CONSEJO FEDERAL DE INVERSIONES

PROVINCIA DE MENDOZA

Programa para la Redefinición e Instrumentación de Nuevos Servicios - Estudio de Factibilidad para la Aplicación de Biotecnología

PRIMER INFORME PARCIAL

AGOSTO 2002

Autoridades

PROVINCIA DE MENDOZA	CONSEJO FEDERAL DE INVERSIONES
GOBERNADOR DE LA PROVINCIA Ing. Roberto Iglesias **Secretario Administrativo Legal y Técnico** Dr. Claudio Romano	**SECRETARIO GENERAL** Ing. Juan José CIÁCERA **Directora de Coordinación** Ing. Marga VELÁSQUEZ CAO **Jefa de Área Red de Información** Lic. Alicia Noemí Rapaccini

Autor

A.U.S. Julio César Monetti

Colaboradores

Ing. Gabriela Loncharich

Cont. Susana Beatriz Mora

Índice General

Índice General 4

Resumen 6

Introducción 7

Qué Es La Autenticación Biométrica ? 7

Contenido 9

Relevamiento De Antecedentes De Aplicación De La Tecnología Biométrica Y Autenticación De Identidad En Organismos Públicos 10

Centros De Estudio 10
Instituto Provincial De La Vivienda 11
Funciones Del Organismo 11
Relevamiento De La Estructura General 11
Sistema De Verificación Implementado 12
Observaciones 13
Software Utilizado 14
Entrevista 16
Rectorado Universidad Nacional De Cuyo 28
Universidad De Odontología De La Universidad Nacional De Cuyo 32
Otros Antecedentes 38

Determinación Del Área De Estudio Y Centros Usuarios Para Detectar Aquellos Procedimientos Que Necesitan De La Identificación Biométrica 44

Penitenciaría De La Provincia De Mendoza 44

Investigación De Productos Existentes En El Mercado 48

Marco Teórico 57

Técnicas De Autenticación Biométrica 57

Huella Dactilar 64
Huellas Dactilares . Desarrollo Técnico 65
Geometría De La Mano 85
Firma Digital Y Certificados Digitales 87
Código De Barras 102
Comparación De Métodos Biométricos 104

Conclusiones 107

Referencias Bibliográficas 108

Resumen

Antes de avanzar hacia la definición de los nuevos esquemas de procedimientos de modernización en la identificación de personas, es importante exponer las diferentes modalidades actuales de trabajo en dicho tema, ya que en función de ellas se definirán las características propuestas.

En primer lugar ha sido relevada la estructura administrativa de las áreas en estudio: algunas dependencias de la Administración Pública Provincial. Tal relevamiento tiene como objetivo identificar procedimientos que requieran la utilización de identificación biométrica. Así también ha sido relevado el mercado de insumos para la recolección de datos e identificación biométrica existente.

Complementando este relevamiento, ha sido necesaria la creación de un marco teórico que permitirá la interpretación y asimilación del mismo.

En esta primera etapa de recolección de datos se han aplicado las siguientes técnicas para obtener los mismos:

1. Entrevistas
2. Investigación Bibliográfica
3. Observación directa
4. Revisión de Registros

Introducción

En la primer etapa del presente trabajo se procuró asimilar el concepto de **tecnología biométrica**, concluyendo en un marco teórico, el cual, en combinación con un relevamiento general de aplicaciones de reconocimiento de personas, como así también de las necesidades de los distintos organismos relevados, permitirá realizar un estudio de factibilidad sobre la creación y formalización de procedimientos que hagan uso de ella.

Los límites que se han encontrado en el desarrollo del relevamiento han sido aquellos impuesto por el área donde se realizó el estudio, en cuanto al no acceso a la información total requerida.

Qué es la Autenticación Biométrica ?

*La **Autentificación Biométrica** consiste en la verificación de la identidad de un sujeto, basándose en ciertos elementos morfológicos que le son inherentes y que solo se dan en ese sujeto.* Es decir, mediante la **Autentificación Biométrica** proponemos recopilar información acerca de un rasgo distintivo de una persona (su voz, su huella dactilar,...) para luego ser capaces de comparar esa muestra con otra, tomada normalmente en ese mismo instante, y poder averiguar si existe una correspondencia entre ellas o no.

En el ámbito de las tecnologías de seguridad, uno de los problemas fundamentales a resolver es la necesidad de autenticar de forma segura (y única) la identidad de las personas que pretenden acceder a un determinado servicio o recinto físico. De este modo, surge la **biometría**, también conocida como técnicas de identificación biométrica.

Estas técnicas de identificación biométrica, frente a otras formas de autenticación personal como el uso de tarjetas o ***PINes*** (Personal Identification Number, o número de identificación personal, como el usado en cajeros automáticos), cuentan con la siguiente ventaja: **los patrones no pueden perderse o ser sustraídos**, ni pueden ser usados por otros individuos en el caso de llegar a tener acceso a nuestra tarjeta personal y/o PIN. Debemos tener en cuenta que gran parte de los sistemas de autenticación actuales están basados únicamente en el uso de una tarjeta personal y/o un PIN. Así, por ejemplo, es habitual que en el caso de pérdida o sustracción de una cartera, cualquiera pueda hacerse pasar por uno mismo, ya que es extremadamente frecuente tener junto a las tarjetas personales, el/los número/s secreto/s (PINes) apuntado/s en la misma. Éste problema de suplantación de identidad quedaría totalmente resuelto con el uso de patrones biométricos como medio de autenticación personal.

Contenido

1. Relevamiento de antecedentes de aplicación de la tecnología biométrica y autenticación de identidad en organismos públicos.

2. Determinación del área de estudio y Centros Usuarios para determinar aquellos procedimientos que necesitan de la identificación biométrica (un relevamiento general de procedimientos y funciones).

3. Investigación de los productos existentes en el mercado

Relevamiento de Antecedentes de Aplicación de la Tecnología Biométrica y Autenticación de Identidad en Organismos Públicos

Centros de Estudio

Previo al diseño del nuevo sistema se tomarán tres puntos de estudio que aportarán valiosa información acerca de la identificación de personas, en lo referente a lo tecnológico, como así también en lo operativo.

Instituto Provincial de la Vivienda

Funciones del Organismo

Proveer al desarrollo social de la Provincia de Mendoza procurando una solución habitacional digna, al alcance de los sectores de la población que requieren apoyo del Estado a través de una política descentralizada y el otorgamiento de créditos accesibles.

Relevamiento de la Estructura General

Ubicación Física: Se encuentra ubicado en calle Lavalle 92. Ciudad.

Cuenta con 380 empleados entre Personal de Planta, Personal Contratado y Pasantes, organizados bajo 2 Secretarias y 5 Gerencias

- Secretaría Técnica
- Secretaría Administrativa
- Gerencia de Evaluación
- Gerencia de Seguimiento
- Gerencia Financiera
- Gerencia de Regularización Dominial
- Gerencia de Planificación Estratégica

Todo el personal cumple con el mismo horario laboral que se extiende desde las 7:30 hs hasta las 14:00 hs.

Sistema de Verificación Implementado

El Instituto implementó un Sistema de Control de Asistencia con reconocimiento Biométrico en enero de 2001. El reconocimiento realizado esta basado en las características geométricas de la mano, para lo cual se utiliza el dispositivo **Hand Push 2000**, provisto por la Empresa DATEC.

Este dispositivo es operado como una estación de control independiente ubicado en la Planta Baja del Edificio. A través del cableado (ver Layout) se conecta a una computadora que almacena toda la información registrada dispuesta en la Oficina de Personal.

La función principal del verificador en el Instituto consiste en el **registro de puntualidad y asistencia** de los empleados del instituto. Dentro de las funciones secundarias capaz de desarrollarse se observa el manejo de la información de personal, listados de tardanzas, listados de ausencias, inasistencias justificadas, personal presente, horas extras.

En cuanto a la administración de este tipo de Identificador Biométrico los usuarios no han registrado ni observado inconvenientes ni fallas en el periodo de **1 año y 6 meses** periodo en que se lleva utilizando el Dispositivo. Tampoco es necesario ningún tipo de mantenimiento periódico del dispositivo, lo cual permite una completa independencia del proveedor.

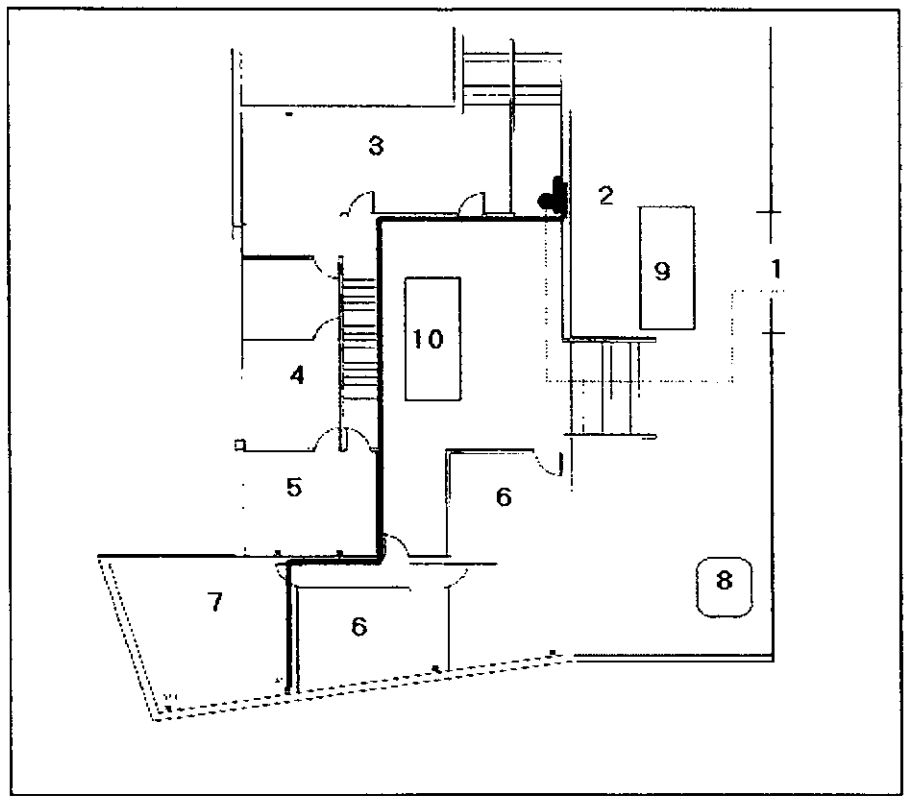
Observaciones

Durante la implementación y etapa de prueba del Verificador Biométrico, el número de empleados existentes en el Instituto provocó embotellamientos y alguna disconformidad en los usuarios durante las horas picos de 7:30hs y 14:00hs. Por estas razones se debió **calibrar el margen de error permitido** por el identificador de manera tal de conseguir una mayor fluidez en el registro de las personas.

Actualmente el personal se ha adaptado completamente a este tipo de identificación y se encuentran conformes con las ventajas obtenidas del mismo.

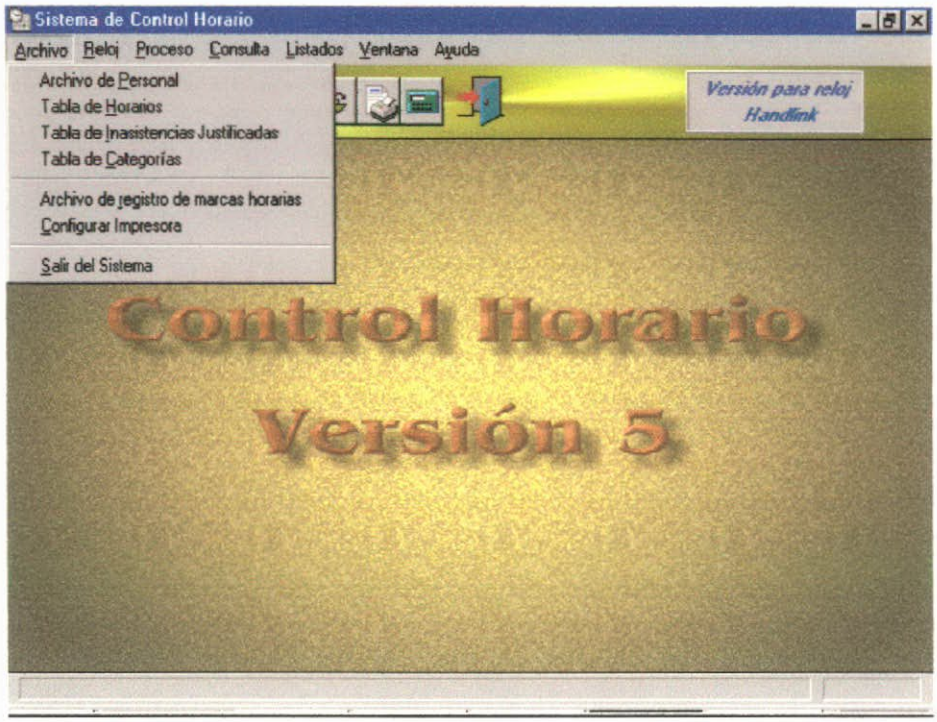
Layout del IPV

Sector : Planta Baja, Lugar de Ubicación del Identificador Biométrico



Software Utilizado

El Paquete de Software utilizado por el IPV fue provisto por la Empresa DATEC, elaborado a medida para el Instituto Provincial de la Vivienda. Tiene una Interfaz completamente amigable para el usuario y de fácil operación. Basado en menúes permite registrar el ingreso y egreso del Personal, además de generar información individual de cada empleado.


Sistema de Control Horario
Archivo Reloj Proceso Consulta Listados Ventana Ayuda
Archivo de Personal
Tabla de Horarios
Tabla de Inasistencias Justificadas
Tabla de Categorías
Archivo de registro de marcas horarias
Configurar Impresora
Salir del Sistema
Versión para reloj Handlink
Control Horario
Versión 5


Sistema de Control Horario
Archivo Reloj Proceso Consulta Listados Ventana Ayuda
Versión para reloj Handlink
Tabla de Horarios
General
Horario Descripcion
1 PLANTA Y ADSCRIPTOS
2 CONTRATADOS
3 PASANTES
4 GUARDIA
5 POLICIA
6 EXCEPCION
7 SOTO
8 MUÑOZ
9 HORARIO NORMAL RUFENERVIVANTE
10 LOPEZ MONICA
11 RIVEROS
12 LOPEZ
Insertar
Modificar
Eliminar
Ayuda
Cerrar

Entrevista

Organización	*Instituto Provincial de la Vivienda*
Lugar de Realización	Instituto Provincial de la Vivienda
Fecha	10 de Julio de 2002
Codificación de la Entrevista	Toma de notas
Entrevistado	Rubén Lucero
Funciones	Gerente de Personal
Realizada por	Gabriela Loncharich

Objetivos de la Entrevista

- Definir el mecanismo de autenticación de personas utilizado en la organización.
- Registrar una comparación entre todos los métodos que se han utilizado en el Instituto
- Evaluar el costo beneficio del sistema implementado.
- Determinar el rendimiento , ventajas y desventajas del método utilizado.
- Definir posibles fallas del mecanismo.
- Evaluar la adaptación del personal al sistema de autenticación implementado en la Organización

Desarrollo de la Entrevista

Funcionamiento del Dispositivo de Autenticación Utilizado por el IPV

Dispositivo de Verificación de la Geometría de la mano, Hand Punch 2000.

El funcionamiento básico del mecanismo "Verificación de la Geometría de la mano" se basa en un dispositivo lector con unas guías que marcan la posición correcta para la lectura de la palma de la mano. Una vez que la mano está correctamente situada, unas cámaras toman una imagen superior y otra lateral, de las que se extraen ciertos datos (anchura, longitud, área, determinadas distancias...), estos se comparan con los almacenados en la base de datos y de acuerdo al resultado de este análisis se valida o no al usuario.

Software Utilizado para Implementación Sistematizada

El software fue brindado por DATEC, junto con el dispositivo, este software incluye un menú en el que además del registro de entrada y salida del personal, se puede optar por generación de listados con, información personal del empleado, Licencias otorgadas, Tardanzas, etc.

Recursos Necesarios para su Implementación

- El Dispositivo lector
- Una PC (características de la misma).
- Cableado desde el dispositivo lector a la PC.

Cual el Costo de la Tecnología Implementada

Precio del Lector U$S 5000, esto incluye además el software utilizado.

Precios registrados durante 01/2001.

Tiempo de Vida del Lector

Se desconoce.

Servicio Técnico Necesario para su Mantenimiento. Se Necesita una Calibración Periódica del Escáner?

Existe una persona encargada del control del dispositivo, esta persona maneja una clave única que lo autoriza a acceder a las funciones del dispositivo. Dentro de estas funciones se incluye tareas como actualizar la fecha o poner en hora el reloj ya que suele adelantarse o atrasarse de vez en cuando, dar de altas a usuarios nuevos realizar modificaciones de los datos registrados, evaluar el margen de error necesario para cada empleado, etc.

Tipo de Administración o Mantenimiento Necesario para el Sistema

Se realiza mensualmente un servicio técnico, llevado a cabo por el personal de DATEC. Principalmente se encarga del mantenimiento de la base de datos, y mantenimiento del software provisto.

Tiempo Medio entre Fallas

No se han observado fallas técnicas del dispositivo de Verificación de la Geometría de la mano durante el tiempo que lleva implementado, aproximadamente 1 año y 6 meses.

Problemas Detectados sobre este Mecanismo (olvidos del personal al ingreso o egreso, temperatura, heridas, crecimiento de la mano, etc.)

El principal problema se ha observado durante la primera etapa de implementación del dispositivo, se observaron algunos inconvenientes en la adaptación del usuario al nuevo mecanismo, empleados que se registraban con guantes, o anillos que entorpecían el funcionamiento correcto de este mecanismo.

Otro problema que se planteo fue el olvido de algunos empleados de registrarse al retirarse del Instituto, esto provocaba que se marcara como hora de salida, la hora de ingreso del día siguiente cuando el empleado llegaba nuevamente al Instituto con lo que se corrían todos los horarios del empleado. Frente a este problema se decidió controlar por fecha y en caso de algún olvido se registran las horas mínimas laborales necesarias, de manera que si se hicieron horas extras estas se pierden.

Además se planteo problemas con mujeres embarazadas, al agrandarse o inchárseles las manos, para ello se debió dar de alta a la empleada nuevamente pero con su código original, lo cual sobrescribe el anterior.

Ventajas Obtenidas Frente al Mecanismo Anterior

El mecanismo anterior se basaba en registrar en una planilla existente el horario de ingreso y egreso del Instituto. Junto a la firma de la persona. Dicha planilla se encontraba en la oficina de Personal, para un control de lo registrado por cada persona. La instalación de dispositivo de Verificación de la Geometría de la mano, suplió completamente al método anteriormente detallado. Y se observa que con este se ha conseguido una mayor seguridad en los datos registrados, mayor eficiencia, rapidez en el registro del personal y un control mas personalizado sobre cada empleado del Instituto.

Como se Llevaron a Cabo el Alta de los Usuarios. Alta de datos (palma de las manos)

El alta de los usuarios se realizo de la siguiente manera:

Se registró un código identificativo de cada empleado, luego se debió colocar la palma de la mano 3 veces, para detectar un margen de error posible, de esta manera quedaba registrado el empleado en el sistema.

Existe un Límite en la Cantidad de Usuarios Permitidos?

Depende de la capacidad de la computadora utilizada, (consultar al proveedor "Datec").

Tiempo de Procesamiento

El dispositivo se encuentra en línea de manera que a medida que los empleados ingresan al instituto o se retiran del mismo, se observan por pantalla inmediatamente.

La Interface que Ofrece el Sistema Provisto es Amigable para el Usuario?

La interface es sencilla y de fácil adaptación, con un formato de menú que expone todas las posibles alternativas de operación por lo que no se ha observado descontento con ella por parte del usuario.

Conclusión de la Entrevista

La entrevista tiene una estructura libre, desarrollada con preguntas cerradas para la obtención de respuestas concretas; y en preguntas abiertas para conocer el funcionamiento de la empresa, siguiendo el lineamiento de los temas.

- El dispositivo puede utilizarse con un margen de error que viene definido por defecto en el software o puede definirse individualmente para cada persona en casos particulares.

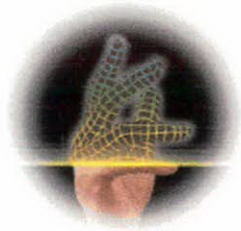
- A la hora de la selección de un dispositivo autenticador se aprobó el de Verificación de la geometría de la mano debido que este ofrecía menos inconvenientes en cuanto al margen de error aceptado (la forma de colocación de la mano ofrece el margen de error que el usuario desee) a diferencia del sistema de huella, el cual ocasiona mayores inconvenientes si la huella no se toma correctamente.

- No se han generado problemas con las condiciones ambientales.

- Se observo que el sistema utilizado con anterioridad (Registro de firma de cada empleado), generaba descontento en el personal, debido a que durante el horario clave de ingreso o egreso se generaba un embotellamiento de personal.

- Se observo a los usuarios completamente satisfechos con el sistema de autenticación de Verificación de la Geometría de la mano provisto.

Verificador de la Geometría de la Mano. Dispositivo utilizado en IPV. Sistema de Control de Asistencia



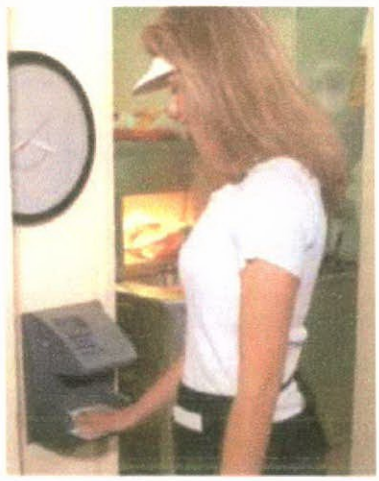
Beneficios y Características

- Sistema Biométrico identifica características geométricas de la mano evitando que chequeen asistencia unos por otros
- Reduce sus costos de nómina (hasta en un 5%) evitando el pago por horas y días no laborados
- Reduce costos de control de asistencia y cálculo de pre-nómina
- Ahorra tiempo y dinero en elaboración de tarjetas y gafetes
- Facilita la aplicación de políticas de puntualidad y asistencia
- Bajo costo de mantenimiento ya que no cuenta con piezas mecánicas
- Conexión por medio de red serial, Ethernet, enlaces digitales y módem
- Trabaja aún con fallas de energía eléctrica
- Compatible con cualquier sistema de nómina

Software ATiempo 100

Incluye las siguientes características

- Calcula tiempo laborado, tiempo extra, retardos, faltas, omisiones, etc.



- Lleva control de vacaciones, incapacidades, etc.
- Genera tarjetas de registro de entrada/salida
- Infinidad de informes y reportes, Kardex
- Recupera registros de asistencia en línea a través de una red serial, módem, Ethernet o redes corporativas (inalámbricas, RDI, Frame Relay, etc.)
- Exportación de incidencias a cualquier sistema de nómina
- Control de comedor
- Cambio de turno automatizado
- Costo aproximado **$1,165.00 USCy + IVA.**

Hand Punch 2000:

Incluye las Siguientes Características

- Capacidad de 512 usuarios
- Comunicación serial RS-232, capacidad de comunicación por módem o red Ethernet
- Teclas de funciones programables
- Costo aproximado $1,630.00 USCy + IVA

Hand Punch 3000:

Incluye las Siguientes Características

- Capacidad de 512 usuarios, con posibilidad de crecimiento hasta 32,512 usuarios
- Comunicación serial RS-422, capacidad de comunicación por módem o red Ethernet
- Puertos disponibles para control de accesos, torniquetes, sirenas y semáforos
- Teclas de funciones programables
- Costo aproximado $2,060.00 USCy + IVA

Los precios son en dólares (USCy), sujetos a cambio sin previo aviso

Opciones de Equipo

- Memoria para 9,728 usuarios y hasta 32,512 usuarios (por equipo) (HP3000 únicamente)
- Módem
- Tarjeta de red Ethernet (LAN y WAN)
- Adaptador de 12Vdc
- Fuente de poder con batería de respaldo
- Control para acceso de puerta o torniquete (HP3000 únicamente)
- Lectura de clave personal a través de tarjeta (proximidad, código de barras o magnética) (HP3000 únicamente)

Opciones de Software

- ATiempo 500, opción económica del AT100
- PunchNet G, recupera registros de entrada y salida
- Firmas, para control de firmas de "Procesados Libres Bajo Caución" Winax, para control de accesos

Rectorado Universidad Nacional de Cuyo

La elección del Rectorado de la Universidad de Cuyo como un punto de estudio de nuestra investigación se debe a que se ha encontrado una valiosa aplicación de la identificación biométrica.

Rectorado Universidad Nacional de Cuyo.

Organización	*Rectorado de la Universidad Nacional de Cuyo*
Lugar de Realización	Rectorado
Fecha	1 de Julio de 2002
Codificación de la Entrevista	Toma de notas
Entrevistado	Matías Grintal
Funciones	Jefe de Personal
Realizada por	Gabriela Loncharich

Objetivos de la Entrevista

- Definir el mecanismo de autenticación de personas utilizado en la organización.
- Registrar una comparación entre todos los métodos que se han utilizado en el Instituto
- Evaluar el costo beneficio del sistema implementado.

- Determinar el rendimiento , ventajas y desventajas del método utilizado.
- Definir posibles fallas del mecanismo.
- Evaluar la adaptación del personal al sistema de autenticación implementado en la Organización.

Desarrollo de la Entrevista

Funcionamiento del Dispositivo de Autenticación Utilizado por el Rectorado.

Identificador Volumétrico Hand Punch 3000

El funcionamiento es idéntico al desarrollado en el Instituto IPV.

Software Utilizado para Implementación Sistematizada.

El Rectorado no compró un software con el dispositivo.

Toman el archivo plano generado por el identificador y lo procesan en un sistema diseñado por el personal de sistemas del Rectorado. Dicho Sistema esta generado en FOXPRO.

Cual es la Empresa Proveedora del Identificador.

El rectorado fue provisto por la Empresa DATEC.

Recursos Necesarios para su Implementación

- El Dispositivo lector

- Una computadora.
- Cableado desde el dispositivo lector a la computadora.

Cual el Costo de la Tecnología Implementada

El precio que se abono por el identificador sin software adicional fue de U$S 5000 aproximadamente en el año 1999.

Tiempo de Vida Medio del Lector

El personal que maneja el dispositivo desconoce un tiempo de vida.

Se han Observado Fallas en el Dispositivo?

Se han observado varias fallas técnicas del dispositivo de Verificación de la Geometría de la mano durante el tiempo que lleva implementado.

El dispositivo en varios ocasiones se apagaba y no funcionaba. También se observaron irregularidades en el funcionamiento principalmente durante los días de lluvia. En una oportunidad fue necesario cambiar el dispositivo por las razones anteriormente señaladas, ya que no se pudo lograr un correcto funcionamiento del mismo.

Cual era el Mecanismo Utilizado con Anterioridad al Verificador Biométrico

Y cuales las ventajas obtenidas frente al mecanismo anterior.

Antes de la biometría implementada, el personal se registraba mediante tarjetas magnéticas, lo cual presentaba las desventajas propias de este sistema antes mencionadas (cualquiera podía registrar teniendo la tarjeta).

El sistema biométrico ayudo a solucionar esta desventaja, ya que con el es imposible que alguien se registre en nombre de otra persona.

Como se Llevaron a Cabo el Alta de los Usuarios para Cargar la Base de Datos?

Se registró un código identificativo de cada empleado, luego se debió colocar la palma de la mano 3 veces, para detectar un margen de error posible, de esta manera quedaba registrado el empleado en el sistema. Idéntico al Sistema del IPV.

Quienes Utilizan este Sistema de Identificación?

Se implemento para validar al personal no docente que trabaja en el Rectorado de la Universidad Nacional de Cuyo.

Cual es el Tiempo de Verificación, Validación y Procesamiento Necesario para cada Registro?

El dispositivo se encuentra en línea de manera que a medida que los empleados ingresan al Rectorado o se retiran del mismo, se observan por pantalla inmediatamente.

Universidad de Odontología de la Universidad Nacional de Cuyo

Organización	*Facultad De Odontología de la Universidad Nacional De Cuyo*
Lugar de Realización	UNC – Odontología
Fecha	02 de Agosto de 2002
Codificación de la Entrevista	Toma de notas
Entrevistado	Nicolás García
Funciones	Jefe Informática
Realizada por	Gabriela Loncharich

Objetivos de la Entrevista

- Definir el mecanismo de autenticación de personas utilizado en la organización.
- Registrar una comparación entre todos los métodos que se han utilizado en el Instituto
- Evaluar el costo beneficio del sistema implementado.
- Determinar el rendimiento , ventajas y desventajas del método utilizado.
- Definir posibles fallas del mecanismo.
- Evaluar la adaptación del personal al sistema de autenticación implementado en la Organización

Desarrollo de la Entrevista

Funcionamiento del Dispositivo de Autenticación Utilizado por la Facultad de Odontología

Dispositivo de Verificación de la Huella Dactilar, TOUCH LOCK II–IDENTIX.

EL dispositivo funciona colocando un dedo a elección de la mano deseada, 3 láser ubicados dentro del dispositivo toman datos de 3 capas de la epidermis, musodermis, endodermis, con lo que arma un mapa de datos al que agrega además la posición de colocación del dedo. Esta información es comparada con la registrada en la base de datos y en caso de no coincidir las 3 capas, se rechaza la identidad del usuario. Caso contrario se acepta y permite la validación del mismo.

Cual es la Empresa Proveedora del Dispositivo?

Proveedor : Tapia Computación.

Domicilio: Dorrego 669. Dorrego-Guaymallén.

Software Utilizado para Implementación Sistematizada.

Se obtuvo un software junto con el dispositivo, provisto por el mismo proveedor del Verificador de Huella Dactilar, el mismo trabaja bajo DOS y permite además del registro de horario la posibilidad de generar diferentes listados, con datos de cada persona.

Función del Identificador Biométrico en la Facultad

La función principal es el Control De horario y puntualidad del personal docente y no docente de la Facultad Odontología.

Recursos Necesarios para su Implementación

- El Dispositivo lector
- Una PC (características de la misma).
- Cableado desde el dispositivo lector a la PC. EN este caso se uso se utilizaron 70 metros de cable par trenzado , para la conexión.

Cual fue el Costo de la Tecnología Biométrica Implementada

El en momento de adquirido, año 1999, el dispositivo costo U$S 7000, esto incluye además el software utilizado.

Tiempo de Vida del Lector

Hasta el momento no han tenido inconvenientes con el verificador, y desconocen el tiempo de vida que tenga.

Servicio Técnico Necesario para su Mantenimiento. Se Necesita una Calibración Periódica del Escáner?

No se necesita ningún tipo de servicio periódico para mantenimiento del dispositivo. Cuando resulta necesario el encargado del aparato en caso de desconfigurarse, lo pone en hora al reloj , que suele ser el único problema puntual, si se corta la energía por mucho tiempo.

Se Detectaron Fallas del Dispositivo, en el Tiempo de Uso del Mismo?

No se presentaron fallas en el tiempo de implementado el dispositivo aproximadamente en 4 años de uso continuo.

Cuales son los Inconveniente Detectados sobre este Mecanismo?

En cuanto a los problemas detectados, al implementarse el dispositivo fue la adaptación de los usuarios al mismo, debido a que estos venían de utilizar un sistema de reloj crono, y por medio de tarjetas registraban el ingreso o egreso. Los usuarios no deseaban el cambio de mecanismo. Por lo tanto se mostraban bastantes desconformes, y mas aun cuando al registrar su huella debían hacerlo repetida veces para ser validados. Hay que tener en cuenta que este mecanismo ofrece la posibilidad de utilizar 2 huellas, en caso de no funcionar alguna se tiene la alternativa.

En general los usuarios solían plantear una serie de excusas, asignándole la culpa al dispositivos de las tardanzas. Como que estuvieron un rato intentando registrarse y no funcionaba.

En cuanto a las irregularidades de registro por olvido que se presentan, quedan registrado y se pasa en informes.

Ventajas Obtenidas Frente al Mecanismo Anterior

El sistema anterior utilizado se basaba en un reloj crono, a través de tarjetas.

Este sistemas presentaba los problemas de fraude conocidos, como la marca de tarjetas de personas que ya se han retirado o que nunca asistieron. El control obtenido con el Verificador, es completo e imposible de violar. La automatización conseguida, aumenta la rapidez y la eficiencia obtenida.

Como se Llevaron a Cabo el Alta de los Usuarios?

Se dividió al personal en grupos y se fue tomando la huella de cada uno en tandas. Se ingreso un código identificativo para la persona y luego esta debía colocar la huella del dedo seleccionado 5 veces para ser registrado.

Tiempo de Reconocimiento y Validación de la Huella

El tiempo de reconocimiento es casi inmediato. Y el tiempo de procesamiento es mínimo , al momento que la persona se esta registrando se puede ver por pantalla el registro.

Qué tipos de Identificadores se Evaluaron al Momento de Decidir el Dispositivo a Implementar?

La facultad evalúo entre 3 alternativas:

- El escáner de iris.
- El identificador volumétrico.
- EL identificador de Huella Digital.

Por qué se Seleccionó este Tipo de Identificador Frente a los Evaluados?

Se selecciono el identificador de Huella Dactilar, por que no se encontraron problemas puntuales como se presentaban con el resto de los dispositivos. Como el planteado con el identificador volumétrico "Geometría de la Mano", que generaba algunos problemas de funcionamiento en el lugar de implementación. El escáner de iris, presenta un grave problema si las personas en ves de acercarse al dispositivo, se apoyan en el, ya que esto puede provocar infecciones o contagios, como conjuntivitis entre los usuarios.

Observaciones

El Verificador de la Huella Digital, utilizado el Facultad de Odontología, no presentó en el tiempo de vida que tiene problemas de reconocimiento. Nunca a confundido huellas entre dos personas, ni a validado a individuos incorrectamente.

Ha ofrecido el 100% de fiabilidad en el tiempo de uso.

Otros Antecedentes

Artículo Periodístico Encontrado en Internet. Publicación de Divulgación Científica Chilena.

Isapres reemplazan con huella digital la compra de bonos para atención médica.

Santiago, Chile. (julio 2000). El sistema ha sido desarrollado por la empresa ATESA.

ATESA es una sociedad anónima cerrada orientada a prestar servicios de "transacciones electrónicas" en el sector de la salud en Chile (en primera instancia). Sus socios son Adexus y las isapres Consalud, Banmédica y Promepart.

ATESA desarrolló el servicio Mediline para las transacciones electrónicas entre los prestadores médicos (consultas, laboratorios, centros hospitalarios etc.) y los aseguradores de salud (Isapres, Fonasa, etc.), que facilita y agiliza los trámites asociados al uso de los seguros de salud.

Hay 3 isapres adscritas a Mediline: Consalud, Banmédica y Promepart. Juntas atienden a 1 millón 700 mil beneficiarios, 50 % de la población inscrita en Isapres. Mediline se desarrolla en una modalidad evolutiva a partir de enero de 2000.

Servicio Mediline Mediline opera desde un terminal computacional ubicado en las oficinas del prestador de salud, el cual se conecta a

través de ATESA con las Isapres que estén adscritas a este servicio. El beneficiario (paciente) acude al prestador médico que dispone del servicio ATESA. El beneficiario se identifica por medio de su número de RUT y su huella dactilar.

La transacción se envía a la Isapre correspondiente, solicitando el monto de copago (diferencia que no cubren el plan de salud) por la atención requerida (consulta, exámenes, etc). El beneficiario paga sólo el copago directamente al prestador médico y recibe la atención, ya que el monto cubierto por el seguro (bonificación) es informado y reconocido por el asegurador mediante las transacciones electrónicas provistas por ATESA.

Enrolamiento Para usar el "bono electrónico ATESA", el beneficiario de la Isapre adherida debe enrolarse. Para enrolarse, el beneficiario se identifica con su Cédula de Identidad (libreta de familia o certificado de nacimiento, para menores de edad), ingresa sus datos y registra sus huellas dactilares en una base de datos de ATESA.

¿Donde se enrola? En las oficinas de las Isapres y en los puntos de atención médica adheridos. Ventajas para el beneficiario Menos trámites y ahorra tiempo, ya que acude directamente al prestador médico, sin necesidad de tener que llevar un bono o acudir a la Isapre a cobrar el reembolso. Seguridad, lectura de huella dactilar (identificación biométrica), impide suplantaciones.

Ventajas para los prestadores de salud Menos trámites de "bonos electrónicos ATESA", al liquidarse directamente en el terminal y enviarlos vía electrónica a la Isapre correspondiente. Facilidad para cobrar honorarios o facturas, al solicitar abono en cuenta bancaria. Información on line del estado de pagos de cada liquidación y abono a cuenta bancaria. Información de atenciones entregadas, valores recibidos y los montos adeudados por Isapres.

A modo de promoción, el servicio será gratuito por el primer año de operación. Ventajas para aseguradores Disminuyen fraudes, por bonificaciones cobradas por quienes no son beneficiarios. Disminuye costos administrativos por "venta de bonos" en oficinas de atención de público. Mejora relación con prestadores, al facilitar los trámites administrativos de éstos.

Glosario Aseguradores (isapres, Fonasa, compañías aseguradoras) Beneficiarios (persona inscrita en un contrato de salud, por el cual tiene derecho a que el asegurador pague en parte los servicios recibidos como paciente) Prestadores de salud (Institución o persona que entrega servicios médicos, como consultas, exámenes de laboratorio, rayos, tratamientos, otros.

También "prestador de servicios médicos") Enrolamiento (proceso por el cual se recoge una muestra biométrica (huella digital), se convierte en datos y se almacena como patrón para posterior comparación.

Publicación de Divulgación Científica. Diario EL MUNDO (Madrid España).

Scanner de Iris. Holanda. Identificación Biométrica para Inmigrantes

El Gobierno holandés ha decidido sacar partido de los avances de la ciencia y utilizarlos para usos mucho más mundanos: **identificar inmigrantes.**

El parecido físico de muchas de las personas que llegan a las fronteras holandesas —muchas de ellas asiáticas— ha llevado al Ministerio del Interior a aprobar esta iniciativa, que a partir de junio hará que todos los inmigrantes que están en el país a la espera de recibir los certificados de residencia o trabajo, tengan que pasar por dispositivos de reconocimiento de iris, cara y voz que hará muy difícil el fraude.

Según declaró Frank van Beers, ministro del Interior a la CNN, "las fotografías de los pasaportes no son lo suficientemente buenas como determinar la identidad de una persona, especialmente si se trata de gente de otras razas, de las que no estamos acostumbrados a reconocer rasgos faciales".

Unos rasgos que no pasarán desapercibidos para los ordenadores. El escáner de iris se basa en el reconocimiento de la banda que rodea a la pupila. Entre los patrones únicos de cada individuo, y que ayudan a la identificación, se encuentran los surcos, la corona, los filamentos, los folículos, las estrías y los anillos. Esta tecnología se ha aplicado con éxito en

el reconocimiento de múltiples grupos étnicos e incluso en personas que utilizan gafas. El reconocimiento facial, por su parte, se realiza a partir del análisis de los rasgos situados en la parte superior de la cuenca de los ojos, los huesos de las mejillas y los músculos situados a ambos lados de la boca del usuario. Esto permite identificar a la persona, independientemente de su vello facial o del hecho de que lleve o no gafas.

Otros sistemas biométricos que se están utilizando para identificar a personas son las huellas dactilares, el reconocimiento de voz, la geometría de la mano, la dinámica de la firma, la dinámica de pulsación o el escáner de la retina.

Pruebas Exitosas

El sistema biométrico del gobierno holandés ya ha sido probado con éxito en Rotterdam, donde 250 inmigrantes han pasado por el escáner de iris. Los datos de cada persona se han introducido en un pequeño microchip de una tarjeta (del tamaño de una de crédito). Para comprobar la verdadera identidad de la persona, basta con introducir la tarjeta en un ordenador, sentar al individuo delante del escáner (totalmente indoloro e instantáneo) y dejar que el ordenador compruebe si los datos de la persona y los de la tarjeta son del mismo individuo.

De esta manera, la Policía espera acabar con los fraudes que se producen hasta ahora. Los inmigrantes que se encuentran en el país a la espera de regularizar la situación tienen que comparecer una vez al mes ante los

oficiales de inmigración, que se ven impotentes para determinar si la foto que aparece en el pasaporte que presentan los inmigrantes es la de la persona que lo porta.

Para el año 2003, todos los ciudadanos holandeses con carnés de identidad de la Unión Europea tendrán sus datos personales biométricos guardados en una tarjeta como la que ahora se proporciona a los inmigrantes. Estas tarjetas, equivalentes al actual pasaporte, se podrán utilizar en cualquier país de la UE, aunque la información de cada individuo no será almacenada en una base de datos, sino en cada una de las tarjetas.

Determinación del Área de Estudio y Centros Usuarios para Detectar Aquellos Procedimientos que Necesitan de la Identificación Biométrica

Penitenciaría de la Provincia de Mendoza

Relevamiento General

El creciente aumento del número de internos ha propiciado la necesidad de estudio de nuevas técnicas de seguridad. El punto de vista tradicional otorga mayor atención a los aspectos de seguridad visibles. La seguridad efectiva requiere la revaloración de un amplio número de aspectos descritos dentro del Concepto de SEGURIDAD DE ACCESO.

Relevamiento de la Estructura General.

Actualmente la Penitenciaría Provincial cuenta con 500 empleados distribuidos de la siguiente forma:

- Visitas : 10 empleados.
- Seguridad Interna: 400. empleados.
- Administración en general 90 en general.

Se utiliza un sistema de Tarjetas Mecánicas para el control de cada empleado en el Ingreso y egreso laboral de la penitenciaria y para el control de los operativos asignados. Cada empleado posee una tarjeta identificatoria que introduce en el reloj mecánico de marcado de tarjeta para registrarse.

Observación:

No se encuentran conformes con este sistema de registro, ya que no se puede asegurar que la persona que se registra sea la dueña de la tarjeta ingresada.

Distribución de Internos

La Penitenciaría tiene a su cargo **2096** internos de los cuales **781** se encuentran distribuidos en 5 unidades , el resto de los penitenciarios están autorizados para salir de la penitenciaria, y regresar de noche en algunos casos, en otros tienen libertad condicional, y no regresan a la penitenciaria.

La distribución por unidad es la siguiente.

Unidad 4: 122 internos.

Unidad 5: 84 internos.

Unidad 9 : 112 internos.

Unidad 10 : 59 internos.

Unidad extrema medida: 404 internos.

Resto : 1315 internos.

Se recomienda para continuar con la reingeniería de procedimientos de las áreas relevadas un detalle sobre:

a) Relevamiento de funciones

b) Relevamiento de Procedimientos

Visita a Internos

Los penitenciarios tienen el derecho de ser visitados **2 veces** a la semana y el derecho de decidir qué personas pueden visitarlos; para lo cual se lleva un registro de cada interno con las visitas no autorizadas por cada uno, este se revisa al llegar la visita para permitirle o no el ingreso. Dicho registro se encuentra asentado manualmente en **tarjetas de visita.**

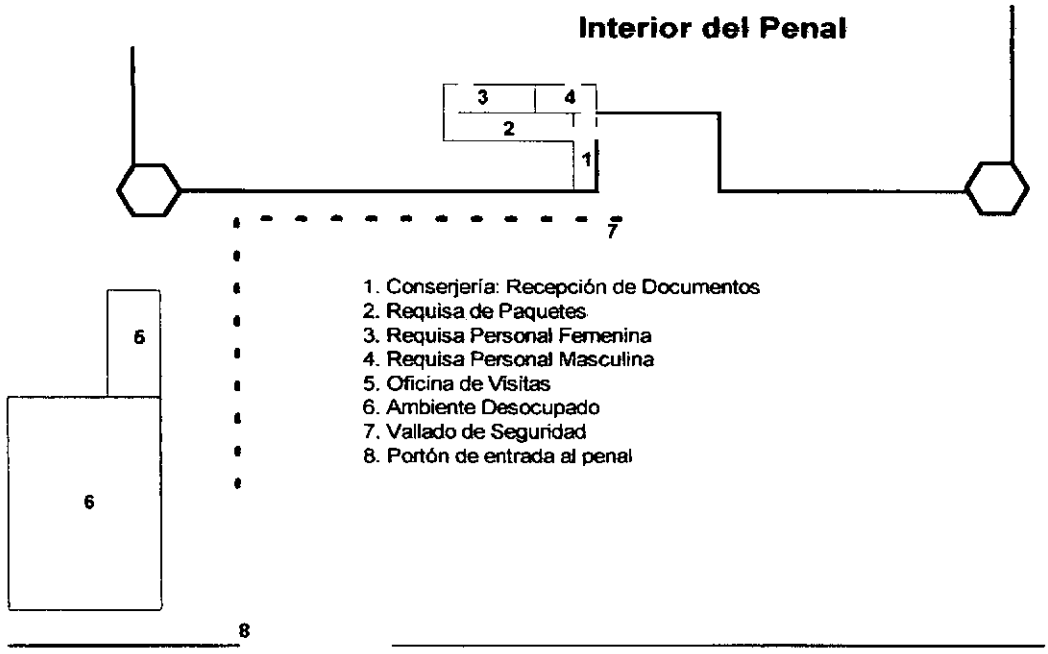
Las visitas se organizan de la siguiente manera:
La penitenciaría Provincial ordena las visitas por pabellón, para ello se le ha asignado un día a cada uno de ellos. Los días ya están establecidos, son inamovibles y permite a los familiares de los Internos conocer que día de visita le corresponde a cada uno de los penitenciarios.

Cada día se realiza un listado con los internos sancionados y para los cuales se les encuentran suspendidas las visitas. De esta manera los familiares se acercan a la penitenciaria verificar el estado del interno que desean visitar.

Circuito de Visita a Internos

Este circuito comienza cuando las visitas se organizan previamente sin intervención del personal penitenciario. Luego la visita se presenta en conserjeria (1) para ser identificado por los guardias de seguridad externa (documentación personal), a continuación la visita se presenta en la sección de requisa de paquetes donde serán examinadas sus pertenencias. Una vez

realizado este trámite la visita se presenta finalmente en la sección de requisa personal para completar este trámite.



Conclusión

Se concluye que el conjunto de procedimientos expuesto anteriormente sobre el circuito de visitas contiene varias falencias al no poseer procedimientos automatizados y formularios normalizados para registro de visitas. Se recomienda la reingeniería de procedimientos y aplicación de técnicas de identificación personal.

Investigación de Productos Existentes en el Mercado

INTEGRISYS S.A. Empresa Proveedora de Productos

Objetivos de la Demostración

- Observar el funcionamiento de los productos de recolección de datos.
- Reunir información detallada de cada uno de los dispositivos ofrecidos por la Empresa.
- Registrar precios y disponibilidad de cada dispositivos.

La empresa Integrisys S.A. ha realizado una demostración de productos en oficinas al grupo de estudios donde se ha podido observar con sumo interés una sesión de captura de datos biométricos por intermedio de un scanner de huella digital.

Con dicha entrevista el grupo concluye que el acceso a los dispositivos de captura de datos (scanners y otros similares) no resultaría tan dificultoso como se presentía anteriormente, ya que la provisión de los mismos puede ser realizada por empresas residentes en la provincia de Mendoza.

También se pudieron recabar una gran cantidad de datos técnicos los cuales han sido volcados en el apartado Marco Teórico del presente documento.

CONTAMEC S.A. Empresa Proveedora de Productos

Objetivos de la Entrevista

- Distinguir los mecanismos de autenticación existentes en el mercado.
- Reunir información detallada de cada uno de los dispositivos ofrecidos por la Empresa.
- Registrar precios y disponibilidad de cada dispositivos.
- Observar la interface para interactuar con el usuario, ofrecida por el producto.
- Registrar precios y disponibilidad de cada dispositivo.

CONTAMEC S.A. es una empresa dedicada a la fabricación e importación de insumos electrónicos para seguridad y captura de datos.

Esta empresa tiene residencia en la provincia de Mendoza, y por lo expuesto por su Gerente General, el acceso a los productos necesarios para la continuación del proyecto resultaría (como en el caso de la empresa Integrisys S.A.) altamente viable.

DATEC. Empresa Proveedora de Insumos

Organización	**DATEC**
Lugar de Realización	Necochea 589 – Cdad. Tel 4380235
Fecha	11 de Julio de 2002
Codificación de la Entrevista	Toma de notas
Entrevistado	Ingeniero Morales
Funciones	Personal encargado de DATEC
Realizada por	Gabriela Loncharich

Objetivos de la Entrevista

- Distinguir los mecanismos de autenticación existentes en el mercado.
- Reunir información detallada de cada uno de los dispositivos ofrecidos por la Empresa.
- Registrar precios y disponibilidad de cada dispositivos.
- Observar la interface para interactuar con el usuario, ofrecida por el producto.
- Consultar sobre limitaciones observadas en los procesos de autenticación.

Detalle de la entrevista

Tipos de Autenticador Ofrecidos por Datec

- Verificador de la huella Dactilar
- Verificador de la Geometría de la mano
- Escáner de Iris.

Precios de Cada Dispositivo

Los precios estimativos oscilan entre **U$S 1000** y **U$S 3000**.

Verificador de la huella dactilar y Verificador de la Geometria de la mano se aproximarían a **U$S 1800**.

Características del Dispositivo

Tiempo de Verificación: Promedio de menos de 2 segundos.

Tamaño de cada registro: Depende del dispositivo a tratar.

Verificador de la Geometría de la mano , tamaño de la plantilla de la mano 9 bytes. Los dispositivos pueden utilizarse en forma individual, o conectarse en red.

Medio de Retención de Memoria : Batería interna.

Condiciones Ambientales Necesarias para el Correcto Funcionamiento del Dispositivo

Temperatura durante la operación: Aproximadamente para los dispositivos en general es necesario una temperatura de operación entre 0° y 44°.

Humedad de operación: 95% no condensada.

La exactitud hay que evaluarla individualmente para cada dispositivo.

Cuales son las Opciones de Configuración que Brindan los Identificadores?

- Pueden ser operados como una estación de control de acceso e identificación de personas totalmente independiente.
- Pueden múltiples aparatos ser conectados dentro de una red para proveer un ambiente de control total centralizado. El control puede ser realizado a través de uno de estos dispositivos o bien a través de un computador.
- Puede ser utilizado en otro ambientes utilizando el puerto de comunicación que suele disponer cada dispositivo para poder incorporar el equipo a otros sistemas de control.

Hardware Necesario para la Implementación del Dispositivo

EL hardware va depender del tipo configuración (red, independiente, etc.) que se disponga para los dispositivos , pero siempre se consideran PCs y Cableado para conectar el verificador a la Pc como hardware imprescindible.

Es de Simple operación?

La operación de cualquiera de los dispositivos es sencilla en general.

En cuanto a los dispositivos de Verificación de la Geometría de la mano y verificación de Huella Dactilar no presentan dificultad en la operación . En cuanto al Verificador del Iris la operación es un poco mas complicada, ya que requiere mayor precisión, en cuanto a la posición del ojo, para la registración.

Ofrecen un Alto Grado de Automatización?

Todos los dispositivos de Verificación con los que trabaja DATEC ofrecen una total automatización de la operación para la cual ha sido implementado.

Consumo Energético

No existe diferencia entre los consumos de los diferentes productos.

Adaptable a Todo Ambiente?

No se registra ambientes específicos en los que los productos no funcionen

Absolutamente Aséptico?

En cuanto al verificador de Huella Dactilar y Geometría de la mano, son un poco menos higiénicos debido al constante contacto de los usuarios con el dispositivo.

El escáner de iris puede provocar contagio de infecciones si los usuarios tiene contacto con el dispositivo.

Interface Amigable con el Usuario?

Depende del software que acompañe al dispositivo.

Puede Configurarse para Uso Fijo o Portable?

Los dispositivos pueden ser trasladados. No es conveniente su continuo movimiento. Se pueden presentar problemas en el funcionamiento de l reloj en caso del verificador de la geometría de la mano, si se realizan movimientos bruscos o constantes.

Cantidad de Usuarios

Aproximadamente los dispositivos permiten a 256 usuarios con posibilidad de ampliación de hasta 27.904 en forma interna.

Adaptable a Personas con Movilidad Reducida?

El dispositivo puede colocarse en donde sea accesible a todo tipo de personas.

El Software Ofrecido Permite Algún Tipo de Actualización?

El software puede ser generado a medida para la organización o utilizarse uno existente. En caso de ser diseñado para la organización, la Empresa ofrece mantenimiento del software.

En Caso de Poseer una Base Datos, es Posible Realizar una Migración para ser Utilizados por este Sistema?

El sistema genera un archivo plano con los datos identificados de cada persona, este archivo luego debe ser tomado por el software implementado.

Conclusión

El relevamiento general arrojó una gran variedad de precios y una gran diversidad de productos, por lo que se recomienda una mayor búsqueda y evaluación de los productos antes mencionados.

Se concluye también que en general no se ha generalizado el uso de tecnología biométrica a lo largo de la Administración Pública Provincial, salvo raras excepciones, donde es necesario un mayor estudio y análisis del uso y resultado del uso de tales tecnologías.

Marco Teórico

Técnicas de Autenticación Biométrica

A continuación describiremos de forma breve las técnicas de autenticación biométrica más extendidas y aplicables, las cuáles presentan características únicas y fundamentales en términos de precisión **(P)**, costo **(C)**, aceptación por parte del usuario **(A)**, y grado de intrusión de la técnica **(I)**. Obviamente, la técnica ideal tendría precisión y aceptación máximas, y coste e intrusión mínimas (P++++, C+, A++++, I+). De este modo, podemos enumerar:

- **Reconocimiento de huella dactilar**: el usuario sólo tiene que situar la yema de un dedo (normalmente el índice) sobre un escáner de huella. Evaluación: P++++, C++, A+++, I++.
- **Reconocimiento facial**: el sistema dispone de una cámara que graba al usuario, analizando el rostro del individuo. Evaluación: P++, C+++, A++, I+.
- **Reconocimiento de voz**: la persona pronuncia un código de acceso prefijado (nombre y/o apellidos, DNI, número de teléfono, PIN, etc.), o una frase diferente cada vez por invitación del sistema (diga usted ...), siendo reconocido por el sistema a partir de las características de la voz grabada en el momento del acceso. Evaluación: P+++, C+, A++, I+.

- **Reconocimiento de la geometría de la mano**: la persona sitúa su mano abierta sobre un escáner específico, siendo reconocido a partir de la forma y geometría de la misma. Evaluación: P++, C+++, A++, I++.
- **Reconocimiento de iris**: el sistema obtiene una imagen precisa del patrón de iris del individuo, y lo compara con el patrón previamente guardado del usuario. Evaluación: P++++, C++++, A+++, I+++.
- **Reconocimiento de firma**: el individuo firma sobre una superficie predeterminada, y la misma es verificada frente a un patrón previamente obtenido de la misma persona.

Sin embargo, sea cual sea la técnica seleccionada para una determinada aplicación, tendremos que ponderar en cada caso las restricciones o peculiaridades que pueden tener cada una de las técnicas, frente al grado de seguridad añadido que conseguimos y del que anteriormente no disponíamos. Estas características a ponderar vienen dadas básicamente por los siguientes aspectos:

- Necesidad de un dispositivo de adquisición específico (lector de huella dactilar, micrófono, cámara, etc.) allí donde esté el usuario.
- Posible variabilidad con el tiempo del patrón a identificar (afonías o catarros en voz, uso de gafas/bigote/barba/etc. en rostro, etc.).
- Probabilidad de error individual de cada una de las técnicas (entre uno por cien y uno entre varios millones, en función de la técnica elegida).

- Aceptación por parte del usuario de cada una de las técnicas, en función de si son o no técnicas intrusivas, cómodas, que mantengan (o al menos lo parezca) la privacidad, sencillas de usar, etc.

De este modo, en función de la situación en que necesitemos realizar autenticación segura del usuario, buscaremos cuál es la técnica (o combinación de técnicas) biométrica más adecuada en función de los cuatro parámetros fundamentales anteriormente mencionados.

Muchas de estas técnicas ya están siendo utilizadas en sistemas reales, como la tarjeta de la Seguridad Social en Andalucía, basada en huella digital, cajeros automáticos con autenticación por iris, o sistemas de compra por teléfono con autenticación por voz, por citar algunos ejemplos.

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, medidas de la palma de la mano),
- **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.

Por tasa de **falsa aceptación** (*False Acceptance Rate*, **FAR**) la probabilidad de que el sistema autentique correctamente a un usuario ilegítimo.

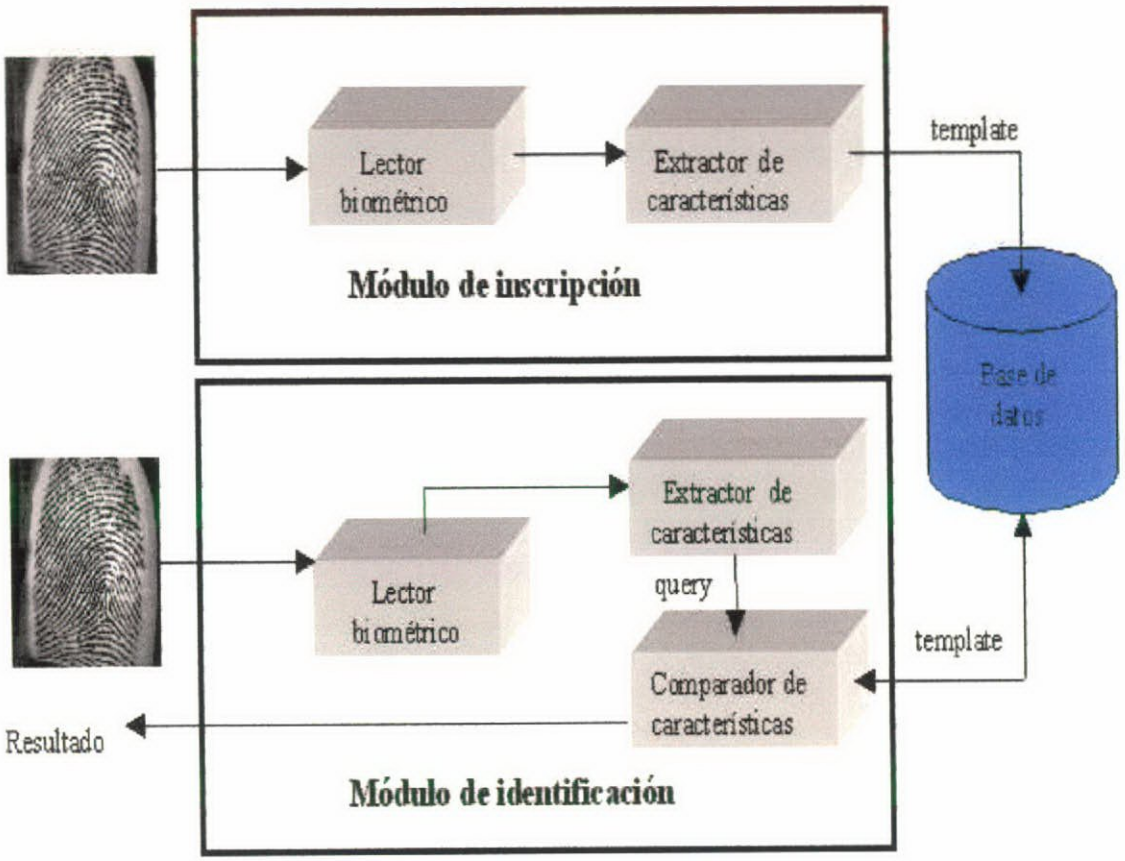
Evidentemente, una **FRR** alta provoca descontento entre los usuarios del sistema, pero una **FAR** elevada genera un grave problema de seguridad:

estamos proporcionando acceso a un recurso a personal no autorizado a acceder a él.

Por último, y antes de entrar más a fondo con los esquemas de autenticación biométrica clásicos, quizás es conveniente desmentir uno de los grandes mitos de estos modelos: la vulnerabilidad a ataques de simulación. En cualquier película o libro de espías que se precie, siempre se consigue 'engañar' a autenticadores biométricos para conseguir acceso a determinadas instalaciones mediante estos ataques: se simula la parte del cuerpo a analizar mediante un modelo o incluso utilizando órganos amputados a un cadáver o al propio usuario vivo (crudamente, se le corta una mano o un dedo, se le saca un ojo...para conseguir que el sistema permita la entrada).

Evidentemente, esto sólo sucede en la ficción: hoy en día cualquier sistema biométrico - con excepción, quizás, de algunos modelos basados en voz son altamente inmunes a estos ataques. Los sistemas Biométricos son capaces, aparte de decidir si el miembro pertenece al usuario legítimo, determinar si éste está vivo o se trata de un cadáver.

Circuito de Recolección de Datos Biométricos



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. El primero se encarga de adquirir datos relativos al indicador biométrico elegido y entregar una representación en formato digital de éste. El segundo extrae, a partir de la salida del lector, características representativas del indicador. El conjunto de características anterior, que será almacenado en una base de datos central u

otro medio como una tarjeta magnética, recibirá el nombre de *template*. En otras palabras un *template* es la información representativa del indicador biométrico que se encuentra almacenada y que será utilizada en las labores de identificación al ser comparada con la información proveniente del indicador biométrico en el punto de acceso.

Huella Dactilar

La identificación por medio de huella dactilar, es una tecnología que funciona al igualar las **relaciones entre minucias**: puntos de sus huellas digitales en donde las rayas terminan o se dividen. No es necesario que sean 100% iguales, sino que se alcance un nivel estadístico importante. Esto permite que la identificación de las huellas digitales funcione aunque el sistema este sucio o la persona se haya cortado un dedo.

La clasificación de huellas corresponde a un análisis a escala "gruesa" de los patrones globales de la huella que permite asignarla a un conjunto predeterminado o ***clase***, lo que se traduce en una *partición* de la base de datos a ser revisada. Por otro lado, el *matching* de huellas lleva a cabo una comparación a escala "fina" de las huellas dactilares a partir de los vectores de características resultantes de representar la geometría de cada una de las *minucias.*

En otras palabras, el *matching* de huellas dactilares consiste en encontrar el **grado de similitud** entre dos vectores de características cuyas componentes representan a las minucias de cada huella.

Las principales dificultades en el proceso de *matching* son:

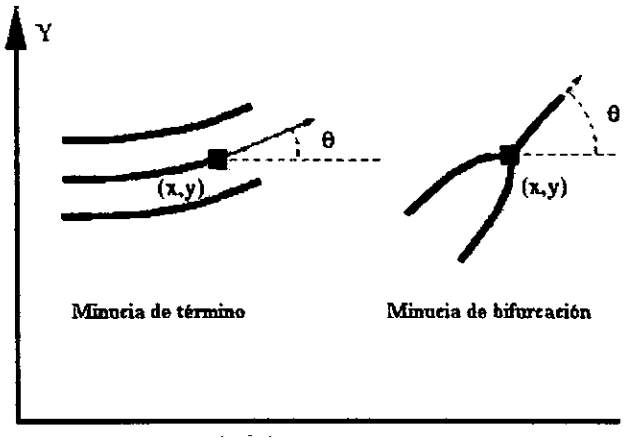
1. Hay traslaciones, rotaciones y deformaciones no lineales de las imágenes que se heredan a las minucias
2. Aparecen minucias espurias, mientras otras verídicas desaparecen

3. La base de datos puede ser muy grande
4. No existe un método de comparación que entregue una coincidencia exacta entre las características de la imagen de entrada y las pertenecientes a la base de datos.

Huellas dactilares . Desarrollo Técnico

Una huella dactilar es la representación de la morfología superficial de la epidermis de un dedo. Posee un conjunto de líneas que, en forma global, aparecen dispuestas en forma paralela (colinas o *ridge lines* y *furrows*). Sin embargo estas líneas se intersectan y a veces terminan en forma abrupta. Los puntos donde las colinas terminan o se bifurcan se conocen técnicamente como minucias. Otros puntos singulares de una huella dactilar son aquellos donde la curvatura de los *ridges* es máxima. Esos puntos reciben el nombre de *cores* y deltas. La característica más interesante que presentan tanto las minucias como los puntos singulares *cores y deltas* es que son únicos para cada individuo y permanecen inalterados a través de su vida. A pesar de esta variedad de minucias (18 tipos distintos de minucias han sido enumerados [10]) las más importantes son las *terminaciones y bifurcaciones* de *ridges*. Esto último se debe a que las terminaciones de *ridges* representan aproximadamente el 60.6% de todas las minucias en una huella y las bifurcaciones el 17.9% [5]. Además varias de las minucias menos típicas pueden expresarse en función de las dos señaladas. Naturalmente, para poder identificar a una persona mediante las minucias de su huella es necesario poder representar a estas últimas para poder compararlas. La

representación estándar consiste en asignar a cada minucia su posición espacial ***(x, y)*** y su dirección **q**, que es tomada con respecto al eje **x** en el sentido contrario a los punteros del reloj. Esta representación se muestra en la siguiente para una minucia de término y una de bifurcación de *ridge*.



Representación de minucias en términos de su posición y dirección.

Para reconocer una huella dactilar se procede desde una escala gruesa a una fina. En primer lugar se clasifica a la huella, es decir, se asigna a una clase previamente determinada de acuerdo a la estructura global de los *ridges*. El objetivo de esta etapa es establecer una partición en la base de datos con huellas. En general la distribución de las huellas en las distintas clases es no uniforme [1], esto obliga a subclasificar a la huella en estudio, es decir, generar un nuevo conjunto de clases a partir de las ya definidas. Luego se procede a la comparación a escala fina. Este proceso recibe el nombre de

matching. El proceso consiste en comprobar si el conjunto de minucias de una huella coincide con el de otra.

Transformada de Hough Generalizada.

Transformada de Hough.

Consideremos el siguiente problema: para una imagen con **n** puntos de interés se desea encontrar subconjuntos de esos puntos que residan sobre líneas rectas. Este problema que a simple vista parece ser sencillo, presenta una complejidad computacional elevada al utilizar una técnica de "fuerza bruta". Una de éstas soluciones consiste en encontrar todas las líneas determinadas por cada par de puntos en la imagen y luego encontrar todos los subconjuntos de puntos que se encuentran cerca de esas líneas. La complejidad de este algoritmo es $O(n^3)$, lo que representa un costo elevado. Hough notó lo siguiente [3]: para un punto con coordenadas (x_i , y_i) el conjunto de rectas que pasan por él satisfacen que $y_i = m\, x_i + c$, donde **m** es la pendiente de la recta y **c** su coeficiente de posición. Este conjunto de rectas es infinito, pues sólo basta variar **m** y **c**. La relación anterior puede escribirse en el espacio de parámetros como $c = -x_i\, m + y_i$, es decir, una recta con pendiente **-xi** y coeficiente de posición **yi** . Si se considera otro punto con coordenadas (x_j , y_j) por donde pasan rectas, se tendrá que su representación en el espacio de parámetros intersectará a la de (x_i , y_i) en un punto con coordenadas **(m', c')**, que corresponden a la pendiente y el coeficiente de posición, respectivamente, de una recta que pasa por (x_i , y_i) y (x_j , y_j).

De lo anterior se desprende que los puntos del espacio de coordenadas pertenecientes a una misma recta se intersectarán todos en un único punto del espacio de parámetros. Si fuese posible contar el número de

"intersecciones" en un punto con coordenadas **(m', c')** del espacio de parámetros entonces se tendría el número de puntos del espacio de coordenadas que pertenecen a una recta con pendiente **m'** y coeficiente de posición c'. Esta idea es la que sirve de base al proceso denominado Transformada de Hough. El primer paso consiste en la discretización del espacio de parámetros en un número finito de celdas para valores discretos tanto de m como de c. El rango en donde se hace esta discretización está dado por los valores mínimo y máximo esperados para las pendientes y los coeficientes de posición. El espacio de parámetros discretizado en celdas puede representarse mediante un arreglo A, denominado arreglo acumulador. La componente A(i, j) del arreglo acumulador representa a la celda asociada a la pendiente mi Î (mmín, mmax) y el coeficiente de posición $\mathbf{c_j}$ **Î** $\mathbf{(c_{mín}, c_{max})}$. Como se notó anteriormente, es de interés contar el número de "intersecciones" de las rectas en el espacio de parámetros asociadas a los puntos del espacio de coordenadas. Para ello se propone el siguiente procedimiento: en primer lugar, todas las componentes de A se hacen nulas. Luego, se toma un punto **(xk , yk)** perteneciente al espacio de coordenadas y para cada uno de los mi se calcula la versión discreta de $\mathbf{c = -x_k\, m_i + y_k}$, es decir, c_j. Se sabe entonces que por el punto del espacio de parámetros con coordenadas **(mi,cj)** pasa al menos la recta asociada al punto del espacio de coordenadas $\mathbf{(x_k\ ,y_k)}$. Esto último se traduce en que A(i,j) se incrementa en una unidad, indicando que un punto del espacio de coordenadas genera una recta que pasa por el punto del espacio de parámetros con coordenadas

(mi,cj). Este algoritmo se aplica a todos los puntos del espacio de coordenadas.

Finalmente, el número de puntos del espacio de coordenadas que se encuentran sobre una recta con pendiente mi y coeficiente de posición **cj** será **A(i,j)** si este último es mayor que 1. Notemos que la complejidad de cálculo de esta estrategia es Mxn, donde n es el número de puntos a revisar y M es el número de niveles de cuantificación del rango (m_{min}, m_{max}). Si el número de niveles de cuantificación para m permanece menor a n2 entonces la transformada de Hough será más eficiente que el método de "fuerza bruta" propuesto.

Es bien sabido que para aplicaciones prácticas la ecuación cartesiana de una línea recta no es de utilidad [6]. Si la recta presenta una pendiente elevada entonces el número de niveles de cuantificación será elevado y hará que una representación discreta del espacio de parámetros no sea adecuada. Además, el coeficiente de posición tampoco está acotado. Una parametrización adecuada de la ecuación de una recta en este contexto, será aquella que posea dos parámetros diferentes con rangos de variación finitos. Para el caso de líneas es usual tomar la representación normal de una recta, es decir aquella en que se utilizan coordenadas polares. El procedimiento en esta representación es completamente análogo: el espacio de parámetros se particiona y se acumula evidencia para los parámetros **r** y **q** en el arreglo acumulador al mover, por ejemplo, el parámetro **q**.

Transformada de Hough Generalizada

La primera generalización de la transformada de Hough está asociada a la creación de un método que permita el reconocimiento de formas geométricas más complejas que la de una línea, por ejemplo circunferencias y elipses [12]. Una conclusión interesante es que la dimensión del arreglo acumulador es igual al número de grados de libertad del problema. El procedimiento anterior puede generalizarse aún más con el objeto de encontrar transformaciones generales entre conjuntos de puntos. En efecto, la transformada de Hough puede extenderse a formas no analíticas y a formas compuestas [12]. En este contexto global se estudia el siguiente problema: la resolución de un sistema de ecuaciones que presenta un conjunto de soluciones a priori desconocidas [12]. Para encontrar estas soluciones se utiliza la THG donde el espacio de parámetros es ahora el espacio de soluciones. Es en este espacio donde se acumulará evidencia y se espera que, en la vecindad de una solución, el valor del arreglo acumulador sea "grande". Esto da lugar a la formación de clusters o clases solución. Para formalizar estos conceptos definamos el siguiente problema: sean p ecuaciones en n variables representadas por el vector = (x1, x2, . . . , xn), cada una con la forma:

$$f_i(\vec{x}) = 0 \quad i = 1,2, \ldots,p \qquad (1)$$

Cada una de las p ecuaciones corresponde a una de j clases solución desconocidas a priori. El problema es determinar el número de clases solución *j* y la solución para cada una de estas clases, con k = 1, 2, ..., j. Es importante destacar que típicamente $j << p$ y que no existe restricción sobre *fi*

de ser lineal o que el sistema sea linealmente independiente. La solución a este problema consiste en encontrar zonas de acumulación o *clusters* de posibles soluciones y considerar aquellos *clusters* más grandes como representantes de las soluciones más probables. Obviamente la resolución de cada ecuación por sí sola no es posible. Tampoco es práctico seleccionar de entre las p ecuaciones todos los posibles subconjuntos y calcular, donde sea posible, las soluciones, debido al elevado número de posibilidades de partición del conjunto de ecuaciones en c conjuntos no vacíos (~ c^p / c!). En este sentido la THG entrega un marco conceptual y práctico al problema de la resolución de (1).

THG y la Transformación entre los Vectores de Características *Query* y *Template*

El problema del *matching* entre vectores de características asociados a los conjuntos de minucias de dos huellas dactilares tiene, como primera tarea, la determinación de la transformación (rotación, traslación, escalamiento) entre ambas.

Esta transformación debe considerar incluso que, para dos vectores de características de una misma huella dactilar pueden existir diferencias entre éstas: la desaparición de algunas minucias, la variación de la posición y orientación local de algunas de éstas debido al ruido que introduce el sensor, y a las deformaciones elásticas que presenta la piel. Esta transformación es, a priori desconocida. De esta manera la **THG** provee un método para la obtención de esta transformación.

Debido a que en aplicaciones civiles las imágenes *query* y *template* serán escaneadas por el mismo sensor, no será necesario considerar en el análisis escalamiento entre los vectores de características [7]. Sea **(qx, qy)** y b las coordenadas de posición y la orientación local de una minucia perteneciente al vector de características *query*. Sean **(tx, ty)** y a la posición y orientación asociadas a una minucia perteneciente al vector de características *template*.

La transformación más general posible a priori, entre ambos conjuntos considerará en forma explícita rotaciones y traslaciones, por lo que tendrá la forma [11]:

$$\begin{pmatrix} qx \\ qy \end{pmatrix} = \begin{pmatrix} \cos 0 & - & \text{sen } 0 \\ \text{sen } 0 & - & \cos 0 \end{pmatrix} \begin{pmatrix} tx \\ ty \end{pmatrix} + \begin{pmatrix} Ax \\ Ay \end{pmatrix} \qquad (2)$$

donde q es igual a **(b -a)**, y **(Dx, Dy)** es una traslación arbitraria. El ángulo q indica la rotación necesaria para que la orientación de la minucia *template* coincida con la de la minucia *query*. La transformación definida por (2) posee tres grados de libertad, esto último indica que el arreglo acumulador A para la búsqueda de la transformación será de dimensión tres, a saber: uno para la cuantificación del ángulo q, y dos para el desplazamiento en el eje x y en el eje y. Notemos que el problema planteado con (2) es análogo al presentado en (1). El cluster del espacio de parámetros que interesa rescatar es aquel que representa la transformación existente entre los vectores *template* y *query*. Se postula que los parámetros que definen a éste corresponden a los índices asociados al máximo valor del arreglo acumulador. De la discusión anterior resulta evidente que la estrategia para encontrar los parámetros de la transformación (2) será aplicar la THG.

Sea **Q** el vector de características *query* con dimensión **dimQ** y T el vector *template* con dimensión **dimT**. Sea además **Q[i]** la i-ésima minucia del vector **Q**, y T[i] la i-ésima minucia del vector T. Notemos que el problema (2) puede

"separarse" en dos etapas: en primer lugar es posible obtener el ángulo de rotación q entre los vectores de características y luego, a partir de éste, el vector de desplazamiento **(Dx, Dy)**.

Esto último reduce el costo computacional que involucra el cálculo de una **THG 3D** al de una **THG 1D** más una **THG 2D**. Además, Es importante notar que el rango al que pertenece un ángulo de rotación entre dos huellas y, por ende, entre dos vectores de características está acotado, sea éste **Dq**. A continuación se presenta un diagrama en bloques del proceso de cálculo de la **THG** propuesto, para la definición del ángulo de rotación. El caso 2D es análogo.

La siguiente figura muestra las principales tareas a realizar por la **THG**. En primer lugar se restan las orientaciones locales de las minucias *query* y *template*. Mediante la consulta **¿d Î Dq ?** se eliminan todas las posibilidades no factibles, lo cual se traduce en una nueva mejora en la eficiencia del algoritmo. El proceso de cuantificación entrega la componente del arreglo acumulador en donde se recopilará evidencia. El algoritmo continúa acumulando evidencia hasta que todas las comparaciones entre minucias han sido consideradas. En ese instante se procede a buscar los máximos del arreglo acumulador A y a tomar una decisión con respecto a cuál es el mejor parámetro para la transformación.

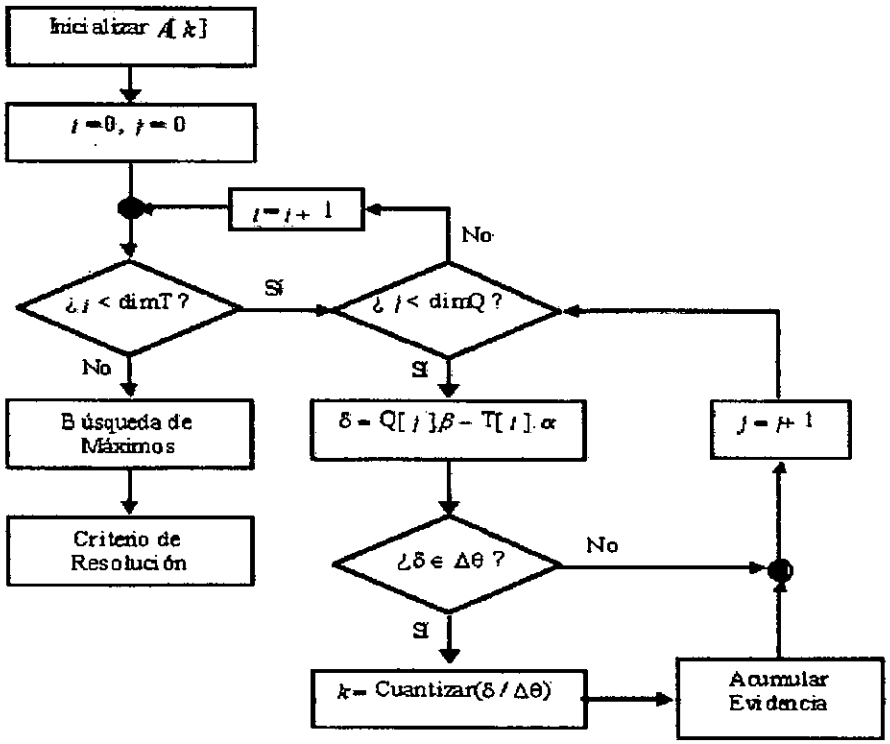


Diagrama en bloques de la THG para el ángulo de rotación entre los vectores P y Q.

Nuevo Criterio de Resolución

El algoritmo presentado en [11] acumula evidencia incrementando al arreglo acumulador en una única posición k en cada iteración. El criterio de resolución para determinar la transformación está basado en encontrar la posición donde se encuentra el máximo del arreglo acumulador. Como se mostrará más adelante esta estrategia sólo funciona bien en ausencia de ruido. En el mismo trabajo se menciona la posibilidad de incrementar, además de la posición ganadora k, a las vecinas inmediatas de ésta. En este trabajo se estudian tres posibilidades de acumular evidencia: la primera es la ya mencionada y presente en [11], en la segunda se incrementa el arreglo acumulador en su posición ganadora k y en las asociadas a sus vecinos k-1 y k+1 en el mismo monto (se incrementa en 1 el arreglo acumulador), la tercera y última incrementa en dos al arreglo en la posición ganadora y en uno a los vecinos inmediatos. El criterio de decisión para esta última es idéntico al del primer caso: el máximo absoluto es el ganador. Para las tres estrategias anteriores se buscarán los valores y las posiciones de los seis mayores máximos locales asociados a la transformación que busca la rotación entre los vectores de características. Además, para la segunda estrategia se presenta un nuevo criterio de decisión. Las definiciones básicas para la comprensión de este nuevo criterio se presentan a continuación.

Definiciones

Sea **I** el arreglo de índices que contiene las posiciones de los máximos relativos del arreglo acumulador A(k). Definamos los siguientes operadores (en negritas):

Max_Vecinos(I): retorna un arreglo con el índice de la posición del valor máximo de A y la de todos los vecinos consecutivos de éste en el arreglo I, en orden creciente. En caso de que existan dos arreglos, retorna el de mayor dimensión y si aún persiste ambigüedad se elige cualquiera de ambos.

Iguales_Max(I): retorna un arreglo con los índices de I que tienen el valor máximo de A.

Vecinos_Max(I): Toma todos los índices vecinos inmediatos presentes en I y los retorna como un arreglo. En caso de existir más de una solución retorna la asociada al máximo.

A continuación se define una función de membresia (en negritas y cursiva):

Cerca(I_1, I_2): indica si los índices del conjunto I_2 están "cerca" de los del I_2.

Definamos además los siguientes conjuntos de índices:

I_1 = **Max_Vecinos(I)**
I_2 = **Vecinos_Max(I Ç I_1^c) = Vecinos_Max(I / I_1)**
I_3 = **Iguales_Max(I)**

Como ejemplo, suponga que el vector de índices con los seis mayores máximos del arreglo acumulador A es **I = [0, 4, -1, 5, -43, 1]** y las

componentes de A asociadas a esos índices son: $A_{|I} = [16, 16, 15, 15, 14, 13]$,

entonces:

I1 = Max_Vecinos(I) =[-1, 0, 1]
I2 = Vecinos_Max(I ∩ I1c) =[4, 5]
I3 = Iguales_Max(I) =[0, 4]

A partir de estas definiciones se pueden construir reglas para decidir cuál será el parámetro que define a la transformación:

Regla 1. $\sim[\ Cerca(\mathbf{I}_1, \mathbf{I}_2)] \wedge (\ |\mathbf{I}_1| \geq |\mathbf{I}_3|) \Rightarrow \hat{k} = \hat{k}_1$

Regla 2. $\sim[\ Cerca(\mathbf{I}_1, \mathbf{I}_2)] \wedge (\ |\mathbf{I}_1| < |\mathbf{I}_3|) \Rightarrow \hat{k} = \hat{k}_3$

Regla 3. $Cerca(\mathbf{I}_1, \mathbf{I}_2) \Rightarrow \hat{k} = \dfrac{\mu_1 \hat{k}_1 + \mu_2 \hat{k}_2}{\mu_1 + \mu_2}$

donde:

$$\hat{k}_j = \frac{\sum_{k \in I_j} kA(k)}{\sum_{k \in I_j} A(k)}, \quad \mu_j = \frac{\sum_{k \in I_j} A(k)}{|I_j|} \quad \text{para } j = 1, 2, 3.$$

Simulaciones

A continuación se presentan los resultados de las simulaciones realizadas para estudiar el desempeño de este nuevo criterio de resolución. Se crearon vectores de características en forma artificial, para ello se generaron posiciones y orientaciones para las minucias con distribuciones aleatorias.

Para cada uno de estos vectores de características se crean versiones rotadas a partir de los mismos, se extraen en forma aleatoria algunas de las minucias, se agrega asimismo a las orientaciones locales de las minucias, ruido con distribución normal con media cero y varianza variable. Además de esto, se crearon versiones con combinaciones de las anteriores, como por ejemplo, versiones rotadas, con menos minucias y con ruido aditivo en la orientación local.

También se ha estudiado [9] el efecto de los niveles de cuantificación tanto en el espacio de coordenadas como en el espacio de parámetros y la posibilidad de utilizar *lógica* difusa para tomar decisiones. En este trabajo no se incluirán estos resultados. Además, no se utilizará cuantificación en el espacio de coordenadas y la resolución en el espacio de parámetros será de 1°. Los resultados obtenidos son los siguientes:

1. Caso ideal (rotación pura, extracción pura, y combinaciones de éstas): Las tres estrategias entregan los mismos resultados. Recordar que la primera y la última sólo consideran el máximo absoluto.

2. Caso con ruido en la orientación de las minucias: Para este caso, independiente de si se incluye o no rotación y extracción de minucias, el desempeño de la primera estrategia y el de la tercera es pobre. Sin embargo el desempeño alcanzado por la segunda estrategia está por encima de las otras.

De la tabla 1 es posible notar que el algoritmo propuesto en [11] entrega el valor -3° como respuesta, siendo que el valor correcto es 0°. Si bien los algoritmos 2 y 3 entregan en su primera componente el valor correcto hay que considerar que los valores máximos de A no presentan una variación alta, lo que se esperaría para el caso 3. Al aplicar las reglas para el caso 2 se obtiene que I_1 =**[-2, -1, 0, 1, 2]**, I_2 =**[-4]**, e I_3 =**[0]**. Por lo tanto la regla gatillada es la número 1. Esto implica que el valor es 0°. Puede parecer que el algoritmo 3 es superior al 2 debido a que, en este caso, para obtener el resultado del 2 se tuvo que llevar a cabo más cálculos para obtener el mismo resultado.

Tabla 1. Acumulación de evidencia por los tres algoritmos. Caso sólo ruido aditivo, s =4.5°

Algoritmo	Arreglo de índices I						A restringido a I					
1	-6	13	39	-15	22	35	8	8	8	7	7	7
2	12	16	22	36	38	-14	17	17	16	16	16	15
3	-6	16	22	12	13	17	23	23	23	22	21	21

Tabla 2. Acumulación de evidencia por los tres algoritmos. Caso rotación en 17° y ruido aditivo, s = 6°

Algoritmo	Arreglo de índices						A restringido a I					
1	-6	13	39	-15	22	35	8	8	8	7	7	7
2	12	16	22	36	38	-14	17	17	16	16	16	15
3	-6	16	22	12	13	17	23	23	23	22	21	21

La tabla 2 presenta un caso más exigente donde tanto el algoritmo 1 como el 3 entregan resultados incorrectos (-6°, para 17°). Sin embargo, veamos el desempeño del algoritmo 2. En este caso, $\mathbf{I_1}$ **=[12]** (puede ser también $\mathbf{I_1}$ **=[16]**), $\mathbf{I_2}$ **=[-14, 16, 22, 36, 38],** e $\mathbf{I_3}$ **=[12, 16]**. Notamos que la regla gatillada es, en este caso, la número 2. Esto implica que el valor resultante es 14°. Este resultado, si bien no coincide con el valor correcto de 17° muestra la superioridad del algoritmo 2.

Comentarios y Conclusiones

En este trabajo se presentó, en primer lugar, una introducción general a los llamados Sistemas Biométricos. Se describió asimismo el Reconocimiento de Huellas Dactilares como una de las técnicas biométricas más maduras y confiables, uno de cuyos componentes fundamentales es el *matching* de huellas dactilares. Para implementar este proceso se desarrollo un algoritmo, que presenta tres mejoras sustanciales al algoritmo propuesto en [11] para encontrar la transformación entre dos vectores de características mediante la transformada de Hough Generalizada.

Las dos primeras tienen relación directa con la reducción de la complejidad del algoritmo hasta la etapa de búsqueda de los máximos. La primera consiste en "separar" una transformada **3D** en una **1D** y otra **2D**. La segunda evita revisar todos los casos posibles restringiendo el rango de variación de la variable que define la rotación.

Finalmente, el aporte más importante es la propuesta de una nueva etapa de Criterio de Resolución. Aquí se determina, a partir de la información proporcionada por el arreglo con los índices de los máximos, el mejor parámetro que define la transformación de rotación entre ambos conjuntos de características.

En todas las situaciones el algoritmo propuesto presenta mejor desempeño que sus pares, en especial cuando la varianza del ruido aditivo impuesto

sobre las orientaciones locales aumenta. La línea actual de trabajo se centra en construir, a partir de las reglas deducidas un sistema de inferencia basado en lógica difusa. Se analiza también la inclusión de nuevas reglas. Además, se estudia la transformación 2D asociada a la traslación espacial de los vectores de características, y el efecto de la cuantificación tanto en el espacio de coordenadas como en el espacio de parámetros.

Geometría de la Mano

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.

Cuando un usuario necesita ser autenticado sitúa su mano sobre un dispositivo lector con unas guías que marcan la posición correcta para la lectura .Una vez la mano está correctamente situada, unas cámaras toman una imagen superior y otra lateral, de las que 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.

Quizás 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 de uno o dos dedos, que además puede usar dispositivos lectores más baratos y proporciona incluso más rapidez.

Firma Digital y Certificados Digitales

Tenemos ahora como propósito tratar de explicar y discutir un poco el concepto de firma digital, que nos llevara al de certificado digital. Primero consideremos que existe la necesidad de comunicación entre dos entes, por ejemplo dos personas que están en dos países diferentes, por lo tanto una de las mejores formas de comunicación es por Internet. Uno de los problemas más sentidos es ¿cómo saber que efectivamente la persona con quien me estoy comunicando es precisamente la que dice ser?. Este problema lo llamaremos el problema de verificación de Identidad o la autenticación.

La firma tradicional o de cualquier otro nombre que se le conozca tiene varias características, la principal de ellas es que es aceptada legalmente, esto quiere decir que si alguna persona firmó un documento adquiere tanto los derechos como las obligaciones que de él deriven, y si estas obligaciones no son acatadas, el portador del documento tiene el derecho de reclamación mediante un litigio. La autoridad competente acepta las responsabilidades adquiridas con sólo calificar a la firma como válida.

Nos dedicaremos a estudiar a la "firma" como elemento que sirve para demostrar la identidad.

Podemos resumir que existen dos procedimientos importantes, el primero el proceso de firma, que es el acto cuando una persona "firma" manualmente un

documento. Y el proceso de verificación de la firma, que es el acto que determina si una firma es válida o no.

Por otro lado es importante hacer notar que la firma comprueba la identidad de una persona, de tal modo que así se sabe quién es la persona quien firmó, y ésta persona no puede negar las responsabilidades que adquiere en un documento firmado.

Descripción de los puntos anteriormente mencionados.

Proceso de Firma

Este proceso es muy simple y consiste sólo en tomar un bolígrafo y estampar, dibujar o escribir garabatos en un papel. En general este garabato debe ser el mismo y es elegido a gusto de la persona. Se usa como una marca personal. Es importante mencionar que por una lado lo que identifica a la persona quien firma (quien hace el garabato) es la forma misma de la firma, pero también características de escritura, como la velocidad de escritura, la presión que se aplica al bolígrafo, la inclinación de la escritura, etc.

Proceso de Verificación

Existen en general dos métodos de verificación de la firma, uno es el más usado y simple, que es el visual, esté método lo aplica cualquier cajero al pagar un cheque, o al efectuar un pago con tarjeta de crédito. En muchos casos la firma es rechazada por no pasar este método, sin embargo legalmente no es suficiente el método visual. El método legalmente definitivo

es el peritaje de la firma en laboratorio, que consiste en verificar a la firma independientemente de la forma, tomando en cuenta otras características como la presión de escritura, la velocidad de escritura, la inclinación de escritura, las características particulares de alguna letra etc. El conjunto de estas propiedades son propias de cada país y sus leyes. Recalcamos que el resultado es tomado como definitivo, legalmente.

Por otra parte hacemos notar que con la firma queda resuelto legalmente el problema de la autenticidad o el de comprobar la identidad de una persona.

Y de la misma manera el problema que podría aparecer sí una persona rechaza ser el autor de una firma es también resuelto con los métodos anteriores, al menos legalmente.

Es importante hacer notar que la firma frecuentemente se encuentra asentada en un documento de identidad oficialmente válido, como el pasaporte, la credencial de identidad, el permiso de conducir un automóvil, y otros.

Antes de continuar es bueno mencionar algunos conceptos necesarios para explicar lo que sigue. Particularmente sobre la criptografía. La criptografía como ciencia, estudia los problemas básicos de la seguridad en la transmisión de la información por un canal inseguro. La criptografía se divide en criptografía simétrica y criptografía asimétrica. La criptografía simétrica resuelve el problema de la confidencialidad y usa algoritmos como TDES y

AES para transmitir información cifrada, y que solo con una única clave simétrica puede leer el contenido de la información. Esta clave la llamaremos "clave simétrica" y tiene una en general una longitud de 128 bits. El problema aquí es que antes de realizar la conexión segura es necesario que ambos lados tengan la misma clave simétrica. La criptografía asimétrica consiste en algoritmos basados en problemas de un solo sentido, es decir que por un lado sea muy fácil realizarlo, pero la inversa sea "difícil" de realizarlo, como es problema de la factorización entera, es fácil realizar el producto de dos números pero es "difícil" factorizar un número producto de dos números primos grandes. En este caso tenemos dos claves en cada caso que se le asocian a una entidad, un usuario por ejemplo. Una clave pública que sirve para cifrar información y solo quien tiene la clave privada asociada a esta clave pública puede descifrar el mensaje. Esto es usado para intercambiar claves simétricas. Por otra parte con la clave privada se firman documentos y se verifica la firma con la clave pública.

Es claro que la clave pública puede ser conocida por cualquier persona, sin embargo la clave privada es solo conocida por el dueño a quien se le asociaron el par de claves. La clave privada debe de guardarse de manera confidencial, ya sea en su computadora personal, en su *PDA*, en un *Smart Card* (tarjeta inteligente) o algún dispositivo personal.

En la práctica la criptografía simétrica y asimétrica se usan conjuntamente. La simétrica para intercambiar grandes volúmenes de información por su rapidez. Y la asimétrica para el intercambio de las claves simétricas y la firma digital.

Con todo lo anterior ya es muy fácil definir los conceptos de firma digital y de certificado digital.

Firma digital
Es un número natural, de mas o menos 300 dígitos si se usa el sistema RSA, que tiene las mismas propiedades que la firma convencional.

Es decir es posible asociar un número único a cada persona o entidad, existe un método de firma y un método de verificación de la firma. Esta firma digital resuelve satisfactoriamente el problema de autenticación y no rechazo.

Certificado Digital
Es un archivo de aproximadamente 1k de tamaño, que contiene, primero los datos del propietario, después su clave pública y la firma digital de una autoridad competente. Cuando una persona solicita un certificado digital, se generan su par de claves, la pública y la privada. La clave pública viene en el certificado digital explícitamente. La clave privada queda en custodia del propietario del certificado. El tercer elemento importante que tiene el certificado digital es la firma digital de una autoridad certificadora, quien esta como aval de que los datos corresponden al propietario. El certificado digital queda muy parecido entonces a un documento oficial de identificación como un pasaporte o una licencia de conducir.

Otra importante característica del certificado digital es que contiene además de lo ya mencionado, El nombre de los algoritmos que se usan para la firma digital.

La firma convencional es usada cuando la comunicación es personal, si esta comunicación fuese por ejemplo por teléfono no es posible usar la firma convencional. La firma digital está precisamente diseñada para poder ser usada a grandes distancias, y principalmente cuando esta comunicación esta hecha por dos computadoras e Internet, además puede ser usada por muchos dispositivos electrónicos.

Cabe también mencionar, que aunque la firma convencional puede ser enviada vía fax o por un documento que copie el garabato, ésta no es válida legalmente. Esta firma convencional se usa solo por conveniencia de alguna corporación o institución, por ejemplo al usar un sello que estampa la firma de algún ejecutivo, es usada sólo por la rapidez que representa usarla, pero legalmente no es válida. Sólo es válida aquella que es derivada del puño y letra de la persona. Por su parte la firma digital garantiza ser mejor que la convencional y sería de gran beneficio si esta tuviese validez legal.

Quizá la mayor diferencia entre la firma convencional y la firma digital es que la primera en su método de verificación existe una gran probabilidad de error, según algunos hasta del 20%, y en el caso de la firma digital, este error es inapreciable. Es una fuerte razón para que la firma digital tenga valor legal.

Es prudente mencionar que tipos de firma y certificados hay:
Primero veremos que tipos de firma digital. El método más usado para firmar digitalmente es el conocido como RSA, lo importante de este método es que es el más usado actualmente y por lo tanto es conveniente usarlo para poder ser compatible. Para que sea seguro la longitud de sus claves (una pública y otra privada) debe de ser de 1024 bits, es decir un número de un poco más de 300 dígitos.

Otro método reconocido para firma digital es el llamado **DSA**, que es oficialmente aceptado para las transacciones oficiales en el gobierno de USA. Este método usa también claves del mismo tamaño que **RSA**, pero esta basado en otra técnica. Aún así, sea podido mostrar que es casi equivalente en seguridad a **RSA**.

Una tercera opción es el método que usa curvas elípticas, este método tiene la ventaja a los dos anteriores a reducir hasta en 164 bits, es decir como 45 dígitos las claves, manteniendo la misma seguridad. Por lo que es más propio para ser usado donde existen recursos reducidos como en *Smart Cards, PDAs*, etc. Actualmente este método se ha integrado como el reemplazo oficial de **DSA** para el gobierno de USA.

Entre los posibles ataques a los anteriores métodos esta la posible remota construcción de una computadora cuántica, esta podría efectuar una cantidad

tan grande de cálculos al mismo tiempo que podría romper los sistemas anteriores, incluso ya existen estos algoritmos que romperían los sistemas. Sin embargo ya existe otro método de forma que aún con la computación cuántica no existe aún algoritmo que pueda romperlos. Este sistema es que esta basado en *lattices* (retículas), se conoce como NTRU (*Number Theory Research Unit*) y entre otras cualidades es más eficiente que RSA.

Existen aún más métodos para firmar, incluso algunos métodos derivados de las anteriores técnicas, sin embargo no han podido tener el impacto de las anteriores, de hecho puede crearse un método de firma para un caso particular.

Ahora veamos la forma de certificado digital:
En la actualidad tenemos un formato (estándar) que se ha extendido casi para todas las aplicaciones, este es el llamado **X.509**. Este formato contiene los datos del poseedor del certificado, la clave pública del propietario, y la firma de una autoridad certificadora. La mejor propiedad del formato **X.509** es que contiene el mínimo necesario de información para poder realizar muchas transacciones, principalmente comerciales y financieras. Sin embargo para otras aplicaciones puede ser un poco robusto.

Conclusión: un certificado digital, es un archivo que contiene una clave pública y su poseedor una clave privada, con la clave privada podemos firmar cualquier documento, con la clave pública es posible verificar la firma e

intercambiar información de forma confidencial, particularmente una clave simétrica.

Para poder obtener un certificado digital es necesario tener un software que genere estos certificados y que nos proporcione ya en formato X.509, para ser compatible. Podemos ver un certificado digital por ejemplo si nos conectamos a un sitio por Internet por ejemplo con los populares *browsers: Netscape* o *Explorer* y hacer *click* en el icono del candado, a partir de ahí podemos llegar a ver el certificado, siempre y cuando este candado este cerrado. La comunicación de un *browser* con un servidos se lleva a cabo por medio del protocolo SSL que puede funcionar con al menos un certificado digital de un lado de la comunicación.

Como siguiente paso para entender lo que es un certificado digital y la firma digital pueden por ejemplo revisar el artículo "Compras Seguras por Internet" que no es más que un ejemplo de SSL usando un certificado digital.

Firma Digital. Aspectos Legales

Ley de Firma Digital

El Poder Ejecutivo Nacional ha promulgado la Ley 25.506 de Firma Digital Boletín Oficial del 14/12/2001)

Qué es la Infraestructura de Firma Digital?

El Poder Ejecutivo Nacional de la República Argentina dispuso la creación de la Infraestructura de Firma Digital, aplicable al Sector Público Nacional, a través de la aprobación del Decreto Nº 427 del 16 de Abril de 1998.

Esta clase de Infraestructura es también conocida como de "clave pública" o por su equivalente en inglés (*Public Key Infrastructure* o **PKI**). La normativa crea el marco regulatorio para el empleo de la firma digital en la instrumentación de los actos internos del Sector Público Nacional que no produzcan efectos jurídicos individuales en forma directa, otorgándole a esta nueva tecnología similares efectos que a la firma ológrafa.

La disposición establece la configuración de la siguiente estructura:

- Organismo Licenciante
- Organismo Auditante
- Autoridades Certificantes Licenciadas
- Suscriptores

La Infraestructura de Firma Digital del Sector Público Nacional pone a su disposición una Autoridad Certificante gratuita a través de la cual podrá obtener su propio certificado digital.

Utilizando este certificado usted podrá asegurar todas sus comunicaciones de correo electrónico, garantizando su autoría y la integridad del mensaje.

Laboratorio de Firma Digital

Para optimizar el proceso de difusión de la tecnología de Firma Digital, se ha implementado un Laboratorio, donde el público en general, y particularmente los funcionarios y agentes de la Administración Pública Nacional, experimenten la generación de un par de claves, la gestión de su propio certificado y el envío de correo electrónico firmado, al tiempo de ofrecerse información diversa sobre esta tecnología.

Ejemplos de Utilización de Firmas Digitales

Subsecretaría de la Gestión Pública

ArCert Coordinación de Emergencias en Redes Teleinformáticas

Descripción

Autenticación del ingreso a bases de datos de la Coordinación de Emergencias en Redes Teleinformáticas para la Administración Pública Nacional.

Usuarios: Organismos Públicos

Contacto: Rodrigo Seguel rseguel@arcert.gov.ar

Inicio de Operaciones: 08/1999

Ministerio de Economía

Circuito Interno de Correo Electrónico firmado digitalmente.

Descripción

Circuito interno de comunicación de textos de resoluciones firmadas dentro del ministerio y áreas dependientes.

Cantidad de Usuarios (aproximada): 150

Contacto: Aldo Rosemberg aldoros@mecon.ar

Inicio de Operaciones: 01/1998

Intercambio de Información con la Oficina Nacional de Contrataciones

Descripción

Incorpora la firma digital en el intercambio de información entre las Unidades Operativas de Compras de los organismos y la Oficina Nacional de Contrataciones.

Cantidad de Usuarios (aproximada): 300

Contacto: Roberto Boccardo ondc@mecon.ar

Inicio de Operaciones: 03/2001

Comisión Nacional de Valores

Autopista de la Información Financiera (AIF)

Descripción

Proyecto desarrollado con el objetivo de recibir y publicar por Internet, a beneficio del público inversor nacional e internacional, la información financiera de las principales empresas del país que cotizan sus acciones y obligaciones negociables en el ámbito bursátil. Algunos ejemplos de información firmada digitalmente recibida por la AIF son: estados contables, prospectos informativos de emisión de acciones y de obligaciones negociables, estatutos, actas de asamblea, calificaciones de riesgo de títulos valores, notificaciones de eventos económicos significativos.

Usuarios:

Agentes CNV: 120

Empresas Cotizantes: 200

Calificadores de Riesgo: 12

Fondos Comunes de Inversión:200

Contacto: J. Andrés Hall jah@mecon.gov.ar

Inicio de Operaciones: 04/1999

Comisión Nacional de Energía Atómica

Circuito Interno de Correo Electrónico firmado digitalmente

Descripción

Circuito de comunicaciones a través de correo electrónico firmado dentro del organismo.

Cantidad de Usuarios (aproximada): 50

Contacto: admin-ca@mecon.gov.ar

Inicio de Operaciones: 11/1998

Poderes Judiciales Provinciales

Convenios de Comunicación Electrónica Interjurisdiccional y Sistema de Información para la Justicia Argentina

Descripción

Los Convenios fueron firmados en la sede del Ministerio de Justicia y Derechos Humanos el 6 de Septiembre de 2001 por la casi totalidad de los

Poderes Judiciales del país, la Procuración General de la Nación y la Defensoría General de la Nación. Promueven la utilización del correo electrónico firmado digitalmente en las comunicaciones entre organismos judiciales de distinta jurisdicción territorial. El artículo 5° del Protocolo Técnico establece que, hasta tanto las Partes organicen su propia Autoridad Certificante, los certificados digitales serán emitidos por alguna de las partes o por la AC de la Subsecretaría de la Gestión Pública, y los firmantes se constituirán como Autoridades de Registración.

Referencia: http://www.justiciaargentina.gov.ar

Código de Barras

El Código de Barras es un arreglo en paralelo de barras y espacios que contiene información codificada en las barras y espacios del símbolo. Esta información puede ser leída por dispositivos ópticos, los cuales envían la información leída hacia una computadora como si la información se hubiera tecleado.

Ventajas del Uso de Código de Barras

Algunas de sus ventajas sobre otros procedimientos de colección de datos son:

- Se imprime a bajos costos
- Permite porcentajes muy bajos de error
- Los equipos de lectura e impresión de código de barras son flexibles y fáciles de conectar e instalar.

Beneficios

Es la mejor tecnología para implementar un sistema de colección de datos mediante identificación automática, y presenta muchos beneficios, entre otros. Virtualmente no hay retrasos desde que se lee la información hasta que puede ser usada

- Se mejora la exactitud de los datos
- Se tienen costos fijos de labor más bajos
- Se puede tener un mejor control de calidad, mejor servicio al cliente

- Se pueden contar con nuevas categorías de información.
- Se mejora la competitividad.

Aplicaciones

Las aplicaciones del código de barras cubren prácticamente cualquier tipo de actividad humana, tanto en industria, comercio, instituciones educativas, instituciones médicas, gobierno, etc.

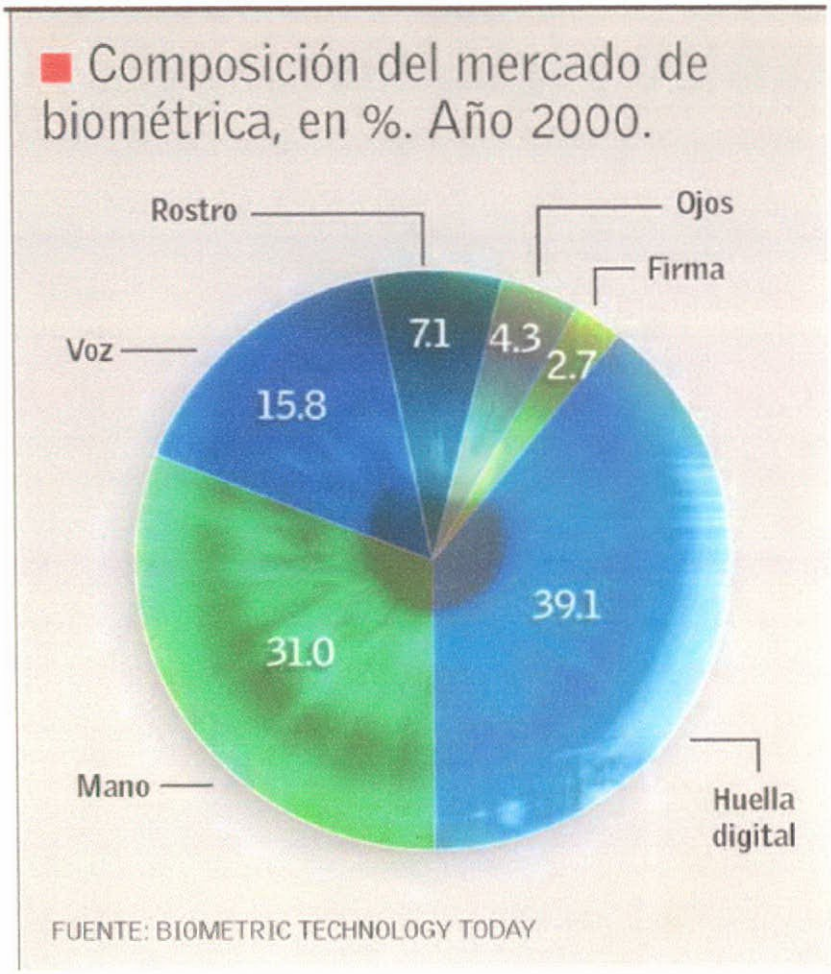
- Control de inventario
- Control de material en proceso
- Control de tiempo y asistencia
- Punto de venta
- Control de calidad
- Control de inventario
- Embarques y recibos
- Control de documentos
- Facturación
- Bibliotecas
- Bancos de sangre
- Hospitales
- Control de acceso
- Control de tiempo y asistencia

Comparación de Métodos Biométricos

	Ojo - Iris	Ojo - Retina	Huellas dactilares	Geometría de la mano	Escritura Firma	Voz
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy Alta	Muy alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta
Estabilidad	Alta	Alta	Alta	Media	Media	Media
Identificación y autenticación	Ambas	Ambas	Ambas	Autenticación	Ambas	Autenticación
Estándares	-	-	ANSI/NIST, FBI	-	-	SVAPI
Interferencias	Gafas	Irritaciones	Suciedad, heridas, asperezas...	Artritis, reumatismo...	Firmas fáciles o cambiantes	Ruido, resfriados...
Utilización	Instalaciones nucleares, servicios médicos, centros penitenciarios	Instalaciones nucleares, servicios médicos, centros penitenciarios	Policía, industrial	General	Industrial	Accesos remotos en bancos o bases de datos

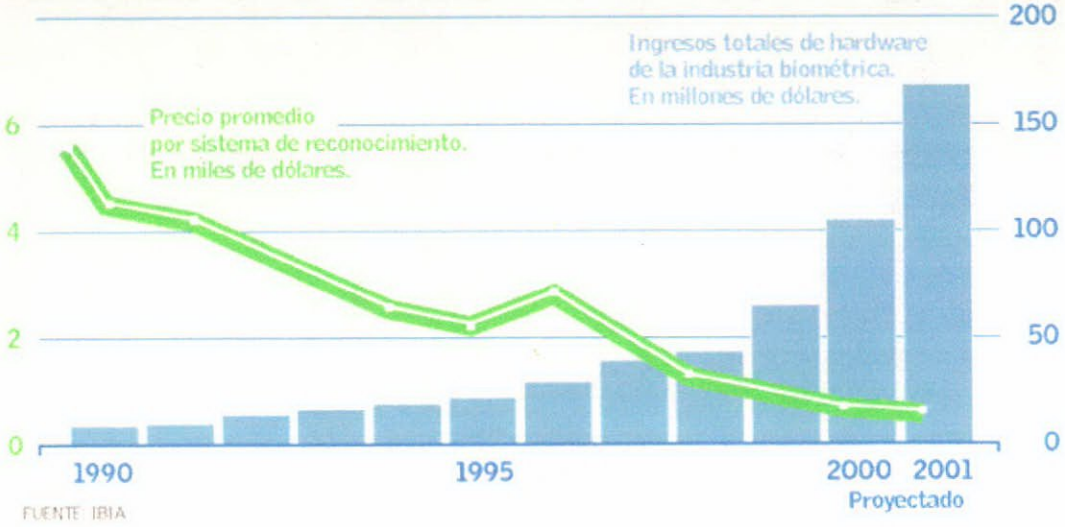
Composición del Mercado de Biométrica.

Fuente Bibliográfica: **REVISTA PODER**



RELACIÓN ESPERADA

■ La penetración de los sistemas de reconocimiento biométrico depende en buena medida de que sus precios en el mercado caigan aún más.



FUENTE: IBIA

Conclusiones

En esta primera parte del trabajo, el grupo de investigación ha concluido con el relevamiento general de estructuras de los organismos bajo estudio. Esto permite un mayor análisis y el planteo de un estudio de factibilidad para la aplicación de técnicas biométricas en las áreas bajo estudio.

El análisis de mercado de insumos para la captura de datos biométricos resultó positivo, aunque se necesitan de mayores detalles para la implementación de los mismos en cuanto a costos, confiabilidad en la vida útil, operación y otras características de los mismos que serán abordadas en los subsiguientes informes.

La reingeniería de procedimientos relacionadas con la implementación de tecnologías biométricas ha sido ampliamente aceptada por los organismos bajo estudio, por lo que en este momento se avanza en un relevamiento detallado junto con personal de los mismos.

Referencias Bibliográficas

[1] G. Drets & H. Liljenström, "Fingerprint Sub-Classification and Singular Point Detection", International Journal of Pattern recognition and Artificial Intelligence, vol. 12, no. 4, 407-422, 1998.

[2] M. Eleccion, "Automatic Fingerprint Identification", IEEE Spectrum, vol. 10, 36-45, 1973.

[3] R. González y R. Woods, Digital Image Processing, Addison-Wesley Publishing Company, Inc., 1992. Chap. 7.2.2.

[4] L. Hong and A. Jain, "Integrating Faces and Fingerprints for Personal Identification", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 12, pp. 1295-1307, 1998.

[5] A. Hrechack and J. McHugh, "Automated Fingerprint Recognition Using Structural Matching", Pattern Recognition, vol. 23, no. 8, pp. 893-904, 1990.

[6] B. Jähne, Digital Image Processing, Springer-Verlag, 1997. Chap. 14.5.

[7] A. Jain and R. Bolle, "On-Line Fingerprint Verification", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 4, 302-313, 1997.

[8] B. Miller, "Vital Signs of Identity", IEEE Spectrum, vol. 31, no. 2, 22-30, 1994.

[9] D. Morales, Reconocimiento Digital de Huellas Dactilares en base a Vectores de Características, Tesis de Ingeniero Civil Electricista, Universidad de Chile, 1999.

[10] N. Ratha, S. Chen, and A. Jain, "Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images", Pattern Recognition, vol. 28, no. 11, 1657-1672, 1995.

[11] N. Ratha, K. Karu, S. Chen and A. Jain, "A Real-Time Matching System for Large Fingerprint Databases", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 18, no. 8, pp. 799-813, 1996.

[12] R. Schalkoff, Digital Image Processing and Computer Vision, John Wiley & Sons, Inc., 1989.