,LONG Year, LONG Month, LONG Day, LONG Hour, LONG Minute, LONG Second,
LONG WorkCode)
This event is triggered after verification succeeds.
[Return Value]
EnrollNumber: UserID of a user.

IsInValid: Whether a record is valid. 1: Not valid. 0: Valid.
AttState: Attendance state (default value). 0—Check-In 1—Check-Out 2—Break-Out 3—Break-In 4—OT-In 5—OT-Out
VerifyMethod: Verification mode. Generally, 0: password verification, 1: fingerprint verification, 2: card verification.
In multi-verification mode:
FP_OR_PW_OR_RF 0
FP 1
PIN 2
PW 3
RF 4
FP_OR_PW 5
FP_OR_RF 6
PW_OR_RF 7
PIN_AND_FP 8
FP_AND_PW 9
FP_AND_RF 10
PW_AND_RF 11
FP_AND_PW_AND_RF 12
PIN_AND_FP_AND_PW 13
FP_AND_RF_OR_PIN 14
FACE 15
Year/Month/Day/Hour/Minute/ Second indicates the time when verification succeeds.
WorkCode: work code returned during verification. Return 0 when the device does not support work code.

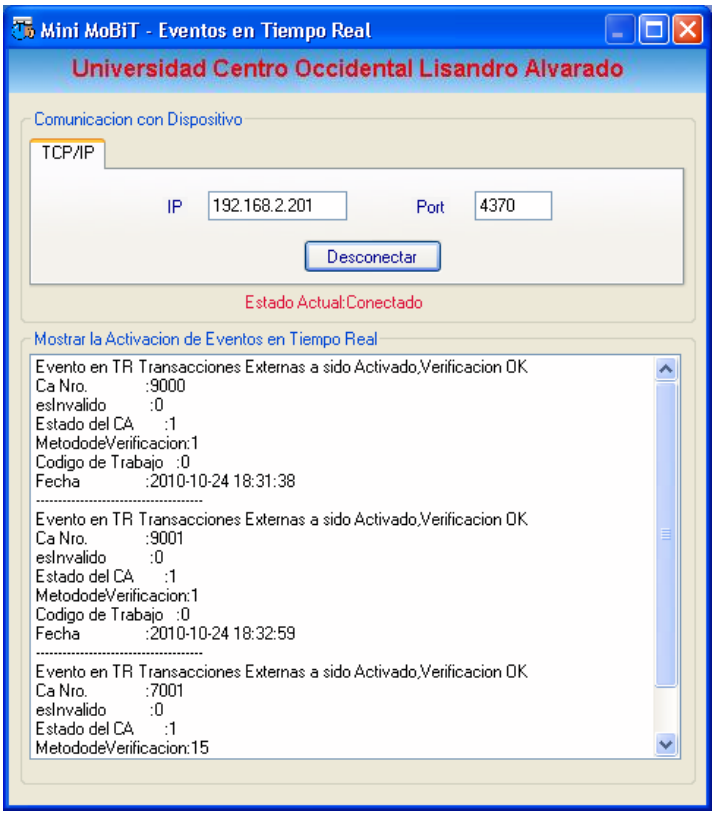


Figura 4.15 Interfase grafica de la aplicación propuesta - Monitor en tiempo real

El ejemplo anterior, mostró cómo podríamos interactuar fácilmente con un dispositivo biométrico siempre que el fabricante haya suministrado las DLLs para integrar su funcionabilidad en nuestra aplicación anfitriona. Aunque los ejemplos deliberadamente han sido escogidos para ser lo más sencillo posible a nuestros propósitos ilustrativos, los principios permanecen similares para funcionabilidades más sofisticadas. Siempre y cuando tengamos un SDK (el juego de desarrollo del software) conteniendo a los DLLs específicos del dispositivo que se desea utilizar, éste será un proceso relativamente fácil. Sin esta información las cosas naturalmente serian un poco más complicadas. Sin embargo, la inmensa mayoría de fabricantes de dispositivo tienen disponible un SDK para simplemente tales propósitos y con la introducción del BioAPI, los desarrolladores de aplicaciones pronto se familiarizarán con la funcionabilidad biométrica y se inclinarán por integrarla en sus propios programas. Hemos por tanto, encapsulado toda la especifica funcionabilidad requerida del dispositivo, dentro de módulos de código único, los cuales entonces puede se referido o llamado desde cualquier parte del programa. Esto efectivamente provee una capa de interfase entre la aplicación principal y la subrayada DLLs suministrada por el fabricante del dispositivo biométrico.

4.5 Conclusiones

Indudablemente hemos cubierto bastante terreno en lo que respecta al desarrollo de aplicaciones y naturalmente cada uno de los asuntos a los que se refirieron, aunque ciertamente merece más consideración que el espacio permitido dentro de este libro, pero el tiempo siempre parece estar escontra. Esperamos haber despertado cierto interés en el punto, además de haber suministrado al lector con algún material de reflexión en este contexto. Recapitulemos algunos de los puntos claves a fin de concluir esta sección.

En primer lugar, la importancia de cómo en realidad el usuario ve y siente el sistema no debería ser subestimado (en el caso del programa principal o anfitrión éste probablemente seria el usuario administrador del sistema). Algunos de los programas antiguos de vendedores biométricos provocaron críticas a este respecto, no porque hubo nada malo operativamente, sino porque a veces fueron no intuitivos y tontos en su ejecución. En estos tiempos, los usuarios están acostumbrados a ver aplicaciones bien presentadas para los requisitos de negocio /oficina de todos los días y esperarán lo mismo de su aplicación biométrica. En el caso de un administrador de sistemas para un sistema público grande, este individuo va a tener suficiente cosas en que pensar para además tener que estar preocupado buscando la forma de resolver algo con el programa, ya que no consigue la opción para ello. Por consiguiente necesitamos hacer las cosas tan fáciles e intuitivas como sea posible, mientras todavía el programa global es presentando en una manera atractiva. Si el administrador ama

el programa, se sentirá un poco más entusiasta acerca del concepto global y a su vez transmitirá esa misma sensación a aquellos que se registran o matriculan en el sistema. El entusiasmo es contagioso. Entonces, desafortunadamente, también lo es la frustración. En cuanto a esto se refiere, una aplicación anfitriona de alto rendimiento bien presentada e intuitiva debería ser nuestro objetivo.

Un elemento afín es la conectividad general y qué tan fácil es conseguir que el sistema este en plena marcha inicialmente. El usuario final no va a estar interesado en emprender operaciones complicadas en su estación de trabajo, simplemente para poner a correr su sistema. Tampoco estará muy contento si tiene que llamarlo a usted a cada momento y peor si es por cobrar, solo porque que no puede conseguir que el sistema trabaje correctamente. Naturalmente la profundidad de esta pregunta dependerá muchísimo del tamaño y tipo de sistema implementado, pero aun con una aplicación sencilla de bajo costo, como el usado en el ejemplo en este capítulo, necesitamos asegurar que el dispositivo biométrico y el servidor de aplicaciones estén simplemente conectados y que todo esté bien documentado. Si hay componentes de la red envueltos, quizás en un sistema de multilectores por ejemplo, entonces éstos también deberían ser metidos en la imagen global, con todo diseñado como una sola pieza y programado para interconectarse perfectamente la primera vez. No deberíamos asumir que la persona responsable para implementar el sistema, necesariamente tenga todos los conocimientos detallados de estos asuntos y por eso deberíamos asegurar que documentamos todo lo referente a la funcionabilidad correcta del sistema, aunque esto conlleve a cubrir artículos no directamente suministrados por el vendedor biométrico, pero para el cuál un cierto nivel de comprensión es requerido. Esta forma de diseño claro en arquitectura y conectividad también debería extenderse a un modelo lógico de localización de fallas bien documentada, que pueda ser fácil de seguir por la mayoría del soporte interno de tecnología de la información dentro de una organización típica. Los vendedores que le ponen atención a tales detalles, encontrarán que su inversión trae beneficios en términos de la satisfacción del cliente.

Esto nos trae a las preguntas de estabilidad del software y rendimiento general. A veces ocurren cosas dentro del ambiente operativo, ya sea globalmente o en la máquina anfitriona para el cual el desarrollador de la aplicación no siempre podrá predecir. Sin embargo, él puede asegurar que su aplicación tiene un detector de errores que reporta el código en las peores condiciones, proporcionándole al usuario información de la situación sin rodeos. Algunas de estas pueden ser emprendidas automáticamente por elementos dentro del motor de base de datos o en algún otro sitio, pero es una buena idea tener previsto lo peor, de manera que el usuario pueda generar algún tipo de acción, quizás en un intento final por resolver el problema, el cual le permita obtener una ruta de salida donde sea pertinente. También deberíamos asegurar que de existir un reset forzado o apagado brusco de la máquina anfitriona no necesita alguna reinicialización complicada de todo el sistema. Hablando de

desempeño, debería ser reconocido que las máquinas usadas dentro del ambiente de desarrollo no sean muy diferentes de las esperadas en el sitio donde la aplicación será utilizada. Esto es en particular el caso con relación a PCs de escritorio, donde el usuario final puede tener el deseo de utilizar hardware existente como PCs viejas. El desarrollador por consiguiente claramente debería especificar el nivel de hardware requerido para un desempeño aceptable, incluyendo tipo de procesador y velocidad, requerimientos de memoria, especificación del adaptador gráficos donde sea pertinente y cualquier metodología requerida para la red o protocolos. Además, si el rendimiento del sistema global es especificado, entonces debería estar claramente indicada con qué hardware estas especificaciones fueron derivadas. De nuevo, no asumamos nada, pero detallemos bien claro exactamente cómo funciona el sistema y que hardware es requerido para facilitar este deseable estado de cosas.

Una filosofía similar debería ser aplicada a asuntos relacionados con la red, aunque ésta es un área mucho más compleja, especialmente dentro de grandes organizaciones. Sin embargo, si la aplicación biométrica es diseñada para alojarse dentro de una estructura existente de la red y pasar información a través de ella, entonces debemos reflexionar acerca de cómo esto podría afectar la situación actual. ¿Tiene la red suficiente ancho de banda para acomodar la carga adicional que estaremos colocando en ella? Si estamos anticipando un número grandes de transacciones en contra de una base de datos central, ¿tiene nuestro servidor suficiente poder de procesamiento para manejar esto además de otros procesos que pueden estar en marcha? ¿Tienen nuestro almacenamiento de datos y procedimiento de respaldo suficiente capacidad para absorber el recargo? Aunque éstas son preguntas que sólo el usuario final puede contestar, ayudaría mucho si el integrador de sistemas o el vendedor le puede proveer de la información necesaria pertinente del sistema en estudio. Las personas que planean la capacidad de usuarios finales entonces pueden comenzar a hacer sus sumas y sacar de entre manos sugerencias consecuentemente.

Finalmente, habiendo desarrollado nuestra aplicación biométrica, deberíamos considerar un robusto y esmerado ejercicio de experimentación, antes de que lo llevemos a la etapa de implementación. Pudo haber corrido bastante bien dentro del ambiente de desarrollo, pero éste puede ser un ambiente relativamente protegido comparado con las condiciones en el sitio, especialmente dentro de un área pública. El desarrollador idealmente debería intentar duplicar tantos los peores escenarios como sea posible con el fin de comprender lo que se requiere para hacer que el sistema se caiga o falle. Sí, todos nosotros sabemos que en sí las pruebas cuestan dinero, pero también las fallas del sistema y la desilusión de los usuarios. Es mucho mejor invertir un poco de esfuerzo a fin de enviar un sistema robusto, que funcione como lo esperado en su primer día y continúe haciéndolo por mucho más tiempo.

Conclusiones Generales

Hemos considerado los orígenes del concepto biométrico en el mundo antiguo y cómo usar la idea de características anatómicas y conductuales para identificar a un individuo. También brevemente hemos hecho referencia a los desarrollos en el campo de la electrónica y cómo éstos han hecho posible la automatización de la verificación biométrica de la identidad, de una manera eficiente en base a costos y realidad. Incluso hemos dirigido la mirada hacia ciertas aplicaciones típicas de la biometría y por supuesto también hemos explorado diversas metodologías populares y sus características particulares.

Una pregunta que surge repetidamente cuándo se discute lo positivo y negativo de la biometría, es la aceptación del usuario. ¿**Hemos alcanzado en realidad el punto donde los ciudadanos ordinarios aceptarán el uso de la biometría** para los procesos en los cuales tienen una elección en participar o no? La respuesta es casi indudablemente **sí**, **siempre y cuando puedan ver un beneficio asociado para ellos mismos al hacer esto**. Éste es un punto, el cual a menudo es eludido por los directivos de las empresas practicantes en el campo de la biometría. Quizás demasiado énfasis, ha sido puesto en el potencial incrementó de la seguridad que la tecnología permite, sin considerar los alegatos de los usuario en suficiente profundidad. Pero ver a la biometría sólo en esta pelea, sería como ver la rueda como algo que es bueno para echarse a rodar por una colina. En ambos casos, **el verdadero potencial esta en que es una tecnología de apoyo a otros procesos**. En resumen, cada vez que salga a flote la cuestión del grado de aceptación del usuario, los vendedores e integradores de sistemas, deberían concentrarse un poco menos en proveerle beneficios al proceso organizativo y un poco mas en proveerle beneficios al usuario. Es poco realista suponer que los usuarios abrazarán un paradigma tecnológico, que a primera vista parece complicado y posiblemente un poco intrusivo, si es que no hay beneficios particulares para ellos al hacer eso. Esto tal vez podría ser beneficioso para el pago de beneficios sociales, control de fronteras, licencias de conducir y otras áreas oficiales donde el usuario no tiene alternativa, pero si tenemos el deseo de ver el uso de la tecnología biométrica aflorar mas allá de estas áreas, entonces necesitamos comenzar a ver el mundo desde la perspectiva del usuario y generar algún pensar innovador alrededor del suministro de beneficios tangibles que a su vez logren crear entusiasmo para usar la tecnología.

Otro obstáculo para la aceptación mas amplia de la biometría, ha sido la forma como la tecnología algunas veces a sido mostrada por algunos mas bien ambiciosos y si no cuestionables vendedores, en cuanto al desempeño de los equipos, mucho de los cuales no han sido simplemente realizados en condiciones operativas del mundo real. Aunque no todos los vendedores caen en esta categoría (ciertamente, algunos vendedores están particularmente abiertos en discutir el desempeño de sus equipos, realizar pruebas y estar muy informados acerca del tema), es un hecho desafortunado que eso sea así, tienden a generar una en particular percepción más bien negativa de la industria entre los usuarios finales, que han probado sus productos y encontrado deficiencias en ellos. Afortunadamente, en los últimos años esto ha sido reconocido y ahora vemos asociaciones de industrias y otros, ser más acuciosos en promover prácticas en el ensayo de metodologías y han publicado criterios de desempeño de sus equipos, mientras todavía aceptan el hecho de que las implementaciones en el mundo real, traen consigo un montón de variables que simplemente no pueden estar descritas o predichas en las pocas y a veces minúsculas especificaciones del producto, provistas por el fabricante del dispositivo y vendedores. Esta, de por si, no es necesariamente una falla de parte de los vendedores, quienes naturalmente desean mostrar sus productos a toda luces, pero si un reconocimiento de la dificultad en predecir el desempeño de equipos a través de situaciones múltiples de las cuales no tienen un conocimiento en particular. Este factor realmente debería ser tratado dentro de la literatura del producto y en anuncios publicitarios. Habiendo mencionado esto aquí, las mejoras en el desempeño de dispositivos biométricos y el incremento en la familiarización con su implementación, no dudamos que por todo esto contribuirá en hacer que sea un asunto menos a ser tratado en el futuro.

Esto no quiere decir que la biometría sea necesariamente la respuesta a todas nuestras plegarias, pero ella nos ofrece algunas herramientas útiles. Los departamentos de mercadeo en organizaciones que lidian con clientes y ciertamente, quizás en entidades del gobierno, en forma útil podrían considerar la posibilidad de proveer niveles más altos de funcionabilidad y automatización al usuario, como resultado de los niveles superiores de confianza en lo que se refiere a la identidad del usuario. Existen mil y una ideas en este contexto que saltan a la mente. La pregunta es cómo pueden todas esta personas ser fácilmente verificadas y finalmente implementados los procedimientos al respecto. Esto es precisamente el por qué se debe realizar un desarrollo aplicativo con **un plan piloto**. Todo esto es realmente factible hoy en día y se volverá aun más fácil con el pasar del tiempo, viendo la introducción de nuevos dispositivos y herramientas.

La importancia de cómo en realidad el usuario ve y siente el sistema no debería ser subestimado ya que en el pasado ciertos programas biométricos recibieron fuertes criticas al respecto, no porque hubo nada malo operativamente en ellos, sino porque a veces eran hechos en forma no intuitiva y un poco toscos en su ejecución. En los tiempos en que vivimos, los usuarios están acostumbrados a ver aplicaciones

bien presentadas y esperarán lo mismo de su aplicación biométrica. **Por consiguiente necesitamos hacer las cosas tan fáciles e intuitivas como sea posible**, mientras todavía el programa global es presentando en una forma atractiva. **El entusiasmo es contagioso pero, desafortunadamente, también lo es la frustración**. Por tanto, una aplicación anfitriona de alto rendimiento bien presentada e intuitiva debería ser nuestro objetivo al diseñar la aplicación biométrica principal.

En lo que respecta a la persona responsable de implementar y mantener el sistema, este debería documentar todo lo referente a la funcionabilidad correcta del sistema, así como la creación de manuales de localización de fallas bien documentadas, que pueda ser fácil de seguir por la mayoría de los técnico de soporte interno dentro de la organización. **Una cosa es segura**, el sistema no se instalará y manejará a sí mismo, y por eso necesitamos algún grado de planificación, experticia en la instalación y subsiguiente administración del sistema. **El esfuerzo y recursos que le asignemos a esto tendrán un impacto en el éxito inicial y la subsiguiente fácil ejecución del sistema en conjunto**. En lo referente al recurso humano necesario para la implantación del sistema biométrico en toda la organización, esto es mejor emprendido por la misma organización, quien después de todo estará usando y viviendo con el resultado final, para lo cual se podría designar un Administrador general del Programa, quien pueda unir a las diversas entidades y mantener la imagen completa de la estructura en cualquier momento. Hay diversas personas que necesitan interactuar con nuestro plan de proyecto, algunos de los cuales vienen realmente de disciplinas y con niveles de conocimientos diferentes. Si esto no está cuidadosamente planificado y orquestado entonces mucho tiempo podría ser desperdiciado en mal entendidos, conduciendo a una aproximación más bien fragmentada de la implementación. Esto es precisamente el porqué un Administrador general del Programa debería ser destinado a manejar el proyecto y resolver algunos asuntos que surjan allí adentro

En conclusión, la tecnología automatizada de la verificación e identificación biométrica, ha estado aproximadamente (al menos en una forma utilizable) por mas de dos décadas, con muchas interesantes especulaciones y predicciones hechas en lo que se refiere a la excelencia de la tecnología en situaciones de todos los días y la tasa de aceptación entre el público en general. Existe inevitablemente un periodo de racionalización a medida que mejores productos e ideas graviten hacia la superficie y se sitúen por si solo, a fin de proveer genuinamente beneficios útiles a los usuarios. Creemos que si hemos alcanzado ese punto en términos del grado de uso del producto y de una cierta cantidad de algoritmos disponibles de comparación de plantillas, pero la presentación del todo en términos de aplicaciones e interfaces con el usuario, necesitan un pequeño ajuste fino. Nos gustaría ver un poco más, que terceros se involucraran ya sea en forma de empresas productoras de software independientes o los mismos usuarios finales, a medida que esto indudablemente nos conduzca hacia el entendimiento común de donde esta tecnología puede genuinamente ser útil y por

qué. En lo que respecta a esto, es bien recibido la encapsulación de la funcionabilidad biométrica dentro de las herramientas de desarrollo (o ciertamente en los sistemas operativos) para proveer acceso mas extenso al desarrollo de ideas. Las iniciativas tales como las BioAPI son quizás un paso hacia ésta, con su intento digno de elogio en proveer una interfaz común. Aunque siempre existirá un lugar para el especialista integrador en sistemas biométricos, necesitamos ensanchar la actividad aplicativa del diseño, si hemos de ver un incremento rápido en la implementación biométrica en los años venideros.

BIBLIOGRAFIA

- Alejandra Noillet., http://www.monografias.com/trabajos11/crida/crida.shtml

- ASHBOURN, J. *Biométrica : Advanced Identity Verification. The Complete Guide.* Springer. 2000.

- MARCHETTE, D.J. *Computer Intrusion Detection and Network Monitoring. A Statistical Viewpoint.* Springler. 2001.

- Davide Maltoni, Dario Maio, Anil K Jain, Salil Prabhakar: Handbook of Fingerprint Recognition. Springer, 2003

- ATTALI, I. *Smart Card Programming and Security.* Springer. 2001.

- MIKE HENDRY. Smart Card Security and applications. 2001

- VARADHARAJAN, V. Y MU, Y. *Information Security Privacy*. Springler. 2001.

- PJ. Phillips et al., "The Feret Evaluation Methodology for Face Recognition Algorithms," NISTIR 6264, Nat'l Institute of Standards and Technology, 1998, http://www.itl.nist.gov/iaui/894.03/pubs.html#face.

- S. Rizvi, PJ. Phillips, and H. Moon, "The Feret Verification Testing Protocol for Face Recognition Algorithms, " NISTIR 6281, Nat'l Institute of Standards and Technology, 1998, http://www.itl.nist.gov/iaui/894.03/pubs.html#face.

- NIST Spoken Language Technology Evaluations, http://www.nist.gov/speech/test.htm.

- C.L. Wilson and R.M. McCabe, "Simple Test Procedurefor Image-based Biometric Verification Systems," NISTIR 6336, Nat'l Institute of Standards and Technology, 1999, http://www.itl.nist.gov/iaui/894.03/pubs.html #fing

- A.K. Jain et al., An Identity-Authentication System Using Fingerprints," *Proc. EuroSpeech 97,* IEEE CS Press, Los Alamitos, Calif, 1997, pp. 1,348-1,388. Electronics magazine.

- http://www.visioningenieria.com/soluciones.html
- http://www.trielo.com.br/ase_productos
- http://www.ast_afis.com.com/es/es-id4.html
- http://www.biometria.com.pe
- http://www.pyratech.hpg.ig.com.br//prmcipal.html
- http://www.ii.uam.es/~abie/docs/biotest.htm
- http://www2.vol.com.br/info/aberto/infonews/052002/20052002-22.shl
- http://www.homini.com/biometria.html
- http://www.homini.com/origen.htm
- http://www.ast_afis.com/biometria.html
- http://homepage.ntlworld.com/avanti/
- http://www.belt.com.es/noticias/02_abril/22_26/23_biometria.html
- http://www.embratel.com.br/internet.wks05/tecnologia/tegnologia
- http://www.iriscan.com/
- www.neotec.com.pa/ComoPorque
- www.neokoros.com
- www.biometrics.org
- www.ibia.org
- www.insys.com.mx/biometria/biometria
- http://www.nrtec.com.mx/biometria.htm
- http://www.e-printing.com.ar/noticias/2002/ene2002/15195679.htm
- http://www.ibia.org
- http://www.biometrics.org
- http://www.afb.org.uk
- http://homepage.ntlworld.com/avanti/
- http://stat.tamu.edu/Biometrics/

APENDICE