UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES

CAMPUS ARAGÓN

"SISTEMA DE RECUPERACIÓN DE INFORMACIÓN A TRAVÉS DE HUELLAS DACTILARES"

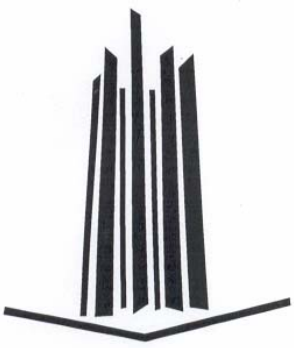
T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

P R E S E N T A:

JOSÉ MARTÍN MORALES LÓPEZ



ASESOR: M. EN I. JUAN CARLOS ROA BEIZA

SAN JUAN DE ARAGÓN EDO. DE MEX. 2006

Agradecimientos

A mi madre:

Porque sin su apoyo incondicional no hubiera podido llegar hasta aquí. Te quiero mamá.

A mi familia:

A mi padre y hermanos, por brindarme su apoyo y cariño.

A mis compañeros:

A todos aquellos que de alguna forma me ayudaron a lo largo de mi trayectoria académica.

Gracias a todos.

J. Martín M. L.

“SISTEMA DE RECUPERACIÓN DE INFORMACIÓN A TRAVÉS DE HUELLAS DACTILARES”

Índice

Introducción VII

Objetivos IX

Capítulo 1. Introducción 1

1.1 Justificación de la empresa conocida 1

1.2 Misión y Visión de la empresa elegida 7

1.3 Conceptos básicos de los sistemas de autenticación 12

1.4 Tipos de sistemas de reconocimiento dactilar 18

1.5 Ventajas y desventajas de lectores de huella dactilar 27

Capítulo 2. Marco teórico 35

2.1 Conceptos básicos de bases de datos relacionales 35

2.2 Características, ventajas y desventajas de SQL Server 2000 49

2.3 Características, ventajas y desventajas de Visual Basic .NET 54

2.4 Seguridad del sistema operativo elegido 58

Capítulo 3. Planteamiento del problema y elección de la solución 68

3.1 Problemática actual 68

3.2 Requerimientos generales y particulares 71

3.3 Búsqueda y análisis de la información 73

3.4 Problemática identificada por áreas y sus posibles soluciones 82

3.5 Opciones de solución y elección de la óptima 88

Capítulo 4. Desarrollo e implantación del sistema 95

4.1 Aplicación de la metodología elegida para el Back End 95

4.1.1 Diagrama de contexto 95

4.1.2 Diagrama de flujos de datos y de procesos 96

4.1.3 Diccionario de datos 106

4.1.4 Diagrama Entidad-Relación 113

4.1.5 Normalización 114

4.2 Diseño y construcción del Back End 118

4.3 Diseño y construcción del Front End 124

4.4 Pruebas e integración del sistema 145

4.5 Generación de reportes para la toma de decisiones 151

4.6 Factibilidad técnica y operativa 157

Manual de usuario y técnico 163

Conclusiones 179

Apéndice A 180

Glosario 183

Bibliografía 188

Introducción

En la actualidad, la seguridad en sistemas informáticos es un tema de vital importancia para las empresas privadas y el sector gobierno ya que la información es considerada uno de los activos más valiosos para la toma de decisiones y la productividad. Los problemas de accesos de usuarios no autorizados a los sistemas y a las bases de datos han causado enormes pérdidas en tiempo y dinero a miles de empresas.

Considerando que cada ser humano es único y en su organismo existen características genéticas y físicas que lo distingue, se decidió usar las huellas dactilares como medio de autenticación para el acceso a las aplicaciones antes mencionadas.

El trabajo llevó a una investigación de los diferentes tipos de sistemas biométricos, de éstos se seleccionó el sistema de detección de huella dactilar por cuestiones prácticas ya que en comparación con otros sistemas biométricos existentes se cuenta con mayor información disponible de este y es de fácil adquisición.

Las herramientas de software utilizadas en el desarrollo de este trabajo fueron Visual Basic .NET para la construcción del Front End y SQL Server 2000 para el Back End, las razones de la utilización fueron simples, se basó en la disponibilidad

comercial, en la relación costo-beneficio, la capacidad de programación y el tiempo para el desarrollo del sistema.

Con el apoyo de diagramas de contexto, de flujo de procesos y de datos, se obtuvo una solución para el control de accesos a aplicaciones que ayuda a mantener una mayor seguridad de la información.

Objetivos

En el presente trabajo se estableció como objetivo principal el desarrollo de un sistema capaz de salvo guardar la información, así como la obtención de información y la administración en el control de accesos a los usuarios en aplicaciones de alto riesgo por medio de la huella dactilar.

Entre los objetivos secundarios se pueden mencionar los siguientes:

- Controlar entradas y salidas de usuarios utilizando tecnología de acceso biométrico.
- Evitar fugas y daños a la información en las empresas.
- Crear un sistema con un ambiente agradable a los usuarios.
- Contar con un registro que permita conocer en todo momento las acciones realizadas por los usuarios dentro de las aplicaciones de la empresa.

Capítulo 1

Introducción

1.1 JUSTIFICACIÓN DE LA EMPRESA CONOCIDA

Anteriormente las empresas utilizaban los sistemas de información más conocidos los aislados o *standalone*, en los cuales las brechas de seguridad por interconexión eran casi nulas debido a su condición. Con el paso de los años surgen sistemas más complejos y con ellos nuevos problemas de seguridad e integridad de los datos. En aquel entonces el reto era mantener a los usuarios no autorizados fuera de los sistemas; hoy el reto consiste en conceder a los usuarios autorizados los derechos de acceso apropiados.

El manejo del flujo de la información nunca ha sido tan crítico o tan cambiante como en estos tiempos. A medida que los negocios crecen, los sistemas y la tecnología de información respaldan las operaciones de todas las comunidades de usuarios: clientes, proveedores, socios de negocios y empleados, por lo cual se requiere un ambiente de control y seguridad para una gran variedad de información y transacciones, por ejemplo: enviar órdenes de compra, pagar cuentas, mantener los registros actualizados, tener acceso a la red, acceder remotamente, proteger la información, etc. En consecuencia, existe una creciente demanda para que las organizaciones administren el acceso adecuadamente a las aplicaciones

corporativas, a las aplicaciones e-business[1], y en general, a los activos de información. En este sentido, las empresas necesitan proveer de una manera rápida, eficiente y controlada el acceso a los sistemas, aplicaciones y datos críticos para el negocio.

Una solución para satisfacer las necesidades de las organizaciones referentes al control de accesos es establecer la autenticación de los usuarios a través de huellas dactilares. Dicha opción tiene la ventaja de permitir accesos a usuarios autorizados con mayor exactitud de acuerdo a los privilegios otorgados a la información y/o los sistemas necesarios para desempeñar las actividades asignadas de acuerdo a su rol o puesto.

El control de acceso se encuentra constituido por etapas:

- **Identificación**: en esta etapa se tiene que asegurar que el sujeto es la identidad que dice ser, se provee a través de un nombre de usuario o cuenta.
- **Autenticación**: aquí se requiere proveer una segunda parte de la identidad del sujeto como: contraseña, llave criptográfica, PIN (Personal Identification Number - Número Personal de Identificación), atributo anatómico o token[2].
- **Autorización**: esta etapa verifica que el sujeto tenga los derechos y privilegios de acceso necesarios para ejecutar las acciones solicitadas.
- **Accountability**: (responsabilidad individual): en esta última etapa se tiene que asegurar que el sujeto, sea identificado individualmente y sus acciones sean registradas.

De las etapas antes mencionadas, la de mayor interés en este trabajo es la Autenticación.

[1] Actividad empresarial realizada a través de las Tecnologías de la Información y las Comunicaciones.
[2] Hardware u objetos físicos que se utilizan para proteger la información o la identidad.

FACTORES DE AUTENTICACIÓN

Existen tres tipos de autenticación:

- Tipo 1: algo que sabes (contraseñas, PIN, etc.).
- Tipo 2: algo que tienes (tokens, tarjetas inteligentes o de banda magnética, etc.).
- Tipo 3: algo que eres (huella dactilar, iris, retina, geometría de mano, etc.).

Autenticación tipo 1

Dentro de las empresas la forma más utilizada y conocida para la autenticación de usuarios es la contraseña, sin embargo esta opción de autenticación presenta varios problemas.

El manejo de contraseñas es un medio que presenta riesgos para la seguridad de la información ya que es mayormente susceptible al mal uso, las contraseñas típicamente son compartidas entre usuarios, aumentando la probabilidad de que existan accesos no autorizados que pueden convertirse en fuga de información, modificación de información, transacciones financieras no autorizadas, etc.

Históricamente las contraseñas seleccionadas por los usuarios son débiles porque incluyen datos relacionados con ellos, tales como su fecha de nacimiento, placas del automóvil, registro del seguro social, nombre de algún familiar, equipo deportivo favorito y frases o palabras comunes o que están de moda y que son fácilmente descubiertas por usuarios no autorizados.

Las contraseñas se consideran débiles si presentan deficiencias en su creación al no presentar las características mínimas recomendadas:

- Longitud mínima de 8 caracteres.
- Incluir letras minúsculas, mayúsculas, números y caracteres especiales.
- Distintas al nombre del usuario.
- No vacías o las de *default* (por defecto) del sistema.

Otra práctica común con el manejo de contraseñas es la utilización de la misma contraseña para todos los accesos que maneja, tanto personales como laborales, por ejemplo la misma contraseña para acceder a la red en la compañía, para su correo personal, para realizar transacciones bancarias personales, etc.

Algunos ataques conocidos dirigidos a las contraseñas débiles son: de fuerza bruta (prueba todas las combinaciones posibles hasta obtener el acceso), de diccionario (utiliza conjunto de palabras comunes y combinaciones en uno o más idiomas y prueba una a una hasta obtener el acceso) y denegación de servicio (al realizar cierta cantidad de intentos fallidos algunos sistemas bloquean las cuentas de usuarios).

Otro ataque conocido para obtener contraseñas y posteriormente acceder a sistemas de forma no autorizada es el *sniffing* (espiar), técnica en donde el atacante interviene las comunicaciones para obtener nombres de usuarios y contraseñas.

Cuando las contraseñas son más complejas frecuentemente, tienden a ser olvidadas por los usuarios y si los sistemas de información tienen implementada la política de bloqueo ante cierto número de intentos fallidos se incrementará el número de llamadas al área de sistemas o de soporte a usuarios para desbloquear cuentas, se desperdiciará tiempo productivo y se incrementará el gasto operativo y administrativo por esta razón.

Además, comúnmente, los usuarios anotarán sus contraseñas y las mantendrán disponibles o incluso visibles para evitar olvidarlas, generalmente en alguna nota de papel pegada en el escritorio, debajo del teclado y/o en algún cajón del lugar de trabajo.

Existen también otros medios de autenticación factor tipo 1 como: PIN, *passphrase* (frase contraseña), contraseña virtual, etc.

Todo lo anterior genera que las empresas cuenten con un mayor nivel de administración y configuración de sistemas, así como un programa de concientización del personal para mitigar los riesgos. Para lo cual deben almacenar al menos 6 generaciones de contraseñas, almacenar todas las contraseñas de forma cifrada, configurar los sistemas para forzar al personal a cambiar las contraseñas cada determinado lapso de tiempo, entre otras actividades con la finalidad de obtener una mayor protección para los activos informáticos de la organización lo cual ocasiona que los gastos se incrementen considerablemente.

Autenticación tipo 2

La segunda forma más común de autenticación que se utiliza es el factor tipo 2 (algo que tienes) que presenta vulnerabilidades similares a las que tiene la autenticación de factor tipo 1. Algunos dispositivos físicos utilizados son: tarjetas inteligentes, tarjetas con banda magnética, tokens, etc., sin embargo se prestan para que los usuarios hagan mal uso como sucede con las contraseñas; es decir, que estos sean cedidos a otro usuario generando accesos no controlados a los activos informáticos de la compañía. Así mismo, estos dispositivos generalmente requieren el uso de un PIN por lo que se encuentra nuevamente la posibilidad de que dicha clave sea olvidada o compartida por los usuarios, provocando el bloqueo de cuentas a causa de la superación de intentos no válidos permitidos. Otro riesgo latente es la pérdida o robo de los dispositivos.

Una desventaja que presenta este tipo de autenticación es la dependencia y disponibilidad de medios físicos para tener acceso a los sistemas, o peor aún, la utilización de más de un dispositivo físico para acceder a cada sistema aumentando el número de tarjetas inteligentes, tokens o cualquier otro dispositivo que los usuarios utilicen.

En el caso del uso de tarjetas inteligentes, aparte de los problemas que puede implicar su uso en sí, existen diversos métodos de ataque como: la ingeniería

inversa contra el circuito de silicio y los contenidos de la ROM (Read Only Memory - Memoria de sólo Lectura), adulterar la información almacenada en la tarjeta u obtener por diferentes métodos el contenido de la memoria EEPROM (Electrically Erasable Programmable Read Only Memory - Memoria de sólo Lectura Electrónicamente Borrable Programable).

Con las tarjetas de banda magnética se presenta el problema del *skimming* o clonación ya que en la actualidad existen diferentes medios por los cuales se puede realizar una copia, ya que por su misma tecnología la información que contiene puede ser leída fácilmente.

Los tokens pueden ser síncronos o asíncronos. Los tokens síncronos requieren sincronización con el servidor de autenticación que puede ser basada en el tiempo o en eventos (uso de llave secreta, cifrado y descifrado). Los tokens asíncronos están basados en esquema de reto y respuesta para autenticar al usuario. Ambos tipos son vulnerables a ataques *masquerading*, el usuario no autorizado se hace pasar por un usuario autorizado utilizando el dispositivo. Adicionalmente los tokens pueden presentar fallas de batería y/o hardware.

Autenticación tipo 3

La autenticación tipo 3 (algo que eres) utiliza mecanismos de acceso biométrico tales como: huellas dactilares, iris, retina, geometría de mano o cara, etc. Los sistemas biométricos verifican la identidad del individuo mediante un atributo personal y único, el cual es el método más efectivo y certero de verificar la identificación.

La autenticación mediante reconocimiento de huellas dactilares presenta la ventaja de no tener más la necesidad de hacer uso de una contraseña o PIN y/o el uso de tarjetas de proximidad, magnética o tokens, este tipo de autenticación utiliza en su lugar características físicas personales y únicas, que no cambian dependiendo de las circunstancias ni con el tiempo.

Una ventaja más que presenta, es la disminución en la capacidad de almacenamiento, ya que no se requiere guardar la imagen completa de la huella dactilar, basta con obtener puntos de referencia de la huella (patrones), adicionalmente este tipo de autenticación presenta mayor seguridad ante ataques de personal no autorizado. A causa de las ventajas que presenta este método de autenticación, las organizaciones presentan disminución en gastos, las llamadas a las áreas de sistemas y de soporte de usuarios disminuyen, los gastos por reemplazo de tarjetas, tokens o cualquier otro dispositivo se elimina y se mejora el control de accesos.

También se obtiene la ventaja de no repudiación de los usuarios a actividades realizadas, los usuarios no pueden negar el haber realizado actividades no permitidas, el no haber cometido errores o el hacer mal uso de los activos informáticos.

1.2 MISIÓN Y VISIÓN DE LA EMPRESA ELEGIDA

En este inciso se expone la misión y visión de las diferentes empresas en las que se puede implementar el Sistema de Recuperación de Información a través de Huellas Dactilares (SRIHD), primeramente se hará referencia a empresas paraestatales como lo es la Comisión Federal de Electricidad (CFE), por citar a una de las más importantes en su género, así mismo se analizará una empresa del sector público como es la Procuraduría General de la República (PGR) y finalmente empresas particulares como las Aseguradoras, en las que se puede implementar y explotar ampliamente el objetivo de la aplicación de identificar a su personal a través de su huella dactilar, tanto en cuestiones de seguridad en sus aplicaciones informáticas como en el registro de las entradas y salidas en sus jornadas laborales. Ayudando así al cumplimiento de los puntos mencionados en sus objetivos y metas de

desarrollo tanto en cuestiones tecnológicas como en lo que a desarrollo personal y de competitividad se refiere.

Siendo el Sistema de Recuperación de Información a través de Huellas Dactilares una opción de tecnología para todos los ramos del sector público y privado, se analizaran los contenidos de su misión y visión, para poder encontrar los fundamentos necesarios y poder así ofrecer con bases firmes la implementación del sistema de recuperación de información.

A continuación se analizará uno de los ramos más importantes, las paraestatales, haciendo referencia a la misión y visión de la Comisión Federal de Electricidad, posteriormente se comentará la misión y visión de dos tipos de empresas más, que son posibles usuarios del sistema a desarrollar.

Misión

- Asegurar, en el contexto de competencia y de modernización tecnológico que ha emprendido CFE, el servicio de energía eléctrica, en condiciones de cantidad, calidad y precio, y con la adecuada diversificación de fuentes de energía.
- Optimizar la utilización de la infraestructura física, comercial y de recursos humanos.
- Proporcionar una atención de excelencia a nuestros clientes.
- Proteger el medio ambiente, promover el desarrollo social y respetar los valores de las poblaciones donde se ubican las obras de electrificación.

Visión

- Mantener a CFE como la empresa de energía eléctrica más importante a nivel nacional.
- Operar con base en indicadores internacionales en materia de productividad, competitividad y tecnología.

- Ser reconocida por nuestros usuarios como una empresa de excelencia que se preocupa por el medio ambiente y que está orientada al servicio del cliente.
- Administrar en forma ágil, eficiente y competitiva, los recursos de la entidad, promoviendo la mejora continua de su gestión y la alta calificación y el desarrollo profesional de sus trabajadores.

Analizando los puntos en particular, y asociándolos a los objetivos y alcances del sistema a desarrollar de recuperación de información a través de huellas dactilares, se puede destacar la importancia de este en el segundo punto de los enlistados anteriormente en la misión de la empresa, ya que hace referencia a la optimización del uso de la infraestructura física, y de recursos humanos, siendo éstas parte medular de las ventajas que ofrece el sistema, al poder controlar adecuadamente el uso de la infraestructura de cómputo.

Así mismo en la optimización de los recursos humanos aplica ampliamente la implementación del sistema, al tener la posibilidad de almacenar, controlar y administrar los registros de accesos tanto a las aplicaciones informáticas, como a las jornadas laborales de los trabajadores de cualquiera de las empresas en las que se decida implantar el sistema descrito en el presente trabajo.

Al igual que en la misión de la empresa paraestatal analizada, el Sistema de Recuperación de Información a través de Huellas Dactilares aplica profundamente en la visión de la Comisión Federal de Electricidad, ya que al buscar operar con base en indicadores internacionales en materia de productividad, competitividad y tecnología se nota una relación directa con los objetivos del proyecto a desarrollar.

Particularmente en materia de productividad, al poder controlar las entradas y salidas del personal, así como optimizar las horas hombre para un buen desempeño de los procesos, manteniendo así los niveles en materia de tecnología aceptables para cumplir con sus objetivos.

El segundo tipo de empresa candidata a utilizar el Sistema de Recuperación de Información a través de Huellas Dactilares es la Procuraduría General de la República, que es el órgano del poder Ejecutivo Federal, que se encarga principalmente de investigar y perseguir los delitos del orden federal y cuyo titular es el procurador General de la República, quién preside al ministerio público de la federación y a sus órganos auxiliares que son la policía investigadora y los peritos.

Misión

- "Representar a la sociedad y a la federación en la investigación y persecución de delitos del fuero federal, con apego a los principios de legalidad, certeza y seguridad jurídica, con respeto a los derechos humanos, que garanticen el Estado de Derecho".

Visión

- "Tenemos una clara visión institucional para el mediano y largo plazo: visualizamos en tres años una estructura funcional de procuración de justicia, en seis un sistema saneado. Lo anterior, para que en el año 2025 las instituciones que participen en la procuración de justicia sean de excelencia, cuenten con personal con vocación de servicio y sólida formación que contribuya a que los ciudadanos vivan en condiciones que promuevan el desarrollo integral dentro del Estado de Derecho".

Al igual que en la paraestatal anteriormente analizada, en el caso de la Procuraduría General de la República también se tiene un gran campo de desarrollo e implementación del Sistema de Recuperación de Información a través de Huellas Dactilares, ya que la institución visualiza a corto y mediano plazo un sistema de procuración de justicia saneado, para cumplir con esta tarea es necesario contar con innovaciones tecnológicas, para lo cuál el sistema a desarrollar resultará una herramienta muy relevante para cumplir este objetivo.

Finalmente se analiza la misión y visión de una empresa particular, para tener los elementos de peso y poder fundamentar con ello que el sistema a desarrollar es útil en cualquiera de los diferentes tipos de empresas.

Siendo una de las más importantes empresas de su ramo, le toca el análisis a la empresa ING Comercial América, de la cuál se mencionan brevemente sus características particulares, servicios y antecedentes, así como su visión y misión, para poder así, al igual que con las empresas anteriores, fundamentar la implementación del sistema.

ING Comercial América es una empresa conformada a partir de la unión entre ING Group, Seguros Comercial América y Afore Bital.

ING Comercial América brinda servicios financieros a todas las personas que buscan concretar sus proyectos de negocios en México. Los servicios que brinda son:

- Seguros
- Afore
- Arrendadora
- Hipotecaria
- Fianzas
- Pensiones
- División Fiduciaria

Misión y visión

- “Ser una empresa orientada al cliente, líder, global, innovadora y proveedora de servicios financieros a costos accesibles, mediante los canales de distribución de preferencia del cliente y en mercados en los que ING pueda crear valor para sus accionistas”.

1.3 CONCEPTOS BÁSICOS DE LOS SISTEMAS DE AUTENTICACIÓN

Un sistema acotado en sus componentes y sus usuarios, es aquél en que es posible hacer una lista de los unos y los otros, es susceptible de emplear un medio que permita a cada componente saber en forma inequívoca con quién está interactuando en un momento dado. Este conocimiento es la base del funcionamiento seguro del sistema. En cada interacción es posible identificar las partes, garantizar su identidad y la integridad, para así registrar lo sucedido atribuyendo las acciones en forma no ambigua.

Además, la identificación y autenticación de las partes que forman un sistema, es la única manera de sustentar un mecanismo de control de acceso a las funciones del mismo. Esto permite entre otras cosas mejorar las propiedades de confidencialidad e integridad, sea este un sistema de información o de otro tipo.

Registro

Cualquier sistema que pretenda hacer uso de mecanismos de identificación y autenticación requiere de un procedimiento de registro de las componentes del mismo, por lo que es necesario contar con un inventario de componentes y/o de usuarios. El sistema se considera acotado a los elementos que consten en este inventario, y aquellos elementos que no aparezcan en este inventario, por definición, no forman parte del sistema. Claro que éste inventario se modifica a lo largo del tiempo, estando sujeto a procesos de altas, bajas y cambios.

Identificación

En el registro de cualquier sistema se anota un identificador del usuario, este puede ser su nombre, un apodo, un número o información que distinga a un usuario de los demás. Mediante este identificador se localiza en el registro el renglón correspondiente al usuario.

Autenticación

Al registrarse el usuario debe depositar o recibir un autenticador, que es un dato que se relaciona con el usuario. La posesión de este dato se considera como evidencia incontrovertible de que el que lo exhibe es quién aparece en el registro.

Como se mencionó anteriormente, los mecanismos de autenticación se clasifican básicamente en tres grupos, algo que el usuario conoce, algo que el usuario tiene y algo que caracteriza al usuario, en este capítulo se explican los sistemas que pertenecen al tercer grupo.

Sistemas de autenticación basada en características físicas

La biometría se basa en obtener medidas o características del cuerpo de una persona para autenticarla, estas características se depositan en el momento del registro y su descripción se guarda en una lista de usuarios. Al solicitar acceso el usuario exhibe la característica que haya registrado, se obtiene la descripción y se la compara con la que se encuentra almacenada (figura 1.3.1).

Las medidas más usuales en los sistemas biométricos son la de los dedos, la geometría de la mano, la retina, el iris y el rostro, dichos sistemas de autenticación se describen a continuación.

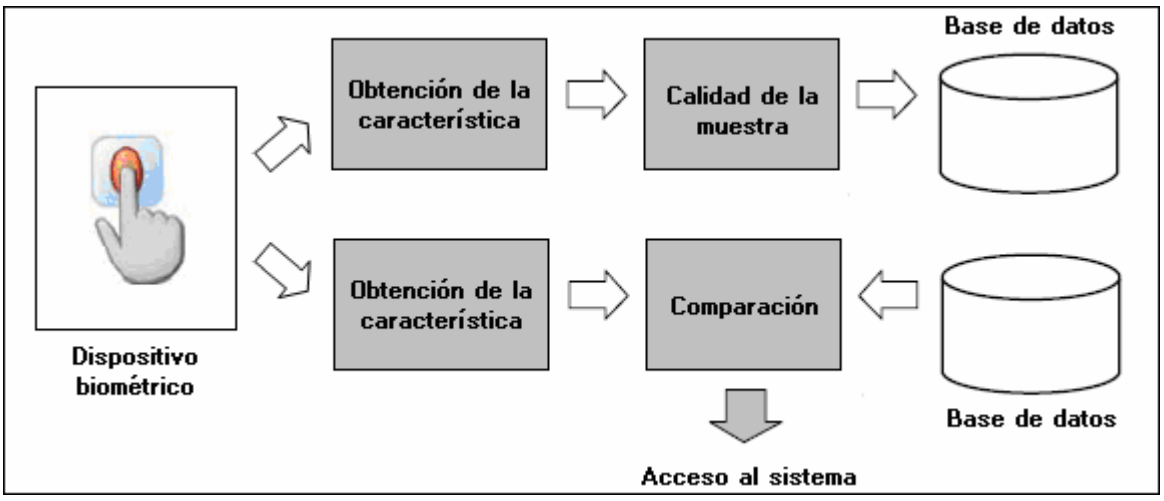


Figura 1.3.1. Proceso de registro y autenticación en un sistema biométrico

- Geometría de la mano.

  Los sistemas de autenticación basados en el análisis de la geometría de la mano son los más rápidos dentro de los biométricos; con una probabilidad de error aceptable en la mayoría de ocasiones.

  Cuando un usuario necesita ser autenticado sitúa su mano sobre un dispositivo lector con unas guías que indican la posición correcta para la lectura. Una vez la mano está correctamente situada, unas cámaras toman una imagen superior y otra lateral, de las que se extraen ciertos datos (anchura, longitud, área, determinadas distancias) en un formato de tres dimensiones (figura 1.3.2). Transformando estos datos en un modelo que se contrasta contra una base de patrones, el sistema es capaz de permitir o denegar acceso a cada usuario.

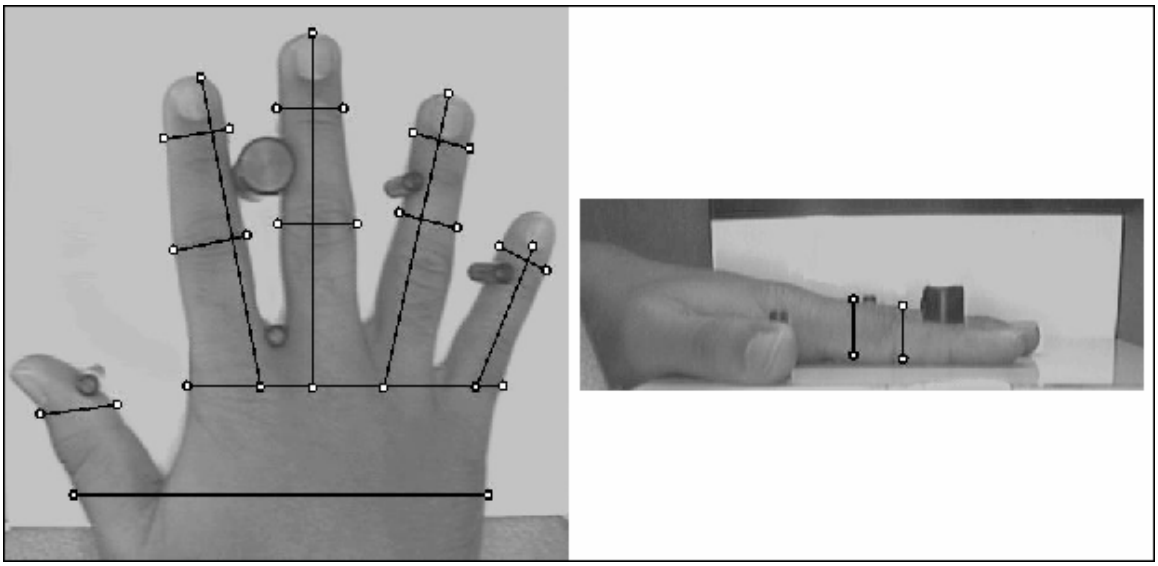


Figura 1.3.2. Verificación de la geometría de la mano

- Huellas dactilares.

  Típicamente la huella dactilar de un individuo ha sido un patrón bastante bueno para determinar su identidad de forma inequívoca, ya que está aceptado que dos dedos nunca poseen huellas similares, ni siquiera entre gemelos o entre dedos de la misma persona.

Cuando un usuario desea autenticarse ante el sistema, sitúa su dedo en un área determinada (área de lectura). Aquí se toma una imagen que posteriormente se normaliza y es de esta imagen normalizada de la que el sistema extrae las minucias (ciertos arcos, bucles o remolinos de la huella), los detalles se identifican y se ubican, y esto constituye el identificador de la huella (figura 1.3.3).

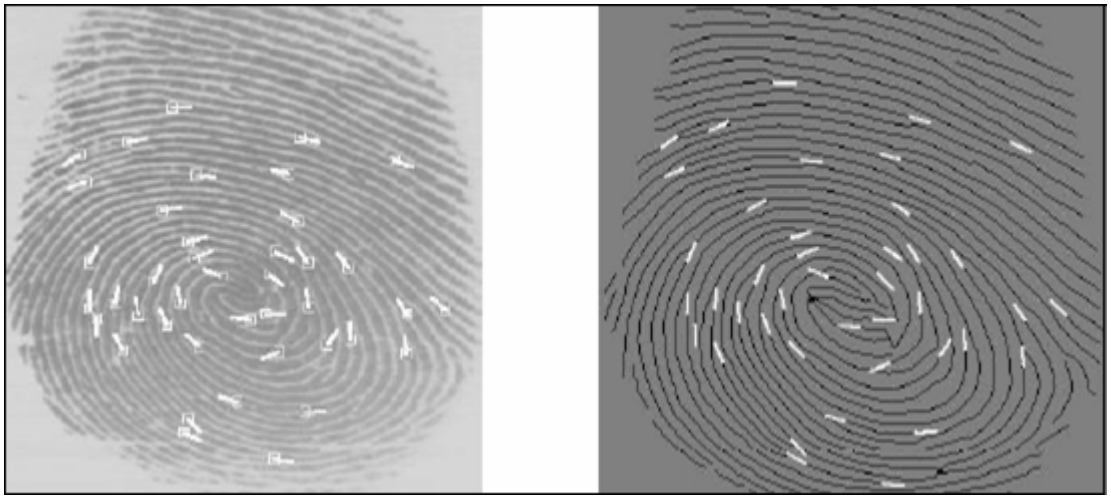


Figura 1.3.3. Puntos característicos de la huella dactilar

- Análisis de la retina.

  La retina está situada en la parte posterior dentro del globo ocular. La sangre alcanza la retina a través de los vasos sanguíneos que vienen del nervio óptico (figura 1.3.4). La vasculatura retinal (forma de los vasos sanguíneos de la retina) es un elemento único en cada persona.

  En los sistemas de autenticación basados en patrones retínales el usuario a identificar debe mirar a través de unos binoculares, ajustar la distancia interocular y el movimiento de la cabeza, mirar a un punto determinado y por último pulsar un botón para indicar al dispositivo que se encuentra listo para el análisis. En ese momento se escanea la retina con una radiación infrarroja de baja intensidad en forma de espiral, detectando los nodos y ramas del área retinal.

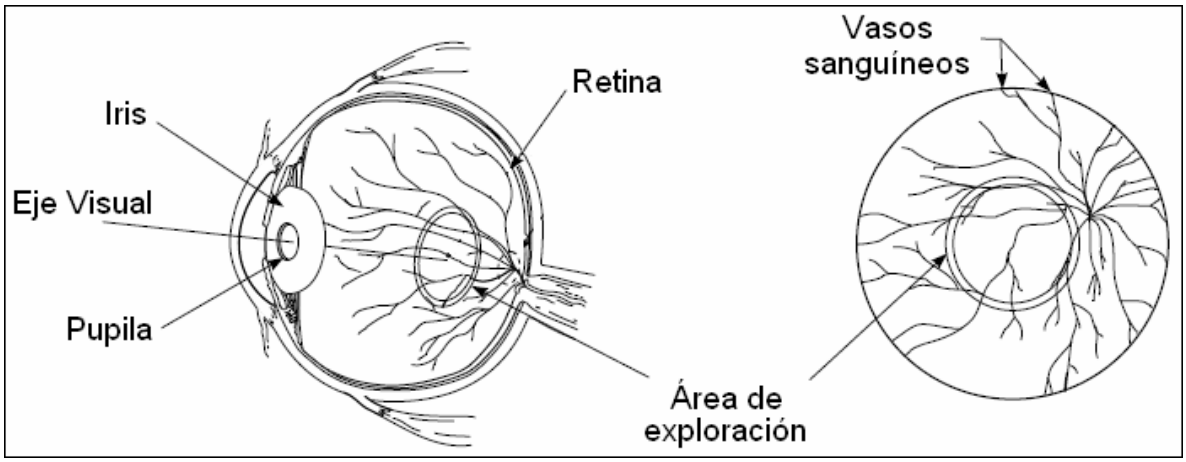


Figura 1.3.4. Diagrama del ojo y área retinal

- Análisis del iris.

  El iris humano tiene una estructura única en cada individuo que forma un sistema muy complejo e inalterable durante toda la vida de la persona.

  En la autenticación basada en el reconocimiento del iris, se emplea una cámara convencional de televisión digital para capturar una imagen en blanco y negro, en un entorno correctamente iluminado; la imagen es analizada reduciéndola por la derecha y por la izquierda para aislar el iris. Simultáneamente se localiza la pupila, y se excluye el segmento de 90 grados inferior.

  Una vez que se ha ubicado el iris se usa un análisis en dos dimensiones para filtrar y mapear partes de él en cientos de vectores, las características que se analizan son los anillos, ralladuras, pecas y la corona. Se toman los valores de la orientación, posición y frecuencia espacial de las áreas seleccionadas. Estos vectores forman un código patentado, que es el identificador. Esa muestra, denominada IrisCode, es la que se almacena en la base de datos (figura 1.3.5).

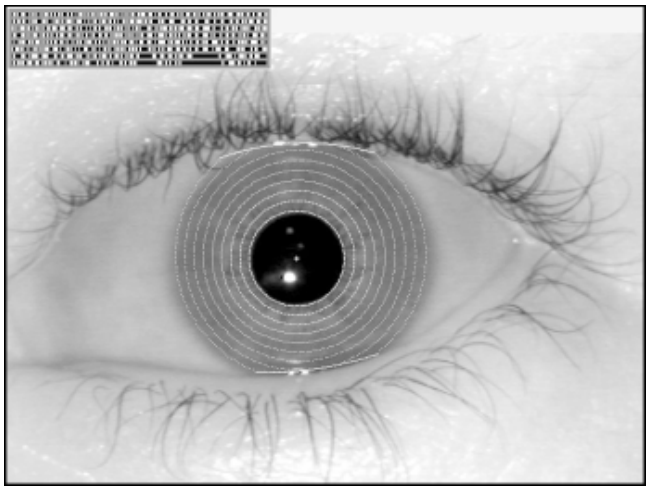


Figura 1.3.5. Aislamiento del iris, y su "IrisCode" resultante

- Análisis del rostro.

  La técnica más usada para el reconocimiento de rostros es la geometría facial, en la cual se tiene una colección de fotografías de personas que son homogéneas, es decir, del mismo tamaño y tomadas desde el mismo ángulo.

  Para verificar la identidad de alguien que aparezca en la colección basta tomar una fotografía o imagen de televisión y extraer las dimensiones, distancias, ángulos y curvaturas de los elementos que constituyen el rostro (ojos, boca, nariz, etc.) y luego compararlos con los datos que se tengan registrados (figura 1.3.6).

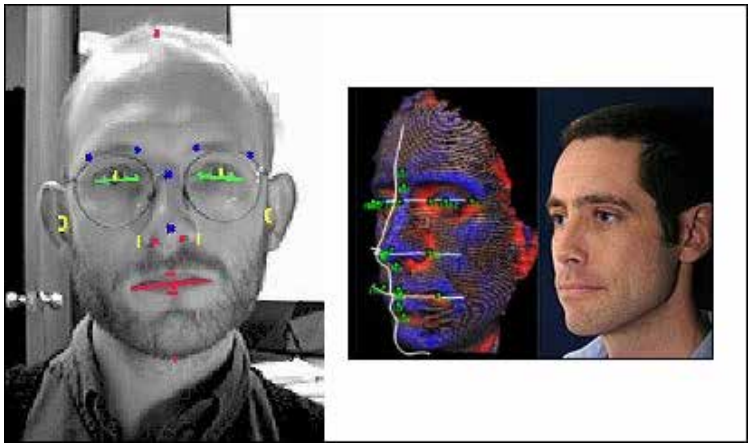


Figura 1.3.6. Verificación de la geometría facial

Precisión

La principal y más crítica característica de los sistemas de autenticación biométricos es su precisión. Si el sistema no puede separar con precisión a los usuarios de los impostores, en realidad no es un sistema de autenticación. Los dos elementos que permiten medir la precisión son la tasa de rechazos falsos (el porcentaje de usuarios que son rechazados por error) y la tasa de aceptaciones equivocadas (el porcentaje de impostores que son aceptados).

Los rechazos falsos no deben confundirse con las fallas de captura. Si el sensor no recibe suficiente información (huellas borrosas, posición incorrecta de la mano, etc.) el sistema no puede verificar la identidad, algunos suplantadores causan estas fallas deliberadamente, buscando que se les otorguen privilegios por fuera del sistema.

Las aceptaciones falsas son las que se consideran más graves en sistemas biométricos, pues permiten el acceso de intrusos o suplantadores. Los sistemas biométricos permiten ajustar algunos parámetros para optimizar su funcionamiento. Si se desea eliminar las aceptaciones falsas un sistema se puede ajustar para lograrlo casi perfectamente. En este estado se tiene una tasa de aceptaciones falsas de cero. Si se desean eliminar los rechazos falsos, el sistema se puede ajustar de otra manera, que permita el acceso con una verificación sólo aproximada.

1.4 TIPOS DE SISTEMAS DE RECONOCIMIENTO DACTILAR

Touch screen

Actualmente existen pantallas táctiles con varias tecnologías distintas: capacitiva, resistiva, infrarroja, de ondas acústicas, etc., aunque todas funcionan con el mismo principio: la alteración de un flujo de energía en algún punto de la pantalla, causado por un dedo, pluma, etc., para medir las coordenadas del punto tocado con relación

a las esquinas de la pantalla, es necesario comparar las ventajas y desventajas de cada una para saber cuál es la mejor.

- Capacitiva.

  Consiste de una membrana de vidrio con una delgada capa metálica sobre la superficie de la pantalla. Se aplica una ligera corriente eléctrica a la pantalla, la cual sólo se altera al ser tocada con un dedo, o bien, con un objeto conductor de electricidad (figura 1.4.1).

  Esta tecnología es excelente para todo tipo de aplicaciones destinadas a ambientes hostiles, como terminales industriales, restauranteras, kioscos informativos, etc. Aproximadamente el 80% de la base instalada a nivel mundial de pantallas *touch screen* (pantalla de contacto) utilizan esta tecnología.

  Las membranas capacitivas funcionan tocando ligeramente, son resistentes a arañazos y su desempeño no se afecta por manchas de grasa, químicas, solventes, polvo o agua.

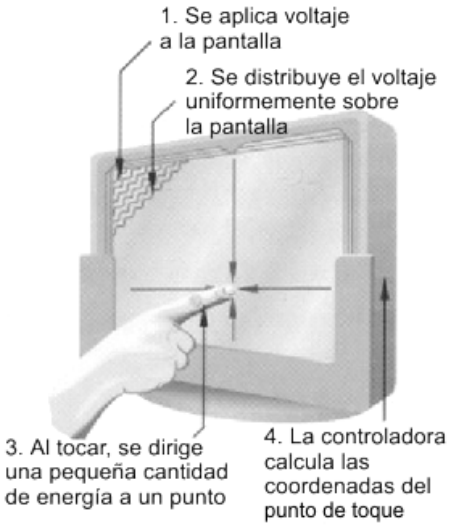


Figura 1.4.1. Funcionamiento de una membrana capacitiva

- Resistiva.

  Se integra por una membrana de vidrio con una delgada capa metálica sobre la que se pone una hoja de poliéster y luego ésta es cubierta con una capa protectora. También se aplica una corriente eléctrica, pero ésta se interrumpe cuando la capa exterior de la membrana toca la capa de vidrio de la misma. Puede activarse con cualquier objeto (guantes, cualquier pluma, etc.), sin embargo se recomienda sólo para ambientes controlados (con supervisión) pues la superficie de la pantalla podría ser dañada por malos tratos al ser de poliéster endurecido (figura 1.4.2).

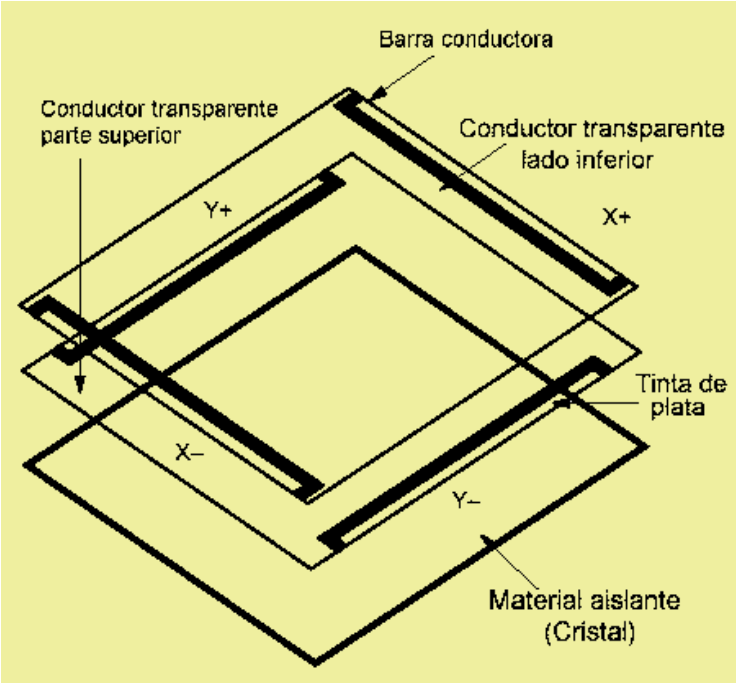


Figura 1.4.2. Funcionamiento de la membrana resistiva

- Ondas Acústicas.

  Se basa en la transmisión de ondas acústicas sobre la superficie de una membrana de vidrio puesta sobre la pantalla, se activa presionando con una pluma con punta suave, guante o dedo. Debe estar en un ambiente limpio, pues su desempeño se afecta cuando caen sobre la pantalla cantidades de polvo, líquidos u otros contaminantes (figura 1.4.3).

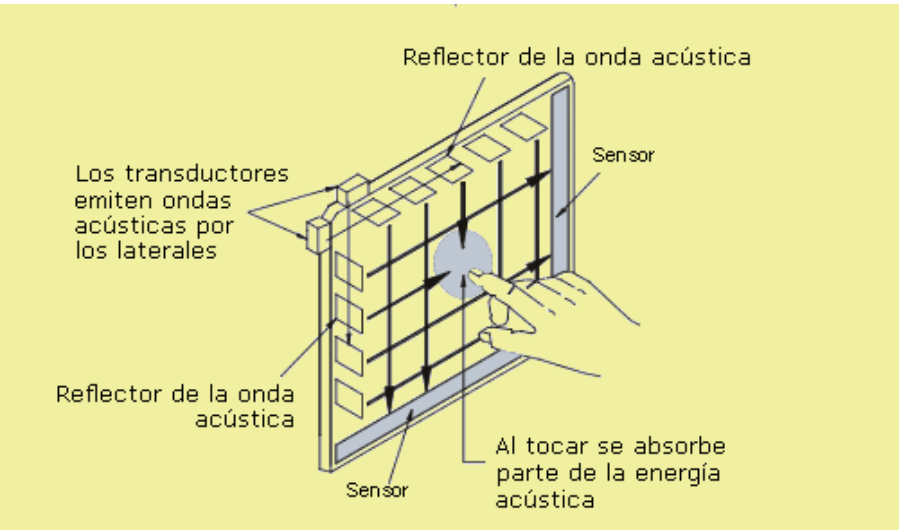


Figura 1.4.3. Funcionamiento de una membrana por ondas acústicas

- Infrarroja.

  Compuesta de tableros cableados y un bisel infrarrojo transparente. Al tocar la pantalla se interrumpe el flujo de los rayos infrarrojos para determinar las coordenadas del toque. Puede activarse sin tocar la pantalla, lo cual podría hacer que registre “toques falsos", además tiene muy baja resolución y requiere un costoso bisel diseñado a la medida de la aplicación. Por estas razones, la tecnología infrarroja está siendo desplazada del mercado por otras tecnologías (figura 1.4.4).

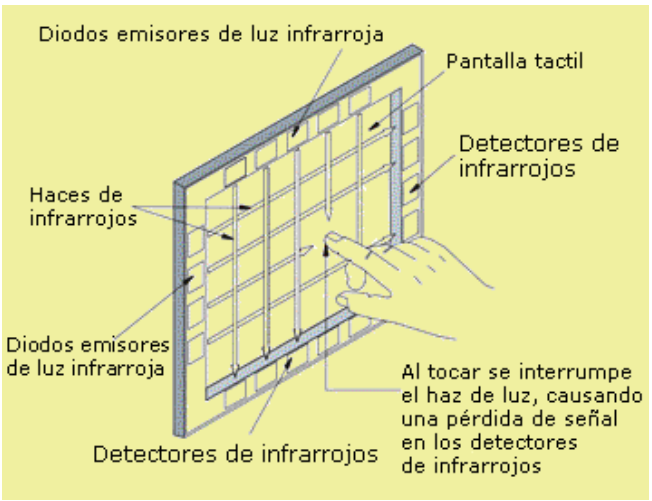


Figura 1.4.4. Funcionamiento de una membrana por infrarrojos

- NFI (Near-Field Imaging).

  Se integra con un sensor con una capa conductora transparente sobre la que se genera un campo electroestático de baja potencia, y un dispositivo procesador de imágenes. En este caso, se monitorea la corriente eléctrica sobre la pantalla, como en el caso capacitivo, pero además el sensor procesador de imágenes determina de modo "inteligente" el punto de toque ignorando en base a las condiciones previas a éste cualquier estática, ruido, objetos grandes o lejanos y por ende “toques falsos". Esta tecnología es muy resistente a daños físicos y a agentes químicos, no afectan su funcionamiento los contaminantes como polvo, agua, etc. y funciona con casi cualquier tipo de guantes (figura 1.4.5).

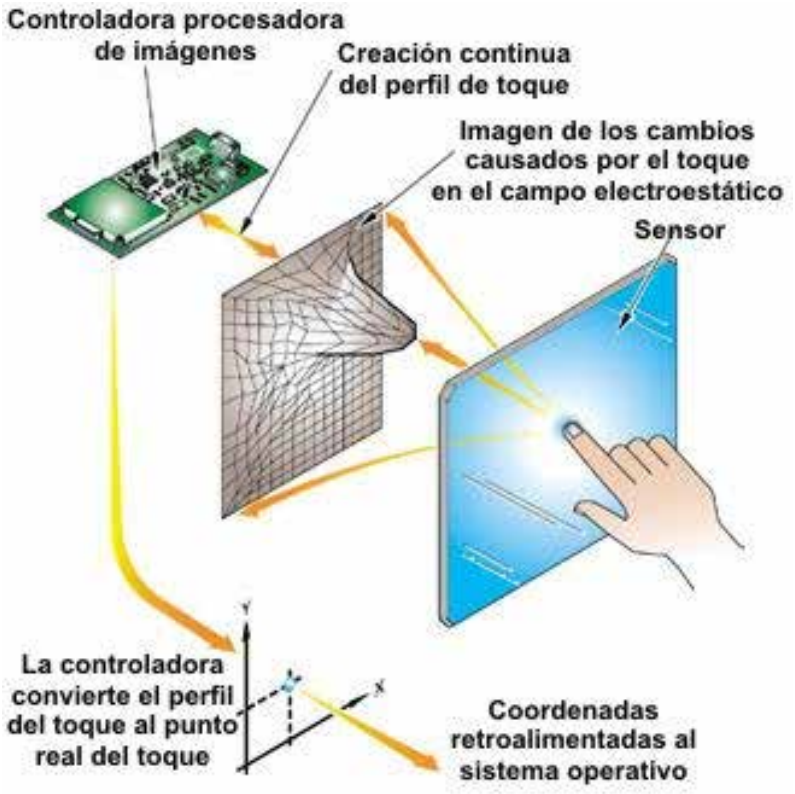


Figura 1.4.5. Funcionamiento de membranas NFI

Escáner

El término digitalización se puede asociar de una manera clara, la forma como una imagen se puede convertir en un idioma comprensible para las computadoras.

En general las señales exteriores que hacen posible la identificación en su estado natural, se transforman en código binario (0's y 1's) que mediante la utilización de programas se pueden transformar de acuerdo a los requerimientos.

Los escáneres son periféricos diseñados para registrar caracteres escritos o gráficos facilitando su introducción en la computadora convirtiéndolos en información binaria comprensible para ésta. El funcionamiento de un escáner es similar al de una fotocopiadora. Se coloca una imagen sobre una superficie de cristal transparente, bajo el cristal existe una lente especial que realiza un barrido de la imagen; al realizar el barrido, la información es convertida en una sucesión de información en forma de unos y ceros que se introducen en la computadora.

Una de sus principales ventajas, es la velocidad de lectura e introducción de la información en el sistema informático con respecto al método tradicional de introducción manual de datos por medio del teclado, llegándose a alcanzar los 1,200 caracteres por segundo.

La cualidad más importante de un escáner, es el grado de finura con el que se puede realizar el análisis de la imagen. Los fabricantes indican dos tipos de definición:

- Óptica, que es la realmente importante, está determinada por el número de elementos CCD (Charge Coupled Device - Dispositivo Acoplado por Carga Eléctrica) y la resolución de la lente. Se mide en puntos por pulgada.
- Interpolada, que es el resultado de una serie de cálculos de difícil verificación.

Al iniciar la exploración de la imagen, ésta es expuesta a una fuente de luz, la cual, refleja la imagen que es conducida mediante un sistema de espejos y lente hacia el CCD (figura 1.4.6 y figura 1.4.7).

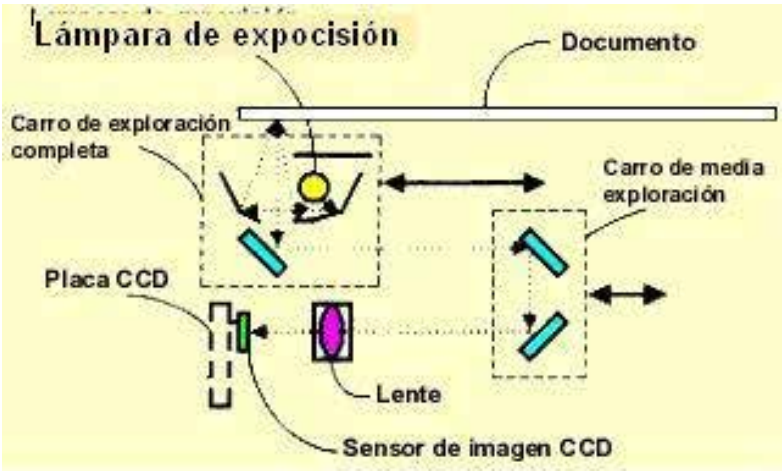


Figura 1.4.6. Funcionamiento del escáner (I)

Los espejos están situados en el carro de exploración, el cual es impulsado por un motor y transmite su movimiento mediante un sistema de correas.

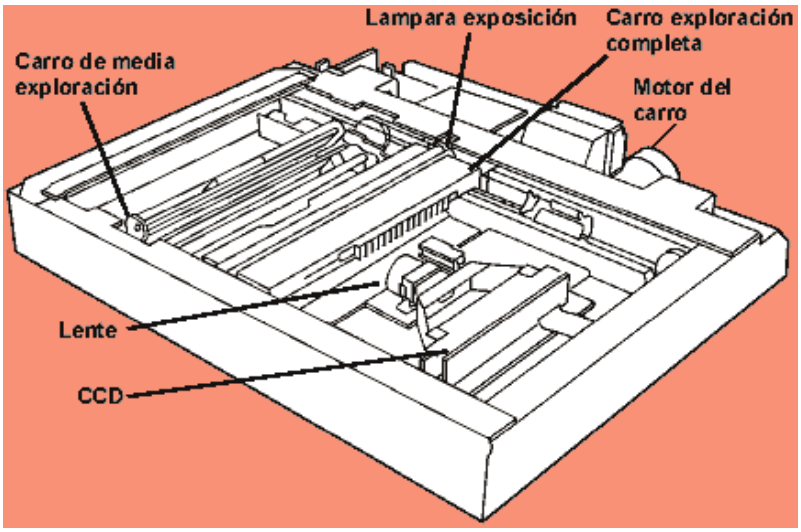


Figura 1.4.7 Funcionamiento de escáner (II)

El CCD, son diodos[3] sensibles a la luz, formado por diodos rojo, verde y azul y lleva tantos según la resolución por pulgada, por ejemplo un escáner de 300 ppp, en una pulgada llevaría 300 diodos rojos, 300 verdes y 300 azul. Estos diodos convierten la luz en corriente eléctrica, dependiendo de la intensidad de luz reflejada, la corriente eléctrica va variando su voltaje obteniendo un formato analógico.

El ADC (Analog to Digital Converter - Conversor Analógico Digital), es un dispositivo en el cual interpreta las variaciones del voltaje eléctrico y lo convierte en píxel digitales. Según la resolución del escáner crea los píxeles por pulgadas. En los escáneres a color la luz pasa por filtros rojo, verde y azul.

Fotografía

El uso de la fotografía ha aumentado considerablemente debido a que produce imágenes instantáneas. La tecnología utilizada en la fotografía digital, se basa en la sustitución de la película por un chip sensible a la luz. CCD es el chip encargado de capturar la imagen y constituye el elemento más importante de una cámara digital. Su estructura es reticular y cada uno de sus puntos es un elemento fotosensible que recibirá más o menos luz. Cuantos más valores sea capaz de recibir el CCD mejor será la calidad obtenida con la cámara. No obstante se debe tener siempre en cuenta cual es el objeto de la imagen capturada ya que de poco servirá obtener imágenes de mucha precisión (muchos puntos sensibles) si su destino es ser reproducida en un medio incapaz de distinguir tanta información (figura 1.4.8).

El formato digital se basa en el almacenamiento de la imagen mediante dígitos (números) que se mantendrán inmutables a lo largo del tiempo, con lo que la calidad de la imagen no disminuirá nunca. La reproducción de una imagen almacenada en un soporte digital puede ser repetida tantas veces como se desee, produciéndose siempre un duplicado de la misma calidad que la imagen original.

[3] Un diodo es un dispositivo electrónico que permite el paso de la corriente eléctrica en una única dirección.

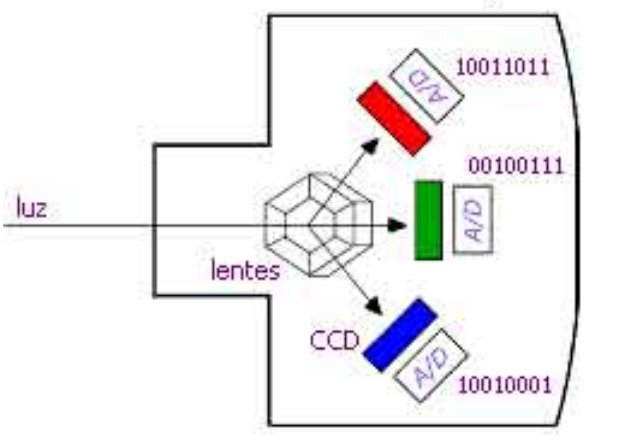


Figura 1.4.8 Funcionamiento de cámara digital

El mayor beneficio en la fotografía se encuentra en el proceso de revelado, mientras que en el proceso convencional se requiere imprimir un negativo para ser llevado a un proceso de revelado y fijación de la imagen el cual puede variar entre horas o días en el caso de las imágenes fotográficas, las imágenes digitales se obtienen en fracciones de segundos, esto puede significar una diferencia entre la obtención o no de una buena imagen. En la fotografía digital el resultado puede ser analizado de inmediato, editado, ampliado, puede aumentarse o disminuirse el contraste y la luminosidad para obtener la mejor imagen posible del objeto en estudio y preservarla de manera electrónica o impresa.

A pesar de ser más lentas y más difíciles de utilizar que los escáneres planos, las cámaras digitales se adaptan a una amplia variedad de documentos y objetos, siendo muy útiles para fotografía de detalle (macrofotografía). Se pueden capturar en forma segura los materiales más frágiles, aunque la necesidad de proporcionar iluminación externa significa que el daño causado por la luz puede ser una preocupación.

Algunas desventajas que pueden presentarse son:

- La facilidad con la que las imágenes electrónicas pueden ser modificadas, despierta la suspicacia de que las mismas pudiesen ser adulteradas para

actos ilícitos. Esta suspicacia ha creado una sombra de duda sobre el uso de las fotografías digitales como documento válido en el respaldo de un trabajo experimental o como pruebas de aspecto legal en conflictos de tipo judicial.

- La compresión de las imágenes capturadas habitual en cámaras portátiles, puede basarse el algoritmos con pérdidas, que eliminan variaciones cromáticas secundarias de un píxel al siguiente, con lo que el detalle de la imagen se reduce, perdiendo calidad. Adicionalmente, se pueden producir errores debidos a una mala interpretación de la información de la imagen durante el proceso de compresión, que pueden ocasionar defectos de color a una imagen JPEG[4].
- Además de estos factores, afectan a la calidad de la imagen obtenida otros también habituales en la fotografía clásica, como enfoque, abertura del diafragma, ajuste de la exposición, etc.

1.5 VENTAJAS Y DESVENTAJAS DE LOS LECTORES DE HUELLA DACTILAR

Como se mencionó anteriormente, en la actualidad la seguridad es un tema de suma importancia en las empresas privadas y el sector gobierno, hoy en día los expertos en seguridad informática encuentran cada vez más frecuente la preocupación de directivos y funcionarios en las áreas que se encargan de manejar recursos e información valiosa ya que la pregunta obligada ante la cual se encuentran de manera muy frecuente es: ¿Quién accede a mi sistema, es quién realmente dice ser?

Se requiere tener la certeza de estar dando privilegios, accesos, servicios o beneficios a terceros (ya sea dentro o fuera de la empresa o gobierno), la huella

[4] Formato de archivo que utiliza un algoritmo de compresión de imágenes con pérdida. El formato de archivos JPEG se abrevia frecuentemente JPG.

digital es un valioso aliado. No obstante los dispositivos lectores de huella dactilar presentan ventajas y desventajas que se indican a continuación.

Los lectores de huella digital computarizados eran una tecnología bastante exótica hasta hace unos años, cuando empezaron a aparecer en todos lados para controlar el acceso a edificios que necesitan alta seguridad, e incluso en el mouse y teclados para computadora, reemplazando o complementando el uso de una contraseña para dar acceso a un equipo de cómputo.

Fundamentos de las huellas dactilares

Los seres humanos nacen con tarjetas de identificación integradas, muy fácilmente accesibles: sus huellas digitales, las cuales son únicas, ya que ni los gemelos unicelulares tienen las mismas huellas y las huellas digitales son diferentes en cada dedo, en resumen son diseños virtualmente únicos.

Cada huella dactilar tiene diminutos “valles y crestas” de piel en la punta de los dedos que eran de gran utilidad a los ancestros de la raza humana, pues les permitían asir con mayor facilidad los objetos. Esos valles y crestas se forman por una combinación de factores genéticos y ambientales aleatorios, como la posición del feto en un momento en particular y la composición y densidad exacta del liquido amniótico que le rodea (figura 1.5.1).

Figura 1.5.1. Huella dactilar del ser humano

Un lector de huella digital lleva a cabo dos tareas:

- Obtener una imagen de la huella digital.
- Comparar un patrón de valles y crestas de dicha imagen con los patrones de las huellas que tiene almacenadas.

Los dos métodos principales de obtener una imagen de una huella digital son por lectura óptica o lectura de capacitancia.

Lectores ópticos

Un lector óptico funciona con un dispositivo CCD, como el usado en las cámaras digitales, que tienen un arreglo de diodos sensibles a la luz que genera una señal eléctrica en respuesta a la luz. Cada diodo graba un píxel, un pequeño punto que representa la luz que le es reflejada. Colectivamente, la luz y perfiles oscuros forman una imagen de la huella leída. El proceso de lectura comienza cuando el usuario pone su dedo sobre la ventana del lector, el cual tiene su propia fuente de iluminación, típicamente un arreglo de LED´s, para iluminar las crestas de la huella digital. El CCD genera, de hecho, una imagen invertida del dedo, con áreas más oscuras que representan más luz reflejada (las crestas del dedo) y las áreas más claras que representan menos luz reflejada (los valles entre las crestas).

Antes de comparar la información obtenida con la almacenada, el procesador del lector se asegura de que el CCD ha capturado una imagen clara. Verifica la oscuridad promedio de los píxeles, o los valores generales en una pequeña muestra, y rechaza la lectura si la imagen general es demasiado oscura o demasiado clara. Si la imagen es rechazada, el lector ajusta el tiempo de exposición para dejar entrar más o menos luz, e intentará leer la huella de nuevo.

Si el nivel de luz es adecuado, el lector revisa la definición de la imagen (que tan precisa es la imagen obtenida). El procesador busca varias líneas rectas que se mueven horizontal y verticalmente sobre la imagen, y si esta tiene buena definición,

una línea que corre perpendicular a las crestas será hecha de secciones alternantes de píxeles muy claros y muy oscuros.

Lectores de capacitancia

Como los lectores ópticos, los lectores capacitivos de huella digital generan una imagen de las crestas y valles que conforman una huella digital, pero en vez de hacerlo con luz, los capacitores utilizan corriente eléctrica.

El diagrama de la figura 1.5.2 muestra un ejemplo de sensor capacitivo. El sensor está hecho de uno o más chips que contienen un arreglo de pequeñas celdas. Cada celda incluye dos placas conductoras, cubiertas con una capa aislante.

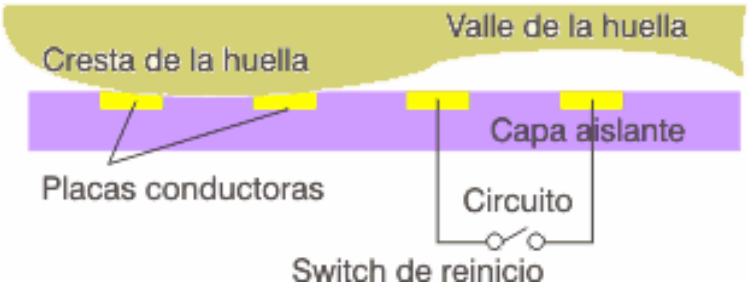


Figura 1.5.2. Diagrama en corte transversal del funcionamiento del lector de huellas digitales mediante placas capacitivas

Las celdas son más pequeñas que el ancho de una cresta del dedo. El sensor es conectado a un integrador, un circuito eléctrico construido sobre la base de un amplificador operacional inversor que altera un flujo de corriente. La alteración se basa en el voltaje relativo de dos fuentes, llamado la terminal inversora y la terminal no-inversora. En este caso, la terminal no-inversora es conectada a tierra, y la terminal inversora es conectada a una fuente de voltaje de referencia y un bucle de retroalimentación que incluye las dos placas conductoras, que funcionan como un capacitor, esto es, un componente que puede almacenar una carga eléctrica. La superficie del dedo actúa como una tercera placa capacitora, separada por las capas aislantes en la estructura de la celda y, en el caso de los valles de la huella, una bolsa de aire.

Al variar la distancia entre las placas capacitoras (moviendo el dedo más cerca o más lejos de las placas conductoras), se cambia la capacitancia (o habilidad para almacenar una carga) total del capacitor. Gracias a esta cualidad, el capacitor en una celda bajo una cresta tendrá una capacitancia más grande que el capacitor en una celda bajo un valle. Ya que la distancia al dedo altera la capacitancia, la cresta de un dedo resultará en una salida de voltaje diferente a la del valle de un dedo.

El procesador del lector toma esta salida de voltaje y determina si es característico de una cresta o un valle. Al leer cada celda en el arreglo de sensores, el procesador puede construir una imagen de la huella, similar a la imagen capturada por un lector óptico.

La principal ventaja de un lector capacitivo es que requiere una verdadera forma de huella digital y no sólo un patrón de luz y oscuridad que haga la impresión visual de una huella digital. Esto hace que el sistema sea más difícil de engañar. Adicionalmente, al usar un chip semiconductor en vez de una unidad CCD, los lectores capacitivos tienden a ser más compactos que los ópticos (figura 1.5.3).

Figura 1.5.3. Ejemplo de un lector capacitivo

Análisis

Empalmar las imágenes de huellas digitales para encontrar una que corresponda no es un modo práctico para comparar las huellas dactilares. Una imagen borrosa puede hacer que dos imágenes de la misma huella se vean bastante diferentes, así

que raramente se podrá obtener un empalme perfecto. Adicionalmente, utilizar la imagen completa de la huella digital en un análisis comparativo utiliza muchos recursos del procesador, y además hace más sencillo robar los datos impresos de la huella de alguien.

En vez de esto, la mayoría de los lectores compara rasgos específicos de la huella digital, generalmente conocidos como minucias (figura 1.5.4). Típicamente, los investigadores humanos y computadoras se concentran en puntos donde las líneas de las crestas terminan o donde se separan en dos (bifurcaciones).

El software del sistema del lector utiliza algoritmos complejos para reconocer y analizar estas minucias. La idea básica es medir las posiciones relativas de la minucias. Una manera simple de pensar en esto es considerar las figuras que varias minucias forman cuando dibuja líneas rectas entre ellas. Si dos imágenes tienen tres terminaciones de crestas y dos bifurcaciones formando la misma figura dentro de la misma dimensión, hay una gran probabilidad de que sean de la misma persona.

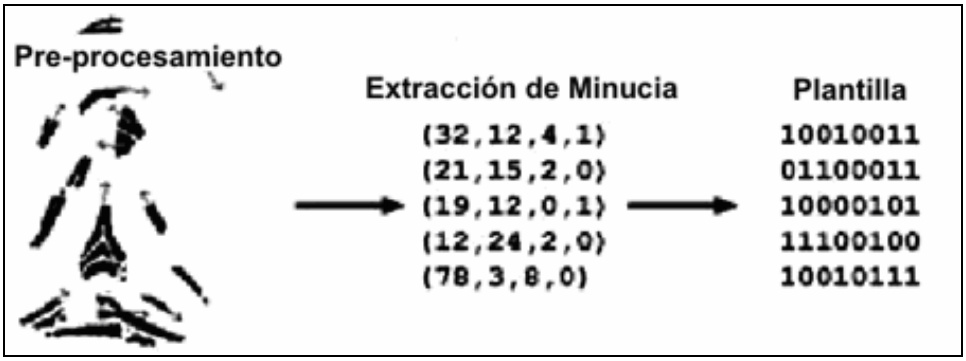


Figura 1.5.4. Proceso de conversión de del huella a información binaria

Principales ventajas

Incorporar esta tecnología a los sistemas de información es relativamente sencillo ya que aumenta significativamente la seguridad y el control de accesos a sistemas e información.

Las principales aplicaciones en las empresas a estos sistemas de acceso se encuentran en:

- Autorización de pagos y transacciones.
- Consulta de información confidencial.
- Kioscos interactivos / Autoservicio.
- Programas de lealtad y beneficios al cliente.
- Registro y acceso de personal.

En el sector gobierno los beneficios son también significativos, ya que se puede controlar de una manera más eficiente y segura la función pública mediante sistemas de validación de personal y encuentra aplicaciones en:

- Administración y procuración de Justicia.
- Otorgamiento de servicios a beneficiarios de programas sociales.
- Control de salubridad y registros de salud pública.
- Educación pública.

Las ventajas de un sistema biométrico de huella digital son que los atributos físicos de una persona suelen ser difíciles de falsificar, uno no puede adivinar una huella digital como adivina una contraseña, no puede perder sus huellas digitales como pierde una llave y no puede olvidar sus huellas digitales como puede olvidar una tarjeta.

Para hacer los sistemas de seguridad más confiables, es una buena idea combinar el análisis biométrico con un medio convencional de identificación, como una contraseña o una tarjeta. Muchas empresas en electrónica ofrecen lectores de huella que además pueden verificar una tarjeta inteligente o una tarjeta *mifare* (tarjeta inteligente sin contacto) en donde se almacene la huella digital del usuario. El lector coteja que la huella codificada en la tarjeta sea la misma que se está poniendo sobre el lector, proporcionando un grado mayor de seguridad y eliminando

las limitaciones de espacio de almacenamiento de huellas en un servidor, pues se pueden emitir credenciales con huellas codificadas de manera infinita.

Desventajas del dispositivo lector de huellas dactilares

Como todo dispositivo creado por el hombre, no es infalible a errores, ya que puede ser fácil alterar una huella digital, basta con tan sólo oprimir y deslizar la huella digital en una superficie rugosa para alterar la posición de los surcos, para que la huella pueda no ser reconocida, pero no hay que olvidar que el propósito es el reconocer y no la de engañar al sistema. En conclusión, existen dos vertientes para hacer la aplicación: la de validación y la del engaño. Otra desventaja para el reconocimiento de la huella lo es el alterar la huella en forma accidental, ya que cualquier lesión o cicatriz o suciedad sobre la huella como lo puede ser la pintura, pegamento o suciedad sobre la huella, esto puede también evitar su detección exacta, otro factor que hay que considerar para el desarrollo del proyecto es que el sistema debe de permitir cierto grado de accesibilidad a claves en el caso de no reconocer la huella.

También el uso continuo de este dispositivo ocasiona que se ensucie, por lo que hay que limpiarlo constantemente con un paño suave, además de considerar que el equipo se debe de cuidar de no sufrir alteraciones en su superficie captora ya que se puede rallar o romper con un impacto accidental.

Capítulo 2

Marco teórico

2.1 CONCEPTOS BÁSICOS DE BASES DE DATOS RELACIÓNALES

Bases de datos

Una base de datos es un conjunto exhaustivo no redundante de datos estructurados y organizados independientemente de su utilización, y su implementación en máquina es accesible en tiempo real y compatible con usuarios concurrentes con necesidad de información diferente y no predicable en tiempo.

Las bases de datos proporcionan la infraestructura requerida para los sistemas de apoyo a la toma de decisiones y para los sistemas de información estratégicos, ya que estos sistemas explotan la información contenida en las bases de datos de la organización para lograr ventajas competitivas. Por este motivo es importante conocer la forma en que están estructuradas las bases de datos y su manejo.

Requerimientos de las bases de datos

El análisis de requerimientos para una base de datos incorpora las mismas tareas que el análisis de requerimientos del software. Es necesario un contacto estrecho con el cliente; es esencial la identificación de las funciones e interfaces; se requiere la especificación del flujo, estructura y asociatividad de la información y debe desarrollarse un documento formal de los requerimientos.

Elementos claves de organización en un ambiente de Bases de Datos:

- Sistema de administración de base de datos.
- Administración de información.
- Tecnología de administración de base de datos.
- Usuarios.
- Planeación de información y tecnología de modelado.

Características de las bases de datos

Una base de datos contiene entidades de información que están relacionadas vía organización y asociación. La arquitectura lógica de una base de datos se define mediante un esquema que representa las definiciones de las relaciones entre las entidades de información. La arquitectura física de una base de datos depende de la configuración del hardware residente. Sin embargo, tanto el esquema (descripción lógica) como la organización (descripción física) deben adecuarse para satisfacer los requerimientos funcionales y de comportamiento para el acceso al análisis y creación de informes.

Ventajas en el uso de bases de datos

La utilización de bases de datos como plataforma para el desarrollo de Sistemas de Aplicación en las organizaciones se ha incrementado notablemente en los últimos años, se debe a las ventajas que ofrece su utilización, algunas de las cuales se comentarán a continuación:

- Globalización de la información: permite a los usuarios considerar la información como un recurso corporativo que carece de dueños específicos.
- Eliminación de información inconsistente: si existen dos o más archivos con la misma información, los cambios que se hagan a éstos deberán hacerse a todas las copias del archivo.
- Permite compartir información.
- Permite mantener la integridad en la información: la integridad de la información es una de sus cualidades altamente deseable y tiene por objetivo que sólo se almacena la información correcta.

- Independencia de datos: el concepto de independencia de datos es quizás el que más ha ayudado a la rápida proliferación del desarrollo de sistemas de bases de datos. La independencia de datos implica un divorcio entre programas y datos.
- Evita la redundancia: en la actualidad la redundancia no parece ser un elemento muy preocupante para los diseñadores de base de datos, pero en tiempos en donde el almacenamiento y el procesamiento de la información era mas costosa y limitada era una regla de suma importancia eliminarla, y ha quedado como un buen habito al momento de diseñar las base de datos.

Modelo de datos Relacional

El Modelo de Datos Relacional organiza y presenta los datos en forma de relaciones. El término de relación es un concepto matemático y representa lo que se podría llamar una tabla de dos dimensiones consistente en columnas y renglones. El modelo relacional se divide en tres partes, las cuales se ocupan de la estructura, la integridad y la manipulación de los datos.

ESTRUCTURA DE DATOS RELACIONAL

Dominio

Los valores escalares representan la menor unidad semántica de la información en el sentido que son atómicos; no poseen estructura interna (es decir no se pueden descomponer). Cabe subrayar que la carencia de estructura interna desde el punto de vista del modelo no implica la falta de estructura interna en términos absolutos.

Se puede definir a un dominio como: Un conjunto de valores escalares, todos del mismo tipo, de los cuales uno o más atributos obtienen sus valores reales.

Relación

Una relación (R) sobre un conjunto de dominios D1, D2, ..., Dn (no necesariamente distintos), se compone de dos partes, una cabecera y un cuerpo.

La cabecera está formada por un conjunto fijo de atributos o, en términos más precisos, de pares de atributo-dominio.

$$\{ (A1:D1),(A2:D2),...,(An:Dn) \}$$

Tales que cada atributo Aj corresponde a uno y sólo uno de los dominios subyacentes Dj(j=1,2, ... n).

El cuerpo está formado por un conjunto de tuplas[1], el cual varía con el tiempo. Cada tupla a su vez está formada por un conjunto de parejas atributo-valor.

$$\{ (A1:vi1), (A2:vi2),...,(An:vin) \} / (i = 1,2 ... m)$$

Donde m es el número de tuplas del conjunto. En cada una de estas tuplas hay uno de estos pares atributo-valor (Aj:vij) para cada atributo Aj de la cabecera. Para cada par atributo-valor (Aj:vij), vij es un valor del dominio único Dj asociado al atributo Aj.

Los valores m y n se llaman cardínalidad y grado, respectivamente, de la relación R. La cardínalidad varía con el tiempo, pero el grado no.

Propiedades de las relaciones

Las relaciones poseen ciertas propiedades, las cuales son:

- No existen tuplas repetidas.
- Las tuplas no están ordenadas (de arriba hacia abajo).
- Los atributos no están ordenados (de izquierda a derecha).
- Todos los valores de los atributos son atómicas.

Todas ellas consecuencia inmediata de la definición formal de relación, y todas ellas muy importantes, estas propiedades se explican a continuación:

[1] Una tupla es una fila de una relación.

- No existen tuplas repetidas.

  Esta propiedad es consecuencia del hecho de que el cuerpo de la relación es un conjunto matemático (es decir, un conjunto de tuplas), en matemáticas los conjuntos por definición no incluyen elementos repetidos.

- Las tuplas no están ordenadas.

  Esta propiedad también se desprende del hecho de que el cuerpo de una relación es un conjunto matemático. Los conjuntos en matemáticas no son ordenados. Esta propiedad servirá también para ilustrar la diferencia entre una relación y una tabla, porque las filas de una tabla tienen un orden obvio de arriba hacia abajo, en tanto que las tuplas de la relación carecen de tal orden.

- Los atributos no están ordenados.

  Esta propiedad se desprende del hecho de que la cabecera de la relación se define también como conjunto (es decir, un conjunto de atributos, dicho en forma más precisa, de pares atributo-dominio). Esta cuestión de ordenamiento de los atributos es otra área en la cual la representación concreta de una relación en forma de tabla sugiere algo que no se cumple en realidad: las columnas de una tabla tienen un orden evidente de izquierda a derecha pero los atributos de una relación carecen de tal orden.

- Todos los valores de los atributos son atómicos.

  Una forma más precisa de expresar esta última propiedad es: “todos los valores de los atributos simples son atómicos”. Se trata desde luego, de una consecuencia del hecho de que todos los dominios subyacentes son a su vez simples: es decir, contienen sólo valores atómicos (aún si existen atributos compuestos, esto no son sino una simple concatenación de atributos simples); en resumen las relaciones no contienen grupos repetitivos.

Tipos de relaciones

A continuación se presentan brevemente los tipos de relaciones que puede contener un sistema relacional.

- Relaciones Base.

  Las relaciones base son aquellas cuya importancia (para la aplicación en cuestión) es tal que el diseñador de la base de datos les da un nombre y las hace parte directa de la base de datos en si, a diferencia de otras relaciones cuya naturaleza es más efímera, como por ejemplo el resultado de una consulta.

- Vistas.

  Son también llamadas relaciones virtuales, una vista es una relación derivada, con nombre, representada dentro del sistema exclusivamente mediante su definición en términos de otras relaciones con nombre: no posee datos almacenados propios, separados y distinguibles (a diferencia de las relaciones base).

- Instantáneas.

  Una instantánea es también una relación derivada, con nombre, como una vista. Pero a diferencia de las vistas, las instantáneas son reales, no virtuales; es decir, están representadas no sólo por su definición en términos de otras relaciones con nombre, sino también por sus propios datos almacenados.

- Resultados intermedios.

  Un resultado intermedio es una relación (casi siempre sin nombre) resultante de alguna expresión relación anidada dentro de alguna otra expresión relacional más grande.

- Relaciones temporales.

  Es una relación temporal es una relación con nombre, similar a una relación base o vista o instantánea, pero (a diferencia de éstas tres últimas) se destruye en forma automática en algún momento apropiado. Las relaciones base, vistas e instantáneas, en cambio son más permanentes, en cuanto a que sólo se destruyen como resultado de alguna acción explícita del usuario.

Reglas de integridad relacional

El modelo relacional incluye dos reglas generales de integridad en el sentido de que se aplican no sólo a una base de datos específica, sino más bien a todas las bases de datos (o por lo menos a todas las bases de datos que digan apegarse al modelo). Estas dos reglas generales se refieren, respectivamente, a las claves primarias y a las claves ajenas.

Claves primarias

Primero es necesario definir el término de clave candidata de la siguiente manera. El atributo K (posiblemente compuesto) de la relación R es una clave candidata de R si y sólo si satisface las siguientes dos propiedades, independientes del tiempo:

- Unicidad: En cualquier momento dado, no existen dos tuplas en R con el mismo valor de K.
- Minimalidad: Si K es compuesto, no será posible eliminar ningún componente de K sin destruir la propiedad de unicidad.

Es importante señalar que toda relación tiene por lo menos una clave candidata, porque las relaciones no contienen tuplas repetidas. En la práctica, las relaciones tienden a tener una y sólo una clave candidata, pero sin duda es posible que tengan más. Del conjunto de claves candidatas de una relación dada, se elige una y sólo una como clave primaria de esa relación; las demás, si existen, se llamarán claves alternativas. Así, una clave alterna es una clave candidata que no es la clave primaria.

La importancia de las claves primarias radica principalmente en que constituyen el mecanismo de direccionamiento a nivel tupla básico en un sistema relacional. El único modo, garantizado por el sistema, de localizar alguna tupla específica es por el valor de su clave primaria. En consecuencia las claves primarias son tan indispensables para el funcionamiento exitoso de un sistema relacional como las direcciones de memoria principal lo son para el funcionamiento exitoso de la computadora. En términos informales: “Una clave primaria es un conjunto de

atributos que fueron designados para identificar plenamente a cada tupla de la relación, su característica principal es que no acepta en su conjunto valores duplicados".

Regla de Integridad de las entidades

Ningún componente de la clave primaria de una relación base puede aceptar nulos.

Regla de integridad referencial y claves ajenas

Un clave ajena es un atributo (quizá compuesto) de una relación R2 cuyos valores deben concordar con los de la clave primaria de alguna relación R1 (donde R1 y R2 no necesariamente son distintos).

Un valor de clave ajena representa una referencia a la tupla donde se encuentra el valor correspondiente de la clave primaria (la tupla referida o tupla objetivo). Por lo tanto, el problema de garantizar que la base de datos no incluya valores no válidos de una clave ajena se conoce como el problema de la integridad referencial. La restricción según la cual los valores de una clave ajena determinada deben concordar con los valores de la clave primaria correspondiente se conoce como restricción referencial. La relación que contiene a la clave ajena se conoce como relación referencial y la relación que contiene a la clave primaria correspondiente se denomina relación referida o relación objetivo.

Se puede definir a la clave ajena de una manera más formal como:

- Una clave ajena dada y la clave primaria correspondiente deben definirse sobre el mismo dominio (el cual puede ser compuesto).
- La clave ajena no necesita ser un componente de la clave primaria de la relación que la confine, de hecho cualquier atributo (en una relación base) puede ser una clave ajena.
- Una relación dada puede ser desde luego tanto una relación referida como una relación referencial.

- Una relación podría incluir una clave ajena cuyos valores (no nulos) deben concordar con los valores de la clave primaria de esa misma relación, a este tipo especial de relaciones se les denomina relaciones auto referenciales.
- Las claves ajenas, a diferencia de la claves primarias (en relaciones base), deben aceptar nulos en ocasiones.
- Las concordancias de la clave ajena con la clave primaria representan ciertas interrelaciones entre las tuplas.

Por lo que la regla de la integridad referencial se puede resumir como sigue: La base de datos no debe contener valores de clave ajena sin concordancia.

El término “valores de clave ajena sin concordancia” se refiere a valores no nulos de la clave ajena para el cual no existe un valor concordante de la clave primaria en la relación objetivo pertinente.

Cardinalidad

La forma en la cual se relacionan las entidades tienen reglas en el modelo entidad relación, este recibe el nombre de cardinalidad y las relaciones se describen de la siguiente forma:

- Relación Uno a Uno.

  Cuando un registro de una tabla está relacionado con un único registro de la otra tabla y viceversa.
- Relación Uno a Muchos.

  Cuando un registro de una tabla (tabla secundaria) sólo puede estar relacionado con un único registro de la otra tabla (tabla principal) y un registro de la otra tabla (tabla principal) puede tener más de un registro relacionado en la primera tabla (tabla secundaria).
- Relación Muchos a Muchos.

  Cuando un registro de una tabla puede estar relacionado con más de un registro de la otra tabla y viceversa.

Álgebra Relacional

La tercera y última parte del modelo relacional, la parte manipulativa, se divide en dos partes:

- Un conjunto de operadores, como los de reunión que forman en conjunto la llamada álgebra relacional.
- Una operación de asignación (por ejemplo, C:= A reunión B) que asigna el valor de alguna expresión arbitraria del álgebra a una relación nombrada.

El álgebra relacional consiste en un conjunto de operadores de alto nivel que operen sobre relaciones. Cada uno de estos operadores toma una o dos relaciones como entrada y produce una nueva relación como salida.

Codd[2] definió un conjunto muy específico de ocho operadores de este tipo, en dos grupos de cuatro cada uno:

- Las operaciones tradicionales de conjuntos unión, intersección, diferencia y producto cartesiano (todas estas con ligeras modificaciones debidas al hecho de tener relaciones con operandos, y no conjuntos arbitrarios; después de todo, una relación es un tipo especial de conjunto).
- Las operaciones relacionales especiales restricción, proyección, reunión y división.

A continuación se explica brevemente cada uno de estos operadores:

- Restricción o Selección.

  Extrae las tuplas especificas de una relación dada (es decir, restringe la relación solo a las tuplas que satisfagan una condición específica).
- Proyección.

  Extrae los atributos específicos de una relación dada.
- Producto.

[2] Edgar Frank Codd. Científico informático inglés (1923 - 2003), conocido por sus aportes a la teoría de bases de datos relacionales.

A partir de dos relaciones especificas, construye una relación que contienen todas las combinaciones posibles de tuplas, una de cada una de las dos relaciones.

- Unión.

  Constituye una relación formada por todas las tuplas que aparecen en cualquiera de las relaciones específicas.

- Intersección.

  Constituye una relación formada por todas las tuplas que aparecen en las dos relaciones específicas.

- Diferencia.

  Constituye una relación formada por todas las tuplas de la primera relación que no aparezca en la segunda de las dos relaciones especificadas.

- Reunión.

  A partir de dos relaciones especificadas, construye una relación que contiene todas las posibles combinaciones de tuplas, una de cada una de las dos relaciones, tales que las dos tuplas participantes en una combinación dada satisfaga alguna condición especificada.

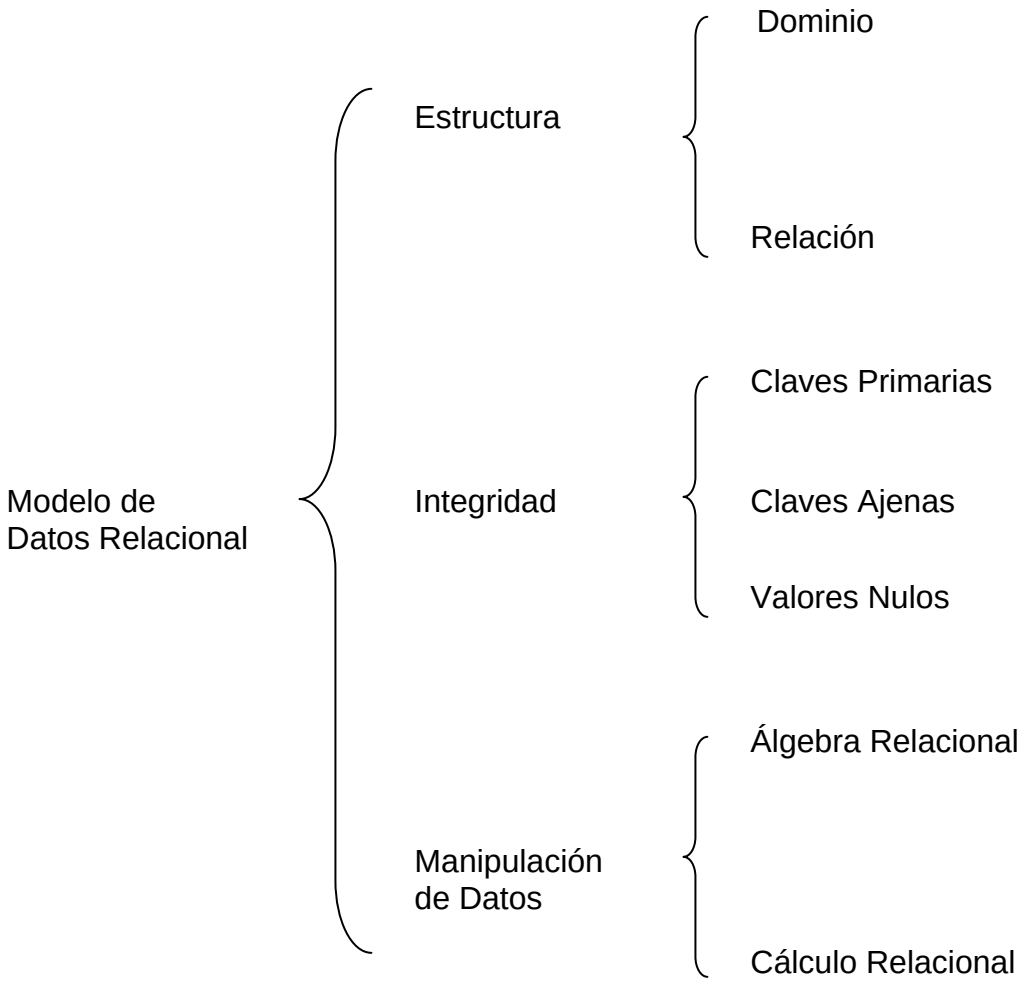
- División.

  Toma dos relaciones, una binaria y otra unaria, y construye una relación formada por todos los valores de un atributo de la relación binaria que concuerdan (en otro atributo) con todos los valores de la relación unaria. El propósito de la operación de asignación es el de poder recordar el valor de alguna expresión algebraica, y así modificar el estado de la base de datos.

Cálculo relacional

El álgebra relacional y el cálculo relacional son dos alternativas para establecer una base formal de la parte manipulativa del modelo. La diferencia entre ellas es la siguiente: mientras que el álgebra ofrece un conjunto de operaciones explicitas reunión, unión, proyección que pueden servir en la práctica para indicar al sistema la forma de construir alguna relación deseada a partir de la relaciones dadas en la

base de datos, el cálculo sólo ofrece una notación para formular la definición de esa relación deseada en términos de esas relaciones dadas.



Diseño de bases de datos relacionales

El problema de diseñar una base de datos se puede expresar de manera muy sencilla: dado algún conjunto de datos que se deben representar en una base de datos, ¿cómo decidir cuál es la estructura lógica adecuada paras esos datos? En otras palabras, ¿cómo decidir cuáles relaciones deberán existir y qué atributos deberán tener?

En este punto es de mayor interés el problema del diseño lógico, no el de diseño físico. Ahora bien, no se intenta sugerir con este comentario que el diseño físico carece de importancia; todo lo contrario, el diseño físico es muy importante.

El presente capítulo se tratará lo que podría llamarse diseño independiente de las aplicaciones. Dicho de otro modo, se tratará de diseñar el esquema conceptual; es decir; producir un diseño lógico abstracto independiente del equipo, independiente del sistema operativo, independiente lo mayor posible del DBMS (Database Management System - Sistema de Administración de Bases de Datos) independiente del lenguaje.

Modelo Entidad-Relación (E-R)

El modelo Entidad-Relación surge como una herramienta para el diseño de bases de datos, el cual esta basado en el Modelo Relacional pero con mayor riqueza semántica que permite una mejor comunicación entre los analistas, diseñadores y usuarios finales durante las fases de análisis de requerimientos y de diseño conceptual debido a que es simple y fácil de entender, Además de incorporar una sintaxis gráfica.

Normalización

La normalización es un proceso que consiste en comprobar que las tablas definidas (también denominadas relaciones en terminología propia del modelo relacional de datos) cumplen unas determinadas condiciones. Se pretende garantizar la no existencia de redundancia y una cierta coherencia en la representación mediante un esquema relacional de las entidades y relaciones del modelo conceptual (diagrama Entidad-Relación). Mediante la normalización se pueden solucionar diversos errores en el diseño de la base de datos así como mejorarlo. También se facilita el trabajo posterior del administrador de la base de datos y de los desarrolladores de aplicaciones.

La normalización es un proceso que permite reemplazar relaciones entre datos. Las tablas deben organizarse de forma tal que no se pierda ninguna de las relaciones existentes entre los datos, las tablas en cuestión son matrices rectangulares que pueden ser discretas matemáticamente y cuyas características son:

- La normalización permite eliminar la duplicidad de la información de las tablas.
- Cada entrada de las tablas se representan por un ítem de datos; no hay grupos repetitivos.
- Son homogéneas por columna: es decir, todo los ítems de una columna son de la misma clase.
- Cada columna tiene nombre propio.
- Todas las filas son diferentes; no se admiten filas duplicadas.
- Tanto las filas como las columnas pueden considerarse en cualquier secuencia y en cualquier momento, sin afectar por ello ni el contenido de la información ni la semántica de cualquier función que utilicen las tablas.

Para que se lleve acabo cada uno de los puntos anteriores es necesario la aplicación de la primera, segunda y tercera forma normal respectivamente.

Primera forma normal

Para que la primera forma se lleve acabo en el Sistema de Recuperación de Información a través de Huella Dactilares es necesario lo siguiente:

- Eliminar datos repetidos en tablas individuales.
- Así mismo crear una tabla separada para cada grupo de datos relacionados.
- Relacionar a los usuarios que tienen como atributo la llave primaria.

Esta forma normal está justificada por su sencillez y la estética. Consiste simplemente en evitar los dominios compuestos de varios valores. Para evitar la duplicidad de información es necesario aplicar la segunda forma normal.

Segunda forma normal

Para el desarrollo de esta forma normal en las tablas del sistema, esto asegurará la eliminación de algunas redundancias, garantizando que ningún atributo venga determinado solamente por una parte de la clave.

Tercera forma normal

Para la tercera forma normal que permite asegurar la eliminación de las redundancias debidas a las dependencias transitivas de las tablas. De esta forma normal se determinan las columnas que son dependientes de otras columnas no llave. Además se eliminan esas columnas de la tabla base.

Una vez realizada la normalización, se completa la creación de las tablas con los campos adicionales que se requiera para cada una de ellas de acuerdo con la información que se almacenará en el sistema.

2.2 CARACTERÍSTICAS, VENTAJAS Y DESVENTAJAS DE SQL SERVER 2000

Microsoft SQL Server 2000 es un sistema de administración de bases de datos (DBMS), cuyo componente principal es una base de datos relacional, escalable, basada en SQL (Structured Query Language - Lenguaje de Consulta Estructurado) con compatibilidad de XML (Extensible Markup Language - Lenguaje de Marcado Extensible) integrada para aplicaciones de Internet. Cada uno de estos términos describe una parte fundamental de la arquitectura del componente de base de datos de SQL Server 2000.

Base de Datos

Una instancia de SQL Server 2000 incluye los archivos que crean un conjunto de bases de datos y una copia del software DBMS. Las aplicaciones que se ejecutan en equipos diferentes utilizan un componente de comunicaciones de SQL Server 2000 para transmitir comandos a través de una red a la instancia de SQL Server.

Cada instancia de SQL Server tiene cuatro bases de datos de sistema (master, model, tempdb y msdb) y una o varias bases de datos de usuario (figura 2.2.1).

Una instancia de SQL Server es capaz de controlar el trabajo de miles de usuarios sobre varias bases de datos al mismo tiempo. Cada instancia de SQL Server deja disponibles todas las bases de datos para todos los usuarios que se conecten, de acuerdo con los permisos de seguridad definidos.

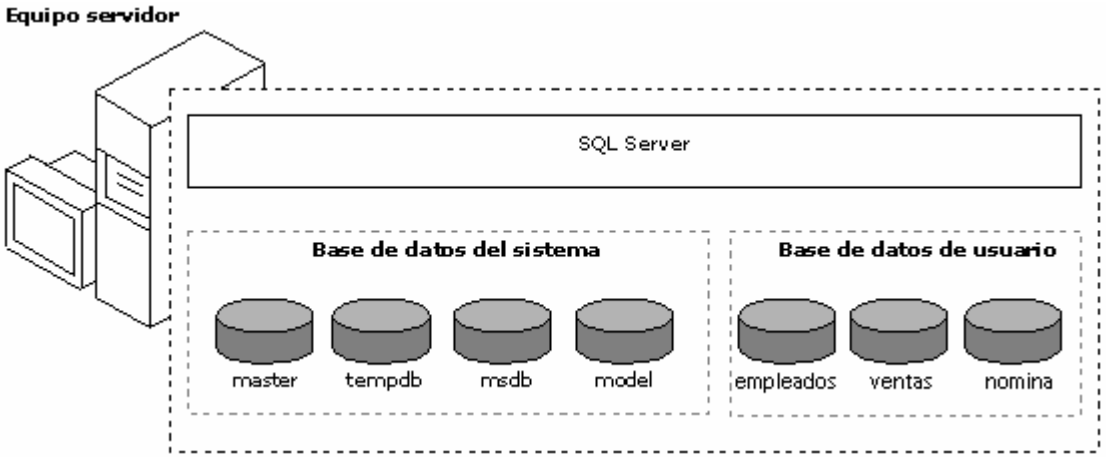


Figura 2.2.1. Bases de datos en SQL Server 2000

Escalabilidad

SQL Server 2000 está diseñado para funcionar como motor de almacenamiento de datos para miles de usuarios que se conectan a través de una red simultáneamente, puede funcionar también como base de datos independiente directamente en el mismo equipo de una aplicación.

Las características de escalabilidad y facilidad de uso de SQL Server le permiten trabajar eficazmente en un único equipo sin consumir demasiados recursos y sin que sean necesarias tareas administrativas por parte del usuario independiente. Las mismas características permiten al manejador de bases de datos adquirir de forma dinámica los recursos necesarios para admitir miles de usuarios, al tiempo que minimizan la administración y la optimización de bases de datos.

Lenguaje de consulta estructurado

Para trabajar con los datos de una base de datos, se debe utilizar un conjunto de comandos e instrucciones (lenguaje) definidos por el software del DBMS, siendo el más común SQL.

SQL Server 2000 admite el nivel de entrada de SQL-92, el estándar de SQL publicado por ANSI (American National Standards Institute - Instituto Nacional Americano de Normalización) e ISO (International Standards Organization - Organización Internacional de Normalización) en 1992. El dialecto de SQL compatible con SQL Server se llama Transact-SQL (T-SQL). T-SQL es el lenguaje principal utilizado por las aplicaciones de SQL Server 2000.

Lenguaje de marcado extensible

XML es el estándar de Internet emergente para datos. XML es un conjunto de etiquetas que se utilizan para definir la estructura de un documento de hipertexto. El lenguaje de marcado de hipertexto, que es el lenguaje más importante para visualizar páginas Web, puede procesar fácilmente los documentos XML.

Aunque la mayoría de las instrucciones SQL devuelven los resultados en un conjunto de resultados relacional, o tabular, el componente de base de datos de SQL Server 2000 admite una cláusula FOR de XML que devuelve los resultados como documento XML. También admite consultas XPath de aplicaciones de Internet e intranet. Los documentos XML se pueden agregar a las bases de datos de SQL Server y la cláusula OPENXML se puede utilizar para exponer los datos de un documento XML como un conjunto de resultados relacional.

Administración

La administración de SQL Server tiene las siguientes características:

- El servidor de base de datos SQL Server 2000 reduce el trabajo de administración en muchos entornos al adquirir y liberar recursos de forma dinámica. El servidor adquiere automáticamente recursos del sistema como

memoria y espacio de disco cuando lo necesita, y libera los recursos cuando ya no los necesita.

- Proporciona un conjunto de herramientas gráficas que permiten realizar tareas administrativas de forma sencilla y eficiente.
- Proporciona un conjunto de servicios que permiten a los administradores programar la ejecución automática de tareas repetitivas.

Almacenamiento de datos

Microsoft SQL Server 2000 permite manejar bases de datos de tipo OLAP (On-Line Analytical Processing - Procesamiento Analítico en Línea) y OLTP (On-Line Transaction Processing - Procesamiento Transaccional en Línea).

Sistemas OLAP

La tecnología OLAP permite un uso más eficaz de los almacenes de datos para el análisis en línea, lo que proporciona respuestas rápidas a consultas analíticas complejas e iterativas. Los modelos de datos multidimensionales de OLAP y las técnicas de agregados de datos organizan y resumen grandes cantidades de datos para que puedan ser evaluados con rapidez mediante el análisis en línea.

Sistemas OLTP

Los sistemas OLTP están diseñados y ajustados para procesar cientos o miles de transacciones que se introducen al mismo tiempo. Los datos son generalmente organizados en tablas relacionales para evitar redundancia e incrementar la velocidad de las actualizaciones.

Especificaciones de capacidad máxima

En la tabla 2.2.1 se especifica los tamaños y cantidades máximas de varios objetos que se definen en las bases de datos de SQL Server 2000 o a los que se hace referencia en instrucciones Transact-SQL.

Objeto	Tamaños y cantidades máximas
Bytes por clave externa	900
Bytes por clave principal	900
Bytes por fila	8,060
Índices agrupados por tabla	1
Columnas por índice	16
Columnas por clave externa	16
Columnas por clave principal	16
Columnas por tabla base	1,024
Columnas por instrucción SELECT	4,096
Columnas por instrucción INSERT	1,024
Conexiones por cliente	Valor máximo de conexiones configuradas
Tamaño de la base de datos	1,048,516 TB
Bases de datos por instancia de SQL Server	32,767
Archivos por base de datos	32,767
Tamaño de archivo (datos)	32 TB
Referencias a tabla de claves externas por tabla	253
Instancias por equipo	16
Objetos en una base de datos	2,147,483,647
Parámetros por procedimiento almacenado	1,024
Filas por tabla	Limitado por el espacio de almacenamiento disponible
Tablas por base de datos	Limitado por el número de objetos de la base de datos

Tabla 2.2.1. Especificaciones de capacidad máxima en SQL Server 2000

Ventajas

- Los datos en SQL Server 2000 pueden ser automáticamente exportados a otros sistemas independientes (Oracle, Sybase, Access, etc.).
- Facilidad de instalación y utilización.
- Compatibilidad con XML.
- Escalabilidad y disponibilidad.
- Bajo costo en comparación con otros productos (como Informix).
- Integración con Internet.
- Soporta Auto-configuración.

Desventajas

- SQL Server es dependiente de la plataforma Windows.
- No permite elaborar formas de edición de datos, reportes, menús de opciones, etc.

2.3 CARACTERÍSTICAS, VENTAJAS Y DESVENTAJAS DE VISUAL BASIC .NET

Visual Basic .NET forma parte de Visual Studio .Net, antes de mencionar las características de Visual Basic .NET, se explicará lo que es Visual Studio .NET. Visual Studio .NET es un conjunto de herramientas integrado para la construcción y desarrollo de aplicaciones, es un IDE (Integrated Development Environment - Entorno Integrado de Desarrollo) que se puede utilizar para:

- Crear aplicaciones basadas en Windows.
- Crear aplicaciones para Pocket PC.
- Crear aplicaciones Web sofisticadas.
- Crear aplicaciones Web inteligentes para dispositivos móviles.
- Utilizar servicios Web XML.
- Evitar conflictos entre archivos DLL (Dynamic Link Library - Biblioteca de Enlaces Dinámicos).

- Eliminar problemas de implementación y mantenimiento de las aplicaciones.

Visual Studio .NET es un entorno de desarrollo creado para permitir la integración con servicios Web XML. Al hacer posible que las aplicaciones compartan datos a través de Internet, los servicios Web XML permiten a los programadores ensamblar aplicaciones a partir de código nuevo y existente, independientemente de la plataforma, el lenguaje de programación o el modelo de objetos.

También incluye un depurador unificado, con el cual se pueden depurar aplicaciones de distintos lenguajes, aunque se ejecuten en equipos locales o remotos. Por último, independientemente del lenguaje utilizado, Microsoft .NET Framework ofrece una amplia gama de API (Application Programming Interface - Interfaz de Programación de Aplicaciones) para Microsoft Windows e Internet.

Visual Basic .NET es un lenguaje de programación orientado a objetos con cualidades similares a C++, se pueden crear clases en Visual Basic .NET derivándolas de otras, ya estén escritas en Visual Basic o bien otros lenguajes .NET, como C#, es decir, admite la herencia de implementación. El diseñador de formularios admite la herencia visual y contiene nuevas características, como el ajuste de tamaño automático de los formularios, localización de recursos y soporte de accesibilidad. Es un lenguaje que tiene la capacidad de sobrecargar métodos, de tal forma que pueden existir múltiples versiones de un mismo método. También cuenta con un control estructurado de excepciones y una mayor consistencia en los tipos de datos.

Las herramientas de datos admiten de forma intrínseca datos XML y se puede trabajar con el enlace de datos en tiempo de diseño con los datos desconectados. Además, Visual Basic .NET se crea directamente en .NET Framework, para que el usuario pueda disponer de acceso completo a todas las características de la plataforma y permita la interoperabilidad con otros lenguajes .NET.

Visual Basic .NET dispone de dos paquetes de formularios (los formularios de Windows y los formularios Web), una nueva versión de ADO (ActiveX Data Objects - Objetos de Datos ActiveX) para obtener acceso a orígenes de datos desconectados y un lenguaje simplificado en el que se eliminan las palabras clave heredadas.

La herencia permite que el lenguaje Visual Basic sea compatible con la Programación Orientada a Objetos (POO). Por su parte, los formularios de Windows ofrecen, de forma nativa, gran accesibilidad y son compatibles con la herencia visual. Asimismo, la distribución de las aplicaciones se realiza de una forma tan simple como copiar archivos ejecutables y componentes de un directorio a otro.

Otra característica importante es que al abrir un proyecto de Visual Basic 6.0 en Visual Basic .NET, la actualización tiene lugar automáticamente: el asistente para la actualización muestra los pasos necesarios para actualizar el producto y crea un nuevo proyecto de Visual Basic .NET (sin modificar el proyecto existente). Es un proceso de sentido único, ya que el nuevo proyecto resultante de Visual Basic .NET no se podrá abrir en Visual Basic 6.0.

Para utilizar Visual Basic .NET 2003 Standard Edition, es preciso contar con algunos requisitos mínimos, los cuales se mencionan en la tabla 2.2.2.

Procesador	Computadora personal (PC) con un procesador Pentium II, 450 Megahertz (MHz)
Sistema Operativo	Windows XP Professional Windows 2000 Professional Windows 2000 Server Windows NT 4.0 Workstation Windows NT 4.0 Server

Memoria	**Windows XP Professional** 160 MB de RAM; se recomiendan 192 MB **Windows 2000 Professional** 96 MB de RAM; se recomiendan 128 MB **Windows 2000 Server** 192 MB de RAM; se recomiendan 256 MB **Windows NT 4.0 Workstation** 64 MB de RAM; se recomiendan 96 MB **Windows NT 4.0 Server** 160 MB de RAM; se recomiendan 192 MB
Disco Duro	500 MB en el disco de sistema, 2.0 gigabytes (GB) en el disco a instalarse
Unidad	CD-ROM o DVD-ROM
Video	Monitor Super VGA (800 x 600) o superior a 256 colores
Mouse	Mouse o dispositivo compatible

Tabla 2.2.2. Requisitos mínimos para instalar Visual Basic .NET

En Visual Basic .NET desaparecen las clases Web. Las aplicaciones que cuentan con clases Web se actualizarán a ASP .NET, sin embargo, una vez se haya realizado la actualización, será necesario realizar ciertas modificaciones. Las aplicaciones Web existentes pueden ínter operar con los formularios Web de Visual Basic .NET.

Visual Basic .NET ofrece una mayor compatibilidad para desarrollar componentes de servicios de componentes COM+ (Component Object Model - Modelo de Objetos basados en Componentes) y MTS (Microsoft Transaction Server - Servidor de Transacciones Microsoft) de nivel medio. El uso del depurador unificado permite ir de una aplicación cliente a un componente MTS/COM+ y viceversa. Asimismo, el depurador permite desplazarse por los distintos componentes MTS/COM+ de Visual Basic 6.0 (siempre que se encuentren compilados en código nativo, con información de depuración simbólica y sin optimizaciones).

2.4 SEGURIDAD DEL SISTEMA OPERATIVO ELEGIDO

SEGURIDAD EN WINDOWS XP

Windows XP ofrece características de seguridad que ayudan a proteger los datos confidenciales y proporcionan soporte para administrar los usuarios de la red. Una de las características más importantes es el uso de GPO (Group Policy Objects - Objetos de Directiva de Grupo). Con los GPO, los administradores del sistema pueden aplicar un mismo perfil de seguridad a varios equipos. Una característica más es el ACL (Access Control List - Lista de Control de Acceso).

Windows XP incluye plantillas de seguridad predefinidas que se pueden implementar sin modificaciones o utilizar como base para una configuración de seguridad más personalizada. Las empresas pueden aplicar las plantillas de seguridad en los siguientes casos:

- Cuando crean un recurso, como una carpeta o archivo compartido, y aceptan la configuración predeterminada de la lista de control de acceso o implementan una configuración predeterminada.
- Cuando colocan a usuarios en los grupos de seguridad estándar y aceptan la configuración predeterminada de la ACL que se aplica a dichos grupos de seguridad.
- Cuando utilizan las plantillas de directiva de grupo básica, compatible, segura o de alta seguridad que se incluyen en el sistema operativo.

Acceso controlado a la red

Cuenta con seguridad integrada para mantener alejados a los intrusos. Para ello, limita a todo el que intente tener acceso al equipo desde una red otorgándole privilegios de Invitado. Si un intruso prueba distintas contraseñas para entrar en el equipo y obtener privilegios no autorizados, sus intentos resultarán fallidos, o sólo conseguirá un acceso limitado a nivel de Invitado.

Administración de la autenticación de red

Para garantizar la seguridad de los equipos que se conectan directamente a Internet en lugar de a un dominio, el sistema exige que todos los usuarios que inicien una sesión a través de la red utilicen la cuenta de Invitado. Este cambio evita que los usuarios no autorizados intenten tener acceso a un sistema a través de Internet mediante el uso de la cuenta de un administrador local sin contraseña para inicio de sesión.

Seguridad simple de recursos compartidos

El modelo de recurso compartidos y seguridad de las cuentas locales permite elegir entre los modelos de seguridad Sólo invitado y Clásico. En el modelo Sólo invitado, quienes intenten iniciar una sesión en el equipo local a través de la red se verán obligados a utilizar una cuenta de Invitado. En el modelo de seguridad Clásico, los usuarios que intentan iniciar una sesión en el equipo local a través de la red se identificarán con sus propios datos. Esta directiva no afecta a los equipos que participan en un dominio. En los demás casos, se habilita el modo Sólo invitado de forma predeterminada.

Si se habilita una cuenta de invitado con la contraseña en blanco, podrá iniciar una sesión y tener acceso a todos los recursos para los que tenga autorización la cuenta Invitado.

Si se habilita la directiva “Forzar a los inicios de red que utilizan cuentas locales a autenticarse como Invitado”, las cuentas locales deben autenticarse como Invitado. Esta directiva determina si una cuenta local que se conecta directamente a un equipo de la red debe autenticarse como un usuario Invitado. Se puede utilizar esta directiva para limitar los permisos de una cuenta local que intenta tener acceso a los recursos del sistema del equipo de destino. Si habilita esta directiva, todas las cuentas locales que intenten conectarse directamente obtendrán únicamente los permisos de Invitado, que suelen ser restringidos.

Restricciones de contraseñas en blanco

Las cuentas sin contraseña sólo se pueden utilizar para iniciar una sesión en la consola física del equipo. Esta medida protege a los usuarios que no protegen sus cuentas con contraseñas. De forma predeterminada, las cuentas con contraseñas en blanco ya no se pueden usar para iniciar una sesión en el equipo de forma remota a través de la red, ni para ninguna otra actividad de inicio de sesión, salvo en la pantalla de la consola física.

Sistema de codificación de archivos

La nueva funcionalidad EFS (Encrypted File System - Sistema de Codificación de Archivos), mejora la capacidad de Windows XP gracias a su flexibilidad para los usuarios corporativos a la hora de distribuir soluciones de seguridad basadas en archivos de datos cifrados.

Si cifra una carpeta, todos los archivos y subcarpetas que se creen o agreguen a ella se cifrarán automáticamente. Se recomienda cifrar las carpetas para evitar la creación de archivos temporales de texto sin formato en el disco duro durante la conversión de archivos.

El usuario que cifra un archivo protegido es el único que puede abrirlo y trabajar con él. Esta característica resulta especialmente útil para los usuarios de equipos móviles, porque si alguien tiene acceso a un portátil extraviado o robado, no podrá ver ninguno de los archivos del disco.

Cuando los archivos están cifrados, sus datos se protegen aunque un intruso tenga acceso total a los datos almacenados en el equipo.

Elementos que se pueden cifrar

Cuando se activa el cifrado de una carpeta, EFS cifra automáticamente los siguientes elementos:

- Todos los archivos nuevos que se crean en la carpeta.
- Todos los archivos de texto sin formato que se copian o mueven a la carpeta
- Opcionalmente, todos los archivos y las subcarpetas existentes.

El sistema EFS también puede cifrar los archivos sin conexión, que en Windows 2000 reciben el nombre de caché en el lado cliente.

Cifrado de archivos sin conexión

El cliente puede utilizar EFS para cifrar los archivos y carpetas sin conexión. Esta característica es particularmente atractiva para los profesionales que viajan y necesitan trabajar periódicamente sin conexión sin renunciar a la seguridad de los datos.

Cifrado de la base de datos de archivos sin conexión

Windows XP ofrece la posibilidad de cifrar la base de datos de archivos sin conexión para proteger todos los documentos guardados en la caché local contra el robo y, al mismo tiempo, dotarlos de mayor seguridad.

Operaciones EFS remotas con archivos compartidos y carpetas Web

Windows XP puede cifrar y descifrar los archivos almacenados en recursos compartidos de archivos de red o en carpetas Web WebDAV (Web Distributed Authoring and Versioning - Autoría y Versionado Distribuidos basados en Web).

Operaciones EFS remotas en un entorno de carpetas Web

Cuando se abren archivos cifrados almacenados en carpetas Web, permanecen cifrados durante la transferencia y EFS los descifra localmente. Tanto la carga como la descarga hacia y desde las carpetas Web son transferencias de datos sin procesar, por lo que aunque un intruso lograra tener acceso a los datos durante la transmisión de un archivo cifrado, los datos capturados carecerían de utilidad.

La unión del sistema EFS y las carpetas Web hace innecesario utilizar software especializado para compartir con seguridad archivos cifrados entre usuarios, empresas u organizaciones.

Servicios de Certificate Server

Los Servicios de Certificate Server son la parte del sistema operativo que permite a una empresa actuar como su propio emisor de certificados (CA) para emitir y administrar certificados digitales. Windows XP tiene soporte para varios niveles jerárquicos de CA y una red de confianza con certificación cruzada que incluye emisores de certificados sin conexión y en línea.

Almacenamiento de certificados y claves públicas

Windows XP guarda los certificados de clave pública en el almacén de certificados personales. Los certificados se almacenan en texto sin formato porque su información es pública, e incluyen la firma electrónica de los emisores de certificados para evitar su falsificación.

Almacenamiento de claves privadas

En el caso de los perfiles usuarios itinerantes, la clave privada se guarda en la carpeta RSA del controlador de dominio y se descarga al equipo, donde permanece hasta que se cierra la sesión o se reinicia el equipo.

Dado que es necesario proteger las claves privadas, todos los archivos de la carpeta RSA se cifran automáticamente con una clave simétrica aleatoria denominada clave de sesión del usuario. La clave de sesión del usuario tiene una longitud de 64 bytes y se obtiene con un generador de números aleatorios seguro. Las claves 3DES (un algoritmo de cifrado) se derivan a partir de la clave de sesión y se utilizan para proteger las claves privadas. La clave de sesión se genera de forma automática y se renueva periódicamente.

Cuando se almacena en el disco, la clave de sesión se protege con el algoritmo 3DES mediante una clave basada en una parte de la contraseña del usuario. Se utiliza para cifrar automáticamente todos los archivos de la carpeta RSA a medida que se crean.

Servidor de seguridad de conexión a Internet

El servidor de seguridad de conexión a Internet (ICF - Internet Connection Firewall) de Windows XP protege de las amenazas de seguridad a los equipos de escritorio y móviles que utilizan conexiones DSL (Digital Subscriber Line - Línea Digital de Suscripción), de módem por cable o de módem de acceso telefónico a un proveedor de servicios de Internet (ISP - Internet Service Provider).

Directiva de grupo sensible a la ubicación del ICF

Una de las características únicas del ICF es su directiva de grupo sensible a la ubicación. Es de ayuda para los usuarios móviles que desean proteger sus equipos móviles de trabajo cuando están en casa o en lugares tales como hoteles, aeropuertos u otras zonas activas de conexión a Internet.

Funcionamiento del ICF

El ICF funciona como un filtro de paquetes de inspección de estado que comparte tecnología con ICS (Internet Connection Sharing - Conexión Compartida a Internet). Aunque la característica ICF es independiente, también puede ejecutarla en el adaptador compartido para proteger su red doméstica.

Cuando está habilitado, el filtro de inspección de estado bloquea todas las conexiones no solicitadas que procedan de la interfaz de red pública. Para ello, el ICF utiliza la tabla de flujo de traducción de direcciones de red (NAT - Network Address Translation) para validar todos los flujos entrantes. Sólo se permite la entrada de los flujos de datos si existe una asignación en la tabla de flujo NAT que proceda del sistema del servidor de seguridad o de la red interna protegida.

Configuración de directivas de grupo relacionadas con la seguridad

Windows XP puede establecer directivas de seguridad para la administración de contraseñas; por ejemplo:

- Determinar la longitud mínima de las contraseñas.
- Definir el intervalo de cambio de las contraseñas.
- Controlar el acceso a los recursos y los datos.

Directivas de restricción de software

Las directivas de restricción de software proporcionan a los administradores un mecanismo impulsado por directivas para identificar el software que se encuentra en ejecución en su dominio y controlar su capacidad de ejecución. El administrador puede utilizar una directiva de restricción de software para impedir la ejecución de aplicaciones no deseadas, como virus, caballos de Troya u otros programas cuya instalación provoque conflictos.

Uso de directivas de restricción de software

Se puede utilizar una directiva de restricción de software para limitar la ejecución a un conjunto de aplicaciones. Para dar a conocer las aplicaciones a la directiva, se puede utilizar la ruta del archivo, el hash del archivo, el certificado firmante de Microsoft o la zona Internet. Una vez identificada, el sistema aplica las directivas definidas.

Las directivas de restricción de software también se pueden usar como protección contra virus basados en secuencias de comandos y caballos de Troya. Se puede configurar una directiva de restricción de software para impedir la ejecución de cualquier secuencia de comandos que no esté firmada por un miembro de la organización de TI. Las directivas de restricción de software también permiten regular las aplicaciones que pueden instalar los usuarios en sus equipos.

FIABILIDAD EN WINDOWS XP

Soporte para hardware y dispositivos

Este sistema operativo supone la unión de las ventajas de los productos Windows Me y Windows 2000 para ofrecer una mayor estabilidad al sistema y mejor compatibilidad con diversos dispositivos. Ofrece soporte Plug and Play, soporte para el periférico USB (Universal Serial Bus), el bus de alta velocidad IEEE 1394 y Componente de Interconexión Periférica (PCI - Peripheral Component Interconnect) y otros tipos de buses.

Soporte DLL colateral

Debido a que son varias las aplicaciones compatibles con Windows que ejecutan funciones similares a menudo comparten componentes del sistema operativo tales como las bibliotecas de enlaces dinámicos (DLL). Si las aplicaciones dependen de versiones distintas de los componentes, el hecho de compartir estos componentes puede provocar problemas. Para compensar las consecuencias negativas derivadas de compartir, Windows XP ofrece soporte para que se pueda hacer de forma segura, lo que se denomina componentes laterales.

En lugar de tener una única versión de un componente que asume una compatibilidad con versiones anteriores, los componentes laterales posibilitan que se ejecuten al mismo tiempo varias versiones de un objeto COM o una interfaz del programador (API) de Win32.

Rastreador de sucesos de apagado

El rastreador de sucesos de apagado proporciona un mecanismo simple y estándar que se puede utilizar para documentar de manera coherente las razones para apagar o reiniciar el equipo. Además de rastrear las causas del apagado, el rastreador de sucesos de apagado registra el estado del sistema antes de que éste sea cerrado, de esta manera identifica las limitaciones del sistema antes de reiniciar el sistema. Recoge una serie de parámetros de todos los procesos que se estaban

ejecutando en el sistema, cada archivo de página, cada disco, y la utilización de todos los recursos. Así posteriormente puede revisar las razones por las que se apagó en el diario del sistema así como los estados del sistema correspondientes y analizar toda esta información.

Comprobador de controladores de Windows

El comprobador de controladores de dispositivos de Windows impide instalar o descargar controladores de dispositivos defectuosos, es decir aquellos que provocan que el sistema se paralice temporalmente o se cierra de repente. Para ello utiliza una base de datos de controladores defectuosos, gestionada por Microsoft, y así decide cuáles deben instalarse o descargarse.

Instalador de Windows

La característica de Instalador de Windows mejora el nivel de ejecución y fiabilidad de Windows XP en la reparación e instalación, lo que ayuda a mantener los sistemas funcionando de forma eficaz y repararlos en caso de que se produzca un error. Se reduce el número de archivos que hay que copiar, lo que mejora la ejecución en los procesos de instalación y reparación y aumenta la fiabilidad y reduce el tiempo de inactividad durante el proceso de reparación /instalación.

Actualizaciones automáticas

Gracias a la característica de actualizaciones automáticas se puede actualizar el equipo sin tener que interrumpir la conexión a la Red. Los archivos que se descargan conservan un tamaño para así reducir al mínimo las consecuencias que esto pueda tener en la capacidad de respuesta de la red. El proceso de descarga se retoma de forma automática si el sistema se desconecta antes de que se haya finalizado.

Configuración con Actualización dinámica

Cuando se ejecuta Configuración mientras se está realizando una instalación o una actualización en el sistema operativo, la Actualización automática aumenta la

fiabilidad del sistema ya que ofrece actualizaciones de compatibilidad de dispositivos y aplicaciones, actualizaciones de los controladores y arreglos de emergencia para cuestiones de configuración o seguridad.

Las copias de seguridad en la sombra (Shadow copy)

Windows XP presenta una tecnología de copias de seguridad llamada Shadow Copy, que realiza copias exactas de los archivos incluso aquellos que están abiertos. Gracias a estas capturas los usuarios o las aplicaciones pueden seguir trabajando sin tener que detenerse mientras se está realizando la copia de seguridad.

Última configuración válida conocida

En Windows XP, además se restaura la última configuración válida conocida de los controladores de dispositivos. De esta manera puede esquivar los problemas derivados de las nuevas instalaciones.

Recuperación automática del sistema

En Windows XP se ha introducido una opción avanzada de la barra de copia de seguridad llamada Recuperación Automática del Sistema (ASR, Automated System Recovery). Gracias a ASR se pueden guardar y restaurar aplicaciones, el estado del sistema y archivos importantes para el sistema y para las opciones de arranque. ASR sustituye al disco de reparación de emergencia

Mejoras en la característica Restaurar sistema

Cuando se han hecho cambios en el sistema susceptibles de causar problemas puede deshacerlos o incluso volver a una configuración anterior a la realización de esos cambios. La característica Restaurar sistema ayuda a que el equipo siga funcionando sin problemas y, además, puede reducir la necesidad de solicitar soporte o ayuda de escritorio.

Capítulo 3

Planteamiento del problema y elección de la solución

3.1 PROBLEMÁTICA ACTUAL

Actualmente la mayoría de las empresas del país, sin importar su tipo o actividad, tienen problemas con el control de los accesos a sus aplicaciones informáticas y al adecuado manejo de sus contraseñas de autenticación de cada uno de los usuarios, sin importar la jerarquía de sus respectivos puestos, o de las actividades que desempeñen dentro de la misma. Generalmente son usadas contraseñas inadecuadas por la simplicidad que las conforma, así mismo el uso de estas y la correcta creación de las mismas resulta de vital importancia para la seguridad de la empresa, ya que de esto depende en gran parte el correcto funcionamiento de cada una de las áreas que la integran, ya sean las áreas administrativas, las áreas de operación, y hasta las áreas directivas, puesto que un ataque en materia de seguridad en cualquiera de las áreas resulta problemático para la empresa entera.

Es por ello que es necesaria la implantación de dispositivos complementarios que ayuden a la mejor y automática validación de los accesos, tanto a las aplicaciones informáticas como a las empresas mismas, siendo esto último un punto de análisis de igual valor que la autenticación a sistemas informáticos, lo que se analizará en este capítulo.

La autorización de acceso a los sistemas juega un papel importantísimo en la implantación de todo tipo de dispositivo o aplicación que busque controlar o administrar esta etapa, ya que al librar con éxito la etapa de identificación, resulta de mayor importancia la asignación adecuada de privilegios y derechos para hacer uso de las aplicaciones disponibles, así como de las funciones que correspondan a la misma.

A continuación se analizan algunas de las problemáticas actuales, comenzando por el impacto tanto económico como social que tienen los sistemas basados en reconocimiento de huellas dactilares, los cuales son relativamente baratos (en comparación con otros sistemas biométricos, como los basados en patrones retinales); sin embargo, tienen en su contra la incapacidad temporal de autenticar usuarios que se hayan podido herir en el dedo a reconocer (un pequeño corte o una quemadura que afecte a varias minucias que pueden hacer inútil al sistema). También elementos como la suciedad del dedo, la presión ejercida sobre el lector o el estado de la piel pueden ocasionar lecturas erróneas. Otro factor a tener muy en cuenta contra estos sistemas es psicológico, no técnico: un sistema de autenticación de usuarios debe de ser aceptable por los mismos, y generalmente el reconocimiento de huellas se asocia a los criminales, por lo que muchos usuarios recelan del lector de huellas y de su uso (figura 3.1.1).

Actualmente no se tienen mecanismos de registro de actividades que apoyen la seguridad en muchas empresas, siendo esto una problemática real y vigente, ya que los activos informáticos resultan burlados, así como la información contenida en ellos, una vez dentro no se tienen registros de las actividades ejecutadas por los usuarios.

De esta forma, en materia de seguridad informática hay una problemática notable, la cuál será mitigada en gran medida con la implantación del Sistema de Recuperación de Información a través de Huellas Dactilares.

Figura 3.1.1. El reconocimiento de huella dactilar en asuntos criminales

Como se comentó al inicio del capítulo, el sistema será aplicado tanto a control de accesos a aplicaciones informáticas como al control de jornadas laborales reales, siendo este otro punto problemático en todo tipo de empresas, basándonos en el hecho de que la productividad en cuestiones administrativas en la mayoría de las áreas que conforman a las empresas está estrechamente ligada al uso de los equipos de cómputo y sus aplicaciones informáticas, se puede considerar como herramienta de control, las horas hombre registradas en el sistema en cada una de las aplicaciones, siendo esto un posible mecanismo de medición en cuestión de productividad laboral, ayudando así al cumplimiento de los objetivos de las empresas e instituciones, tanto particulares como del sector público.

Actualmente la mayoría de las empresas cuentan con métodos de registro de entradas a las jornadas laborales muy anticuados, como lo son el uso de relojes checadores de golpe, con tarjetas que resultan fácilmente burladas, o tarjetas de cinta magnética, que aunque más confiables, siguen siendo un punto débil en cuestión de seguridad al ser fácilmente transferibles entre los trabajadores, siendo estas opciones muy inseguras y fácil de burlar ya que es común encontrar

empleados que piden a otros compañeros que registren por ellos su entrada o salida, generando un verdadero problema tanto en términos de productividad como en términos de control de jornadas laborales, así como de ausentismos en las diferentes áreas. Es por ello que resulta necesario combatir estos puntos débiles con una mejor alternativa en materia de registro de incidencias, una solución que sea segura, confiable y la cuál sea difícil de burlar.

El Sistema de Recuperación de Información a través de Huellas Dactilares es una opción para dar solución a la mayoría de los problemas en materia de registros de entrada y salida de personal, así como de administración y control de productividad, ya que como se ha analizado anteriormente, la huella dactilar resulta un mecanismo altamente confiable ya que es un elemento que a diferencia de las credenciales magnéticas no se olvida, no se puede dar a un compañero para que registre la entrada o salida por otro, y además, la huella resulta única e irrepetible en cada persona, siendo esto un elemento de peso para cuestiones de seguridad.

3.2 REQUERIMIENTOS GENERALES Y PARTICULARES

Requerimientos generales

- Manipulación y obtención de datos.

  Se necesita generar una base de datos robusta que contenga toda la información de los usuarios de la empresa, para que se pueda realizar el control de accesos de los usuarios a las diferentes aplicaciones.
- Desarrollo en una herramienta actual y confiable.

  El sistema a desarrollar tiene que presentarse en una herramienta actual, para evitar problemas de falta de mantenimiento por ser una herramienta vieja y obsoleta en muchos casos.
- El sistema debe de diseñarse de modo que pueda ser actualizado sin mucha dificultad y en un plazo corto de tiempo.

El sistema tiene que ser desarrollado de una manera clara y organizada, debe de encontrarse el código identado y comentado para que al realizar actualizaciones no se tenga complicación o retrasos en tiempo.

- Generación de ventanas.

  El sistema deberá de contar con ventanas según las necesidades de la empresa. Además las ventanas tendrán que presentar la funcionalidad de que sean multiusuario, para que los usuarios tengan acceso a las diferentes aplicaciones.

- Diseño de ventanas con un entorno amigable.

  Que el sistema se presente en un entorno amigable es de gran ayuda para que no se presenten inconvenientes en su uso por parte de los usuarios.

- Instalación fácil.

  El módulo de instalación debe de ser relativamente fácil en su instalación para que no presente rechazo por parte del personal encargado de su instalación.

- Manejo multiusuario.

  El sistema tiene que manejarse en una red local, donde cualquier usuario tiene que poder contar con él para acceder a las aplicaciones que requiera.

Requerimientos particulares

- Diseño de ventanas.

  Las ventanas que presente el sistema tienen que mostrar una forma estándar en cuanto a tamaño, color, tipo y tamaño de letra y ubicación. Las ventanas tienen que presentar colores no molestos para la vista y con una diferencia clara en el contraste entre las letras y el color del fondo de la ventana generando con ellos que la familiarización de los usuarios con el sistema sea más rápido.

- Seguridad.

  Los usuarios podrán generar sesiones de trabajo en diferentes equipos, ocasionando que la última sesión sea la que se encuentre activa y

desactivando las anteriores a esta. No se podrá estar trabajando en más de un equipo con diferentes sesiones activadas por un mismo usuario.

- Generación de reportes.

  El sistema debe de ser capaz de generar reportes del control de accesos, donde se muestre el usuario, las aplicaciones del negocio a las que tuvo acceso y la hora y fecha del acceso. Esto para evitar negación en la modificación o mal uso de la información por parte de los usuarios.

- Accesibilidad a aplicaciones.

  El sistema deberá de ser capaz después de haber sido autenticado el usuario de poder entrar a las aplicaciones que este requiera sin la necesidad de autenticarse aplicación por aplicación. Esto ya que no es conveniente modificar todas las aplicaciones para que se pueda acceder a ellas a través de la huella dactilar.

3.3 BÚSQUEDA Y ANÁLISIS DE LA INFORMACIÓN

Control de contraseñas

No importando el sistema operativo, hoy en día la mayoría de los sistemas informáticos son susceptibles a ser alterados, dañados o espiados. Los procedimientos tradicionales de seguridad han sido fácilmente detectables para los expertos en violar la seguridad con fines de espionaje o daño intencional a la información. Esto nos introduce en categorías de usuarios que a continuación se definen.

Usuario común

Es un usuario que pasa sin pena ni gloria en una sesión normal, comúnmente sólo ingresa y consulta información como una actividad cotidiana en su vida. Este usuario por lo regular no se interesa en temas especiales de computación y ve a la computadora como una simple herramienta de trabajo sin cuestionarse nada sobre su funcionamiento.

Usuario Experto

Se entiende como “Usuario experto” o “*Expert Partner*”, aquella persona que por sus características técnicas y humanas ha demostrado que actúa (o puede llegar a actuar) como primer nivel de soporte técnico, para sus compañeros de trabajo y que actúa como enlace o transmisor de tecnología.

Por la experiencia acumulada, se sabe que una parte muy importante de los problemas del usuario final se resuelven en muy poco tiempo y no entrañan gran dificultad; sin embargo dado el proceso que se ha detallado anteriormente, la demanda de alta tecnología, asignación del técnico, etc., hace que el sistema no sea instantáneo (la necesidad de recursos humanos sería casi infinita).

La idea para abaratar los costos totales de posesión de equipos informáticos, se basaría en integrar a esos usuarios en la dinámica de formación propia de Asistencia Técnica, o llegado el caso, enfocar una serie de sesiones dedicadas que engloben los problemas más comunes y sus soluciones.

Hackers

Los Hakers son usuarios cuyo nivel de conocimientos es lo suficiente como para acceder a los sistemas confidenciales de información, son usuarios que en el ámbito informático se clasifican como los “benignos de la seguridad”. Sus objetivos son los de vulnerar los servidores, sistemas main y sitios Web en Internet para demostrar su inseguridad. Son tan antiguos como la computación misma, ya que ellos han demostrado la inseguridad de los sistemas informáticos, incluso empresas y gobiernos mundiales han patrocinado pruebas de vulnerabilidad a sistemas y han hecho convocatorias a grupos de hakers para probar sus sistemas de seguridad.

Cracker

El término cracker se creó alrededor de 1985 por algunos hackers como una defensa en contra de quienes hacían mal uso del nombre, ya que lo utilizaban para hacer cosas totalmente ilegales, porque aunque el cracker hace lo mismo que un

hacker, el primero no lo hace de forma altruista ni por amor al arte. Los crackers suelen tener ideales políticos o filosóficos, o bien se mueven por arrogancia, orgullo, egoísmo, ambición o avaricia.

Un cracker actúa del mismo modo que un hacker, pero una vez que logra ingresar al sistema no se da por satisfecho, sino que le hace “crac”, es decir, lo quiebra. Sus hazañas típicas son la copia de información confidencial, movimientos de pequeñas sumas de dinero y compras a nombre de otros.

El cracker maneja el arte de reventar protecciones de software y hardware mediante ingeniería inversa, ya que sin el programa fuente es posible analizar el comportamiento del programa y modificarlo. Lo único que se necesita para lograrlo es interés y paciencia.

Los crackers están ligados también a la piratería, al permitir que las compañías utilicen demos de ciertas aplicaciones como si tuvieran la licencia de las mismas.

Ingeniería social

Uno de los sistemas más utilizados es el llamado por los atacantes ingeniería social, no es técnico sino que se basa en descubrir las contraseñas directamente de los usuarios. Los métodos pueden ser: observar el teclado cuando se introduce la contraseña, descubrirlo escrito en un papel, pedirlo por correo electrónico o teléfono haciéndose pasar por el administrador, etc. Aunque parezca imposible, las estadísticas dicen que es uno de los sistemas más utilizados.

Phrackers

Estos son expertos que trabajan a nivel de sistemas de comunicación de electrónica digital, y se especializan en acceder a los sistemas de enlace terrestre, celular e incluso satelital, afectan los protocolos de *routers* y servidores de cómputo. Se han detectado a este tipo de expertos ingresando sistemas que vulneran e incluso llegan a dañar equipos electrónicos.

Cada uno de estos usuarios merece un trato especial, pero todo concuerda que la seguridad debe de ser controlada por un dispositivo que apoye al idea de hacer un sistema más confiable. Es por esto que se debe de hacer clara idea que una contraseña seguirá existiendo en todo sistema pero también existen formas de proteger las contraseñas y el dispositivo lector de huellas dactilares es uno de ellos.

Problemática actual

Para realizar su labor, un cracker necesita llevar a cabo dos tareas. La primera consiste en obtener información (o copias de ella) y analizarla para obtener resultados. Su principal función no es destruirla, sino obtenerla, analizarla y modificarla de la manera más discreta posible.

Quien suministre la información al cracker intentará que la víctima del ataque no sea consciente de que ha ocurrido algo anormal. Para ello, lo mejor es realizar una discreta copia de los datos contenidos en la computadora de la víctima de manera directa o través del módem o las redes de la compañía. La idea es que una operación de cracking (un "asalto") establece necesariamente un vínculo entre el cracker y la computadora de la víctima.

Una vez que el cracker tiene la información en su poder, comienza la segunda parte: lograr que sea de utilidad. En la actualidad, esto no resulta tan complicado como pareciera. Sólo tiene que ejecutar las aplicaciones o abrir los archivos de bases de datos usando software comercial y dedicarse a hacer listados. Esta labor es un tanto trabajosa, pero fructífera, y en unos días de trabajo una persona profesionalmente calificada puede "vaciar" toda la información que se le ha suministrado a una computadora e incluso a la red.

Si se instala en una máquina un programa llamado *sniffer*, éste captura toda la información que circula por la Ethernet o Token Ring (tipos de redes de área local) de la máquina. Estos programas descubren las contraseñas mientras circulan por la

red. Si no están cifradas (hay muchos sistemas que no cifran las contraseñas para enviarlas), el atacante ya ha conseguido su medio de acceso. Pero si están cifradas también los puede utilizar repitiendo el mensaje como respuesta a una petición de identificación. El atacante únicamente necesita poder instalar en el servidor o en una máquina de la misma LAN un programa de este tipo.

Las contraseñas son un punto débil de los sistemas de seguridad, pero para realizar control de acceso por usuario son el sistema más sencillo, popular y probado. Se puede hacer un símil con las protecciones físicas de los edificios, la puerta y su sistema de abertura (llaves, combinaciones, la cerradura,...) son imprescindibles pero también son el principal método utilizado para acceder sin permiso.

En los sistemas operativos y las aplicaciones con filtro las contraseñas se deben guardar cifradas en archivos. El problema es que estos archivos no pueden tener permisos de usuarios restringidos ya que al entrar la contraseña el usuario puede ser cualquiera. Una forma de evitar este problema sería dar permiso de administrador al archivo y que el usuario por defecto cuando se introdujera la contraseña fuera el administrador, pero esto sería muy peligroso porque cualquiera tendría permiso de administrador por un momento.

Así este archivo sin permisos en principio es accesible por todos los usuarios, pero se utilizan técnicas para evitar este acceso. Un ejemplo: en Windows de Microsoft el archivo se está utilizando siempre por el sistema y los archivos que utiliza el sistema no son accesibles para escritura, esta protección ya ha sido vencida por los programas de los atacantes.

La propuesta es resolver la problemática de seguridad mediante el lector de huella digital combinado con una clave cifrada para hacer el acceso sumamente complicado para cualquier tipo de usuario que no tenga acceso al sistema de base de datos.

Propuesta de solución

Para este punto, se establece que las políticas deben ser administradas perfectamente por el administrador informático. Los sistemas operativos actuales, permiten establecer políticas restrictivas a los usuarios limitando así su incursión a los puntos vulnerables de la red y/o servidores. El sistema operativo Windows 95 y Windows 98 presentaron el POLEDIT (editor de Políticas) como herramienta de administración en una red LAN, apoyados con Windows NT Server 4.0 se complementaron, no obstante están latentes los ataques. En la actualidad los equipos con sistema operativo Windows XP y el Servidor con Windows 2003 Server, la seguridad se ha incrementado, pero esta latente aún el desarrollo de nuevas técnicas para afectar la seguridad de redes en ambiente del sistema operativo Windows.

Qué hacer para solucionar el problema de intercambio de claves. Para defenderse de estos ataques se puede trabajar en tres líneas:

- Políticas de personal.
- Herramientas de programas.
- Sistemas de contraseña de un uso.

Las políticas de personal van orientadas a aconsejar u obligar al personal de la empresa a cumplir ciertas normas para proteger sus propias contraseñas. Tanto los ataques con acceso al archivo como los de ingeniería social se basan en aprovechar que los usuarios no tienen cuidado con la elección y el mantenimiento de sus contraseñas. Así una política puede fijar normas como:

- Tamaño mínimo.
- Intercalar entre las letras números y signos de puntuación.
- Prohibir contraseñas de diccionario.
- Cambiarlo cada cierto tiempo.
- Si un atacante entra utilizando la contraseña de un usuario, sancionarlo.

Las herramientas pueden ser opciones del sistema operativo, programas complementarios al sistema o programas de inspección. Los objetivos son:

- Obligar por software a cumplir las políticas de personal comentadas en el anterior párrafo.
- Atacar con un cracker u otro programa para probar la resistencia del sistema de contraseñas.
- Cancelar cuentas que han recibido intentos de acceso fallidos. Se recuperan después de un tiempo o a través del administrador.

Una manera de aumentar mucho la seguridad en los accesos remotos es utilizar unos sistemas, llamados OTP (One-Time Password – Contraseña de un Solo Uso), donde la contraseña de un usuario cambia cada vez que se usa, o sea, contraseñas de un uso. El origen es el sistema SIKey propietario de la empresa Bellcore, pero actualmente el IETF (Internet Engineering Task Force - Grupo de Trabajo en Ingeniería de Internet) ya ha estandarizado el método con el nombre de OIP. El servidor y el usuario deben estar sincronizados para saber en cada momento que contraseña se debe utilizar. Si algún atacante descubre una contraseña no le sirve porque para el siguiente acceso se necesita otra.

Los sistemas OIP necesitan servidores preparados para calcular cada vez la contraseña que toca y clientes con un software o un equipo electrónico capaz de realizar la misma función. Estos equipos electrónicos se llaman testigos (tokens) y se pueden considerar de la familia de control de accesos por posesión de un objeto combinado con contraseñas.

En OIP para calcular la contraseña se utilizan los siguientes parámetros:

- Una frase secreta del usuario (*Passphrase*).
- Una palabra aleatoria conocida por el servidor y el software o hardware del usuario.
- Una función *Hash*.

- El número de accesos que se han realizado desde el inicio, o sea, el número de secuencia.

Así se entra a una función hash, la passphrase y la palabra aleatoria, al resultado se le aplica varias veces la misma función Hash según marca el número de secuencia. El resultado se envía al servidor como contraseña, éste realiza el mismo proceso y se comparan los resultados.

Sistema biométrico de lectura de huella dactilar

Como se mencionó en el capítulo 1, los sistemas biométricos utilizan una característica física del usuario. La característica debe ser única en las personas y no cambiar con las circunstancias (estado de ánimo, temperatura ambiente, iluminación, etc.) ni con el tiempo (insensible al envejecimiento). Estos sistemas son mucho más seguros que los de contraseña, sobre todo si se combinan con otros, las ventajas que tienen estos sistemas son los siguientes:

- Intransferibles, el atacante no los puede utilizar aunque los conozca. Esta característica es suficiente para considerar el sistema mejor que los de contraseña o posesión de objetos.
- No necesitan gestión del usuario, como cambiarlos a menudo, recordar frases largas, guardar objetos (tokens), etc.
- Sirven tanto para accesos físicos como lógicos.
- Son muy seguros a cualquier ataque.

Actualmente aún tienen algunas desventajas, las cuales se corregirán con el tiempo, dichas desventajas son:

- Necesitan electrónica adicional para realizar las lecturas de imágenes y, por lo tanto, son más caros a excepción del lector de huellas digitales que hoy en día es muy económico.
- La tecnología no está muy avanzada.
- Tienen un cierto rechazo del usuario delante de la exposición física a un sensor.

En una identificación biométrica se realizan las siguientes fases:

- Captar la imagen o sonido relativa al autenticador de la persona mediante un sensor.
- Modificar los datos brutos de la imagen o sonido mediante técnicas de tratamiento de señal para extraer los parámetros básicos y únicos del usuario (modelos/patrones), así como eliminar los datos dependientes de las condiciones externas de la medida.
- Comparar estos parámetros con los almacenados.

Como se puede deducir del proceso, la comparación de resultados nunca es exacta, por lo tanto se busca un grado de aproximación a partir del cual se considera que los parámetros medidos son de la misma persona que los almacenados. Así es posible tener errores, éstos están medidos estadísticamente para cada método biométrico con los siguientes índices:

- FAR (False Acceptance Rate - Tasa de Falsa Aceptación). Mide en tanto por ciento la relación de identificaciones erróneas consideradas correctas.
- FRR (False Rejection Rate - Tasa de Falso Rechazo). Mide en tanto por ciento la relación de rechazos al acceso que eran correctos.
- SR (Succes Rate). Da un índice global de la calidad del sistema, relacionando los índices anteriores, se utiliza la fórmula: SR = 100 - (FAR+FRR).

En el proceso de comparación se pueden diferenciar dos métodos: identificación y verificación. La identificación consiste en encontrar en una base de datos de parámetros biométricos si los medidos coinciden aproximadamente con algún usuario, es para un sistema de acceso donde no se introduce el nombre de usuario o para búsqueda de personas (por ejemplo en archivos policiales). La verificación compara directamente los parámetros medidos con los del usuario y según la aproximación matemática se considera el acceso permitido o denegado, es el sistema de acceso más habitual. Lógicamente la verificación tiene índices de FAR y FRR mucho más elevados que la identificación.

3.4 PROBLEMÁTICA IDENTIFICADA POR ÁREAS Y SUS POSIBLES SOLUCIONES

El objetivo es lograr una organización eficiente, clara y concisa sobre la base de su estructura, por lo que se hace necesario establecer rangos y posiciones de acuerdo a las necesidades de la organización. La forma como se encuentra estructurada la empresa en estudio, puede ser apreciada en el siguiente organigrama (figura 3.4.1).

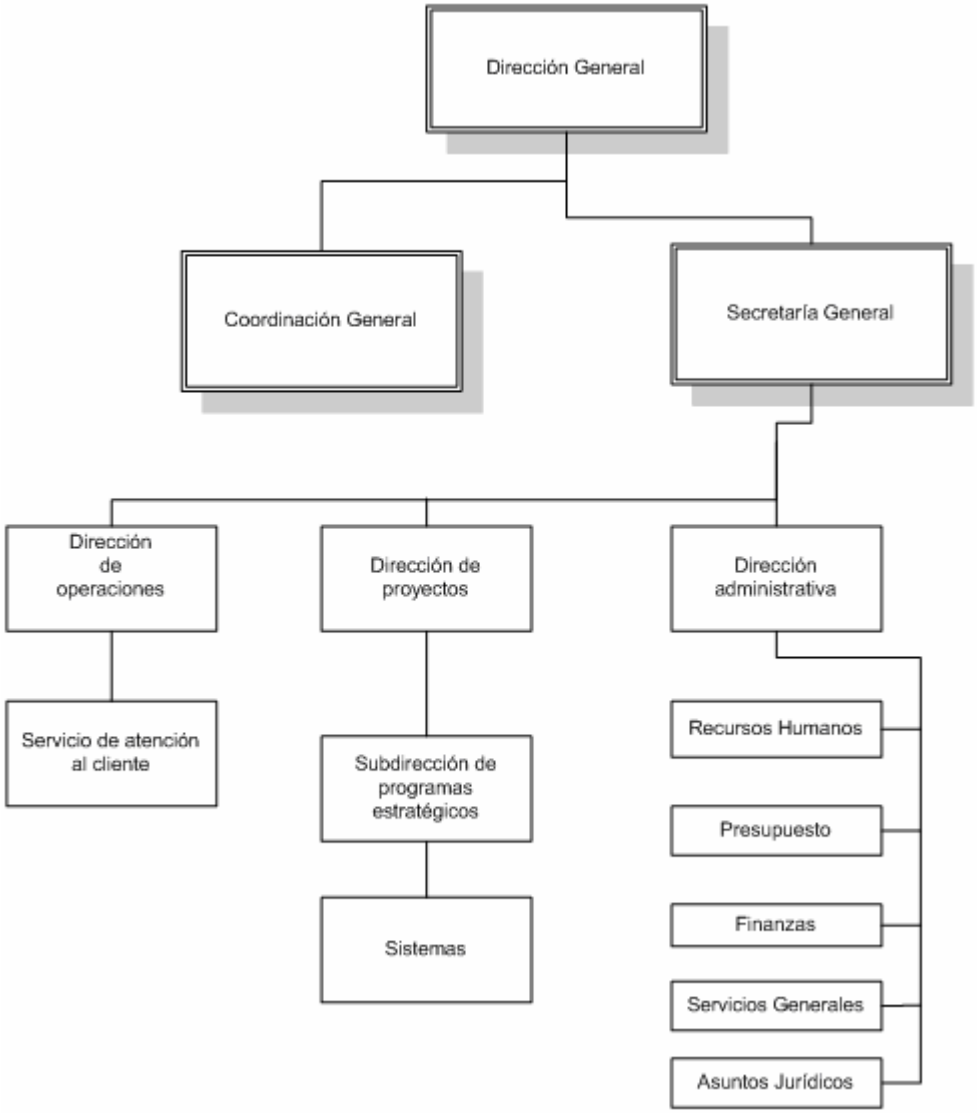


Figura 3.4.1. Organización de la empresa en estudio

Problemas detectados en la empresa

A través del organigrama se pueden detectar los siguientes problemas en el área de administración y sistemas donde es muy importante considerar posibles soluciones.

Acceso lógico

El acceso lógico de entrada de personal interno o externo a los sistemas es uno de los factores de mayor riesgo en las empresas e instituciones por el tipo de información que se maneja en el área administrativa. Es primordial que solo personal autorizado pueda hacerlo.

¿Por qué cuidar el acceso lógico a los sistemas?

- 71% del fraude por medios informáticos se debe a actividad interna.
- Cuatro de cada cinco trabajadores divulgarán su clave secreta a un compañero, si éste se los pregunta.
- La administración de claves o contraseñas, centros de llamadas, personal, procedimientos e infraestructura tienen un costo importante por usuario.
- El 40% de las llamadas a centros de soporte para empleados están relacionados con la pérdida, robo u olvido de claves o contraseñas.
- La suplantación de identidad es un tema de alta prioridad.

Administración del personal

Administrar los eventos de entradas y salidas del personal es importante para todo negocio, si se desea tener una idea más exacta de cómo el personal cumple sus obligaciones o verificar el acceso a lugares para personal restringido como la unidad de cómputo y el site donde se encuentran los servidores que proporcionan el servicio de Internet, correo electrónico, antivirus, sistemas que maneja la empresa con información confidencial, es un riesgo en la actualidad no contar con la debida protección para los lugares de uso exclusivo de personal autorizado ya que continuamente se han registrado robos en equipo de cómputo e información o mal uso de las contraseñas como la de administrador.

Es necesario implantar una medida de seguridad que de solución a estos problemas.

Incorporar un sistema de reconocimiento con características que permitan determinar si el usuario está realmente presente y es el que “dice” ser, o si por el contrario, está utilizando algún método de fraude.

Escenario de identificación lógico, en el que un usuario utilice un identificador propio para acceder a una aplicación en red.

Escenario de acceso físico, en el que se emplea el mismo identificador para acceder a un área restringida, esto contribuirá para evitar la pérdida de equipo.

Incrementar la seguridad, reducir el robo de identidad y proteger la privacidad de las personas debe ser el objetivo.

También la falta de control del personal en cuanto a su asistencia y horario de trabajo es un problema al realizar la nomina de empleados; existe la necesidad de tener mayor rendimiento y productividad en los empleados.

El mecanismo de control detecta cualquier desvío de los patrones normales, haciendo posible la debida regulación, como la función restrictiva de un sistema para mantener a los participantes dentro de los patrones deseados y evitar cualquier desvío. Es el caso del control de frecuencia y expediente del personal para evitar posibles abusos.

En estos tiempos de intensa competencia, es vital conocer la respuesta a estas preguntas: ¿Cuál es el índice de ausentismo? ¿Tiempo extra? ¿Puntualidad? ¿El costo de mano de obra por departamento? ¿Faltó hoy algún operario o supervisor clave de la línea de operación?

Desafortunadamente, los sistemas antiguos de control de tiempo trabajado con los que cuenta la empresa, son manuales, a base de relojes checadores mecánicos y tarjetas reloj, haciendo muy lento y trabajoso disponer de esta información. Una vez que las tarjetas se encuentran preparadas se colocan en los tarjeteros respectivos. Los empleados registran sus entradas y salidas diarias en estas tarjetas y son revisadas y corregidas diariamente por una secretaria o supervisor. Al final del período deben de ser revisadas nuevamente. Finalmente, los capturistas dan entrada a esta información al sistema de nómina. Este procedimiento consume tiempo de capturistas, personal de nóminas e incluso gerentes, en preparar y revisar las asistencias de los empleados. Como todo sistema manual, está expuesto a vulnerabilidad de los registros de entrada y salida, así como errores en la captura de esta información. Adicionalmente, los relojes mecánicos se descomponen con frecuencia.

Por otra parte, si falta algún empleado clave en la línea de producción, esa operación o máquina estará detenida hasta que se haya manualmente determinado un reemplazo.

La solución al problema anterior es un Control de Tiempo y Asistencia o Control de Asistencia, que otorga los siguientes beneficios:

- Eliminación de tarjeta reloj y el trabajo manual asociado a su procesamiento.
- Detección inmediata de ausentismo y retardos.
- Cálculo de tiempo trabajado; ordinario y extra.
- Generación automatizada de la información necesaria para la nómina.
- Disponibilidad de reportes con información actualizada al último minuto.
- Al conocer al instante el personal ausente, puede auxiliar para seleccionar un empleado de reemplazo en forma inmediata.
- Proporciona un sistema de control de acceso básico, capaz de operar puertas con chapas eléctricas.

El sistema de control de muchas empresas de hoy en día, con tarjetas y contraseñas, no da garantías de éxito, pero un sistema creado para dar soluciones deberá garantizar un control intransferible, exhaustivo y completo del personal de la compañía.

La idea del sistema es que la computadora base reciba y genere información a partir de los productos que controlan la presencia y productividad de los empleados, así como de los sistemas de alarmas y control de acceso. Por otro lado, el servidor de red deberá facilitar la consulta de los datos desde cualquier dispositivo que, a partir de la huella dactilar, permita acceder a todos los servicios ofrecidos.

Los intrusos intentan utilizar muchos métodos para obtener acceso a un sistema y aumentar sus privilegios.

Las áreas clave a tener en cuenta son:

- Impedir el robo de sesiones.
- Impedir el envenenamiento DNS.
- Impedir la copia IP.
- Proteger el archivo de contraseñas.
- Impedir los desbordamientos de búfer.

Las herramientas de robo de sesiones permiten que un intruso interrumpa, finalice o robe una sesión en curso. Estos tipos de ataques tienden a centrarse en las aplicaciones basadas en sesiones.

Desarrollar un plan de seguridad efectivo requiere entender de qué modo los intrusos obtienen acceso a los sistemas y luego modifican sus privilegios de acceso o de seguridad.

Todo esto implica tener una barrera más que impida el acceso a información o instalaciones restringidas, a partir de este punto es necesario contar con un sistema

capaz de identificar y autenticar al personal por medios biométricos. El reconocimiento a través de huella dactilar puede ser usado en cualquier aplicación que requiera seguridad, control de acceso, e identificación o comprobación del usuario.

Actualmente, la tecnología biométrica puede ser integrada con éxito en ratones y teclados para PC's, soluciones de seguridad para redes, soluciones de seguridad para Internet, sistemas bancarios on-line, cerraduras para puertas, sistemas de control de acceso, máquinas con tiempo de acceso.

Como se mencionó anteriormente, la metodología del reconocimiento de la huella dactilar está dividida en dos procesos diferentes: verificación e identificación.

El proceso de verificación es un proceso de combinación de uno-a-uno. El usuario confirma quién es el usuario. Una nueva muestra de la huella dactilar es tomada del usuario y comparada a la otra previamente registrada o archivada. Si las huellas dactilares coinciden, el usuario es "verificado" como siendo quién ellas dicen que es y concediendo todos los privilegios y accesos del usuario confirmado, es decir, que el sistema pudo verificar como siendo del usuario.

El proceso de identificación es un proceso de combinación de uno-a-muchos. El usuario no precisa confirmar quién es. La nueva muestra de la huella dactilar es tomada del usuario y comparada a una ya existente en el banco de datos de huellas dactilares, registradas o archivadas de todos los usuarios. Cuando es encontrada una combinación, el usuario es "identificado" como un usuario preexistente, es decir, el sistema encuentra quién es.

Áreas donde será implantado el sistema

La aplicación irá dirigida a los departamentos de recursos humanos y área de sistemas principalmente ya que en estas áreas es donde se han detectado los problemas que con ayuda de la aplicación será posible darles solución.

El área de recursos humanos cuenta con una base de datos que lleva el registro de todo el personal con que cuenta la empresa. El sistema de autenticación a través de la huella dactilar proporcionará una mejor administración en las entradas y salidas del personal; todos los empleados se dan de alta con su huella en el sistema la primera ocasión, y subsecuentemente utilizarán su huella para registrar dichos eventos. Con esto se eliminarán los checadores mecánicos y el trabajo de registrar en las tarjetas haciendo más eficiente el control de asistencia del personal.

En el departamento de sistemas se llevará un mejor control en el acceso a áreas restringidas como el Site donde se encuentran los servidores que dan el soporte a toda la empresa y en el cual sólo personal autorizado podrá entrar. Asimismo el acceso a los sistemas también podrá ser controlado; si la huella corresponde al empleado registrado es aceptado en el sistema, mismo que además registra características específicas de esa fecha en la que sucede este evento. Si por el contrario la huella no coincide con las registradas en la base de datos, el evento es rechazado para esta persona, y un registro se queda en la base de datos.

3.5 OPCIONES DE SOLUCIÓN Y ELECCIÓN DE LA ÓPTIMA

Para la construcción de un sistema de información, la elección de herramientas es muy importante, en la actualidad existen muchas opciones que facilitan esta labor. Para llevar acabo una buena elección se tienen que tomar en cuenta varios aspectos tales como el tamaño de la aplicación, el costo-beneficio, capacidad de los programadores, disponibilidad de equipo, tiempo de entrega del sistema y factores imprevistos, considerando estos factores se analizan algunas opciones de solución para posteriormente seleccionar la que mejor se ajuste a los requerimientos del sistema que se desea desarrollar.

Entre las opciones que se proponen para la implementación del Back End se encuentran: SQL Server, MySQL y Oracle. Y para el desarrollo del Front End las herramientas con que se cuenta son: Visual Basic .NET, Visual C++ .NET y Delphi para .NET. Las características de estas opciones se mencionan a continuación.

ELECCIÓN DEL BACK END

MySQL

Es un Sistemas Gestor de Bases de Datos SQL bajo la filosofía de código abierto. La desarrolla y mantiene la empresa MySQL AB pero puede utilizarse gratuitamente ya que su código fuente está disponible.

La siguiente lista describe algunas de las características más importantes de MySQL:

- Velocidad y robustez.
- API's disponibles para los siguientes lenguajes de programación: C, C++, Eiffel, Java, Perl, PHP, Python, Ruby, y Tcl.
- Multiproceso, es decir puede usar varias CPU si éstas están disponibles.
- Puede trabajar en distintas plataformas y sistemas operativos distintos.
- Proporciona transacciones, llaves externas y actualización/borrado en cascada (integridad referencial).
- Sistema de contraseñas y privilegios flexible y seguro.
- Registros de longitud fija y variable.
- Posibilidad para crear 60,000 tablas y cerca de 5 mil millones de filas.
- 64 índices por tabla, cada índice puede estar compuesto de 1 a 16 columnas.
- El servidor soporta mensajes de error en distintos idiomas.
- Provee diversos tipos de columnas como enteros, punto flotante, doble precisión, caracter, fechas, enumerados, etc.
- Los clientes se pueden conectar con el servidor de MySQL usando sockets. TCP/IP (Transmition Control Protocol/Internet Protocol - Protocolo de control de transmisión/Protocolo Internet) en cualquier plataforma.

Oracle

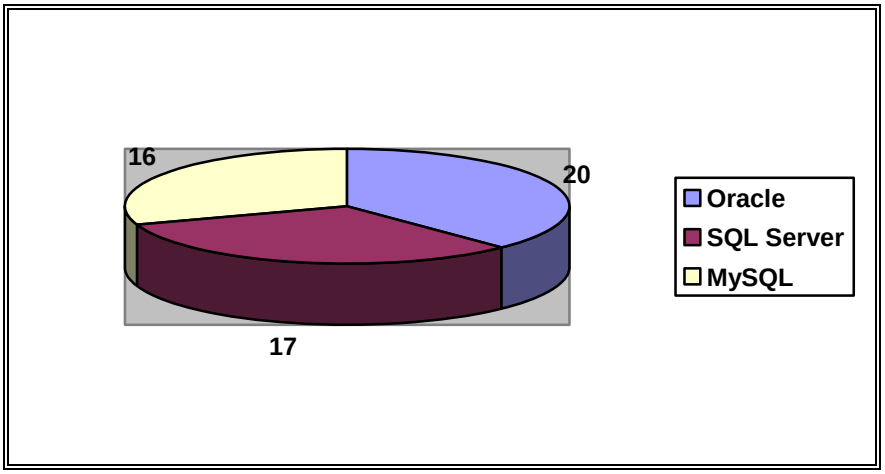
Es un DBMS fabricado por Oracle Corporation, utiliza SQL para el manejo de los datos. Es uno de los sistemas de bases de datos más completos, aunque su mayor defecto es su elevado precio. Sus principales características son:

- Manejo de varios tipos de datos como: number, char, varchar2, date, long raw, clob y blob.
- Manejo de diferentes objetos de datos como sinónimos, vistas, procedimientos almacenados, funciones, diagramas de base de datos, tablas, especificaciones de paquete y cuerpos de paquete.
- Esta provisto de un sistema de seguridad contra fallas, para limitar y monitorear el acceso a datos.
- Garantiza la integridad de los datos, llevando un control de los registros modificados dentro de una transacción.
- Soporta un gran número de conexiones de usuarios.
- Posee herramientas para desarrollo Web.
- Controla selectivamente la disponibilidad de los datos según el nivel y subnivel de la base de datos.
- Es multiplataforma.

Tabla comparativa para la elección del Back End

Características	Oracle	SQL Server	MySQL
Tipos de datos soportados	2	2	1
Estructura de índices	2	1	1
Estructura de tablas	2	2	2
Creación de Stored Procedures	2	2	-
Cursores	1	2	2

Soporte a Internet	2	1	2
Proporciona Seguridad	2	1	1
Integridad referencial	2	2	1
Escalabilidad	2	2	2
Facilidad de uso	1	2	2
Multiplataforma	2	-	2
Total	20	17	16



Bueno = 2 puntos Regular = 1 punto No aplica = -

La elección del gestor de base de datos, además de todo lo anterior, se basó en la disponibilidad comercial y en la relación costo beneficio, por lo que se determinó el utilizar SQL Server 2000 como Back End del sistema.

ELECCIÓN DEL FRONT END

Visual C++ .NET

Visual C++ .NET es un entorno integrado de desarrollo que permite la Programación Orientada a Objetos, contiene un conjunto de herramientas para la creación de aplicaciones basadas en Microsoft Windows y Microsoft .NET, aplicaciones Web dinámicas y servicios Web XML utilizando el lenguaje de programación C++. Entre sus principales características se encuentran:

- Compatibilidad con COM y con integración de código de plataformas.
- Incluye seguridad de tipos.
- Proporciona seguridad por medio de mecanismos de confianza intrínsecos del código.
- Compatible con componentes XML basados en Web y conceptos de metadatos extensibles.
- Interoperabilidad con otros lenguajes, entre plataformas y con datos heredados.
- Capacidad de control de versiones para facilitar la administración y la implementación.
- Conjunto de clases de C++ basadas en plantillas que simplifica la programación de objetos COM.
- Conjunto de clases nativas de C++ que permite crear aplicaciones Web, servicios Web XML y otras aplicaciones de servidor.
- Conjunto de plantillas para la obtención de acceso a datos OLE DB (Object Linking and Embedding for DataBases).
- Permite depurar en C/C++: Aplicaciones de consola, Archivos DLL, Aplicaciones Windows y Servicios Web XML.
- Servicios de Windows.
- Incluye las bibliotecas estándar del sector ATL (Active Template Library) y MFC (Microsoft Foundation Class).

Delphi para .NET

Delphi es un IDE diseñado para la programación de propósito general con énfasis en la programación visual, permite crear archivos ejecutables para Windows, Linux y la plataforma .NET. Es producido comercialmente por la empresa estadounidense Borland. En Delphi se utiliza como lenguaje de programación una versión mejorada de Pascal[1] llamada Object Pascal, el cual permite POO (Programación Orientada a Objetos).

[1] Lenguaje de programación de alto nivel y propósito general. Es un lenguaje procedimental, estructurado y con una gran riqueza de tipos.

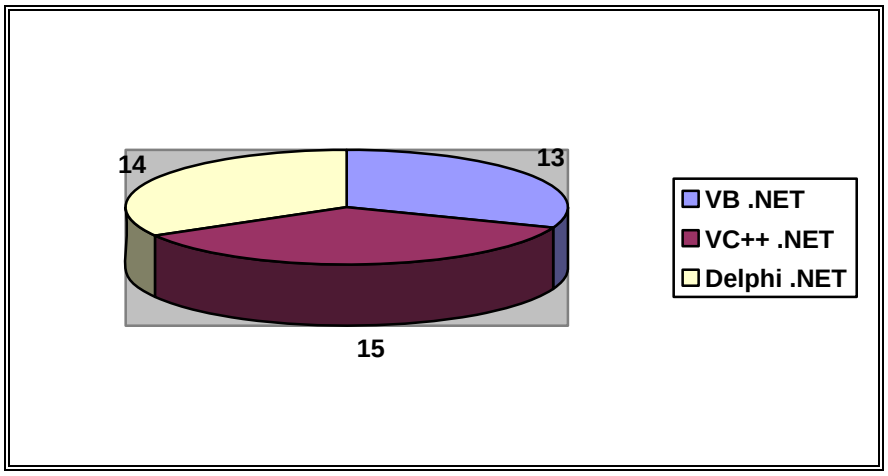
Borland Delphi para .NET Framework ofrece un entorno de desarrollo productivo y basado en estándares para el desarrollo en .NET, algunas de las características de Delphi para .NET son:

- Permite crear aplicaciones en un entorno visual con soporte para Delphi, C#, .NET, ASP .NET, VCL .NET, VCL y Win32.
- Soporte para FCL (Foundation Class Library), con clases que encapsulan funciones para acceso a datos, carga de archivos, generación de imágenes, transacciones, etc.
- Permite desarrollar componentes reutilizables, COM y ActiveX.
- Ofrece ASP .NET para crear servicios Web XML y aplicaciones HTML dinámicas basadas en formularios Web ASP .NET.
- Programación Orientada a Objetos 100%, permite encapsulamiento, herencia y polimorfismo.
- Soporte avanzado de Bases de Datos mediante BDE (Borland Database Engine), ADO (ActiveX Database Objects) y acceso nativo a InterBase, para desarrollo Cliente/Servidor.
- Componentes integrados en el lenguaje, lo que reduce considerablemente la utilización de bibliotecas y controles externos.
- Integración directa del modelado UML, el desarrollo y las fases de ejecución mediante Borland Enterprise Core Objects (ECO) para .NET.
- Incrementa la fiabilidad, la seguridad y la interoperabilidad de las aplicaciones Windows gracias a .NET Framework.
- Asistentes y componentes para Internet/Intranet.

Tabla comparativa para la elección del Front End

Características	**Visual Basic .NET**	**Visual C++ .NET**	**Delphi .NET**
Interfaz amigable	2	2	1
Facilidad de	2	1	1

programación			
Soporte cliente/servidor	2	2	2
Seguridad	1	2	2
Multiplataforma	1	2	2
Soporte a Internet	2	2	2
Programación Orientada a Objetos	2	2	2
Velocidad de ejecución	1	2	2
Total	13	15	14



Bueno = 2 puntos Regular = 1 punto

Por las características antes mencionadas, las capacidades de programación y de conocimiento del lenguaje, se eligió Visual Basic .NET para la construcción del Front End del sistema.

Capítulo 4

Desarrollo e implantación del sistema

4.1 APLICACIÓN DE LA METODOLOGÍA ELEGIDA PARA EL BACK END

En este trabajo de tesis se eligió la metodología de análisis estructurado, en donde se divide un problema complejo en componentes más pequeños y se realizan las relaciones definidas entre ellos. Esta metodología está principalmente orientada a procesos, concentrándose en las funciones del sistema requerido.

4.1.1 DIAGRAMA DE CONTEXTO

También conocido como modelo fundamental del sistema, el diagrama de contexto representa una sola burbuja o proceso, que identifica la función principal, con flujo de informaciones de entrada y salida, representadas por flechas que lo relacionan con otros sistemas y personas (terminadores). Este diagrama resume el requisito principal del sistema: recibir entradas, procesarlas de acuerdo con una demanda, generar una función y entregar salidas. La figura 4.1.1.1 muestra el diagrama de contexto del Sistema de Recuperación de Información a través de Huellas Dactilares.

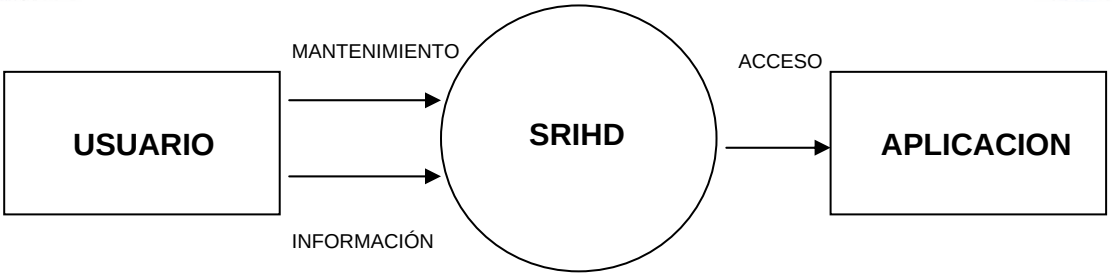


Figura 4.1.1.1. Diagrama de contexto (Nivel 0)

4.1.2 DIAGRAMA DE FLUJO DE DATOS Y DE PROCESOS

Diagramas de flujo de procesos

Una vez desarrollado el diagrama de contexto, se procede a la construcción de diagramas de flujo de procesos como se muestra en la figura 4.1.2.1, en él se define a mayor escala de detalles los flujos de información y procesos de transformación que ocurren en el sistema.

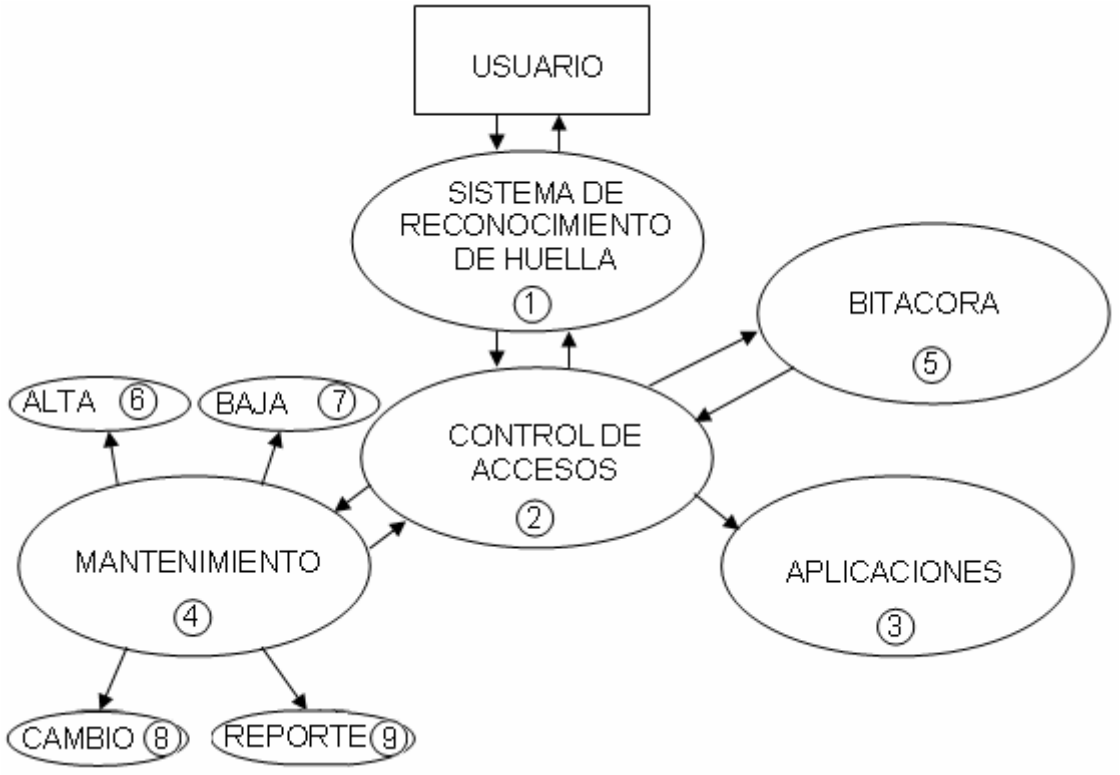


Figura 4.1.2.1. Diagrama de flujo de procesos (Nivel 1)

Los procesos que se muestran son los siguientes:

- Bitácora. Este proceso almacena el registro de acceso y acciones de los usuarios al sistema, informando que usuario accedió y cuándo lo hizo. Es importante en todo sistema de información poder auditar los accesos para prevenir daños a la información.
- Mantenimiento. El administrador del sistema se encarga de introducir los datos de los usuarios para poder acceder a manipular la información y otorga permisos de acceso a la información.
- Control de acceso. Una vez que el usuario existe en la base de datos, es posible asignar un perfil de seguridad y de esta manera se controla el acceso a los datos.

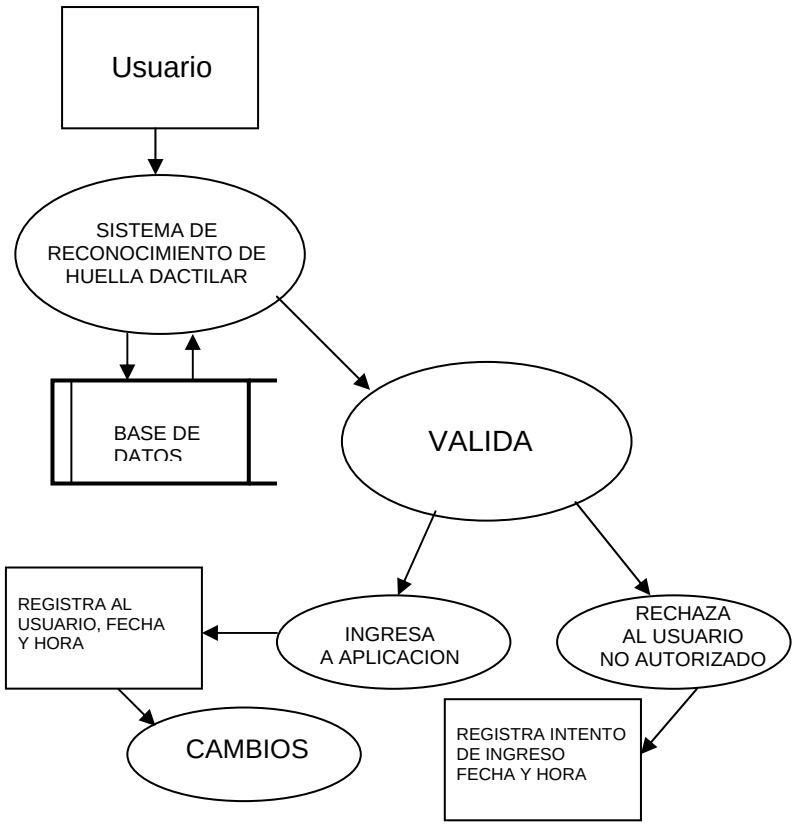


Figura 4.1.2.2. Diagrama de flujo de procesos para la bitácora de accesos al sistema y/o la aplicación (Nivel 2)

En la figura 4.1.2.2 se visualiza el proceso de Bitácora, el cual es de suma importancia para supervisar y administrar el acceso y la recuperación de información de los usuarios mediante la huella dactilar.

La figura 4.1.2.3 se muestra como el usuario se valida antes de poder hacer modificaciones a los registros de los datos y los programas, en caso de que no exista el usuario, este no tiene acceso a la aplicación, en este procedimiento se puede dejar opcional que el usuario pueda o no ser dado de alta.

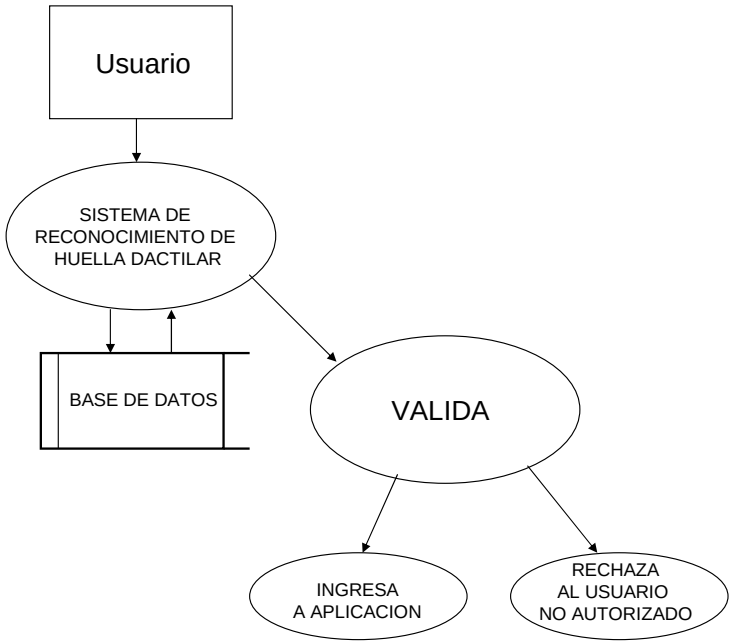


Figura 4.1.2.3. Diagrama de flujo de procesos para la validación (Nivel 3)

En la figura 4.1.2.4 se esquematiza el flujo de información en el procedimiento que es único para el administrador del sistema, desde la etapa de diseño de la misma, se ha optado por hacer lo más seguro en su mantenimiento, para ello sólo el administrador es quien puede asignar los perfiles dadas las contraseñas y las huellas de los usuarios.

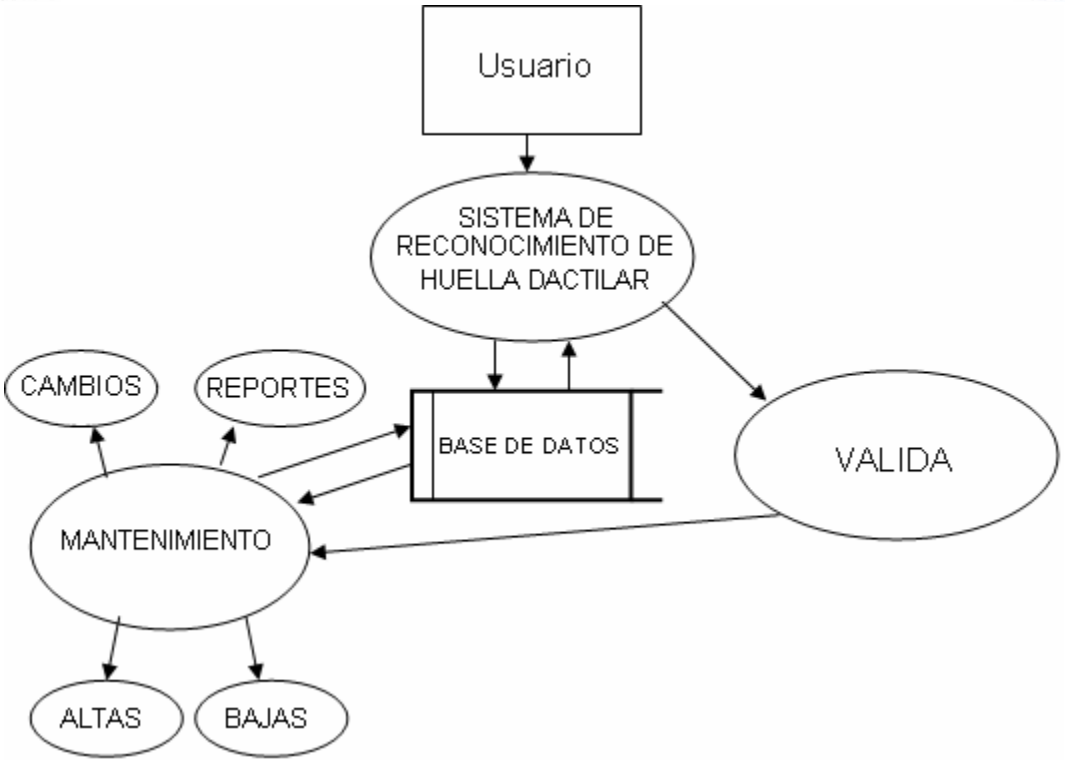


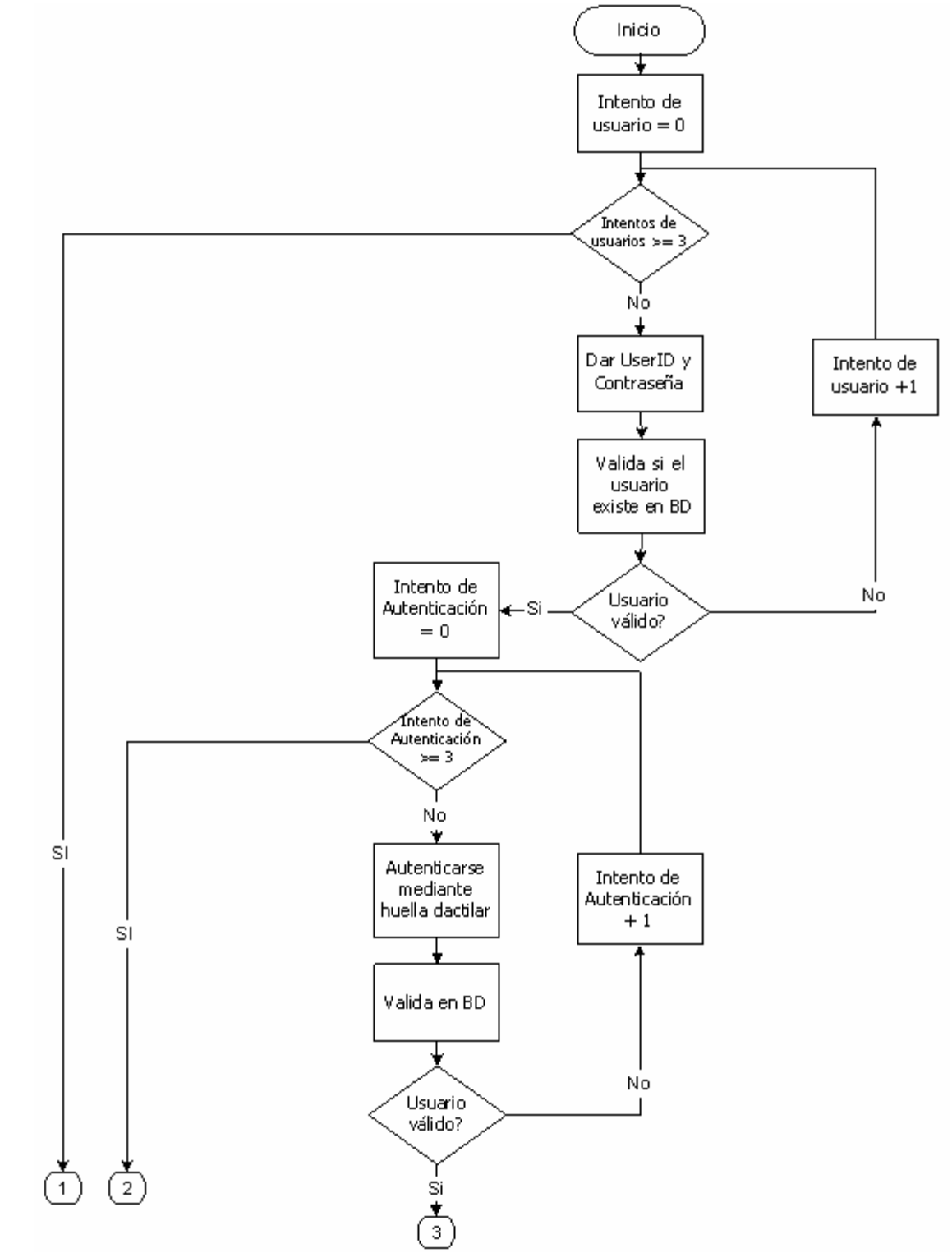
Figura 4.1.2.4. Diagrama de flujo de procesos del mantenimiento de la base de datos

Diagramas de flujo de datos

Todo usuario tendrá que validarse en primera instancia mediante el uso de UserID y contraseña, esta información es cotejada en la base de datos, para saber si existe, el usuario tiene tres intentos para dar correctamente la información solicitada, en caso de superar el número de intentos el sistema no permite la entrada al usuario. Si el usuario existe en la base de datos, entonces tendrá que autenticarse mediante la huella dactilar, de igual manera se otorgan tres intentos.

Cuando el sistema ha validado el UserID, contraseña y huella dactilar, se detecta si el usuario tiene permisos de administrador o no. Si el usuario no tiene permisos de administrador, este sólo accede al sistema, donde se registra la hora y fecha de ingreso. Si el usuario tiene permisos de administrador, se le presenta un menú con las opciones de acceso a la aplicación, acceso a bitácora o dar mantenimiento al

sistema, donde se encuentran las opciones de dar de alta a un nuevo usuario, bajas y modificaciones o cambios (figura 4.1.2.5).



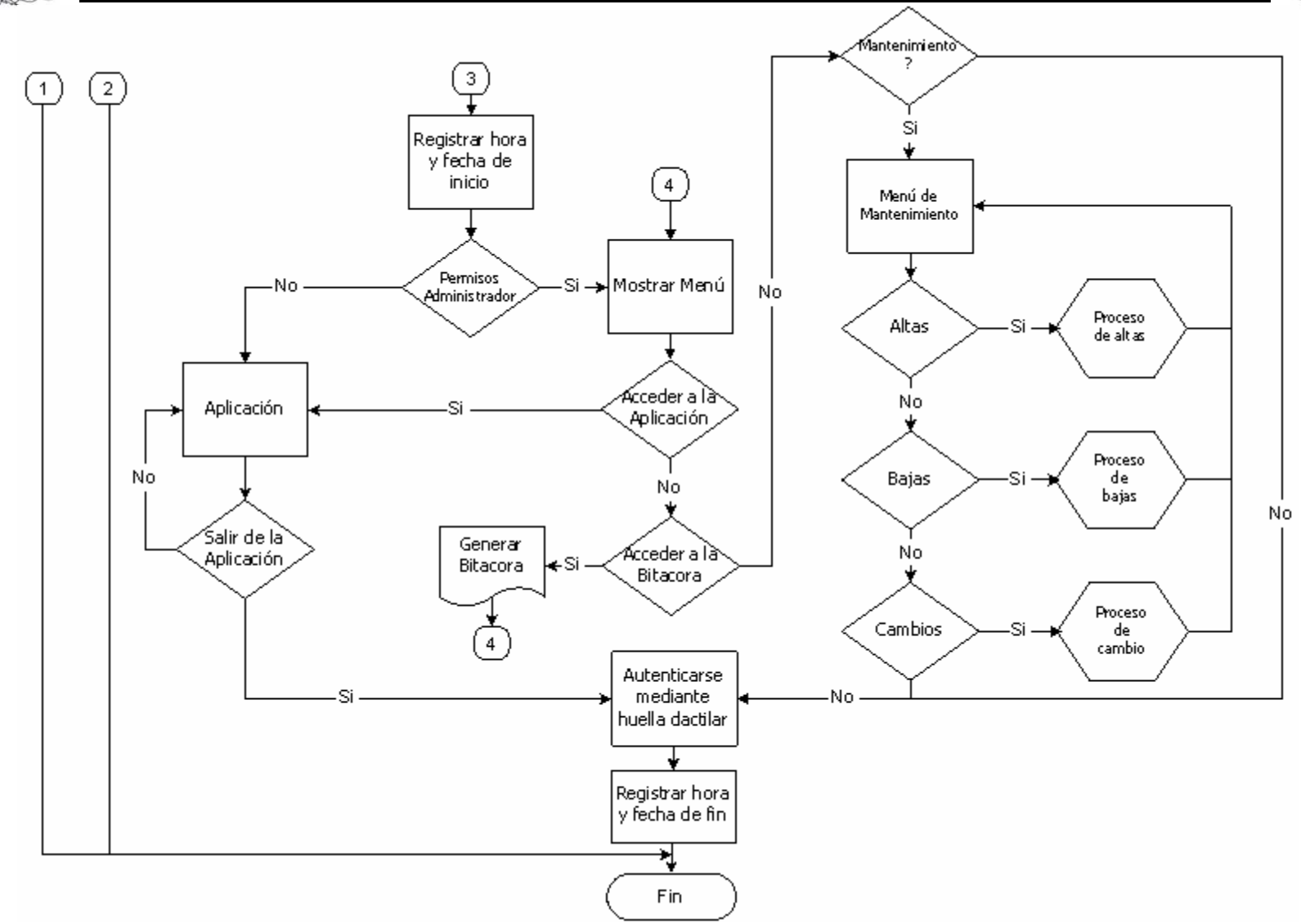
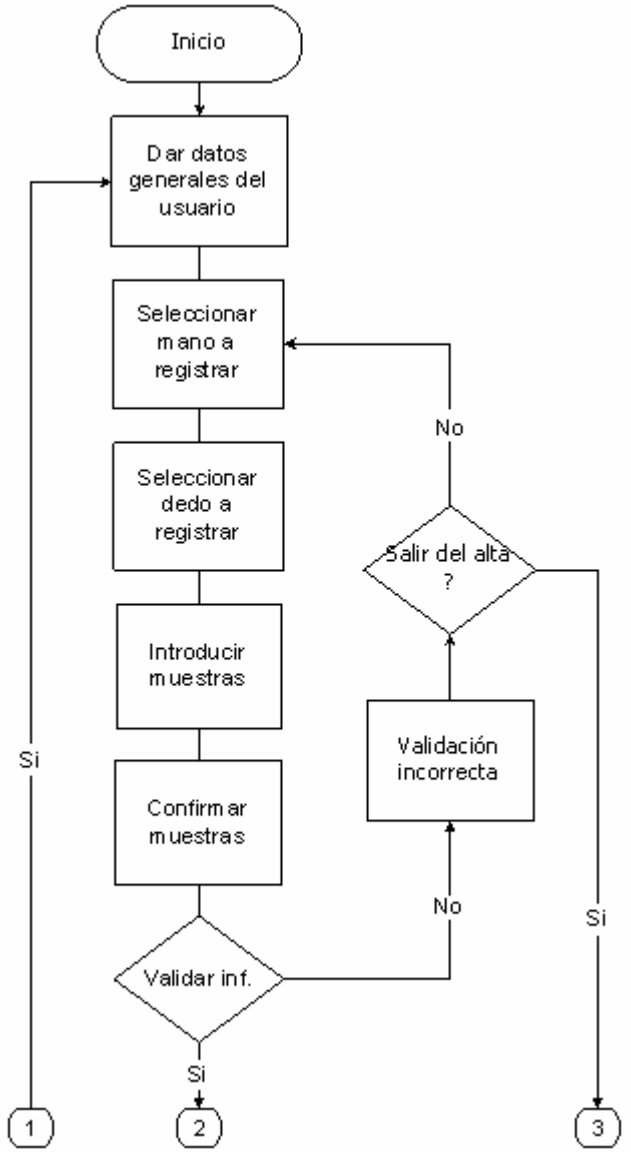


Figura 4.1.2.5. Diagrama de flujo de datos del SRIHD

Proceso de altas

En el proceso de Altas, se ingresan los datos generales del nuevo usuario a dar de alta, posteriormente se selecciona la mano y el dedo de donde se tomará la información para guardar la huella dactilar en la base de datos, la información se toma y se valida, si durante el paso de validación no se presentan errores, la información del usuario se da de alta en la base de datos, si se presentan errores se tiene que comenzar el proceso nuevamente (figura 4.1.2.6).



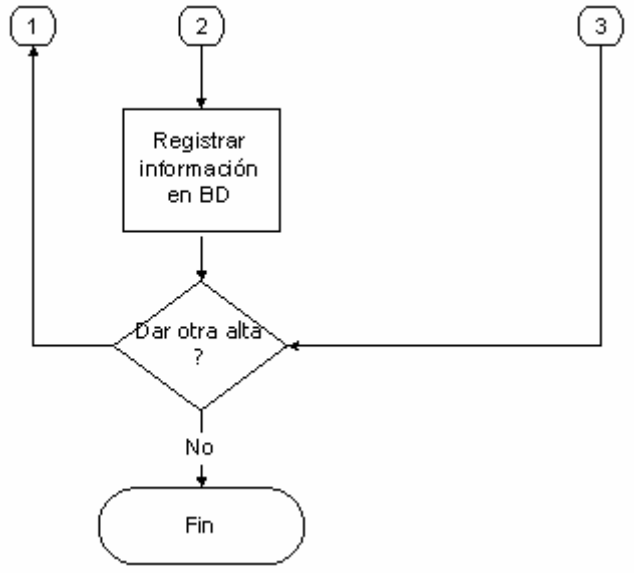
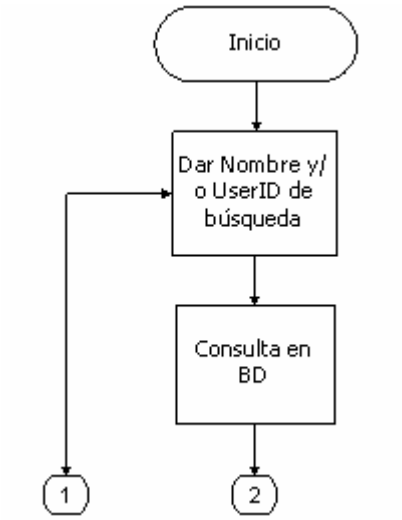


Figura 4.1.2.6. Proceso de altas

Proceso de bajas

Para este proceso, se otorga información del usuario que se desea dar de baja, si esta información existe en la base de datos se muestra en pantalla y se solicita una confirmación, si esta confirmación se da, el usuario dueño de esa información es eliminado del sistema y se da la opción de realizar una nueva búsqueda para eliminar más usuarios de la base de datos. En dado caso que la información buscada no exista se envía un mensaje de error en la eliminación (figura 4.1.2.7).



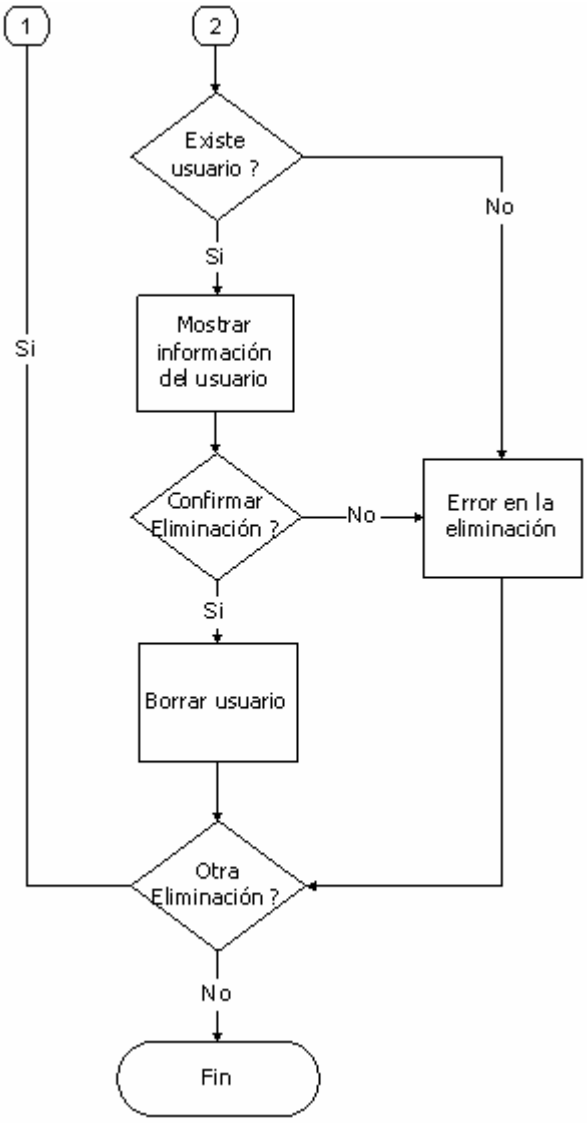


Figura 4.1.2.7. Proceso de bajas

Proceso de cambios

Aquí nuevamente se comienza con una búsqueda del usuario que se desea modificar, si este se encuentra en la base de datos se proporciona la opción de realizar cambios, después de realizar los cambios necesarios, estos son guardados en la base de datos. Si en la búsqueda del usuario no se encuentran información, se muestra un mensaje de usuario no existente (figura 4.1.2.8).

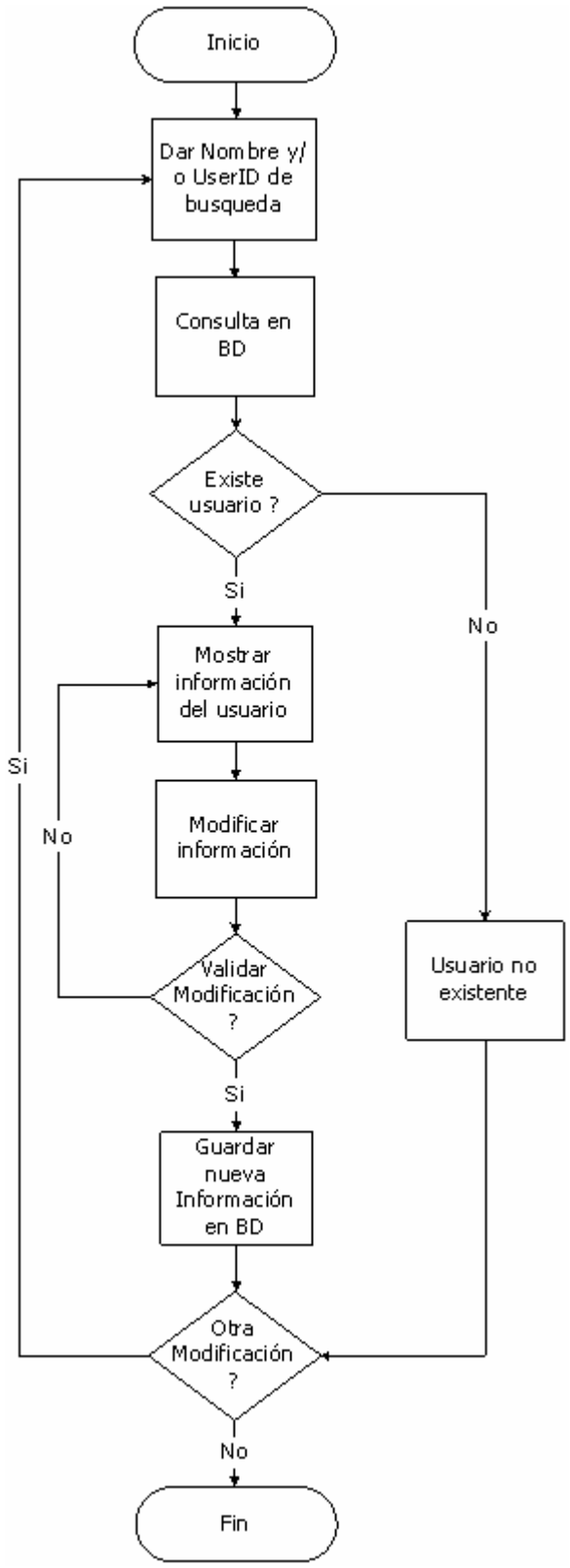


Figura 4.1.2.8. Proceso de cambios

4.1.3 DICCIONARIO DE DATOS

Es un catálogo que contiene información de los elementos en una base de datos. Como su nombre lo sugiere, estos elementos se centran alrededor de los datos y la forma en que están estructurados para satisfacer los requerimientos de los usuarios y las necesidades de la organización. En un diccionario de datos se encuentra la lista de todos los elementos que forman parte del flujo de datos en todo el sistema. El diccionario guarda los detalles y descripciones de todos estos elementos.

El diccionario de datos se desarrolla durante el análisis de flujo de datos y sirve para auxiliar a los analistas que participan en la determinación de los requerimientos de sistemas.

Importancia del diccionario de datos

El diccionario de datos se utiliza por cinco razones importantes:

- Para manejar los detalles en sistemas grandes.
- Para comunicar un significado común para todos los elementos del sistema.
- Para documentar las características del sistema.
- Para facilitar el análisis de los detalles con la finalidad de evaluar las características y determinar dónde efectuar cambios en el sistema.
- Localizar errores y omisiones en el sistema.

El diccionario contiene dos tipos de elementos, datos y estructuras de datos. Los elementos de datos se agrupan para formar una estructura de datos.

- Elemento dato.

  El nivel más importante de datos es el elemento dato (otros nombres que se le dan a este término son: campo dato o parte elemental.). Los elementos dato son los bloques básicos para todos los demás datos del sistema. Por si mismo conllevan suficiente significado para los usuarios.

- Estructuras de datos.

  Una estructura de datos es un grupo de datos elementales que están relacionados con otros y que en conjunto describen un componente del sistema (tablas).

La base de datos DB_HUELLAS cuenta con cinco tablas (o entidades) principales

- PERSONA
- USUARIO
- PER_HUELLAS
- PER_HUELLAS_BIT
- PER_HUELL_BITACC

A continuación se describe el diccionario de datos de cada una de estas tablas.

En la tabla PERSONA se almacenan los datos personales de los usuarios que se registrarán en el sistema SRIDH (tabla 4.1.3.1).

Nombre	Acrónimo	Tipo y longitud	Tipo Llave	Admite Null	Tabla con que se asocia	Descripción
Identificador de persona	Id_persona	Number(8)	Primaria	No		Identificador de cada persona
Nombre de usuario	Nombre	Varchar(40)		No		Nombre de la persona
Apellido paterno	Apellido_pat	Varchar(20)		No		Apellido paterno de la persona
Apellido materno	Apellido_mat	Varchar(20)		No		Apellido materno de la persona
Sexo	Cve_sexo	Varchar(1)		No		Femenino o masculino
Fotografía	Fotografia	Varchar(120)		No		Ubicación de la fotografía del usuario
Estado civil	Estado_civil	Varchar(12)		Sí		Estado civil de la persona registrada
Fecha de nacimiento	F_nacimiento	Datetime		Sí		Fecha de nacimiento de cada persona
Clave Única de Registro de Población	CURP	Varchar(18)		Sí		Clave Única de Registro de Población de cada persona
Registro Federal de Contribuyentes	RFC	Varchar(14)		Sí		RFC de cada persona
Profesión	Profesion	Varchar(30)		Sí		Profesión de la persona
Teléfono de domicilio	Telef_casa	Varchar(14)		Sí		Número telefónico particular
Teléfono de oficina	Telef_oficina	Varchar(14)		Sí		Número telefónico de trabajo
Correo electrónico	E_mail	Varchar(40)	No	Sí		Dirección de correo electrónico del usuario

Tabla 4.1.3.1. Tabla PERSONA

La tabla de USUARIO (tabla 4.1.3.2) sirve para guardar los datos de un usuario, como son el tipo de usuario, el login y la contraseña.

Nombre	Acrónimo	Tipo y longitud	Tipo Llave	Admite Null	Tabla con que se asocia	Descripción
Identificación de usuario	Id_usuario	Number(8)	Primaria	No	Persona	Identificador de cada usuario
Identificador de persona	Id_persona	Number(8)	Foránea	No		Identificador de la persona
Login	Login	Varchar(10)		No		Login de cada usuario
Contraseña	Pwd	Varchar(10)		No		Contraseña de cada usuario
Clave del tipo de usuario	Cve_tipo_usr	Varchar(6)		No		Tipo de usuario (Administrador o Usuario)

Tabla 4.1.3.2. Tabla USUARIO

En la tabla 4.1.3.3 se muestra la estructura de la tabla PER_HUELLAS, esta entidad contendrá la información de las huellas dactilares de cada persona.

Nombre	Acrónimo	Tipo y longitud	Tipo Llave	Admite Null	Tabla con que se asocia	Descripción
Identificación de persona	Id_persona	Number(8)	Primaria Foránea	No	Persona	Identificador de cada persona
Clave de mano	Cve_mano	Varchar(6)	Primaria	No		Clave de la mano que se registra
Clave de dedo	Cve_dedo	Varchar(6)	Primaria	No		Clave del dedo que se registra
Clave de situación	Cve_situación	Varchar(6)	No	No		Estado en el que se encuentra la huella (Activa o Inactiva)
Texto de huella	Tx_huella	Varbinary(2048)	No	Sí		Campo donde se almacenan los datos de la huella dactilar

Tabla 4.1.3.3. Tabla PER_HUELLAS

La tabla 4.1.3.4 muestra el diccionario de datos de la tabla PER_HUELLAS_BIT, en dicha tabla se registran las acciones que se realizan sobre las huellas dactilares, altas, bajas y modificaciones

Nombre	Acrónimo	Tipo y longitud	Tipo Llave	Admite Null	Tabla con que se asocia	Descripción
Identificación de persona	Id_persona	Number(8)	Primaria Foránea	No	Per_huellas	Identificador de cada persona
Clave de mano	Cve_mano	Varchar(6)	Primaria Foránea	No	Per_huellas	Clave de la mano que se registra
Clave de dedo	Cve_dedo	Varchar(6)	Primaria Foránea	No	Per_huellas	Clave del dedo que se registra
Identificador de huella	Id_huella	Number(8)	Primaria	No		Identificador de cada huella
Clave de la acción	Cve_accion	Varchar(6)		No		Clave de la acción que se realiza (Registro, modificación o eliminación)
Fecha de acción	Fh_accion	Datetime		No		Fecha de la acción que se ejecuta
Clave de usuario alta	Cve_usu_alta	Varchar(8)		Sí		Clave de usuario que da de alta el registro
Clave de usuario modifica	Cve_usu_modif	Varchar(8)		Sí		Clave de usuario que modifica el registro

Tabla 4.1.3.4. Tabla PER_HUELLAS_BIT

La tabla. 4.1.3.5 muestra el diccionario de datos de la entidad PER_HUELL_BITACC, en esta tabla se lleva la bitácora de accesos al sistema.

Nombre	Acrónimo	Tipo y longitud	Tipo Llave	Admite Null	Tabla con que se asocia	Descripción
Identificador de persona	Id_persona	Number(8)	Primaria Foránea	No	Persona	Identificador de persona
Identificador de bitácora	Id_bitacora	Number(8)	Primaria	No		Identificador de bitácora
Número de intentos	Num_intentos	Numerico(2)		No		Número de intentos para acceder a la aplicación
Acceso de entrada	B_acceso_e	Varchar(1)		No		Indica si el acceso es exitoso o no
Clave de la Aplicación	Cve_aplicacion	Varchar(10)		No		Clave de la aplicación a la que se tiene acceso
Fecha de bitácora	Fh_bitacora	Datetime		Sí		Fecha del intento de acceso
Identificador de usuario	Id_usu_acceso	Number(8)		Sí		Identificador del usuario que intenta acceder

Tabla 4.1.3.5. Tabla PER_HUELL_BITACC

4.1.4 DIAGRAMA ENTIDAD-RELACIÓN

Una entidad caracteriza a un tipo de objeto, real o abstracto, del problema a modelar. Toda entidad tiene existencia propia, es distinguible del resto de las entidades, tiene nombre y posee atributos definidos en un dominio determinado. Una entidad es todo aquello de lo que se desea almacenar información. En el diagrama E-R las entidades se representan mdiante rectángulos. El diagrama Entidad-Relación de la base DB_HUELLAS se muestra en la figura 4.1.4.1.

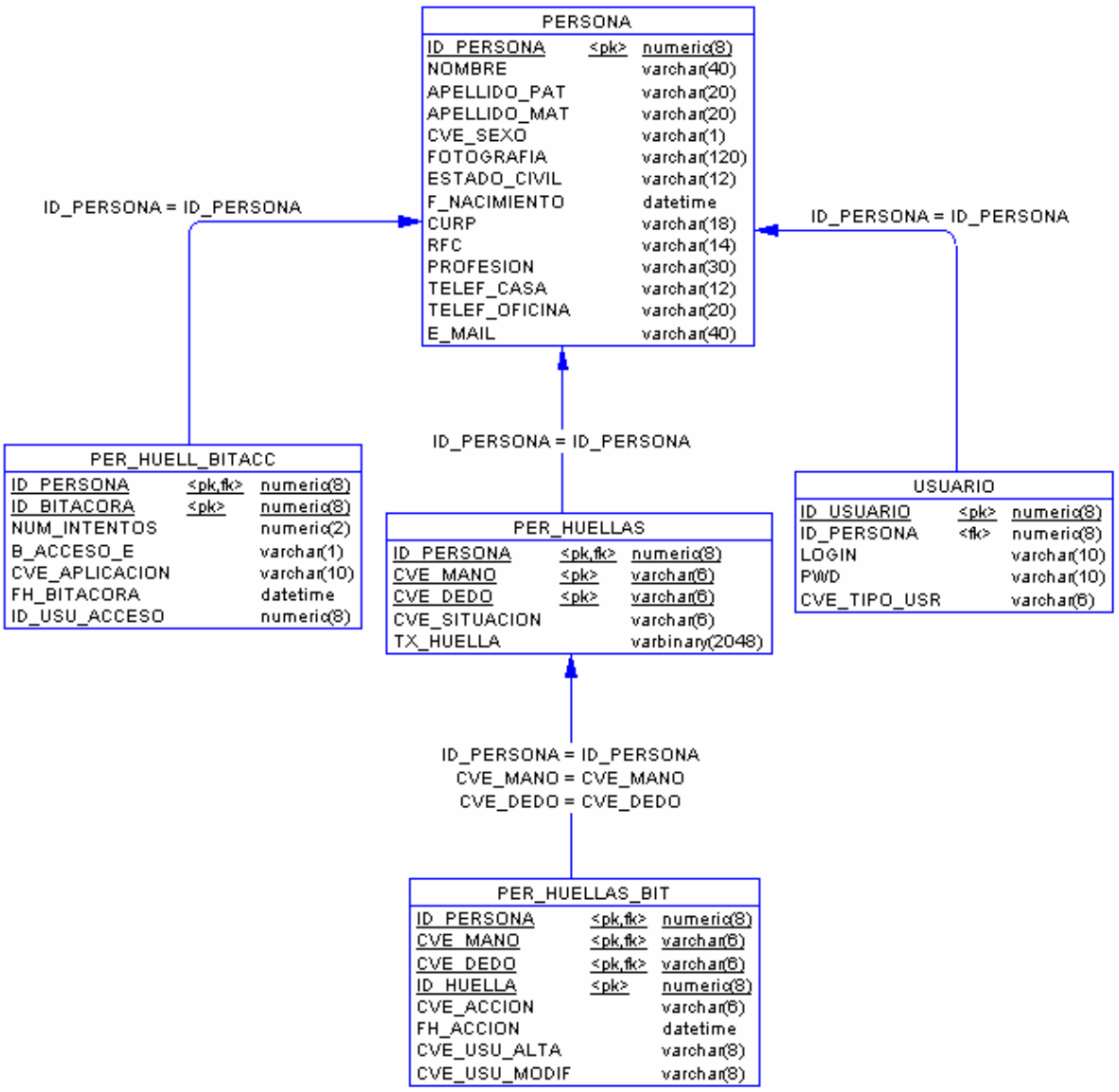


Figura 4.1.4.1. Diagrama Entidad-Relación de la base DB_HUELLAS

Una relación es una asociación o relación matemática entre varias entidades. Las relaciones también se nombran. Se representan en el diagrama E-R mediante flechas. Cada entidad interviene en una relación con una determinada cardinalidad.

La cardinalidad (número de instancias o elementos de una entidad que pueden asociarse a un elemento de la otra entidad relacionada) se representa mediante una pareja de datos, en minúsculas, de la forma *(cardinalidad mínima, cardinalidad máxima)*, asociada a cada uno de las entidades que intervienen en la relación. Son posibles las siguientes cardinalidades: *(0,1), (1,1), (0,n), (1,n), (m,n)*.

4.1.5 NORMALIZACIÓN

El proceso de normalización es un estándar que consiste, básicamente, en un proceso de conversión de las relaciones entre las entidades, evitando:

- La redundancia de los datos: repetición de datos en un sistema.
- Anomalías de actualización: inconsistencias de los datos como resultado de datos redundantes y actualizaciones parciales.
- Anomalías de borrado: pérdidas no intencionadas de datos debido a que se han borrado otros datos.
- Anomalías de inserción: imposibilidad de adicionar datos en la base de datos debido a la ausencia de otros datos.

Antes de proceder a la normalización de cada una de las tablas, primero se debe definir una clave, esta clave debe contener un valor único para cada registro (no podrán existir dos valores iguales en toda la tabla) y podrá estar formado por un único campo o por un grupo de campos. Una vez definida la clave es posible obtener la primera forma normal. A continuación se aplican las tres formas normales a algunas de las tablas del sistema.

Primera forma normal (1NF)

Una tabla se encuentra en primera forma normal (1NF) si y solo si cada uno de los campos contiene un único valor para un registro determinado.

Se tiene una tabla (tabla 4.1.5.1) que contiene la información de las personas y registro de huellas. Se observa que no cumple con la primera forma normal

Id_persona	Nombre	Cve_dedo	Cve_mano
0003	Javier Alberto	P	Derecha
0004	Maria Elena	P, I	Izquierda
0005	Maria De Los Angeles	P	Derecha
0006	Ma. Sara Andrea	P, I	Derecha

Tabla 4.1.5.1. Tabla sin normalizar

Aplicando la primera forma normal se obtienen las siguientes tablas (ver tabla 4.1.5.2 y tabla 4.1.5.3):

Id_persona	Nombre
0003	Javier Alberto
0004	Maria Elena
0005	Maria De Los Angeles
0006	Ma. Sara Andrea

Tabla 4.1.5.2. Aplicando 1FN

Id_persona	Cve_dedo	Cve_mano
0003	P	Derecha
0004	P	Izquierda
0004	I	Izquierda
0005	P	Derecha
0006	P	Derecha
0006	I	Derecha

Tabla 4.1.5.3. Tabla normalizada

Segunda Forma Normal (2NF)

La segunda forma normal compara todos y cada uno de los campos de la tabla con la clave definida. Si todos los campos dependen directamente de la clave se dice que la tabla está es segunda forma normal (2NF).

Id_persona	Id_depto	Nombre	Departamento	Años
0001	06	Javier Alberto	Contabilidad	6
0002	03	Maria Elena	Sistemas	3
0003	02	Maria De Los Angeles	Recursos humanos	1
0004	03	Ma. Sara Andrea	Sistemas	10

Tabla 4.1.5.4. Tabla de usuarios

Tomando como punto de partida la tabla 4.1.5.4, su clave está formada por los campos código de la persona y código de departamento. El campo nombre no depende funcionalmente de toda la clave, sólo depende del código del empleado.

El campo departamento no depende funcionalmente de toda la clave, sólo del código del departamento. El campo años sí depende funcionalmente de la clave ya que depende del código del empleado y del código del departamento (representa el número de años que cada empleado ha trabajado en cada departamento). Por tanto, al no depender todos los campos de la totalidad de la clave la tabla no está en segunda forma normal.

Id_persona	Nombre
1	Javier Alberto
2	Maria Elena
3	María De Los Angeles
4	Ma. Sara Andrea

Tabla 4.1.5.5. 2FN

Id_depto	Departamento
2	Recursos humanos
3	Sistemas
6	Contabilidad

Tabla 4.1.5.6. 2FN

Id_persona	Id_depto	Años
1	6	6
2	3	3
3	2	1
4	3	10

Tabla 4.1.5.7. 2FN

Se puede observar que ahora sí se encuentran las tres tablas en segunda forma normal, considerando que la tabla 4.1.5.5 tiene como índice el campo Id_persona, la tabla 4.1.5.6 Id_depto y la tabla 4.1.5.7 una clave compuesta por los campos Id_persona e Id_depto.

Tercera forma normal (3NF)

Se dice que una tabla está en tercera forma normal si y sólo si los campos de la tabla dependen únicamente de la clave, dicho en otras palabras los campos de las tablas no dependen unos de otros. Utilizando la tabla 4.1.5.8.

Id_persona	Nombre	Cve_dedo	Cve_mano	Id_bitacora
0003	Javier Alberto	P	Derecha	05
0004	Maria Elena	P	Izquierda	06
0004		I	Izquierda	
0005	Maria De Los Angeles	P	Derecha	07
0006	Ma. Sara Andrea	P	Derecha	08
0006		I	Derecha	

Tabla 4.1.5.8. Tabla sin normalizar

Id_persona	Nombre
0003	Javier Alberto
0004	Maria Elena
0004	Maria Elena
0005	Maria De Los Angeles
0006	Ma. Sara Andrea
0006	Ma. Sara Andrea

Tabla 4.1.5.9. 3FN

Cve_dedo	Cve_mano	Id_bitacora
P	Derecha	05
P	Izquierda	06
P	Derecha	07
P	Derecha	08

Tabla 4.1.5.10. 3FN

En las tablas anteriores 4.1.5.9 y 4.1.5.10 se aplicó la tercera forma normal donde se ve la dependencia de los campos, es decir en la tabla 4.1.5.9 los campos Id_persona y nombre dependen directamente. El Id_bitácora, aunque en parte también depende de la persona, está más ligado a las claves de la mano y dedo que la persona está utilizando.

4.2 DISEÑO Y CONSTRUCCIÓN DEL BACK END

Para la construcción del Back End del sistema se utilizó SQL Server 2000. A continuación se describe el procedimiento para crear una base de datos utilizando el **Administrador Corporativo** de SQL Server, el nombre de la base donde se almacenará toda la información será **DB_HUELLAS**, (figura 4.2.1), los pasos a seguir son:

- Expandir un grupo de servidores y después seleccionar un servidor.
- Clic con el botón secundario del ratón en **Bases de datos** y a continuación, en **Nueva base de datos**.
- Se especifica el nombre para la base de datos y dejar los valores predeterminados para **Archivos de datos** y **Registro de transacciones**.

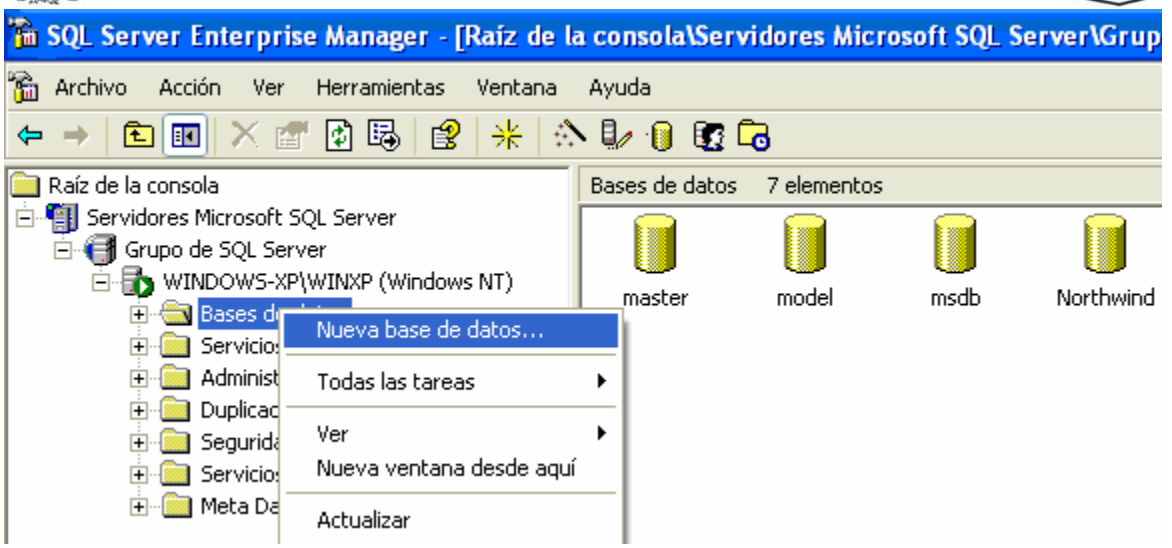


Figura 4.2.1. Creación de la base de datos DB_HUELLAS

Una vez creada la base de datos, se crean las tablas donde se almacenará la información, como se mencionó anteriormente, la base contendrá cinco tablas:

- PERSONA
- USUARIO
- PER_HUELLAS
- PER_HUELLAS_BIT
- PER_HUELL_BITACC

Las tablas se crearán mediante código desde el **Analizador de consultas** de SQL Server, como se muestra en la figura 4.2.2.

Para simplificar esta tarea se utilizó el software PowerDesigner, el cuál permite crear el modelo de la base de datos relacional de una forma gráfica y sencilla, pasando después todo a código Transact-SQL (código que puede interpretar SQL Server 2000 para la creación de las tablas), señalando cuáles atributos funcionan como llaves primarias, cuáles como llaves foráneas, restricciones, el tipo y la longitud del dato de cada campo.

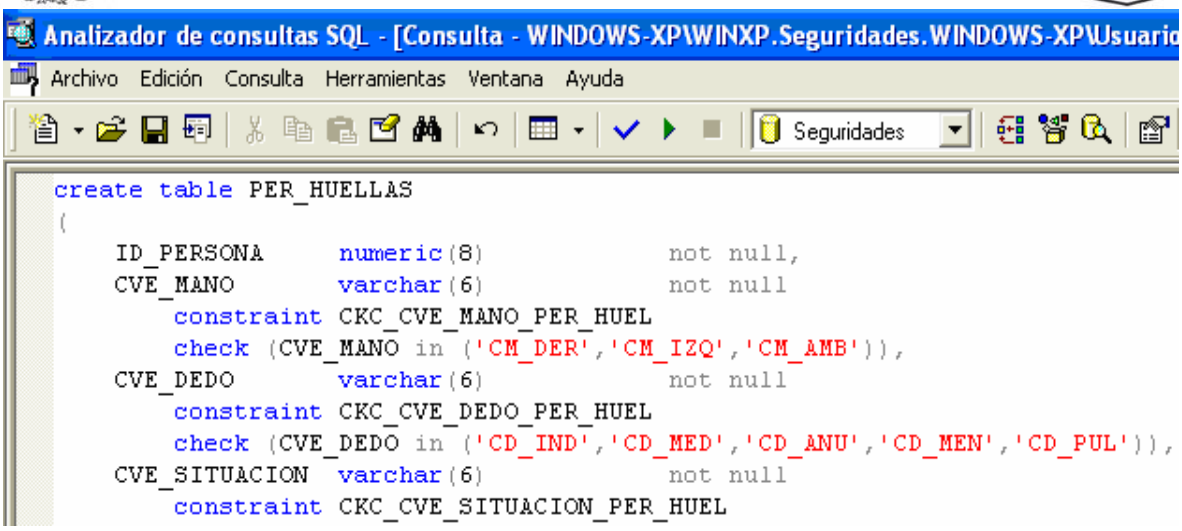


Figura 4.2.2. Creación de la tabla PER_HUELLA mediante el Analizador de consultas

En la figura 4.2.3 se muestra un ejemplo del diseño y construcción de la tabla PER_HUELLAS_BIT con PowerDesigner.

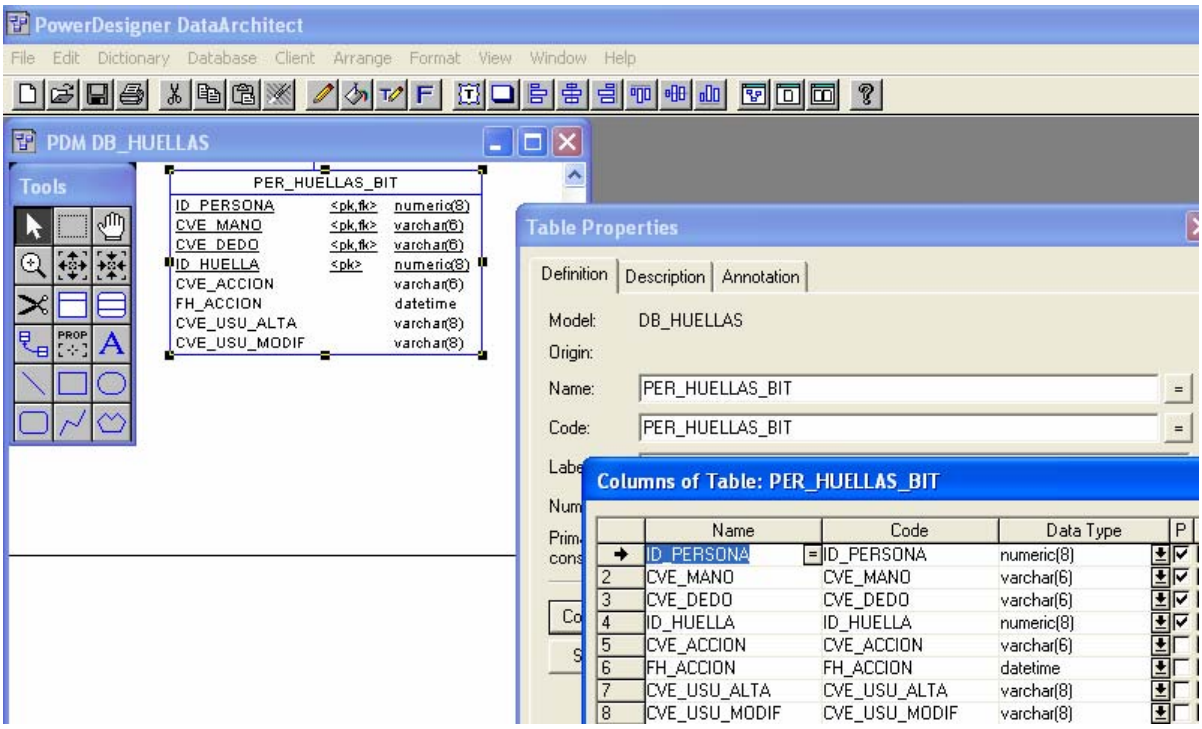


Figura 4.2.3. Creación de las tablas con ayuda de PowerDesigner

Una vez que se diseñaron todas las tablas con sus especificaciones y las relaciones que existen entre ellas, se genera el código con una herramienta que tiene este software (menú **Database** -> **Generate Database** -> **Generate Script**), la cual se muestra en la figura 4.2.4.

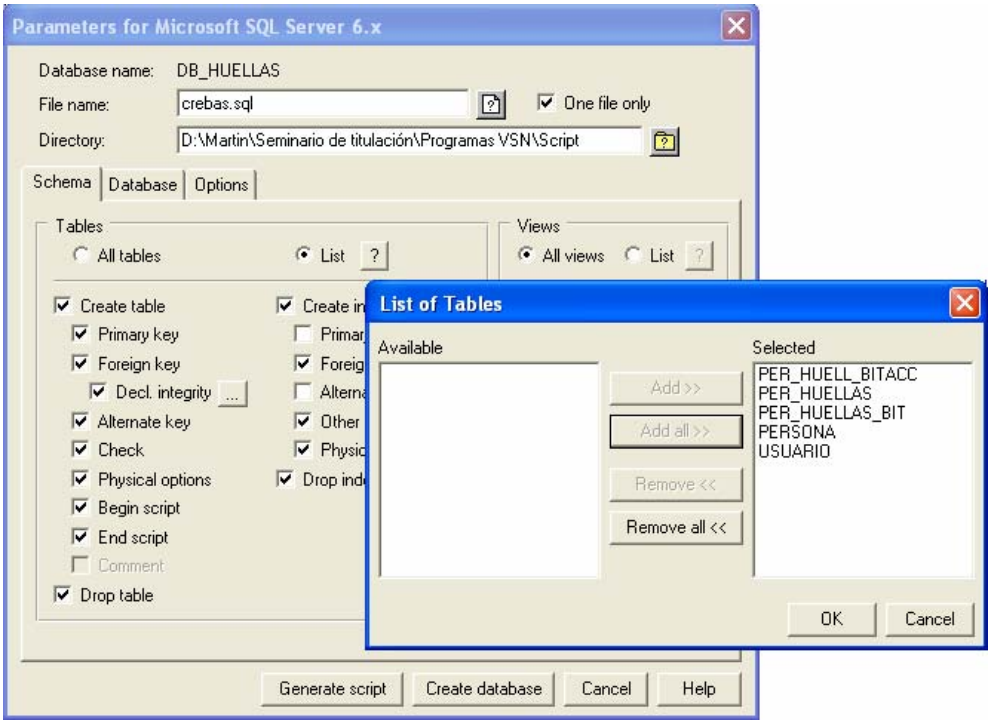


Figura 4.2.4. Creación del código SQL con PowerDesigner

Una vez generado el código, se inserta en el **Analizador de consultas** del servidor SQL Server y se genera la base de datos, con lo que se puede ahora insertar los datos correspondientes a cada una de las tablas.

También se pueden crear las tablas por medio del **Administrador Corporativo** de SQL Server, en el que se establecen cada uno de los campos de la tabla, asignándole el nombre y sus características, datos que contendrá, tamaño, descripción, formato, etc. La pantalla que presenta el programa para tal efecto es la que se ve en la figura 4.2.5.

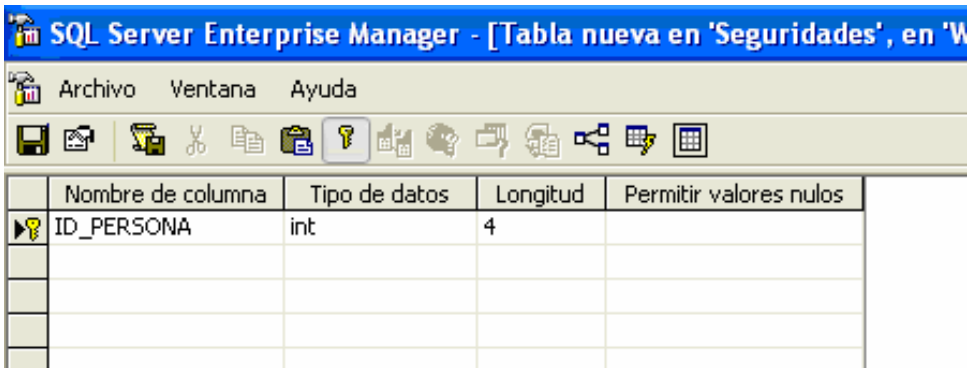


Figura 4.2.5. Creación de una tabla en SQL Server

En la primera columna (**Nombre de columna**) se escribe el nombre con el que se quiere identificar a dicho campo.

En **Tipo de datos**, se selecciona de una lista predeterminada el tipo de datos que almacenará el campo, entre las opciones están las siguientes; binary, char, datetime, decimal, float, int, money, real, text, varchar, entre otros.

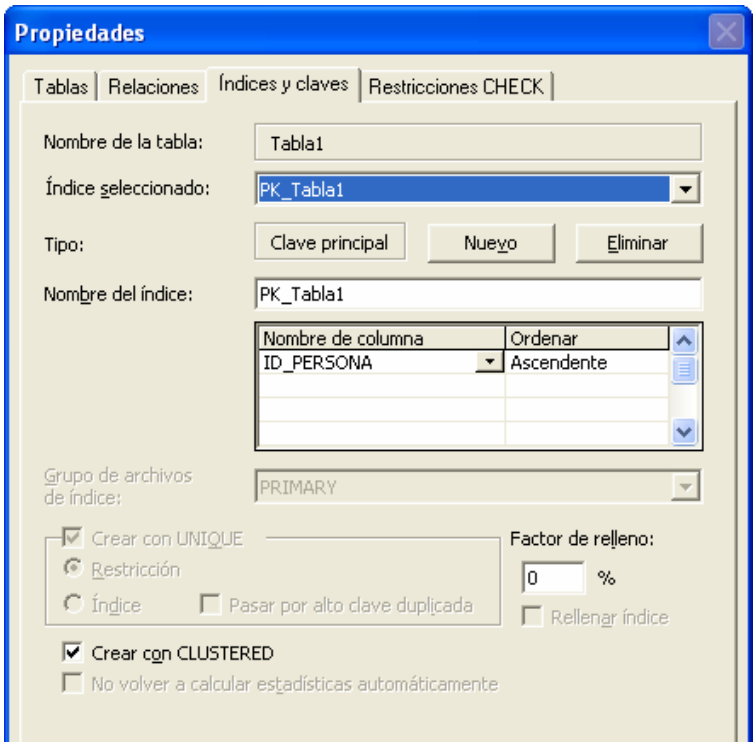


Figura 4.2.6. Asignación de una llave primaria y llave foránea a una tabla

Además de indicar el nombre y el tipo de dato de los campos de la tabla, también se debe indicar la llave primaria, llaves foráneas y las restricciones, este proceso se ilustra en la figura 4.2.6.

En la figura 4.2.7 se puede observar el árbol final de tablas de la base DB_HUELLAS.

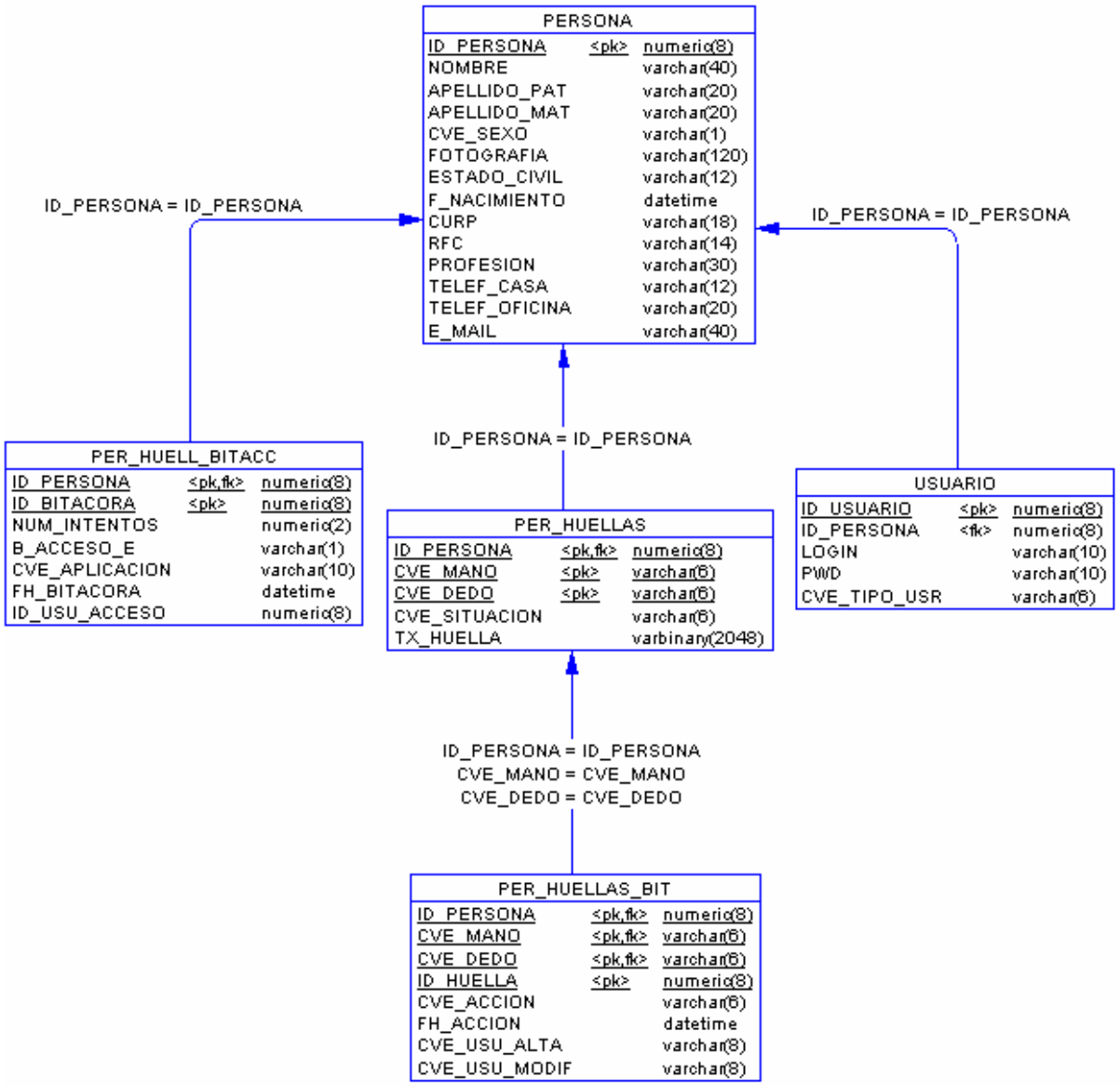


Figura 4.2.7. Árbol final de tablas de la base de datos DB_HUELLAS

Para obtener los datos de alguna de las tablas, se puede hacer mediante el **Analizador de consultas** de SQL Server 2000. Una vez que se ha seleccionado el servidor al que se desea conectar, y la base sobre la cual se va a trabajar (en este caso DB_HUELLAS), se escribe la instrucción y se ejecuta para obtener los resultados (menú **Consulta** -> **Ejecutar** o con la tecla F5), como lo ilustra la figura 4.2.8.

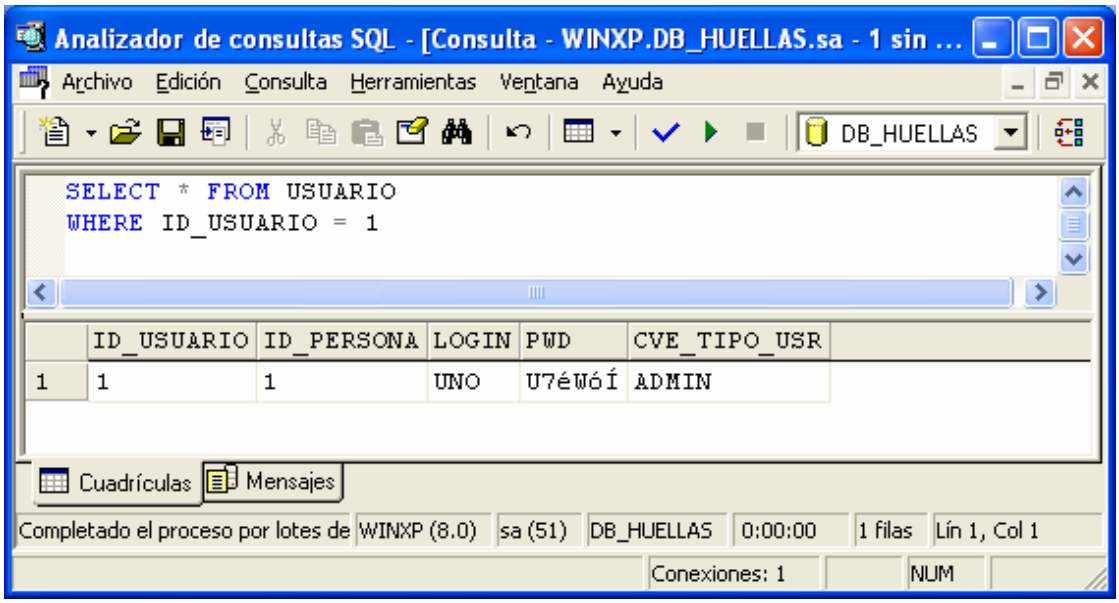


Figura 4.2.8. Consulta de información mediante el Analizador de consultas

4.3 DISEÑO Y CONSTRUCCIÓN DEL FRONT END

Para la construcción del Front End se utilizó Visual Basic .NET. A continuación se describe la estructura general del sistema y se proporciona una descripción de las pantallas que lo conforman, también se explica como crear el proyecto en Visual Studio, así como también se da una explicación para generar las pantallas y reportes en la plataforma .NET.

La estructura general del sistema se muestra en la figura 4.3.1.

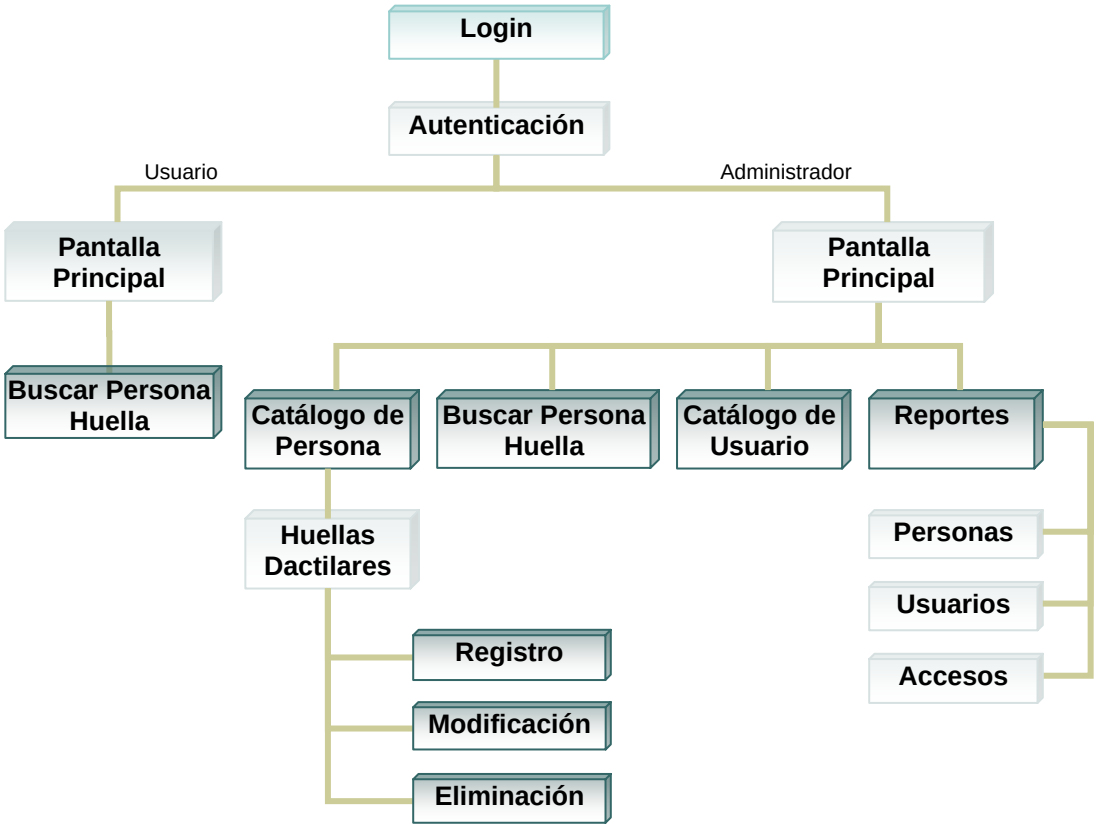


Figura 4.3.1. Diagrama del menú y pantallas del sistema SRIHD

Descripción de pantallas

Además de las pantallas que se mencionan a continuación, se pueden agregar otras opciones al menú principal como puede ser el acceso a Word, Excel u otras aplicaciones propias de la empresa, cuando el usurario acceda a éstas aplicaciones su entrada quedará registrada. Las pantallas principales del sistema son:

- Login.

  En esta pantalla se obtiene el nombre del usuario y su contraseña para determinar los permisos que tendrá dentro del sistema.

- Autenticación.

  El objetivo de esta pantalla es verificar la identidad del usuario por medio de la huella dactilar, de lo cual dependerá el acceso o la negación de la entrada al sistema. Otra de las funciones de esta pantalla es la de registrar en la base

de datos el intento de los usuarios de acceder al sistema, sea este exitoso o no.

- Pantalla Principal.

  Esta pantalla muestra las opciones a las que tiene permiso el usuario, si el usuario es de tipo Administrador, tiene habilitadas todas las opciones del menú (Catálogo de Persona, Catálogo de Usuario, Buscar Persona Huella, Reportes y aplicaciones de uso general que estén en el menú principal), de lo contrario solo tiene visible la opción de Buscar Persona Huella y aplicaciones de uso general.

- Buscar Persona Huella.

  Esta pantalla permite obtener la información de una persona a partir de su huella dactilar.

- Catálogo de Persona.

  En esta pantalla se da de alta una nueva persona, se elimina o se modifican sus datos, también se puede buscar una persona registrada previamente.

- Huellas Dactilares.

  Esta pantalla muestra las opciones para manipular la huella de una persona, registro, eliminación o modificación de las huellas.

- Registro Huella.

  El objetivo de esta pantalla es asociar una huella dactilar a una persona.

- Modificación Huella.

  Esta pantalla se utiliza para actualizar una huella dactilar asociada a una persona.

- Eliminación Huella.

  El objetivo de esta pantalla es eliminar una huella dactilar.

- Catalogo de Usuario.
- Sirve para dar de alta, baja, modificación y búsqueda de los usuarios del sistema.
- Reportes.
- Esta pantalla permite la elección de tres reportes, Persona, Usuarios y Accesos, en cada reporte se puede seleccionar distintos criterios para la

impresión de los mismos, es decir, se puede elegir, por ejemplo, el día de acceso al sistema o un usuario en específico.

- Reporte Personas.

  Muestra los datos de las personas registradas en el sistema.

- Reporte Usuarios.

  Muestra los datos de los usuarios registrados en el sistema.

- Reporte Accesos.

  Muestra la bitácora de accesos al sistema y a las aplicaciones generales.

Construcción del sistema

Antes de crear el proyecto en Visual Studio .NET, se deben instalar los controladores del lector de huellas dactilares con el cual se va a trabajar, el lector es el U.are.U 4000B Reader (ver apéndice A), de la empresa DigitalPersona, los controladores del dispositivo viene con un asistente de instalación, por lo que sólo se tiene que ejecutar y seguir las instrucciones hasta finalizar (figura 4.3.2).

Figura 4.3.2. Asistente para la instalación de los controladores del lector U.are.U 4000B Reader

Una vez que se han instalado los controladores necesarios para que la computadora reconozca el lector de huellas, lo siguiente es instalar el SDK[1] de desarrollo (Software Development Kit - Kit de Desarrollo de Software), el SDK contiene las DLL's donde se encuentran las funciones necesarias para manipular el lector, tales como obtener la huella, verificar la calidad de la huella, etc. El SDK también cuenta con un asistente de instalación al igual que los controladores del dispositivo (figura 4.3.3).

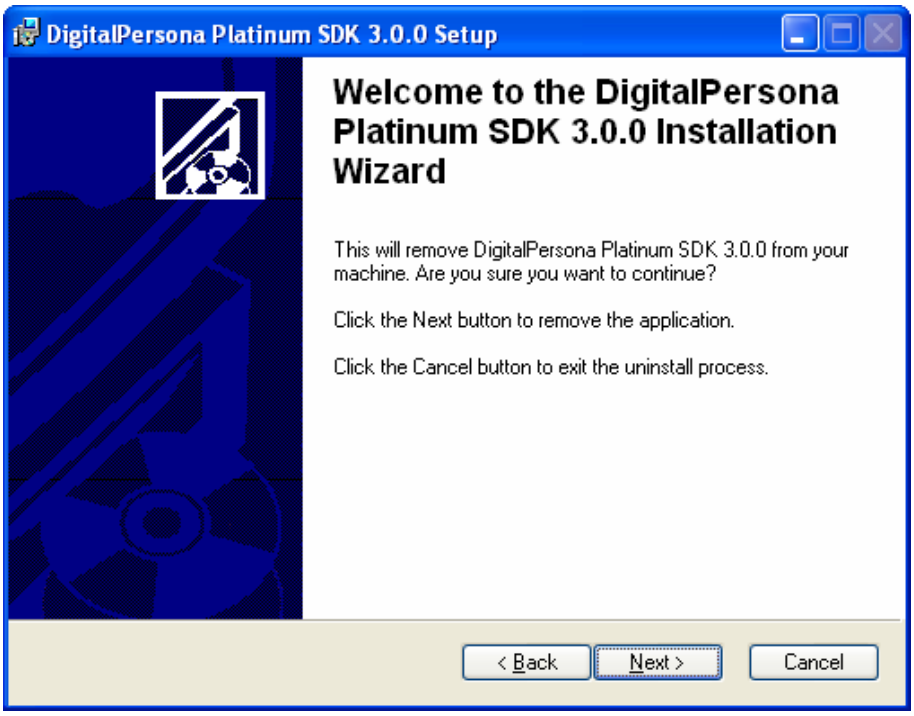


Figura 4.3.3. Asistente para la instalación del SDK del lector de huellas dactilares

Visual Studio .NET

El IDE (entorno integrado de desarrollo) que se utilizó para el desarrollo del sistema es Microsoft Visual Studio .NET 2003. Para crear el proyecto, lo primero es arrancar el entorno de desarrollo de Visual Studio, una vez que se muestra la pantalla principal del IDE, seleccionando del menú **Archivo** -> **Nuevo** -> **Proyecto…**, se

[1] Es un conjunto de aplicaciones para desarrollar programas en un determinado lenguaje o para un determinado entorno.

mostrará un cuadro de diálogo para escoger el lenguaje a usar y el tipo de aplicación que se desea construir, se selecciona **Proyectos de Visual Basic** y **Aplicación para Windows**, a continuación se debe especificar el nombre del proyecto (**prySRIHD**) y la ruta donde se guardará (figura 4.3.4).

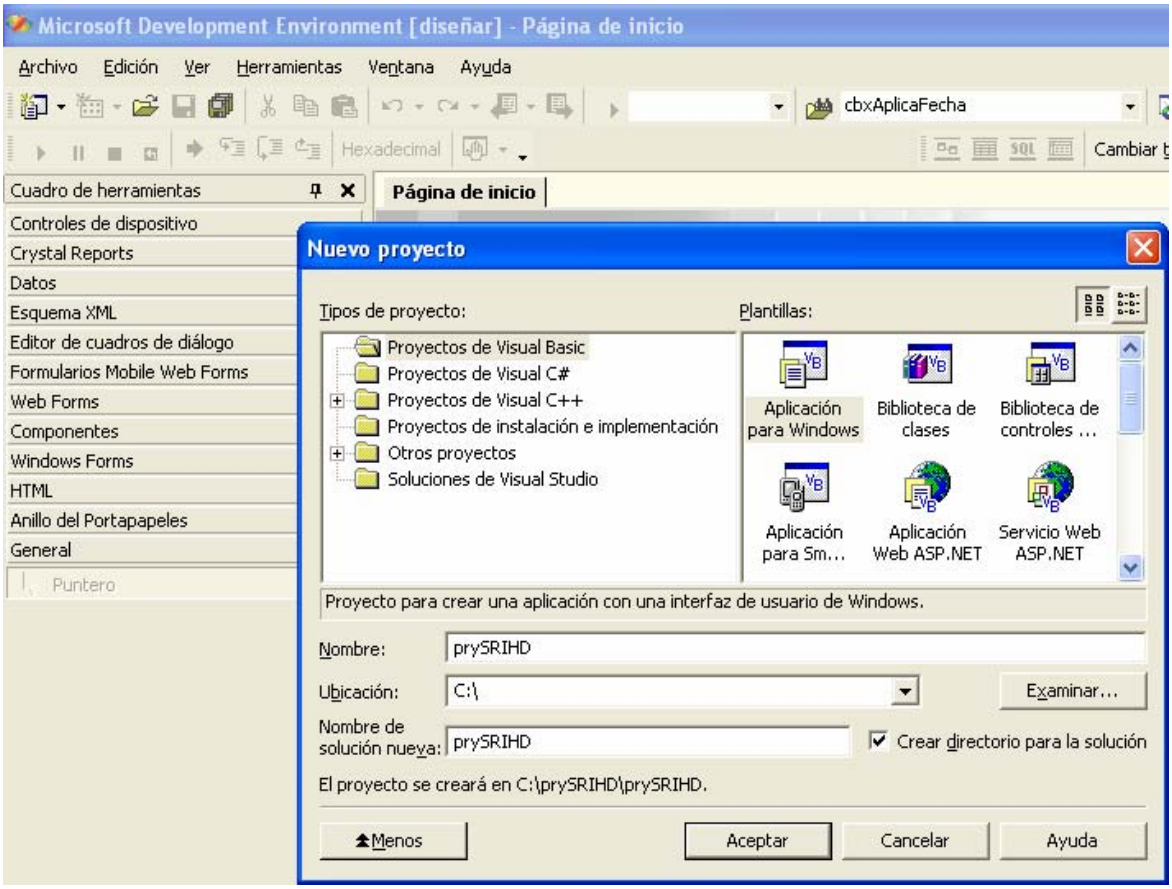


Figura 4.3.4. IDE de desarrollo de Visual Studio .NET

Antes de crear las pantallas de la aplicación es necesario agregar las referencias a las bibliotecas que contienen las funciones para manipular el lector de huellas, para ello se selecciona el menú **Proyecto** -> **Agregar Referencia…** se mostrará el cuadro de diálogo del la figura 4.3.5, en la pestaña **COM** se verifica si ya existen la referencias de DigitalPersona, si no existen, se agregan con el botón **Examinar…** y se busca la ruta de las DLL, la ruta por defecto es: **C:\Archivos de programa\DigitalPersona\Bin**, y las bibliotecas que se deben agregar son:

- DpSdkEng.dll
- DpSdkOps.dll
- DpSdkUsr.dll

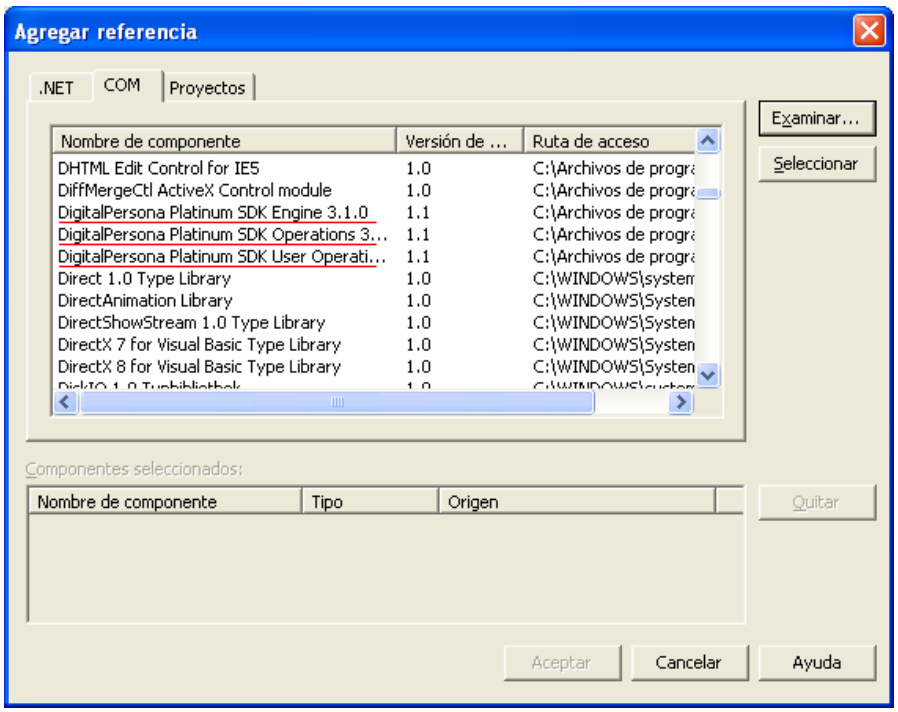


Figura 4.3.5. Bibliotecas de referencia para el proyecto prySIRHD

Lo siguiente, es establecer la conexión a la base de datos que se va a utilizar, la conexión se hace desde código en Visual Basic utilizando las clases Connection de ADO .NET, que permiten establecer una conexión a un origen de datos, por lo que no es necesario crear ningún ODBC[2] (Open DataBase Connectivity - Conectividad Abierta a Bases de Datos), con las siguientes instrucciones se indica el servidor y el origen de datos (la base DB_HUELLAS):

```
Public conDataBase As SqlConnection
Public sGlobalConn As String = "user id=sa; pwd=; Initial Catalog=DB_HUELLAS; data source=WINXP"
```

[2] Estándar de acceso a Bases de Datos desarrollado por Microsoft, cuyo objetivo es hacer posible el acceder a cualquier dato de cualquier aplicación, sin importar qué Sistema Gestor de Bases de Datos almacene los datos.

```
conDataBase = New SqlConnection(sGlobalConn)
conDataBase.Open()
```

Construcción de la pantalla Registro de Huellas

Para crear la pantalla de **Registro de Huellas**, se selecciona menú **Archivo** -> **Agregar nuevo elemento…** -> **Windows Form**, las propiedades y controles de esta ventana son los siguientes:

Control	Nombre	Título	Estilo/ Apariencia	Tamaño	Otra Propiedad
Form	frmRegHuella	Registro de Huellas	Standard	406,342	-
TabControl	tabcRegHuellas	-	FlatButtons	384, 272	-
Button	cmdAnterior	Anterior	Standard	80, 25	-
Button	cmdSiguiente	Siguiente	Standard	80, 25	-
Button	cmdCancelar	Cancelar	Standard	80, 25	-
Label	lbTitulo	Presentación	Standard	88, 19	-

El TabControl tendrá tres controles TabPage, que a su vez contendrán los siguientes controles:

TabPage 1

Control	Nombre	Título	Estilo/ Apariencia	Tamaño	Otra Propiedad
TabPage	TabPresentacion	-	None	376, 243	-
TextBox	txtClave	-	Fixed3D	79, 20	Caracter Casing – Upper ReadOnly – True
TextBox	txtNombPers	-	Fixed3D	264, 20	Caracter Casing – Upper ReadOnly – True

Button	cmdBuscar	-	Standard	23, 23	Imagen
GroupBox	gbSeleccMano	Seleccione el dedo que desea registrar	Standard	376, 184	-
RadioButton	rbtManoIzq	Izquierda	Normal	72, 24	-
RadioButton	rbtManoDer	Derecha	Normal	72, 24	-
ComboBox	cbDedosIzq	-	Standard	104, 21	Ítems – Pulgar Indice Medio Anular Meñique
ComboBox	cbDedosDer	-	Standard	104, 21	Ítems – Pulgar Indice Medio Anular Meñique
Label	Label1	Persona	Standard	46, 16	-
Label	Label2	Paso 1/3	Standard	46, 16	-
PictureBox	imgManoIzq	-	None	76, 85	SizeMode - AutoSize
PictureBox	imgManoDer	-	None	76, 85	SizeMode - AutoSize

TabPage 2

Control	**Nombre**	**Título**	**Estilo/ Apariencia**	**Tamaño**	**Otra Propiedad**
TabPage	TabCaptura	-	None	376, 243	-
GroupBox	gbInstrucc	Instrucciones	Standard	376, 96	-
RichTextBox	meAyuda	-	None	304, 46	-
Label	Label3	Nota: Es necesario tomar 4 muestras de la huella.	Standard	265, 16	-
Label	Label4	Paso 2/3	Standard	46, 16	-
PictureBox	ImgHuella	-	None	100, 120	SizeMode – Stretch Image

PictureBox	PictureBox9	-	None	50, 50	SizeMode – Stretch Image
PictureBox(*)	PictureBox1	-	None	62, 62	SizeMode – AutoSize

(*) Nota: Esta pestaña tiene 7 controles más de este tipo, con las mismas propiedades, por lo que no es necesario incluirlos en la descripción de la tabla.

TabPage 3

Control	Nombre	Título	Estilo/ Apariencia	Tamaño	Otra Propiedad
TabPage	TabConfirmacion	-	None	376, 243	-
RichTextBox	meInfo	Si esta conforme con las muestras obtenidas...	None	304, 46	-
Label	Label5	Paso 3/3	Standard	46, 16	-
Button	cmdRecapturar	Recapturar	Standard	128, 40	-
PictureBox	PictureBox10	-	None	29, 30	SizeMode – Stretch Image
PictureBox(**)	imgMuestra1	-	None	84, 104	SizeMode – Stretch Image

(**) Nota: Esta pestaña tiene 3 controles más de este tipo, con las mismas propiedades, por lo que no es necesario incluirlos en la descripción de la tabla.

El aspecto final de la pantalla se muestra en la figura 4.3.6, cada pantalla corresponde a una de las tres pestañas descritas anteriormente.

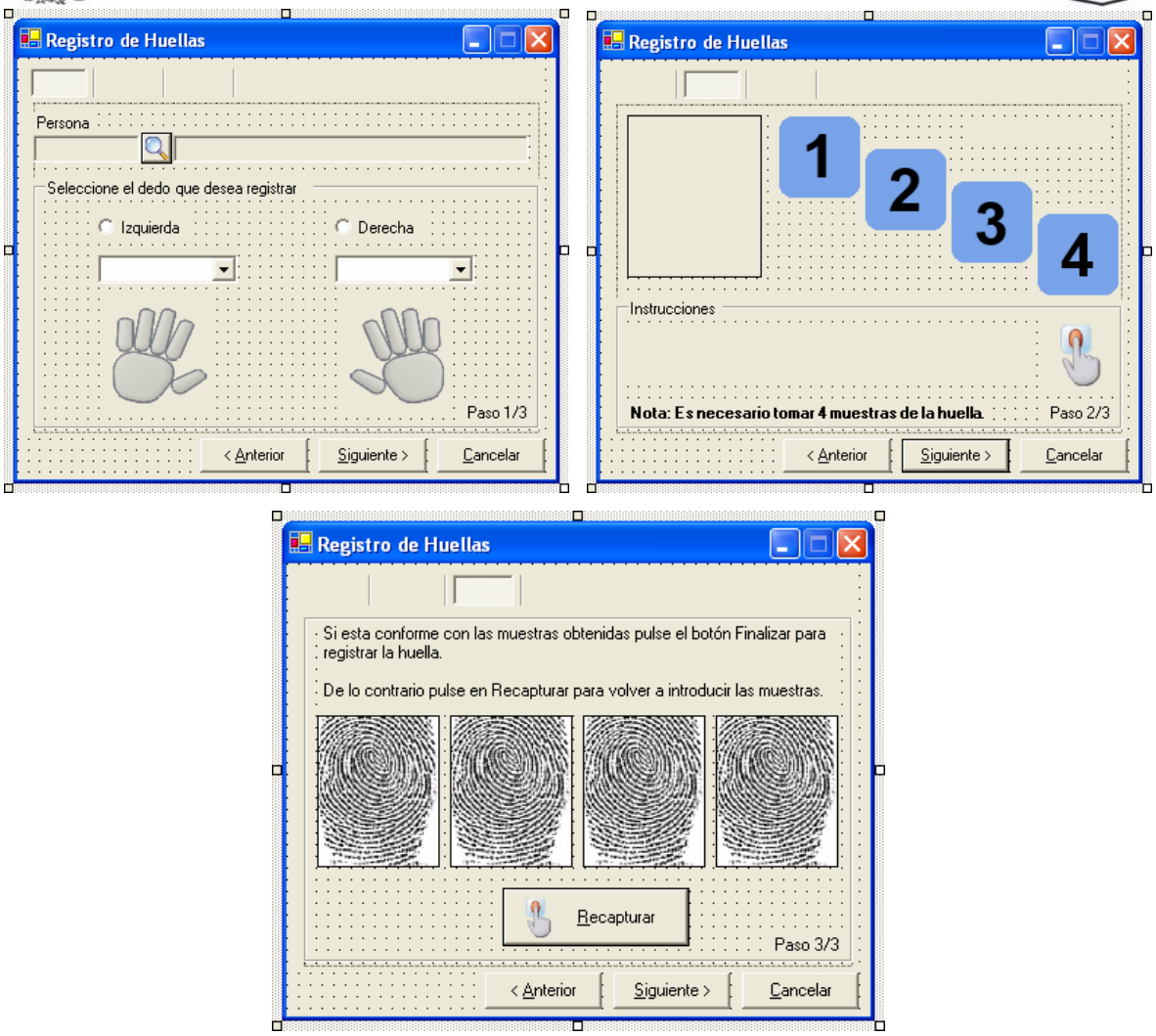


Figura 4.3.6. Pantallas de Registro de Huellas

Funcionalidad de la pantalla

Una vez finalizado el diseño visual de la forma, se escribe el código necesario para darle la funcionalidad a la pantalla, en la tabla 4.3.1 se muestra el código asociado al botón **Siguiente >** de esta pantalla.

```
    Private Sub cmdSiguiente_Click(ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles cmdSiguiente.Click
        Dim sSQL As String
        Dim cmdHuellasReg As SqlCommand
        Dim cmdInstruccSQL As SqlCommand
        Dim sqlTrans As SqlTransaction
        Dim iIdHuella As Integer
```

```
        Dim sCve_Accion As String
        Dim sUsr_Alta As String
        Dim sUsr_Modif As String
        Dim sfechaHora As String

        If tabcRegHuellas.SelectedTab Is TabPresentacion Then
'Comprueba que pestaña esta activa
            If (Trim(txtNombPers.Text) = "") Or (Me.IdPersona = 0)
Then
                MsgBox("Debe Especificar la Persona para Poder
Continuar.", MsgBoxStyle.Exclamation, Me.Text)
            Else
                Me.sCve_Sit = ExisteRegistro()
                If (TipoReg = modGlobal.TTipoReg.rgModif) Or
((Me.sCve_Sit <> "SH_ACT") And (TipoReg = modGlobal.TTipoReg.rgAlta))
Then
                    cmdAnterior.Enabled = True
                    cmdSiguiente.Enabled = False
                    ImgHuella.Image = Nothing

                    ImgInv1.Visible = False
                    ImgInv2.Visible = False
                    Imginv3.Visible = False
                    ImgInv4.Visible = False

                    tabcRegHuellas.SelectedTab = TabCaptura
                    PresentaAyuda()
                    fpRegTemplate.Run()         'Habilitamos el sensor
para capturar las huellas
                Else
                    If TipoReg = modGlobal.TTipoReg.rgAlta Then
                        MsgBox("La Persona Especificada ya esta
Registrada con las Opciones Seleccionadas. Favor de Verificar.",
MsgBoxStyle.Exclamation, Me.Text)
                    End If
                End If
                lbTitulo.Text = "Captura de Huellas"
            End If
        ElseIf tabcRegHuellas.SelectedTab Is TabCaptura Then
            tabcRegHuellas.SelectedTab = TabConfirmacion
            cmdAnterior.Enabled = False
            cmdSiguiente.Text = "&Finalizar"
            lbTitulo.Text = "Confirmación del Registro"
        ElseIf tabcRegHuellas.SelectedTab Is TabConfirmacion Then
            Try
                sfechaHora = FormatDateTime(Now, DateFormat.ShortDate)
& " " & _
                             FormatDateTime(Now, DateFormat.ShortTime)

                sSQL = " SET DATEFORMAT dmy "   'Especifica el formato
de fecha que se utilizara

                cmdInstruccSQL = conDataBase.CreateCommand
'Estblece el comando SQL
                cmdInstruccSQL.CommandText = sSQL
```

```
                cmdInstruccSQL.ExecuteNonQuery()

                iIdHuella = ObtenerIdHuella(sDedo, sMano)
                sqlTrans = conDataBase.BeginTransaction()
                cmdHuellasReg = conDataBase.CreateCommand
'Estblece el comando SQL
                cmdHuellasReg.Transaction = sqlTrans

                If TipoReg = modGlobal.TTipoReg.rgAlta Then
                    If Me.sCve_Sit = "" Then
                        sSQL = " INSERT INTO per_huellas
(id_persona,cve_mano,cve_dedo,cve_situacion) " & _
                               " VALUES(" & Str(Me.IdPersona) & ",'" &
sMano & "','" & sDedo & "'," & "'SH_ACT'" & ")"
                    Else
                        sSQL = " UPDATE per_huellas SET cve_situacion
= 'SH_ACT'" & _
                               " WHERE id_persona = " &
Str(Me.IdPersona) & _
                               " AND   cve_mano = '" & sMano & "' " &
_
                               " AND   cve_dedo = '" & sDedo & "' "
                    End If

                    cmdHuellasReg.CommandText = sSQL
                    cmdHuellasReg.ExecuteNonQuery()
'Ejecuta la instrucción
                End If

                sSQL = " UPDATE PER_HUELLAS SET TX_HUELLA = @CampoBlob
" & _
                       " WHERE id_persona = " & Str(Me.IdPersona) & _
                       " AND   cve_mano = '" & sMano & "' " & _
                       " AND   cve_dedo = '" & sDedo & "' "

                cmdHuellasReg.CommandText = sSQL
                    cmdHuellasReg.ExecuteNonQuery()
'Ejecuta la instrucción
                End If

                sSQL = " UPDATE PER_HUELLAS SET TX_HUELLA = @CampoBlob
" & _
                       " WHERE id_persona = " & Str(Me.IdPersona) & _
                       " AND   cve_mano = '" & sMano & "' " & _
                       " AND   cve_dedo = '" & sDedo & "' "

                cmdHuellasReg.CommandText = sSQL
                cmdHuellasReg.Parameters.Add(New
SqlParameter("@CampoBlob", SqlDbType.VarBinary))
                cmdHuellasReg.Parameters("@CampoBlob").Value = blob
                cmdHuellasReg.ExecuteNonQuery()
'Ejecuta la instrucción
                If TipoReg = modGlobal.TTipoReg.rgAlta Then
                    sUsr_Alta = "'" & Str(Me.IdUsrSesion) & "'"
                    sUsr_Modif = "NULL"
```

```
                    sCve_Accion = "'CA_REG'"

                    sSQL = " INSERT INTO per_huellas_bit " & _
                           " (ID_PERSONA, CVE_MANO, CVE_DEDO,
ID_HUELLA, CVE_ACCION, " & _
                           " FH_ACCION, CVE_USU_ALTA, CVE_USU_MODIF) "
& _
                           " VALUES (" & Str(Me.IdPersona) & ", " & _
                           "'" & sMano & "', " & _
                           "'" & sDedo & "', " & Str(iIdHuella) & ", "
& _
                           sCve_Accion & ", '" & _
                           sfechaHora & "', " & _
                           sUsr_Alta & ", " & sUsr_Modif & ")"
                Else
                    sUsr_Modif = "'" & Str(Me.IdUsrSesion) & "'"
                    sCve_Accion = "'CA_MOD'"

                    sSQL = " INSERT INTO per_huellas_bit " & _
                           " (ID_PERSONA, CVE_MANO, CVE_DEDO,
ID_HUELLA, CVE_ACCION, " & _
                           " FH_ACCION, CVE_USU_MODIF)" & _
                           " VALUES (" & Str(Me.IdPersona) & ", " & _
                           "'" & sMano & "', " & _
                           "'" & sDedo & "', " & Str(iIdHuella) & ", "
& _
                           sCve_Accion & ", '" & _
                           sfechaHora & "', " & _
                           sUsr_Modif & ")"
                End If
                cmdHuellasReg.CommandText = sSQL
                cmdHuellasReg.ExecuteNonQuery()
'Ejecuta la instrucción
                sqlTrans.Commit()
                'ImgHuella.Image.Save(Application.StartupPath &
"\Huellas\huella.jpg", ImageFormat.Jpeg)
                MsgBox("La Huella fue Registrada Exitosamente.",
MsgBoxStyle.Information, Me.Text)

            Catch ex As Exception
                sqlTrans.Rollback()
                MsgBox("Error al Tratar de Registrar la Huella.",
MsgBoxStyle.Critical, Me.Text)
                MsgBox(ex.Message, MsgBoxStyle.Critical, Me.Text)
            End Try
            Me.Close()
        End If
    End Sub
```

Tabla 4.3.1. Código asociado al botón Siguiente de la pantalla de Registro de Huellas

Construcción de la pantalla Usuario

Esta pantalla tendrá las siguientes características:

Control	Nombre	Título	Estilo/ Apariencia	Tamaño	Otra Propiedad
Form	frmUsuario	Usuario	Standard	464, 264	Accept Button – CmdAceptar
GroupBox	gpoDatosUsr	Datos del Usuario	Standard	352,216	-
GroupBox	gbTipoUsr	Tipo Usuario	Standard	224, 48	-
Label	Label1	Persona	Standard	46, 16	-
Label	Label2	Clave Usuario	Standard	75, 16	-
Label	Label3	Usuario	Standard	43, 16	-
Label	Label4	Contraseña	Standard	63, 16	-
Label	Label5	Confirmar Contraseña	Standard	116, 16	-
RadioButton	rbtAdmin	Administrador	Normal	96, 24	-
RadioButton	rbtUsr	Usuario	Normal	64, 24	-
TextBox	txtClave	-	Fixed3D	79, 20	Caracter Casing – Upper ReadOnly – True
TextBox	txtNombPers	-	Fixed3D	232, 20	Caracter Casing – Upper ReadOnly – True
TextBox	txtClaveUsr	-	Fixed3D	104, 20	Caracter Casing – Upper ReadOnly – True
TextBox	txtUsuario	-	Fixed3D	104, 20	Caracter Casing – Upper
TextBox	txtContrasena	-	Fixed3D	104, 20	Caracter Casing – Upper
TextBox	txtConfirmar	-	Fixed3D	104, 20	Caracter Casing – Upper
Button	cmdBuscar	-	Standard	88, 30	Image
Button	cmdNuevo	Nuevo	Standard	368, 16	-

Button	cmdModificar	Modificar	Standard	368, 16	-
Button	cmdEliminar	Eliminar	Standard	368, 16	-
Button	cmdBuscarUsr	Buscar	Standard	368, 16	-
Button	cmdAceptar	Aceptar	Standard	368, 16	-
Button	cmdCancelar	Cancelar	Standard	368, 16	-
Button	cmdSalir	Salir	Standard	368, 16	-
PictureBox	PictureBox1	-	None	32, 32	SizeMode – AutoSize

La apariencia final de esta pantalla se muestra en la figura 4.3.7. Terminado el diseño, se asocia el código correspondiente a cada uno de los botones y controles del formulario.

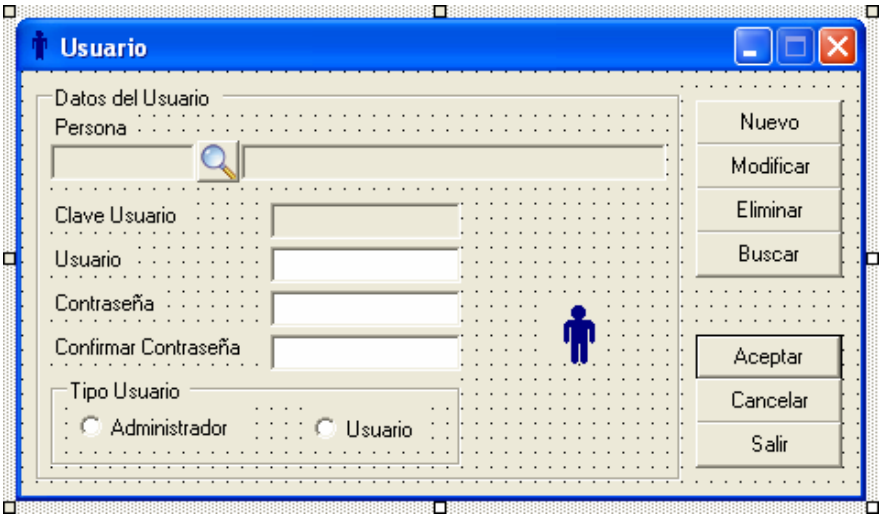


Figura 4.3.7. Diseño final de la pantalla de Usuario

La creación de las otras pantallas del sistema es similar al descrito anteriormente.

Construcción del Reporte de Personas

Para los reportes del sistema se utilizó la plantilla CrystalReport que provee Visual Studio .NET y el elemento DataSet como origen de datos para poblar los reportes.

Para el Reporte de Personas se crea un nuevo formulario con las características siguientes:

Control	Nombre	Título	Estilo/ Apariencia	Tamaño	Otra Propiedad
Form	frmRptPers	Reporte de Personas	Standard	712, 500	-
CrystalReport Viewer	crvRptPer	-	Standard	704, 466	Dock - Fill

El formulario se muestra en la figura 4.3.8.

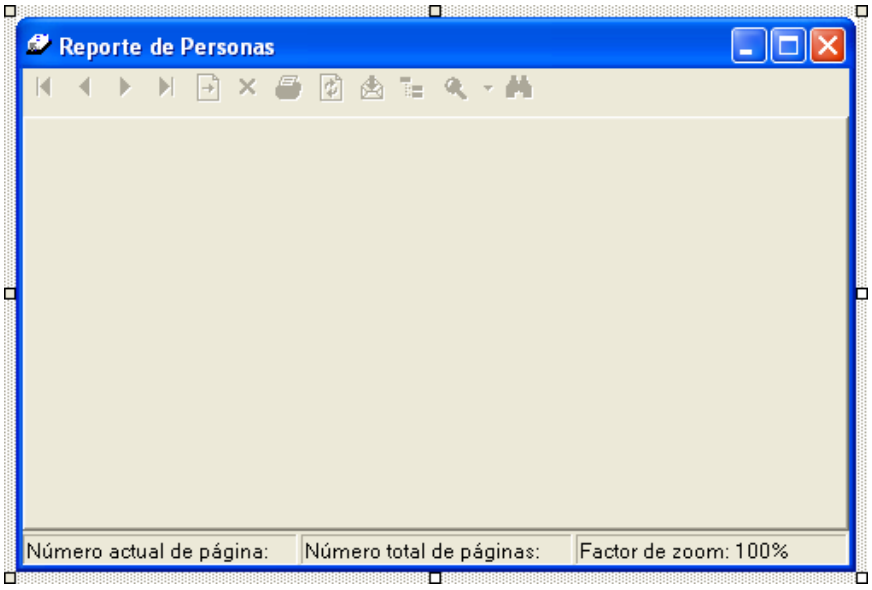


Figura 4.3.8. Formulario para el Reporte de Personas

El siguiente paso es agregar un DataSet al proyecto, el cual sirve para enlazar el reporte con los datos en la base, para ello se selecciona menú **Archivo** -> **Agregar nuevo elemento...**, y se mostrará el cuadro de diálogo de la figura 4.3.9.

Se selecciona el elemento **DataSet** y se escribe el nombre, al dar clic en **Abrir**, aparece el siguiente mensaje:

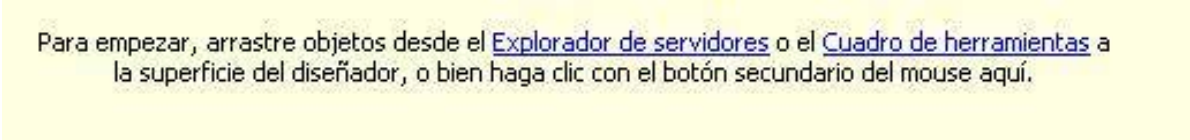


Figura 4.3.9. Cuadro de diálogo para agregar un nuevo elemento al proyecto

Se selecciona **Explorador de Servidores** y se expande **Servidores** (tal como lo indica la figura 4.3.10), después se arrastra la tabla **Persona**.

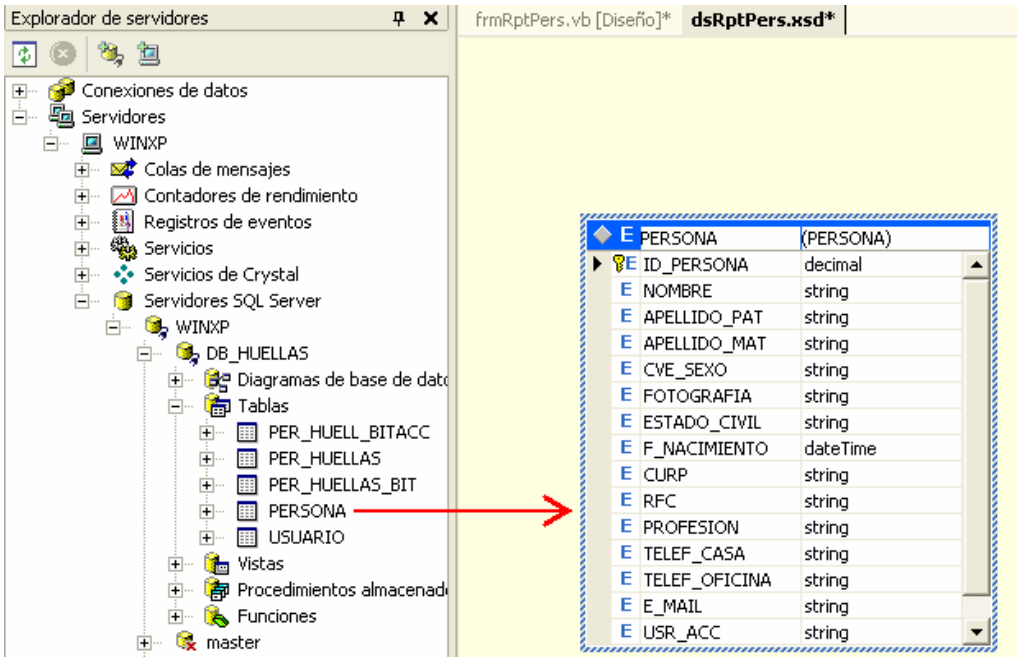


Figura 4.3.10. Explorador de Servidores y la tabla Persona

Ahora se añade el elemento CrystalReports, con el nombre **RptPersona.rpt** (de la misma forma como se agregó el DataSet), al hacerlo aparece la pantalla de la figura 4.3.11, se selecciona la opción **Mediante el asistente de informes** y se finaliza con un clic en **Aceptar**.

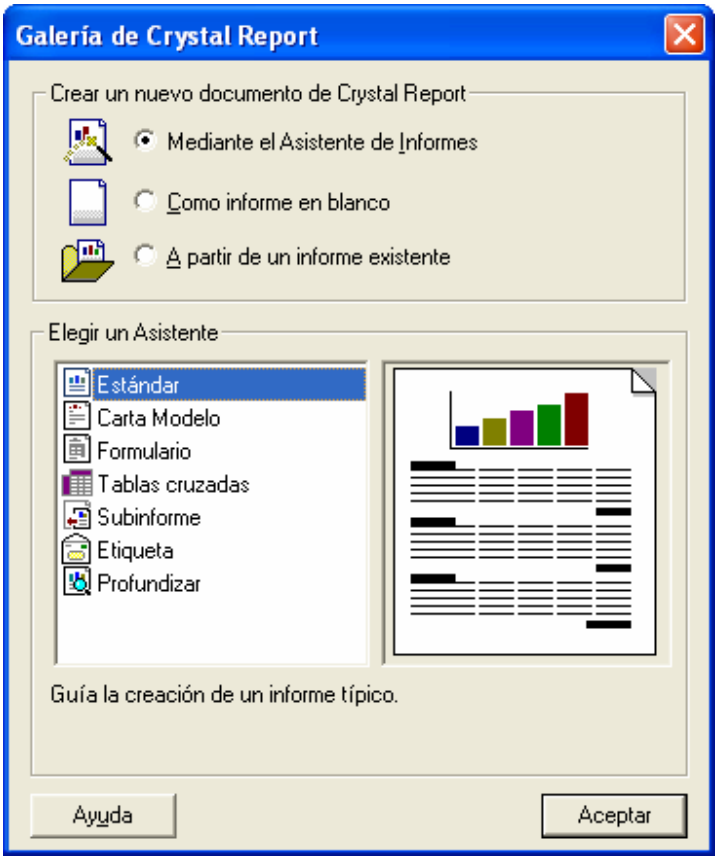


Figura 4.3.11. Cuadro de diálogo para crear un nuevo reporte en Crystal Report

Al hacerlo, aparece una pantalla como la que se muestra en la figura 4.3.12, en **Datos del proyecto** -> **ADO. NET DataSets** -> **prySRIHD.dsRptPers**, se selecciona la tabla **Persona** y se da clic en **Insertar tabla** y después en **Siguiente**, en esta pantalla (figura 4.3.13) se agregan todos los campos que va a desplegar el reporte (botón **Agregar todos**). En la casilla **Estilo**, se escribe el título del reporte **Reporte de Personas**.

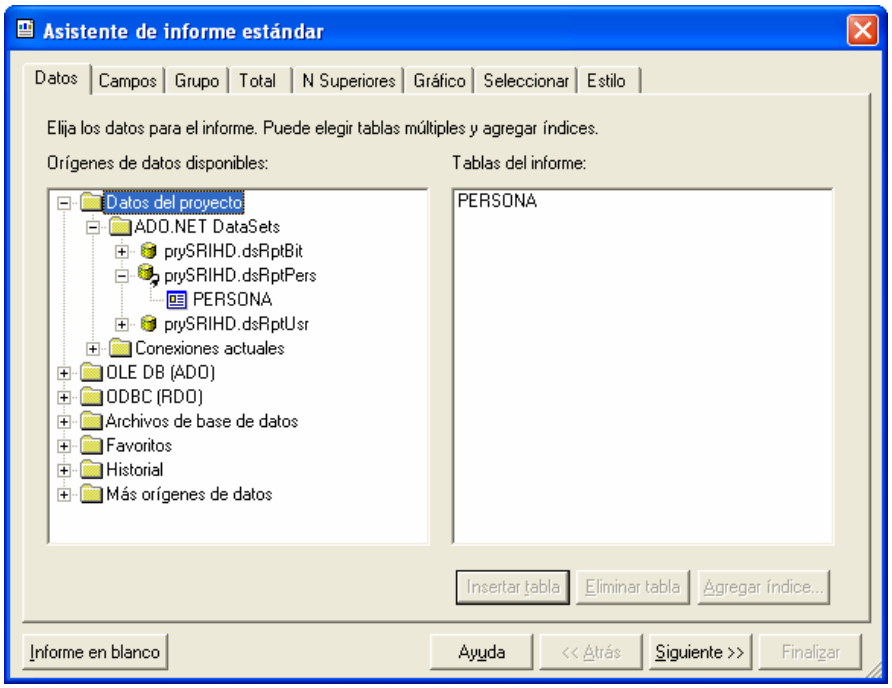


Figura 4.3.12. Origen de datos para el reporte de Personas

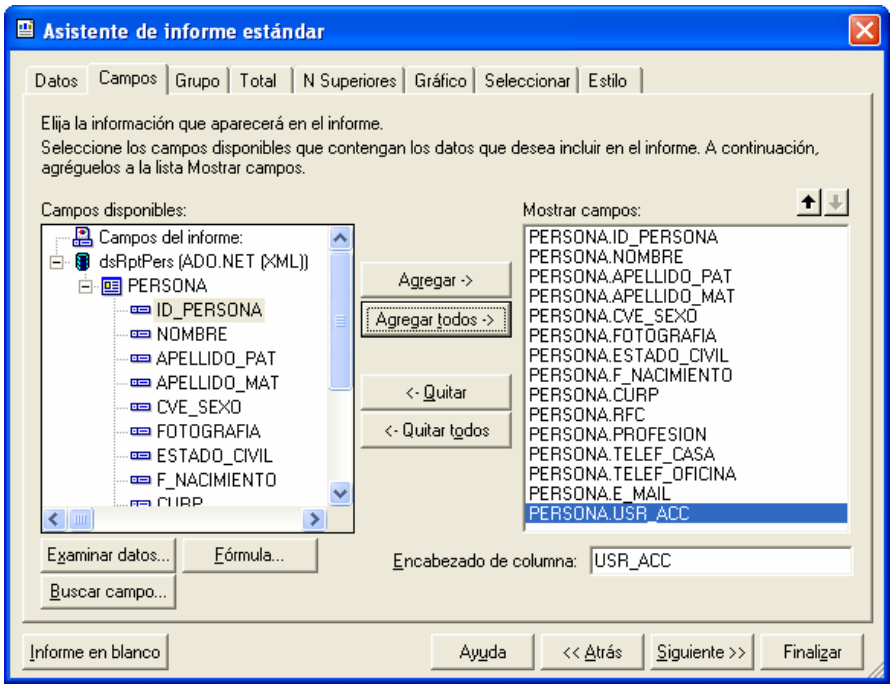


Figura 4.3.13. Campos a visualizar en el reporte de Personas

Una vez que se eligió el origen de datos, aparece el reporte, el formato final de este se muestra en la figura 4.3.14.

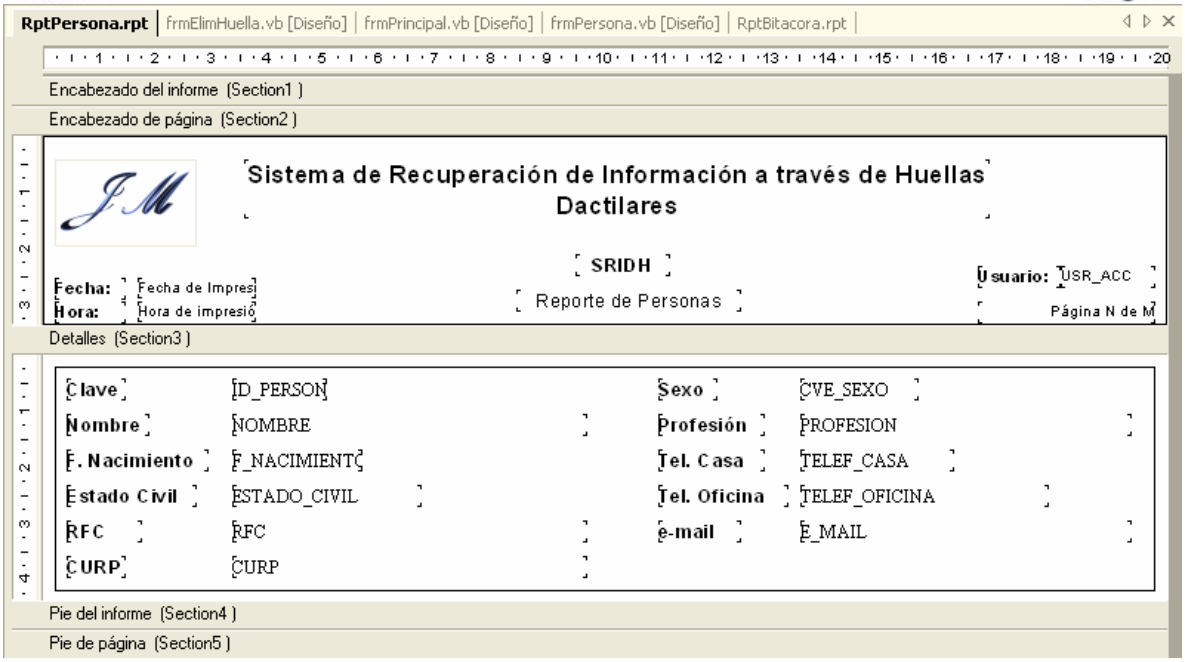


Figura 4.3.14. Reporte de Personas

Finalmente, para visualizar el reporte escribimos el código siguiente:

```
        Dim sSql As String
        Dim sSqlPer As String
        Dim sSqlUsr As String
        Dim sSqlBit As String
        Dim sFiltros As String

        If rbPersona.Checked Then
            Dim sqldaPersona As SqlDataAdapter
            Dim dsDataSet As DataSet = New DataSet
            Dim dsRepPersona As New dsRptPers
            Dim frmRptPers As New frmRptPers
            Dim RptPersona As New RptPersona

            If Trim(txtClave.Text) <> "" Then
                sFiltros = "AND ID_PERSONA = " + Trim(txtClave.Text)
            End If
            If cbxAplicaSexo.Checked Then
                If rbtSexoF.Checked Then
                    sFiltros = sFiltros + "AND CVE_SEXO = 'F' "
                Else
                    sFiltros = sFiltros + "AND CVE_SEXO = 'M' "
                End If
            End If
            sSql = " SELECT " & _
                   "    '" & sLoginUsr & "' USR_ACC, " &
```

```
                    "    ID_PERSONA, " & _
                    "    NOMBRE + ' ' + APELLIDO_PAT + ' ' +
APELLIDO_MAT AS NOMBRE, " & _
                    "    APELLIDO_PAT, " & _
                    "    APELLIDO_MAT, " & _
                    "    FOTOGRAFIA, " & _
                    "    CASE CVE_SEXO WHEN 'F' THEN 'FEMENINO' ELSE
'MASCULINO' END AS CVE_SEXO," & _
                    "    ESTADO_CIVIL, " & _
                    "    CONVERT (CHAR,F_NACIMIENTO,103) AS
F_NACIMIENTO, " & _
                    "    CURP, " & _
                    "    RFC, " & _
                    "    PROFESION, " & _
                    "    TELEF_CASA, " & _
                    "    TELEF_OFICINA, " & _
                    "    E_MAIL " & _
                    " FROM PERSONA " & _
                    " WHERE 1 = 1 " & _
                    sFiltros

            sqldaPersona = New SqlDataAdapter(sSql, conDataBase)

            Try
                sqldaPersona.Fill(dsRepPersona, "PERSONA")
                RptPersona.SetDataSource(dsRepPersona)

                frmRptPers.crvRptPer.ReportSource = RptPersona
                frmRptPers.ShowDialog()
            Catch ex As Exception
                MessageBox.Show(ex.Message, "Reporte de Personas", _
                MessageBoxButtons.OK, MessageBoxIcon.Error)
            End Try
```

Tabla 4.3.2. Código para visualizar el reporte de Personas

Para crear el reporte de **Usuarios** y de **Accesos**, se sigue el procedimiento descrito anteriormente para el reporte de **Personas**.

4.4 PRUEBAS E INTEGRACIÓN DEL SISTEMA

Tipos de pruebas

Existen dos tipos de pruebas principalmente:

- Pruebas del tipo Caja Blanca, que permite examinar la estructura interna del programa.

- Pruebas del tipo Caja Negra, donde los casos de prueba se diseñan considerando exclusivamente las entradas y salidas del sistema, sin preocuparse por la estructura interna del mismo (figura 4.4.1).

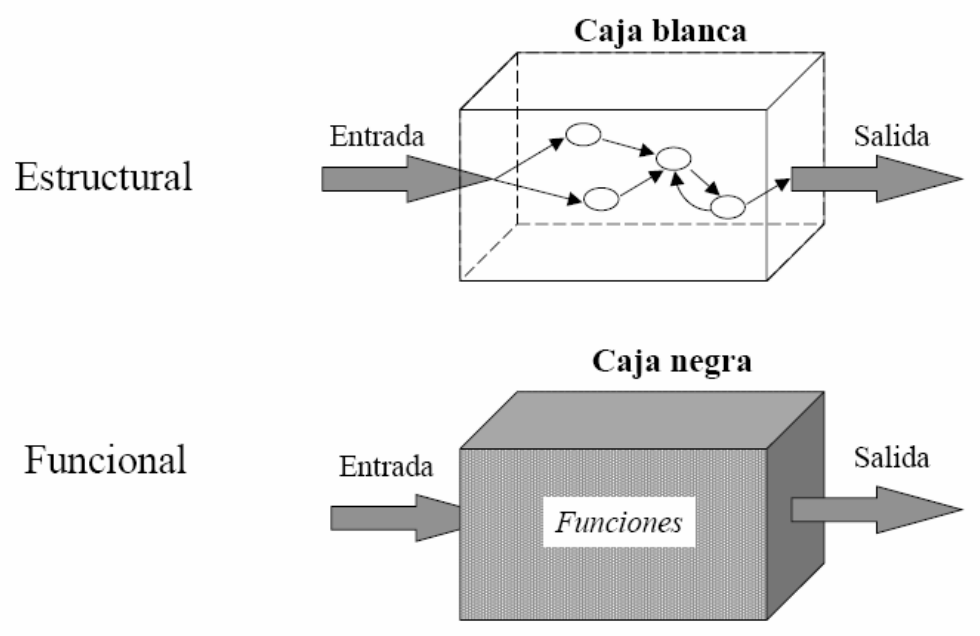


Figura 4.4.1. Diagrama de las pruebas de Caja Blanca y Caja Negra

Pruebas de caja blanca

Utilizan la estructura de control del diseño procedural para derivar casos de prueba.

Los casos derivados pueden ser:

- Garantizar que todas las trayectorias independientes dentro de un módulo, hayan sido ejecutadas dentro de éste al menos una vez.
- Ejecutar todos los lados de las decisiones lógicas.
- Ejecutar todos los ciclos en sus límites operacionales.
- Ejecutar las estructuras de datos internas para asegurar su validez.

Pruebas de caja negra

Se enfocan en los requerimientos funcionales del software. Es un enfoque complementario a las pruebas de caja blanca. Intentan encontrar errores de las siguientes categorías:

- Funciones incorrectas o faltantes.
- Errores de interfase.
- Errores de estructura de datos o accesos de BD.
- Errores de eficiencia.
- Inicialización y/o terminación.

Criterios que satisfacen los casos de prueba de caja negra:

- Casos que reducen el número de pruebas a ser diseñadas.
- Casos que indiquen acerca de la presencia o ausencia de las clases de error, en lugar del error asociado con una prueba específica.

Validación y verificación

- Validación.

  Conjunto de actividades que aseguran que el software creado satisface los requerimientos del usuario (¿Se esta construyendo el producto correcto?).
- Verificación.

  Conjunto de actividades que aseguran que el software implementa correctamente una función específica (¿Se esta construyendo el producto correctamente?).

La validación y verificación abarcan un amplio rango de actividades de aseguramiento de la calidad del software, que incluyen revisiones técnicas formales, auditorias de configuración y calidad, simulación, revisión de la documentación y de la base de datos, análisis de algoritmos, pruebas de desarrollo e instalación, entre otros.

Pruebas unitarias o de módulo

Estas pruebas enfocan el esfuerzo de verificación en las unidades más pequeñas de diseño de software, es decir, el módulo, probando los caminos de control importantes con el fin de descubrir errores dentro de los límites de éste.

Las pruebas unitarias se facilitan cuando los módulos tienen alta cohesión, ya que el número de casos de prueba se reduce y los errores pueden ser más fácilmente predichos y descubiertos.

Objetivos de los casos de prueba

- Interfaz.

  Asegurar que la información fluye de manera adecuada hacia y desde el módulo.
- Estructura de datos.

  Asegurar que los datos que se mantienen temporalmente conservan su integridad durante todos los pasos de ejecución del algoritmo.
- Condiciones frontera.

  Asegurar que el módulo funciona correctamente en los límites establecidos como restricciones de procesamiento.
- Trayectorias independientes.

  Asegurar que todas las sentencias del módulo se ejecuten por lo menos una vez.
- Manejo de errores.

  Asegurar el correcto funcionamiento de todos los caminos de manejo de errores.

Pruebas de integración

Existen varios tipos fundamentales de integración, los cuales son:

- Integración incremental.

  Se combina el siguiente módulo que se debe probar con el conjunto de módulos que ya han sido probados.
- Integración no incremental.

  Se prueba cada módulo por separado y luego se integran todos de una vez y se prueba el programa completo.
- Ascendente.

  Se comienza por los módulos hoja.

- Descendente.

  Se comienza por el módulo raíz.

Es una técnica sistemática para construir la estructura del programa, mientras que al mismo tiempo se llevan a cabo las pruebas para detectar errores asociados con la interacción.

Tipos

- Big-bang.

  Se integran todos los módulos y se hacen pruebas. Mediante este enfoque no incremental, es difícil corregir los errores, ya que es muy complicado aislar las causas cuando se tiene en ejecución un programa entero.

- Top-down.

  Este es un enfoque incremental, en el cual los módulos se integran en jerarquía descendente, iniciando con el módulo de control principal. Se incorporan los módulos a la estructura ya sea por lo ancho o por lo profundo.

Regresión

Cada vez que se añade un módulo nuevo como parte las pruebas de integración, el software cambia: se establecen nuevos caminos en el flujo de datos, pueden existir nuevas Entradas/Salidas, y se invoca a una nueva lógica de control, lo cual puede ocasionar problemas con funciones que ya trabajaban correctamente. Las pruebas de regresión consisten en volver a ejecutar un subconjunto de pruebas que se han llevado a cabo anteriormente, para asegurarse que los cambios no han ocasionado efectos colaterales indeseados.

Pruebas de validación o aceptación

La información contenida en una sección de la especificación de los requerimientos de software, forma la base para un enfoque de pruebas de validación.

Criterios para las pruebas de validación

La validación del software se logra por medio de las pruebas de caja negra que demuestran la conformidad con los requerimientos del usuario.

Pruebas Alfa y Beta

Las pruebas Alfa son llevadas a cabo por el usuario en el lugar del desarrollo, donde el desarrollador participa como observador. Las pruebas Beta se llevan cabo por los usuarios finales, en el lugar de trabajo de éstos, y el desarrollador generalmente no está presente.

Pruebas de stress

Las pruebas de stress ayudan a simular casos en los que el número de clientes o la recuperación masiva de datos de una base de datos aumentan. De este modo es posible evaluar tanto el tiempo de respuesta de un sistema como su capacidad de responder ante esos casos.

Pruebas aplicadas al Sistema de Recuperación de Información a través de Huellas Dactilares

De todas las pruebas mencionadas en éste capítulo se hace referencia de las aplicadas en el sistema, siendo todas éstas de igual importancia y útiles en las etapas de prueba e implementación.

Las pruebas realizadas al sistema en su etapa inicial fue la de caja blanca, ya que se examinó la estructura interna del programa, particularmente los diagramas tanto de Flujo de Datos como de Contexto.

De las pruebas de caja negra, en lo que a la parte funcional del sistema se refiere, se realizaron las pruebas particulares de:

- Errores de interfase.

  Esto se realizó al inicio del proceso, ya que fue necesario un profundo esfuerzo para hacer funcionar el dispositivo de reconocimiento de huellas

dactilares, presentándose problemas de compatibilidad con el lenguaje de programación elegido y la falta de bibliotecas (DLL's) para el dispositivo.

- Errores de estructura de datos o accesos de BD.

  En este caso, se revisaron frecuentemente errores de conexión a la base de datos, quedando a punto lo que a conectividad corresponde, así mismo se verificó la estructura de la base de datos, detectando algunas anomalías que se corrigieron oportunamente.

Referente a las pruebas de validación se verificó que el software creado satisface los requerimientos del usuario ya que a cada paso del desarrollo del sistema se formulaba la pregunta ¿Se esta construyendo el producto correcto? Confirmando en todo momento el camino correcto. Aplicando también la verificación, para asegurar que el software se está construyendo correctamente.

En el sistema desarrollado se implementaron también las Pruebas de integración, empleando particularmente la prueba de Integración incremental, ya que al finalizar cada módulo del sistema se realizaron pruebas con el conjunto de módulos que ya habían sido probados.

Finalmente se realizó la prueba de Stress o de volumen, que aunque la aplicación no se desarrolló en red, es posible simular un uso extremo, intentando la saturación o caída del sistema, lo cuál no ocurrió, librando exitosamente las pruebas antes descritas.

4.5 GENERACIÓN DE REPORTES PARA LA TOMA DE DECISIONES

El sistema SRIHD, cuenta con la capacidad de otorgar tres diferentes reportes que son de ayuda para la administración del mismo. La información necesaria para generar los reportes se obtienen de la base de datos, el sistema hace una consulta (Query) a la base de datos indicando la tabla o las tablas de las cuales se va a

extraer la información, al igual que los filtros que se desea aplicar al reporte para que este se presente de una manera más personalizada. La pantalla que el sistema muestra para realizar la elección del reporte deseado y los filtros a utilizar se presenta en la figura 4.5.1.

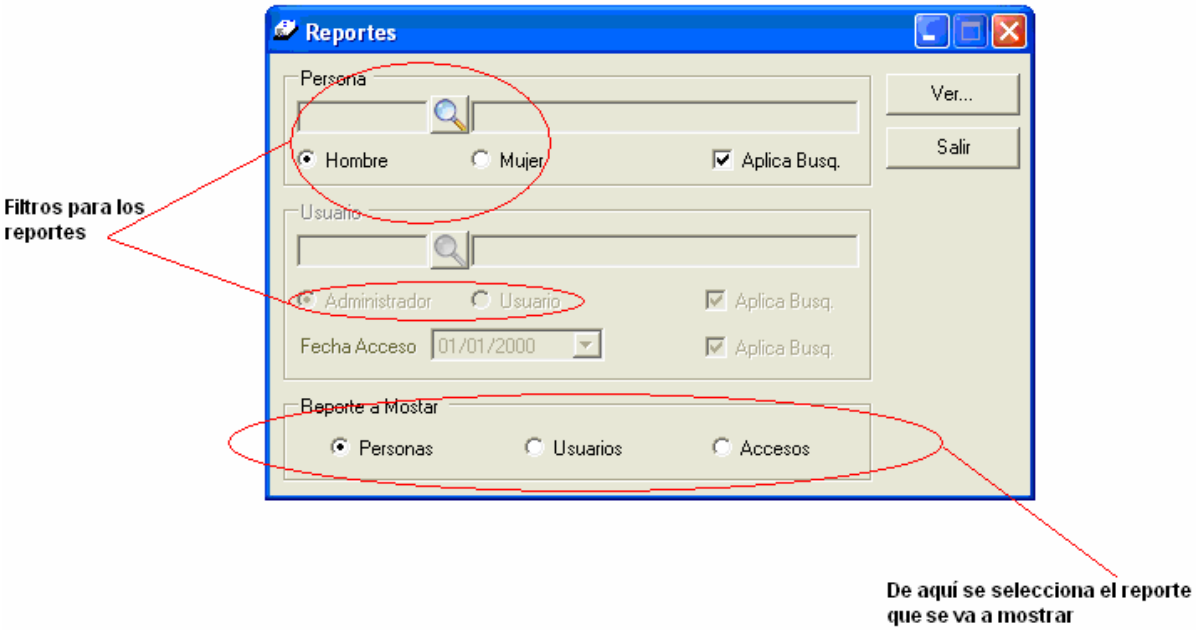


Figura 4.5.1. Pantalla de elección de reportes

La función de los filtros en el sistema es para poder obtener reportes de sólo usuarios hombres o sólo mujeres, esto cuando se tiene seleccionada la opción de **Aplicar Búsqueda**, si no se encontrara seleccionado mostraría el universo completo de usuarios. Si se quiere realizar una búsqueda de un solo individuo, se utiliza el botón de búsqueda que esta destacada por la imagen de una lupa colocado en la parte media del segmento persona, al utilizar dicho botón se abrirá una ventana con todo el universo donde se podrá seleccionar al individuo deseado, llenándose con la información del usuario los campos que se encuentran a los extremos del botón de búsqueda.

Cabe mencionar que las opciones se encontraran habilitadas o deshabilitadas dependiendo del tipo de reporte que se requiera y estos sólo podrán ser obtenidos por usuarios que tengan permisos de administrador.

Reporte de usuarios

El reporte de usuario, muestra la información de los usuarios que se tiene registrados en el sistema, mostrando solamente cierta información de estos (Clave de usuario, Login, Nombre completo y Tipo de usuario), un ejemplo de lo antes mencionado se muestra en la figura 4.5.2.

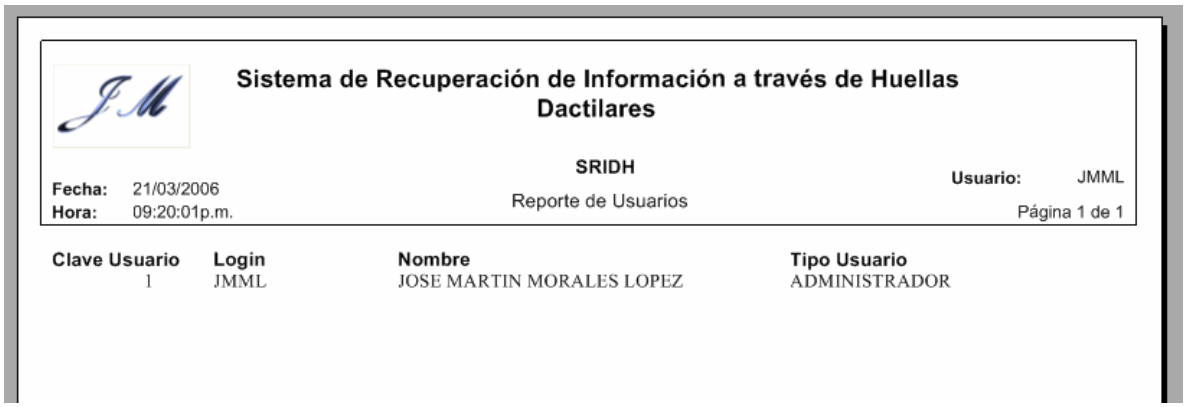


Figura 4.5.2. Reporte de usuarios

La información necesaria para la construcción de dicho reporte se obtiene de la base de datos DB_HUELLAS, en específico de las tablas llamadas USUARIO y PERSONA. A continuación se muestra de que tablas de la base de datos se obtiene la información que construye al reporte (tabla 4.5.1).

Descripción	Tabla(s)	Campo(s)
Clave Usuario	USUARIO	ID_USUARIO
Login	USUARIO	LOGIN
Nombre	PERSONA	NOMBRE APELLIDO_PAT APELLIDO_MAT
Tipo Usuario	USUARIO	CVE_TIPO_USR

Tabla 4.5.1. Tablas y campos del Reporte de usuarios

Para un mejor entendimiento se muestra el diagrama de Entidad-Relación utilizado figura 4.5.3).

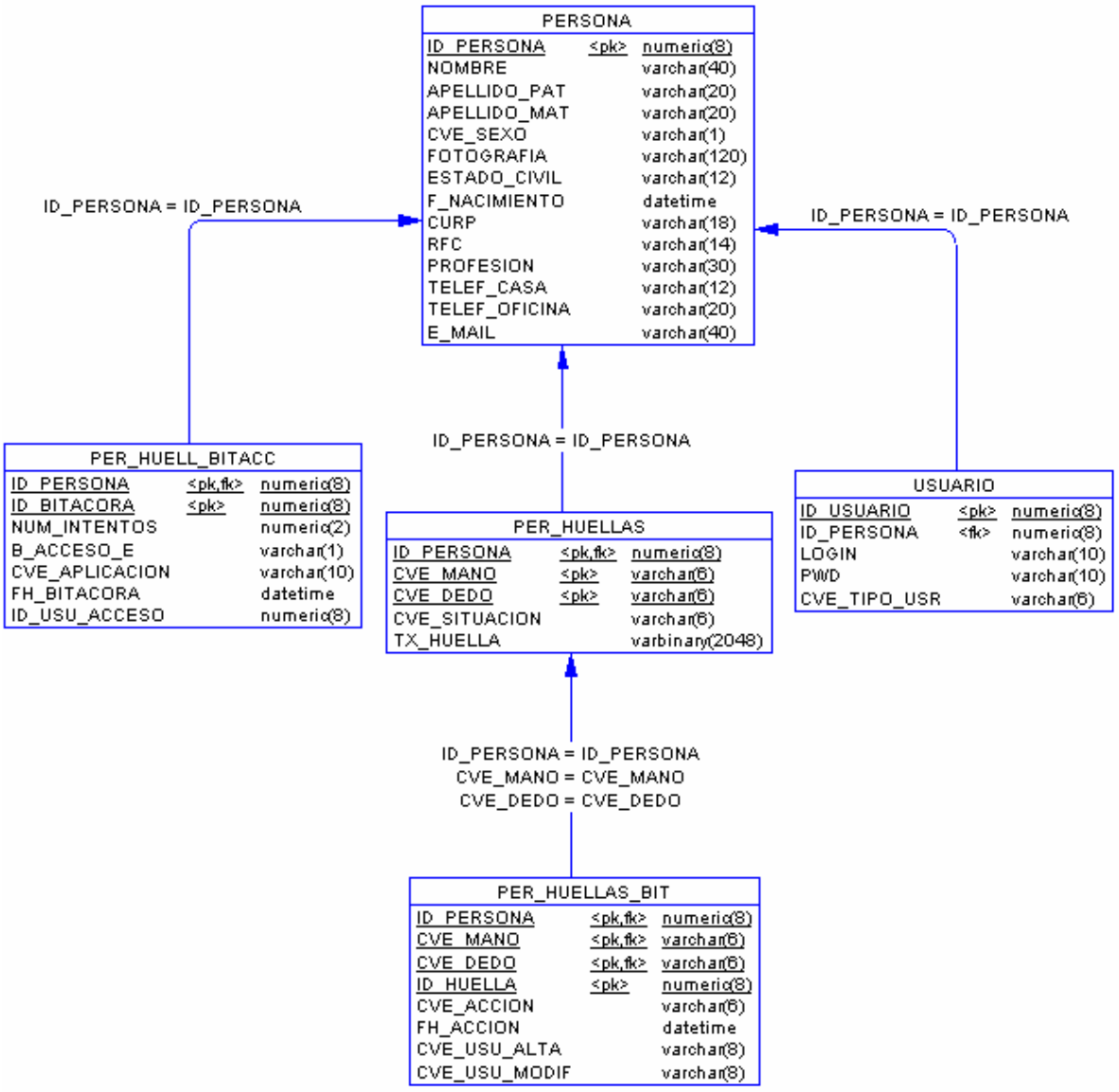


Figura 4.5.3. Diagrama E-R de la base DB_HUELLAS

Reporte de Personas

Este reporte permite mostrar la información de un usuario en específico con información personal del mismo (figura 4.5.4).

Figura 4.5.4. Reporte de personas

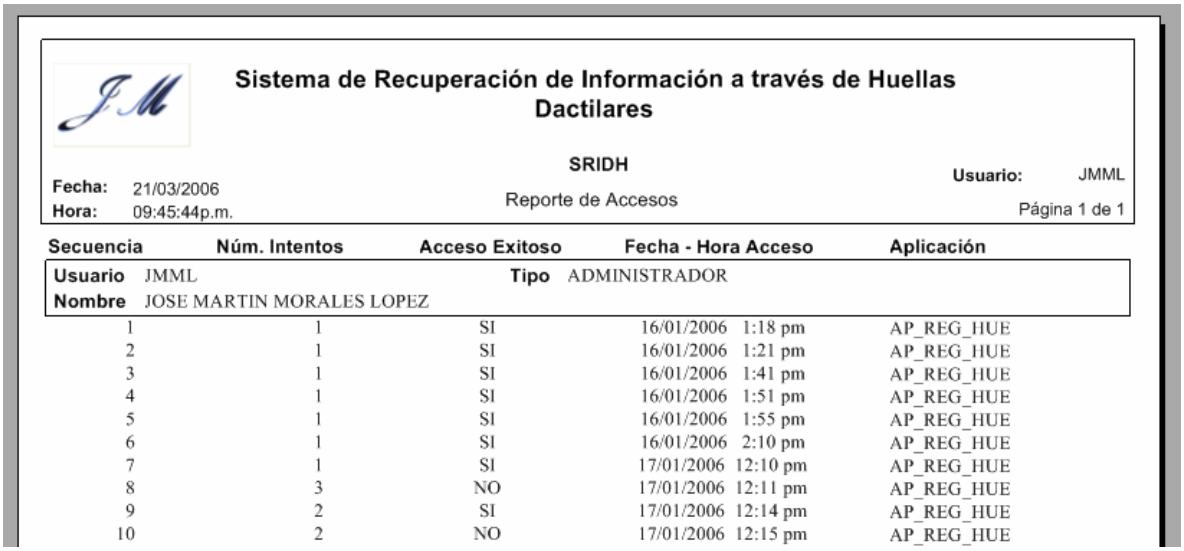
Para la construcción de este reporte la información se obtiene de la tabla PERSONA y los campos que se utilizan se muestran en la tabla 4.5.2.

Descripción	Tabla(s)	Campo(s)
Clave	PERSONA	ID_PERSONA
Nombre	PERSONA	NOMBE APELLIDO_PAT APELLIDO_MAT
F. Nacimiento	PERSONA	F_NACIMIENTO
Estado Civil	PERSONA	ESTADO_CIVIL
RFC	PERSONA	RFC
CURP	PERSONA	CURP
Sexo	PERSONA	CVE_SEXO
Profesión	PERSONA	PROFESION
Tel. Casa	PERSONA	TEL_CASA
Tel. Oficina	PERSONA	TEL_OFICINA
e-mail	PERSONA	E_MAIL

Tabla 4.5.2. Tablas y campos del Reporte de Personas

Reporte de Accesos

Este tercer tipo de reporte que genera el sistema es considerado el más importante, puesto que ayuda a observar que usuarios han intentado o han entrado a las aplicaciones, en cuántos intentos, la fecha y hora en la que entró o intentó entrar a la aplicación y el nombre de la aplicación (figura 4.5.5).



Sistema de Recuperación de Información a través de Huellas Dactilares

SRIDH

Fecha: 21/03/2006
Hora: 09:45:44p.m.

Reporte de Accesos

Usuario: JMML
Página 1 de 1

Usuario JMML Tipo ADMINISTRADOR
Nombre JOSE MARTIN MORALES LOPEZ

Secuencia	Núm. Intentos	Acceso Exitoso	Fecha - Hora Acceso	Aplicación
1	1	SI	16/01/2006 1:18 pm	AP_REG_HUE
2	1	SI	16/01/2006 1:21 pm	AP_REG_HUE
3	1	SI	16/01/2006 1:41 pm	AP_REG_HUE
4	1	SI	16/01/2006 1:51 pm	AP_REG_HUE
5	1	SI	16/01/2006 1:55 pm	AP_REG_HUE
6	1	SI	16/01/2006 2:10 pm	AP_REG_HUE
7	1	SI	17/01/2006 12:10 pm	AP_REG_HUE
8	3	NO	17/01/2006 12:11 pm	AP_REG_HUE
9	2	SI	17/01/2006 12:14 pm	AP_REG_HUE
10	2	NO	17/01/2006 12:15 pm	AP_REG_HUE

Figura 4.5.5. Reporte de accesos

Para la construcción de este reporte como en los anteriores, toda la información que contiene se obtuvo de la base de datos, para un mayor detalle se muestra la tabla 4.5.3.

Descripción	Tabla(s)	Campo(s)
Usuario	USUARIO	LOGIN
Tipo	USUARIO	CVE_TIPO_USR
Nombre	PERSONA	NOMBRE APELLIDO_PAT APELLIDO_MAT
Aplicación	PER_HUELL_BITACC	CVE_ APLICACION
Fecha-Hora Acceso	PER_HUELL_BITACC	FH_BITACORA
Acceso Exitoso	PER_HUELL_BITACC	B_ACCESO_E
Número de Intentos	PER_HUELL_BITACC	NUM_INTENTOS
Secuencia	PER_HUELL_BITACC	ID_BITACORA

Tabla 4.5.3. Tablas y campos del Reporte de accesos

4.6 FACTIBILIDAD TÉCNICA Y OPERATIVA

Factibilidad técnica

La factibilidad técnica del presente trabajo se basó en la evaluación del equipo con el que se cuenta así como las herramientas de software disponibles para su desarrollo. Como se ha mencionado a lo largo de este trabajo, se optó por desarrollar el Front End en Visual Basic .NET, también se cuenta con el SDK Platinum del fabricante DigitalPersona Inc. para el desarrollo de aplicaciones, que se utiliza para manipular el dispositivo U.are.U 4000B Reader, el cual cuenta con soporte para aplicaciones en Visual Basic. Otro factor de decisión para el desarrollo de esta aplicación fue el Back End que es el motor de base de datos SQL Server 2000, ya que en la actualidad es uno de los manejadores de base de datos relaciónales que más se utilizan con aplicaciones para Windows.

El lector de huella dactilar U.are.U 4000B Reader es muy fácil de instalar, ya que sólo se conecta al puerto USB de un equipo personal y se instalan los controladores en versiones del sistema operativo Windows que van desde la versión 98 SE hasta Windows XP con Service Pack 2.0.

En la tabla 4.6.1 se presenta los requisitos básicos del hardware para el dispositivo U.are.U 4000-B.

Procesador	Procesador de familia Pentium con 133 MHz. de velocidad o superior
Sistema Operativo	Versión de Windows 98 SE o superior
Memoria RAM	64 MBytes
Espacio en Disco Duro	270 MBytes Libres
Periféricos Obligatorios	Unidad de CD ROM 4x o superior

Tabla 4.6.1. Requerimientos para el lector de huellas dactilares U.are.U 4000B

En lo que se refiere a las herramientas de software, se debe tener clara idea que el sistema operativo en el cual se basó el desarrollo del trabajo fue Windows XP Profesional, por lo que el rendimiento se vería afectado si se trata de ejecutar la aplicación en equipos de cómputo muy antiguos. Es conveniente considerar un equipo de cómputo que se encuentre en el promedio de las empresas y sectores de gobierno, por lo que se propone un equipo con procesador Pentium III o Celeron con velocidad superior a los 500 MHz, con capacidad de memoria RAM de 256 MBytes y Disco Duro de 40 GBytes.

En la tabla 4.6.2 se muestran los requisitos mínimos para la instalación del Motor de Base de datos SQL Server 2000, el cual se instaló en modalidad de Cliente-Servidor.

Procesador	Pentium II o superior
Memoria RAM	128 MBytes
Sistemas Operativos	Windows 98 SE Windows ME Windows 2000 Windows NT 4.0 Windows Server 2003 Windows XP
Adaptador de Video	SVGA a 800 x 600 pixeles
Capacidad del Disco Duro	2 Mbytes libres (mínimo)

Tabla 4.6.2. Requerimientos del SQL Server 2000

Por lo que respecta al Visual Basic .NET, los requisitos mínimos del equipo que se necesita se describen en la tabla 4.6.3.

Procesador	Procesador de tipo Pentium II a 450 MHz. se recomienda procesador Pentium III a 600 MHz.
Memoria RAM	160 MBytes de Capacidad Mínimo (512 MB es el adecuado para el Sistema)
Sistemas Operativos	Windows 98 Windows ME Windows 2000 Windows NT 4.0 Windows Server 2003 Windows XP
Adaptador de vides	Super VGA (1024x768) o pantalla de resolución más alta con 256 colores

Tabla 4.6.3. Requerimientos del Visual Basic .NET

Factibilidad operativa

La operación del sistema deberá de satisfacer los siguientes puntos:

- Desempeño.

  De acuerdo a las plataformas sobre las que se instalará el sistema, el rendimiento es adecuado, tomando en cuenta que el volumen de la información es acorde a los recursos de los equipos promedio existentes en la actualidad.

- Economía.

  El gasto principal para la implementación del sistema es la adquisición de las licencias para el software empleado, ya que el desarrollo del programa no tendrá ningún costo.

- Eficiencia.

  Permite además contar con una base de datos amplia con información valiosa y sobre todo se puede obtener de ella dicha información sin necesidad de contar con datos ni claves de acceso, haciendo más eficiente y rápida la extracción de datos.

- Control.

  Los Administradores de seguridad en los centros y sistemas de cómputo pueden tener el control absoluto de los accesos además de poder auditar en forma real los usuarios que accedan un sistema o aplicación.

- Seguridad.

  Con este sistema se elimina la incertidumbre de los usuarios preocupados por la seguridad de la información y los sistemas de cómputo y se puede controlar e incluso bloquear usuarios no autorizados a los accesos restringidos.

Se considera viable la aplicación del sistema en un amplio rango del sector público y privado, ya que su uso puede ser a nivel de equipo de cómputo personal o hasta el corporativo.

Tipos de mantenimiento

El mantenimiento es una acción inherente a toda aplicación recién instalada y es tan importante considerarla como lo es el diseño y el desarrollo, de hecho un sistema sin mantenimiento esta condenado a ser obsoleto en un tiempo muy corto. Los programas deben ser modificados con el tiempo ya que las necesidades de los usuarios cambian junto con la tecnología. Por ello se describe a continuación los diferentes tipos de mantenimientos.

- Mantenimiento preventivo.

  Es la actividad en la cual se realizan ajustes a la aplicación para evitar el mantenimiento futuro, la estabilidad y confiabilidad en la operación. También es útil para proporcionar bases seguras sobre las que podrán implementarse mejoras posteriores.

- Mantenimiento correctivo.

  Es el conjunto de actividades dedicadas a corregir defectos en el hardware o en el software detectados por el usuario cuando ocurre un error en la operación normal del sistema.

- Mantenimiento adaptativo.

Son las actividades para adaptar el sistema a los cambios (hardware o software) en su entrono tecnológico. Se presenta cuando se generan cambios en los requerimientos de tal manera que la especificación sea adaptada a los nuevos requerimientos verificando que la nueva implementación cumpla con ellos, además que este opere correctamente en un nuevo hardware.

- Mantenimiento perfectivo.

  Conjunto de actividades para mejorar o añadir nuevas funcionalidades requeridas por el usuario. Se realiza cuando existe la necesidad de optimizar los procesos, sin que cambien forzosamente los requerimientos. La especificación permite entender claramente el impacto de los cambios de manera que éstos se implanten confiadamente.

Capacitación para la operación del sistema

El factor humano que será el operario final de sistema, deberá de contar con conocimientos básicos en computación mediante el siguiente programa de capacitación:

- Introducción a la computación y el sistema operativo Windows XP.

  En 10 horas, se establece como objetivo el familiarizar a un usuario totalmente inexperto en temas de cómputo e informática.

- Introducción a la Administración de las Bases de Datos relaciones mediante SQL Server 2000.

  Este curso es considerado un elemento fundamental para el usuario del sistema, es importante para el conocimiento de la base de datos para evitar a toda costa el mal uso de los datos se considera que en 10 hrs. el usuario puede alcanzar este objetivo.

- Uso y cuidados del dispositivo U.are.U 4000B Reader.

  Curso de 4 horas tiene como meta el familiarizar a los usuarios con algunas de las funciones del lector de huellas digitales, tales como el registro, almacenamiento y captación de huellas, además de brindarle el conocimiento sobre el cuidado del lector dactilar así como su limpieza.

- Instalación y operación del sistema SRIHD.

  Una vez superado los temas anteriores, se plantea mediante un curso de 5 horas, contempla que el usuario debe de conocer el sistema, desde la instalación hasta la manipulación de cada uno de los módulos y pantallas, así como la interacción con el dispositivo.

Diagrama de Gantt para el desarrollo del proyecto

El diagrama de Gantt[3] de la figura 4.6.1 muestra las diferentes etapas de desarrollo del Sistema de Recuperación de Información a través de Huellas Dactilares, el cual plantea un total de 13 semanas para su implementación.

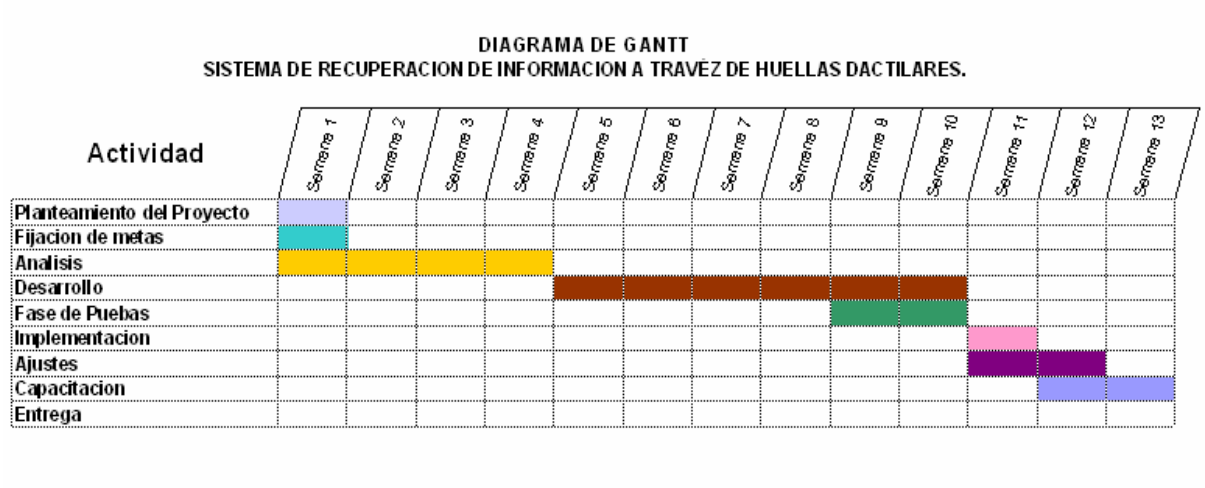


Figura 4.6.1. Diagrama de Gantt

[3] Es una representación gráfica de barras, en él se muestran las fechas de comienzo y finalización de las tareas del proyecto y las duraciones estimadas.

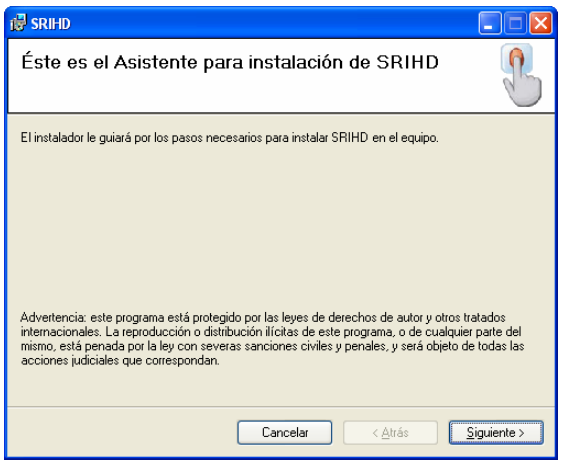
Manual de usuario y técnico

MANUAL DE USUARIO

Es necesario contar con un manual que muestre el funcionamiento de la aplicación al usuario final. Por medio de este manual se proporcionará la información necesaria para conocer la operabilidad del Sistema de Recuperación de Información a través de Huellas Dactilares (SRIHD).

Instalación del sistema

El programa SRIHD cuenta con un asistente de instalación, el cual crea un acceso directo al programa en el botón de Inicio de Windows XP (figura 1). Una vez instalado el sistema se puede acceder desde **Inicio** -> **Todos los programas** -> **SRIHD** -> **SRIHD**.



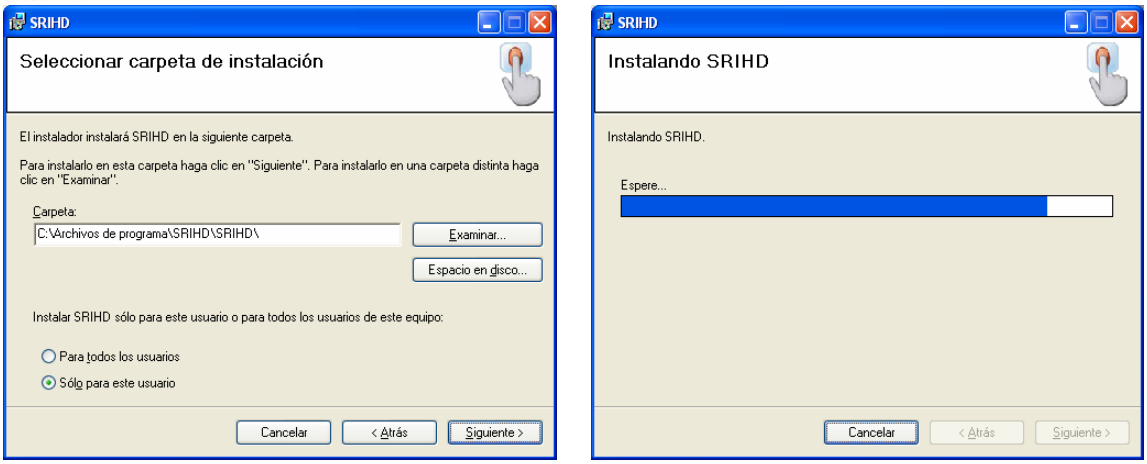


Figura 1. Asistente de instalación del programa SRIHD

Acceso al sistema

El sistema cuenta con una pantalla de acceso que será la primera en desplegarse (figura 2).

Figura 2. Ventana de acceso

El usuario cuenta con tres intentos para acceder a la aplicación, una vez que se ha validado el usuario y contraseña, se muestra la pantalla de **Verificar Persona** que se muestra en la figura 3, el usuario debe colocar su dedo sobre el lector de huellas dactilares para poder acceder al sistema.

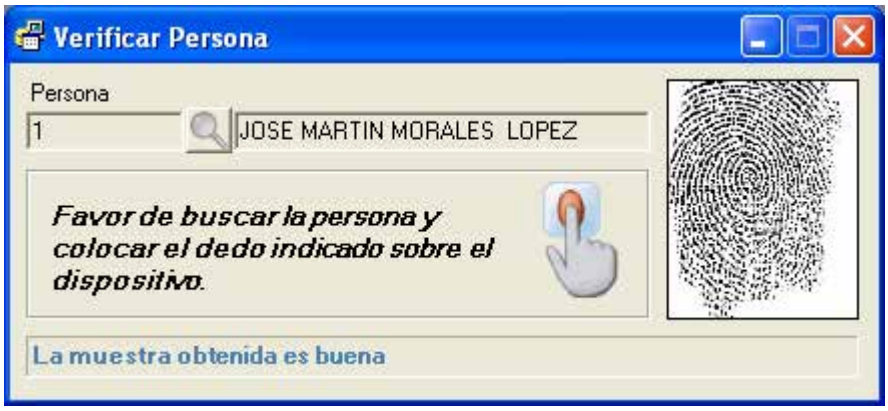


Figura 3. Pantalla de verificación de la huella dactilar

Menú Principal

Si coincide la huella, se muestra la pantalla del **Menú Principal** (figura 4), de lo contrario se muestra un mensaje de error y se cierra la aplicación.

En el menú principal se encuentran una lista de aplicaciones a las que el usuario tiene acceso, las opciones principales que puede seleccionar el usuario son las siguientes:

- Usuarios
- Personas
- Reportes
- Busca Huella
- Otras aplicaciones corporativas

Si el usuario que accedió al sistema es de tipo Administrador se muestran todas las opciones, sino solo se muestra la opción de **Busca Huella** y aplicaciones de uso general.

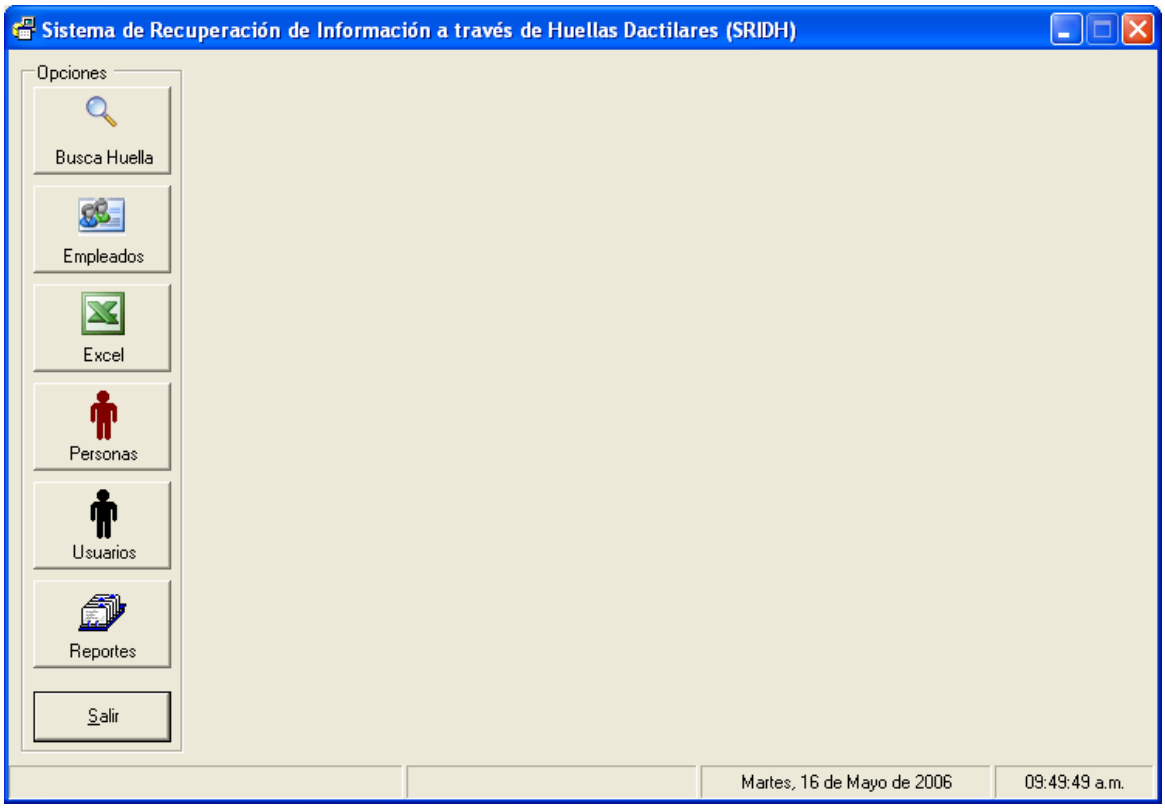


Figura 4. Menú Principal

Catálogo de Usuario

Esta opción permite ver el catálogo de **Usuario** (figura 5), el cual cuenta con las opciones básicas de dar de alta, baja, modificación y búsqueda de un registro en el sistema.

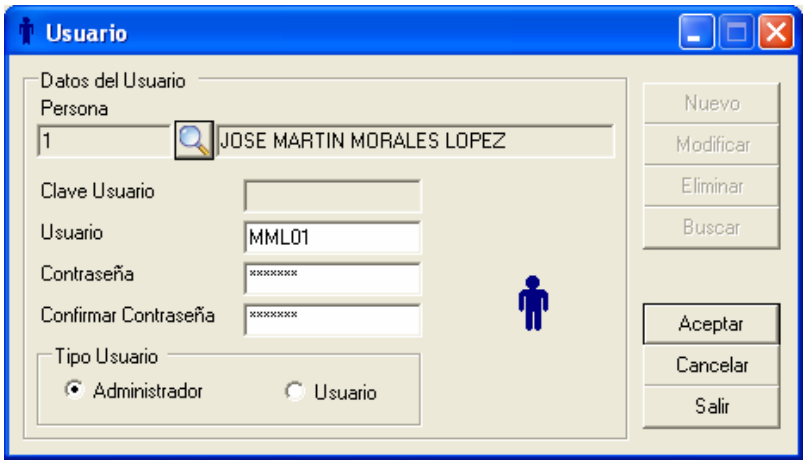


Figura 5. Catálogo de Usuario

Catálogo de Persona

Esta opción muestra los datos personales registrados de cada usuario, al igual que el catálogo de **Usuario**, tiene las opciones de dar de alta, baja, modificación y búsqueda de una persona en el sistema (figura 6).

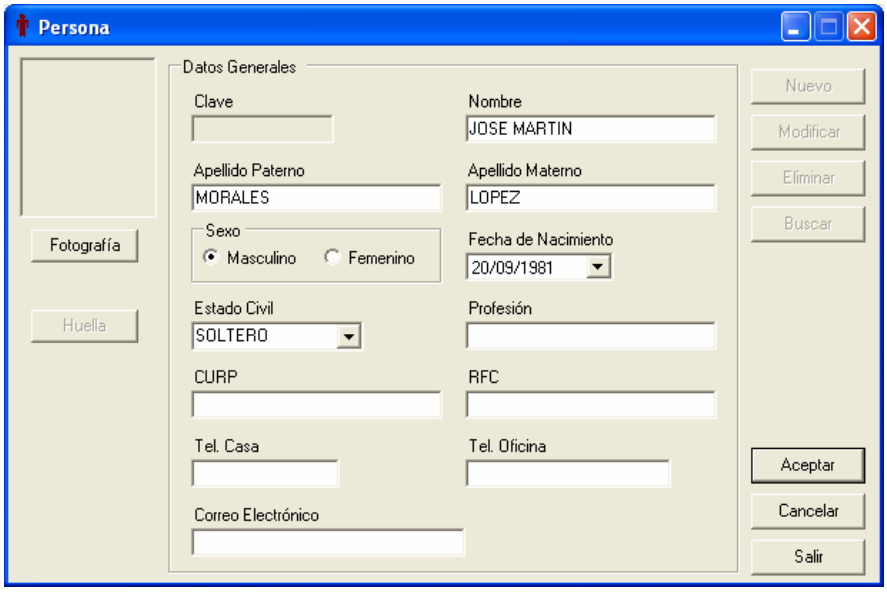


Figura 6. Catálogo de Persona

Huella

Dentro del catálogo de **Persona**, existe un botón con el título de **Huella**, este botón sólo se habilita si se ha seleccionado una persona con el botón buscar, o se registra una nueva persona. Al dar clic sobre el botón **Huella**, se muestra la pantalla **Opciones Huella** (figura 7). En ella es posible elegir si se registra, modifica o elimina la huella dactilar que corresponde a la persona seleccionada anteriormente.

Figura 7. Opciones de Huella

Registro de Huella

Al elegir la opción de **Registrar**, aparecerán las siguientes ventanas. Ver figura 8, 9 y 10. En la primera pantalla, se debe seleccionar la mano y dedo que corresponderá a la huella que será registrada de cada persona.

Figura 8. Registro de huellas

Figura 9. Captura de la huella

Al dar clic en **Siguiente**, el sistema esta listo para poder capturar la huella, se tomarán cuatro muestras de la huella seleccionada para su registro. Una vez capturadas las cuatro huellas, se habilita el botón **Siguiente** para poder continuar con el registro, de lo contrario permanecerá inhabilitado hasta que se hayan capturado todas las huellas (figura 9).

En la siguiente ventana se presentan las cuatro muestras de la huella dactilar que se capturaron previamente; si el usuario esta conforme con ellas se oprime el botón **Finalizar**, sino, al dar clic en **Recapturar**, aparecerá nuevamente la pantalla de **Captura de Huellas**. Ver figura 10.

Figura 10. Confirmar el registro de huella

Modificar Huella

Al seleccionar la opción de **Modificar** en la ventana de **Opciones de Huella** se visualizarán las siguientes ventanas (figura 11, 12 y 13). Sólo se muestra esta pantalla si la persona elegida previamente tiene alguna huella registrada, de lo contrario el sistema muestra un mensaje y regresa al catálogo de **Persona**. En la figura 10 se muestra la opción para modificar la huella del usuario, aparecerá el nombre, la mano y el dedo o dedos de las huellas que se tienen ya registradas.

Figura 11. Modificación de huellas

Se solicitará nuevamente ingresar cuatro muestras de la huella elegida (figura 12).

Figura 12. Captura de huellas

Posteriormente se confirma que las muestras sean correctas de lo contrario se vuelven a capturar dando clic en el botón **Recapturar** (figura 13).

Figura 13. Confirmar modificación de la huella

Eliminar Huella

La opción **Eliminar** muestra la ventana de la figura 14. Esta ventana tienen una lista de todos los dedos que tenga registrada esa persona, para eliminar un registro basta con desmarcar el dedo que se desea borrar y dar clic en **Aceptar**.

Figura 14. Eliminar registro de huella

Generación de Reportes

En el menú principal se encuentra una opción con la cual se muestra la pantalla donde se generarán los reportes de personas, usuarios o accesos dependiendo de

la opción seleccionada, además de seleccionar el tipo de reporte, la pantalla presenta algunas opciones para filtrar los datos que se desea visualizar, como por ejemplo el tipo de usuario, la fecha de acceso, una persona en especifico, etc. Ver (figura15).

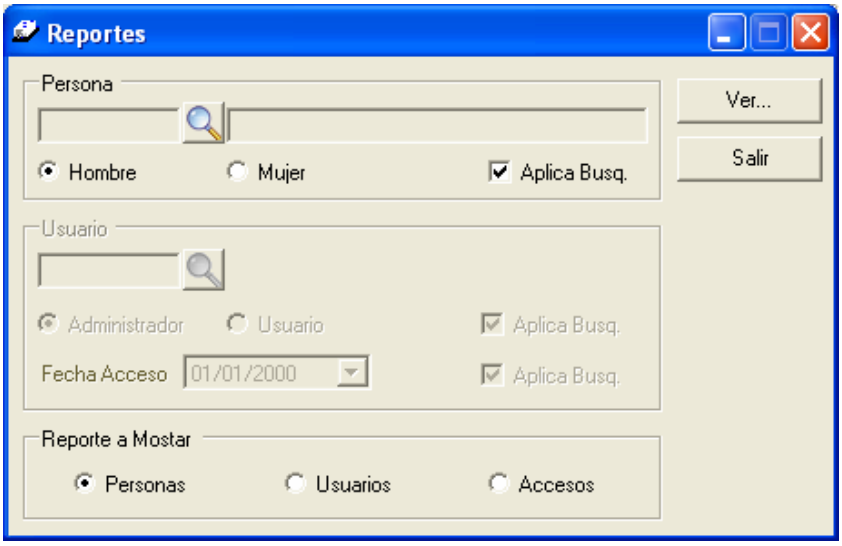


Figura 15. Generar reportes

Si la opción elegida para mostrar es el **Reporte de Usuarios** se presentará de la siguiente manera. Ver figura 16.

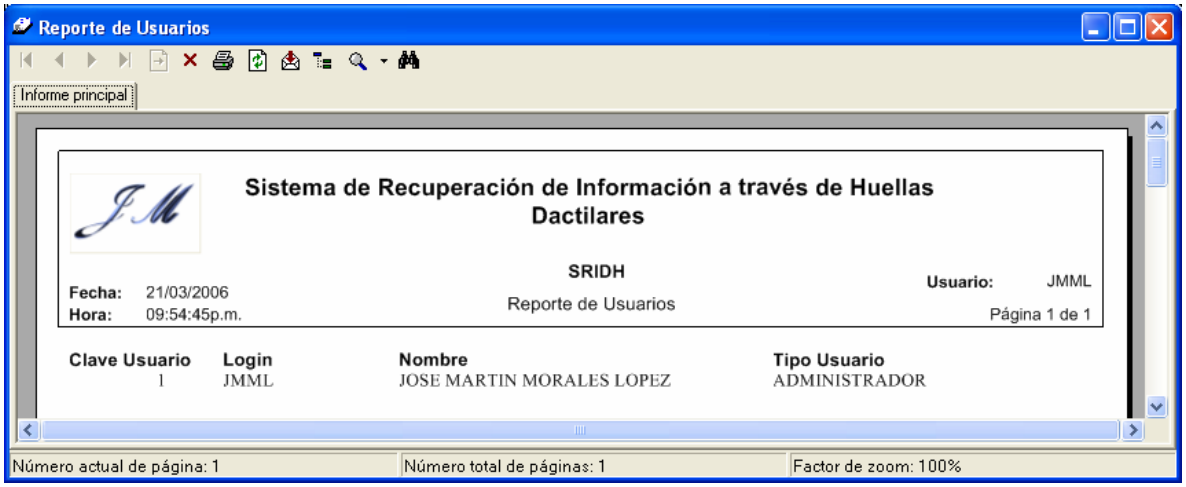


Figura 16. Reporte de Usuarios

El **Reporte de Personas** y **Reporte de Accesos** se presentan en las figura 17 y figura 18 respectivamente.

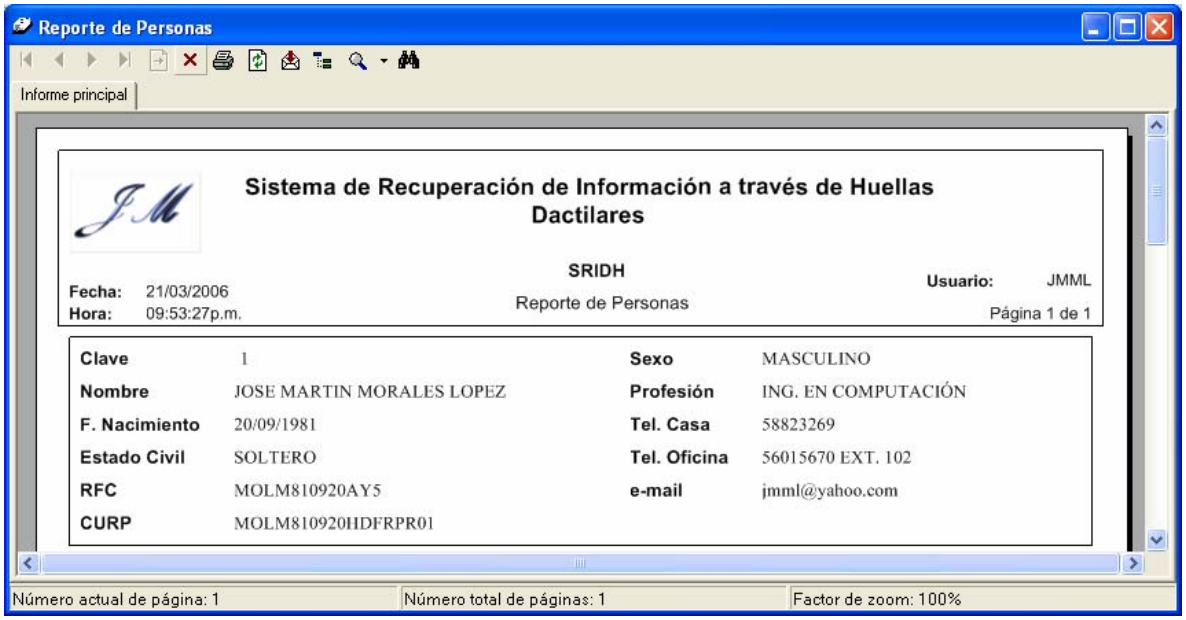


Figura 17. Reporte de Personas

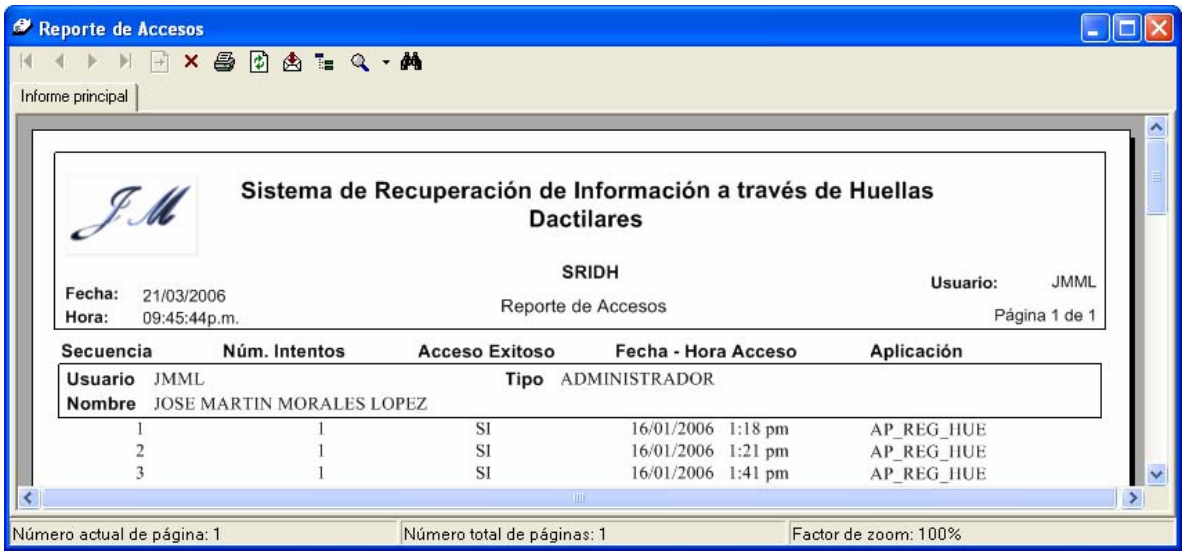


Figura 18. Reporte de Accesos

MANUAL TÉCNICO

Es importante contar con un manual técnico que muestre el Back End del sistema, esto será de gran utilidad para quien administre el sistema ya que se mostrará información y requerimientos técnicos necesarios en la instalación del sistema.

En la tabla 1 se muestran los requerimientos mínimos para instalar y operar adecuadamente el sistema SRIHD.

Procesador	Procesador Pentium III, con velocidad superior a 500 Megahertz (MHz)
Memoria	256 MB de RAM o superior
Disco Duro	500 MB en el disco de sistema, 2.0 gigabytes (GB) en el disco a instalarse
Video	Super VGA (1024x768) o pantalla de resolución más alta con 256 colores
Periféricos Obligatorios	➢ Unidad de CD ROM 4x o superior ➢ Mouse o dispositivo compatible ➢ Lector de huellas dactilares U.are.U 4000B Reader ➢ Interface de Red LAN 10/100 ➢ 1 Puerto disponible USB 2.0
Software	➢ Sistema operativo Windows XP Professional con Service Pack 2 ➢ Adobe Reader 5 o superior ➢ Controladores para el dispositivo U.are.U 4000B Reader v. 2.2.4.85 ➢ Office 2000 o superior

Tabla 1. Requerimientos mínimos para la instalación del sistema SRIHD

Mantenimiento de la base de datos

Es necesario restaurar la base de datos para poder manipularla, para ello se necesita como primer paso, una vez instalado SQL Server 2000, desde el menú de inicio:

- Abrir la opción **Administrador Corporativo**
- En la opción **Raíz de la consola** seleccionar la opción **Servidores Microsoft SQL Server** y a su vez **Bases de datos** que se encuentra dentro de **(local)(Windows NT)**
- Dar clic con botón derecho del mouse y seleccionar la opción **Todas las tareas** -> **Restaurar base de datos…** como se muestra en la figura 1.

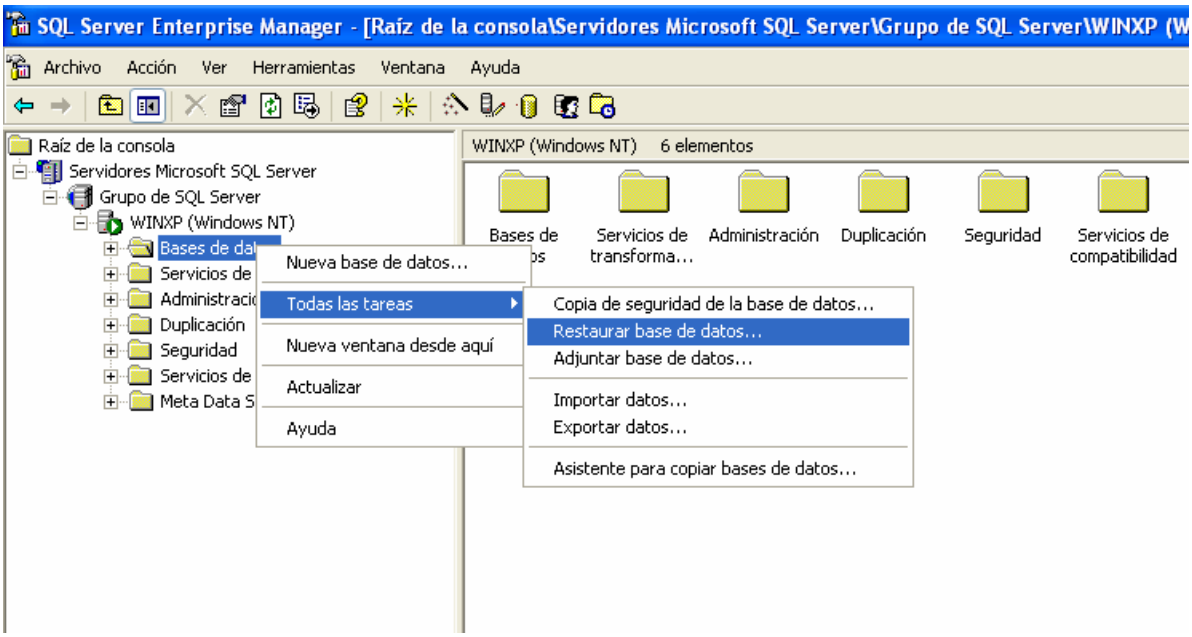


Figura 1. Opción de restauración de la base

Aparecerá una ventana como la que se muestra en la figura 2, para establecer las condiciones de restauración de la base de datos.

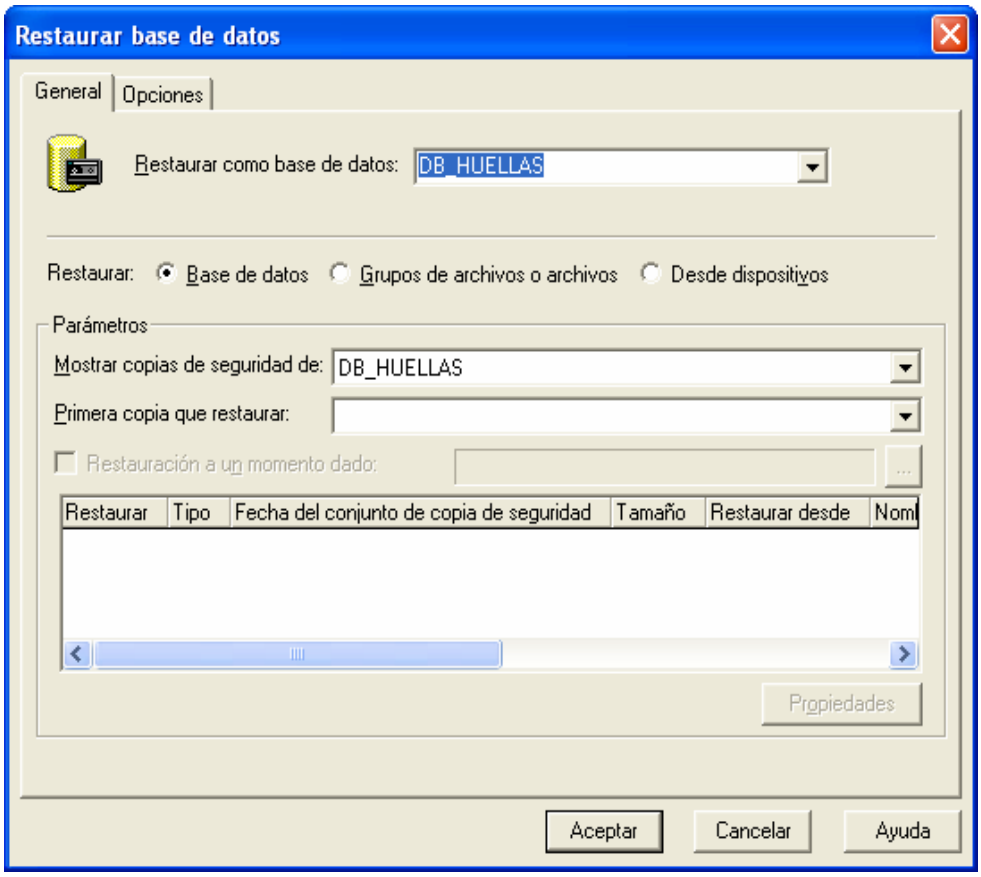


Figura 2. Restaurar base de datos

Si es necesario restaurar desde dispositivo se selecciona la opción **Desde dispositivo** y aparecerá la siguiente ventana (figura 3).

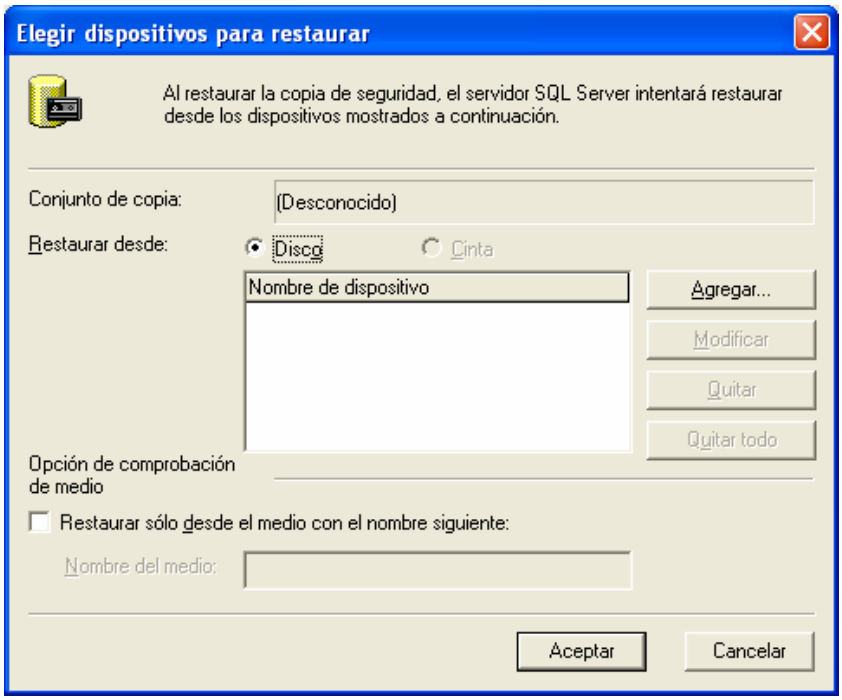


Figura 3. Seleccionar dispositivo de restauración

En la siguiente ventana se escoge la ruta donde se restaurará la base figura 4.

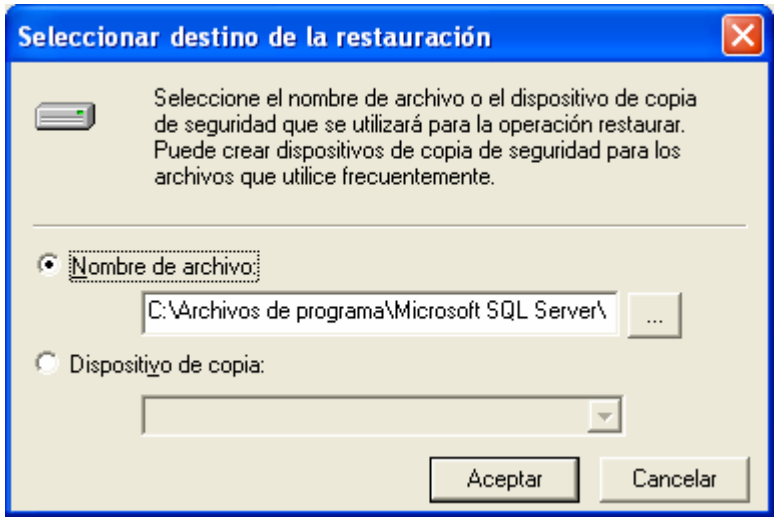


Figura 4. Ruta donde se va a restaurar la base

Una vez seleccionada la base de datos que se desea restaurar se debe dar clic en **Aceptar** y se llevará acabo la restauración de la base de datos figura 5.

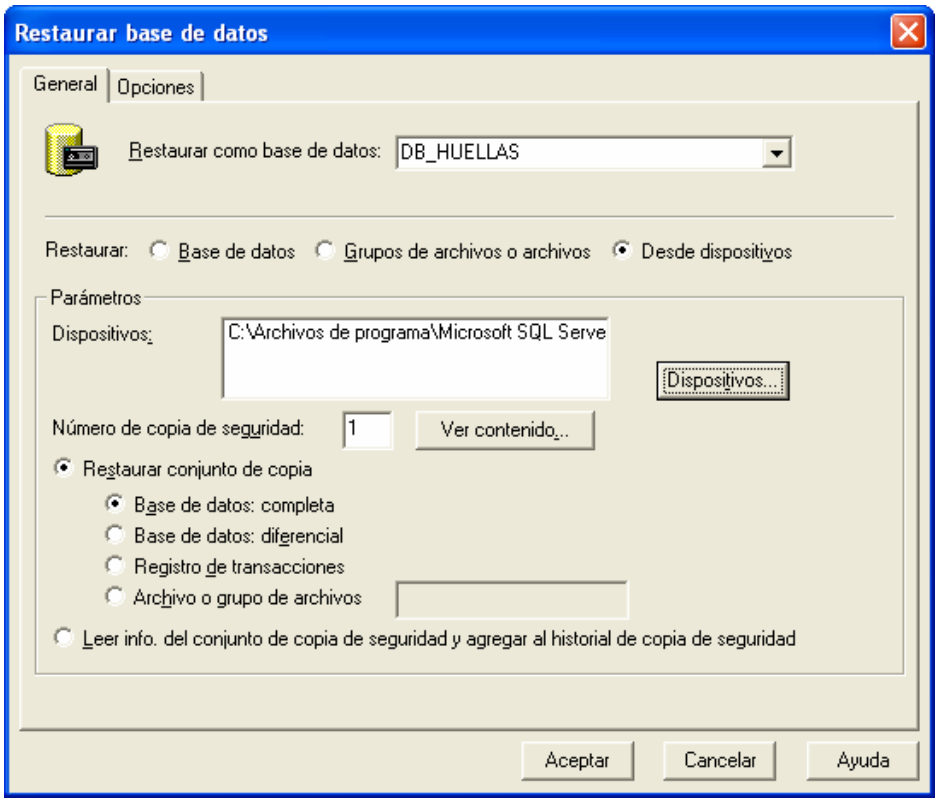


Figura 5. Restauración completa de la base de datos

Conclusiones

El objetivo principal de este trabajo fue el plantear las bases para implementar un sistema capaz de obtener información a través de la huella dactilar, el objetivo se cumplió al desarrollarlo a la par del presente documento que le dio seguimiento a sus múltiples etapas. El sistema es capaz de recuperar el historial de la persona y registrar accesos a las aplicaciones, en el caso de equipos de cómputo, quedando listo para su implementación en cualquier empresa de gobierno o del sector privado que la necesite, no olvidando que esta aplicación se pretende que sea un punto de partida para futuros proyectos más sofisticados, y poder así contribuir con la innovación tecnológica del país.

En cuanto al desarrollo del sistema SRIDH, la integración de las aplicaciones que provee la suite de desarrollo de Visual Studio .NET de Microsoft es de gran utilidad, ya que aprovechando las ventajas de cada uno de los productos que contiene el IDE el desarrollo la integración de un sistema es relativamente sencilla a través de los servicios del sistema operativo Windows.

Para finalizar, durante el desarrollo del presente trabajo se observó el proceso de análisis, diseño implementación y pruebas de un sistema real, lo cual comprueba que los conocimientos adquiridos en las materias impartidas en la carrera de Ingeniería en Computación de la FES Aragón dotan al egresado de los conocimientos necesarios para el desarrollo de cualquier sistema.

Apéndice A

Especificaciones técnicas del lector de huellas dactilares U.are.U 4000B Reader

U.are.U 4000B Reader

USB Fingerprint Reader
Part Number 50008-001

digitalPersona

Applications

- Desktop PC security
- Mobile PCs
- Custom applications
- Home and Office Use

Features

- Small form factor
- Excellent image quality
- Encrypted image data
- Fake finger rejection
- Low cost
- Rugged
- Works well with dry, moist, or rough fingerprints
- Compatible with all U.are.U applications
- Compatible with Windows XP, 2000, Me, 98, NT4.0 and Windows Server 2003

Product Description

The **U.are.U 4000B** is a USB fingerprint reader designed for use with DigitalPersona's U.are.U applications and developer tools.

The user simply places his/her finger on the glowing reader window, and the device quickly and automatically captures the fingerprint image. On-board electronics calibrate the device and encrypt the image data before sending it over the USB interface.

DigitalPersona products utilize optical fingerprint scanning technology for superior image quality and product reliability. The **U.are.U 4000B** reader and DigitalPersona recognition software have an unmatched ability to identify even the most difficult fingerprints.

Key Specifications

- Pixel resolution:
  - 512 dpi (average x,y over the field)
- Image capture area:
  - 14.6 mm (nom. width at center)
  - 18.1 mm (nom. length)
- 8-bit grayscale (256 levels of gray)
- Reader size (approximate):
  - 79 mm x 49 mm x 19 mm
- Compatible with USB 1.0, 1.1 and 2.0 (full-speed) Specifications
- 0.01% False Accept Rate with <1% False Reject Rate using DigitalPersona recognition software

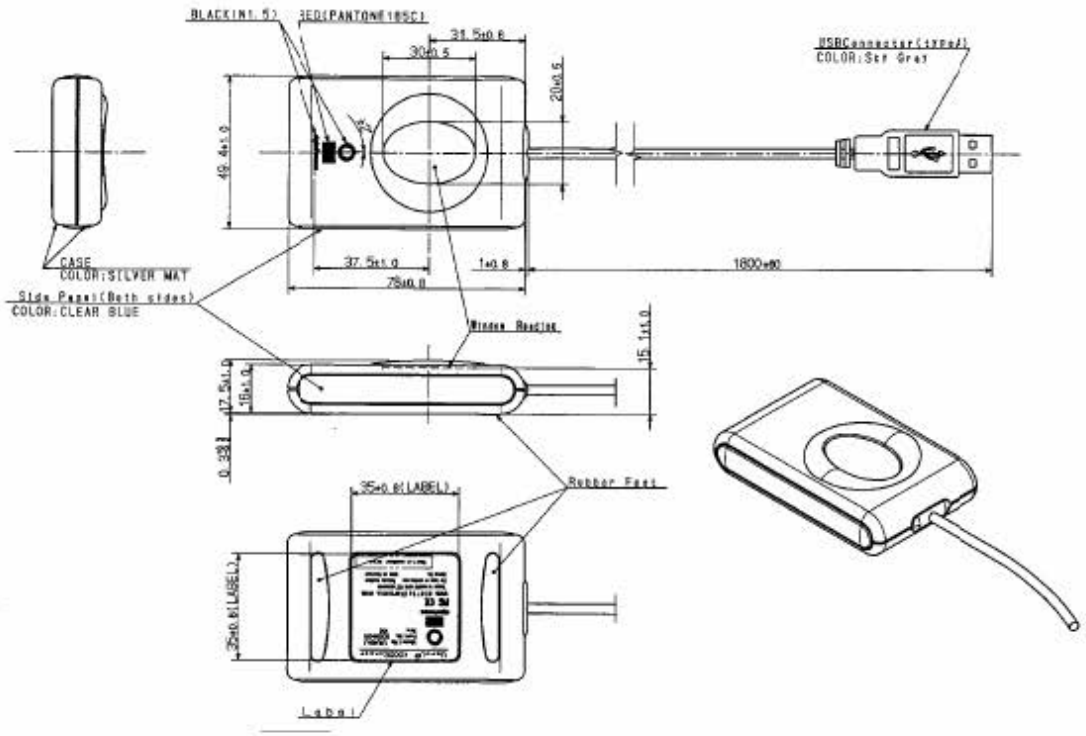
Technical data subject to change without notice
Digital Persona, Inc., 720 Bay Road, Suite 100, Redwood City, CA 94063 USA
Tel: (650) 474-4133 Fax: (650) 298-8318
www.digitalpersona.com email: sales@digitalpersona.com

Part Number	Description
50008-001	DigitalPersona USB fingerprint reader

Ratings

Supply Voltage	5.0V ±5% supplied by USB
Supply Current – scanning	190 mA (typical)
Supply Current – idle mode	140 mA (typical)
Supply Current – suspend mode	1.5 mA (maximum)
ESD Susceptibility	>15 KV, mounted in case
Temperature, Operating	0° - 40° C
Humidity, Operating	20% - 80% non-condensing
Temperature, Storage	-10° - 60° C
Humidity, Storage	20% - 90% non-condensing
Image data	8-bit grayscale
Standards Compliance	FCC Class B, CE, USB, WHQL

Mechanical Specification



Technical data subject to change without notice
Digital Persona, Inc., 720 Bay Road, Suite 100, Redwood City, CA 94063 USA
Tel: (650) 474-4133 Fax: (650) 298-8318
www.digitalpersona.com email: sales@digitalpersona.com

Glosario

Active Server Pages (ASP). Tecnología del lado servidor de Microsoft que permite combinar elementos HTML y componentes reutilizables de ActiveX con documentos *scripts* para crear páginas dinámicas en la Web.

ActiveX. Controles propios del entorno Windows, utilizados en programación. Denominados antiguamente OCX, son módulos separados del programa principal, que se distribuyen con él mismo. Tienen la ventaja de ser portables entre unos y otros lenguajes y su contenido puede ser cualquiera, no tienen una utilidad específica para un desarrollo concreto.

ActiveX Data Object (ADO). Interfaz de Microsoft que permite el acceso rápido a diferentes clases de base de datos.

Application Programming Interface (API). Colección de funciones que un entorno concreto (por ejemplo, un Sistema Operativo) pone a disposición del usuario para poder interactuar con él.

Back End. Es la parte del software que procesa y almacena los datos introducidos desde el Front End.

Bus. Concepto muy amplio referido al hardware de la computadora. En general, son caminos por los que se desplaza la información a través de los elementos encargados de manipularla. Por ejemplo entre la CPU y los discos o la memoria de la computadora.

Cliente/Servidor. Arquitectura a dos capas, es decir, una capa servidor, u computadora que contendrá los datos y los programas gestores asociados, y capas clientes, u computadoras que se dirigirán al anterior para obtener información.

Component Object Model (COM). Arquitectura de Software que permite construir aplicaciones a partir de componentes de software binarios, con el objeto de expandir las funciones del sistema operativo a nivel personalizado.

Controladores. Software que permite al Sistema Operativo reconocer y utilizar los periféricos que se tienen conectados a la computadora.

DataBase Management System (DBMS). Es un tipo de software muy específico, dedicado a servir de interfaz entre las bases de datos y las aplicaciones que la utilizan. Se compone de un lenguaje de definición de datos, un lenguaje de manipulación de datos y un lenguaje de consulta.

EEPROM. Memoria ROM que se puede grabar y borrar tantas veces como se desee. El proceso de borrado se realiza eléctricamente.

Ethernet. Nombre de una tecnología de redes de computadoras de área local (LAN´s) basada en tramas de datos.

Framework. En el desarrollo de software, es una estructura de soporte definida en la cual otro proyecto de software puede ser organizado y desarrollado. También puede incluir soporte de programas y librerías para ayudar a desarrollar y unir los diferentes componentes de un proyecto.

Front End. Es la parte del software que interactúa con el usuario. El Front End es el responsable de recolectar los datos de entrada del usuario, que pueden ser de muchas y variadas formas como pueden ser las pantallas de una aplicación.

Hipertexto. Texto que contiene elementos a partir de los cuales se puede acceder a otra información.

IEEE 1394. Estándar multiplataforma para entrada/salida de datos en serie a gran velocidad. Suele utilizarse para la interconexión de dispositivos digitales.

Integrated Development Environment (IDE). Programa compuesto por un conjunto de herramientas para el desarrollo de aplicaciones, puede dedicarse en exclusiva a un sólo lenguaje de programación o bien, puede utilizarse para varios. Sus componentes principales son un editor de texto, un compilador, un intérprete y un depurador.

Local Area Network (LAN). Interconexión de varias computadoras y periféricos para compartir recursos e intercambiar datos y aplicaciones. Su extensión esta limitada físicamente a un edificio o a un entorno de unos pocos kilómetros.

Microsoft Transaction Server (MTS). Sistema de procesamiento de transacciones basado en componentes para desarrollar aplicaciones distribuidas.

Object Linking and Embedding (OLE). Conjunto de bibliotecas, que permiten crear conexiones entre aplicaciones distintas, aunque también permite la interacción entre el Sistema Operativo y otros programas.

Peripheral Component Interconnect (PCI). Bus estándar para conectar dispositivos periféricos directamente a la placa base de una PC, estos dispositivos pueden ser circuitos integrados ajustados a ésta.

Perl. Lenguaje de programación traducido, no compilado, dirigido a servidores de Internet en Unix y Linux (principalmente). Este lenguaje se utiliza en los servidores Web gracias a sus posibilidades de creación desde pequeñas rutinas o enlaces hasta grandes servidores de comercio electrónico.

PHP. Lenguaje de programación destinado a la Red, y que una vez interpretado por el servidor Web genera código HTML.

Píxel. (Del inglés *picture element*). Representa el elemento más pequeño que compone una imagen digital, que se define por su brillo y color.

Programación Orientada a Objetos (POO). Es un método de implementación en el que los programas se organizan como colecciones cooperativas de objetos, cada uno de los cuales representa una instancia de alguna clase, y cuyas clases son todas miembro de una jerarquía se clases unidas mediante relaciones de herencia.

Query. Consulta a una base de datos generalmente utilizando sentencias SQL.

ROM. Memoria no volátil en la que la información se almacena de forma permanente, pudiendo ser recuperada pero no modificada. La memoria ROM, a diferencia de la memoria RAM, conserva su contenido. Este tipo de memorias se emplea para almacenar código de autocomprobación o instrucciones de inicialización del sistema.

Service Pack. Nombre que da Microsoft a las actualizaciones que corrigen errores del sistema operativo o le añaden características nuevas. También existen Service Pack para paquetes como Office.

Servidor. Computadora o sistema que comparte sus recursos con otras máquinas, denominadas clientes, que se los solicitan.

Site. Máquina remota que realiza solicitudes o consultas en el servidor, se encuentra determinado por la dirección IP de la máquina.

TCP/IP. Protocolo en el que se basa Internet y que en realidad consiste en dos. El TCP, especializado en fragmentar y recomponer paquetes y e IP, para direccionarlos hasta su destino.

Token Ring. Arquitectura de red con topología lógica en anillo y técnica de acceso de paso de testigo o *token*.

UML. Se le denomina así al Lenguaje Unificado de Modelado, basados en los primeros métodos de Programación Orientada a Objetos (POO) y está pensado para realizar análisis completos para desarrollo de aplicaciones de dimensiones amplias.

Universal Serial Bus (USB). Interfaz que provee un estándar de bus serie para conectar dispositivos a una computadora (generalmente a una PC).

Bibliografía

[1] Charte Ojeda Francisco
Programación con Visual Basic .NET
Primera edición
Ed. Anaya Multimedia, 2002, 672 pp.

[2] Hawryszkiewycz I. T.
Análisis y Diseño de Base de Datos
Primera edición
Ed. Megabyte, Noriega Editores, 1994, 671 pp.

[3] Laudon Kenneth C. y Laudon Jane Price
Administración de los Sistemas de Información: Organización y Tecnología
Tercera edición
Ed. Prentice-Hall, 1996, 885 pp.

[4] Silberschatz Abraham, Korth Heny F. y Sudarshan S.
Fundamentos de Bases de Datos
Tercera edición
Ed. Mc Graw Hill, 1998, 739 pp.

[5] Carlo Batini, Stefano Ceri y Shamkant B. Navathe
Diseño conceptual de Bases de Datos: Un enfoque de entidades interrelaciónales

Primera edición
Ed. Addison Wesley, 1994, 546 pp.

[6] Hansen Gary W. y Hansen James V.
Diseño y Administración de Bases de Datos
Segunda edición
Ed. Prentice Hall, 1997, 608 pp.

[7] Date, C. J.
Introducción a los Sistemas de Bases de Datos
Quinta edición
Ed. Addison - Wesley, 1993, 860 pp.

[8] Witten Jeffrey L., Bentely Lonnied D. y Barlow Victor M.
Análisis y diseño de Sistemas de Información
Tercera edición
Ed. Mc Graw Hill, 1996, 800 pp.

[9] Harris Shon
CISSP Certification: All-in-one Exam Guide
Second edition
Ed. Mc Graw Hill, 2003, 1008 pp.

[10] Krutz Ronald L. y Vines Rusell Dean
The CISSP Preparation Guide
First edition
Ed. Wiley, 2001, 556 pp

[11] Libros en pantalla de SQL Server, documentación de Microsoft® SQL Server™ 2000.

COLECCIONES DE URL

Internacional Biometric Group

http://www.biometricgroup.com

http://www.finger-scan.com

The Biometric Consortium

http://www.biometrics.org

Digital Persona, Inc.

http://www.digitalpersona.com

Oracle Corporation

http://www.oracle.com

MySQL Hispano

http://www.mysql-hispano.org

Database Journal

http://www.databasejournal.com

Borland

http://www.borland.com

Microsoft Windows XP

http://www.microsoft.com/windowsxp

http://www.microsoft.com/spain/download/seguridad/fiabilidad_windows.doc

http://www.microsoft.com/spain/download/seguridad/novedades.doc

MSDN (Microsoft Developer Network)

http://msdn.microsoft.com

http://www.microsoft.com/spanish/msdn/spain/default.mspx

TEC Electrónica

http://www.tec-mex.com.mx/promos/bit/bit0702-compts.htm

Ingeniería de Software

http://www.angelfire.com/scifi/jzavalar/apuntes/IngSoftware.html

SecurityDocs: Directory of information security articles

http://www.securitydocs.com/library/3003

TLDP-ES/LuCAS: Servicios editoriales para la documentación libre en español

http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node112.html

http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node113.html

WikiLearning

http://www.wikilearning.com/control_de_accesos_de_usuario-wkccp-3394-3.htm

Artículos de TI

http://www.pc-news.com/

http://www.iec.csic.es/criptonomicon/articulos/expertos47.html