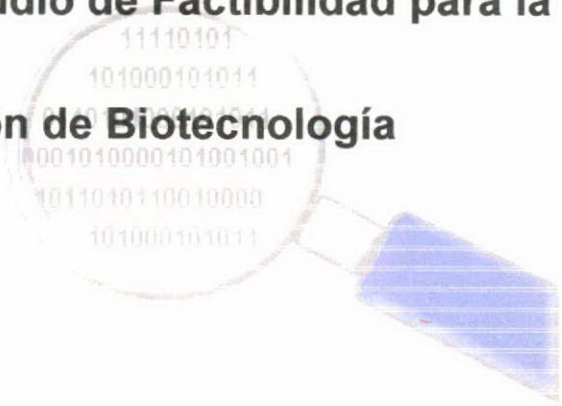
CONSEJO FEDERAL DE INVERSIONES

PROVINCIA DE MENDOZA

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



INFORME FINAL

DICIEMBRE 2002

Resumen del Trabajo Realizado

La experiencia experimentada con la ejecución el presente proyecto se considerar sumamente fructífera, puesto que se estiman alcanzados los objetivos planteados por el grupo de desarrollo al emprender el proyecto.

Se ha conseguido en este punto dejar sentadas las bases para una implementación exitosa de procedimientos de seguridad de acceso a la información (física o lógicamente), dejando una puerta abierta para la realización de un proyecto de aplicación de la tecnología. Dichas bases están conformadas por los diseños globales de aplicaciones estudiados en el presente trabajo, como así también por la asimilación que se ha logrado de los temas técnicos referentes a la biometría. Pretendemos hacer hincapié sobre este punto en particular, puesto que el principal beneficio obtenido, a nuestro entender, fue dotar a distintas áreas de un interés por la investigación y el desarrollo de nuevas aplicaciones, obviando en muchos casos los productos ofrecidos por terceros.

En la primer etapa del trabajo se consiguió conocer en forma global el accionar de algunas áreas, que a entender del grupo de desarrollo, resultaban de interés para aplicar los temas de estudio. Como se expresó anteriormente, se encontró en estos grupos de trabajo capacidades técnicas en muchos casos desaprovechadas, que si bien no estaban en su gran mayoría a la altura de desarrollar aplicaciones finales para atender la identificación

biométrica de su ámbito, pudieron analizar, comprender, y avanzar sobre los planes propuestos.

En la segunda etapa se realizó un diseño preliminar del la tecnología en base a la observación de algunas variables operativas, técnicas y económicas que determinaran la factibilidad de aplicación.

Por último, y concluyendo con el trabajo, se avanzó en el diseño de prototipos y en la observación más precisa de algunos procedimientos sobre seguridad de la información utilizados en la Administración Pública Provincial, dando ello lugar a la determinación de productos capaces de atender las necesidades técnicas y ubicándolos en el mercado existente (local o internacional).

Un objetivo no planteado al comienzo de trabajo, pero de orden personal fue poder estimular e impulsar a áreas de la Administración Pública Provincial a encarar nuevas actividades técnicas con personal propio. Un interés marcado en áreas como las relevadas permitió darle un mayor interés a la conclusión del proyecto.

La última tarea del grupo consistió en visualizar nuevamente, y dejar planteadas futuras acciones junto con personal técnico y superior de las áreas, para que estos puedan tender al desarrollo o contratación de la tecnología estudiada.

Autoridades

PROVINCIA DE MENDOZA	CONSEJO FEDERAL DE INVERSIONES
Gobernador de la Provincia Ing. Roberto Iglesias	**Secretario General** Ing. Juan José CIÁCERA
Secretario Administrativo Legal y Técnico Dr. Claudio Romano	**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

Resumen

El presente informe tiene por finalidad establecer la relación entre el relevamiento realizado al comienzo del proyecto y el diseño conceptual de una aplicación biométrica, en base a los requerimientos de seguridad existentes las actividades citadas de la Administración Pública Provincial. Asimismo, se realizarán recomendaciones sobre la implementación y uso de la tecnología biométrica en casos puntuales.

Se analizarán también algunas variables operativas para apoyar en un futuro la implementación de la tecnología biométrica.

Se ha utilizado la **guía orientadora de trámites** para ilustrar una de los puntos cruciales de este estudio, referente a **donde se debe realizar la autenticación** de usuarios y donde debe residir la base de datos conteniendo la información biométrica.

En cuanto a la aplicación de procedimientos para apoyar a la seguridad física de la entidad bajo estudio se ha realizado una subdivisión en cuanto a tres grandes campos de aplicación: 1) seguridad física, 2) enrolamiento de nuevos datos, 3) almacenamiento.

Análisis de Integración con Proyectos Actuales

A continuación se analizará el empleo y la adaptación que tiene la biometría en actividades actuales dentro de la Administración Pública Provincial, mas particularmente aquellos llevados a cabo dentro de la Unidad de Reforma del Estado.

Objetivos de este análisis:

1. uniformizar datos personales para su reutilización
2. uniformizar datos biométricos
3. uniformizar procedimientos

Los proyectos y actividades observadas en este punto son.

1. Sistema de Mesa de Entradas
2. Guía Orientadora de Trámites
3. Informatización del Registro Civil
4. Expedición de Cédula de Identidad
5. Control de Accesos y Asistencia

Sistema de Mesas de Entradas

El punto principal de análisis en este apartado es la integración de verificación biométrica con el sistema S.E.P.A. (seguimiento de expedientes y piezas administrativas).

La inquietud del personal de mesa de entradas es la puesta en marcha de un sistema de *workflow* que permita la transferencia de expedientes en forma electrónica. Un primer paso para conseguir esta operatoria es la aplicación tanto de seguridad lógica para certificar la veracidad de los documentos y transacciones, como de seguridad física para autenticar el acceso del agente público autorizado a las terminales destinadas a tal fin.

El objetivo principal de un sistema de mesa de entradas es agilizar el traspaso de la documentación que ingresa y/o egresa, descentralizando el control de Mesa de Entradas. A partir de ésta, y una vez efectuado los pases a las distintas oficinas, cada sector registra los pases efectuados y el tratamiento aplicado a los mismos. Al llevar el registro de estos pases, se reduce el pase de expedientes a Mesa de Entradas, y se pueden controlar los pases internos entre oficinas de un mismo sector.

La utilización de identificación biométrica en terminales adicionales ubicadas en distintas oficinas generadoras de pases descentralizaría aún más el trabajo de mesa de entradas, pudiendo cada agente identificarse unívocamente ante el sistema y operar movilizando piezas.

Tener el control de la información en cada sector poseedor del documento y, el hecho de poder registrar el tratamiento aplicado a cada pieza administrativa, hace posible el seguimiento y control del estado de situación de cada una de ellas. Para ello el sistema permite registrar la fecha de vencimiento del Trámite (pronóstico de culminación del trámite), activando una serie de alarmas para su seguimiento.

El tratamiento de expedientes y notas, requiere la definición de parámetros que rigen dicha actividad, niveles de confidencialidad, tipos de expedientes, tratamientos que se aplican a los mismos, nivel de prioridad, Temas generales de los que trata el expediente o la nota, etc. Todo esto configura un esquema de seguridad lógica que asegura la consistencia de los datos contenidos.

Administración del Sistema

1. Alta de Parámetros
    a. Códigos de Áreas
    b. Datos personales de agentes públicos
2. Alta de Usuarios
    a. Niveles de Verificación
    b. Niveles de Autorización y acceso
    c. Nivel de Confidencialidad
3. Enrolamiento de Datos Biométricos

Alcances

Se deberán tener en cuenta los nuevos requerimientos que podrían surgir de las distintas áreas usuarias que impliquen una adaptación del *software*. Este proceso involucraría tareas de adaptación de formularios y documentos, definición las reglas de integridad referencial que sustenten la validación de los procedimientos administrativos y el acceso a la información, tanto para la gestión interna como para la vinculación con otros sistemas o herramientas.

Las prestaciones del sistema propuesto están de acuerdo con aquellos sistemas de mesa de entradas tipo observados en el mercado, y a grandes rasgos abarca:

a. **Gestión de Notas**
b. **Ingreso de Notas**
c. **Pases**
d. **Recepción de Notas**
e. **Consultas**
f. **Gestión de Expedientes**
g. **Inicio de Expedientes**
h. **Pases**
i. **Recepción de Expedientes**
j. **Adjuntar Expedientes**

Políticas de Seguridad

Las políticas de seguridad para acceso y registración de datos estará determinada en base a políticas generales de acceso emanadas de las normas reguladoras de la actividad informática, vigentes en la Administración Pública Provincial (ej. Normas

ETAP). En particular se dictarán políticas de acceso físico a las terminales, basadas en las capacidades del sistema de seguridad biométrica. Las políticas de seguridad física deberán recaer en los siguientes puntos:

- Personal autorizado para Enrolamiento
- Personal autorizado para Baja de Usuarios
- Personal autorizado para manipulación de información enrolada
- Mantenimiento de las terminales. (dispositivos de captura biométrica y verificar la seguridad de acceso por la red informática) .

Guía Orientadora de Trámites

Esta herramienta informática fue creada para transmitir información al ciudadano sobre aquellos trámites de uso común realizados en la Administración Pública.

La creciente necesidad de utilizar transacciones vía Internet para actualizar la información, advierte la exigencia de nuevos métodos para la seguridad de acceso a las bases de dato de esta herramienta.

Para cubrir la necesidad de seguridad en la modificación de datos se propuso en una primera instancia la utilización de certificados digitales, con lo cual se garantiza el acceso solo de la terminal autorizada.

Se ha planteado que complementariamente se verifique el acceso del agente autorizado de la misma forma antes explicada para el caso de una mesa de entradas. Con esto conseguiríamos un producto inmediato a costo cero, que sería utilizar los puestos de consulta de la **guía orientadora de trámites** a lo largo de la provincia de Mendoza como mesa de entradas anexas a la Administración Central.

Tareas Realizadas en la Actualización de Datos. Procedimientos

1. Ingreso del usuario al sistema. Vía *tcp/ip* (página *Web*).
2. Autenticación de la terminal.
3. Autenticación del usuario (por intermedio de *password*).
4. Operación del Sistema

5. Cierre de sesión

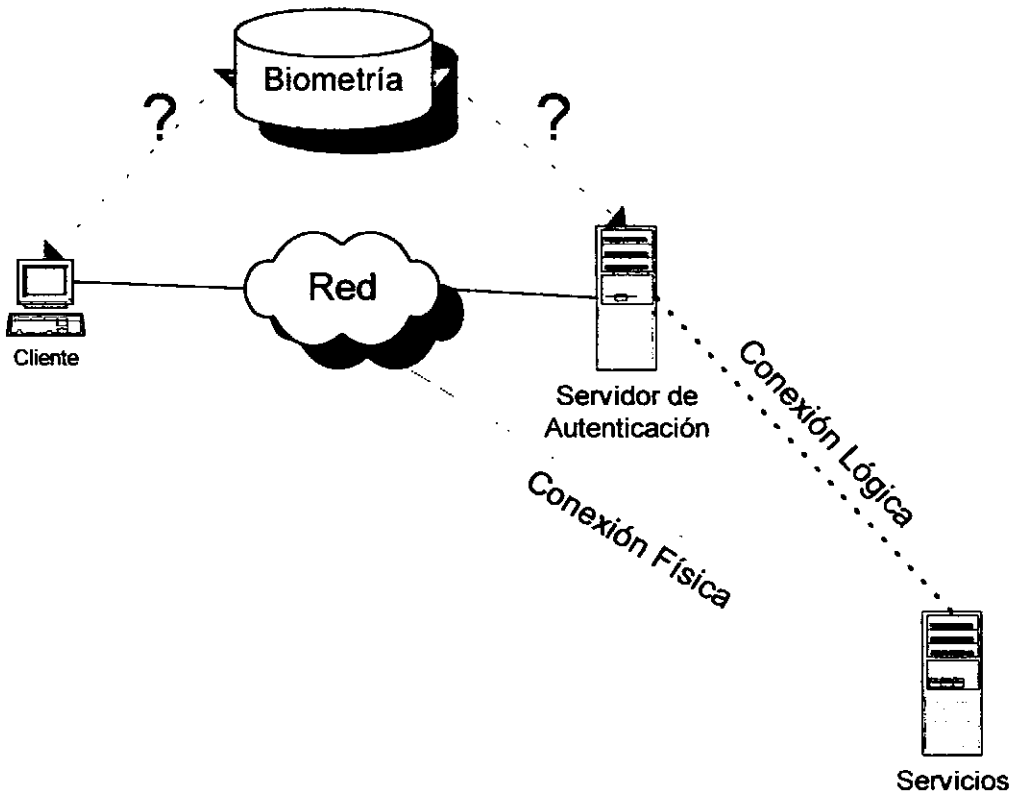
Autenticación Local. Autenticación Remota

Este punto es ideal para destacar un tópico sumamente polémico en lo referente a la autenticación biométrica en una red informática (de área local, metropolitana o ancha cualquiera fuere su naturaleza). Quién realiza la autenticación? El terminal cliente? El servidor ?

Si bien el dispositivo biométrico reside (está de más cualquier aclaración) junto a quien quiere autenticar su presencia; la duda surge cuando se pretende ejecutar el proceso (*software*) encargado de realizar la comparación contra la base de datos que contiene los datos enrolados. No es solo un tema técnico. Ambas soluciones funcionan!

La decisión sobre donde colocar los procesos de autenticación deberían ser evaluados a la luz de variables legales, técnicas, operativas. Por ejemplo, al distribuir los datos biométricos del personal enrolado deberían tenerse en cuenta todas aquellas normativas, provinciales, nacionales e internacionales que resguardan la privacidad de los datos personales.

La ubicación de los datos para la comparación (salvando aquellos aspectos referidos al diseño) indistintamente podría ser en el servidor o terminal cliente.



No solo se deberá tener en cuenta la ubicación de los datos, sino también los procedimientos de comparación.

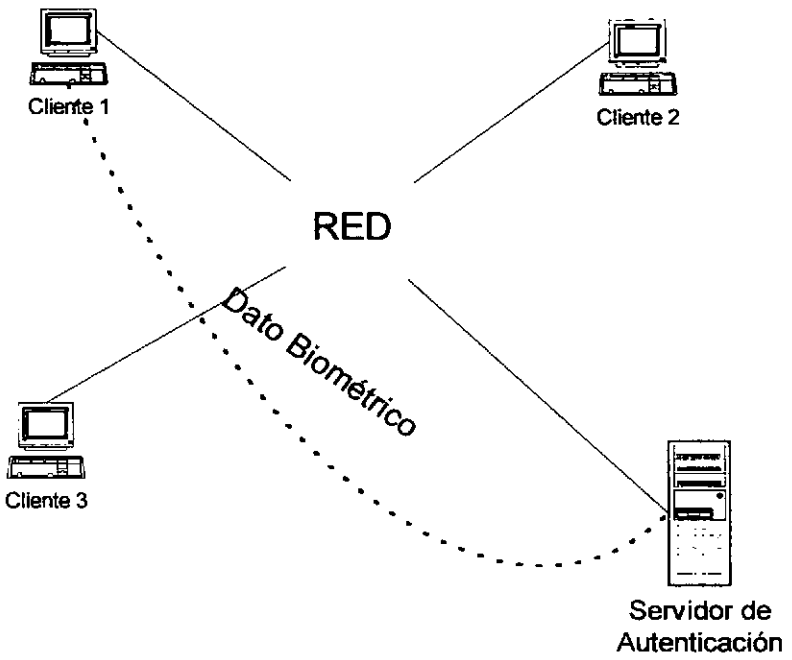
Un esquema muy utilizado actualmente es la verificación vía página web. Este formato es perfectamente aplicable a los procedimientos de carga de la **guía orientadora de trámites** (como así también a todos aquellos procedimientos que actúen transaccionando vía protocolo tcp/ip-página web-).

Para poder implementar este formato se deberá contar con componentes un poco más elaborados que páginas *html*. Una buena solución hallada, en base a una extensa investigación, son componentes *JAVA (java applets)* capaces de comunicarse con el

scanner del cliente. Una vez solucionada la comunicación scanner-máquina cliente-máquina servidora, se deberá tener en cuenta un canal seguro de envío de información (biométrica o no). Para ello se aconseja complementar la autenticación biométrica, con la implementación de un canal seguro (protocolo SSL).

Flujo de Información

El problema que podría presentarse una vez realizada la autenticación biométrica, sería el robo de información en un canal compartido, situación que echaría por tierra todos los esfuerzos realizados al asegurar la identidad del operador.



Supongamos la situación en donde el cliente es correctamente identificado por el sistema biométrico (y posteriormente autorizado a operar). De uno u otra forma la información sobre la correcta identificación deberá viajar desde el cliente hasta el servidor para que el mismo haga disponibles sus servicios al cliente. Esta transmisión, como ya fue expresado, se realiza sobre un canal compartido (red informática). La intercepción de tal información por parte de un intruso provocaría una situación muy desagradable.

Para ello es conveniente, utilizar una comunicación codificada, apoyada por protocolos de comunicación que permitan la encriptación de la sesión entre el cliente y el servidor para tornar ilegible tal información para cualquier intruso intentando "leer" el canal.

Informatización del Registro Civil

Este proyecto tiene por principal objetivo la digitalización del índice general de libros y actas existente en el Archivo General del Registro Civil.

La relación principal con la tecnología biométrica fue observada durante el proceso de carga del índice general de actas, al advertir que algunas de las mismas contaban con la impresión de dígito pulgar derecho, al no poder contar con la información estándar requerida.

Sería deseable también, si bien su implementación es sumamente dificultosa, asentar algún dato biométrico de la persona inscripta; puesto que si alguna base debería contenerla, sin dudas debería ser la utilizada por el Registro Civil y Capacidad de las Personas, por su carácter de Responsable de la registración de los datos personales de la población.

Expedición de Cédula de Identidad

La Policía de Mendoza, evalúa actualmente junto con el Comité de Reforma del Estado la implementación de mejoras en la expedición de la Cédula de Identidad Policial. Se ha evaluado, junto a empresas locales la posibilidad de modernización de la misma, teniendo en cuenta los siguientes puntos:

- Material base para la impresión
- Inclusión de un carácter biométrico de mayor calidad al actual.
- Fotografía Digital
- Almacenamiento de los datos fotográficos y biométricos.
- Generación de un índice de los datos almacenados.

Control de Accesos y Asistencia

Los sistemas comunes de control de acceso y asistencia, generalmente, se basan únicamente en un código que identifica a cada miembro de su personal, y que está grabado en una tarjeta de papel, banda magnético o código de barras.

En algunos casos se cuenta con un *PIN* adicional. Sin embargo **no existe una garantía de que la persona que marca su tarjeta sea efectivamente la persona a quien está frente al dispositivo**. Los sistemas biométricos se basan en características individuales de las personas y por lo tanto no pueden ser suplantadas.

De todos los sistemas biométricos en el mercado, el uso de la huella digital ocupa el primer lugar por su efectividad.

Se ha evaluado a este respecto un sistema que permita manejar el acceso a los dispositivos biométricos.

Capacidades del Sistema Evaluado

- Generación de Reportes

  Los mismos permiten filtrar la información capturada de acuerdo con una gran variedad de criterios personalizados.
- Puede mostrar accesos del personal a las áreas controladas por estos dispositivos.

- Puede calcular el número de horas trabajadas por cada persona en un período determinado, lo que facilita el cálculo exacto y oportuno de la nómina, con la certeza de que el personal ha cumplido sus obligaciones.

Si bien el propósito de los sistemas de este tipo es la generación de estadísticas de acceso para su posterior contabilización, se ha encontrado en el mismo una solución sumamente importante para nuestro trabajo. En informes anteriores se hizo notar la necesidad de dispositivos para garantizar la seguridad de acceso a determinados recintos (por ejemplo la Penitenciaría Provincial).

La utilización de este sistema podría proveer a la Penitenciaría Provincial de un instrumento para registrar (unívocamente) a quien ingresa a su interior, pudiendo enrolar a aquellos individuos realmente autorizados a ingresar.

Estudio de los Modelos de Datos de Proyectos Afines

Datos Personales

Se han analizado los datos contenidos en las principales bases de datos que contienen información personal. (Policía de Mendoza y Registro Civil y Capacidad de las Personas).

La primer etapa es la generación de un diccionario de datos general para identificar los principales **elementos de dato** con el fin de diseñar un posible cruzamiento de la información contenida en ambas bases de datos; con la posibilidad de poder reutilizar la misma.

Se recomienda en este punto, trabajar conjuntamente con personal de análisis y diseño de sistemas de cada una de las áreas interesadas en la reutilización de datos. A los fines de este estudio no se ha contado con la colaboración suficiente como para concluir totalmente el diseño de la base de datos general. No obstante ello, se ha realizado un examen de los datos principales utilizado en las bases de datos centrales de tales organismos.

Datos Comunes Relevados

Datos Comunes	
Lugar de Nacimiento	
Tipo de Documento	
Número Documento	
Nombre y Apellido	
Sexo	
Tipo Documento Madre	
Número Documento Madre	
Nombre y Apellido Madre	
Tipo Documento Padre	
Número Documento Padre	
Nombre y Apellido Padre	
Fecha de Inscripción	
Fecha Nacimiento	
Observaciones	
Datos propios de la institución	Información puntual de la operatoria electrónica de cada una de las áreas de estudio
Índices a otros datos	Datos Prontuariales. Policía de Mendoza. Registro Civil
Metadatos Varios	Información varia contenida en las bases de datos para permitir la mejor recuperación desde la misma; y la relación con archivos relacionados.

El fin principal de este estudio (determinación de los datos comunes) es allanar el camino para la introducción de información biométrica **normalizada** para todas aquellas instituciones que necesiten hacer uso de ella.

A partir de los datos **reutilizables** se aconseja que en el diseño detallado se consideren procedimientos seguros de migración de datos hacia una base de datos única.

Migración de Procedimientos de Seguridad Convencionales

La migración de procedimientos de seguridad deberán estar provistos de métodos confiables que garanticen la continuidad de los procesos. Para ello se aconsejan los siguientes pasos a seguir.

1. Determinación de Políticas de Seguridad y Objetivos

   Determinar:

   Para qué cambiar mi sistema de acceso a los datos?

   Quién podrá...? Quién no podrá...?

2. Determinación de Procedimientos

   Conjunto de tareas y pasos para la autenticación, verificación y acceso a la información.

3. Determinación de Métodos y Estándares

   Determinar las bases técnicas y tecnológicas en las que se basarán los técnicos para realizar las tareas en forma precisa.

4. Difusión

   Concebida en la etapa de determinación de políticas de accesos y aplicadas en este punto, hacer conocer al personal del área de aplicación en detalle los objetivos y a grandes rasgos los nuevos procedimientos de acceso a la información.

5. Capacitación

   Capacitar al personal encargado de acceder a la información protegida los nuevos procedimientos. Se recomienda circular el manual de procedimientos.

6. Control y Retroalimentación

   El sistema deberá poseer distintos niveles de control para poder cumplir con los estándares vigentes sobre seguridad de sistemas.

Controles

1. Control General del Sistema de Seguridad

   Este tipo de control debe ser administrado por el personal jerárquico del área encargada del procesamiento de datos, en concordancia con las políticas de seguridad oportunamente establecidas.

   - Compra, mantenimiento y uso de dispositivos e insumos.
   - Determinar el personal autorizado a operar el subsistema de seguridad.

2. Controles Administrativos

   a. Verificar la existencia de una políticas de controles
   b. Control del Personal autorizado a operar el subsistema de seguridad.
   c. Determinación de un Plan de Sistemas de Información Estratégico

d. Verificación de la vigencia de garantías sobre los equipos utilizados, uso de patentes, etc.

3. Controles de Entrada
    a. Verificación de introducción de información. Se deberá analizar la correspondencia entre el dato biométrico tomado, con los procedimientos de recuperación de la base de datos de los datos enrolados.
    b. Verificación de campos

4. Controles de Procesamiento
5. Controles de la Base de Datos
    e. Físico
    f. Bibliotecario
    g. Respaldo de datos
6. Controles de Salida
7. Control de documentación
8. Controles de Hardware
    h. Control integrado
    i. Control del software del proveedor
9. Control del Sistema Operativo
10. Control de Operaciones de la Computadora
11. Controles de Seguridad
    j. Control de Acceso físico

k. Ubicación Física

l. Protección Física

12. Técnicas de Seguridad de Procedimientos

m. Integridad

n. Aislamiento

o. Identificación

p. Autorización

q. Verificación de Autenticidad

r. Monitoreo de los procesos de autorización. Generación de estadísticas.

Integración con Técnicas de Identificación Unívoca (no biométricas)

La Firma Digital

La utilización de firma digital para la ejecución de transacciones es un complemento esencial para la aplicación de técnicas de seguridad física. Por ello, en este punto, expondremos las capacidades de la misma y la forma de integración con la tecnología biométrica.

Ventajas Ofrecidas por la Firma Digital

El uso de la firma digital satisface los siguientes aspectos de seguridad:

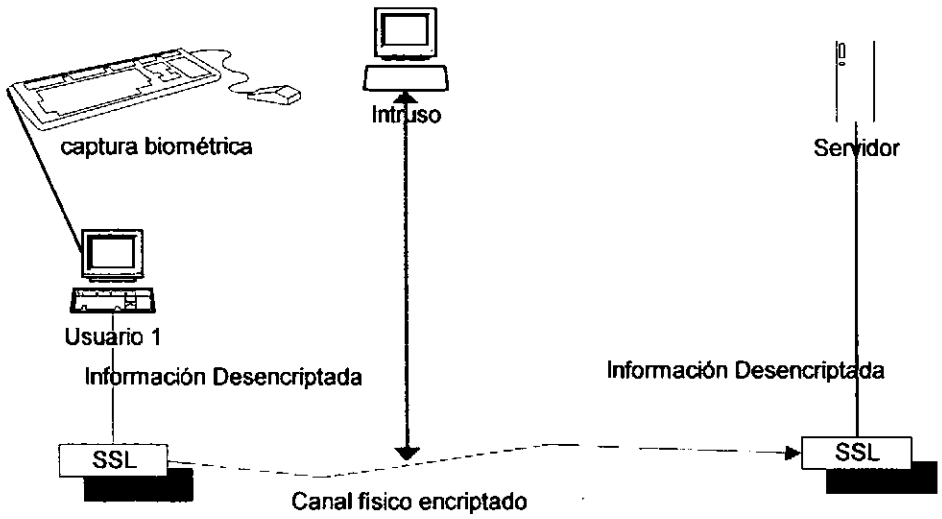
- **Integridad de la información**: la integridad del documento es una protección contra la modificación de los datos en forma intencional o accidental. El emisor protege el documento, incorporándole a ese un valor de control de integridad, que corresponde a un valor único, calculado a partir del contenido del mensaje al momento de su creación. El receptor deberá efectuar el mismo cálculo sobre el documento recibido y comparar el valor calculado con el enviado por el emisor. De coincidir, se concluye que el documento no ha sido modificado durante la transferencia.

- **Autenticidad del origen del mensaje**: este aspecto de seguridad protege al receptor del documento, garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema. Esto se logra mediante la

inclusión en el documento transmitido de un valor de autenticación (MAC, Message autentication code). El valor depende tanto del contenido del documento como de la clave secreta en poder del emisor.

- **No repudio del origen**: el no repudio de origen protege al receptor del documento de la negación del emisor de haberlo enviado. Este aspecto de seguridad es más fuerte que los anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje, transformándose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema.

Cuando hablamos sobre firma digital, nos referimos comúnmente a archivos que han sido **alterados** introduciendo en ellos una marca que relaciona la misma de una manera única con el contenido del archivo. Ello permite asegurar la autoría del este. En nuestro estudio utilizaremos este concepto para hablar de **sesiones o comunicaciones firmadas**.



Un modelo muy común utilizado para proteger un canal inseguro, por intermedio de la encriptación de los datos transferidos es la utilización del protocolo SSL. (Para muchos autores el concepto de canal seguro difiere mucho del concepto de firma digital. Nosotros utilizamos ambos a un mismo nivel para señalar mecanismos de protección).

Otra beneficio encontrado en la utilización de firma digital es, como fue expresado anteriormente, la identificación del autor de un documento.

Descripción Detallada de los Procedimientos (manual/automatizado)

A continuación se describirán aquellos procesos manuales observados en la etapa de relevamiento y la intención de automatización de los mismos.

Trámite de Cédula Identidad Utilizando Dispositivos Biométricos

Entrega de Turnos – Mesa Entrada

A la persona que necesita realizar el trámite se le entrega un turno, para ser atendido posteriormente. El turno especifica el nombre, **apellido, y DNI de la persona, fecha y hora del turno, y trámite** que desea realizar. Con estos datos (Nombre, Apellido y DNI) se consulta el Sistema para verificar la existencia o no de Prontuario ya asentado. Dependiendo de la existencia o no de prontuario se confirma la hora del turno.

Con este turno se debe esperar en el salón a ser llamado. En caso de no encontrarse presente la persona al momento de la llamada, se pierde definitivamente el turno obtenido.

Si la persona tiene prontuario se coloca en el turno el número de prontuario correspondiente para ser verificado posteriormente. Si la persona no tiene prontuario se deberá, se coloca en el turno como **NIL – (No Identificada Legalmente)**.

Control de Identificación Legal - Mesa Entrada

Se solicita la presencia del interesado por mesa de entrada (Salón), luego se toma el Turno entregado, y se controla el estado de la persona que solicita la generación de cédula de Identidad, el mismo puede ser:

A. Identificada legalmente o

B. No Identificada Legalmente

A. Si la persona se encuentra Identificada Legalmente para lo cual se cuenta con el Número de prontuario colocado en el Turno, se analiza el prontuario correspondiente y verifica la existencias de causas pendientes.

A.1. En caso de **constar alguna causa** en el Prontuario, se detiene inmediatamente el trámite comenzado y se deriva a la persona a Causas Judiciales para la resolución de su estado judicial.

A.2. En caso de **no constar causas judiciales pendientes**, se audita la información contenida y si se encuentran inconsistencias en la base de datos, se deberán actualizar los datos almacenados.

B. Si la persona no se encuentra Identificada Legalmente se envía a Dactiloscopia.

Dactiloscopia

En esta área son tomadas las huellas dactilares mediante el **verificador Biométrico (situación propuesta).** Se confrontan las mismas con las huellas dactilares almacenadas en el sistema, lo que arroja las posibles alternativas encontradas en la base de datos, por intermedio de una interfaz de usuario.

El personal dactiloscópico se encarga de definir finalmente la concordancia de la información Biométrica tomada de la persona con la existente en la base de Datos. A continuación se imprimen las huellas tomadas.

En caso de no encontrarse correspondencia con los datos mantenidos, se debe proceder a la carga de los datos de la persona no identificada legalmente. Contrariamente, en caso de encontrarse los datos, se coloca el número de prontuario correspondiente, y vuelve el trámite a Mesa de entrada para comenzar con los pasos mencionados.

Carga de Datos

Junto a la información biométrica tomada se procede a la carga de información de la persona para dejar registrada Identificación legal de la misma. Los datos que deberán registrarse en esta instancia son los siguientes:

- Datos Personales
- Domicilio Real
- Datos prontuariales
- Datos Complementarios
- Antecedentes judiciales
- Ficha
- Señas particulares
- Familiares y Amigos
- Antecedentes Judiciales

A continuación se tomará la **foto digital de la persona (situación propuesta)**, la que será colocada en la Cédula y se mantendrá en la Base de Datos.

Una vez concluida la carga de datos y la toma de datos biométricos se envía a la persona a abonar el trámite realizado.

Generación de Recibo - Mesa Entrada

Se emitirá un recibo comprobante de Pago del Trámite realizado "Cédula Identidad" para retirar. Se pretende que esta tarea quede también bajo los límites de automatización propuestos.

Entrega de Cédula Identidad - Expedición

La persona se acerca con el Comprobante de pago emitido, y se le entrega la Cédula de identidad.

Certificado de Buena Conducta

Entrega de Turnos

A la persona que necesita realizar el trámite se le entrega un turno, para ser atendido posteriormente. El turno especifica el **nombre, apellido, y DNI de la persona, fecha y hora del turno, y trámite** que desea realizar.

Con estos datos (Nombre, Apellido y DNI) se consulta al Sistema para verificar la existencia o no de Prontuario. Dependiendo de la existencia o no de prontuario se confirma la hora del turno. Con el comprobante del mismo se debe esperar en el salón ser llamado. En caso de no encontrarse presente la persona al momento de la llamada, se pierde definitivamente el turno obtenido. (no registrándose la novedad de la visita).

Si la persona tiene prontuario se coloca en el turno el número de prontuario correspondiente para ser verificado posteriormente. Si la persona no tiene prontuario se deberá, se coloca en el turno como **NIL - NO IDENTIFICADA LEGALMENTE.**

Mesa Entrada

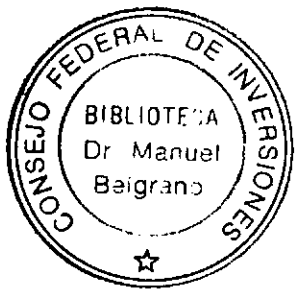
Se solicita la presencia del interesado por mesa de entrada (Salón), se toma el Turno entregado, y se controla el estado de la persona que solicita la generación de cédula de Identidad, el mismo puede ser, **Identificada legalmente o no Identificada Legalmente**

Si la persona se encuentra Identificada Legalmente, se analiza el prontuario correspondiente y verifica la existencias de causas judiciales pendientes.

1. En caso de **constar alguna causa judicial** en el Prontuario, se detiene inmediatamente el trámite comenzado y se deriva a la persona a Causas Judiciales para la resolución de su estado judicial.
2. En caso de **no constar causas judiciales pendientes**, se auditan la información contenida y si se encuentran inconsistencias en la base de datos, se deberán actualizar los datos almacenados.

Si la persona no se encuentra Identificada Legalmente se envía a Dactiloscopia.

Se puede observar que los últimos trámites relevados cuentan con un alto grado de similitud en su operatoria. Esto facilitará las tareas a la hora de automatizar dichos procesos.



Procedimientos con Detenidos

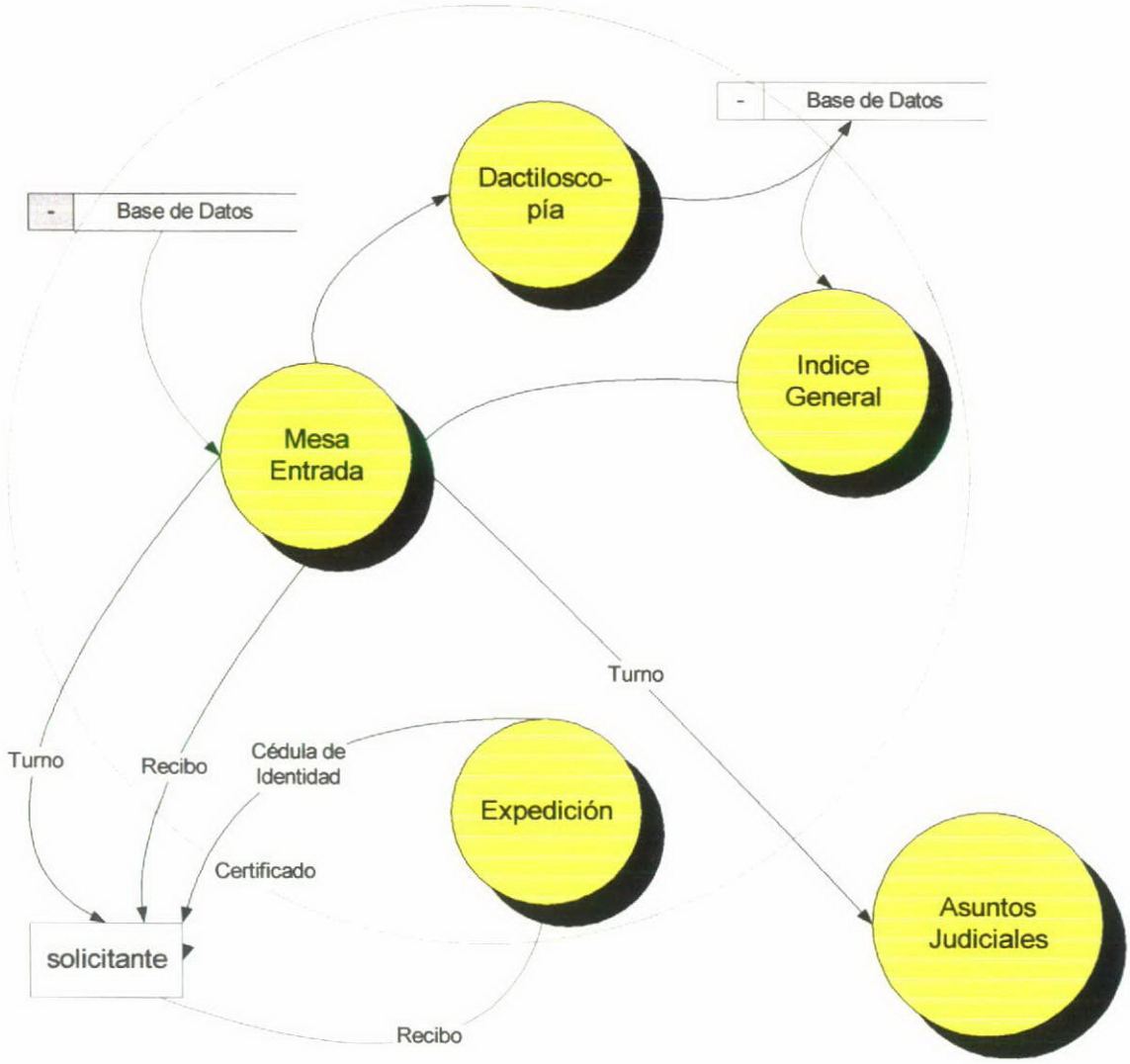
Mesa de Detenidos

El procedimiento es muy similar al del trámite de la Cédula. La persona detenida, se demora en Guardia de Prevención, Mesa de Entrada

Se envía a Índice General los datos que para verificar existencia de prontuario, si se encuentra **NIL** se envía a dactiloscopia para confrontación con la información almacenada.

A continuación, dependiendo de la información obtenida se generan distintos procesos internos que no abordaremos en nuestro estudio.

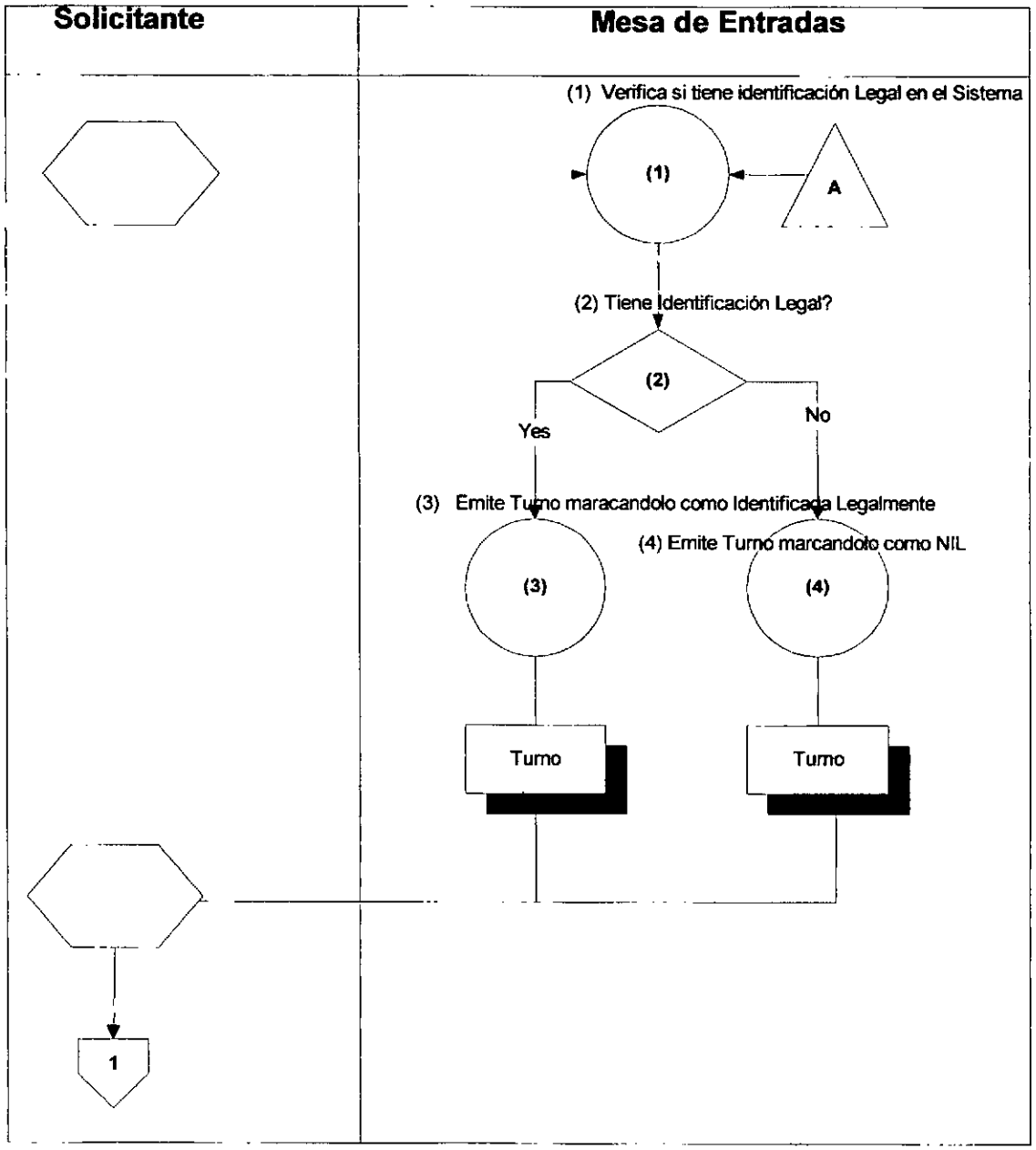
Limites de Automatización de la Propuesta



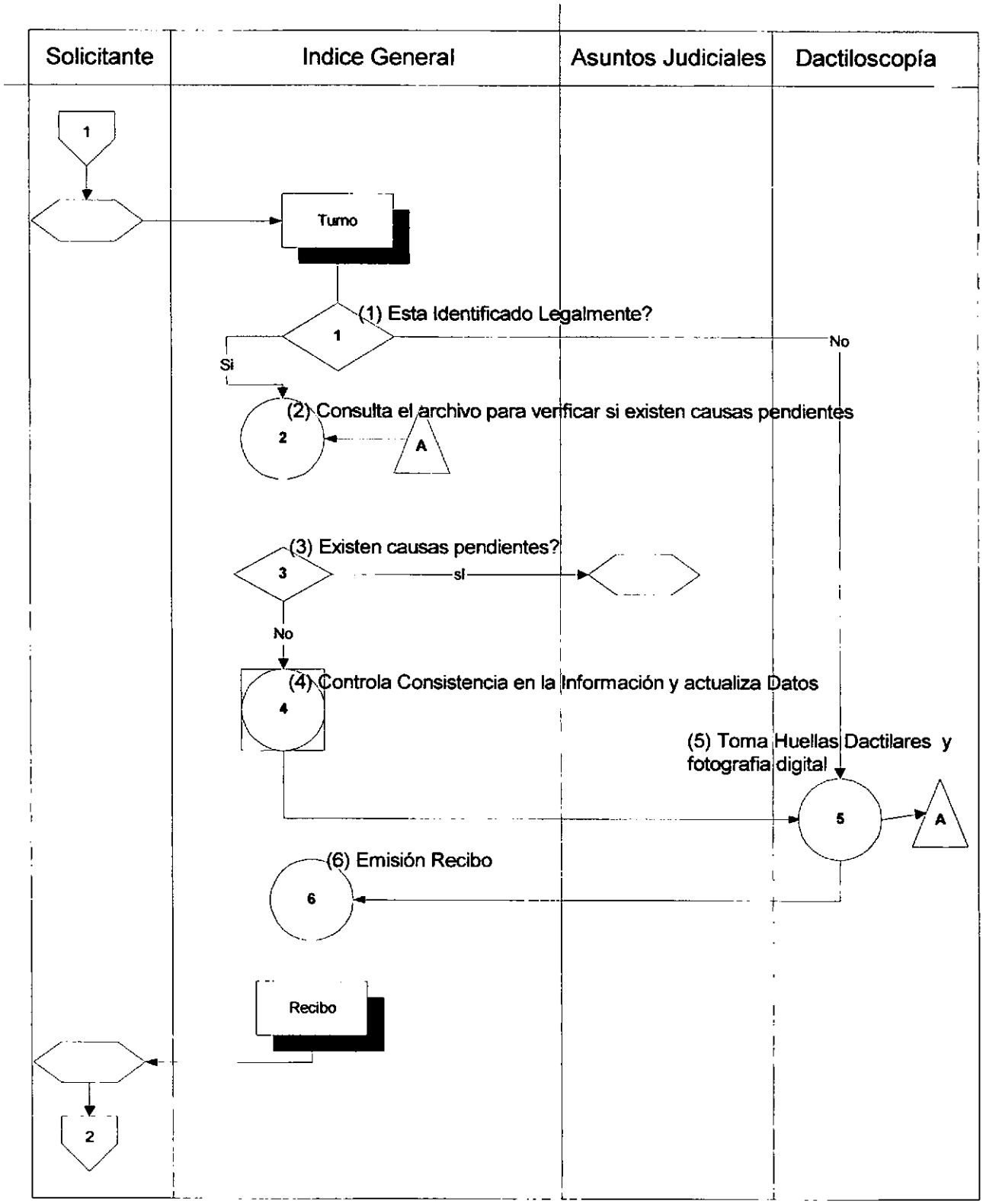
DFD- Diagrama de Flujo de Datos

Tramite Cédula Identidad

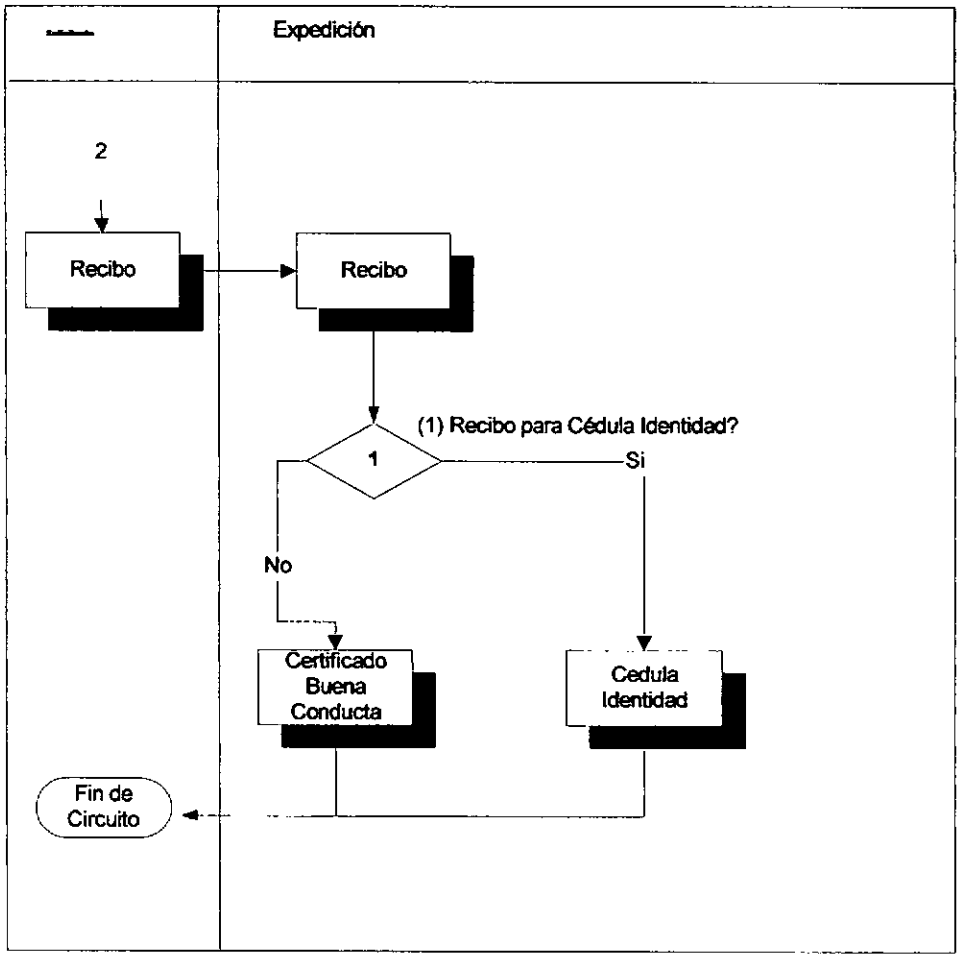
Entrega Turno



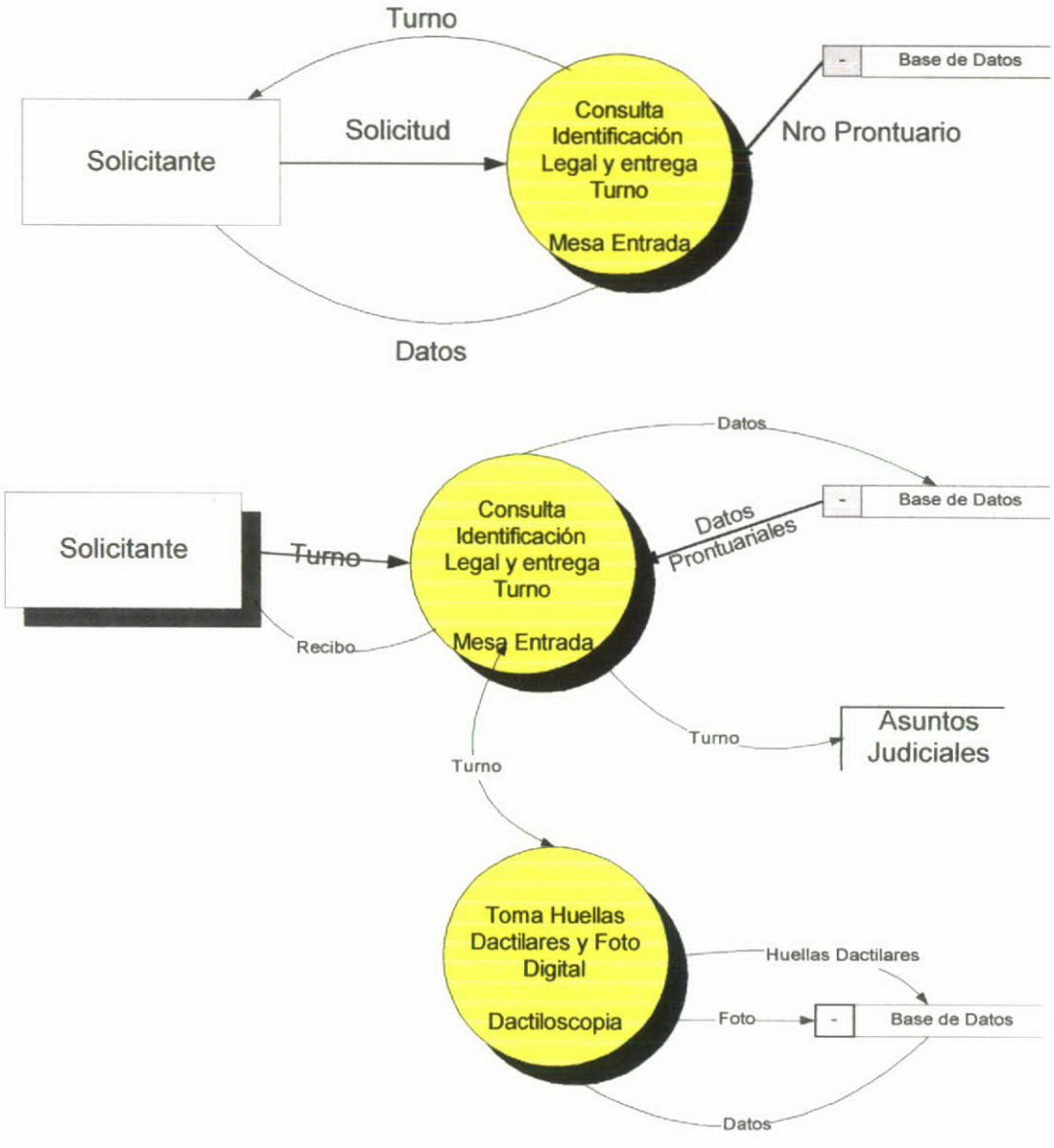
Identificación Legal



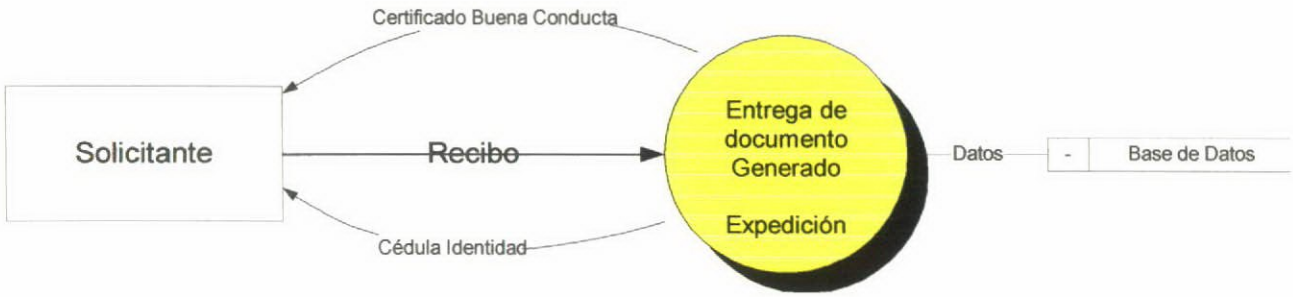
Expedición de Documento



Entrega de Turnos e Identificación Legal



Entrega de Documento



En forma similar se han analizado los procedimientos de

1. Trámite Certificado Buena Conducta
2. Detenidos
3. Consultas Externas

Identificación del Universo de Aplicación de la Biometría

A continuación en forma resumida, se nombrarán aquellas aplicaciones a tener en cuenta para la aplicación de biometría en la Administración Pública Provincial.

Penitenciaría Provincial

- Subsistema de Registración de Internos
- Subsistema de Registración de visitas
- Subsistema de Administración de Personal.
- Subsistema de control y transferencia de información.

Policía Provincial

- Cédula de identidad
- Archivo general de prontuarios

Guía Orientadora de Trámites

- Subsistema de carga y modificación de datos

Registro Civil

- Subsistema de captura de datos biométricos.
- Subsistema de firma de registro

Propuesta de Aplicación

La propuesta a realizar se basará en dos variables

- Los productos observados en el mercado.
- Prototipo conceptual de una aplicación biométrica.

Relevamiento de Productos

Hardware

En cuanto al equipamiento necesario utilizado para la captura de datos biométricos se han analizado, y se recomiendan tres tipos principales.

Ratón Biométrico

Este dispositivo es sumamente fácil de instalar y mantener. Generalmente el software de este dispositivo, en el momento del enrolado solicita el ingreso de la huella tres veces comparando las tres tomas para asegurar una buena calidad de la toma.

Los precios observados para este tipo de dispositivos puede rondar entre los $400 y $750. El hardware y software de scanneo provisto por un BioMouse compara una muestra de huella digital tomada contra una ya almacenada en memoria. El proceso es rápido, seguro y amigable.

Si cada computadora personal tiene un usuario designado, por defecto se podría obviar el *login* por intermedio de usuario y *password* facilitando el acceso al terminal solamente con la presión del dedo enrolado. La toma de un dedo no enrolado puede

producir una caída en la performance en el proceso de comparación, pero generalmente en estos dispositivos el software no es demasiado sensible a estos problemas.

Estándares Técnicos Aceptables para Este Dispositivo

1. Resolución de 440 dpi
2. Medidas. Ancho: 54mm. Largo: 65mm. Alto: 27mm
3. Falsa aceptación esperada: 1 / 1.000.000
4. Falto rechazo esperado: 1 / 100.000
5. Interfaz USB.

Scanner Biométrico

Este es un dispositivo dedicado exclusivamente a tomar una muestra de huella digital.

Este dispositivo generalmente utiliza tecnología óptica de alta calidad, que asegura la calidad de la toma aún cuando el dedo se encuentra sucio, húmedo o dañado.

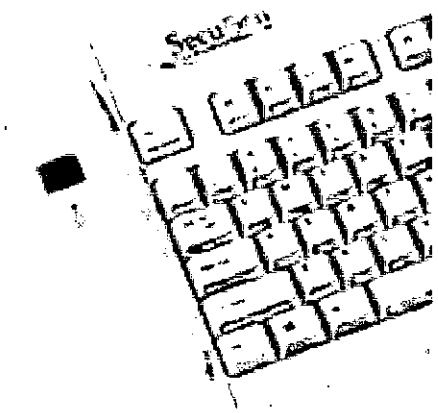
Estándares Técnicos Aceptables para Este Dispositivo

1. Medidas. Largo: 96mm. Ancho: 60mm. Alto: 31mm.
2. Peso: 150 gramos
3. Sensor Biométrico: Área de captura: 17mm x 17mm.
4. Resolución Horizontal: 530 DPI.
5. Resolución Vertical: 380 DPI.
6. Rotación Permitida: 360°.
7. Interface: USB. Transferencia de datos hasta 12MB.
8. Voltaje: 4.4 a 5.25 V por el puerto USB. 8mA en modo ahorro de energía.

Teclado Biométrico

Este innovativo teclado provee un mecanismo de seguridad en paralelo al incorporar un lector de huella digital.

Con este dispositivo, encontramos una solución para el ingreso autenticado a una red informática compartida, a un bajo costo y con beneficios extra suministrados por el software provisto con el equipamiento.



Características

- Reconocimiento del estado y clase de la huella digital.
- Sensor de resistencia y prueba contra impacto.
- Rápida velocidad de verificación (menor a un segundo).
- Layout estándar de teclas
- 6 teclas para multimedia
- Puerto USB o paralelo

Estándares Técnicos Aceptables para Este Dispositivo

1. Tiempo de Verificación menor a un segundo.
2. Resolución: 500 DPI
3. Área testeo 0.55 x 0.65 pulgadas (16,6mm x 16,2 mm)
4. Dimensiones. Ancho: 195mm. Largo: 510mm. Alto: 45mm.

5. Peso de la unidad óptica: 28 gramos
6. Temperatura soportada: -40° a 70°
7. Voltaje: 5VDC +- 5%

Software Incluído

Desktop Security, incluyendo *login* para *windows*, salvapantallas y codificación de archivos y carpetas.

Ejemplos de Aplicaciones de Seguridad

Este teclado ha sido probado por el proveedor en los siguientes servicios:

- Seguridad en PC/Workstations
- Seguridad en redes de la empresa
- Contenido de seguridad para Internet
- E-COMMERCE
- Transacciones electrónicas
- Sistemas de bancos y financieros
- Sistemas de información médica
- Cualquier aplicación basada en *passwords*,

no encontrando inconvenientes en cuanto a la confiabilidad de la autenticación de personas ante los sistemas de producción.

Tarjeta Inteligente

La tarjeta inteligente ofrece una solución alternativa al problema de control de acceso y autenticación. También ofrece ventajas adicionales al ser capaz de almacenar certificados digitales.

Con un lector anexo a la computadora, este sistema provee la primer línea de autorización de ingreso a una red informática.

En lugar de una banda magnética, como se puede visualizar comúnmente en tarjetas de crédito, las tarjetas inteligentes contienen un *chip* de almacenamiento aproximadamente de un centímetro cuadrado. El estándar ISO 7816 define las características físicas y lógicas de una tarjeta inteligente, como la forma, posición de los contactos, sus funciones, interfaces de usuario y estructura de archivos.

Dependiendo de la función de la tarjeta, el *chip* puede consistir en una memoria EPROM a un conjunto de procedimiento ejecutables insertados en el mismo chip, incluyendo un pequeño procesador (de 8 bits por lo general), RAM, ROM y EEPROM.

La CPU contenida puede procesar información compartida y almacenada, permitiendo que la tarjeta sea utilizada en una gran variedad de aplicaciones.

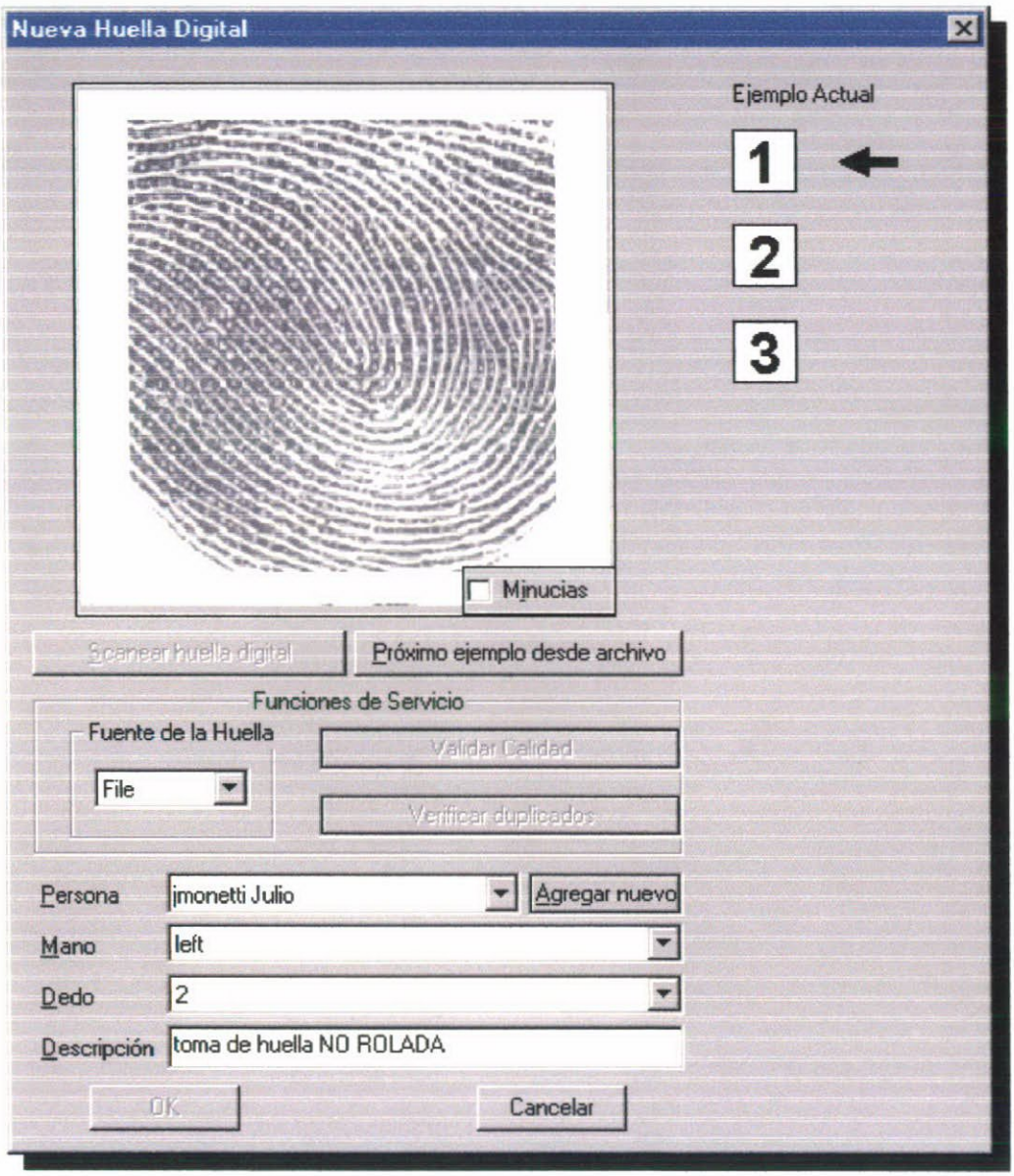
Cuando se inserta una tarjeta en un lector, esta provoca un contacto eléctrico a través de sus conectores que transfieren datos desde y hacia el *chip*.

Software

La investigación sobre la existencia de software (independiente del *hardware* utilizado) arrojó un conjunto de productos aptos para su utilización, los cuales presentan generalmente precios accesibles.

Se experimentó simulando una toma de muestra con el *software FingerPoint*, obteniendo un buen resultado al intentar analizar una huella digital. Como lo ilustrar la siguiente imagen, este *sofware* permite obtener diferentes muestras desde un archivo o directamente del scanner de huella digital, asignándole distintos datos a cada una de las imágenes.

Esta imagen muestra la imagen de una huella digital obtenida de un archivo gráfico con formato estándar.



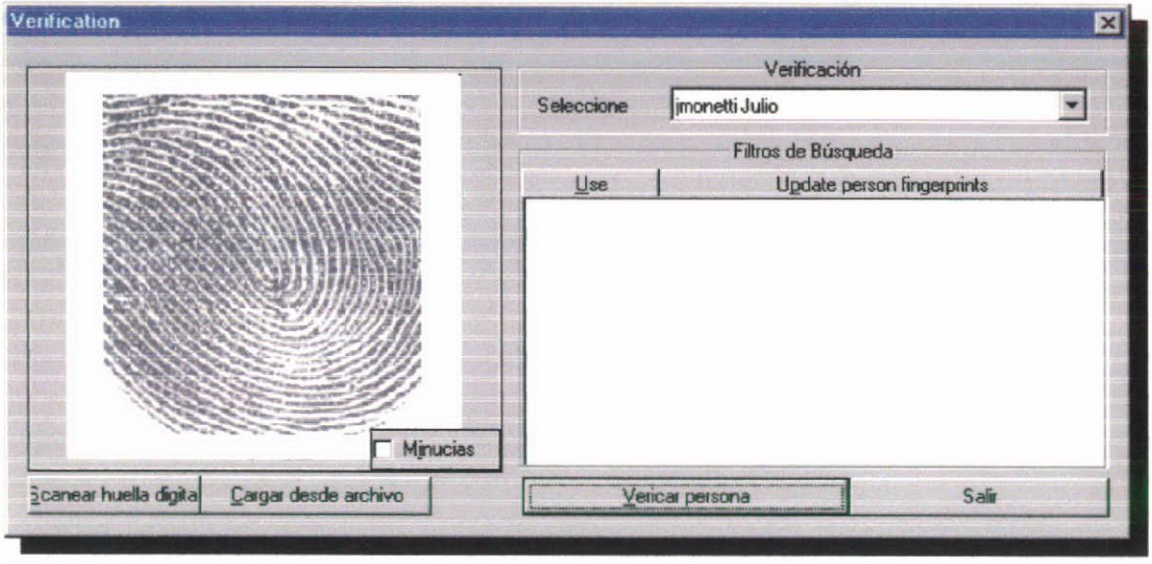
Una de las capacidades buscadas por quien trabaja en el mundo de la biometría, más particularmente con el análisis de huella dactilar es la determinación de los puntos particulares, o minucias.

Las minucias son extraídas por software especializado, encargado de recorrer la imagen analizada a través de sus líneas, identificando rotaciones, curvaturas y puntos de cruce. Con esta información el software podrá determinar puntos discretos a lo largo de la curva de cada una de las líneas analizadas.

Este análisis permitirá una mejor comprensión de las características de la huella digital, como así también agilizar su almacenamiento, utilizando una porción mínima de almacenamiento comparada con el almacenamiento de la imagen completa.

El *software* permite el análisis de los puntos característicos de la huella, con la posibilidad de aislar las **minucias** de la misma.

El software posibilita también, relacionar distintas tomas (los distintos dedos de un individuo) con la ficha personal.



Otros Productos Observados

- **Veritas**
- **Veriprint**

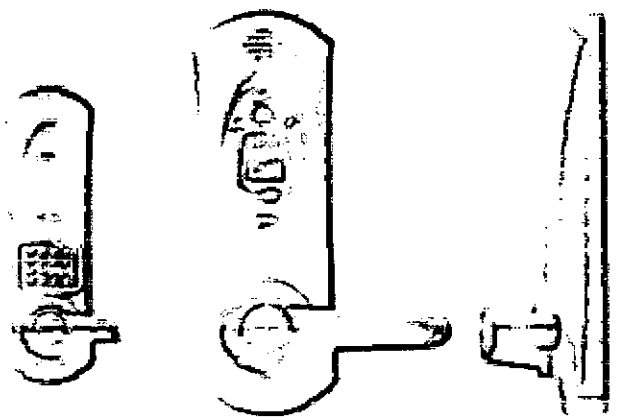
Prototipo Conceptual de Aplicación

Aplicado a la Seguridad Física

La implementación de un prototipo en ambiente simulado deberá contener equipamiento de captura, sistemas de información y un plan de implementación que no afecte la normal ejecución de las tareas del área.

Insumos para Seguridad de Acceso Físico

Se han analizado la utilización de productos, tales como como el **FingerDoor**, el cual integra en un mismo módulo el sistema de captura, verificación y bloqueo. analizar



Como se observó en la primer parte de este trabajo, la utilización de este tipo de equipamiento sería totalmente aprovechable en donde la seguridad de acceso físico sea fundamental, como en la Penitenciaría Provincial. Luego de largas deliberaciones con el personal de la Penitenciaría se concluyó que las dificultades no son de orden técnico, sino que residen en algunas variables de implementación operativa.

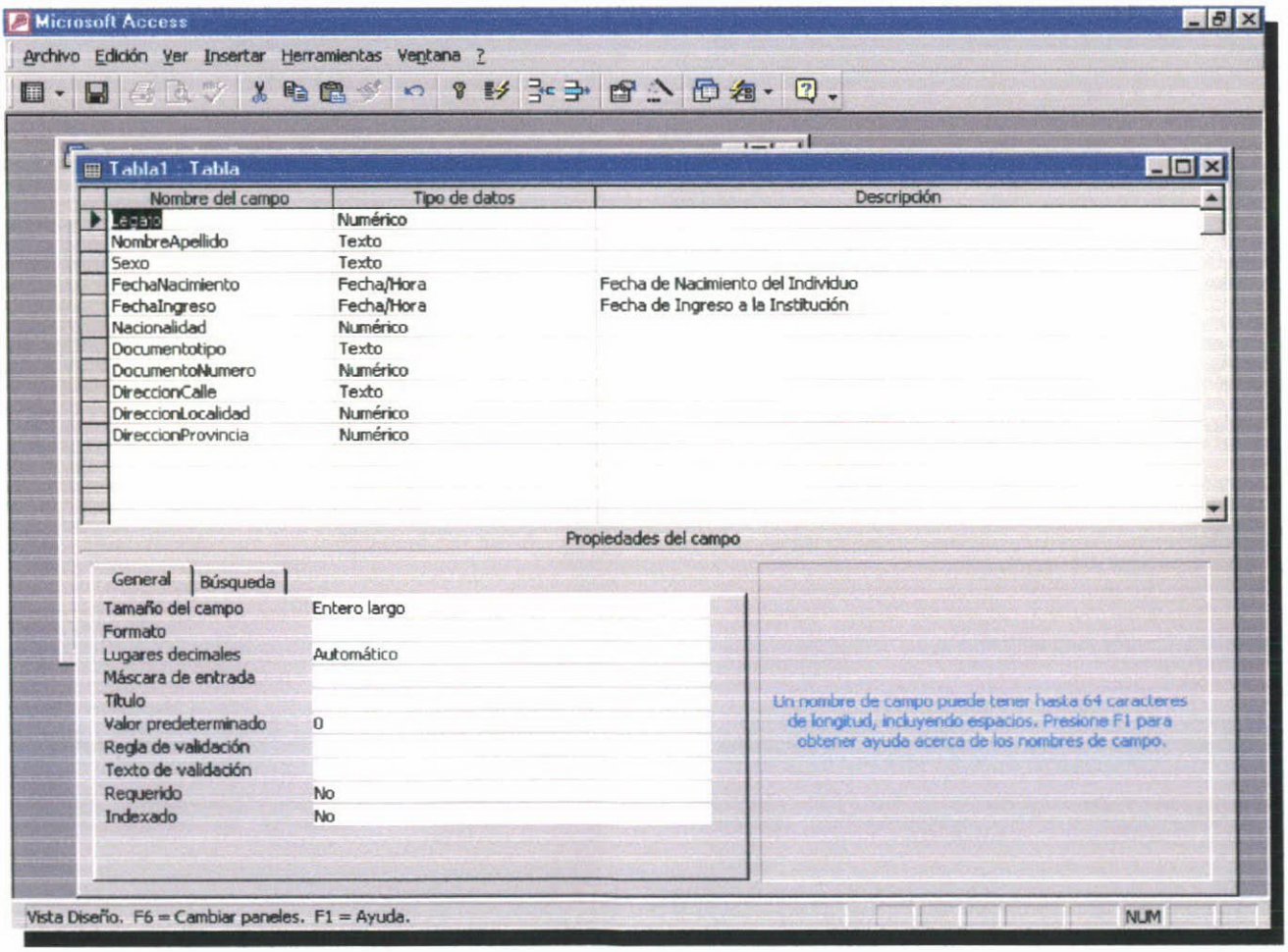
Aplicado al Enrolamiento y Verificación

El enrolamiento de individuos por intermedio de sus datos biométricos, abarca la toma de los mismos, y una primer verificación para asegurar la buena calidad de la toma.

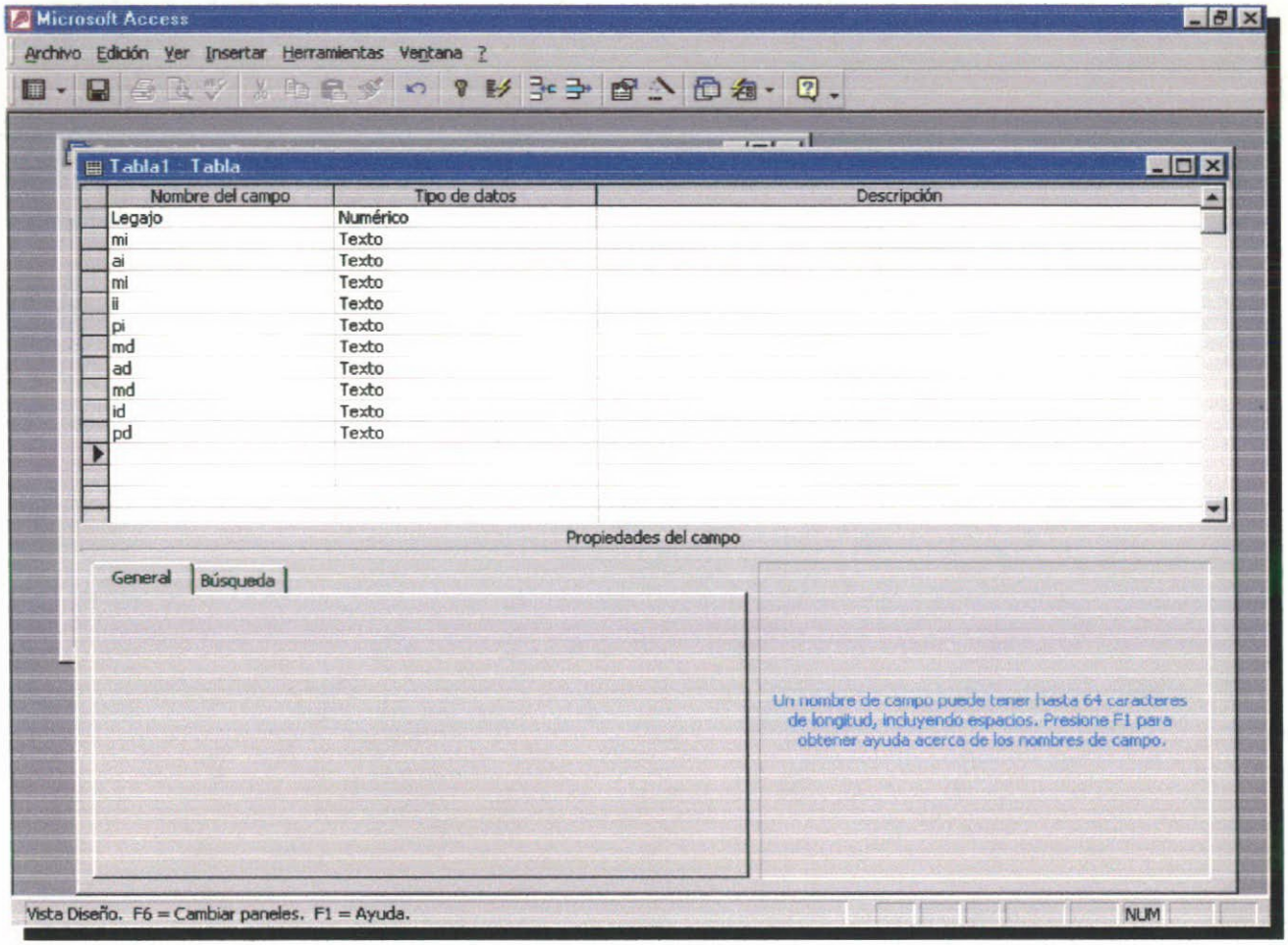
Para realizar un prototipo global se utilizó como ejemplo un sistema de control de personal estándar.

Modelo de Datos

Archivo de Personas

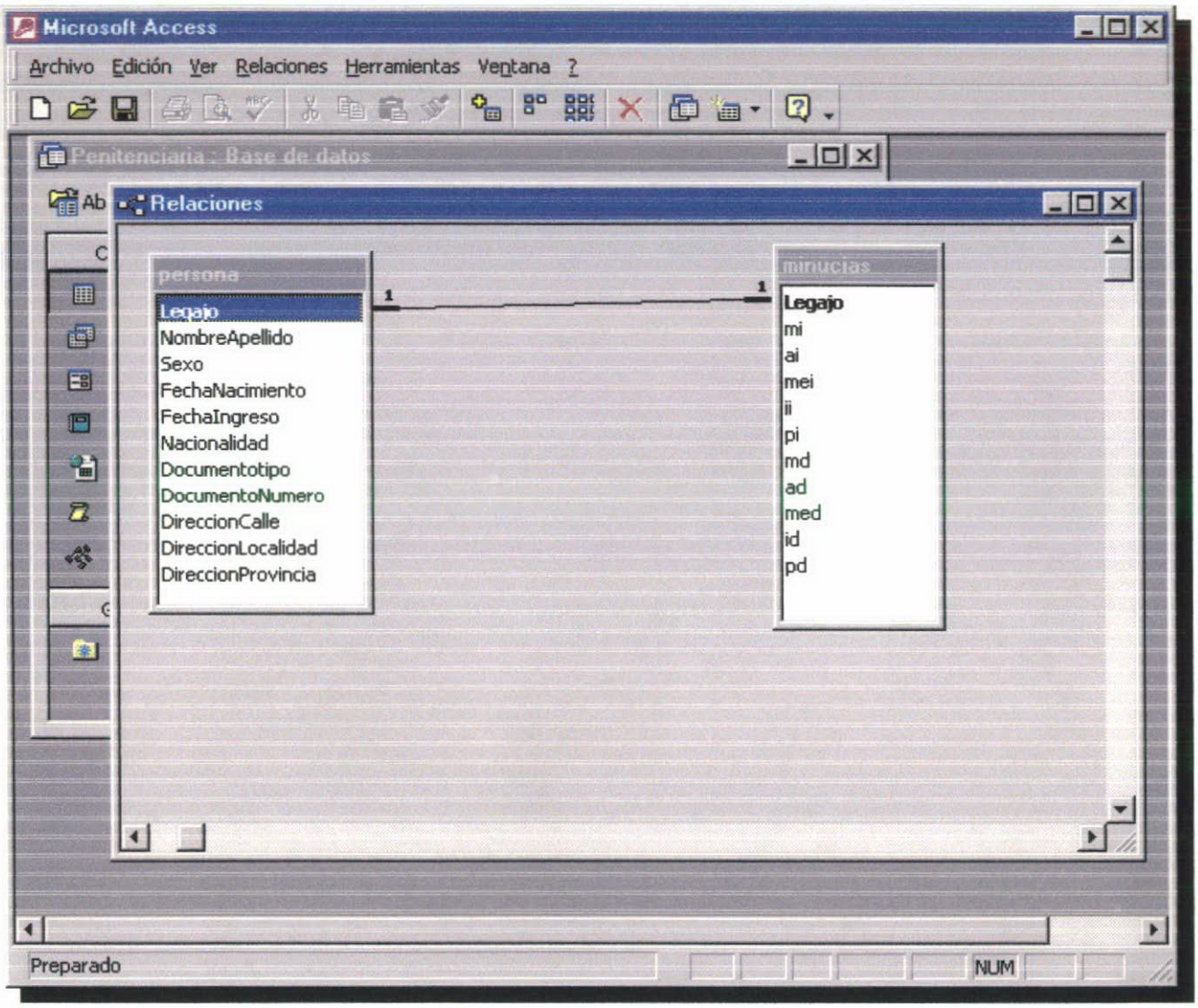


Archivo de Minucias



Este archivo contendrá en cada registro un análisis de las minucias (análisis de la huella los diez dedos) de cada uno de los individuos asentados en el archivo. Las minucias deberán ser examinadas por un software capaz de extraerlas correctamente de la imagen de la huella digital. El presente archivo solo servirá para contenerlas.

Relaciones entre Archivos



El componente que diferencia a este prototipo de un sistema tipo de personal es la capacidad para registrar sus huellas personales. Tal información, como ya se explicó será contenida en un archivo secundario, el cual estará relacionado con el archivo de personas por medio de una clave única. (en este caso el número de legajo).

Aplicado al Almacenamiento y Recuperación

En cualquiera de los casos anteriormente estudiados, el almacenamiento de la información biométrica merece contar con un plan diseño cuidadosamente meditado. En el apartado anterior se observó una forma muy práctica de almacenar la información biométrica: por intermedio de sus minucias.

Uno de los puntos cruciales al diseñar un sistema de identificación biométrica será, en el momento de la definición de datos, decidir que almacenar: la imagen o el análisis de la imagen (las minucias). En el primero de los casos, se deberá contar con un índice adecuado y una muy precisa forma de almacenar imágenes en nuestro disco rígido, asegurando.

- una ubicación física fija dentro del dispositivo de almacenamiento. (Como almacenar las imágenes/minucias en mi disco rígido?, debo utilizar necesariamente un disco rígido?)
- Inalterabilidad de la imágenes. No es aconsejable que las imágenes estén disponibles para su alteración por intermedio de programas editores de imágenes. Con la intención de "mejorar" la calidad de la misma, por intermedio de la manipulación de parámetros (tonos, contrastes, brillos) puede perderse algunos de los puntos característicos de esta.
- Una recuperación fácil y segura.

Sistema de Archivo de Huellas. Policía de Mendoza

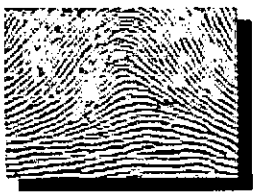
Una de las principales necesidades encontradas en la etapa de relevamiento, y luego en la determinación de requerimiento de los usuarios de la tecnología biométrica fue la carencia de un sistema de archivo automatizado (desde el punto de vista electrónico) para el almacenamiento y recuperación de huellas dactilares. Se tomó como base para el desarrollo de este prototipo alguna de las prestaciones de sistemas ya constituidos como el AFIS METAMORPHO, detallado mas adelante.

Objetivos

1. Resguardo de la información biométrica
2. Clasificación de la información biométrica
3. Rápido acceso a las tarjetas
4. Asimilación de la operatoria electrónica.

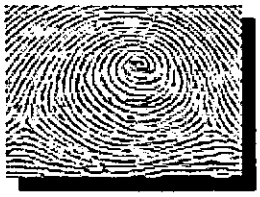
Para una mejor ilustración de las siguientes secciones, destacamos ahora aquellas particularidades de una huella digital utilizadas para la primer clasificación.

Según su disposición general:



Arco

Presilla



Verticilo

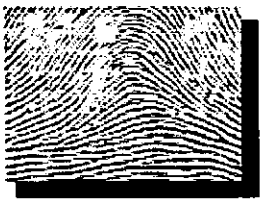
Característica de la línea

Canto Final

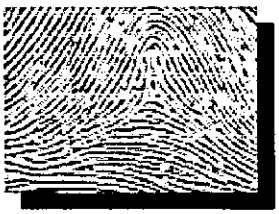
Bifurcación

Isla o Punto

De acuerdo a su disposición particular:

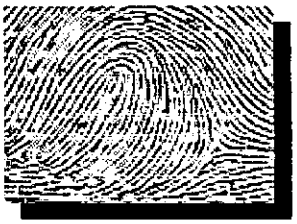


Arco Plano

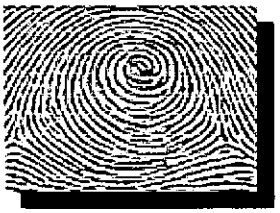


Arco tendido

Presilla Plana Derecha



Presilla Plana Izquierda



Verticilo

Verticilo Central

Verticilo Lateral

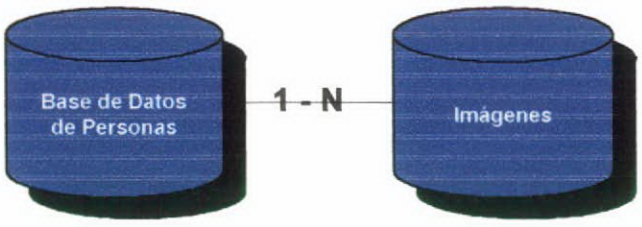
Verticilo Trenzado

Accidental

Se tomarán a continuación las principales formas para diseñar un algoritmo capaz de generar una primer clasificación de una ficha decadactilar.

Base de Datos

La base de datos contendrá dos componentes principales. Los archivos referenciales conteniendo los datos personales de los individuos; un archivo (o físicamente conjunto de archivos) conteniendo los datos biométricos.



En una primera instancia se normalizará el contenido de la base de datos de individuos, en base a datos ya utilizados en distintas dependencias públicas. Es recomendable la reutilización de dichos datos, puesto que los mismos han sido utilizado a lo largo de años con un resultado aceptable; el cual se pretende incrementar por medio de la operatoria electrónica.

La información contenida en dichos archivos estará compuesta por:

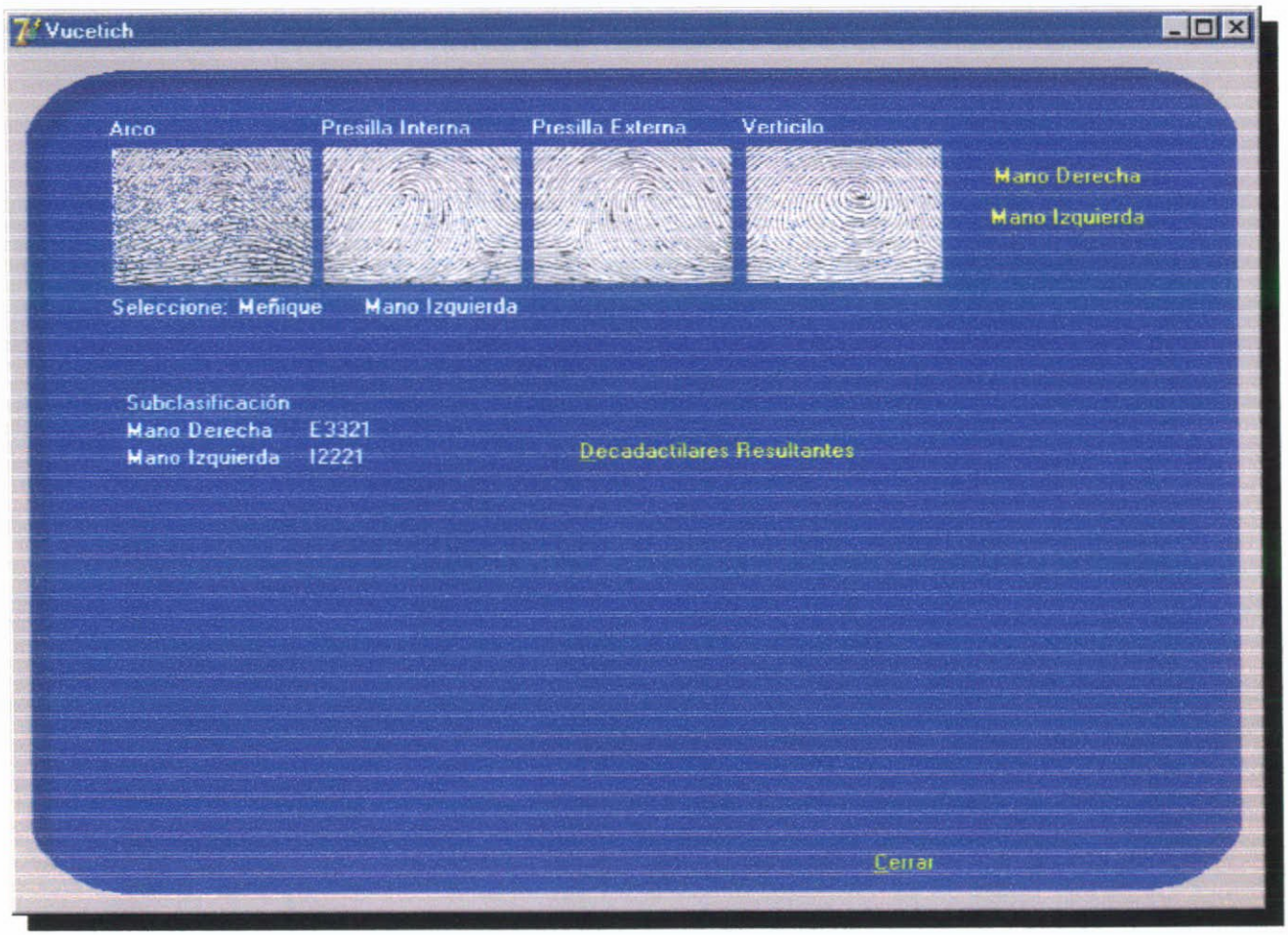
Base de Datos de Personas
Datos Personales
Datos Filiatorios
Datos Prontuariales
Metainformación. Índices de Búsqueda

Se recomienda la reutilización de los datos personales y filiatorios contenidos en la base de datos actual, previendo un cruzamiento de datos con otras base de datos de origen público. Según lo observado, en distintos relevamientos, las dos bases de datos más grandes actualmente en la Administración Pública Provincial son:

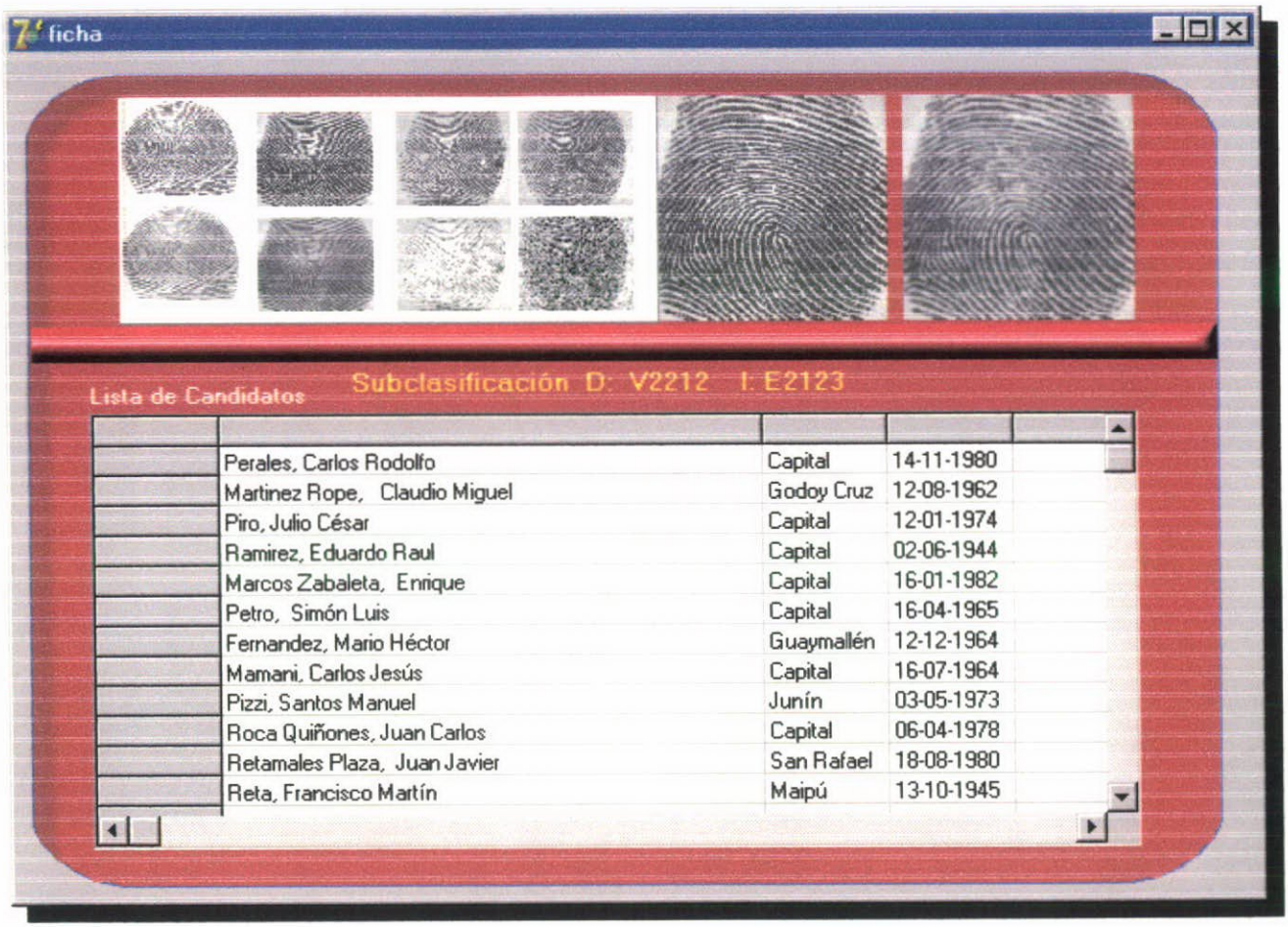
- Base de datos de Personas y Prontuarios en la Policía de Mendoza.
- Base de datos en construcción del Registro Civil y Capacidad de las Personas.

A partir del análisis realizado a la base de datos del Registro Civil y Capacidad de las personas, y atendiendo a las necesidades del presente sistema se concluye que la misma es utilizable.

La siguiente captura de pantalla ilustra la aplicación principal. En la misma el operador podrá seleccionar para cada mano las particularidades de la huella contenida en cada uno de los dedos, provocando este proceso la generación de la clasificación.



Una vez culminada la tarea de codificación el operador estará en condiciones de tener un primer filtro sobre todo el dominio de datos, el cual coincide con el conjunto resultante.



Estándares Biométricos para Aplicaciones Emergentes

Al hablar de estándares, en un ambiente donde la tecnología biométrica está bajo discusión, el primer nombre que viene a la mente es el del estándar **AFIS**.

AFIS es un sistema informático compuesto de *Hardware* y *Software* que permite la captura, consulta y comparación automática de huellas dactilares agrupadas por fichas decadactilares o en forma de rastro o latente (parte degradada de huella levantada en la escena de crimen).

Clasificación

Las huellas dactilares se clasifican por la forma fundamental de las líneas que la componen (arco, verticilo, presilla interna, presilla externa). Para la identificación manual de una persona es necesario contar con las diez huellas de la misma, dado que se utilizan los diez dedos para generar un código que es utilizado para la búsqueda. En este punto podemos encontrar algunas diferencias en cuanto a los métodos utilizados por la Policía Provincial y algunos sistemas de reconocimiento y clasificación de huellas dactilares.

En el sistema *AFIS MetaMorpho* la clasificación se utiliza para limitar el universo de búsqueda. El *AFIS MetaMorpho* es el único en poseer la tecnología y desarrollo que permite la clasificación automática de las huellas lo que se traduce un una gran productividad del sistema.

Codificación

Consiste en la extracción de los puntos característicos o minucias de una huella dactilar. Mediante este procedimiento, la información de la huella se reduce a un código generado por un algoritmo matemático que es propietario de cada proveedor. En las oficinas de la Policía muchos de estos procesos se realizan en forma actualmente manual.

Los peritos utilizan las minucias para comparar las huellas entre si o un rasgo y una huella. El *AFIS MetaMorpho* realiza la codificación automática de las huellas lo que significa una gran productividad del sistema. Es importante notar que algunos de los productos mejor desarrollados detectan los siete tipos de puntos característicos necesarios para una identificación óptima.

Conversión

Es un proceso de escaneo, autoclasificación, autocodificación y preparación de las fichas decadactilares para su inserción en una Base de Datos AFIS. Los datos alfanuméricos son ingresados por **doble digitación** para garantizar la exactitud de la información tomada. Durante la conversión es necesario poder ubicar una ficha en cualquier etapa de su procesamiento, permitiéndole al organismo dueño de la fichas el libre acceso y control de su información. El resultado de la conversión es llevar la información de huellas de la base papel al sistema AFIS en un tiempo corto.

AFIS Criminal Morpho

El objetivo primario de un sistema **AFIS Criminal** es la identificación de criminales por intermedio de un método científico confiable (determinación de sus huellas personales). Se utiliza el AFIS para buscar rastros (una huella **latente** encontrada en la escena de un crimen), contra una base de datos AFIS con el objeto de identificar a la persona poseedora de dicha huella o comprobar que el dueño de la huella latente no se encontraba en otra escena de un crimen donde dejo sus huellas.

Una huella latente puede ser una fracción ínfima de una huella dactilar, de la cual generalmente el perito no conoce a que dedo pertenece, ni su orientación, ni su centro, ni ningún otro dato que reduzca el universo de búsqueda (sexo del dueño, color de piel...). El problema que se presenta actualmente en la Policía de Mendoza con este tipo de muestras, es la dificultad de asentar la muestra en papel o digitalmente para ser procesada en una computadora.

El sistema observado AFIS MetaMorpho, se considera el único en tener la capacidad de efectuar una rotación automática de 360° de la muestra para compararla con los elementos contenidos en la base de datos AFIS de fichas decadatilares (búsqueda CAXI). Por lo tanto el sistema AFIS cotejará dicho rastro contra cada uno de los 10 dedos de cada persona presente en la base de datos, y contra otra base de datos donde se encuentran todos los rastros no identificados que se guardaron de escenas de crímenes anteriores.

Además, este sistema permite averiguar la presencia o no de una persona en la base de datos. Esto permite identificar un sospechoso pero también personas que requieren, por ejemplo, un certificado de buena conducta. O sea, que el sistema permite identificar a una persona que tenemos físicamente con nosotros. El sistema permite la búsqueda con los 10 dedos (la ficha decadactilar) o bien con las huellas de los 2 índices.

Los usuarios de un AFIS Criminal manejan generalmente un archivo de fichas decadactilares y uno de latentes. El sistema AFIS permite modernizar este archivo gracias a la conversión y usarlo con un alto rendimiento en cuanto a resultados de identificación.

Los requisitos funcionales básicos de un AFIS Criminal son:

- Guardar en formato informático las fichas decadactilares lo que permite no usar mas el voluminoso archivo papel (base TP, o base decadactilar)
- Adquisición de nuevas fichas sin duplicación de la información y permitiendo la identificación para tener una base de datos optimizada y limpia (búsqueda TP/TP, o búsqueda Decadactilar contra Decadactilar)
- Guardar en formato informático las latentes de casos no resueltos (base UL, o base de Latentes No Resueltas)

- Al adquirir una ficha decadactilar, buscar si esta persona cometió un crimen sin resolver (búsqueda TP/UL, o búsqueda Decadactilar adquirida contra la base de Latentes No Resueltas)

- Al adquirir una nueva latente, buscar si esta latente pertenece a una persona ya conocida, o si esta latente es una huella de otro caso (búsqueda LT/TP, o búsqueda Latente adquirida contra la base Decadactilar; y búsqueda LT/UL, o búsqueda Latente adquirida contra la base de Latentes No Resueltas)

El sistema AFIS MetaMorpho es un sistema experto, es decir que los usuarios del mismo no tienen que ser necesariamente peritos expertos en huellas dactilares, dado que el sistema realiza en forma automática todos los procedimientos de clasificación, codificación, búsqueda y presentación de lista de candidatos. La decisión final con respecto a la identificación positiva o no de una persona es siempre tomada por un perito en huellas dactilares.

AFIS Civil Morpho

Un AFIS Civil se diferencia de un AFIS Criminal en los siguientes puntos:

- Generalmente no se usan los 10 dedos sino 2 o 4 (generalmente se utilizan 2 dedos índices);
- Las huellas son generalmente planas y no rodadas;
- Normalmente, no se realizan búsquedas de tipo Latente;
- Generalmente solo se realizan búsquedas TP/TP (utilizando 2 dedos índices, también llamada búsqueda 1/N), y verificaciones 1:1 (utilizando 1 o 2 dedos índices) u *on-line* (usando la base de datos centralizada de minucias);
- El resultado de la búsqueda 1:N es un listado de candidatos, del mismo tipo que el generado en una búsqueda TP/TP criminal;
- El resultado de la verificación de identidad (verificación 1:1) es un SI o un NO (misma persona o no). La verificación 1:1 puede ser realizada *off-line*, utilizando las minucias registradas en el documento (por ejemplo, en la memoria local de una tarjeta inteligente o en un código de barras bidimensional). En este caso, el acceso a la base de datos central AFIS no es necesario.

El AFIS Civil es una poderosa herramienta para luchar contra el fraude de identidad. Permite atribuir a UN ciudadano, UN documento (de identidad, de conducir, de tenencia...), UN derecho (de voto, de seguro social...). Tanto en el AFIS Civil como en el AFIS Criminal se utiliza el sistema MetaMorpho, con configuraciones diferentes, pero con corazón similar.

Un sistema civil se utiliza por ejemplo para garantizar que una persona no logre, mediante la presentación de documentos apócrifos, poseer doble o múltiple identidad. Por lo tanto en el momento de que cada ciudadano solicita su cédula, se capturan generalmente las dos huellas dactilares de sus índices, y se comparan contra una base de datos AFIS que posee los dedos índice derecho e izquierdo de todas las personas que ya retiraron un documento.

Aquí conocemos de que dedo se trata, su orientación, centro, y el sexo de la persona. Toda esta información se utiliza para reducir el universo de búsqueda, y por lo tanto estos sistemas se caracterizan por permitir una gran cantidad de búsquedas en un corto tiempo. Es importante notar que el Sistema AFIS MetaMorpho puede ser utilizado sin ningún otro criterio que la información proveniente de las huellas dactilares.

A pesar de que la precisión no se puede medir en forma absoluta (depende de factores relacionados con el sistema y el tratamiento de la huella dactilar), es un muy importante elemento para la elección de un sistema AFIS sobre otro. Cuando se evalúa el precio de un sistema, es importante saber que la precisión es una función básica del diseño del sistema y no se relaciona con la cantidad de procesadores con que cuenta el mismo. La precisión se mide de varias formas diferentes, entre las cuales se encuentran pruebas comparativas e cálculos estadísticos.

El sistema *AFIS MetaMorpho* ha sido exhaustivamente evaluado en pruebas (*benchmark*) comparativas y ha resultado ser altamente preciso, a tal punto que la tecnología de codificación y búsqueda que se incluyen en cada uno de los sistemas ha sido escogida por el FBI para su sistema FBI *IAFIS (Integrated Automated Fingerprint Identification System)*. Y, como resultado del desarrollo de nueva tecnología para cumplir con los altos requerimientos de precisión y capacidad de trabajo exigidas por le FBI, en los dos últimos años la precisión de los sistemas AFIS que se ofrece se ha incrementado en un 50%.

Cuando los vendedores de AFIS hablan sobre la velocidad de sus sistemas, en general se refieren a diferentes tipos de velocidad. La velocidad de procesamiento es: luego de que la imagen o archivo de una huella dactilar ha sido ingresada al sistema, el AFIS determina si existe o no un archivo en la base de datos que sea "igual" al buscado.

Capacidad de trabajo es la cantidad de archivos que pueden ser ingresados en un determinado período de tiempo. Capacidad de trabajo incluye el tiempo que le toma al operador ingresar el archivo, y el tiempo que le toma al operador analizar el resultado de la búsqueda.

Durante los diez últimos años la velocidad de los sistemas AFIS han sido incrementados diez veces, y luego duplicados nuevamente como resultado de los desarrollos efectuados para el proyecto FBI IAFIS. Son tres las razones más importante que han permitido el aumento general de la velocidad del sistema: recuperación en

tiempo real de la imagen de la huella utilizando tecnología RAID (*Redundant Arrays of Independent Disks*), incremento exponencial de la capacidad de procesamiento de las computadoras, e incremento en la velocidad de ingreso de archivos y codificación en las estaciones de trabajo. La mejoría de las interfaces con los usuarios (pantallas más amigables) han también influido en el incremento de la velocidad general del sistema.

La correcta utilización de un sistema AFIS requiere de personal entrenado. Si un sistema es demasiado difícil de aprender, el proceso de aprendizaje toma demasiado tiempo, o el sistema es demasiado lento en su utilización, se está desperdiciando recursos de personal. O peor aún, se deberá contratar y entrenar constantemente personal para evitar la acumulación de trabajo.

Tarde o temprano, todos los sistemas AFIS requieren actualización y/o expansión. Muchos vendedores utilizan estas circunstancias para facturar exorbitantes sumas de dinero. Algunas de las experiencias relevadas ha demostrado que algunos organismos han pagado más por las actualizaciones o expansiones que por el sistema inicial. Y algunos vendedores, con limitados recursos humanos en investigación y desarrollo, dependen de técnicos e ingenieros que vuelan de un lugar a otro sin poder permanecer en un lugar para verificar el correcto funcionamiento de las mejoras o expansiones.

Como el sistema AFIS MetaMorpho está basado en *software*, las nuevas funciones o aplicaciones pueden ser fácilmente instaladas y a costo reducido. La investigación y desarrollo de SAGEM tienen el respaldo de ingenieros propios con extensa experiencia

en sistemas de tratamiento de imágenes. SAGEM cumplió totalmente con el "Year 2000 compliance" y el sistema de escala de grises.

Algunos vendedores no le dan la verdadera importancia al proceso de conversión de tarjetas decadactilares. Pero el mejor sistema AFIS posible comienza con el resultado de un proceso de conversión que cumpla con los más altos niveles de calidad posible. La precisa conversión o digitalización de tarjetas es esencial para garantizar la mejor performance del sistema.

SAGEM ha sometido su proceso de conversión a numerosas pruebas de calidad realizadas por empresas u organismos independientes. En pruebas realizadas sobre grandes bases de datos, los archivos convertidos por SAGEM han demostrado tener menos del 0.1% de error.

La excelencia de la conversión efectuada por SAGEM motivó al FBI a adoptarla para la conversión de su base de datos nacional compuesta de 31.5 millones de fichas decadactilares. SAGEM finalizó este proceso llamado **FICO** (*Fingerprint Image Conversion Operation*) en el tiempo previsto y de acuerdo al presupuesto estimado. Para la mayoría de las agencias y organismos, es imperativo que sus AFIS puedan interactuar con otros sistemas, incluyendo IAFIS, *live scan*, captura de imágenes, historia criminal computarizada, otros AFIS, sistemas de terceras partes, y estaciones multifuncionales de captura de información.

El AFIS MetaMorpho de SAGEM puede poner otras bases de datos, incluyendo IAFIS y de otros vendedores, a su disposición. El subsistema "*Gateway Service Provider*" de SAGEM cumple totalmente con los estándares ANSI/NIST para el Intercambio de Información de Huellas Dactilares.

La tecnología AFIS (*Automated Fingerprint Identification System*) ha sido probada y debatida durante los últimos 25 años, y el uso de la misma se está expandiendo rápidamente en un gran número de nuevas áreas de aplicación.

Sin embargo, la presión para capitalizar los beneficios de la tecnología antes de la definición de estándares apropiados y métodos de validación de la tecnología es probable que resulte en una generalizada falla para conseguir las expectativas tanto esperadas.

Para aplicaciones serias a larga escala de identificación positiva, ninguna técnica biométrica se le acerca a la identificación por huella digital. La identificación por huella digital está:

- **Bien establecida**: la identificación por huella digital ha sido utilizada por los procesos legales durante los últimos cien años, y se ha convertido en el estándar internacional para la identificación positiva de individuos.
- **Probada**: La tecnología AFIS ha sido desarrollada, refinada y probada según los requerimientos demandados por las fuerzas legales a lo largo del mundo durante las últimas dos décadas.

- **Aceptada Legalmente**: Los precedentes legales que han sido establecidos en las cortes norteamericanas hacen que las huellas digitales sean la única técnica biométrica aceptada como prueba de identificación en procedimientos legales.

- **Madura**: Las tecnologías de identificación de la huella digital están bien más allá de la etapa de investigación y desarrollo, según lo evidenciado por el hecho de que un número de fabricantes viables producen los productos de competición para un mercado extenso y establecido. En la mayoría de otros tipos de medición biométrica, la tecnología está solamente disponible en un solo vendedor, haciendo cualquier uso a largo plazo muy aventurado.

Los avances recientes en computación y tecnología digital de la proyección de imagen han conducido a la introducción de las nuevas metodologías de AFIS usando electrónica "*live-scan*" para impresión de imágenes planas de huella digital como la base para la identificación. La proliferación de los sistemas de impresión plana AFIS es rápida y acelarada en el nivel gubernamental incluyendo licenciar de conducir, control es fronterizos, la inmigración y la identificación militar del personal, etc.

Estos nuevos usos de la identificación se están tratando como usos directos de la tecnología AFIS.

Considere las diferencias entre los usos probados de AFIS y usos clásicos manuales de la biometría:

- Los usos de la aplicación utilizan tomas roladas de la huella digital del como la base para todo proceso de identificación. Una toma plana puede abarcar menos del 50% del área de la toma rolada equivalente, proporcionando perceptiblemente menos datos para el proceso de la identificación.
- Los usos probados de la aplicación AFIS utilizan 8 o 10 imágenes del dedo para alcanzar exactitud de la identificación. Los usos de la toma plana AFIS utilizan solamente 1 o 2 imágenes del dedo. Las otras 8 huellas digitales no se capturan, y no están disponibles para las comparaciones de reserva.
- Los sistemas de AFIS fueron diseñados para hacer frente a los problemas típicos de huellas digitales entintadas, tales como mancharse y sobreentintar o subentintar.

- En usos comunes, el AFIS produce una lista de candidatos de posibles prontuarios coincidentes con la huella digital (generalmente 10 - 100) que son repasados manualmente por un examinador experto de la huellas digitales para determinarse si alguno de los expedientes del candidato coinciden con el deseado. La mayoría de los nuevos usos de la toma plana son completamente automáticos, y requieren que el sistema identifique a un candidato único, sin la intervención manual.

La exactitud, la rentabilidad y la interoperabilidad de AFIS es totalmente dependiente de la calidad de las imágenes de la huella digital tomada.

Según el AFIS los elementos para tener en cuenta al adquirir un scanner son:

- Los *scanners* electrónicos de huella digital deben estar de acuerdo a algunos tipos de distorsión geométrica, como la desintegración de la imagen y otros tipos de problemas de la calidad de la imagen (que no tienen un análogo en la toma de huella dactilar entintada).

- Aunque un AFIS se puede ajustar para ser insensible a los problemas de la distorsión de una marca en particular *scanner*, la introducción de imágenes de huella digital de otro *scanner* con distintas características de exactitud, degradará el funcionamiento de la identificación del AFIS de una manera indeterminada.

- Organismos Internacionales han notado que las imágenes de mala calidad de la huella digital son considerablemente más susceptibles cuando la degradación de la imagen y pérdida de información es mayor. (por ejemplo con la con la técnica de compresión WSQ del FBI utilizada en función de las telecomunicaciones y/o almacenaje).

No existen estándares formales para la medición o calidad de control de una imagen de un dedo en particular

La carencia de estándares técnicos podría conducir (como en muchos casos ha sucedido) a la creación de una base de datos mal formadas o muy grandes, de tal mala calidad que un gran porcentaje de las imágenes no puede ser procesada. Además

pueden existir problemas en cuanto a la incompatibilidad de dispositivos de captura que conllevarían a la ilegibilidad de datos tomados por otros *scanneres*.

Análisis de un Sistema de Tarjeta Inteligente

Uno de los problemas aún no planteados en este documento es el acceso a la base de datos para realizar la comparación con una toma, determinando si el individuo ha sido anteriormente enrolado en el sistema y cuenta con la autorización pertinente para operarlo.

Existen dos formas principales de realizar la comparación: 1 a 1 (la toma actual comparada contra otra) o 1 a N (la toma actual comparada contra una base de datos de huellas digitales). La segunda modalidad la dejaremos de lado en este momento, y se tendrá en cuenta solo en aquellos casos donde el individuo necesite ser ubicado dentro de un gran dominio de personas (en una situación criminal por ejemplo).

La autenticación 1 a 1 es la más utilizada para acceso a pequeños sistemas, cajeros automáticos, etc. Y consiste en lo siguiente. El individuo es portador (lógicamente) de sus huellas personales y de una tarjeta inteligente (o cualquier otro medio similar) que contiene sus datos impresos y archivada en ella también los datos biométricos previamente enrolados. Por lo tanto, la autenticación ante cualquier sistema consiste en comparar los **datos de su dedo con los datos de su dedo grabados en la tarjeta**.

El *Foro Java Card* ha procurado atender la necesidades de este tipo de comparación con la programación de una aplicación interna dentro del una tarjeta inteligente (*Java Card).* Específicamente, esta API soporta seguridad biométrica *Match-on-Card* de tal

modo que los datos biométricos sensibles no abandonarán nunca la tarjeta, todo esto mientras se consume un mínima cantidad de memoria.

Se han analizado los requerimientos, la razón fundamental y el diseño del API biométrico para la Tarjeta Java que desarrollado bajo el alcance del *Java Card Forum Biometric Task Force y el Biometric Consortium Working Group*.

Ya que la utilización de este tipo de tarjetas es creciente hoy en día, sobre las plataformas computacionales mas pequeñas, los desarrolladores deberían asegurar la interoperabilidad de varias tecnologías biométricas con tarjetas java, y permitir múltiples e independientes aplicaciones sobre una misma tarjeta para acceder la funcionalidad biométrica de la misma. (múltiples aplicaciones).

Recomendaciones

En base al diseño general de aplicaciones y procedimientos antes descritos, se recomienda tener en cuenta los siguientes puntos para plantear una exitosa implementación.

- Análisis exhaustivo de la tecnología.
- Utilización de Estándares
  Como recomendación fundamental, el grupo de desarrollo establece que es sumamente necesario apegarse a estándares internacionales en cuanto al uso de la tecnología biométrica y análisis y diseño de sistemas (automatización de los procesos).
- Creación de grupos interdisciplinarios, que cuente con técnicos expertos en biometría y técnicos expertos en informática (procesamiento y almacenamiento de datos).
- Concientización
  Es necesario realizar una profunda concientización del alcance de los nuevos procedimientos de seguridad física a los distintos niveles del área.
- Migración ordenada de los actuales procedimientos de seguridad

Conclusiones

En esta última etapa del trabajo, se ha realizado un giro significativo en cuanto a la decisión de implementación de técnicas biométricas en la Administración Pública Provincial.

En este momento estamos en condiciones de tomar la decisión clave:

Desarrollar tecnología?
Contratar/Comprar tecnología biométrica ?

1. Se considera factible el desarrollo de aplicaciones, donde la necesidad sea la autenticación 1 a 1.

2. No se cuenta con las condiciones técnicas necesarias para desarrollar aplicaciones donde la autenticación necesaria sea **1 a N**, (criminalística, policía científica, etc.). La solución a este problema estará dada en la adquisición de tecnología de punta, la cual por una cuestión de orden económico no se encuentra al alcance de los organismos bajo estudio.

3. Los costos de adquisición (o desarrollo) son aceptables, salvo en el caso de adquisición de sistemas criminalísticos, los cuales cuentan con tecnología de punta (estándares AFIS) capaces de satisfacer las necesidades observadas.

4. Se encuentra factible el desarrollo de sistemas de autenticación para acceso a redes informáticos y servicios por intermedio de la captura de huella digital. Para ello se deberán adquirir junto a los dispositivos seleccionados, librerías fuentes de programación.

Glosario

A continuación se presenta un listado de términos relacionados con la operatoria informática. (Marcados con **[B]** aquellos vocablos y expresiones relacionadas directamente con tecnología biométrica).

Aceptación de Impostor Pasivo [B] Cuando un impostor envía su propio huella biométrica exigiendo autorización en nombre de otra persona (intencional o inadvertidamente)

ActiveX Tecnología desarrollada por Microsoft con el fin de elaborar aplicaciones exportables a la red las cuales deben ser capaces de operar sobre cualquier plataforma a través de navegadores WWW de forma que le da dinamismo a las páginas web.

AFIS [B] Un sistema biométrico altamente especializado que compara una sola imagen del dedo con una base de datos conteniendo elementos del mismo tipo. Se utiliza predominante para criminalística, pero también se está poniendo al uso en ámbitos civiles. Para la aplicación criminalística, las imágenes del dedo se recogen de las escenas del crimen, conocidas como **latentes**, o se toman de sospechosos criminales cuando son arrestados. En usos civiles, las imágenes del dedo pueden ser capturadas colocando un dedo en un scanner o electrónicamente explorando impresiones entintadas en el papel.

Binning
Una técnica especializada usada por los vendedores de algún AFIS. Binning es el proceso de clasificar imágenes del dedo según patrones de la imagen del dedo. Esto ocurre predominante en usos de la aplicación criminalísitcas. Aquí las imágenes del dedo son categorizadas por características tales como arcos, lazos y verticilos; y almacenadas en bases de datos más pequeñas, separadas (o compartimientos) según su categoría. Las búsquedas se pueden hacer contra compartimientos particulares, así acelerando el tiempo de reacción y exactitud de la búsqueda de AFIS.

Booking
El proceso de capturar las imágenes digitales entintadas en el papel, para el subsiguiente procesamiento de un AFIS.

Filtering
Una técnica especializada usada por algunos vendedores de AFIS. Es el proceso de clasificar las imágenes digitales según datos que no están relacionados a la propia imagen digital. Esto puede involucrar la filtración por el sexo, envejecimiento, color de pelo u otros factores personales.

Latent
Una toma de una huella digital en el lugar del crimen.

Algoritmo En programación, porción de código del programa que resuelve o ejecuta funciones específicas para la resolución de un problema o un proceso.

Algoritmo de Encriptación (o de Cifrado) [B] Sistema de encriptación (con mayor grado de sofisticación cada día) que permite mover información por las redes telemáticas con seguridad. Existen varios algoritmos, a cual más complejo y eficaz, destacando entre todos MD5, DES, DES2, RC3, RC4 y, sobre todo, el SSL (Secure Sockets Layer) de Netscape que, posiblemente, se convierta en el algoritmo que adopte definitivamente 'Internet'. Estos sofisticados algoritmos se caracterizan por sus claves de encriptación que oscilan entre 40 y 120 bits. Las claves de encriptación superiores a 40 bits no son legalmente exportables fuera de los EE.UU. por razones de seguridad.

ANSI American National Standard Institute. Instituto Nacional Americano de Estándar.

Ancho de banda (Bandwidth). Cantidad de información que puede enviarse a través de una conexión. Usualmente, se mide en bits por segundo. (Ver también: BPS, Bit).

API Application Program Interface (Interfaz para programas de aplicación) (Conjunto de convenciones de programación que definen como se invoca un servicio desde un programa.

Applet Se llama applet a cualquier programa pequeño hecho en Java que puede referenciarse en una página HTML. Los applet difieren de los programas hechos específicamente para Java en que no serán autorizados a acceder ciertos recursos de la PC local, como archivos y dispositivos de hard, y no puede comunicarse con otras computadoras conectadas a una red local.

ASCII (American Standard Code For Information Interchange o Código numérico estándar).Utilizado por las computadoras para representar todas las letras mayúsculas y minúsculas del alfabeto, así como también números y signos de puntuación. Existen 128 códigos ASCII, los cuales pueden ser representados mediante números binarios del 0000000 al 1111111.

Base de Datos Colección de datos organizada de tal modo que el ordenador pueda acceder rápidamente a ella. Una base de datos relacionar es aquella en la que las conexiones entre los distintos elementos que forman la base de datos están almacenadas explícitamente con el fin de ayudar a la manipulación y el acceso a éstos.

Benchmark. Prueba de sistemas. Prueba de elementos de Hardware. Prueba de software.

Binario Sistema de numeración de base 2 que utiliza los símbolos 0 y 1; se representan por la presencia y la ausencia de tensión eléctrica.

Binario Sistema de numeración en el que hay sólo dos símbolos, 0 y 1 (en oposición al sistema decimal ordinario, en el que hay diez símbolos: 0, 1, 2, 3, 4, 5, 6, 7, 8 y 9). Los ordenadores "piensan" en términos binarios.

Bit (Binary Digit o Dígito Binario). Es un dígito en base 2,es decir, 0 ó 1.Un bit es la unidad más pequeña de información que la computadora es capaz de manejar. El ancho de banda se suele medir en bits por segundo. (Ver también : Ancho de banda, Byte, kilobyte, megabyte).

Byte Unidad de medida de la cantidad de información en formato digital. Usualmente un byte consiste de 8 bits. Un bit es un cero (0) o un uno (1). Esa secuencia de numeros(byte) pueden simbolizar una letra o un espacio (un caracter). Un kilobyte(Kb) son 1024 bytes y un Megabyte(Mb) son 1024 Kilobytes. (Ver también: bit).

Campo Colección de caracteres que forman un grupo distinto, como un código de' identificación, un nombre o una fecha generalmente un campo forma parte de una información.

Campo Conjunto de caracteres tratados como un bloque único; área reservada para datos de un tipo determinado.

Captura Viva [B]
El proceso de capturar una muestra biométrica por intermedio de la interacción entre un usuario final y un sistema biométrico.

CAXI. Búsqueda [B] Con este tipo de búsqueda no se requiere una orientación precisa del centro de la muestra o muestras latentes para asegurar una comparación apropiada.

Certificado Digital [B] Es un archivo de aproximadamente 1k (1.024 bytes) 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.

CGI (Common Gateway Interface). Conjunto de reglas que describen cómo un servidor web se comunica con un programa dentro de la misma máquina (El "programa CGI").Cualquier programa puede ser un CGI, con tal de que maneje sus entradas y salidas de acuerdo con dichas reglas. Usualmente, cuando se está usando un

programa CGI, puede verse "cgi-bin" en el URL del navegador, aunque no siempre sucede así. (Ver también: WINCGI, Web, URL)

Clave de Acceso [B] *Password (Palabra de acceso)* Conocida también por su expresión en castellano: 'palabra de acceso'. Palabra o clave privada utilizada para confirmar una identidad en un sistema remoto que se utiliza para que una persona no pueda usurpar la identidad de otra.

Certificación [B] El proceso de probar un sistema biométrico para asegurar que se encuentra bajo cierto nivel de aceptación.

Cliente Se dice que un programa es un "cliente" cuando sirve sólo para obtener información sobre un programa "servidor". Cada programa "cliente" está diseñado para trabajar con uno ó más programas "servidores" específicos, y cada "servidor" requiere un tipo especial de "cliente". Un navegador es un programa "cliente".(Ver también: navegador, servidor)

Cliente-Servidor Se denomina así al binomio consistente en un programa cliente que consigue datos de otro llamado servidor sin tener que estar obligatoriamente ubicados en el mismo ordenador. Esta técnica de consulta 'remota' se utiliza frecuentemente en redes como 'Internet'.

Comparación [B] El proceso de comparar una muestra biométrica con una plantilla de referencias previamente almacenada.

Correo Electrónico Mensaje, usualmente de texto, enviado de una persona a otra a través de Internet o de cualquier otra red. Es posible enviar automáticamente un mismo mensaje a muchos destinatarios.

Cookie Pequeño archivo de texto que un sitio web coloca en el disco rígido de una computadora que lo visita. Al mismo tiempo, recoge información sobre el usuario.

CPU Central Processing Unit. Unidad central de procesamiento. Es el dispositivo que contiene los circuitos lógicos que realizan las instrucciones de la computadora.

Criptografía [B] Ciencia dedicada al estudio de técnicas capaces de conferir seguridad a los datos. La encriptación es fundamental a la hora de enviar datos a través de las redes de telecomunicaciones con el fin de conservar su privacidad.

Cursor Símbolo en pantalla que indica la posición activa, generalmente titilante. Muestra la posición en que aparecerá el próximo carácter a visualizar cuando se pulse una tecla

Datos Biométricos [B] La información extraída de una muestra biométrica y utilizada o para construir una referencia o para compararla con una referencia tomada previamente.

DPI Dots per inch: puntos por pulgada. En las impresoras, la calidad de la imagen sobre el papel se expresa en dpi.

D Prime [B] Una medida estática de que tambien un sistema biométrico puede discriminar entre diferentes individuos. Mientras más grande sea el valor D-Prime, mejor discrimina el sistema biométrico ambos individuos.

Enrolamiento [B] Corresponde al proceso por el cual se recoge una muestra biométrica, se convierte en datos y se almacena como patrón para posterior comparación.

ETAP, Normas Normas reguladores de sistemas de información vigentes en la Administración Pública Provincial.

Extranet Parte de una Intranet de acceso disponible a clientes y otros usuarios ajenos a la compañía.

Falsa Aceptación [B] Cuando un sistema biométrico identifica incorrectamente o verifica incorrectamente la identidad de un impostor contra la identidad reclamada. También conocido como "error tipo II".

Falso Rechazo [B] Cuando un sistema biométrico falla al identificar a una persona enrolada o falla al verificar la legítima identidad reclamada por una persona. También conocido como "error tipo I".

FAR [B] Tasa de falsa aceptación (False Acceptance Rate)

FRR [B] Tasa falso rechazo (False Rejection Rate)

GIF (Graphics Interchange Format). Un formato de archivos (comprimidos) de imágenes. También existen los llamados GIFs Animados, estos permiten de manejar imágenes transparentes e incluso varias imagenes superpuestas que permiten algunos browsers como Netscape y Explorer.

Giga Prefijo que indica un múltiplo de 1.000 millones, o sea 10^9. Cuando se emplea el sistema binario, como ocurre en informática, significa un múltiplo de 2^{30}, o sea 1.073.741.824.

GUI Graphical User Interface (Interfaz Gráfica de Usuario) Componente de una aplicación informática que visualiza el usuario y a través de la cual opera con ella. Está formada por ventanas, botones, menús e iconos, entre otros elementos

Hacker [B] Una persona que goza alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, de una PC o de una red. Este término se suele utilizar indebidamente como peyorativo, cuando sería mas correcto utilizar el término "cracker".

Hardware Son todos los componentes fisicos que componen una PC.

Hertz Hercio.Unidad de frecuencia electromagnética. Equivale a un ciclo por segundo.

Hipertexto Generalmente, cualquier texto que contiene enlaces hacia otros documentos. Los enlaces son palabras o frases que pueden ser cliqueadas por el lector para visualizar otro documento relacionado.

Hoax [B] (engaño, broma) Término utilizado para denominar a rumores falsos, especialmente sobre virus inexistentes, que se difunden por la red, a veces con mucho éxito causando al final casi tanto daño como si se tratase de un virus real.

Host (sistema central) Computadora que permite a los usuarios comunicarse con otros sistemas centrales de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet, WWW y FTP.

Hosting Espacio para un sitio o página de Internet en uno de los servidores SGI activos. Es decir, es un espacio en un disco rígido de una computadora conectada las 24 hs del día a Internet para que el autor del sitio pueda darse a conocer en la red.

HTML (*HyperText Markup Languaje*) Lenguaje de programación para la generación de páginas WWW de Internet.

HTTP (*HyperText Transport Protocol*). Protocolo utilizado para transferir archivos de hipertexto a traves de Internet. Reqiuere de un programa "cliente" de HTTP en un extremo y un "servidor" de HTTP en el otro extremo. Es el protocolo más importante de la WWW. (Ver también: Cliente, Servidor, Hipertexto, WWW).

HTTPS (HyperText Transport Protocol Secured). El protocolo de comunicación seguro empleado por los servidores de WWW con en clave. Esto es usado para trasportar por internet información confidencial como el número de tarjeta de crédito.

Icono Símbolo gráfico que aparece en la pantalla de una PC para representar determinada acción a realizar por el usuario, ejecutar un programa, leer una información, imprimir un texto, etc. Un icono hace referencia a un programa o archivo computacional y por lo tanto le permite el acceso al mismo por parte del usuario.

Identificación (uno a muchos) [B] El reconocimiento o identificación es el proceso por el cual se encuentra a qué persona corresponde un patrón de huella dactilar capturado

en el dispositivo, comparando éste con todos los patrones almacenados en una base de datos.

Impostor [B] Persona que intenta voluntaria o involuntariamente hacerse pasar por otra persona debidamente enrolada, entregando una muestra biométrica.

Internet Conjunto de redes conectadas entre sí, que utilizan El protocolo TCP/IP para comunicarse.

Internet2 Proyecto de interconexión de más de 100 universidades estadounidenses. El objetivo es desarrollar una red de altísima velocidad para la educación y la investigación.

IEEE *Institute of Electrical and Electronic Engineers* (Instituto de Ingenieros en Eléctricidad y Electrónica) Asociación de profesionales informáticos con base en los EE.UU.

Información Biométrica Normalizada [B] En nuestro trabajo utilizamos este concepto para nombrar aquella información común para las distintas áreas que hacen uso de ella; respetando estándares y métodos de uso prefijados.

Intranet Red privada dentro de una empresa que utiliza el mismo software y protocolos empleados en la Internet global, pero que sólo es de uso interno. (VER también: Internet, Red).

IP (Internet Protocol). Número único que consta de 4 partes separadas por puntos. Cada computadora conectada a Internet tiene un único número de IP. Si la maquina ni tiene un IP fijo, no está en realidad en Internet, sino que pide "prestado" un IP a un servidor cada vez que se conecta a la Red (usualmente vía módem). (Ver también: Dominio, Internet, TCP/IP).

ISO *International Organization for Standardization* (Organización Internacional para la Normalización) Organización de carácter voluntario fundada en 1946 que es responsable de la creación de estándares internacionales en muchas áreas, incluyendo la informática y las comunicaciones. Está formada por las organizaciones de normalización de sus países miembro.

Java Lenguaje de programación orientado a redes. Fue diseñado por *Sun Microsystems* específicamente para escribir programas que pudieran bajarse y ejecutarse en la computadora local, sin temor que éstos pudieran contener virus o provocar algún daño en los archivos. Las páginas web pueden contener pequeños programas hechos en Java llamados *applets*, por ejemplo: para producir animaciones u otros efectos vistosos (también se puede programar aplicaciones completas, como calculadoras, clientes de *chat*, etc.).

JavaScript Lenguaje de programación que soportan los navegadores. Su código se programa directamente dentro de la página *HTML*, y es interpretado por navegador al leerla. A pesar de su nombre, no tiene nada que ver con Java, ya que los *applets* creados por este ultimo se bajan, compilan y ejecutan al ser invocados por la página.

JPEG Formato gráfico comprimido desarrollado por la *'Join Photographic Expert Group'*. El formato JPEG soporta 24 bits por *pixel* y 8 bits por *pixel* en imágenes con escala de grises.

Kbps (kilobits por segundo) Unidad de medida de la capacidad de transmisión de una línea de telecomunicación. Cada kilobit esta formado por mil bits.

Keyword (clave de búsqueda, palabra clave) Conjunto de caracteres que puede utilizarse para buscar una información en un buscador o en un sitio web.

LAN (Local Area Network). (Red de Area Local). Red de computadoras ubicadas en El mismo ambiente, piso o edificio. (Ver también: Red).

Latente. Huella. [B] Huella digital tomada como muestra en el lugar de un crimen. Generalmente presenta muy mala formación que torna muy dificultosa su identificación.

LINUX Versión de libre distribución del sistema operativo UNIX; fue desarrollada por Linus Torvald

Link (enlace/enlazar, vínculo/vincular) Apuntadores hipertexto que sirven para saltar de una información a otra, o de un servidor a otro, cuando se navega por Internet o bien la acción de realizar dicho salto.

Login Nombre de usuario utilizado para obtener acceso a una computadora o a una red. A diferencia del *password*, el *login* no es secreto, ya que generalmente es conocido por quien posibilita el acceso mediante este recurso.

Megabyte (MB) 1.048.576 bytes; 1.024 Kilobytes.

Megahertz Unidad de medida de la frecuencia de reloj del microprocesador (en millones de ciclos por segundo).

MIME *Multipurpose Internet Mail Extensions* (Extensiones Multipropósito del Correo Internet) Conjunto de especificaciones Internet de libre distribución que permiten tanto el intercambio de texto escrito en lenguajes con diferentes juegos de caracteres como el correo multimedia entre ordenadores y aplicaciones que sigan los estándares de correo Internet.

Minucia [B] Una minucia, en el ambiente biométrico, describe las características de una huella digital en forma binaria para su más fácil almacenamiento y comparación.

Motor Biométrico [B] El elemento software de un sistema biométrico encargado de procesar datos biométricos durante las etapas de enrolamiento, captura, extracción, comparación.

Password [B] Palabra clave utilizada para obtener acceso a una computadora o a una red. Un password generalmente contiene una combinación de números y letras que no tienen ninguna lógica.

Penetración Genética [B] The degree to which characteristics are passed from generation to generation.

Plug-in Porción de software que agrega funciones a un programa más grande. Los plug-ins más comunes son los de los navegadores o los de programas para diseño gráfico, como photoshop. Los plug-ins son creados por terceros para agregar funciones que no se encuentran originalmente en los programas.

PIN [B] E una cadena aleatoria de números y/o letras asignada a cada individuo para su posterior identificación ante un sistema informático que lo requiera.

Píxel [B] Punto componente de una imagen digital.

POP (*Post Ofice Protocol*). Manera en que los programas clientes de correo electrónico obtienen los mensajes de un servidor de correo. Cuando se obtiene una cuenta *SLIP* o PPP, en general también se obtiene una cuenta POP para poder acceder al servidor de correo y leer los mensajes.

PPP (*Point to Point Protocol*). Protocolo que le permite a la computadora usar una línea telefónica y un módem para realzar una conexión *TCP/IP* y así simular que está realmente dentro de Internet.

RAM (*Random Access Memory*) Memoria de acceso aleatorio y de tipo volátil o temporal. Es la memoria de trabajo de una PC.

Red Se tiene una red cada vez que se conectan dos o más computadoras de manera que pueden compartir recursos. Al conectar dos o más redes en conjunto, se obtiene una Internet.

RS-232 *Acrónimo de Recommended Standard 232* [Estándar recomendado 232] Se trata del principal medio por el cual se conecta un ordenador a un periférico (sobretodo el módem). El interfaz tiene 25 conexiones denominado 'DB25' aunque existe otro de sólo 9, denominado 'DB9'. Es un estándar de 'Electronic Industry Association' ('EIA'). Es también conocida como: 'IEEE-448'.

RS-232-C *Acrónimo de Recommended Standard 232-C* [Estándar recomendado 232-C] Se trata del medio más adoptado en la actualidad por el cual se conecta un ordenador a un periférico (sobretodo el módem). El interfaz tiene 25 conexiones denominado 'DB25' aunque existe otro de sólo 9, denominado 'DB9'. Es la revisión 'C', la más utilizada, del estándar 'RS-232' de 'Electronic Industry Association' ('EIA').

RS-232 Norma de conexión estándar que conecta un Modem, o el equipo asociado a la terminal, a un ordenador .

RSA [B] Siglas de *Rivest-Shamir-Ardleman*, los tres inventores de la criptografía de clave pública. La empresa RSA Data Security, Inc. (Redwood City, California, USA) se ha hecho famosa por sus algoritmos de encriptación ampliamente utilizados en la transmisión de datos por redes de telecomunicaciones.

Scanner [B] Dispositivo informático utilizado para la captura óptica de información analógica y posterior digitalización de datos.

Servidor Computadora o programa que brinda un servicio específico al "cliente", que se ejecuta en otras computadoras. El término puede referirse tanto a una pieza de software en particular como a una computadora en donde se ejecuta este tipo de software. (Ver también: cliente, red).

SLIP (Serial Line Internet Protocol). Un estándar para usar la línea telefónica y un módem para conectarse a Internet. Se está reemplazando gradualmente por El PPP. (Ver también: PPP).

Socket Tipo de conexión (zócalo) entre el microprocesador y la placa madre (*socket* 5, *socket* 7, *Slot* 1 son algunos de los mas comunes).

Software Todos los componentes no físicos de una computadora (Programas).

SSL [B] (*Secure Socket Layer*) Sistema de seguridad en el cual los mensajes son encriptados de manera que solamente quien los emite y quien los recibe podrán descifrarlos.

Taxonomía Biométrica [B] Un método para clasificar el datos biométricos. Por ejemplo, la taxonomía biométrica de la Universidad de San (SJSU) utiliza particiones para clasificar el papel de datos biométricos dentro de una aplicación del dada.

TCP/IP (*Transmisor Control Protocol/Internet Protocol*). Conjunto de protocolos que definen a la Internet. Fueron originalmente diseñados para el sistema operativo Unix, pero actualmente puede encontrarse en cualquier sistema operativo. (Ver también: IP, Internet, Unix).

Uno a Muchos [B] Sinónimo de "identificación"

Uno a Uno [B] Sinónimo de "verificación".

URL (*Uniform Resource Locator*). Dirección de algún recurso de Internet que forma parte de la WWW.Ver también: navegador, WWW).

USB Tecnología que facilita la conexión de periféricos a la computadora. Esta reconoce automáticamente los dispositivos nuevos y no hay que insertar una placa controladora para el dispositivo en cuestión, sino que se conecta a la parte trasera de la computadora a un enchufe especial (puerto *USB*). La tarjeta madre debe tener esta tecnología en su *CHIPSET* para poder conectar dispositivos de este tipo.

Verificación (de identidad, o uno a uno) [B] La verificación o autentificación permite comprobar la identidad de una persona, comparando el patrón de su huella dactilar capturado en el dispositivo, con el patrón almacenado de la persona quien dice ser.

WAN (*Wide arrea Net*), red de area ancha. Una red de computadoras de gran tamaño, dispersa por un país o incluso por todo el planeta.

WWW (*World Wide Web*). Conjunto de recursos que pueden accederse utilizando un Navegador, mediante el protocolo *HTTP*.

Fuentes de Información

NIST. National Institute of Standards and Technology

International Association for Identification

Biometrics In Human Services User Group, Newsletter. www.dss.state.ct.us/digital.htm

FingerPrint USA

Java Card Forum Biometric Task Force

Biometric Consortium Working Group

Blanch, Leonardo. Cabrera, Federico M. Cafure, Martín J.

Organización IAFIS.