Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

DISEÑO DE UN SISTEMA DE PAGOS DE PLANILLA CON AUTENTICACIÓN BIOMÉTRICA EN ENTIDADES BANCARIAS

CARLOS EDUARDO CIFUENTES RAMOS

ASESORADO POR: ING. EDGAR SANTOS

GUATEMALA, AGOSTO DE 2005

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO DE UN SISTEMA DE PAGOS DE PLANILLA CON AUTENTICACIÓN BIOMÉTRICA EN ENTIDADES BANCARIAS

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

CARLOS EDUARDO CIFUENTES RAMOS
ASESORADO POR: ING. EDGAR SANTOS

AL CONFERÍRSELE EL TÍTULO DE
INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, AGOSTO DE 2005

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Vacante
VOCAL II	Lic. Amahán Sánchez Álvarez
VOCAL III	Ing. Julio David Galicia Celada
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Sydney Alexander Samuels Milson
EXAMINADOR	Inga. Virginia Tala
EXAMINADOR	Ing. Ricardo Moralez
EXAMINADOR	Ing. Edgar Santos
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

DISEÑO DE UN SISTEMA DE PAGOS DE PLANILLA CON AUTENTICACIÓN BIOMÉTRICA EN ENTIDADES BANCARIAS

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha 11 de febrero de 2004.

Carlos Eduardo Cifuentes Ramos

DEDICATORIA A:

Dios	A ti padre santo por darme la vida y sabiduría para concluir mi carrera a ti dedico este logro.
Mis Padres	Moisés Cifuentes y Juana Ramos, por todo el esfuerzo, comprensión, amor y dedicación que me han brindado y por los valores y principios que me inculcaron con su ejemplo, a ustedes en especial dedico este triunfo.
Mis Hermanos	Marisol Cifuentes,Eric Cifuentes, Hugo Cifuentes,Sandra Cifuentes por la amistad y el apoyo que siempre me han dado.
Mis Sobrinos	Daniel Campos, Miguel Campos, Yonny Campos, Cristian Campos, Jonathan Campos por todo el amor que me han regalado.

Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala junio de 2005

Ingeniero Carlos Azurdia
Coordinador del Área de Trabajos de Graduación
Escuela de Ciencias y Sistemas

Ingeniero Azurdia:

Por este medio me permito informarles que he procedido a revisar el trabajo de graduación titulado "**DISEÑO DE UN SISTEMA DE PAGOS DE PLANILLA CON AUTENTICACION BIOMETRICA EN ENTIDADES BANCARIAS**", elaborado por el estudiante **CARLOS EDUARDO CIFUENTES RAMOS** y de acuerdo a mi criterio el mismo se encuentra concluido y cumple con los objetivos propuestos para su desarrollo.

Sin otro particular me suscribo de ustedes,

Atentamente,

Ing. Edgar Santos
No De Colegiado: 5266

Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala 17 de febrero de 2005

Ingeniero
Luis Alberto Vettorazzi España
Coordinador de la Carrera de Ingeniería en
Ciencias y Sistemas

Respetable Ingeniero Vettorazzi:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **CARLOS EDUARDO CIFUENTES RAMOS**, titulado: "**DISEÑO DE UN SISTEMA DE PAGOS DE PLANILLA CON AUTENTICACION BIOMETRICA EN ENTIDADES BANCARIAS**",, y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme.

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados y
Revisor

Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

El coordinador de la carrera de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, al trabajo de graduación titulado: Diseño de un sistema de pagos de planilla con autenticación biométrica en entidades bancarias, presentado por el estudiante universitario Carlos Eduardo Cifuentes Ramos, aprueba el presente trabajo y solicita la autorización del mismo.

Ing. Jorge Armin Mazariegos Rabanales
Director
Ingeniería en Ciencias y Sistemas

Guatemala, Agosto de 2005

1. ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

Figuras

Tablas

GLOSARIO

Biométria: Conjunto de técnicas y procedimientos utilizados para medir una característica física de una persona y compararla con una representación de tal característica almacenada previamente

Commit: Graba una transacción en la base de datos.

Copiba: Control de pagos de planilla para instituciones bancarias.

Enrollment: Inscripción de las personas en el dispositivo biométrico.

Far: Tasa de falsa aceptación (False Acceptance Rate).

Frr: (False Rejection Rate) Tasa de falso rechazo.

Hacker: Intruso cibernético, que busca entrar a los sistemas, sin contar con autorización.

Huella Dactilar: Representación de la morfología superficial de la epidermis de un dedo.

Iriscode: Representación matemática de los patrones obtenidos a partir del iris del ojo humano.

Minucias: Los dedos poseen un conjunto de líneas que, en forma global, aparecen dispuestas en forma paralela. Sin embargo, estas líneas se intersectan y a veces terminan en forma abrupta. Las minucias son los puntos donde éstas terminan o se bifurcan

Pin: (Personal Identificación Number) Número de Identificación Personal.

Template Es el conjunto de características biiometricas, que será almacenado en una base de datos central u otro medio como una tarjeta magnética.

Toolbar: Barra de botones .

Rollback: Reversar una transacción ejecutada en la base de datos.

OBJETIVOS

General

- Diseño de un sistema de pagos de planilla con autenticación biométrica para instituciones bancarias que nos permita realizar pagos de forma confiable, segura y rápida.

Específicos

1. Diseño de una aplicación gráfica para el pago seguro de planillas.

2. Diseñar un sistema de pagos que sea fácil y rápido y que evite las Colas en las ventanillas.

3. Diseño de un sistema que sea fácil y rápido en la transferencia de la Información en cada una de las agencias de la entidad bancaria.

2. INTRODUCCIÓN

El Sistema de Pagos de Planilla utilizando autenticación Biométrica es el método más seguro que existe en el medio de la identificación personal, ya que utiliza las características del ser humano como lo son las huellas digitales, que es difícil o imposible que dos personas tengan las mismas características en las huellas dactilares: en estos tiempos en que la seguridad informática es cada vez más importante, este sistema ayudará a que no hallan falsificaciones en la identificación de las personas: he ahí lo importante de la autenticación biométrica.

El sistema ayudará al receptor-pagador de una forma segura y rápida a identificar a las personas que vayan a realizar una transacción en el banco, en este caso el cobro de planilla. Con anterioridad, la persona ha registrado dos huellas de los dedos de las manos, esto se hace por si se tuviera algún problema en alguna de sus huellas, se tiene otra para poder identificarlos, estas huellas se guardarán en la base de datos de la central del banco: el proceso de registrar la huella digital dura aproximadamente de 10 a 15 minutos por persona, pues se trata de seleccionar la mejor huella dactilar. Teniendo los datos personales, información de pago, fotografías y las huellas dactilares, se forma una base de datos que nos permitirá identificar a cada una de las personas..

Las personas pasan a las ventanillas de pago colocando uno de sus dedos en el dispositivo biométrico, éste procede a identificarlo positiva o negativamente, luego el dispositivo biométrico se comunica con la computadora

mediante una conexión serial: también existirá una aplicación gráfica que monitoreará los resultados obtenidos por el dispositivo biométrico si la identificación es positiva la aplicación tomará el código de la huella que se identificó y buscar en la base de datos obteniendo de allí sus características personales, total a pagar, así como su fotografía, estos datos son presentados al receptor pagador, luego es impreso el recibo correspondiente de pago, la persona firma este recibo y le queda al receptor como constancia del pago realizado.

Si el resultado de la identificación es negativo, la aplicación le muestra al receptor pagador un mensaje de identificación negativa. Con este método rápido seguro y novedoso de pagos se garantizará que la persona que va cobrar es la persona a la que se le tiene que pagar, también el sistema reducirá las colas en las ventanillas.

Las fotografías, huellas dactilares, datos personales y la información del pago serán enviados de la central del banco donde se encuentran almacenadas, a las sucursales donde se harán efectivos los pagos de planilla.

Las fotografías almacenadas de los empleados deben tener un promedio de 12 kb. y el contenido de las huellas dactilares debe de ser de 1 kb. con estos tamaños garantizamos la resolución de las fotografías y huellas dactilares, también nos permitirá con facilidad y rapidez enviar toda la información a las diferentes agencias de la institución bancaria que las requieran.

1. GENERALIDADES DE LA BIOMETRÍA

1.1. Definición de Autenticación

La autenticación es el proceso que permite el reconocimiento de una persona mediante una prueba de identidad, ésta puede ser un documento físico, como un carné o utilizar la huella digital en sistemas biométricos.

Se emplea sistemas de autenticación en la mayoría de las actividades diarias de negocios. En las transacciones relacionadas con información personal o financiera, se debe mostrar una prueba de identidad. Por ejemplo, cuando deseamos cambiar un cheque en un banco, el cajero nos pide primero que le mostremos un documento de identidad antes de entregarnos el valor del cheque.

1.1 1.2. Formas de Autenticación

Por supuesto, las distintas formas de autenticación deben ser únicas, capaces de distinguir a la persona de entre las demás.

- Las firmas escritas son las más usuales aunque hay falsificadores expertos en la copia de firmas.
- Los nombres y claves de acceso a sistemas informáticos pueden ser obtenidos casi fácilmente por otros usuarios gracias a la utilización de tecnologías como analizadores de red, funciones especiales en la implementación de las tarjetas de red, etc.

- El escaneo de huellas digitales.

Con todo esto queda de manifiesto que es muy difícil asegurar la veracidad de la identidad de las personas. Para ello lo que se hace es complicar el sistema de autenticación, para hacer más difícil a los que intentan hacerse pasar por quienes no son el acceso a los lugares privados o personales.

1.3. Métodos de autenticación de usuario

El objetivo de la autenticación de usuario es permitirle a una persona autorizada el acceso a un recurso físico, telemático o informático, previa verificación de que cumple con las condiciones exigidas para dicho acceso.

Los métodos de autenticación de usuario que existen hoy en día son muy variados. Una forma de clasificarlos es de acuerdo a su relación con el usuario y estos pueden ser:

- Aquellos que se basan en datos conocidos por el usuario,
- Los que requieren que el usuario lleve un dispositivo,
- Y finalmente los métodos biométricos que se basan en rasgos físicos o en patrones de comportamiento del usuario.

1.3.1. Datos conocidos por el usuario

En esta categoría están las contraseñas usadas para el acceso a recursos informáticos, generalmente con un nombre de usuario asociado, y los PINs o NIPs (Número de Identificación Personal) para acceso a transacciones bancarias.

1.3.2. Dispositivos

Los dispositivos incluyen las tarjetas plásticas de banda magnética, las tarjetas inteligentes y los tokens o módulos de seguridad, entre otros. Proporcionan una mayor seguridad que el método anterior, pero siempre y cuando sea el usuario autorizado quien las tenga en su poder.

1.3.3. Sistemas Biométricos

Los métodos anteriores verifican si un usuario está o no autorizado para tener acceso a un recurso pero no nos dicen nada relacionado con su identidad. Los métodos biométricos verifican la identidad del usuario, y con base en esta identificación proporcionan acceso a los recursos autorizados para ese usuario en particular. Podemos dividir los métodos biométricos en:

- Los que se basan en rasgos físicos del usuario según tabla 1.
- Y aquellos basados en patrones de comportamiento del usuario según tabla 1.

Tabla I. Métodos biométricos

Rasgos físicos	Escaneo de retina Reconocimiento de huella digital Reconocimiento de iris Reconocimiento de la cara Geometría de la mano Patrón de venas Análisis de DNA
Comportamiento	Análisis de firma Reconocimiento de voz Ritmo de uso del teclado

El escaneo de retina es de los métodos biométricos más antiguos. Se originó en investigaciones realizadas en los años 30. Hoy en día no es muy usado debido a que muchos consideran que es invasivo y que viola la privacidad: el usuario se debe situar el ojo a uno o dos centímetros del escáner y mirar una luz verde mientras se lee el patrón de vasos sanguíneos del fondo de su ojo. Además de lo molesto del procedimiento, este escaneo puede revelar datos adicionales a la identidad, como por ejemplo la existencia de un embarazo.

De los demás métodos, el sistema de reconocimiento de huellas digitales es el más popular en la actualidad, y le sigue el de reconocimiento de iris. Ambos métodos ofrecen un alto grado de seguridad.

Es posible que el análisis de DNA se use ampliamente en un futuro como método de autenticación, aunque hoy en día se emplea principalmente para investigaciones forenses y pruebas de paternidad.

Entre los métodos basados en patrones de comportamiento del usuario, el reconocimiento de voz es por ahora el menos confiable. El método de reconocimiento de firma no solo analiza la firma como tal sino la presión empleada en cada trazo de la misma. Los métodos biométricos tienden a generalizarse, usados en combinación con otros métodos de autenticación.

1.3.3.1. Dispositivos biométricos

Los dispositivos biométricos tienen tres partes principales:

- Por un lado, disponen de un mecanismo automático que lee y captura una imagen digital o analógica de la característica a analizar.

- Además disponen de una entidad para manejar aspectos como la compresión, almacenamiento o comparación de los datos capturados con los guardados en una base de datos (que son considerados válidos).
- Y también ofrecen una interfaz para las aplicaciones que los utilizan.

El proceso general de autenticación sigue unos pasos comunes a todos los modelos de autenticación biométrica: captura o lectura de los datos que el usuario a validar presenta, extracción de ciertas características de la muestra (por ejemplo, las minucias de una huella dactilar), comparación de tales características con las guardadas en una base de datos, y decisión de si el usuario es válido o no.

Es en esta decisión donde principalmente entran en juego las dos características básicas de la fiabilidad de todo sistema biométrico (en general, de todo sistema de autenticación): las tasas de falso rechazo y de falsa aceptación. Por tasa de falso rechazo (False Rejection Rate, FRR) se entiende la probabilidad de que el sistema de autenticación rechace a un usuario legítimo porque no es capaz de identificarlo correctamente, y por tasa de falsa aceptación (False Acceptance Rate, FAR) la probabilidad de que el sistema autentique correctamente a un usuario ilegítimo; evidentemente, una FRR alta provoca descontento entre los usuarios del sistema, pero una FAR elevada genera un grave problema de seguridad: estamos proporcionando acceso a un recurso a personal no autorizado a acceder a él.

1.4. Utilidad de la biometría

En lugar de utilizar una contraseña como forma de identificarse, ¿por qué no utilizar una característica física como la voz, la cara o la huella digital? Estas medidas corporales, conocidas como biometría, tienen la ventaja:

- No pueden ser extraviadas, olvidadas o traspasadas de una persona a otra,
- Son sumamente difícil falsificarlas.

Sin embargo, la tecnología biométrica debe todavía enfrentar algunos desafíos técnicos considerables como:

- El hardware es costoso,
- Los diferentes sistemas son incompatibles entre sí
- Y la tecnología se encuentra en pleno proceso de maduración.

Conforme las computadoras se vuelven parte del tejido de la vida cotidiana y más transacciones -desde firmas de contratos a compras- se realizan digitalmente, las firmas especializadas en biometría piensan que sus productos pronto serán indispensables.

Los sistemas modernos de biometría por computadora se emplean para dos funciones básicas:

- La primera es la identificación ('¿quién es esta persona?'), en la que la identidad de un sujeto es determinada comparando su medida biométrica con una base de datos de registros almacenados.
- La segunda es la verificación (¿es esta persona quien afirma ser?), que efectúa una comparación de una medida biométrica con otra que sabe que proviene de una persona en particular.

Una cartilla en un reciente FBI Law Enforcement Bulletin, de acuerdo con el artículo, las huellas digitales son lo mejor para aplicaciones en las que hay una gran cantidad de usuarios. Las iris pueden igualar o exceder la precisión de las huellas digitales, pero "el número limitado de vendedores y la carencia de precedentes de reconocimiento a través del iris no los hacen tan atractivos". La geometría de la mano ha dado buenos resultados en las prisiones. El reconocimiento facial puede identificar a las personas "discretamente y sin su cooperación". El reconocimiento por la voz es menos preciso, pero podría ser lo mejor para identificar a alguien en el teléfono.

Los lectores biométricos utilizados por el Software Puntual son el HandKey y el HandPunch, para el Software de control de Acceso Handnet for Windows son los Handkey, Ambos equipos son fabricados desde 1986 por la empresa norteamericana **Recognition Systems**, y fueron introducidos en el mercado mexicano en 1990 por DICSA, A la fecha existen más de 1,700 unidades instaladas a lo largo y ancho del país en empresas e Instituciones de todos los tamaños cubriendo aplicaciones de Control de Puntualidad y Asistencia, Acceso, Firma Digital, Acceso a Comedores, Etc....

Estos equipos están basados en el reconocimiento tridimensional de la mano, largo, ancho y espesor, son algunas de las más de 90 medidas que toman en cuenta para conformar la identidad biométrica de la persona. Esta tecnología es la más utilizada mundialmente, siendo líder del mercado con una participación del 36% según la publicación inglesa Biometric Technology Today.

1.5. Características de un indicador biométrico

Un indicador biométrico es alguna característica con la cual se puede realizar biometría. Cualquier indicador debe cumplir los siguientes requisitos:

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

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

1.6. Características de un sistema biométrico para identificación personal

Las características básicas que debe tener un sistema biométrico para identificación personal es cumplir con expresarse mediante las restricciones que deben ser satisfechas. Ellas apuntan, básicamente, a la obtención de un sistema biométrico con utilidad práctica. Las restricciones antes señaladas apuntan a que el sistema considere:

1.6.1. El desempeño

Se refiere a la exactitud, la rapidez y la robustez alcanzada en la identificación, además de los recursos invertidos y el efecto de factores ambientales y operacionales. El objetivo de esta restricción es comprobar si el sistema posee una exactitud y rapidez aceptable con un requerimiento de recursos razonable.

1.6.2. La aceptabilidad

Está indica el grado en que la gente está dispuesta aceptar un sistema biométrico en su vida diaria. Es claro que el sistema no debe representar peligro alguno para los usuarios y debe inspirar "confianza" a los mismos. Factores psicológicos pueden afectar esta última característica. Por ejemplo, el reconocimiento de una retina, que requiere un contacto cercano de la persona con el dispositivo de reconocimiento, puede desconcertar a ciertos individuos debido al hecho de tener su ojo sin protección frente a un "aparato".

Sin embargo, las características anteriores están subordinadas a la aplicación específica. En efecto, para algunas aplicaciones el efecto psicológico de utilizar un sistema basado en el reconocimiento de características oculares será positivo, debido a que este método es eficaz implicando mayor seguridad.

1.6.3. La fiabilidad

Que refleja cuán difícil es burlar al sistema. El sistema biométrico debe reconocer características de una persona viva, pues es posible crear dedos de látex, grabaciones digitales de voz prótesis de ojos, etc. Algunos sistemas incorporan métodos para determinar si la característica bajo estudio corresponde o no a la de una persona viva. Los métodos empleados

son ingeniosos y usualmente más simples de lo que uno podría imaginar. Por ejemplo, un sistema basado en el reconocimiento del iris revisa patrones característicos en las manchas de éste, un sistema infrarrojo para chequear las venas de la mano detecta flujos de sangre caliente y lectores de ultrasonido para huellas dactilares revisan estructuras subcutáneas de los dedos.

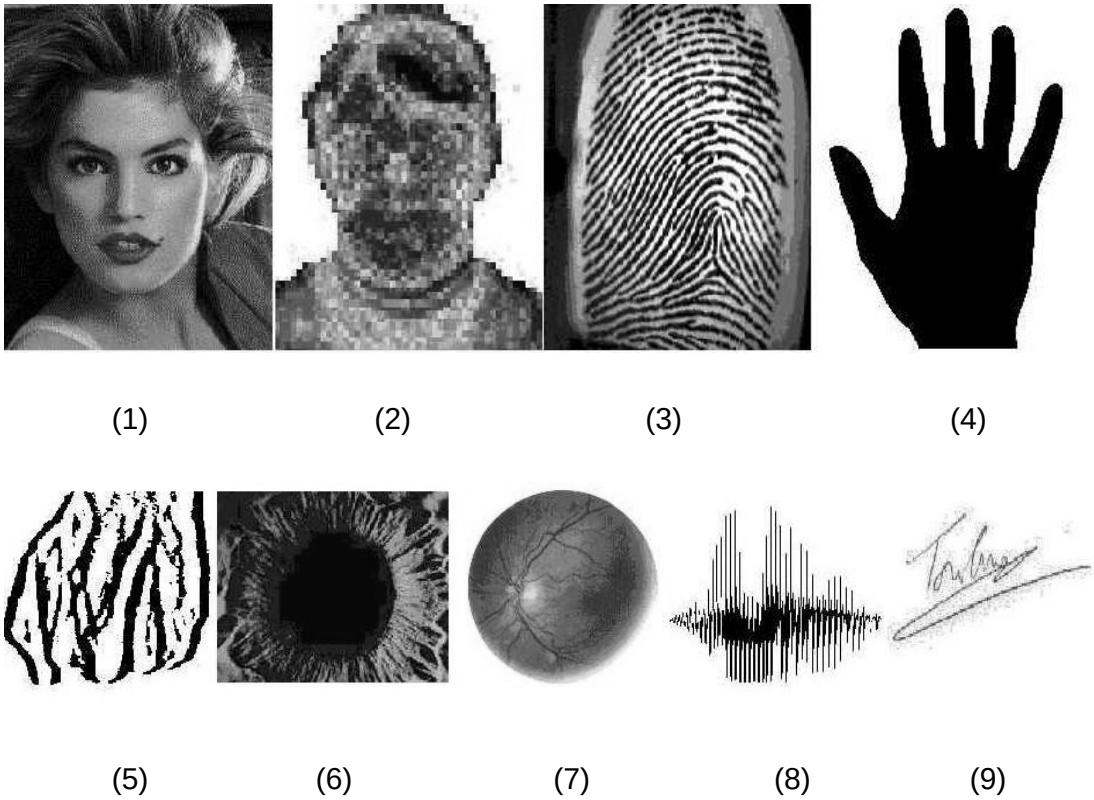
2.1.1. 2. TIPOS DE BIOMETRÍA

2.1. Introducción

En la actualidad existen sistemas biométricos que basan su acción en el reconocimiento de diversas características, como puede apreciarse en la figura 2.1. Las técnicas biométricas más conocidas son nueve y están basadas en los siguientes indicadores biométricos:

1. Rostro,
2. Termograma del rostro,
3. Huellas dactilares,
4. Geometría de la mano,
5. Venas de las manos,
6. Iris,
7. Patrones de la retina,
8. Voz,
9. Firma.

Figura 1: Técnicas biométricas actuales (1) Rostro, (2) Termografía Facial, (3) Huella dactilar, (4) Geometría de la Mano,(5) Venas de la mano (6) Iris, (7) Patrones de la retina, (8) Voz e (9) Firma.



(1) (2) (3) (4)

(5) (6) (7) (8) (9)

2.2. Reconocimiento del Rostro

Una técnica controvertida; desde el punto de vista del usuario es atractiva pero presenta muchas dificultades prácticas, tales como reconocer una cara dentro de un grupo, algo diferente a realizar el contraste entre dos imágenes. Resueltos los inconvenientes técnicos es evidentemente una tecnología de auspicioso futuro.

Esta tecnología que ha ganado terreno en los últimos años gracias a la baja de los precios de las computadoras. Funciona analizando la imagen en video o una fotografía e identificando las posiciones de varias decenas de nodos en el rostro de una persona. Estos nodos, en su mayoría entre la frente y el labio superior, no se ven afectados por la expresión o la presencia de vello facial. A diferencia de otras biometrías, ésta puede operar de manera pasiva, es decir, sin que la persona se dé cuenta de que está siendo analizada.

2.3. Verificación de patrones oculares

Los modelos de autenticación biométrica basados en patrones oculares se dividen en dos tecnologías diferentes:

- Los que analizan patrones retínales,
- Y los que analizan el iris.

Estos métodos se suelen considerar los más efectivos: para una población de 200 millones de potenciales usuarios la probabilidad de coincidencia es casi cero, y además una vez muerto el individuo los tejidos oculares se degeneran rápidamente, lo que dificulta la falsa aceptación de atacantes que puedan robar este órgano de un cadáver.

La principal desventaja de los métodos basados en el análisis de patrones oculares es su escasa aceptación; el hecho de mirar a través de un binocular (o monocular), necesario en ambos modelos, no es cómodo para los usuarios, ni aceptable para muchos de ellos: por un lado, los usuarios no se fían de un haz de rayos analizando su ojo, y por otro un examen de este órgano puede revelar enfermedades o características médicas que a muchas personas les puede interesar mantener en secreto, como el consumo de alcohol o de ciertas drogas. Aunque los fabricantes de

dispositivos lectores aseguran que sólo se analiza el ojo para obtener patrones relacionados con la autenticación, y en ningún caso se viola la privacidad de los usuarios, mucha gente no cree esta postura oficial.

Por si esto fuera poco, se trata de sistemas demasiado caros para la mayoría de organizaciones, y el proceso de autenticación no es todo lo rápido que debiera en poblaciones de usuarios elevadas. De esta forma, su uso se ve reducido casi sólo a la identificación en sistemas de alta seguridad, como el control de acceso a instalaciones militares.

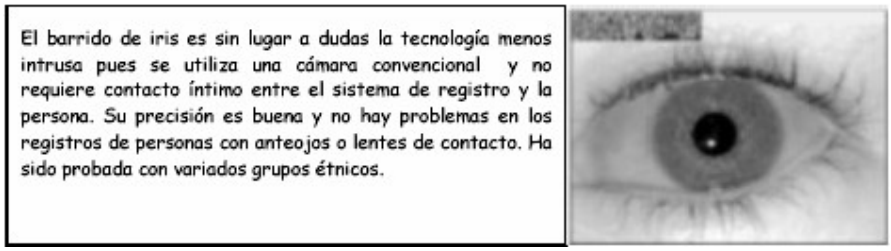
2.4. Barrido de la Retina

La vasculatura retinal (forma de los vasos sanguíneos de la retina humana) es un elemento característico de cada individuo, por lo que numerosos estudios en el campo de la autenticación de usuarios se basan en el reconocimiento de esta vasculatura como se puede apreciar en la figura 2.2 .

En los sistemas de autenticación basados en patrones retínales el usuario a identificar ha de mirar a través de unos binoculares, ajustar la distancia ínter ocular y el movimiento de la cabeza, mirar a un punto determinado y por último pulsar un botón para indicar al dispositivo que se encuentra listo para el análisis. En ese momento se escanea la retina con una radiación infrarroja de baja intensidad en forma de espiral, detectando los nodos y ramas del área retinal para compararlos con los almacenados en una base de datos; si la muestra coincide con la almacenada para el usuario que el individuo dice ser, se permite el acceso.

La compañía EyeDentify posee la patente mundial para analizadores de vasculatura retinal, por lo que es la principal desarrolladora de esta tecnología.

Figura 2: Barrido de iris



El iris humano (el anillo que rodea la pupila, que a simple vista diferencia el color de ojos de cada persona) es igual que la vasculatura retinal una estructura única por individuo que forma un sistema muy complejo, inalterable durante toda la vida de la persona. El uso por parte de un atacante de órganos replicados o simulados para conseguir una falsa aceptación es casi imposible con análisis infrarrojo, capaz de detectar con una alta probabilidad si el iris es natural o no.

La identificación basada en el reconocimiento de iris es más moderna que la basada en patrones retínales; desde hace unos años el iris humano se viene utilizando para la autenticación de usuarios. Para ello, se captura una imagen del iris en blanco y negro, en un entorno correctamente iluminado; esta imagen se somete a deformaciones pupilares (el tamaño de la pupila varía enormemente en función de factores externos, como la luz) y de ella se extraen patrones, que a su vez son sometidos a transformaciones matemáticas hasta obtener una cantidad de datos (típicamente 256 KBytes) suficiente para los propósitos de autenticación.

La muestra, denominada iriscode (en la figura se muestra una imagen de un iris humano con su iriscode asociado) es comparada con otra tomada con anterioridad y almacenada en la base de datos del sistema, de forma que si ambas coinciden el usuario se considera autenticado con éxito; la probabilidad de una falsa aceptación es la menor de todos los modelos biométricos .

También existe el sistema de **escáner ocular**. Examinando las fibras, surcos y pecas del iris (la parte coloreada del ojo) por medio de una cámara de video a un brazo de distancia del ojo se obtiene suficiente información para identificar a alguien. No obstante, si bien es considerada como la tecnología más confiable de todas, ésta resulta relativamente costosa.

El escáner del iris que suministra IriScan, compañía con sede en Marlton, Nueva Jersey; principal desarrolladora de tecnología (y de investigaciones) basada en reconocimiento de iris que existe actualmente, ya que posee la patente sobre esta tecnología, está siendo utilizado en más de 20 cárceles de EEUU para identificar a los prisioneros, el personal y los visitantes; asimismo, está siendo probado por bancos de Gran Bretaña, Japón y Estados Unidos para identificar a los usuarios de los cajeros automáticos.

Todas estas medidas para identificar a las personas tienen un objetivo: ofrecer mayor seguridad en vista de los niveles de fraude y falsificaciones.

2.5. Verificación por Voz

En los sistemas de reconocimiento de voz no se intenta, reconocer lo que el usuario dice, sino identificar una serie de sonidos y sus características para decidir si el usuario es quien dice ser. Para autenticar a un usuario utilizando un reconocedor de voz se debe disponer de ciertas condiciones para el correcto registro de los datos, como ausencia de ruidos, ecos; idealmente, estas condiciones han de ser las mismas siempre que se necesite la autenticación.

Cuando un usuario desea acceder al sistema pronunciará unas frases en las cuales reside gran parte de la seguridad del protocolo; en algunos modelos, los denominados de texto dependiente, el sistema tiene almacenadas un conjunto muy limitado de frases que es capaz de reconocer: por ejemplo, imaginemos que el usuario se limita a pronunciar su nombre, de forma que el reconocedor lo entienda y lo autentique.

Estos modelos proporcionan poca seguridad en comparación con los de texto independiente, donde el sistema va “proponiendo”' a la persona la pronunciación de ciertas palabras extraídas de un conjunto bastante grande. De cualquier forma, sea cual sea el modelo, lo habitual es que las frases o palabras sean características para maximizar la cantidad de datos que se pueden analizar (por ejemplo, frases con una cierta entonación, pronunciación de los diptongos, palabras con muchas vocales...). Conforme va hablando el usuario, el sistema registra toda la información que le es útil; cuando termina la frase, ya ha de estar en disposición de facilitar o denegar el acceso, en función de la información analizada y contrastada con la de la base de datos.

El principal problema del reconocimiento de voz es la inmunidad frente a replay attacks, un modelo de ataques de simulación en los que un atacante reproduce (por ejemplo, por medio de un magnetófono) las frases o palabras que el usuario legítimo pronuncia para acceder al sistema.

Este problema es especialmente grave en los sistemas que se basan en textos preestablecidos: volviendo al ejemplo anterior, el del nombre de cada usuario, un atacante no tendría más que grabar a una persona que pronuncia su nombre ante el autentificador y luego reproducir ese sonido para conseguir el acceso; casi la única solución consiste en utilizar otro sistema de autenticación junto al reconocimiento de voz. Por contra, en modelos de texto independiente, más interactivos, este ataque no es tan sencillo porque la autenticación se produce realmente por una especie de desafío-respuesta entre el usuario y la máquina, de forma que la cantidad de texto grabado habría de ser mucho mayor - y la velocidad para localizar la parte del texto que el sistema propone habría de ser elevada.

Otro grave problema de los sistemas basados en reconocimiento de voz es el tiempo que el usuario emplea hablando delante del analizador, al que se añade el que éste necesita para extraer la información y contrastarla con la de su base de datos; aunque actualmente en la mayoría de sistemas basta con una sola frase, es habitual que el usuario se vea obligado a repetirla porque el sistema le deniega el acceso (una simple congestión hace variar el tono de voz, aunque sea levemente, y el sistema no es capaz de decidir si el acceso ha de ser autorizado o no; incluso el estado anímico de una persona varía su timbre.

A su favor, el reconocimiento de voz posee la cualidad de una excelente acogida entre los usuarios, siempre y cuando su funcionamiento sea correcto y éstos no se vean obligados a repetir lo mismo varias veces, o se les niegue un acceso porque no se les reconoce correctamente.

Durante los últimos dos años, el mercado de reconocimiento de voz se ha reducido a favor del mercado del reconocimiento facial.

2.6. Verificación de firma

La verificación de firma goza de una aceptación que las otras técnicas no tienen. Es suficientemente preciso y su uso es especialmente adecuado a aplicaciones en las que la firma es un identificador aceptado. Curiosamente no se ha desarrollado lo que debiera.

Aunque la escritura (generalmente la firma) no es una característica estrictamente biométrica, de la misma forma que sucedía en la verificación de la voz, el objetivo aquí no es interpretar o entender lo que el usuario escribe en el lector, sino autenticarlo basándose en ciertos rasgos tanto de la firma como de su características.

La verificación en base a firmas es algo que todos utilizamos y aceptamos día a día en documentos o cheques; no obstante, existe una diferencia fundamental entre el uso de las firmas que hacemos en nuestra vida cotidiana y los sistemas biométricos; mientras que habitualmente la verificación de la firma consiste en un simple análisis visual sobre una impresión en papel, estática, en los sistemas automáticos no es posible autenticar usuarios en base a la representación de los trazos de su firma. En los modelos biométricos se utiliza además la forma de firmar, las

características dinámicas (por eso se les suele denominar Dynamic Signature Verification, DSV): el tiempo utilizado para escribir, las veces que se separa el bolígrafo del papel, el ángulo con que se realiza cada trazo, etc.

Para utilizar un sistema de autenticación basado en firmas se solicita en primer lugar a los futuros usuarios un número determinado de firmas ejemplo, de las cuales el sistema extrae y almacena ciertas características; esta etapa se denomina de aprendizaje, y el principal obstáculo a su correcta ejecución son los usuarios que no suelen firmar uniformemente. Contra este problema la única solución (aparte de una concienciación de tales usuarios) es relajar las restricciones del sistema a la hora de aprender firmas, con lo que se disminuye su seguridad.

Una vez que el sistema conoce las firmas de sus usuarios, cuando estos desean acceder a él se les solicita tal firma, con un número limitado de intentos (generalmente más que los sistemas que autentican mediante contraseñas, ya que la firma puede variar en un individuo por múltiples factores). La firma introducida es capturada por un lápiz óptico o por una lectora sensible (o por ambos), y el acceso al sistema se produce una vez que el usuario ha introducido una firma que el verificador es capaz de distinguir como auténtica.

2.7. Huellas Digitales

Las huellas digitales son la biometría más ampliamente utilizada. Los sistemas electrónicos modernos convierten los arcos, rizos y espirales en códigos numéricos, los cuales pueden ser comparados con una base de datos en unos cuantos segundos con un extraordinario grado de exactitud.

Las huellas tienen la ventaja de ser más baratas y sencillas que otras biometrías y ya representan 40% del mercado. El escáner de los dedos está llamado a convertirse en la opción biométrica para que las personas se incorporen a las redes corporativas.

Las compañías tecnológicas afirman que una gran proporción de las llamadas a los departamentos de soporte en solicitud de ayuda se deben al olvido de las contraseñas, razón por la cual están apoyando el uso del escáner de dedos para reducir los costos por servicio de soporte. El nuevo escáner de dedos que Polaroid lanzó al mercado en mayo (2001) cuesta cerca de 50 dólares y está siendo instalado en los teclados de algunas nuevas PC.

Típicamente la huella dactilar de un individuo ha sido un patrón bastante bueno para determinar su identidad de forma inequívoca, ya que está aceptado que dos dedos nunca poseen huellas similares.Ni siquiera entre gemelos o entre dedos de la misma persona. Por tanto, parece obvio que las huellas se convertirían antes o después en un modelo de autenticación biométrico: desde el siglo pasado hasta nuestros días se vienen realizando con éxito clasificaciones sistemáticas de huellas dactilares en entornos policiales, y el uso de estos patrones fué uno de los primeros en establecerse como modelo de autenticación biométrica.

Cuando un usuario desea autenticarse ante el sistema sitúa su dedo en un área determinada (área de lectura, no se necesita en ningún momento una impresión en tinta). Aquí se toma una imagen que posteriormente se normaliza mediante un sistema de finos espejos para corregir ángulos, y es de esta imagen normalizada de la que el sistema extrae las minucias (ciertos arcos, rizos y espirales de la huella) que va a comparar contra las que tiene

en su base de datos; es importante resaltar que lo que el sistema es capaz de analizar no es la huella en sí sino que son estas minucias, concretamente la posición relativa de cada una de ellas. Está demostrado que dos dedos nunca pueden poseer más de ocho minucias comunes, y cada uno tiene al menos 30 o 40 de éstas. Si la comparación de las posiciones relativas de las minucias leídas con las almacenadas en la base de datos es correcta, se permite el acceso al usuario, denegándosele obviamente en caso contrario.

Los sistemas basados en reconocimiento de huellas son relativamente baratos (en comparación con otros biométricos, como los basados en patrones retinales); sin embargo, tienen en su contra la incapacidad temporal de autenticar usuarios que se hayan podido herir en el dedo a reconocer (un pequeño corte o una quemadura que afecte a varias minucias pueden hacer inútil al sistema). También elementos como la suciedad del dedo, la presión ejercida sobre el lector o el estado de la piel pueden ocasionar lecturas erróneas. Otro factor a tener muy en cuenta contra estos sistemas es psicológico, no técnico: un sistema de autenticación de usuarios ha de ser aceptable por los mismos, y generalmente el reconocimiento de huellas se asocia a los criminales, por lo que muchos usuarios recelan del reconocedor y de su uso.

Esta tecnología consiste en digitalizar la forma, el tamaño y otras características, como la longitud de los dedos, de parte o la totalidad de la mano. A los usuarios se les pide que presenten algún tipo de identificación -deslizando una tarjeta, por ejemplo- ante el escáner. La plantilla biométrica de la persona que afirman ser (que en algunos casos está almacenada en la misma tarjeta) es comparada luego con la lectura.

Se extraen ciertos datos (anchura, longitud, área, determinadas distancias...) en un formato de tres dimensiones. Transformando estos datos en un modelo matemático que se contrasta contra una base de patrones, el sistema es capaz de permitir o denegar acceso a cada usuario.

Uno de los elementos más importantes del reconocimiento mediante analizadores de geometría de la mano es que éstos son capaces de aprender: a la vez que autentican a un usuario, actualizan su base de datos con los cambios que se puedan producir en la muestra (un pequeño crecimiento, adelgazamiento, el proceso de cicatrizado de una herida...); de esta forma son capaces de identificar correctamente a un usuario cuya muestra se tomó hace años, pero que ha ido accediendo al sistema con regularidad.

Este hecho, junto a su rapidez y su buena aceptación entre los usuarios, hace que los autenticadores basados en la geometría de la mano sean los más extendidos dentro de los biométricos a pesar de que su tasa de falsa aceptación se podría considerar inaceptable en algunas situaciones: no es normal, pero sí posible, que dos personas tengan la mano lo suficientemente parecida como para que el sistema las confunda.

Para minimizar este problema se recurre a la identificación basada en la geometría se trata de la medición de las características físicas de manos y dedos desde una perspectiva tridimensional. Estos sistemas son adecuados a bases de muchos usuarios con acceso infrecuente y pueden estar menos predispuestos y disciplinados a ser detectados. La precisión puede ajustarse hasta ser elevada y son técnicas muy flexibles a los escenarios. De uno o dos dedos, que además puede usar dispositivos lectores más baratos y proporciona incluso más rapidez.

Los sistemas de autenticación basados en el análisis de la geometría de la mano son sin duda los más rápidos dentro de los biométricos: con una probabilidad de error aceptable en la mayoría de ocasiones, en aproximadamente un segundo son capaces de determinar si una persona es quien dice ser.

Los sistemas de geometría de la mano ya están siendo utilizados en sistemas de control de acceso y verificación de identidad en muchos aeropuertos, oficinas, fábricas, escuelas, hospitales, plantas de energía nuclear y edificios gubernamentales de alta seguridad. El mejor ejemplo es el del programa Inpass, que les permite a los viajeros frecuentes que llegan a Estados Unidos saltarse las colas ante inmigración en siete grandes aeropuertos deslizando una tarjeta y colocando la mano en un escáner.

2.8. Otras técnicas

Existen otra técnicas tales como el uso de perfumes, marcas indelebles y los lóbulos de las orejas, pero no son considerados como aplicables en forma masiva.

3. Código de Barras contra Biometría

Tabla II. Código de Barras contra Biometría

CONCEPTO	CODIGO DE BARRAS	BIOMETRIA	CONCLUSIONES
TECNOLOGIA	Sistema de tecnología de punta, que incluye comunicación por puerto ethernet, tiene capacidad de crecimiento en memoria.	Sistema de Tecnología de punta, con opción de comunicación por puerto ethernet. Tiene capacidad de crecimiento en memoria.	Ambos sistemas cuentan con opción electrónica actualizada, sólo que el biométrico es un equipo distinto de reconocimiento, ya que identifica personas, lo cual lo hace más confiable que código de barras, banda magnética o proximidad.
IDENTIFICACION	Estos sistemas reconocen OBJETOS, mediante el uso de credenciales con código de barras,	Este sistema reconoce PERSONAS, mediante el uso de la forma tridimensional de la mano.	No es lo mismo reconocer OBJETOS, que reconocer PERSONAS.

FRAUDE	El codigo de barras se puede copiar, cualquier persona puede prestar su credencial para que otra persona cheque su asistencia, horas extras, etc.	Con este sistema, nadie puede suplantar a otra persona, ya que la credencial es la mano. No se pierde, no se olvida y no se presta.	Los fraudes de puntualidad y asistencia en una empresa, por lo general existen, pero difícilmente detectamos a la persona que lo hace. Con un sistema biométrico, estos fraudes se van a 0%.
VELOCIDAD	Estos sistemas pueden ofrecer un tiempo de respuesta en el registro de puntualidad y asistencia de hasta dos segundos por empleado.	Estos sistemas pueden ofrecer un tiempo de respuesta en el registro de puntualidad y asistencia entre tres y seis segundos, dependiendo del equipo que se utilice.	En ocasiones es importante el tiempo de respuesta y la velocidad que los equipos ofrecen, pero se tiene que considerar la veracidad del registro final, el cual se puede obtener en dos segundos (identificación de objetos, no se sabe quién lo hace) o en seis segundos (identificación de personas, único por empleado).

MANTENIMIENTO	Las fallas más comunes en estos equipos ocurren en el teclado, en caso de que venga incluido, y en la base de deslizamiento de la tarjeta, la cual se desgasta con el tiempo. Solo requiere de limpieza general y en especial el área de lectura del código de barras o de la cabeza lectora en la banda magnética.	La falla más común en este equipo ocurren en el teclado, el cual tiene movimiento mecánico, requiere de limpieza general y en especial en el lente óptico donde se registra la huella dactilar	En ambos casos, las fallas más comunes se pueden corregir con un mantenimiento preventivo o en caso de ser correctivo, estas piezas son consumibles normales. También, en ambos casos, este material es una refacción poco costosa y fácil de remplazar.

VANDALISMO	Los sistemas de código de barras o de banda magnética pueden ser dañados, metiendo objetos en la ranura del lector, rociándoles algún líquido o simplemente agrediéndolos físicamente, mientras que en los lectores de proximidad, el vandalismo es muy reducido.	Estos sistemas pueden ser dañados, si se les rocía algún líquido o si se rompen sus espejos y/o postes, también si se agreden físicamente	Entre más restrictivo sea un equipo, más susceptible será al vandalismo, ya que representará mayor obstáculo a las personas que lo utilizan.

COSTOS	Según la calidad del equipo y de las funciones que incluyan, se pueden conseguir desde los $1,000.00 US hasta los $8,000.00 US	Un equipo Biométrico para 512 usuarios, tiene un costo desde $1,800.00 US.	Los costos son siempre importantes en la toma de decisiones para la adquisición de un equipo. Siempre se deberá tomar en cuenta aspectos como: ¿Qué se desea controlar? ¿Cuál es la seguridad que se desea tener en la veracidad de la información?, etc. De tal forma que en una tabla de comparativo costo-beneficio, se obtenga la mejor decisión para una compañía.
COSTO CONSUMIBLE	En un sistema de código de barras, banda magnética o proximidad, se pueden elaborar credenciales con precios desde $1.00 U.S., hasta los $15.00 U.S., dependiendo de la tecnología a utilizar.	En un sistema biométrico el costo del consumible es de $0.00, ya que la mano no le cuesta a la empresa.	En cada proyecto de puntualidad y asistencia, si éste es de código de barras o cualquier otra tecnología que identifique objetos, se debe considerar un 30% adicional a las credenciales que se necesiten, ya que la rotación y las pérdidas necesitarán de

			reposición inmediata. En un biométrico no se da este caso.

3.2 Métodos Biométricos

Table III. Características de los diferentes sistemas biometricos

	IDENTIFICACION AUTENTICACION	INTERFERENCIA	FIABILIDAD	FACILIDAD DE USO	PREVENCION DE ATAQUES	ACEPTACION	ESTABILIDAD	UTILIZACION
OJO - IRIS	AMBAS	GAFAS	MUY ALTA	MEDIA	MUY ALTA	MEDIA	ALTA	INSTALACIONES NUCLEARES,SER-
OJO-RETINA	AMBAS	IRRITACIONES	MUY ALTA	MEDIA	MUY ALTA	MEDIA	ALTA	CIOS MÉDICOS CENTROS PENITEN-
HUELLAS DACTILARES	AMBAS	SUCIEDAD HERIDAS	ALTA	BAJA	ALTA	MEDIA	ALTA	CIARIAS
GEOMETRIA DE LA MANO	AUTENTICACION	ARTRITIS REUMATISMO	ALTA	ALTA	ALTA	ALTA	MEDIA	POLICIA NDUSTRIAL GENERAL INDUSTRIAL
ESCRITURA FIRMA	AMBAS	FIRMAS FACILES O CAMBIANTE	ALTA	ALTA	MEDIA	MUY ALTA	MEDIA	ACCESOS REMOTOS A BANCOS O
VOZ	AUTENTICACION	RUIDO RESFRIADO	ALTA	ALTA	MEDIA	ALTA	MEDIA	BASES DE DATOS

4. DEFINICIONES DEL PROYECTO

4.1. Introducción

En la actualidad la seguridad en las transacciones bancarias cada día debe ser más robusta pues existen muchos métodos de fraude que hace inseguro un sistema bancario.

Existen empresas que contratan los servicios a entidades bancarias para realizar sus pagos de planillas y estas deben de velar por la seguridad para evitar cualquier tipo de fraude. Este proyecto muestra como se puede utilizarse la biometría como medio para la autenticación de las personas utilizando la huella digital.

4.2. Fines específicos y generales del sistema COPIBA

El presente Sistema de Software tendrá como fin automatizar el pago de planillas utilizando la biometría como medio de seguridad para la autenticación de la persona, de tal manera que se cumplan los siguientes objetivos:

- Mejora en el servicio de pago de planillas.
- Utilizar el sistema biométrico como medio de autenticación.
- Datos estadísticos que ayuden a encontrar fallas en el sistema de pagos.
- Disminución de tiempo por parte del operador que atiende los clientes.

- Disminución del coste en los servicios por pago de planillas
- Uso eficiente de la tecnología.

Para alcanzar estos objetivos se propone la creación de un sistema que cumpla con lo siguiente:

- Crear un sistema de pagos de planilla que utilice la huella digital como medio de autenticación segura, rápida y eficiente para identificar a una persona.

4.3. Funcionamiento esperado del Sistema COPIBA

El sistema ayudara al receptor a identificar a la persona que quiere realizar una transacción bancaria de una forma segura, rápida y eficiente. Se utilizará la huella digital como medio para identificar a la persona con la ayuda del sistema biométrico para su validación.

El sistema bancario debe de tener una base de datos que contenga la siguiente información mínima para poder realizar la autenticación por el sistema biométrico: se debe tener registrado con anterioridad 2 huellas de diferentes dedos de cada persona.

Estas huellas se almacenan en el aparato biométrico y en la computadora donde se encuentra el sistema COPIBA. El proceso de registrar la huella digital dura aproximadamente de 15 a 20 minutos por persona pues se trata de buscar la mejor huella que tenga la persona. Teniendo los datos personales y las huellas de los trabajadores se forma una base de datos que nos permitirá identificar a cada uno de los trabajadores de la siguiente manera:

Los trabajadores pasan a las ventanillas tecleando su numero de pin y luego colocan uno de sus dedos en el dispositivo biométrico este procede a identificarlo positivamente o negativamente, luego el dispositivo biométrico se comunica con la computadora principal mediante una conexión serial, en la computadora existirá una interfase monitorizará los resultados obtenidos por el biométrico y si la identificación es positiva la interfase grafica tomara el código de la huella que se identifico y lo buscara en la base de datos de los trabajadores obteniendo de allí sus datos personales, total a pagar, así como su fotografía. Los datos incluyendo la fotografía son presentados al receptor pagador, luego es impreso el recibo de pago correspondiente de la cancelación luego este es firmado por el trabajador y le queda como prueba del pago.

4.4. Descripción del Sistema Biométrico

El proyecto fue creado por la necesidad de dar mayor seguridad y agilizar el proceso de pago de empleados de empresas que manejan personal y que solicitan este servicio a las entidades bancarias, dicho sistema permite garantizar la identificación de las persona que son pagadas en la sucursal del banco, ahorrando el uso de documentos de identificación personal pues estos pueden ser fácilmente falsificados.

4.4.1. Arquitectura del sistema biométrico para identificación personal

El dispositivo biométrico posee tres componentes básicos que se definen a continuación:

1. Se encarga de la adquisición análoga o digital de algún indicador biométrico de una persona, este es la adquisición de la imagen de una huella dactilar mediante un escáner.
2. Maneja la compresión, procesamiento, almacenamiento y comparación de los datos adquiridos (la huella digital) con los datos almacenados.
3. La arquitectura del sistema biométrico se presenta en la figura 4.1. Esta puede entenderse conceptualmente como dos módulos:
    - Módulo de inscripción (enrollment module)
    - Módulo de identificación (identification module)

4.4.2. Módulo de inscripción (enrollment module)

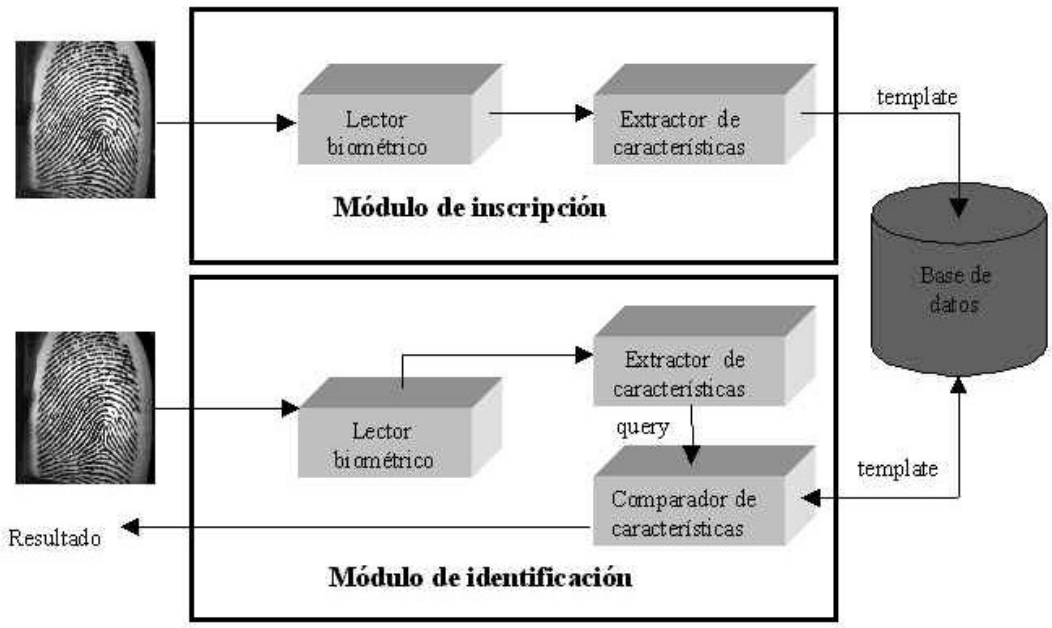
El módulo de inscripción se encarga de adquirir y almacenar la información proveniente del indicador biométrico con el objeto de poder contrastar a ésta con la proporcionada en ingresos posteriores al sistema. Las labores ejecutadas por el módulo de inscripción son posibles gracias a la acción del lector biométrico y del extractor de características.

4.4.3. Módulo de identificación : *(identification module).*

Es el responsable del reconocimiento de individuos, el proceso de identificación comienza cuando el lector biométrico captura la característica del individuo a ser identificado y la convierte a formato digital, para que a

continuación el extractor de características produzca una representación compacta con el mismo formato de los *templates*. La representación resultante se denomina query y es enviada al comparador de *características* que confronta a éste con uno o varios *templates* para establecer la identidad. El conjunto de procesos realizados por el módulo de inscripción recibe el nombre de *fase de inscripción*, mientras que los procesos realizados por el módulo de identificación reciben la denominación de *fase operacional*.

Figura 3: Arquitectura de un sistema biométrico para identificación personal



4.5. Fase operacional del sistema

El sistema biométrico en su fase operacional puede operar en dos modos:

- Modo Operacional de verificación
- Modo Operacional de identificación

4.5.1. Modo Operacional de verificación

Comprueba la identidad de un individuo comparando las característica de los templates del individuo. Por ejemplo, si una persona ingresa su código de usuario entonces no será necesario revisar toda la base de datos buscando él témplate que más se asemeje al de él, sino que bastará con comparar la información de entrada sólo con él témplate que está asociado al usuario. Esto conduce a una comparación uno-a-uno para determinar si la identidad reclamada por el individuo es verdadera o no. De manera más sencilla el modo de verificación responde a la pregunta: ¿eres tú quién dices ser?.

4.5.2. Modo Operacional de identificación

Con el pin ingresado el dispositivo busca la huella correspondiente en la base de base de datos de templates . Esto conduce a una comparación de la huella para establecer la identidad del individuo. En términos sencillos el sistema responde la pregunta: ¿quién eres tú?.

4.6. Medidas de desempeño

La información provista por los templates permite particionar su base de datos de acuerdo a la presencia o no de ciertos patrones particulares para cada indicador biométrico. Las "clases" así generadas permiten reducir el rango de búsqueda de algún template en la base de datos. Sin embargo, los templates pertenecientes a una misma clase también presentarán diferencias conocidas como *variaciones intraclase*. Las variaciones intraclase implican que la identidad de una persona puede ser establecida sólo con un cierto nivel de confianza. Una decisión tomada por un sistema biométrico distingue "personal autorizado" o "impostor". Para cada tipo de

decisión, existen dos posibles salidas, verdadero o falso. Por lo tanto existe un total de cuatro posibles respuestas del sistema:

1 Una persona autorizada es aceptada,
2 Una persona autorizada es rechazada,
3 Un impostor es rechazado,
4 Un impostor es aceptado.

Las salidas números 1 y 3 son correctas, mientras que las números 2 y 4 no lo son. El grado de confidencia asociado a las diferentes decisiones puede ser caracterizado por la distribución estadística del número de personas autorizadas e impostores. En efecto, las estadísticas anteriores se utilizan para establecer tasas de errores .

4.7. Recursos de Hardware

Se necesita como mínimo los siguientes equipos, con las características que se detallan a continuación:

- El servidor principal debe ser una computadora personal con procesador Pentium 4 de 1 Ghz o superior, con 1 GBb de espacio en disco duro para almacenar los programas y los templates y 256 Mb de memoria RAM. Teclado, monitor color 15” o superior, ratón y medio de intercambio de datos (red) y un puerto serial.
- Las computadoras que serán utilizadas como clientes deben de tener un procesador Pentium 4 de 1 Ghz o superior, con 1 GBb de espacio en disco duro y 256 Mb de memoria RAM. Teclado, monitor color 15” o superior, ratón y medio de intercambio de datos (red) y un puerto serial.
- El dispositivo biométrico a utilizar es el Veriprint v2100

4.8. Recursos de Software

La PC que será utilizada como servidor necesita que tenga instalado los siguientes productos:

- Sistema operativo MS Windows 2000 Profesional
- Base de datos Oracle Personal
- Oracle Developer
- Very test

Las PC's que será utilizada como clientes necesitan tener instalado los siguientes productos:

- Sistema operativo MS Windows 2000 Profesional
- Oracle Developer
- Very test

4.9. Recursos Humanos

Como mínimo se necesita una persona que atenderá a las personas a solicitar el pago de planilla, llamado receptor pagador el cual debe tener las siguientes características como mínimo:

- Titulo a nivel medio
- Acostumbrado a trabajar en base a metas y objetivos
- Vocación de servicio al cliente
- Buenas relaciones interpersonales
- Dominio de paquetes de computación en ambiente Microsoft.

5. DISEÑO Y PROPUESTA

5.1 introducción

El sistema COPIBA se vale de la tecnología de punta tanto en software y hardware para crear toda una nueva metología de pagos de personal, pues introduce dentro de sus mecanismos el uso de un identificador biométrico que permite la captura de las características biométricas de las hullas dactilares de las personas para poder identificarlos.

El dispositivo biométrico, se comunica con una interfase grafica que le requiere constantemente si la persona que en ese momento esta siendo identificado es aceptado o no, si es aceptado la interfase grafica también valida si existe como código de empleado en la base de datos que se tienen (el dispositivo biométrico le proporciona 2 valores el primero es el código del empleado , y el segundo si es aceptado o no) si existe como empleado muestra al receptor pagador la fotografía de la persona que fue autenticado previamente por el dispositivo biométrico, así como los datos básicos del empleado (la fotografía permite tener un doble control de seguridad pues al visualizarla el receptor pagador le permite comprobar si es el empleado o no), el sistema muestra al receptor el total a pagar al empleado, al finalizar toda la operación el sistema imprime un recibo de pago el cual firma la persona que fue pagada, y una copia le queda al receptor pagador como respaldo del pago.

El sistema lleva internamente una bitácora el cual registra el no. de empleado que fue pagado,el monto total pagado, la fecha y la hora, así también el código de usuario del receptor pagador, toda esta información permite generar diferente tipo de reportes gerenciales de bastante utilidad para la empresa.

5.2 Consideraciones Iniciales

Las consideraciones iniciales del sistema COPIBA se detallan a continuación:

- Transportabilidad de las fotografías:

  Las fotografías almacenadas de los empleados deben tener un tamaño promedio de 12 kb. Con este tamaño permitirá mantener una resolución media y transportar mejor la información en cada una de las agencias bancarias, pues hay que tener en cuenta que existen agencias que no tienen enlaces dedicados sino que la conexión se realiza vía telefónica, reduciendo la información al máximo se podrá enviar toda la información de las empresas con mayor facilidad y rapidez.

- Transportabilidad de las Huellas dactilares:

  Las huellas dactilares de los empleados tendrán un promedio de 1 kb de tamaño. Con este tamaño se garantiza la resolución de cada una de las huellas de los empleados registrados, a la vez nos permite con facilidad y rapidez enviar la base de datos de las huellas de los empleados.

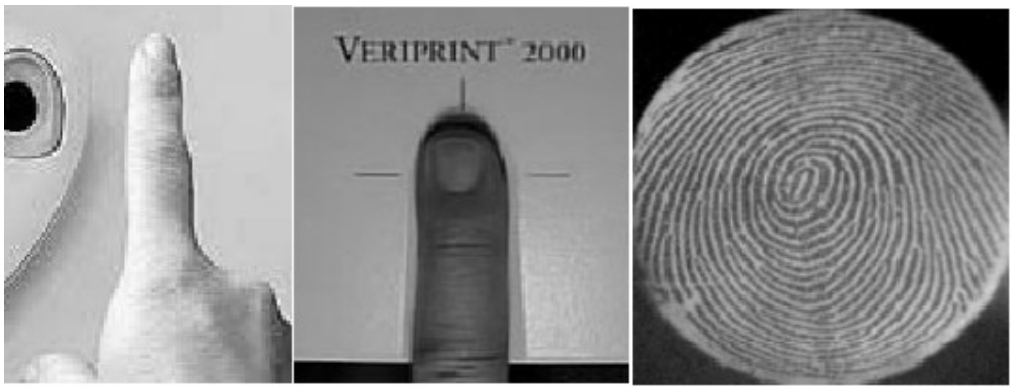
  Se guardaran 2 huellas dactilares de cada uno de los empleados, una de cada mano, si se tiene problemas con una huella se tendrá otra para su identificación.

5.3. Metodología del Control de pago de planilla.

5.3.1. Registro de huellas Dactilares

En primer lugar se registran las huellas dactilares y fotografías de cada uno de los empleados según se muestra en la figura 4.

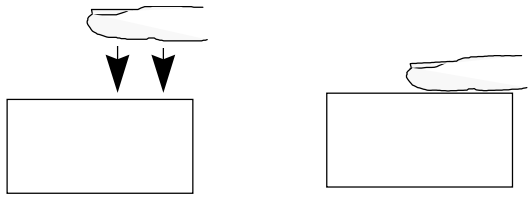
Figura 4: Registro de huella Digital en el dispositivo biométrico



La clave de un buen registro de la huella Dactilar consisten en la Colocación digital apropiada, esto consiste en posicionar la porción de la huella digital en el centro del sensor. La cutícula nos proporciona un método seguro para localizar la información fácilmente.

Encuadrando su cutícula en la cruz horizontal (encuentre el perímetro de la guía digital), baje su dedo hacia el plato óptico. Es importante que usted ponga huella dactilar mientras aplica presión moderada. No resbale ningún dedo según se muestra en la figura 5.

Figura 5: Colocación del dedo correctamente



Una mala colocación del dedo causara un mal registro en la obtención de la huella digital .Resbalando el dedo en lugar de bajarlo hacia el plato óptico causarán distorsión de la huella digital y degradarán calidad de la imagen como lo muestra la figura 6 y figura 7.

Figura 6: Colocación incorrecta

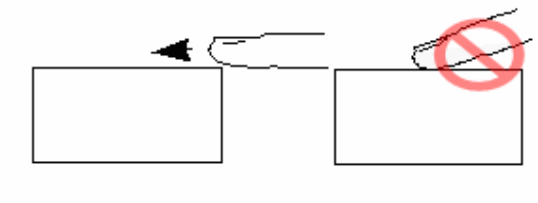
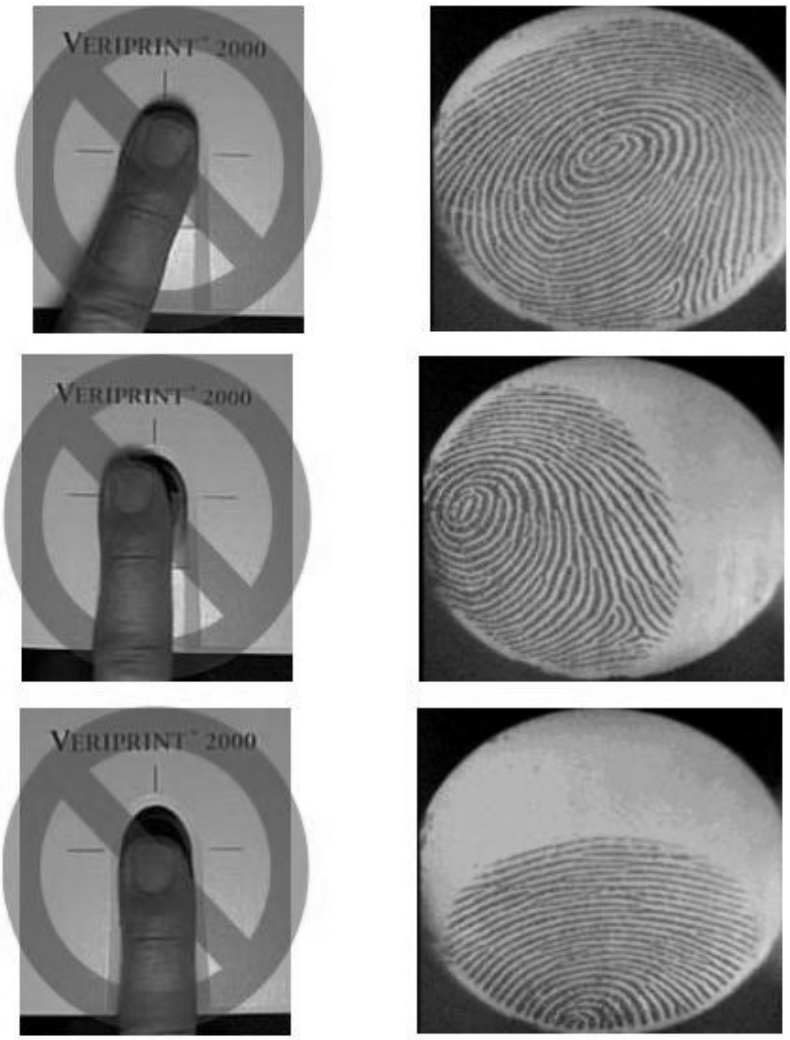


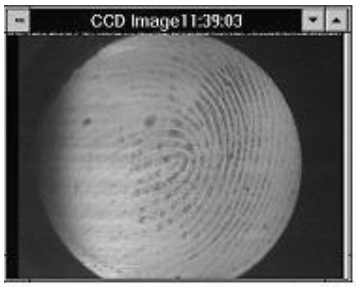
Figura 7: Posiciones incorrectas en el registro de la huella dactilar



La piel seca es otro factor que puede contribuir a una imagen inestable de una huella digital. La huella digital se centra pero el dedo del usuario está demasiado seco. Demasiado o poca humedad hace la imagen no tenga una buena resolución y esto hace que cuando se identifique a la persona el dispositivo rechace la imagen durante procesar. Hidratando el dedo

ligeramente reforzarán el contraste de la impresión y proporcionarán comprobación más fiable según se muestra en la figura 8.

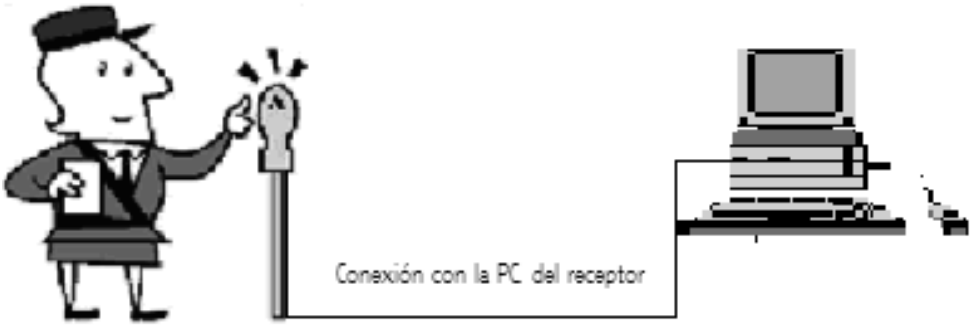
Figura 8: Imagen con poca resolución



Las huellas dactidales juntamente con las fotografías y los datos básicos de cada uno de los empleados son grabados y enviados a una base de datos central de la institución bancaria, para luego reenviarlos en la agencia bancaria especifica donde los empleados llegaran a realizar el cobro de planilla.

El empleado llega a la ventanilla y se identifica con su huella dactilar registrada según se muestra en la figura 9.

Figura 9: Identificación de la huella dactilar

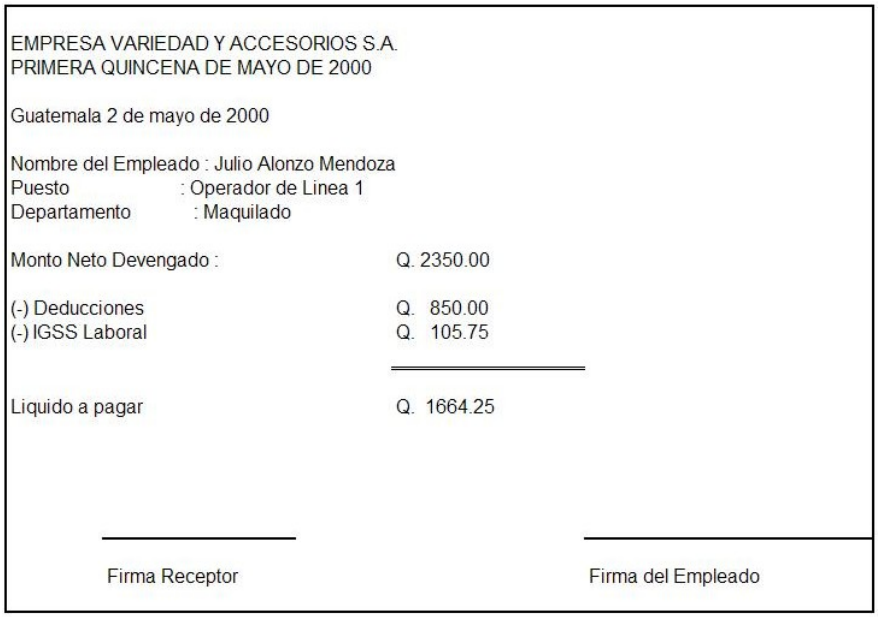


El empleado es autenticado por el dispositivo biométrico y se comunica con la interfase grafica si la identificación es positiva el sistema COPIBA lo busca en la base de datos y muestra al receptor pagador la fotografía del empleado así como lo muestra la figura 10.

Figura 10: Fotografía del empleado

El sistema COPIBA se comunica con la base de datos de la empresa para ir a obtener los datos del pago (total devengado, bonificación, descuentos etc.) El receptor pagador obtiene la información general del pago y en la pantalla le muestra el liquido a apagar, cuando es terminada la transacción el sistema imprime un recibo para tener constancia física del pago dicho recibo es firmado por el empleado y queda una copia al receptor pagador dicho recibo se muestra en la figura 11.

Figura 11: Recibo de Pago



EMPRESA VARIEDAD Y ACCESORIOS S.A.
PRIMERA QUINCENA DE MAYO DE 2000

Guatemala 2 de mayo de 2000

Nombre del Empleado : Julio Alonzo Mendoza
Puesto : Operador de Linea 1
Departamento : Maquilado

Monto Neto Devengado :	Q. 2350.00
(-) Deducciones	Q. 850.00
(-) IGSS Laboral	Q. 105.75
Liquido a pagar	Q. 1664.25

Firma Receptor

Firma del Empleado

5.4. Dispositivo biométrico Veriprint 2000

El Veriprint 2000 es uno de los sistema de reconocimiento de huella digital más económico y robusto comercialmente disponible. El sistema óptico de Veriprint no puede ser engañado por falsificaciones ni por deformaciones del dedo por causa de cortaduras u otro tipo de daños en el dedo del usuario.

El Veriprint 2000 devolverá una decisión con una exactitud del 99.9% de todos los casos.

La unidad de Veriprint, puede almacenar sin aumento de memora 3500 plantillas de huella digital. El tiempo de la contestación es menos de 1.0 segundos para el registro de la huella digital y menos de 1.5 segundos para la comprobación de la huella digital. El sistema es compacto, versátil, y se

puede configuró para permitir standalone, el funcionamiento puede permitir múltiples unidades.

5.5. Uso del Veritest

El software Veritest es compatible con Microsoft Windows 98/2000/XP. Este software permite la manipulación de las huellas dactilares del Veriprint por medio de la PC. del administrador del sistema .

Este software permite transportar la base da datos de las huellas de la PC. al dispositivo biométrico Veriprint entre otras funciones generales.

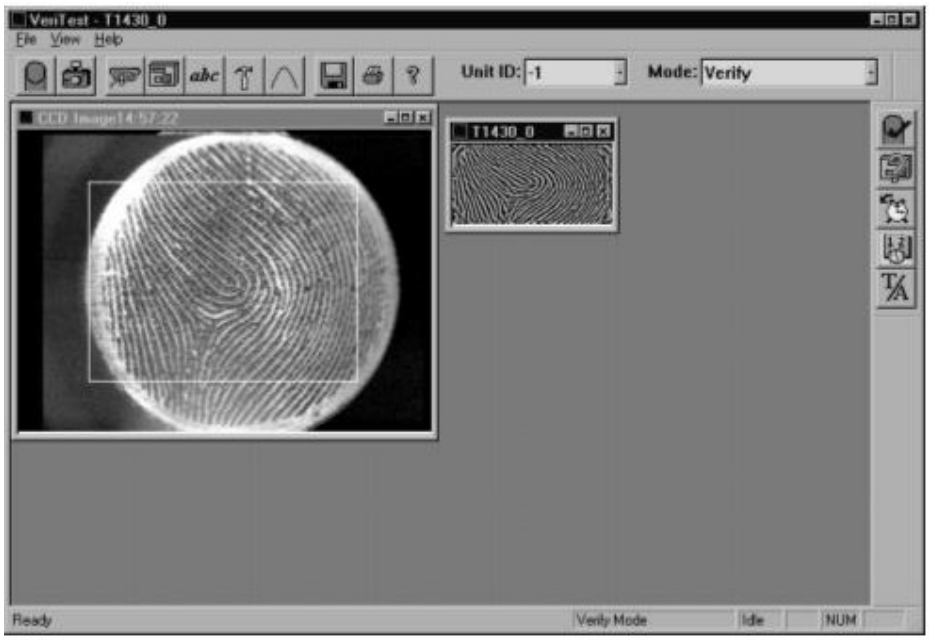
Este esta disponible como un suplemento al software de Veritest en un equipo de desarrollo de software está con una biblioteca del librerías dinámicas para aplicaciones que requieren conexión de PC y customization de la interfase. El Veritest contiene el código fuente útil al desarrollo rápido de aplicaciones. Estas librerías permitirán a la interfase grafica poder interactuar con la Veriprint.

Con el software de aplicación del Veritest se puede hacer las siguientes funciones:

- Operar el sistema de Veriprint desde su PC.
- Realizar direccionamientos de banco de datos de Huellas Digitales
- Permite el despliegue grafico de imágenes de de Huellas Digital.
- Permite la Inspección de la calidad de la imagen de Huella Digital.
- Contiene bibliotecas de desarrollo de software para la conectividad con una PC.

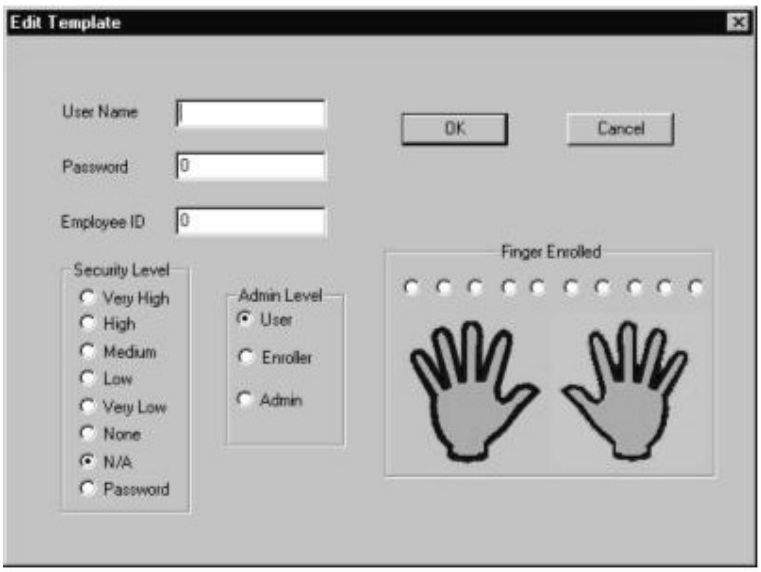
A continuación se muestra en la figura 12 una huella dactilar digitalizada que es utilizada por el dispositivo biométrico.

Figura 12: Huella dactilar digitalizada



El veritest permite editar las plantillas de los empleados registrados te en el dispositivo biométrico Veriprint como se muestra en la figura 13.

Figura 13: Plantilla de una huella digital



En el témplate de cada uno de las huellas se registran los siguientes campos:

- Nombre del empleado (16 caracteres)
- Contraseña (Obligatorio si es el administrador del sistema).
- Código del empleado
- El nivel de seguridad de la Huella que puede ser
  - Muy alto
  - Alto
  - Mediano
  - Bajo
  - Muy bajo
  - Sin seguridad
  - Valor predefinido de seguridad del sistema.
  - Password (se ingresara un password numérico).
- Nivel Administrativo de la Huella del Usuario
  - El usuario solo tendrá acceso al modo de comprobación

- El Usuario que registra a los nuevos empleados.
- El Usuario Administrador del sistema.

- El Número del dedo de las manos del 0 al 9.

El Veritest permite restablecer el tiempo en la unidad de Veriprint e igualar el tiempo del sistema de PC como se muestra en la figura 14.

Figura 14: Traslado de la hora de la PC. Al dispositivo biométrico Veriprint

5.6. Diseño de la interfase Grafica

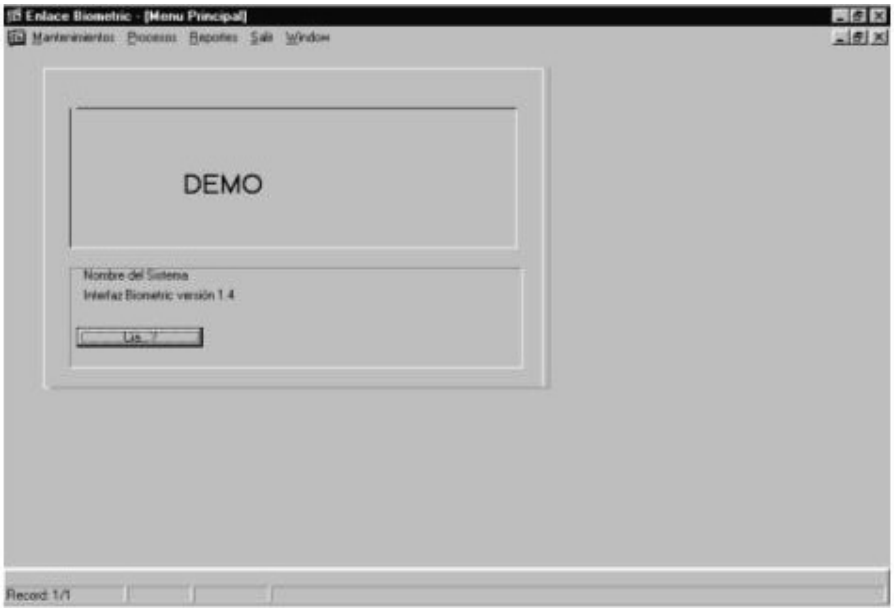
El diseño de la interfase grafica considera la inserción, actualizacion, consulta,y eliminación de registros de los datos básicos de los empleados, con su respectiva acceso de seguridad pues hay ciertas opciones del menú que solo los gerentes tendrán acceso.

A continuación se muestra las pantallas básicas de la interfase grafica del control de pagos.

5.6.1. Menú Mantenimientos:

Este menú agrupa los procesos necesarios para definir las entidades elementos Básicos del sistema de interfase grafica según se muestra en la figura 15, por ejemplo códigos de planillas, fichas de empleados Departamentos, definición de puestos.

Figura 15: Menú principal del sistema COPIBA

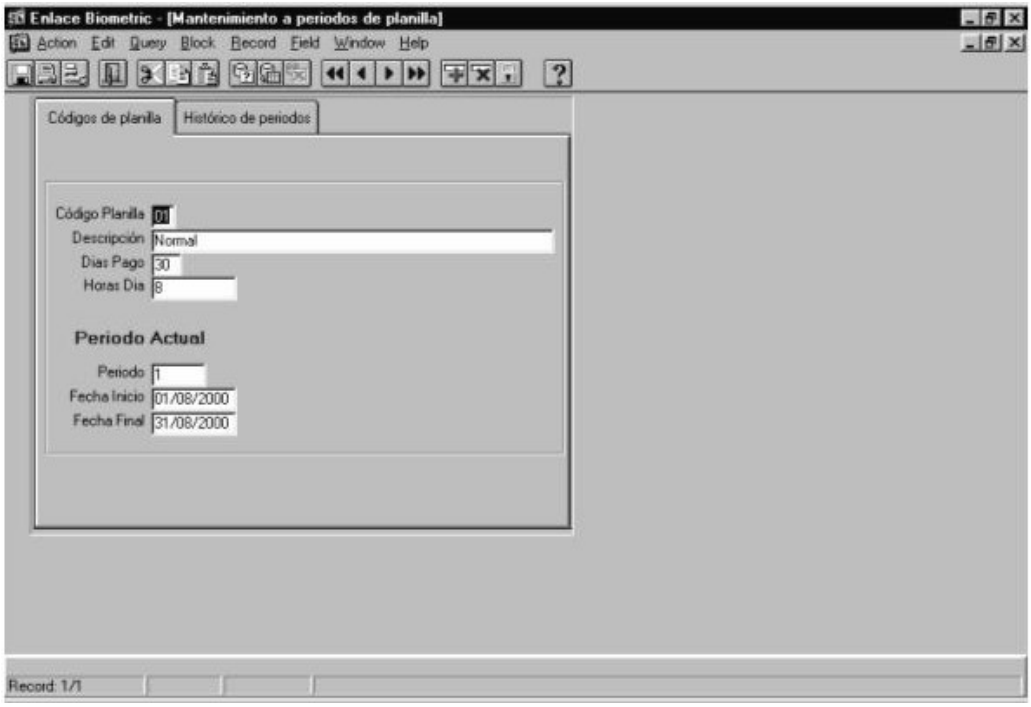


Opciones del menú

-Código de planillas .

En esta opción se definen los tipos de planillas que tengan la empresa creadas según se muestra en la figura 16. Por ejemplo planilla de empleados administrativos, planilla de empleados de planta etc.

Figura 16: Definición de tipo de planillas del sistema COPIBA

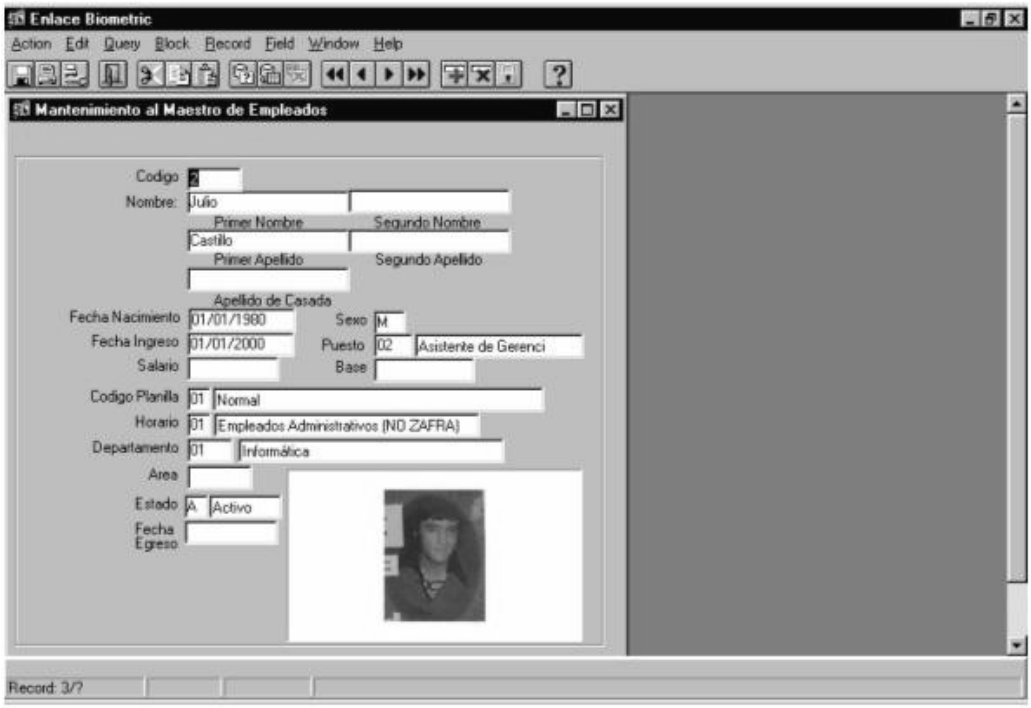


Por medio de este proceso se define las múltiples planillas que maneja una empresa.

Maestro de Empleados.

Aquí se definirán los datos básicos de los empleados esta forma permitirá también consultar,actualizar y eliminar registros según se muestra en la figura 17, esta opción la tendrá habilitada únicamente el administrador del sistema.

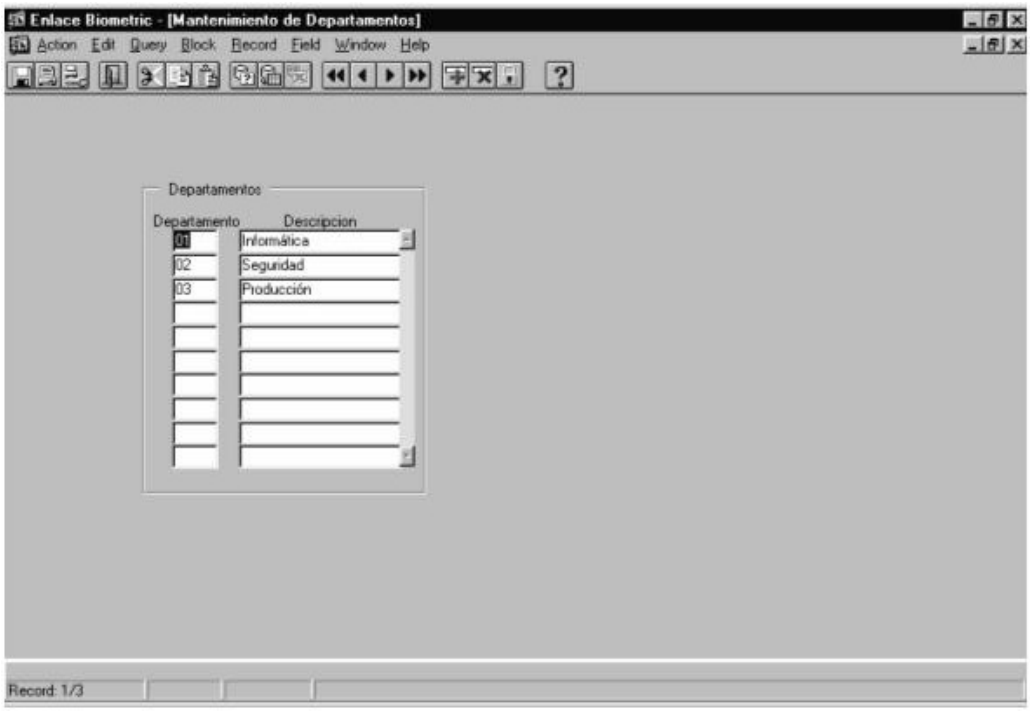
Figura 17: Ficha de datos de los empleados en el sistema COPIBA



Maestros Departamento:

En esta opción se definen los diferentes tipos de departamentos que se tendrán definidos por empresa según se muestra en la figura 18.

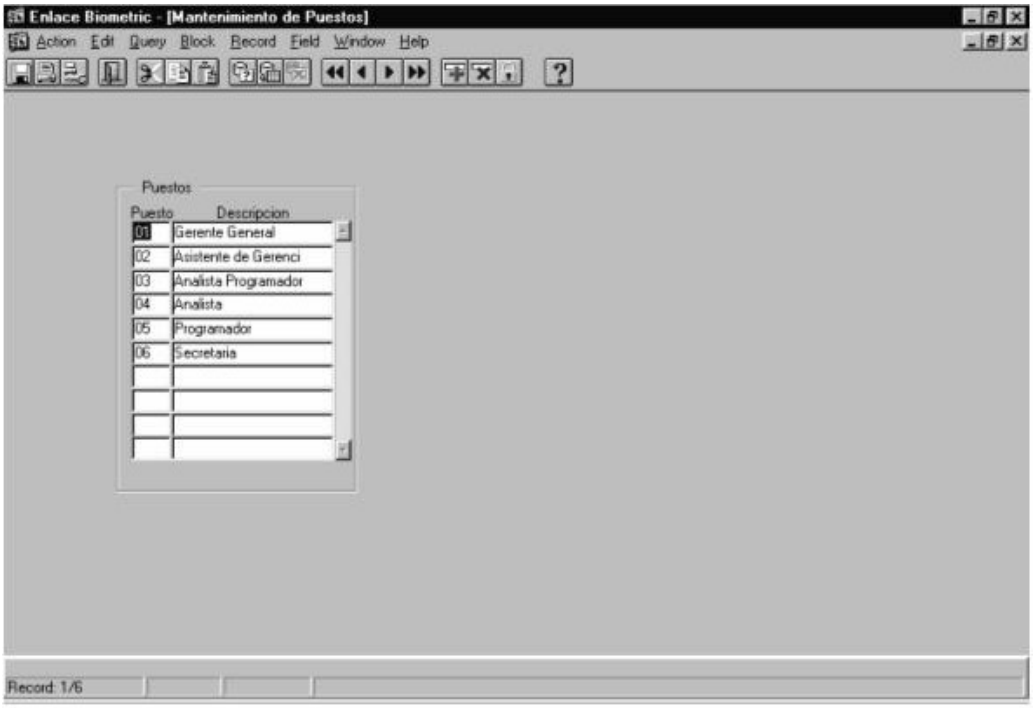
Figura 18: Definición de los departamentos del sistema COPIBA



Maestros Puestos

En esta opción se definen los diferentes tipos de puestos que se tendrán por empresa según se muestra en la figura 19.

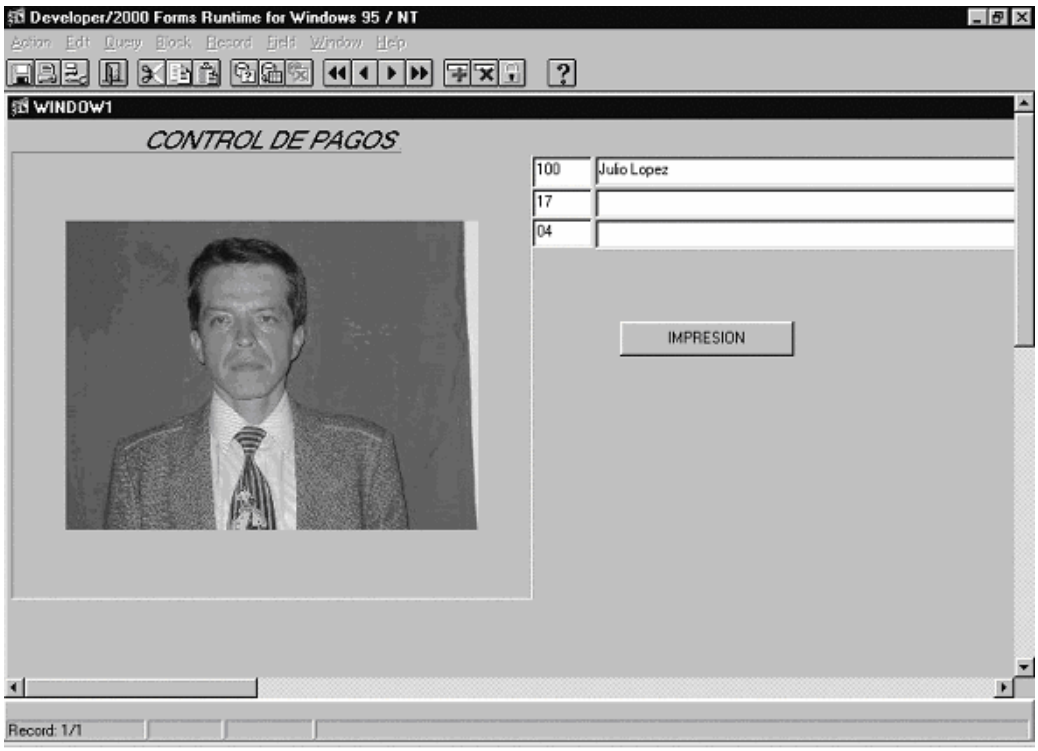
Figura 19: Definición de Puestos del sistema COPIBA



5.6.2. Menú Procesos

Este menú contiene el proceso de reconocimiento de los empleados cuando se entra a esta opción el sistema inicia el reconocimiento del empleado comparando la huella del empleado con las que tiene el dispositivo biométrico si el resultado es positivo este se comunica con la interfase grafica la cual busca en la base datos si existe este empleado el receptor pagador se le mostrara la siguiente figura 20.

Figura 20: Despliegue de los empleados aceptados



Después de mostrar los datos principales y la fotografía del empleado el receptor puede mandar a imprimir el recibo de pago.

Si el empleado no es reconocido en la Veriprint o no existe en la base de datos se muestra la siguiente figura 21.

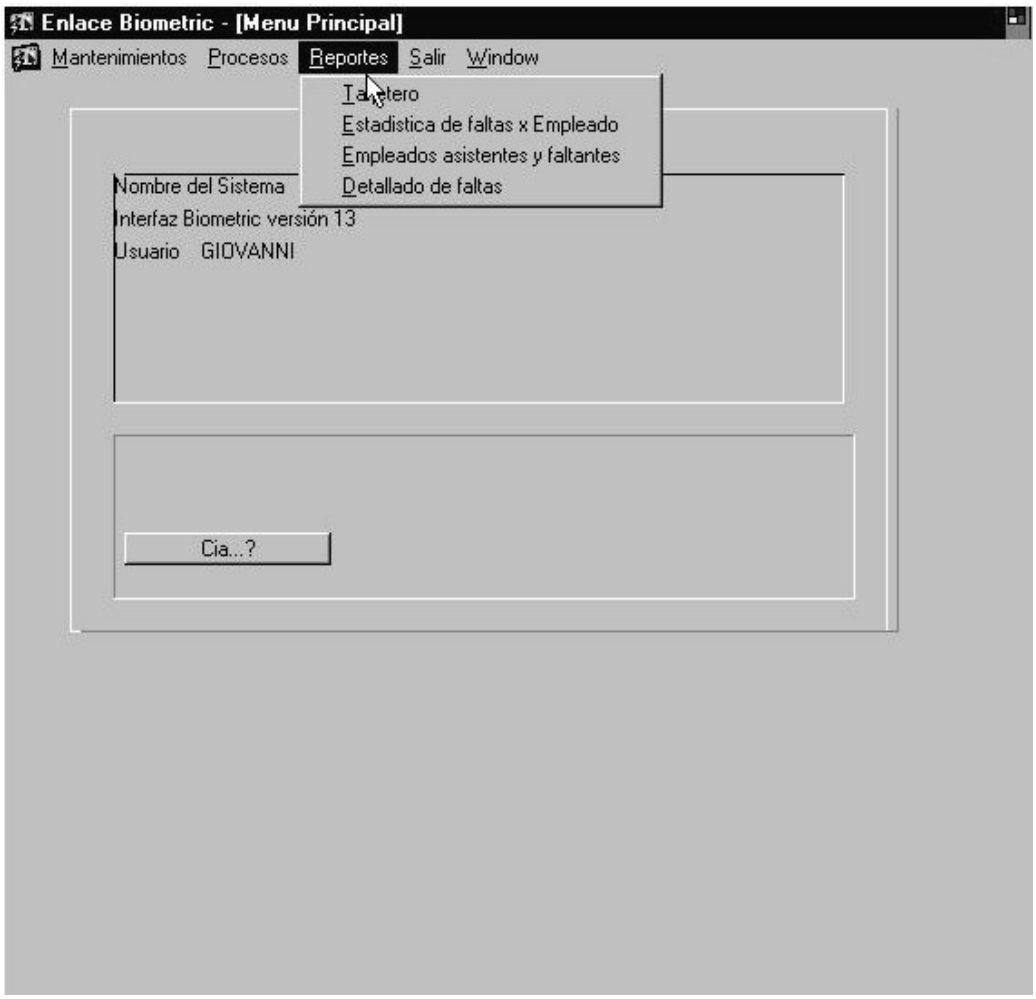
Figura 21: Despliegue de los empleados no aceptados

En el menú de reportes se tendrá los reportes básicos como listado de empleados, listado de departamentos,listado de puestos.

5.6.3. Menu de Reportes

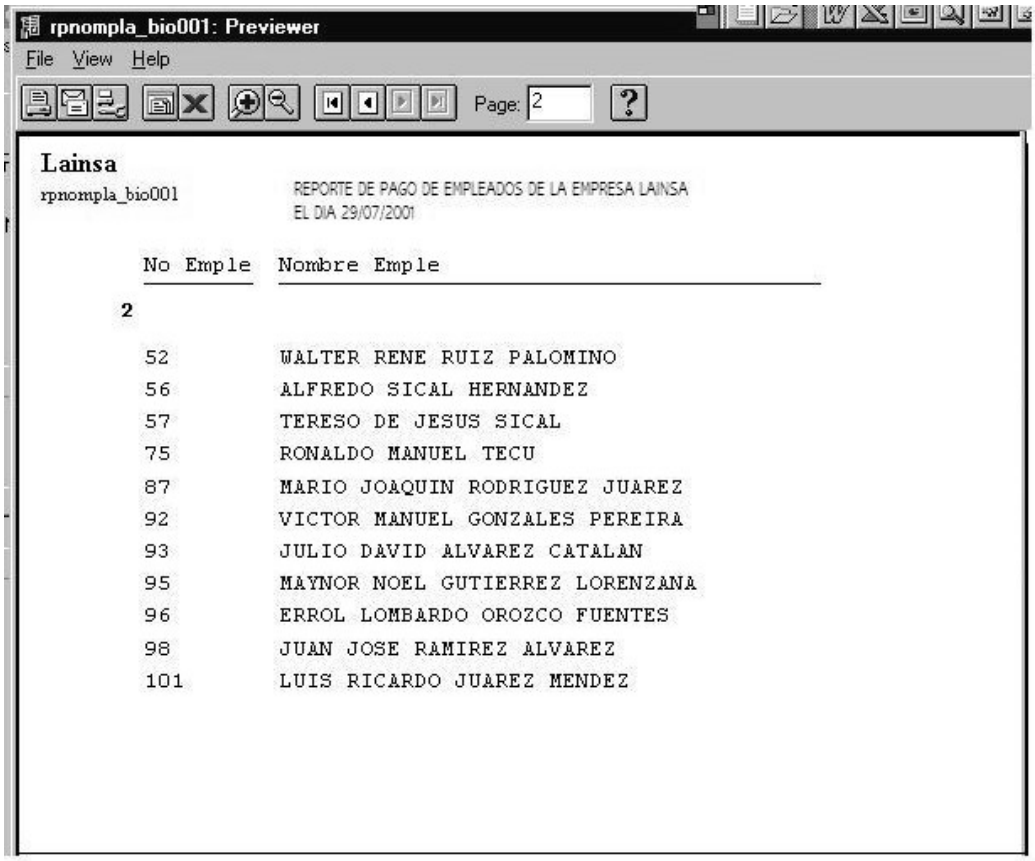
Este menú menú contiene los principales reportes del sistema COPIBA según figura 22.

Figura 22: Menú de reportes del sistema COPIBA



Entre los reporte que contiene la interfase grafica es el listado de empleados pagados según figura 23.

Figura 23: Reporte de empleados pagados del sistema COPIBA



5.6.4. Barra de botones (Toolbar)

Figura 24: Barra de botones

Descripción General.

El Toolbar es una paleta de iconos o botones estándar a todas las aplicaciones. Su función es que el usuario se familiarice con estos iconos y no tenga que estar recurriendo al uso de las teclas.

Sin embargo, el hecho de que este Toolbar exista, no significa que el usuario no pueda usar las teclas. De hecho, una de estas ayudas están el la opción Help del menú este nos permite ver las teclas asociadas.

Se explicaran los botones principales de manipulación de las formas.

Figura 25: Salir

Este botón permite salir de la pantalla en que se encuentra y retorna al menú principal.

Figura 26: Consultar

Si se presiona el botón la pantalla se pone en un estado de ENTER QUERY, lista para que se den los criterios de selección de la consulta que se va a realizar.

Figura 27: Ejecutar consulta

Si se presiona se ejecuta la consulta .

Figura 28: Bloque anterior

Este botón permite que en pantallas que tienen múltiples bloques, se pueda regresar al bloque anterior.

Figura 29: Bloque siguiente

Este botón permite avanzar al siguiente bloque de la tabla en que se encuentra ubicado el cursor.

Figura 30: Registro anterior

Este botón permite regresar al registro anterior de la tabla del bloque en el que se encuentra ubicado el cursor.

Figura 31: Registro siguiente

Este botón permite avanzar al siguiente registro de la tabla del bloque en el que se encuentra ubicado el cursor.

Figura 32: Grabar

Este botón permite grabar en la base de datos lo que se hizo en la pantalla.

Figura 33: Reversar

Este botón permite limpiar la pantalla.

3. CONCLUSIONES

1. El sistema de control de pagos de planilla usando autenticación biométrica, es la forma segura para la identificación y el pago de los empleados.

2. El sistema agilizará el pago evitando colas en las ventanillas pues no se necesitará tener ningún tipo de documento de identificación, únicamente la huella dactilar de la persona.

3. El uso de la huella digital como método de identificación agiliza la forma de pago y trabajo del receptor pagador de la agencia. Ya que el sistema se encarga de verificación de la identificación de la persona.

4. El sistema es fácil y rápido en la transportabilidad de la información a cada una de las agencias bancarias. Ya que la información que se traslado como lo es la huella digital, es de un tamaño de 1kb. más que suficiente en traslado de información en líneas telefónicas.

RECOMENDACIONES

1. Para tener una buena imagen de la huella dactilar de las personas hay que hacer tres pruebas como mínimo para obtener la mejor.

2. Se debe almacenar por lo menos dos huellas digitales por persona, por algún problema que se pueda tener en alguna de las manos y se recomienda que sean los índices de cada una de las manos.

3. El tamaño promedio de las fotografías debe ser de 12 kb. para poder hacer transportable la información entre la central bancaria y las agencias.

4. Para mayor seguridad en el sistema de control de pagos de planillas se debe tener guardadas las fotografías y las huellas digitales en la base de datos.

5. El número de ventanillas de pago debe ser proporcional al número de empleados que se tenga planeado pagar, y cada una debe de tener un dispositivo biométrico.

BIBLIOGRAFIA

1. http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm
2. http://www.insys.com.mx/biometria/lectores.htm
3. http://www.lagente.com/cgi-bin/contenido.pl?Art=56
4. http://www.lagente.com/cgi-bin/contenido.pl?Art=56
5. http://www.aymsb.com.uy/rp02.htm
6. http://www.biomedios.com/biometria.php
7. http://www.segured.com/article.php?sid=90
8. http://www.barware.com.mx/webpage/captura.htm
9. http://www.chiletech.cl/link.cgi/empresas/n/nec/9688
10. http://www.tekhnosur.com/pdf/hand.pdf
11. http://www.nec.cl/htm/productos/identificación_biométrica
12. http://www.tumaster.com/seccion-identifiacion+biométrica

APÉNDICE A: DISEÑO DE LA BASE DE DATOS

Diseño de Base de Datos.

En el diseño de la base de datos para el control de pagos en las agencias bancarias, se guardarán los datos básicos de cada uno de los empleados, pues se guardará información del pago .

Las tablas básicas son las siguientes:

Maestra de Compañías:

```
Create table Mae_Cia (
  CIA                VARCHAR2(2) NOT NULL,
  NOMBRE             VARCHAR2(80) not null,
  DIRECCION          VARCHAR2(80),
  TELEFONO           VARCHAR2(20),
  CONSTRAINT idt_mae_cia primary Key (cia)
)
```

Permite almacenar los registros de los empleados pagados

```
Create table Registros_empleados (
  CIA            VARCHAR2(2) NOT NULL,
  EMPLE          VARCHAR2(6) NOT NULL,
  FECHA          DATE NOT NULL,
  Constraint idt_Registros_Reloj primary key (cia, emple, fecha)
)
```

Maestro de Puestos

```
Create table puestos (
 CIA                VARCHAR2(2) NOT NULL,
 PUESTO             VARCHAR2(3) NOT NULL,
 DESCRIPCION  VARCHAR2(30),
 Constraint Pk_puestos primary key (cia,puesto)
)
```

Maestro de Departamentos

```
Create table Depto (
CIA                 VARCHAR2(2) NOT NULL,
DEPTO               VARCHAR2(3) NOT NULL,
DESCRIPCION      VARCHAR2(30),
 Constraint Pk_Depto primary key (cia,depot)
)
```

Maestro de Planillas

```
Create table planilla (
CIA               VARCHAR2(2) NOT NULL,
CODPLA          VARCHAR2(2) NOT NULL,
DESCRIPCION VARCHAR2(30),
Constraint Pk_planilla Primary key (cia,codpla)
)
```

Maestro de Empleados

```
Create table Mae_Emp (
  CIA                   VARCHAR2(2) NOT NULL,
  EMPLE                 VARCHAR2(6) NOT NULL,
```

```
 NOMBRE          VARCHAR2(80),
 PUESTO          VARCHAR2(4),
 F_INGRESO       DATE,
 F_EGRESO        DATE,
 SALARIO         NUMBER(9,6),
 ESTADO          VARCHAR2(1) CHECK (ESTADO IN ('A', 'I', 'S')),
 HORA            VARCHAR2(2) Not null,
 F_NACIMI        DATE,
 BASE            NUMBER(10,2),
 CodPla          VARCHAR2(2) not null,
 DEPTO           VARCHAR2(5),
 SEXO            VARCHAR2(1),
 P_NOMBRE        VARCHAR2(20),
 S_NOMBRE        VARCHAR2(20),
 P_APELLIDO      VARCHAR2(20),
 S_APELLIDO      VARCHAR2(20),
 C_APELLIDO      VARCHAR2(20),
 Constraint Pk_mae_emp primary Key (cia, emple),
 Constraint Emp_Cia foreign key (cia) references mae_cia (Cia)
 Constraint Planilla foreign Key (cia, CodPla) references Periodo_Plani (Cia,
CodPla),
)

Create table Foto (( CIA VARCHAR2 (2) NOT NULL,
  CODPLA VARCHAR2(2) NOT NULL,
  EMPLE VARHCAR2(6) NOT NULL,
  FOTO  LONG
  Constraint Pk_Foto Primary key (cia,codpla,emple)
)
```

APÉNDICE B: CÓDIGO FUENTE EN PASCAL QUE EJECUTA LAS LIBRERÍAS DEL VERIPRINT.

```
unit Unit1;

interface
uses
  Windows, Messages, SysUtils, Classes, Graphics, Controls, Forms,
Dialogs,
  StdCtrls;

{ Definición de tipos para la captura de la información del Veriprint}
type
 bii_time =record
       sec :byte;
       min :byte;
       hour:byte;
       flag:byte;
       end;

 bii_date = record
     day :byte;
     month:byte;
     year :short;
     end;

 bii_verify = record
       id:integer;
       key:byte;
       flag:byte;
```

```
      filler:array [1..2] of byte;
      time: bii_time;
      date: bii_date;
 end;

{estructura para los template }
 temp = record
       m_id:byte;
         m_employee_id:word;
         m_password:word;
       m_sensor_version:byte;
         m_template_version:byte;
         m_name:array [1..16] of byte;
         m_finger:byte;
         m_admin_level:byte;
         m_schedule:byte;
         m_security_thresh:byte;
         m_noise_level:array [1..18] of char;
         m_corramb:array [1..3] of char;
         m_ihcore:array [1..3] of char;
         m_ivcore:array [1..3] of char;
         m_reserved:array [1..3] of char;
       m_inphase:array [1..2048] of char;
 end;

 procedure leer;
implementation
procedure bii_buffer;STDCALL external 'C:\TEMP\BIIDLL.DLL' name
'_bii_buzzer@0'
```

```
function get_queue(var queue:bii_verify;offset:integer;n:integer):integer
;STDCALL; external 'C:\TEMP\BIIDLL.DLL' name '_get_verify_queue@12'
function dowload_text (mensaje:string ; modo:integer):integer;STDCALL
external 'C:\TEMP\BIIDLL.DLL' name '_download_text@8'
function get_vq_readptr(var queue:bii_verify;offset:integer;n:integer):integer
;STDCALL; external 'C:\TEMP\BIIDLL.DLL' name
'_get_vq_from_readptr@12'
function baud_rate(baud:integer):integer;STDCALL external
'C:\TEMP\BIIDLL.DLL' name '_set_baud_rate@4'
function select_network(network:integer):integer;STDCALL external
'C:\TEMP\BIIDLL.DLL' name '_select_network_id@4'
function upload_template(id:integer;templade:temp):integer;STDCALL
external 'C:\TEMP\BIIDLL.DLL' name '_upload_template@8'
function
upload_temp(id:integer;index:integer;templade:temp):integer;STDCALL
external 'C:\TEMP\BIIDLL.DLL' name '_upload_template_dup@12'
{$R *.DFM}


procedure leer;
var
valor :array [1..7] of bii_verify;
top,num,retorno :integer;
begin
   top:=0;
   num:=7;
   retorno:=get_queue(valor[1],top,num);
end;
end.
```

This document was created with Win2PDF available at http://www.daneprairie.com.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.