UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

SISTEMA DE CONTROL DE ACCESO

T E S I S
QUE PARA OBTENER EL TITULO DE
INGENIERO EN COMPUTACION
PRESENTAN

IZANAMI MENDOZA GONZALEZ
SARAI MENDOZA GONZALEZ

Asesora: MTRA. MA. JAQUELINA LOPEZ BARRIENTOS

MEXICO, D.F. 2008

DEDICATORIAS

A mis padres,

Por brindarme el privilegio de la vida, por ser un ejemplo y guía excepcional, por su apoyo incondicional y mucho mas...

A mi hermana Citlalli,

Espero ser un buen ejemplo y apoyo para ti. Que el presente trabajo te inspire para alcanzar tus metas.

A Sergio,

Por todo el apoyo moral, sentimental e intelectual a lo largo de nuestra formación profesional.

Saraí Mendoza González

DEDICATORIAS

A mis padres,

Rosalía González y Miguel Ángel Mendoza por el apoyo, por fomentar en mí el deseo de saber, de conocer lo novedoso, por brindarme un hogar cálido y enseñarme que la perseverancia y el esfuerzo son el camino para lograr objetivos. Gracias por su amor incondicional.

A mi hermana,

Citlalli que tratando de mostrarte el mejor camino de la formación profesional te dedico con todo el corazón este trabajo el cual espero te motive a alcanzar tus objetivos. Siempre estaré para ti querida hermana.

A José Manuel,

Por ser la llave que siempre abre puertas, la mano que acompaña y tranquiliza. Porque en tu compañía las cosas malas se convierten en buenas, la tristeza se transforma en alegría y la soledad no existe. Gracias chiquito.

Izanami Mendoza González

AGRADECIMIENTOS

*A la **Universidad Nacional Autónoma de México** y en especial a la **Facultad de Ingeniería** por la formación profesional y ética.*

*A todos los **profesores** que participaron en nuestro desarrollo profesional durante la carrera, por todo el conocimiento transmitido, por los consejos proporcionados y por el ejemplo de la buena práctica.*

*A la **Mtra. Jaquelina López Barrientos** nuestra asesora, guía y amiga que nos brindó apoyo durante el desarrollo de este trabajo.*

G R A C I A S

Izanami y Saraí

Contenido

Capítulo 2. Análisis del sistema

Capítulo 3. Diseño del sistema

INTRODUCCIÓN

En los años en que la informática y las telecomunicaciones no presentaban tanto desarrollo no se sabía con exactitud cuál era la magnitud del problema de la falta de seguridad. Sin embargo actualmente la situación está cambiando, ya que la inseguridad se ha convertido en uno de los mayores problemas de la sociedad moderna, lo cual se confirma con la ayuda del desarrollo de las comunicaciones mundiales.

México no ha sido la excepción ya que ha presentado índices alarmantes de inseguridad, lo cual se ve reflejado en todos los sectores de la población.

En el caso específico de la comunidad universitaria hechos como asaltos, robos y extracción de materiales de oficina han sido la forma en que se ha manifestado este problema.

Ahora bien, si partimos de la definición etimológica de la palabra seguridad tenemos que:

El concepto “seguridad” proviene del latín *securitas* que a su vez se deriva del adjetivo *securus* , el cual está compuesto por *se*, sin y *cura*, cuidado o procuración, lo que significa sin temor, despreocupado o sin temor a preocuparse; es decir, la seguridad denota confianza: pensar que no debe pasar nada, tranquilidad: no debe tener amenaza, prevención: estar atento a todo riesgo, protección: tomar medidas preventivas, preservación: protegerse o cubrirse de algún riesgo, previsión: anticiparse a un hecho, defensa: resguardarse y estar a la defensiva, control: dominar todo tipo de mala reacción y por último estabilidad: firmeza antes, durante y después de algún riesgo.

Desde hace muchos años las empresas u organizaciones se conformaban con proporcionar a sus empleados un juego de llaves para acceder a su espacio laboral y resguardar así sus bienes materiales y la integridad física de sus trabajadores, con el paso del tiempo la inseguridad incrementó y surgió la necesidad a demás de contratar personal de seguridad. Desgraciadamente en el siglo XXI esto no ha sido suficiente y se ha tenido que echar mano del avance de la tecnología como por ejemplo los complejos sistemas de seguridad para el control de acceso físico, los cuales requieren de un identificador personal que permitan el acceso o deniegue el mismo.

Por lo que el objetivo del presente trabajo de tesis es: Diseñar e implementar un sistema de seguridad que proporcione la confidencialidad, integridad y disponibilidad de la información para controlar el acceso de personal a instalaciones resguardadas por empresas u organizaciones según sus intereses, considerando para ello criterios establecidos que le permitan otorgar o denegar dicho acceso, llevando un control del uso del sistema a fin de identificar situaciones de riesgo y emitir alarmas de seguridad.

Para lo cual en el capítulo 1 “Marco Teórico” se presenta a detalle toda la información considerada como un apoyo conceptual necesario para el desarrollo de la aplicación. Es decir, en este capítulo se describen los conceptos principales correspondientes a los temas *Seguridad Informática* y *Bases de Datos* desde los más básicos hasta los más específicos. Dentro de la *Seguridad Informática* se hace una introducción a lo que es: amenaza, ataque, ataque pasivo, ataque activo, escudo, vulnerabilidad, servicio de seguridad, confidencialidad, autenticación, integridad, control de acceso, disponibilidad y criptografía. Mientras que dentro de Bases de Datos se hace la introducción a lo que es: un dato, información, base de datos, DBMS, RDBMS, modelo relacional, llaves, asociaciones, relaciones y normalización.

En el capítulo 2 “Visión General del Sistema” se presenta el panorama de la problemática a resolver para que en función de esa problemática se establezcan los requerimientos lógicos que el sistema debe de cumplir organizados en base a tres niveles de usuarios identificados como: nivel administrador, nivel propietario y nivel usuario final. Se plantea además con base en los requerimientos de operación una alternativa de solución la cual consta de: un

sistema de software y un sistema de control electromagnético. Sin embargo a pasar de contar con una solución dividida en dos ramas, ambas pueden tener varias opciones de solución por lo que en este capítulo de muestran varias de ellas para realizar una comparación y un análisis que permita terminar con una elección de solución optima.

En el capítulo 3 “Diseño del Sistema” se desarrolla un diagrama de flujo de datos para permitir definir entradas, procedimientos y salidas de la información en el sistema KeYzara. Es importante contar con este diagrama porque muestra de manera gráfica los límites del sistema en desarrollo, los movimientos de los datos y la transformación de los mismos a través del mismo. Dentro de este capítulo también se desarrolla y presenta el diseño de la base de datos y la descripción de cada una de las tablas utilizadas.

El capítulo 4 “Funcionalidades del Sistema” tiene como objetivo describir la estructura y las principales funcionalidades con las que cuenta el sistema KeYzara a través de la explicación de cada una de las pantallas con las que cuenta el sistema.

En el capítulo 5 “Tendencias de la tecnología a futuro” se presenta un análisis de lo que puede llegar a ser la tecnología con el paso del tiempo en lo que corresponde al control de acceso.

Y finalmente en las conclusiones se mencionan los puntos benéficos que se obtienen con el desarrollo del software, algunas nuevas utilidades que se le podrían dar, el tiempo de vida estimado, y por último, se propone un escalamiento en el funcionamiento del sistema para un mayor control del mismo.

CAPÍTULO 1

MARCO TEÓRICO

En el presente capítulo, se mencionan algunos de los conceptos básicos de seguridad informática, necesarios para la implementación del sistema, tales como: amenazas, vulnerabilidades, servicios de seguridad y criptografía. Al igual que los conceptos básicos de Bases de Datos: dato, información, llave, modelo relacional, etc.

Haciendo énfasis en los servicios de seguridad, en los cuales se basa el tema de esta tesis y resaltando la importancia de la criptografía.

1.1 Seguridad informática

Garantizar que los recursos informáticos de una compañía estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos, es una definición útil para conocer lo que implica el concepto de seguridad informática.
En términos generales, la seguridad puede entenderse como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial. En este sentido, es la información el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales.

La seguridad es muy importante por la existencia de personas ajenas a la información, también conocidas como piratas informáticos o hackers, que buscan tener acceso a la red empresarial para modificar, sustraer o borrar datos. Tales personajes pueden, incluso, formar parte del personal administrativo o de sistemas, de cualquier compañía; de acuerdo con expertos en el área, más de 70 por ciento de las violaciones e intrusiones a los recursos informáticos se realiza por el personal interno, debido a que éste conoce los procesos, metodologías y tiene acceso a la información sensible de su empresa, es decir, a todos aquellos datos cuya pérdida puede afectar el buen funcionamiento de la organización.

Esta situación se presenta gracias a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías a nivel mundial, y porque no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas. El resultado es la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización, lo que puede representar un daño con valor de miles o millones de dólares.

Es así que toda organización debe estar a la vanguardia de los procesos de cambio ya que disponer de información continua, confiable y en tiempo, constituye una ventaja fundamental porque tener información es tener poder.

La información se reconoce como:

- Crítica, indispensable para garantizar la continuidad operativa de la organización.
- Valiosa, es un activo corporativo que tiene valor en sí mismo.
- Sensitiva, debe ser conocida por las personas que necesitan los datos.

Donde identificar los riesgos de la información es de vital importancia.

La seguridad informática debe garantizar:

- La Disponibilidad de los sistemas de información.
- La Recuperación rápida y completa de los sistemas de información
- La Integridad de la información.
- La Confidencialidad de la información.

1.1.1 Amenaza

Una amenaza se representa a través de una persona, una circunstancia o evento, un fenómeno o una idea maliciosa, las cuales pueden provocar daño cuando existe una violación de la seguridad.
Las amenazas de la seguridad provienen de diversas fuentes, entre ellas podemos mencionar las siguientes:

- De humanos
- Errores de hardware
- Errores de la red
- Problemas de tipo lógico
- Desastres

1.1.1.1 Ataque

Un ataque de la seguridad, no es más que la realización de una amenaza. Es decir, que las amenazas están en cualquier parte de nuestro entorno informático y cuando se presenta una oportunidad de realizar la violación, automáticamente se

está llevando a cabo un ataque. Cualquier ataque necesita, para efectuarse, tres elementos: motivación, capacidad y oportunidad.

Los ataques tienen varios objetivos incluyendo el fraude, la extorsión, el robo de información, la venganza o simplemente el desafío de penetrar un sistema. Esto puede ser realizado por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red.

Los ataques se clasifican tomando en cuenta si los perpetradores alteran o no la información, de manera tal que se tienen dos grandes grupos:

1.1.1.2 Ataque pasivo

Reciben su nombre debido a que el atacante – también llamado perpetrador, oponente o persona que se entromete – no altera en ningún momento la información, es decir, únicamente la observa, escucha, obtiene o monitorea mientras está siendo transmitida. Cualquier ataque pasivo tiene los siguientes objetivos principales:

- Intercepción de datos.
- Análisis de tráfico.

Con los ataque pasivos se obtiene información que puede consistir en:

- Obtención del origen y destinatario de la comunicación.
- Control del volumen de tráfico intercambiado entre las entidades monitoreadas.
- Control de las horas habituales de intercambio de daros entre las entidades de la comunicación.

Desafortunadamente los ataques pasivos son muy difíciles de detectar e interceptar, debido a que no provocan ninguna alteración de los datos. Aún cuando su detección es prácticamente imposible, es necesario tomar en cuenta que puede evitarse el éxito de este tipo de ataques si se considera el uso del

cifrado de la información, así como la existencia y utilización de otros mecanismos.

1.1.1.3 Ataque activo

Se nombran así debido a que implican algún tipo de modificación de flujo de datos transmitido (modificación de la corriente de datos) o la creación de un falso flujo de datos (creación de una corriente falsa).

Los ataques activos pueden clasificarse de la siguiente manera:

- Enmascaramiento o Suplantación de identidad.
- Réplica o Reactuación.
- Modificación de mensajes.
- Degradación fraudulenta del servicio.

1.1.1.4 Escudo

Un escudo es una técnica, procedimiento o cualquier otra medida que reduzca la vulnerabilidad, un escudo hace que las amenaza se vuelvan débiles o probablemente haya menos.

1.1.2 Vulnerabilidad

Una vulnerabilidad es una debilidad que puede ser explotada para violar la seguridad.

1.1.3 Servicios de seguridad

Un servicio de seguridad es el segundo aspecto que se considera en la seguridad de la información – cabe recordar que el primer aspecto es el ataque de seguridad.
Un servicio de seguridad es aquel que mejora la seguridad de un sistema de información y el flujo de la información de una organización. Los servicios están

dirigidos a evitar los ataques de seguridad y utilizan uno o más mecanismos de seguridad para proveer el servicio.

Los servicios de seguridad se clasifican dentro de seis grandes grupos:

1.1.3.1 Confidencialidad

Es la capacidad de asegurar que solo las personas autorizadas tienen acceso a algo. Es un aspecto primario y sumamente importante de la seguridad, significa mantener la información secreta para proteger los recursos y la información contra el descubrimiento intencional o accidental por personal no autorizado, es decir, es la protección de los datos transmitidos de cualquier ataque pasivo.
Los servicios de confidencialidad proveen protección de los recursos y de la información en términos del almacenamiento y la información, para asegurar que:

- Nadie pueda leer, copiar, descubrir o modificar la información sin autorización.
- Nadie pueda interceptar las comunicaciones o los mensajes entre entidades.

Estos dos aspectos de la confidencialidad son llamados confidencialidad de contenido y confidencialidad de flujo del mensaje.
La criptografía es utilizada para proveer los servicios de confidencialidad. De manera más sofisticada los métodos de cifrado basados en la criptografía son los mecanismos para asegurar que el descubrimiento no autorizado de la información sea computacionalmente imposible.

1.1.3.2 Autenticación

Es uno de los servicios más fáciles de comprender. Es simplemente: “verificar” la identidad.

Trata de asegurar que una comunicación sea auténtica. Es utilizada para proporcionar una prueba al sistema de que en realidad se es la entidad que se pretende ser.

La autenticación es realizada principalmente a través de:

- Algo que se sabe.
- Algo que se tiene.
- Algo que se es.

1.1.3.3 Integridad

En la integridad de los datos algo de lo más utilizado son lo sellos, especialmente en el área comercial.

En el mundo físico generalmente la verificación de la integridad de los "datos" se ha hecho en forma visual.

La integridad de datos provee controles que aseguran que el contenido de los datos no haya sido modificado, y que la secuencia de los datos se mantenga durante la transmisión. Al proporcionar la integridad de los datos se evita la inserción, borrado o cualquier otra modificación no autorizada.

Existen dos tipos de servicios: servicio de integridad del contenido y servicios de integridad de la secuencia del mensaje.

Los servicios de integridad de los datos pueden ofrecerse a través de varios mecanismos de seguridad:

- Código de detección de modificaciones.
- Código de autenticación del mensaje.
- Firma digital.
- Número de secuencia del mensaje.

1.1.3.4 No repudio

Previene a los emisores o a los receptores de negar un mensaje transmitido. Por lo que cuando un mensaje es enviado, el receptor puede probar que el mensaje

fue enviado por el presunto emisor. De manera similar, cuando un mensaje es recibido, el remitente puede probar que el mensaje fue recibido por el presunto receptor.

El no repudio se aplica al problema de la denegación falsa de la información que se recibe de otros o de la que uno ha enviado a otros. Los servicios de no repudio suministran pruebas que pueden ser demostradas a una tercera entidad. Los siguientes servicios son los que pueden ser proporcionados:

- No repudio de origen.
- No repudio de envío.
- No repudio de presentación.
- No repudio de transporte.
- No repudio de recepción.

1.1.3.5 Control de acceso

El acceso a un medio de información puede ser controlado ya sea a través de un dispositivo pasivo tal como una puerta cerrada o a través de un dispositivo activo como lo puede ser un monitor. Un monitor de control de acceso, determina qué usuario está autorizado para usar un recurso de manera requerida. Antes de otorgar el acceso, el monitor puede validar la identidad de usuario. En algunos casos, los procesos para determinar la autorización esta combinada con la autenticación.

En el contexto de la seguridad de la red, el control de acceso es la habilidad para limitar y controlar el acceso a los sistemas anfitriones y las aplicaciones mediante los puentes de comunicación. Para lograr este control, cada entidades que trata de ganar acceso pueden ser adaptados de manera individual.
Un control de acceso se ejecuta con el fin de que un usuario sea identificado y autenticado de manera exitosa para que entonces le sea permitido el acceso.
Los componentes básicos de un mecanismo de control de acceso son las entidades de red, los recursos de la red y los derechos de acceso. Los derechos de acceso describen los privilegios de la entidad o los permisos bajo cuáles

condiciones las entidades pueden tener acceso a un recurso de la red y cómo estas entidades son permitidas para tener acceso a un recurso de la red.

Ejemplos de los privilegios o permisos de una entidad:

- Creación o destrucción.
- Lectura o escritura.
- Adición, supresión o modificación del contenido.
- Exportación o importación.
- Ejecución.

Los privilegios o permisos pueden ser revocados y/o cambiados por el administrador autorizado de la red o del sistema en cuestión.
Los usuarios, loas recursos y la información pueden ser clasificados al asignarse diferentes niveles de seguridad, cualquier usuario permitido recibe autorización para un cierto nivel, por lo que puede tener acceso únicamente a la información que se encuentra clasificada en el nivel autorizado y niveles inferiores pero nunca podrá tener acceso a los niveles superiores al que se está autorizado.
El control de acceso puede ejecutarse de acuerdo a los niveles de seguridad y en recursos de la red particulares, pueden ejecutarse mediante la administración de la red o por una entidad individual de acuerdo a las políticas de control de acceso.

Una lista de control de acceso (LCA) puede ser empleada para la protección de los recursos individuales. Una LCA es una lista de permisos que determinan quién puede tener acceso a los recursos individuales de la red y qué puede hacerse con los recursos, esta lista deja que el propietario de u recurso permita o deniegue el acceso a los recursos a una entidad o a un grupo de entidades.

1.1.3.6 Disponibilidad

Se cumple si las personas autorizadas pueden acceder a la información deseada cuando lo requieran y tantas veces como sea necesario. Aclarando que la disponibilidad se refiere únicamente al tiempo para obtener la información y no importa si la información es correcta o no.

1.1.4 Criptografía

Es una rama de la criptología – un campo que trata con las comunicaciones seguras, la criptología es un arte tan antiguo como lo fue la propia escritura, permaneció durante muchos siglos relacionada muy directamente en el ámbito militar y diplomático, dado que éstos eran los únicos que en principio tenían auténtica necesidad de ella - , la otra rama de la criptología es el criptoanálisis éste se refiere a la ruptura o derrota de la criptografía, es decir, es el proceso que intenta descubrir el texto o la clave, la estrategia utilizada por el criptoanalista depende de la naturaleza del esquema de cifrado y de la información que tenga disponible. Por lo tanto la criptografía y el criptoanálisis siempre están unidos.

La criptografía (kryptós =escondido, oculto; graphé = grafía, escritura) es el arte y la ciencia de transformar la información para asegurar su secreto, su autenticidad o ambas y prevenir a los usuarios de acciones no autorizadas o ilegales en contra de la información, los recursos de red y los servicios, es decir, es la encargada del diseño de procedimientos, controlados por una clave, para cifrar o enmascarar una determinada información de carácter confidencial.

La criptografía está íntimamente relacionada con la seguridad y asume un papel cada vez más importante debido a la gran cantidad de información que las organizaciones actualmente necesitan generar, procesar, almacenar y / o distribuir de manera segura (confidencial e integra).

Por miles de años la criptografía ha sido utilizada para secretos militares y diplomáticos. Actualmente la criptografía es utilizada entre otras muchas actividades para:

- Autenticar transacciones comerciales y bancarias.
- Autenticar transacciones entre negocios o entre gobiernos y negocios.
- Proteger la integridad de las transferencias electrónicas de fondos.
- Proteger el secreto de las comunicaciones personales, militares y comerciales.
- Proveer el secreto y la integridad de las transacciones por Internet.
- Proteger la integridad del software y de las bases de datos.

- Autenticar la identidad de los usuarios de la red y las entidades.

La criptografía intenta garantizar:

- Discreción.
- Integridad de la información.
- Autenticación de usuarios.
- Autenticación de remitente.
- Autenticación del destinatario.
- Autenticación de actualidad.

En la criptografía, los mensajes originales se conocen como texto en claro o texto fuente y a la operación con la cual los símbolos básicos se transponen o sustituyen para transformar los datos, se denomina puesta en cifra. El resultado (mensaje cifrado) de la puesta en cifra se conoce como texto cifrado o criptograma, que luego es transmitido por un canal público. A este conjunto de elementos se le denomina criptosistema o sistema criptográfico el cual se aprecia en la Fig.1.1.

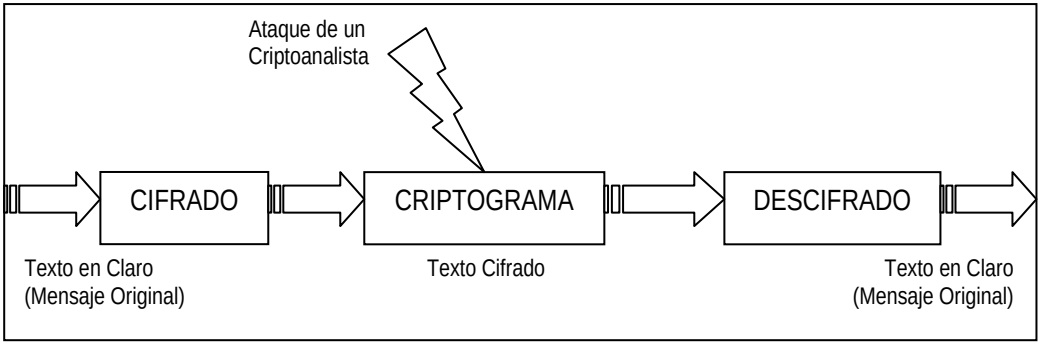


Fig.1.1 Proceso Criptográfico.

Los sistemas criptográficos se clasifican de acuerdo tres grandes grupos:

1. El tipo de operaciones utilizadas para transformar el texto en claro en texto cifrado. Todos los algoritmos de cifrado se basan en dos principios generales:

a) Sustitución: En el cual cada elemento del texto (bit, letra, grupo de bits o letras) es cambiado por otro elemento. Consiste en determinar una correspondencia entre las letras del alfabeto en que está escrito el mensaje original y los elementos de otro conjunto, el cual puede ser el mismo o diferente alfabeto. De tal manera cada letra del mensaje original se sustituye por su símbolo correspondiente en su elaboración del criptograma. El receptor, que conoce así mismo la correspondencia definida, recupera el mensaje original sustituyendo cada símbolo del criptograma por el símbolo correspondiente del alfabeto original. Existen tres tipos de sustitución:

- Sustitución monoalfabética.
- Sustitución por desplazamiento.
- Sustitución polialfabética.

b) Transposición: Los elementos del texto son reacomodados. Consiste en intercambiar los símbolos del mensaje original, de tal forma que el criptograma tenga los mismos elementos que el mensaje original pero que sea difícil de comprender. A diferencia de los métodos de sustitución, que reemplazan los elementos del texto en claro por símbolos, los métodos de transposición rodean las letras. Se cambia la posición de los caracteres en un mensaje.

2. El número de claves utilizadas

a) Algoritmos Simétricos: Si el emisor y el receptor usan la misa clave, el sistema es llamado cifrado simétrico, de clave simple, de clave secreta o convencional.

b) Algoritmos Asimétricos: Si el emisor y el receptor utilizan diferentes claves, el sistema es llamado sistema asimétrico, de doble clave o de clave pública.

3. La manera en que el texto es procesado.

a) Por bloque: Si el texto es procesado mediante un cifrador de bloque que opera sobre grupos o bloques de bits u octetos, generalmente 64 bits u 8 octetos, entonces u bloque de código procesa la entrada de un bloque de elementos a la vez, produciendo un bloque de salida por cada bloque de entrada.

b) Serial: Si se procesa el texto mediante un cifrador continuo que opera con cadenas continuas de datos, generalmente bits u octetos, entonces una secuencia de código procesa los elementos de entrada de manera continua, produciendo un elemento de salida a la vez.

1.1.4.1 Criptografía simétrica o de clave secreta

Los métodos simétricos son aquellos en los que la clave de cifrado es la misma que la clave de descifrado. Para ello, es necesario que la clave únicamente sea conocida por el emisor y el receptor. Dado que la misma clave es usada para cifrar y descifrar el mensaje, a este método de criptografía se le llamó “secreto compartido”, el término más formal para este método es la cronografía simétrica. Es importante mencionar que el cifrado convencional también es llamado cifrado simétrico, de clave secreta o de clave sencilla, y éste fue el primer tipo de cifrado en utilizarse a principios de 1970.

Un esquema de cifrado convencional cuenta con cinco elementos principales:

1. Texto en claro.
2. Algoritmo de cifrado.
3. Clave secreta.
4. texto cifrado o criptograma.
5. Algoritmo de descifrado.

Existen dos requerimientos para el uso seguro del cifrado convencional:

1. Se necesita un algoritmo de cifrado fuerte.
2. El emisor y el receptor deben tener copias de la clave secreta en un lugar secreto y deben mantenerla segura.

1.1.4.1.1 DES (Data Encryption Standard)

La Norma de Cifrado de Datos es un algoritmo para cifrar desarrollado por IBM e introducido en 1977 por el instituto Americano de estandarización y Tecnología, fue aprobado por la Oficina Nacional de Normas de los Estados Unidos como una Norma Oficial para la información no clasificadas y para ser usada por los sistemas de comunicaciones de los sectores privado y gubernamental.
El DES es un algoritmo de cifrado de bloque, donde la longitud de bloque es de 64 bits y la longitud de la clave es de 56 bits, si el texto es más grande entonces se procesa en bloques de 64 bits. La norma pide obligatoriamente que el DES se implemente mediante un circuito integrado electrónico.

1.14.1.2 IDEA (Internacional Data Encryotion Algorithm)

El algoritmo interna zonal de cifrado de datos, es un cifrado de bloque simétrico que fue desarrollado por Huejia Lai y James Massey del Instituto Federal Suizo de Tecnología en 1991, está diseñado par ser más seguro que el DES contra los ataques de fuerza bruta y diferentes tipos de criptoanalistas. IDEA difiere del Des tanto en la función iterativa como en la función generadora de subclaves. La efectividad de este tipo de cifrado está basada en el concepto de mezclar operaciones aritméticas de grupos algebraicos diferentes. La clave es de 128 bis, lo que hace que la búsqueda sea más difícil que para la clave de 56 bits del DES debido que la longitud de la clave es mayor y por lo tanto aumenta el número de operaciones aritméticas.

1.1.4.2 Criptografía asimétrica o de clave pública

Los métodos asimétricos son aquellos en los que la clave de cifrado es diferente a la de descifrado. En términos generales, la clave de cifrado es conocida por todo el público, mientras que la de descifrado sólo es conocida por el usuario. Los investigadores Whitfield Diffie y Martin Hellman, desarrollaron el uso de una clave asimétrica en 1975 para resolver el problema de poseer una solo clave simétrica. De esa manera, todos los que quieran comunicarse posiblemente

tienen un par de claves. Las dos claves utilizadas en un cifrado de clave pública son llamadas clave pública y clave privada.

Un esquema de cifrado de clave pública contiene los siguientes elementos:

- Texto en claro.
- Algoritmo de cifrado.
- Clave pública y privada.
- Texto cifrado.
- Algoritmo de descifrado.

Los sistemas criptográficos asimétricos pueden clasificarse, dependiendo de su uso, en tres categorías:

1. Cifrado y descifrado.
2. Firma digital.
3. Intercambio de claves.

1.1.4.2.1 Algoritmo RSA

Es uno de los primeros esquemas de clave pública desarrollado por Ron Rivest, Adi Shamir y Len Adleman en MIT 1978. El algoritmo está basado en la dificultad para realizar factorizaciones de números largos. RSA es un bloque cifrador en el cual el texto original y el texto cifrado son enteros entre 0 y n – 1 para cualquier n.

1.1.4.2.2 Algoritmo DIFFIE – HELLMAN

El primer algoritmo de clave pública que definía la criptografía de clave pública – generalmente se hace referencia a este algoritmo como el intercambio de clave Diffie – Hellman - , fue introducido por Diffie y Hellman en 1976, los cuales propusieron que se utilizara dicha idea para distribuir las claves secretas de cifrado. El propósito del algoritmo es habilitar a los dos usuarios para intercambiar una clave secreta de manera más segura que puede ser utilizada

para el subsecuente cifrado de mensajes. El algoritmo sólo se limita al intercambio de claves.

1.2. Bases de datos

1.2.1. Dato

Un dato es la unidad mínima de información, puede representar hechos, ideas o conceptos, que pueden ser reunidos y representados electrónicamente en forma digital. Los datos son hechos aislados y en bruto que deben ser procesados por varias operaciones para obtener resultados relacionados con la evaluación identificación de personas, eventos y objetos (información).

1.2.2 Información

La información es un conjunto de datos interrelacionados entre sí que tienen un significado del cual podemos obtener conocimientos para una futura toma de decisiones.
La información se obtiene asociando los hechos en un contexto determinado, es decir, la adición o el procesamiento de los datos proporcionan un conocimiento o entendimiento de ciertos factores.
Las operaciones que se les pueden aplicar a los datos son de dos tipos:

1. Lógicas: Seleccionar, Ordenar, Actualizar, Verificar, Calcular.
2. Técnicas: Clasificación, Almacenamiento, Destrucción, Reproducción y Distribución.

Características del valor de la información:

- Accesible: Facilidad y rapidez con que se obtiene la información.
- Clara: Integridad y entendimiento de la información sin ambigüedades.

- Precisa: Que sea la más exacta posible, hay dos tipos de errores: captura y cálculo.
- Propia: La relación entre el resultado y lo solicitado por el usuario.
- Oportuna: Menor duración del ciclo: entrada, procesamiento, entrega al usuario.
- Flexible: Adaptabilidad de la información a la toma de decisiones.
- Verificable: Examinar la información.
- Imparcial: No se puede alterar o modificar la información.
- Cuantificable: Datos procesados que producen información.

1.2.3 Base de datos

Una base de datos es un conjunto de datos relacionados entre sí con un objetivo común. Es un conjunto de datos integrados y generalizados, estructurados.

Una base de datos debe cumplir con las condiciones siguientes:

- Los datos han de estar almacenados juntos.
- Tanto los usuarios finales como los programas de aplicación, no necesitan conocer los detalles de las estructuras de almacenamiento.
- Los datos son compartidos por diferentes usuarios y programas de aplicación en el cual existe un mecanismo común de inserción borrado, actualización y consulta de los datos.
- Debe ser capaz de mantener la integridad, seguridad, consistencia y confidencialidad de los datos. Tanto datos como procedimientos pueden ser transportables conceptualmente a través de diferentes DBMS.

1.2.4. Sistema Manejador de Bases de Datos (DBMS)

Es un conjunto de programas que controla la organización, almacenamiento, recuperación, seguridad e integridad de los datos en una base haciendo uso de algún modelo de datos. Acepta pedidos de datos desde un programa de aplicación o cliente y le ordena al sistema operativo transferir los datos apropiados.

Cuando se usa un DBMS, los sistemas de información pueden ser cambiados más fácilmente a medida que cambian los requerimientos de la organización.
Así podemos decir que entre la base de datos física en sí (es decir almacenamiento real de la BD) y los usuarios del sistema existe un nivel de software, que a menudo recibe el nombre de sistema manejador de base de datos.
El sistema manejador de BD es el software que controla todos los accesos a la BD.

1.2.4.1 Componentes de los RDBMS (Relacional Data Base Management System)

- Lenguaje de definición de datos. (DDL). Permite crear y alterar objetos dentro de la base de datos.
- Lenguaje de manipulación de datos (DML). Permite insertar, actualizar, eliminar y consultar los datos.
- Lenguaje de control de datos (DCL). Permite otorgar o revocar permisos a nivel comando y objeto.
- Diccionario de datos. Datos acerca de los datos (metadatos).
- Almacena información acerca de la estructura de la BD, información de autorización, como las restricciones de la clave y sobre los datos mismos.

1.2.5. Modelo Relacional

Modelo lógico de una BD. Un DBMS utiliza un modelo de datos para definir la estructura fundamental de los mismos. Un modelo de datos expresa entidades y sus relaciones y es la herramienta utilizada para representar la organización conceptual de los datos.

Una BD relacional es aquella cuyos usuarios la perciben como un conjunto de tablas.

- Entidad: Es una persona, lugar, evento o un objeto identificado en forma única y del cual se registra información.
- Campo: Conjunto de datos de un mismo tipo.

- Registro: Conjunto de datos pertenecientes a una misma entidad. El registro consta de campos, cada campo tiene una longitud definida, por lo tanto los registros son de longitud fija.

- Tablas: Dentro del enfoque relacional es conocida como entidad de dos dimensiones (columna, renglón). Es una estructura de almacenamiento bidimensional, formada por tuplas (registros, renglón) y atributos (columnas, campos).

- Atributos: Características propias de la entidad, se modelan como columnas de una entidad. La forma de diferenciar las entidades es por medio de atributos y cada uno de ellos debe tener por lo menos un atributo diferente.

- Tuplas: Conjunto de valores que componen un renglón de la relación, es equivalente a una instancia de un registro. Es el renglón "n" de una tabla.

- Grado: Número de atributos que tiene una tupla.

- Cardinalidad: Número de tuplas de una relación.

- Propiedades del campo. Es la apariencia que tiene los datos, evita la introducción incorrecta de los mismos, especifica valores predeterminados, acelera la búsqueda y la ordenación de la tabla mediante índices. Las propiedades de los campos se visualizan y se modifican individualmente para cada campo.

1.2.5.1 Llaves

Se denomina llave o clave, al atributo que permite significar de manera única a una entidad. Una llave es en otras palabras, el campo a partir del cual se pueden inferir otros campos de una tabla, por lo que, cada tupla debe estar asociada con una llave que permita su identificación.

- Candidata: Atributo o conjunto de atributos que son susceptibles de ser elegidos como PK.

- Primaria (PK, Primary Key): Atributo o conjunto de atributos que permiten identificar de manera única cada renglón dentro de la tabla.

- Alterna (AK, Alternate Key): Atributo o conjunto de atributos que pueden ser seleccionados en un futuro como parte de la PK o incluso sustituirla.

- Foránea (FK, Foreing Key): Atributo o conjunto de atributos que en la tabla padre forman la llave primaria y en la tabla hija son un atributo más y en algunos casos con la relación fuerte forman parte de la llave primaria.

1.2.5.2 Asociaciones

Es la unión o enlace de dos o más entidades, las cuales se encuentran dentro del enlace del sistema y por ello el sistema debe mantener, correlacionar o desplegar información. Generalmente las asociaciones requieren de al menos dos entidades. Existen tres tipos de asociaciones:

Uno a uno. (1:1): Las ocurrencias de una entidad se pueden relacionar sólo a una ocurrencia de la otra entidad. Al modelar este tipo de asociaciones hay que hacerlo de manera que los valores nulos se minimicen o se eviten totalmente. Ver Fig.1.2.

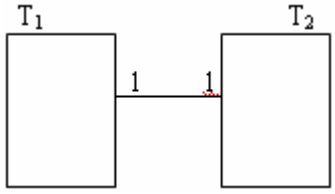


Fig.1.2 Asociación Uno a Uno (1:1)

Uno a muchos (1:M): Se dice que una relación entre entidades es uno a muchos sí: las ocurrencias de una entidad están relacionadas con una o varias de la otra entidad. Ver Fig.1.3.

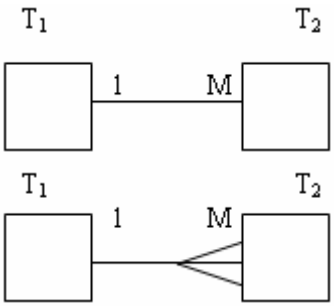


Fig.1.3. Asociación Uno a Muchos (1:M)

Muchos a muchos (M.M). Ocurren cuando se asocian una ocurrencia en una entidad con muchas ocurrencias en la otra entidad y viceversa. Ver Fig.1.4.

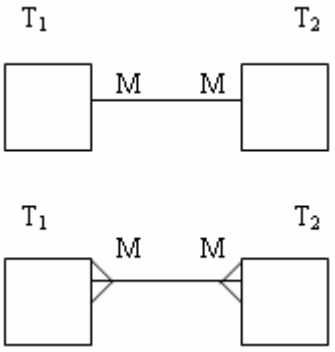


Fig.1.4 Asociación Muchos a Muchos (M:M)

1.2.5.3 Tipos de Relaciones

Las relaciones sirven para poder utilizar datos procedentes de otras tablas como si formaran parte de la tabla en la que se esté trabajando. Establecer una relación entre dos tablas equivale a establecer una unión entre ellas, para poder hacer esto se debe dar una condición muy concreta: en las dos tablas tiene que haber un

campo que contenga el mismo dato. Una relación describe cierta interdependencia (de cualquier tipo) entre dos o más entidades. Una relación no tiene sentido sin las entidades que relaciona.
DÉBIL (independiente). Ver Fig.1.5.

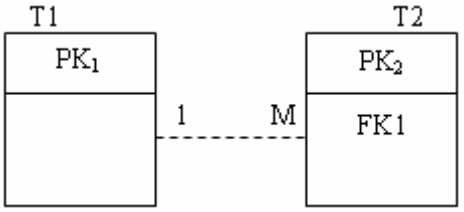


Fig.1.5. Relación débil (independiente)

FUERTE (dependiente). Ver Fig.1.6

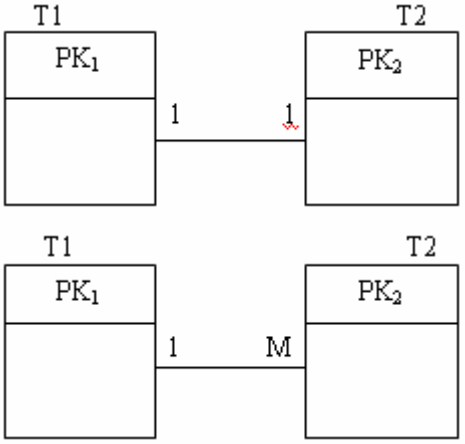


Fig.1.6 Relación fuerte (dependiente)

1.2.6. Normalización

La normalización es una técnica que se utiliza para comprobar la validez de los esquemas lógicos basados en el modelo relacional, ya que asegura que las relaciones (tablas) obtenidas no tengan datos redundantes. La normalización se utiliza para mejorar el esquema lógico, de modo que satisfaga ciertas

restricciones que eviten la duplicidad de datos. La normalización garantiza que el esquema resultante se encuentre lo más próximo al flujo de la información, que sea consistente y que tenga la mínima redundancia y la máxima estabilidad.
La normalización es un proceso que permite decidir a qué entidad pertenece cada atributo. Uno de los conceptos básicos del modelo relacional es que los atributos se agrupan en entidades (tablas) porque están relacionados a nivel lógico. En la mayoría de las ocasiones, una base de datos normalizada no proporciona la máxima eficiencia, sin embargo, el objetivo ahora es conseguir una base de datos normalizada por las siguientes razones:

- Un esquema normalizado organiza los datos de acuerdo a sus dependencias funcionales.
- El esquema lógico no tiene porqué ser el esquema final. Debe representar el significado de los datos, de hecho, la normalización obliga a entender completamente a cada uno de los atributos que se han de representar en la base de datos.
- Un esquema normalizado es robusto y carece de redundancias, por lo que está libre de ciertas anomalías que éstas pueden provocar cuando se actualiza la base de datos.
- Los equipos informáticos de hoy en día son mucho más potentes, por lo que en ocasiones es más razonable implementar bases de datos fáciles de manejar.
- La normalización produce bases de datos con esquemas flexibles que pueden extenderse con facilidad.

La normalización se lleva a cabo en una serie pasos. Cada paso corresponde a una forma normal que tiene unas propiedades. Conforme se va avanzando en la normalización, las relaciones tienen un formato más estricto y, por lo tanto, son menos vulnerables a las anomalías de actualización. El modelo relacional sólo requiere un conjunto de relaciones en primera forma normal. Las restantes formas normales son opcionales. Sin embargo, para evitar las anomalías de actualización, es recomendable llegar al menos a la tercera forma normal.

1.2.6.1 Primera forma normal (1FN)

Una relación está en primera forma normal si, y sólo si, todos los dominios de la misma contienen valores atómicos, es decir, no hay grupos repetitivos. Si se ve la relación gráficamente como una tabla, estará en 1FN si tiene un solo valor en la intersección de cada fila con cada columna.

Si una relación no está en 1FN, hay que eliminar de ella los grupos repetitivos. Un grupo repetitivo será el atributo o grupo de atributos que tiene múltiples valores para cada tupla de la relación. Hay dos formas de eliminar los grupos repetitivos. En la primera, se repiten los atributos con un solo valor para cada valor del grupo repetitivo. De este modo, se introducen redundancias ya que se duplican valores, pero estas redundancias se eliminarán después mediante las restantes formas normales. La segunda forma de eliminar los grupos repetitivos consiste en poner cada uno de ellos en una relación aparte, heredando la clave primaria de la relación en la que se encontraban.

1.2.6.2 Segunda forma normal (2FN)

Una relación está en segunda forma normal si, y sólo si, está en 1FN y, además, cada atributo que no está en la clave primaria es completamente dependiente de la clave primaria.

La 2FN se aplica a las relaciones que tienen claves primarias compuestas por dos o más atributos. Si una relación está en 1FN y su clave primaria es simple (tiene un solo atributo), entonces también está en 2FN. Las relaciones que no están en 2FN pueden sufrir anomalías cuando se realizan actualizaciones.
Para pasar una relación en 1FN a 2FN hay que eliminar las dependencias parciales de la clave primaria. Para ello, se eliminan los atributos que son funcionalmente dependientes y se ponen en una nueva relación con una copia de su determinante (los atributos de la clave primaria de los que dependen).

1.2.6.3 Tercera forma normal (3FN)

Una relación está en tercera forma normal si, y sólo si, está en 2FN y, además, cada atributo que no está en la clave primaria no depende transitivamente de la

clave primaria. La dependencia es transitiva si existen las dependencias, siendo atributos o conjuntos de atributos de una misma relación.
Aunque las relaciones en 2FN tienen menos redundancias que las relaciones en 1FN, todavía pueden sufrir anomalías frente a las actualizaciones. Para pasar una relación de 2FN a 3FN hay que eliminar las dependencias transitivas. Para ello, se eliminan los atributos que dependen transitivamente y se ponen en una nueva relación con una copia de su determinante (el atributo o atributos no clave de los que dependen).

1.2.6.4 Forma normal de Boyce-Codd (BCFN)

Una relación está en la forma normal de Boyce-Codd si, y sólo si, todo determinante es una clave candidata.
La 2FN y la 3FN eliminan las dependencias parciales y las dependencias transitivas de la clave primaria. Pero este tipo de dependencias todavía pueden existir sobre otras claves candidatas, si éstas existen. La BCFN es más fuerte que la 3FN, por lo tanto, toda relación en BCFN está en 3FN.

La violación de la BCFN es poco frecuente ya que se da bajo ciertas condiciones que raramente se presentan. Se debe comprobar si una relación viola la BCFN si tiene dos o más claves candidatas compuestas que tienen al menos un atributo en común.

Tanto el diseño conceptual, como el diseño lógico, son procesos iterativos, tienen un punto de inicio y se van refinando continuamente. El diseño conceptual y el diseño lógico son etapas clave para conseguir un sistema que funcione correctamente. Si el esquema no es una representación fiel del flujo de información, será difícil, definir todas las vistas de usuario (esquemas externos), o mantener la integridad de la base de datos. Además, hay que tener en cuenta que la capacidad de ajustarse a futuros cambios es un sello que identifica a los buenos diseños de bases de datos. Por todo esto, es fundamental producir el mejor esquema que sea posible.

CAPÍTULO 2

ANÁLISIS DEL SISTEMA

En el presente capítulo, se da un amplio panorama de la estructura del sistema de seguridad para el control de acceso físico "KeYzara", el cual tiene como principal objetivo proteger la integridad de las personas y de la información que resguarda.

2.1 Panorama de la problemática

Históricamente, las sociedades y el ser humano han tenido la necesidad de controlar el acceso a ciertas áreas y lugares. Esta necesidad es motivada inicialmente por temor que personas inescrupulosas o delincuentes puedan robar o extraer material valioso de acuerdo a criterios personales, sociales, comerciales, etc. Vemos cómo los castillos y fortalezas fueron construidos de tal forma que sus principales vías de acceso eran diseñadas con puentes que se elevaban o recogían mediante mecanismos manuales, quedando así abajo un círculo de agua y caimanes que rodeaban dicho castillo o fortaleza. En tal sentido, el acceso a estas edificaciones no sólo era posible suministrando un nombre. En efecto, las palabras claves (passwords), eran utilizadas por pocas personas para acceder al castillo. Este no fue el único mecanismo de seguridad de acceso, también se debía hacer un reconocimiento visual de las características de ella/él o de un único elemento, como por ejemplo un anillo.

Ahora bien, si hacemos referencia a las últimas décadas, las empresas u organizaciones contaban con controles de acceso físico que se basaban en proporcionar a sus empleados un juego de llaves para acceder a su espacio laboral y resguardar así sus bienes materiales y la integridad física de sus trabajadores; años después esos controles de acceso se basaban esencialmente en el trabajo de los vigilantes que en el mejor de los casos eran asistidos por equipos de circuito cerrado de televisión CCTV.

Hoy en día, tecnológicamente han cambiado ciertas cosas, pero en el fondo persisten las razones y motivos para mantener mecanismos de control de acceso sobre áreas e información que se desea proteger ya que actualmente la inseguridad se ha convertido en uno de los mayores problemas de las sociedades modernas y en donde México no es la excepción ya que ha presentado índices alarmantes de inseguridad, lo cual se ve reflejado en todos los sectores de la población. En el caso específico de la comunidad universitaria hechos como asaltos, robos y extracción de materiales de oficina han sido la forma en que se ha manifestado este problema.

Ahora bien, si partimos de la definición etimológica de la palabra seguridad tenemos que:

El concepto "seguridad" proviene del latín securitas que a su vez se deriva del adjetivo securus, el cual está compuesto por se, sin y cura, cuidado o procuración, lo que significa sin temor, despreocupado o sin temor a preocuparse; es decir, la seguridad denota **confianza**: pensar que no debe pasar nada, **tranquilidad**: no debe tener amenaza, **prevención**: estar atento a todo riesgo, **protección**: tomar medidas preventivas, **preservación**: protegerse o cubrirse de algún riesgo, **previsión**: anticiparse a un hecho, **defensa**: resguardarse y estar a la defensiva, **control**: dominar todo tipo de mala reacción y por último **estabilidad**: firmeza antes, durante y después de algún riesgo.

Con lo que nos podemos dar cuenta que con confianza, tranquilidad, prevención, protección, preservación, previsión, defensa, control y estabilidad no se cuenta dentro de los cubículos del Departamento de Ingeniería en Computación de la Facultad de Ingeniería por lo que diseñar e implementar un sistema de seguridad que tenga el control de las personas que accedan ayudaría a mitigar este serio problema que se enfrenta en Ciudad Universitaria.

Es por ello que el objetivo del presente trabajo sea el de diseñar e implementar el sistema de seguridad para el control de acceso físico "KeYzara", que proporcione la confidencialidad, integridad y disponibilidad de la información para controlar el acceso de personal a instalaciones resguardadas por empresas u organizaciones según sus intereses, considerando para ello criterios establecidos que le permitan otorgar o denegar dicho acceso, como por ejemplo, con base en su identidad, horarios y áreas autorizadas, llevando un control del uso del sistema a fin de identificar situaciones de riesgo y emitir alarmas de seguridad.

2.2 Descripción de los requerimientos lógicos del sistema

Tomando en cuenta lo establecido en el apartado previamente presentado, los requerimientos lógicos del sistema se dividen dependiendo de cada uno de los tres niveles de usuario, los cuales se describen a continuación:

2.2.1 Nivel administrador

La labor del administrador del Sistema, en primer término, es decidir cuáles datos deben almacenarse en la base de datos y establecer políticas para mantener y manejar los datos una vez almacenados. Se encargará también de garantizar el funcionamiento adecuado del sistema y de proporcionar otros servicios de índole técnica relacionados. Es decir, el administrador es la persona que tiene el control centralizado sobre el sistema y que controla tanto los datos como los programas que tienen acceso a ellos.

Tareas del administrador:

- Decidir el contenido de la base de datos.
- Crear la estructura del almacenamiento y los métodos de acceso.
- Administrar y controlar la seguridad física y lógica de los datos.
- Monitorear el comportamiento y crecimiento de la base de datos.
- Procedimientos de respaldos y depuración de la base de datos.
- Salvaguardar la documentación, respaldos y diccionario de datos tanto de la base de datos como del sistema.
- Procedimientos de contingencia y recuperación de la base de datos.
- Modificar la base de datos o la descripción de la organización física.
- Otorgar permisos de acceso y prioridades a los diferentes usuarios.
- Especificar las limitaciones de integridad.
- Ser enlace con los usuarios.

Sus requerimientos son:

- **Protección**

  Como KeYzara está pensado ser un sistema de seguridad que controle el acceso de personal a instalaciones resguardadas por empresas u organizaciones según sus intereses, la necesidad que proporcione la confidencialidad, integridad y disponibilidad de la información constituye el principal requerimiento del administrador de este sistema.

- **Generar reportes**
  El administrador debe poder crear reportes hechos a la medida con información de todas las transacciones, en varias formas, a intervalos automáticos o a voluntad; con parámetros específicos tales como: nombres, números, horas, fechas, puertas, etc.

- **Emitir alarmas**
  Es de fundamental importancia para el administrador que el sistema emita alarmas que puedan detectar: el intento de ataques al sistema lógicamente o la intrusión de usuarios no autorizados al área restringida físicamente. Con el fin de identificar el origen del ataque.

2.2.2 Nivel propietario

El propietario del Sistema, tiene el privilegio para manejar la información de tal forma que puede:

- Añadir y eliminar usuarios a la base de datos.
- Crear objetos dentro de la base de datos (es decir, tablas, vistas, procedimiento almacenado).
- Dar permisos sobre objetos y comandos.
- Monitorear la base de datos.
- Realizar respaldos o restauraciones.
- Organizar la estructura de la base de datos.

Sus requerimientos son:

- **Control**
  El sistema KeYzara debe tener el control del acceso físico de personas mediante un sistema de software y un sistema mecánico adaptado a las puertas de entrada al área restringida.

- **Acceso otorgado**

El acceso será otorgado con la validación de la voz, una huella digital, una tarjeta, de una clave, etc., en combinación con los horarios y áreas autorizadas al usuario.

- **Acceso denegado**
  El acceso del usuario será denegado cuando la voz, la huella digital, la tarjeta, la clave, etc. no coincida con los parámetros autorizados al usuario y cuando se ingresen datos no registrados en la base de datos,

- **Generar reportes**
  El propietario puede crear reportes hechos a la medida con información de todas las transacciones, en varias formas, a intervalos automáticos o a voluntad; con parámetros específicos tales como: nombres, números, horas, fechas, puertas, etc.

- **Emitir alarmas**
  Es de fundamental importancia para el administrador que el sistema emita alarmas que puedan detectar: el intento de ataques al sistema lógicamente o la intrusión de usuarios no autorizados al área restringida físicamente. Con el fin de identificar el origen del ataque.

2.2.3 Nivel usuario final

Son aquellos que usan las aplicaciones del sistema.

Sus requerimientos son:

- **Facilidad de uso**
  El sistema KeYzara, en conjunto con una combinación de unidades de control para puertas, debe ser claro, sencillo y práctico para el usuario.

2.3 Alternativa de solución

Con base en los requerimientos de operación se plantea una alternativa de solución que consta de:

1. Un **sistema de software** que administre y controle los accesos y los permisos para áreas restringidas y

2. Un **sistema de control electromecánico** para el acceso físico a las áreas restringidas.

2.3.1 Sistema de Software

El desarrollo de aplicaciones de escritorio y el de servicios web han sufrido un auge muy importante durante los últimos años. Frente a esta nueva demanda surgen dos plataformas distintas para su desarrollo J2EE (Java 2 Enterprise Edition) de Sun MicroSystems y .NET de Microsoft**.** Ambas tienen un fin común pero metodologías sustancialmente diferentes en el momento de abordar problemas. Ahora bien, para poder decidir entre una de estas plataformas, en la que se llevará a cabo el desarrollo de nuestro software, se realizará un estudio comparativo independiente acerca de los siguientes aspectos del sistema:

- desarrollo
- rendimiento
- portabilidad
- seguridad
- escalabilidad
- coste

2.3.1.1 Desarrollo

- Herramientas de desarrollo

.NET: Microsoft integró su producto dentro de un paquete de desarrollo llamado "Visual Studio .NET", que como bien se podrá intuir, es el heredero natural del paquete "Visual Studio 6″ de la misma compañía. Y han querido seguir la misma filosofía de sencillez y comodidad en la programación de aplicaciones, con los ahorros de tiempo y costes que esto supone. Esto significa que podremos desarrollar una aplicación .NET de la misma manera que programábamos en Visual Basic con este paquete, con la ventaja de que todo lo que necesitemos para el funcionamiento de dicha aplicación está presente en el programa de desarrollo.

J2EE: J2EE es un estándar, una serie de reglas y pautas a seguir, con lo que no cuenta con un entorno de desarrollo tipo "Visual Studio". Como alternativa, son múltiples los productos que existen en el mercado ofreciendo entornos de desarrollo adecuados, tales como Forte de Sun**,** Visual Café de WebGain**,** Visual Age for Java de IBM**,** JBuilder de Borland entre otros. Si bien estas herramientas facilitan mucho la labor de los programadores, siguen sin llegar a nivel de integración ofrecido por Microsoft.

- Lenguajes de Programación

.NET: Una de las principales características la plataforma .NET consiste en la posibilidad de programar los distintos componentes de una aplicación empleando distintos lenguajes (siempre que cumplan con los criterios de la Common Language Specification). Es posible programar en una gran cantidad de lenguajes como C# (su lenguaje estrella), Visual Basic**,** C++**,** Cobol**,** Delphi, etc., etc.

Pero .NET va más allá de soportar estos lenguajes, sino que también ofrece plena interoperabilidad entre ellos, por lo que es posible construir un componente en un lenguaje, introducirlo en una aplicación escrita en otro distinto e incluso heredarlo y añadir nuevas características en un tercero. Por ejemplo: un componente programado en C++ puede incluirse en una aplicación realizada en C#, y además es posible crear un

componente en Cobol que herede del primero (hecho en C++) e incrustarlo también en la aplicación C#.

En los últimos años, Microsoft ha incluido la posibilidad de programas sus aplicaciones en Java mediante una adaptación del lenguaje para .NET llamado J#**.**

J2EE: El único lenguaje que soporta J2EE es Java y es el que se tendrá que utilizar para desarrollo de todos los componentes. Existen sólo dos formas oficiales para acceder a la plataforma J2EE con otros lenguajes, la primera es a través de JNI (Java Native Interface) y la segunda es a través de la interoperabilidad que ofrece CORBA.

- Datos de interés

  Algunos estudios estadísticos dejan algunos datos interesantes acerca de la cantidad de código necesario para realizar una misma tarea en cada plataforma. Según los datos del siguiente estudio del Software Productivity Research, J2EE necesita más líneas de código que .NET para realizar la misma funcionalidad. A la hora de codificar un determinado punto de función en Java necesitaron unas 53 líneas de código, mientras que en .NET sólo hicieron falta 16 líneas, del mismo modo para la implementación de una aplicación seleccionada se necesitaron 3.484 líneas en .NET y 14.273 en Java.

2.3.1.2 Rendimiento

Una gran mayoría de las aplicaciones empresariales contiene mucha más lógica de datos que de negocio. Es por ello que, al ser el acceso a base de datos la clave para un rendimiento óptimo, será la tecnología que mejor gestione este punto la que se lleve el punto en cuanto a rendimiento.

Microsoft ofrece una manera más sencilla, y por ello menos exigente, de abordar este objetivo, mientras que J2EE dedica más control a bajo nivel (control de "statements" y recogida selectiva de datos), de manera que es más aconsejable si

se cuenta con expertos desarrolladores, en caso contrario es más recomendable .NET, ya que es más complicado introducir errores fatales en el sistema.

2.3.1.3 Portabilidad

Portabilidad, o la posibilidad de ejecutar las aplicaciones desarrolladas en cualquier sistema operativo y/o máquina del mercado. Es el famoso dicho: *"escríbelo una vez, ejecútalo en cualquier parte"*.

J2EE es un estándar y no un producto en sí. Este hecho, que facilita la adopción de esta tecnología por parte de varios fabricantes, también conlleva que las implementaciones de J2EE no son 100% compatibles entre sí, ya que cada vendedor ha realizado su propia interpretación del estándar y ha añadido nuevas características que no tienen por qué incluir el resto de competidores. Lo que sí es cierto, es que todas las empresas que ofrecen sus productos basados en J2EE tienen versiones para los distintos sistemas operativos, por lo que una misma aplicación será portable entre los distintos sistemas siempre y cuando mantengamos la solución del mismo vendedor. En definitiva, pasar de una implementación J2EE a otra requerirá de modificaciones en el código de la aplicación y la portabilidad se pierde en cierta parte. Es por esto que muchos programadores prefieren escribir: *"escríbelo una vez, depúralo en todas partes"*.

De todas maneras, si que es cierto que estos productos ofrecen mucha más portabilidad que .NET, que sólo está preparada para ejecutarse sobre plataformas Microsoft (Windows). También hay que señalar que, como era de prever, la plataforma de Microsoft está en vías de salvar esta circunstancia gracias a proyectos como MONO, un intento de crear un CLR para otras maquinas y sistemas. Pero conviene preguntarse, en este caso, hasta qué punto llegará la plataforma a ser realmente portable.

Según el documento "J2EE vs Microsoft .NET" realizado por los desarrolladores de Sun MicroSystems Chad Vawter **y** Ed Roman, la elección de la plataforma (atendiendo a la portabilidad) debería elegirse en base a los siguientes escenarios:

- Si se desarrolla software para otros negocios, o si es una compañía consultora, y los usuarios tienen una gran variedad de plataformas, recomiendan especializarse en la arquitectura J2EE. Si no puedes garantizar que tus clientes aceptarán Windows/.NET como solución, estarás perdiendo a las grandes empresas que seguramente han desarrollado sus soluciones en UNIX o Mainframes.
- Si los clientes están en la plataforma Windows, en ese caso puede servir tanto J2EE como .NET ya que ambas soluciones se ejecutan en Windows. En este caso lo normal es averiguar qué middleware utiliza el cliente, y tomar la decisión basándose en ello.
- Si alojas tus propias soluciones, entonces controlas el entorno de implantación. Esto te permite escoger libremente entre J2EE y .NET. Utilizando esta última te estás casando con Microsoft, y nunca se sabe lo que deparará el futuro.

Es en los dos últimos puntos donde se centra la controversia, la pregunta es clara: en caso de igualdad de posibilidades, ¿cuál de las dos es más conveniente? La respuesta no es sencilla, ya que hay quien dice, por ejemplo, que en entornos Microsoft, .NET se comporta mucho mejor al ofrecer una mayor integración al ser productos de la misma compañía y estar optimizados para ello. Aunque también es verdad que J2EE ha demostrado un alto rendimiento en sistemas operativos Windows. Como siempre, es cuestión de gustos (y modas).

2.3.1.4 Seguridad

Este es uno de los aspectos más importantes a la hora de evaluarlas dos plataformas, ambas utilizan sistemas y filosofías diferentes para abordar el problema. A continuación pasamos a realizar una explicación comparativa entre ambos sistemas.

J2EE y .NET proporcionan servicios de seguridad sencillos, aunque con enfoques diferentes. Los servicios de autenticación y autorización de .NET son proporcionados mediante el sistema operativo y sus ficheros de identificación. En cambio, J2EE no especifica qué métodos o ficheros se deberían usar para ejecutar estas funciones, dejando estas decisiones a los distribuidores y

desarrolladores. Aunque su uso no es requerido, la funcionalidad de autenticación y autorización es proporcionada por Sun mediante JAAS (Java Authentication and Authorisation Service), basado en PAM.

Ambas plataformas usan conceptos similares para manipular el acceso a los recursos por usuario y por código, basándose ambos en permisos. Además, se usa el concepto de perfiles en ambos.

Mientras J2EE usa el concepto de "Perfiles Organizacionales" para delimitar responsabilidades a varios niveles del proceso de desarrollo y explotación (Product Provider, Application Component Provider, Application Assembler, Deployer y System's Administrador, por defecto), .NET no define la jerarquía tan claramente.

.NET proporciona un modelo sólido de seguridad mediante código tratado en el CLR, lo cual supone un peligro: la habilidad para ejecutar código no tratado confiere la posibilidad de traspasar la seguridad del CLR mediante llamadas directas a los APIs subyacentes del sistema operativo.

Java, para ello, examina la procedencia de las clases mediante el Class-Loader, realizando una comprobación exhaustiva de éstas. Aunque esto implica también que código firmado y confiado tiene acceso ilimitado a los recursos del sistema. Además, las llamadas de Java a código nativo (C/C++) mediante JNI confiere la posibilidad de traspasar la seguridad del JRE de una manera tan segura como se puede traspasar la seguridad de .NET ejecutando código no tratado en el CLR.

Uno de los más importantes retos para los distribuidores de Microsoft y J2EE al desarrollar sus respectivas plataformas es la manipulación segura de código obtenido de múltiples fuentes (fuera de la máquina local). Las funciones de verificación de código de la JVM están bastante maduras a estas alturas. Además, se ha aprendido de los errores cometidos en el pasado. El modelo CLR es similar, pero la implementación está relativamente sin probar.

Con todo esto, parece que ambas plataformas han llegado a un sistema de seguridad bastante aceptable, aunque nos atreveríamos a citar a Vince

Dovydaitis, ingeniero jefe de Foliage Software Systems Inc.: *"J2EE ofrece una mejor solución para grandes sistemas que corren mediante aplicaciones críticas y múltiples plataformas remotas, mientras que .NET ofrece mejor respuesta para gestionar autorizaciones basadas en usuarios y roles"*. Aunque dicha cita nos parezca exagerada, ya que creemos que .NET puede, a estas alturas, ofrecer una gran solución de seguridad en proyectos grandes de comunicación remota.

2.3.1.5 Escalabilidad

Escalabilidad es la capacidad de un sistema para soportar más carga de trabajo, usualmente debida al aumento de usuarios que lo utilizan. Tanto J2EE como .NET ofrecen métodos de escalabilidad como la carga balanceada que permite a un cluster de servidores (varios servidores) colaborar y dar un servicio de forma simultánea.

También en este tema se produce un importante foco de disparidad de opiniones. Mientras los defensores de J2EE opinan que existe hardware disponible más potente en el entorno UNIX que en el entorno Windows, por lo que es necesario un menor número de máquinas para ofrecer el mismo rendimiento en las dos plataformas, los correspondientes amantes de .NET afirman que no sólo esto no es cierto, sino que ofrecen pruebas numéricas de que no es así.

Por ejemplo, Roger Sessions, de objectwatch.com, remarca que la plataforma .NET puede escalar desde 16.000 transacciones por minuto a más de 500.000 transacciones por minuto, mientras que IBM WebSphere, usando tecnología J2EE/UNIX, no puede conseguir nada mejor que pasar de 17.000 a 110.000 transacciones por minuto, con un coste monetario mucho mayor por transacción. Por lo tanto con .NET obtendríamos mayor posibilidad de escalado a un mejor precio.

2.3.1.6 Coste

A simple vista, y aplicando la lógica, cabría suponer que un producto como .NET, fruto de la ambición empresarial de la más grande de las empresas capitalistas, fuera más caro de implantar que una aplicación realizada mediante

estándares ideados por un grupo de empresas que ni siquiera venden el producto como tal. Y la verdad es que no es así.

Los costes reducidos suelen ser otra de las ventajas de los productos Microsoft. Si bien es cierto que se pueden encontrar en el mercado productos basados en J2EE a precios muy reducidos e incluso gratis, en función de la solución escogida (hay que tener en cuenta que las soluciones gratuitas o baratas no incluyen algunos servicios realmente útiles), para hacerse con un abanico de soluciones y servicios realmente importante resultará más barato con .NET que con J2EE.

2.3.2 Sistema de Control Electromecánico

2.3.2.1 Autenticación basada en posesión.

Esta consiste en tener una tarjeta u objeto inteligente que tenga un microprocesador y memoria que se pueda implementar como una herramienta de autenticación.

Por ejemplo para poder evitar trasmitir la contraseña en clara por parte de un usuario, esta tarjeta la puede cifrar antes de trasmitirla.

Otra posibilidad es que el dispositivo genere contraseñas con una frecuencia de 30 segundos, en forma sincronía con el sistema que va hacer la autenticación.
Los dispositivos que se emplean para este propósito son tarjetas inteligentes similares a las bancarias, anillos Java, tarjeta que se insertan a una computadora. Uno de los inconvenientes problema es que se pueden perder o dañarse impidiendo al usuario el acceso.

Hay una gran variedad de estos dispositivos:

Tarjetas con código de barras. Ver Fig.2.1.

Fig.2.1. Tarjeta con código de barras

Tarjetas de plástico con banda magnética son las bien conocidas tarjetas bancarias. Ver Fig.2.2.

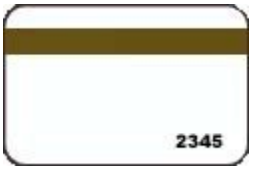


Fig.2.2. Tarjeta de plástico con banda magnética

Tarjetas con platico con registro láser fabricadas con la misma tecnología que un disco compacto y grabadas en forma parecida. Ver Fig.2.3.

Fig.2.3. Tarjeta con platico con registro láser

Tarjetas con memoria o tarjetas con memoria y procesador. Ver Fig.2.4.

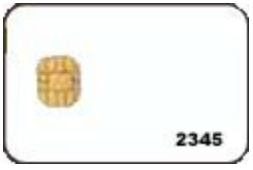


Fig.2.4. Tarjeta con memoria o tarjetas con memoria y procesador

Este tipo de tarjeta se puede emplear como autenticador, o como herramienta de autenticación remota. Por ejemplo, para evitar transmitir en claro la contraseña del usuario, un dispositivo inteligente puede cifrarla para su posterior transmisión, o inclusive la puede transmitir directamente, participando en algún protocolo que evite los ataques de retransmisión de información interceptada.

2.3.2.2 Autenticación basada en características físicas (autenticación biométrica).

Este tipo de autenticadores se basan en características físicas del usuario. El reconocimiento de patrones, la inteligencia artificial y el aprendizaje son utilizados para el desarrollo de sistemas de identificación biométricos.

La autenticación basada en características físicas tienen su aparición desde que el hombre existe, y en nuestra vida cotidiana es la que mas utilizamos: a diario identificamos a personas por los rasgos de su cara o por su voz. Obviamente aquí el agente reconocedor lo tiene fácil porque es una persona, pero en el modelo aplicable a redes o sistemas el agente ha de ser un dispositivo que, basándose en características del sujeto a identificar, le permita o deniegue el acceso.
Identificadores

Son los datos que caracterizan a una instancia del sistema biométrico. Pueden ser de dos tipos:

1. Identificador. Se crean durante el registro del usuario, y se almacenan para usarse posteriormente.

2. Verificador. Se utilizan durante su solicitud de acceso y se descartan después de que han servido su propósito

.
El primer tipo de identificadores son generados más cuidadosamente y estos no son ínter operables con sistemas diferentes donde se crearon.

a. Verificación de huellas dactilares

Estos identificadores requieren de unos 1000 bytes, y son de los más grandes identificadores biométricos. Son muy precisos, pues la tasa de aceptaciones falsas es menos de una en un millón, y la de rechazos equivocados es de alrededor del 3%, casi siempre por errores en la posición del dedo, heridas y la calidad de la imagen capturada. Ver Fig.2.5.

Fig.2.5. Verificación de huellas dactilares

Como se muestra en la figura de la huella dactilar solo se toman algunos puntos de comparación, como son líneas que terminan o uniones estrellas de esta manera se establecen los puntos de comparación a este método se basa en detalles.

Los métodos basados en correlación requieren establecer con alta precisión un punto de referencia para de allí calcular las correlaciones en ambas imágenes.
Sistemas biométricos no son ínter operables porque cada empresa sigue un patrón y algoritmo diferentes de reconocimiento.
Este tipo de autenticadores son los más utilizados por algunas empresas para la implementación de acceso por autenticación biométrica.

b. Geometría de la mano

Se emplean las características físicas tridimensionales de la mano y los dedos. Es una tecnología particularmente adecuada cuando se tienen grandes números de usuarios o usuarios que requieren acceso esporádicamente y por ello no tengan adecuada capacitación en el uso de otras tecnologías. Los registros manuales se han implantado masivamente en controles de asistencia industrial, y acceso a grandes instalaciones (fábricas). Ver Fig.2.6.

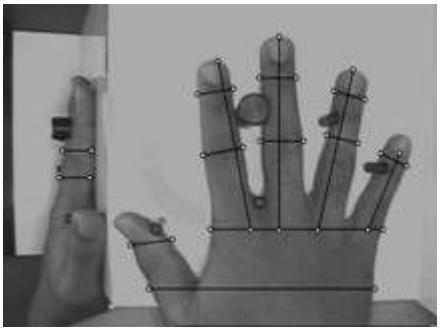


Fig.2.6. Geometría de la mano

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

c. Verificación de voz

Es muy común que mucha gente piense que los sistemas de verificación de voz intentan reconocer los que el usuario dice, pero lo que realmente se reconoce es una serie de sonidos y sus características para decidir si el usuario es quien dice ser. Ver Fig.2.7.

Fig.2.7. Verificación de voz

Para autenticar a un usuario utilizando un reconocedor de voz se debe disponer de ciertas condiciones para el correcto registro de los datos, como ausencia de

ruidos, reverberaciones o ecos; idealmente, estas condiciones han de ser las mismas siempre que se necesite la autenticación.

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

d. Análisis de la retina

Los patrones de los vasos sanguíneos capilares de la retina son únicos y distintos en cada persona. Si se les analiza mediante una fuente luminosa de baja intensidad y un acoplador óptico se obtiene una imagen parecida a la de una huella dactilar. Siendo un patrón más sencillo, solo se requieren 35 bytes para almacenar el identificador. Presenta problemas para quienes emplean anteojos, y requieren que el ojo se apoye en un ocular, lo cual parece desagradable para muchos usuarios. Ver Fig.2.8.

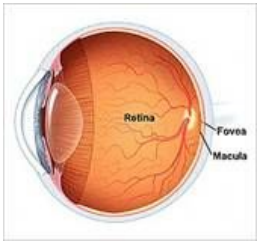


Fig.2.8. Análisis de la retina

e. Análisis del iris

El iris humano (el anillo que rodea la pupila, que a simple vista diferencia el color de ojos de cada persona) es igual que la vasculatura retinal una estructura única por individuo que forma un sistema muy complejo - de hasta 266 grados de libertad - , inalterable durante toda la vida de la persona. El uso por parte de un atacante de órganos replicados o simulados para conseguir una falsa

aceptación es casi imposible con análisis infrarrojo, capaz de detectar con una alta probabilidad si el iris es natural o no. Ver Fig.2.9.

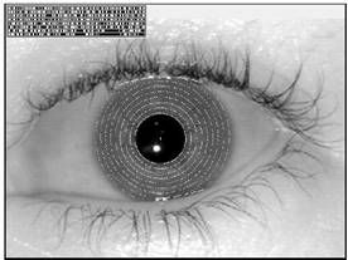


Fig.2.9. Análisis del iris

Se coloca una cámara a un metro del ojo, y 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 al iris se usa un análisis de ondoletas en dos dimensiones para filtrar y mapear partes del iris en cientos de vectores. Que toman sus valores de la orientación y posición y frecuencia espacial de las áreas seleccionadas. Estos vectores forman un código patentado, que es el identificador.

f. Reconocimiento de rostros

Usando una colección de fotografías de personas que sean homogéneas, es decir, del mismo tamaño y tomadas desde el mismo ángulo se puede convertir cada fotografía a una serie de números. Por ejemplo si se empieza, en cada foto, por el rincón superior izquierdo, y se va haciendo una lista del valor que describe cada uno de los píxeles (tonos de gris). Ver Fig.2.10.

Fig.2.10. Reconocimiento de rostros

g. Verificación de firmas.

No es una característica estrictamente biométrica, pero se suele agrupar dentro de esta categoría; de la misma forma que sucedía en la verificación de la voz, el objetivo aquí no es interpretar o entender lo que el usuario escribe en el lector, sino autenticarlo basándose en ciertos rasgos tanto de la firma como de su rúbrica.
La verificación en base a firmas es algo que todos utilizamos y aceptamos día a día en documentos o cheques; no obstante, existe una diferencia fundamental entre el uso de las firmas que hacemos en nuestra vida cotidiana y los sistemas biométricos; mientras que habitualmente la verificación de la firma consiste en un simple análisis visual sobre una impresión en papel, estática, en los sistemas automáticos no es posible autenticar usuarios en base a la representación de los trazos de su firma. En los modelos biométricos se utiliza además la forma de firmar, las características dinámicas (por eso se les suele denominar Dynamic Signature Verification, DSV): el tiempo utilizado para rubricar, las veces que se separa el bolígrafo del papel, el ángulo con que se realiza cada trazo.

2.3.2.3 Electromecánico.

Chapa de Control de Acceso de NIP. Ver Fig.2.11.

Fig.2.11. Chapa de Control de Acceso de NIP

Características:

- Sistema simple y Conveniente
  ¡Sólo introduzca el NIP 3-8 para abrir la cerradura! Totalmente 3 códigos de grupos podrían ser matriculados.

- Seguridad de diseño
  El LP 901 es diseñado para cumplir con el Fuego global y Normas de seguridad. La puerta siempre puede ser abierta fácilmente en caso de una salida rápida en caso de una emergencia o fuego. La palanca formada del L reduce las posibilidades de atorarse con la ropa u otros artículos.

- Prohíbe el uso Malévolo por operación
  La entrada números personales de identificación incorrectos más de cinco veces activaría la inactividad de sistema durante 5 minutos para proteger contra cualquier operación malévola intencional de la cerradura.

- Fácil operación de registro de claves
  El registro de usuario y la eliminación son hechos por el teclado numérico. Todas las operaciones pueden ser completadas en aproximadamente 10 segundos y no requieren ninguna habilidad especial o formación.

- Entrada Clave Opcional
  Como un rasgo adicional una cerradura clave estándar puede ser montada en el mecanismo de mango. Este proporciona la opción de usar una llave como anular para unidades de funcionamiento defectuoso.

- Suministro de energía
  El LP 901 es impulsado por 4 baterías alcalinas AA 1.5V. El consumo de poder es muy bajo y esto puede apoyar 4000-5000 operaciones. Para una familia típica estas baterías durarán 6-12 meses. Alta calidad – Se recomienda baterías alcalinas para una larga vida.

- Demostración Clave de la Noche
  Presione cualquier botón durante 3 segundos para activar la función de demostración clave de la noche para la conveniencia de los usuarios.

- Alarma de baja carga de baterías
  Cambio de Batería, advertencia Audible para recordar al usuario para sustituir las baterías.

- Precio Competitivo
  LP 901 se encuentra en uno de los niveles del mundo más altos de interpretación y funcionalidad en un precio muy competitivo.

- Configuraciones Variables
  La operación del la chapa puede ser ajustada a las necesidades específicas del usuario. Por ejemplo un usuario puede programar la puerta para quedarse abierto hasta no reinicializado vía "el Manual" que Cierra con llave el Modo, o puede tener un período de cerradura predeterminado usando el Modo de cierre "Automático". La función "Libre" permite para abrir la puerta fácilmente con la bocacalle de la forma de manija dentro y fuera automáticamente para la conveniencia del usuario.

Especificaciones:

- Dimensión: 210(L) x 65(W) x25(H)mm
- Material: Aleación de Zincum
- Color: Niquelado
- Poder: Batería (Para Sistema) DC1.5V (AA, LR6) x 4
- Contraseña válida: 3 grupos de Código de número personal de identificación (mínimo:3 dígitos, máximo: 8 dígitos)
- Modo de Control: Embrague
- Consumo de Poder Dinámico: 50-90mA
- Procesamiento de Tiempo: menos de 1 segundo
- Consumo de Poder Estático: <50uA
- Dispositivo de Emergencia: Llave Segura Anula
- Temperatura:-20 a 50°C /-16 a 122°F
- Humedad: Humedad Relativa del 10 a 80 %
- Voltaje de ESD: resistencia:> 15000V

- El Primer Diseño de Seguridad Encuentra Códigos de Seguridad de Fuego permitiendo al usuario abrir la puerta simplemente girando el mango del interior.

2.4 Criterios para elegir solución

1. TECNOLOGIA
2. IDENTIFICACION
3. FRAUDE
4. VELOCIDAD
5. MANTENIMIENTO
6. VANDALISMO
7. COSTOS
8. COSTO CONSUMIBLE

2.5 Selección de la solución

Matriz de Resultados (Sistema de Software)

EVALUACION	EXPLICACION	PLATAFORMA SOBRESALIENTE
Información disponible	En igualdad de Condiciones, no se observa ventaja por parte de una de las plataformas.	.NET y Java
Información Disponible en Español	En igualdad de Condiciones, no se observa ventaja por parte de una de las plataformas.	.NET y Java
Curva de Aprendizaje	.NET sobresale tímidamente por el hecho de presentar aplicaciones funcionales en menor tiempo que el presentado por J2EE.	.NET
Consumo de Material Relacionado	.NET supera con creces a J2EE en cuanto al material buscado, descargado y pagado por él.	.NET
Acceso a Software Relacionado	Los Software en los primeros lugares de ventas en la Web y tiendas investigadas dan a .NET como una de las más	.NET

	accedidas por los usuarios.	
Retardo de Aplicaciones	Para ambas plataformas se observan los mismos retardos al acceder una mayor cantidad de usuarios. En repetición de mensajes presentan mismos tiempos de ejecución.	.NET y Java
Manejo de Base de Datos local	Para el manejo de base de datos ambas plataformas presentan buenas funcionalidades. Tiempos de respuesta mejores por J2EE y simpleza de código, aunque más complicado. .NET más simple el desarrollo de estas aplicaciones pero de manera local se presenta de mejor forma J2EE. Mysql se comporta mejor con J2EE y Postgres con .NET	.NET y Java
Manejo de Base de Datos remota	Para los sistemas anteriores ejecutados de forma remota estos presentan semejantes funcionamientos que de manera local, con salvedades que al cargar datos por 1era vez .NET mostró pequeñas demoras con respecto a J2EE. Luego de ejecutados ambos sistemas .NET presento un mejor funcionamiento.	.NET y Java
Uso de Recursos	Para obtener resultados óptimos, J2EE necesita ocupar mas recursos tanto CPU, memoria Ram como espacio físico. Para esto mismo .NET ofrece resultados óptimos con menos utilización de recursos.	.NET
Curva de Explotación	Ambas plataformas presentaron un nivel de explotación semejante al momento de salir al mercado. Actualmente sobresale la utilización de páginas ASP y su semejantes Web Forms ASPx, dejando a JSP de J2EE más atrás en el presente.	.NET
Explotación	El nivel de Explotación es aparentemente superior en la actualidad por la tecnología .NET. Dejando a J2EE en un mercado global de aplicaciones robustas de servicios Web.	.NET
Distribución	Aunque las páginas JSP presentan un número menor de apariciones en la Web. Se observa la utilización de ambas tecnologías por sitios de importancia y relevancia en el medio.	.NET y Java
Cantidad Servidores Web	Para esta característica no se presenta algún tipo de variable que haga que alguna plataforma destaque sobre la otra.	.NET y Java
Capacidad Servidores Web	A través de los distintos Servidores Web, Tomcat instalado en un sistema operativo Linux, da a J2EE una ventaja clara por sobre .NET al poder ejecutar correctamente un mayor tipo de páginas dinámicas (ASP, JSP y PHP).	Java

Líneas de Código	Ambas tecnologías arrojan un número semejante y considerado para el distinto tipo de aplicación Web presentada. Ambos tipos de TAG se consideran a un nivel mayor por parte de .NET en cuanto a diseño. Y mayor número de líneas de código más que TAG por parte de JSP.	.NET y Java
Herramientas Extras	Aunque Visual Studio.NET facilita de mayormente el diseño y desarrollo de aplicaciones WEB. J2EE presenta un número de herramientas extras que facilitan el trabajo del programador.	Java
Facilidad de desarrollo	En el análisis de los IDE's seleccionados, .NET presenta uno de mejor diseño para la facilidad de aplicaciones Web que J2EE, facilitando el desarrollo, mejorando tiempos de creación y ejecución.	.NET
Claridad en los códigos	Al acceder a los códigos J2EE da menos información a personas ajenas a éste.	Java
Manejo de Errores	Se puede considerar a J2EE con su IDE de desarrollo Netbeans como un mejor manejo de error, al indicar claramente cual vendría a ser éste.	Java
Atractivo del IDE de Desarrollo	Visual Studio .NET ofrece lo mejor de ambos mundos de programas de desarrollo, principalmente un atrayente atractivo visual, y por detrás un poderoso lenguaje de codificación.	.NET
Necesidad de Componentes	Para el desarrollo de aplicaciones Web con manejo de base de datos, ambas plataformas necesitaron de componentes extras, tanto J2EE con JDBC como .NET con las utilidades de conexión.	.NET y Java
Claridad de Uso de Licencias.	Ambas licencias no presentan consideraciones engorrosas que generen algún tipo de interpretación ajena a la que éstas presentan.	.NET y Java
Consideración de paquetes educacionales.	Solo J2EE considera la descarga gratuita de muchos de sus productos e IDE's de desarrollo e incluso la maquina virtual es libre de acceso.	Java
Costos de herramientas simples.	Refiriéndose al enunciado anterior por contar con paquetes educacionales o considerados de licencia libre J2EE ofrece sus productos gratis, incluso se pueden acceder a través de Internet y llegarían al hogar del cliente.	Java
Costos por aplicaciones Creadas.	La licencia de .NET permite al usuario desarrollar sus propias aplicaciones comerciales sin necesidad de acceder a una licencia especial. Este hecho contrasta con J2EE que	.NET

	para cierto tipo de aplicaciones se debe acceder a licencias extras para incluir a sus productos que puedan formar parte de otra aplicación comercial.	

Matriz de Resultados (Sistema de Control Electromecánico)

CONCEPTO	CODIGO DE BARRAS, BANDA MAGNETICA O PROXIMIDAD	BIOMETRIA	CONCLUSIONES
TECNOLOGIA	Sistema de tecnología de punta, que incluye comunicación por puerto ethernet, tiene capacidad de crecimiento en memoria.	Sistema de tecnología de punta, con opción de comunicación por puerto ethernet. Tiene capacidad de crecimiento en memoria.	Ambos sistemas cuentan con opción electrónica actualizada, sólo que el biométrico es un equipo distinto de reconocimiento, ya que identifica personas, lo cual lo hace más confiable que código de barras, banda magnética o proximidad.
IDENTIFICACION	Estos sistemas reconocen OBJETOS, mediante el uso de credenciales con código de barras, banda magnética o tarjetas de proximidad.	Este sistema reconoce PERSONAS, mediante el uso de: Verificación de huellas dactilares, Geometría de la mano, Verificación de voz, Análisis de la retina, Análisis del iris, Reconocimiento de rostros y Verificación de firmas.	No es lo mismo reconocer OBJETOS, que reconocer PERSONAS.
FRAUDE	Con estos sistemas, cualquier persona puede prestar su credencial para que otra persona cheque su asistencia, horas extras, etc.	Con este sistema, nadie puede checar por otra persona, ya que la credencial es la mano de ésta. No se pierde, no se olvida y no se presta.	Los fraudes de puntualidad y asistencia en una empresa, por lo general existen, pero difícilmente detectamos a la persona que lo hace. Con un sistema biométrico, estos fraudes se van a 0%.

VELOCIDAD	Estos sistemas pueden ofrecer un tiempo de respuesta en el registro de puntualidad y asistencia de hasta dos segundos por empleado.	Estos sistemas pueden ofrecer un tiempo de respuesta en el registro de puntualidad y asistencia entre tres y seis segundos, dependiendo del equipo que se utilice.	En ocasiones es importante el tiempo de respuesta y la velocidad que los equipos ofrecen, pero se tiene que considerar la veracidad del registro final, el cual se puede obtener en dos segundos (identificación de objetos, no se sabe quién lo hace) o en seis segundos (identificación de personas, único por empleado).
MANTENIMIENTO	Las fallas más comunes en estos equipos ocurren en el teclado, en caso de que venga incluido, y en la base de deslizamiento de la credencial, la cual se desgasta con el tiempo. Solo requiere de limpieza general y en especial el área de lectura del código de barras o de la cabeza lectora en banda magnética. Proximidad requiere muy poco mantenimiento.	Las fallas más comunes en estos equipos ocurren en el teclado, el cual tiene movimiento mecánico y también, la base de posición de la mano, la cual puede desgastarse con el uso. Sólo requiere de limpieza general y en especial en la base donde se coloca la mano y los espejos	En ambos casos, las fallas más comunes se pueden corregir con un mantenimiento preventivo o en caso de ser correctivo, estas piezas son consumibles normales. También, en ambos casos, este material es una refacción poco costosa y fácil de remplazar.
VANDALISMO	Los sistemas de código de barras o de banda magnética pueden ser dañados, metiendo objetos en la ranura del lector, rociándoles algún líquido o simplemente agrediéndolos físicamente, mientras que en los lectores de proximidad, el vandalismo es muy reducido.	Estos sistemas pueden ser dañados, si se les rocía algún líquido o si se rompen sus espejos y/o postes, también si se agreden físicamente	Entre más restrictivo sea un equipo, más susceptible será al vandalismo, ya que representará mayor obstáculo a las personas que lo utilizan.
COSTOS	Según la calidad del equipo y de las funciones que incluyan, se pueden	Un equipo Biométrico para 512 usuarios, tiene	Los costos son siempre importantes en la toma de decisiones para la adquisición

	conseguir desde los $1,000.00 US hasta los $8,000.00 US	un costo desde $1,800.00 US. Dependiendo de la aplicación en que se vaya a instalar.	de un equipo. Siempre se deberá tomar en cuenta aspectos como: ¿Qué se desea controlar? ¿Cuál es la seguridad que se desea tener en la veracidad de la información?, etc. De tal forma que en una tabla de comparativo costo-beneficio, se obtenga la mejor decisión para una compañía.
COSTO CONSUMIBLE	En un sistema de código de barras, banda magnética o proximidad, se pueden elaborar credenciales con precios desde $1.00 U.S., hasta los $15.00 U.S., dependiendo de la tecnología a utilizar.	En un sistema biométrico el costo del consumible es de $0.00, ya que la mano no le cuesta a la empresa.	En cada proyecto de puntualidad y asistencia, si éste es de código de barras o cualquier otra tecnología que identifique objetos, se debe considerar un 30% adicional a las credenciales que se necesiten, ya que la rotación y las pérdidas necesitarán de reposición inmediata. En un biométrico no se da este caso.

CAPÍTULO 3

DISEÑO DEL SISTEMA

En el presente capítulo, se da un amplio panorama de la estructura del sistema de seguridad para el control de acceso físico "KeYzara", el cual tiene como principal objetivo proteger la integridad de las personas y de la información que resguarda.

3.1 Diagrama de flujo de datos (DFD)

Un diagrama de flujo de datos, en general, muestra cómo se mueven los datos en un sistema. La técnica de diagrama de flujo de datos, es una representación gráfica que permite al analista definir entradas, procedimientos y salidas de la información en la organización bajo estudio, permitiendo así comprender los procedimientos existentes con la finalidad de optimizarlos, reflejándolos en el sistema propuesto. Tiene por objetivo representar gráficamente el sistema a nivel lógico y conceptual, ilustrando los componentes esenciales de un proceso y la forma en que interactúan.

Esta técnica del diagrama de flujo de datos es útil por lo siguiente:

- Representa gráficamente los límites del sistema en estudio.
- Muestra el movimiento de los datos y la transformación de los mismos a través del sistema.
- Facilita el mantenimiento del sistema.

3.1.1 Elementos básicos de los diagramas de flujo de datos

El DFD utiliza 4 símbolos básicos para representar procesos, flujo de datos, almacenaje de datos y entidades externas.

3.1.1.1 Proceso

Al menos debe tener un “data flow” que entre y uno que salga del proceso. El nombre del proceso debe ser un verbo junto a un nombre en singular. El nombre del proceso identifica la función del proceso. En el DFD, el proceso aparece como una caja negra (black box), pues el Input, el Output y la función general se conocen, pero no así los detalles del proceso. Ejemplo: Calcular Paga Neta, Crear Facturas, Verificar Orden, Calcular Nota. Ver Fig. 3.1.

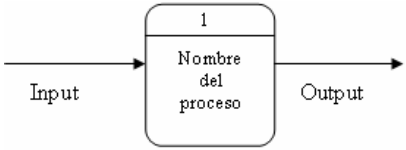


Fig.3.1. Elemento Proceso de los diagramas de flujo.

3.1.1.2 Data Flow

Es el camino por donde los datos se mueven de una parte del sistema a otra. Se utiliza una flecha como símbolo. Ver Fig. 3.2.

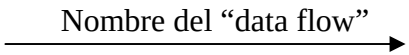


Fig.3.2. Elemento Flujo de Datos de los diagramas de flujo.

El nombre del “data flow” debe ser en singular; solo se debe usar en plural para clarificar el contenido del “data flow”. Ejemplos: Factura, Horas Trabajadas, Salario por Hora, Orden, Nota del Estudiante, Parámetros de nota (este último está en plural). Todo “data flow” debe tener un proceso en uno de sus extremos.

Ejemplos incorrectos (no son posibles en un DFD) Ver Fig.3.3:

Generación espontánea – no tiene input

Hoyo negro (black hole) – no tiene output

Hoyo gris (gray hole) – el input no es suficiente para generar el output

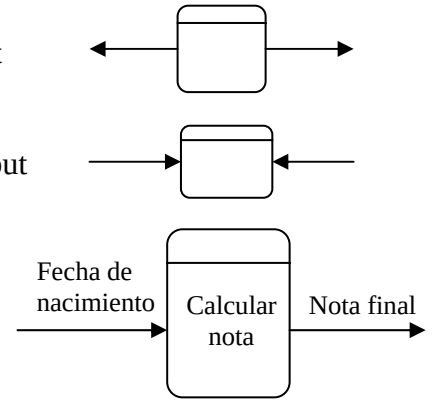


Fig.3.3. Elemento Flujo de Datos de los diagramas de flujo.

3.1.1.3 Data Store

También conocido como "data repository"; representa cuando el sistema tiene que retener datos porque serán usados más tarde por uno o más procesos. Ver Fig. 3.4.

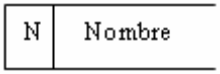


Fig.3.4. Elemento Data Store de los diagramas de flujo.

El nombre debe ser en plural o un nombre colectivo; se puede usar un adjetivo. Debe estar conectado a procesos. Debe tener al menos un Data Flow que entra y uno que sale (cada data flow conectado en el otro extremo a un proceso).

3.1.1.4 Entidad

Persona, departamento, organización u otro sistema de información que provee datos al sistema y/o recibe datos del sistema. Ver Fig.3.5.

Fig.3.5. Elemento Entidad de los diagramas de flujo.

Presenta los límites del sistema de información y cómo éste interacciona con su ambiente externo. El nombre debe ser en singular. Debe estar conectado a un proceso con un Data Flow.

3.1.2 Reglas para dibujar los Diagramas de Flujo de Datos

1. Cada diagrama de contexto debe estar en una sola página.
2. El nombre del proceso debe ser el nombre del sistema de información.
3. Use nombres únicos para cada símbolo.

4. No cruce las líneas de flujo de datos. Si es necesario, duplique una entidad o Data Store (utilice un asterisco -*- para explicarlo).
5. Use identificaciones abreviadas en entidades y Data Store; son más fáciles de recordar).
6. Use un número de referencia único para cada proceso.

3.1.3 Diagrama de Contexto

Presenta los límites y el alcance del sistema. Es el nivel más alto de los Diagramas de Flujos de Datos. Para dibujarlo se deben seguir los siguientes pasos:

1. Hacer el símbolo del proceso en el centro con el nombre del sistema.
2. Dibujar las entidades alrededor del proceso.
3. Usar los Data Flow para conectar las entidades al proceso.
4. NO se muestran los Data Store.

3.1.4 Diagrama 0 (cero)

Es el DFD que describe los detalles del proceso del Diagrama de Contexto. Los Input, Output, Data Flows y entidades deben ser idénticos en el Diagrama de Contexto y el Diagrama 0. Se pueden dibujar Data Store si son necesarios. Cada proceso recibe un número de referencia que no tiene que ver con el orden en que los procesos se realizan. Puede existir un flujo de datos en donde la misma data se dirija a dos o más localizaciones, lo que se conoce como “diverging data flow”. Ver Fig.3.6.

3.1.5 Diagramas de niveles más bajos

Muestran detalles adicionales de los procesos. Deben ser nivelados y balanceados.

- Nivelar – proceso de dibujar diagramas detallados hasta que se alcance el nivel de detalles deseados.

- Balancear – Mantener consistencia en todos los diagramas, flujo de datos (Input/Output), definiciones de datos y descripciones de procesos.

Cuando un proceso consiste de una función que no se puede descomponer se dice que es una función primitiva.

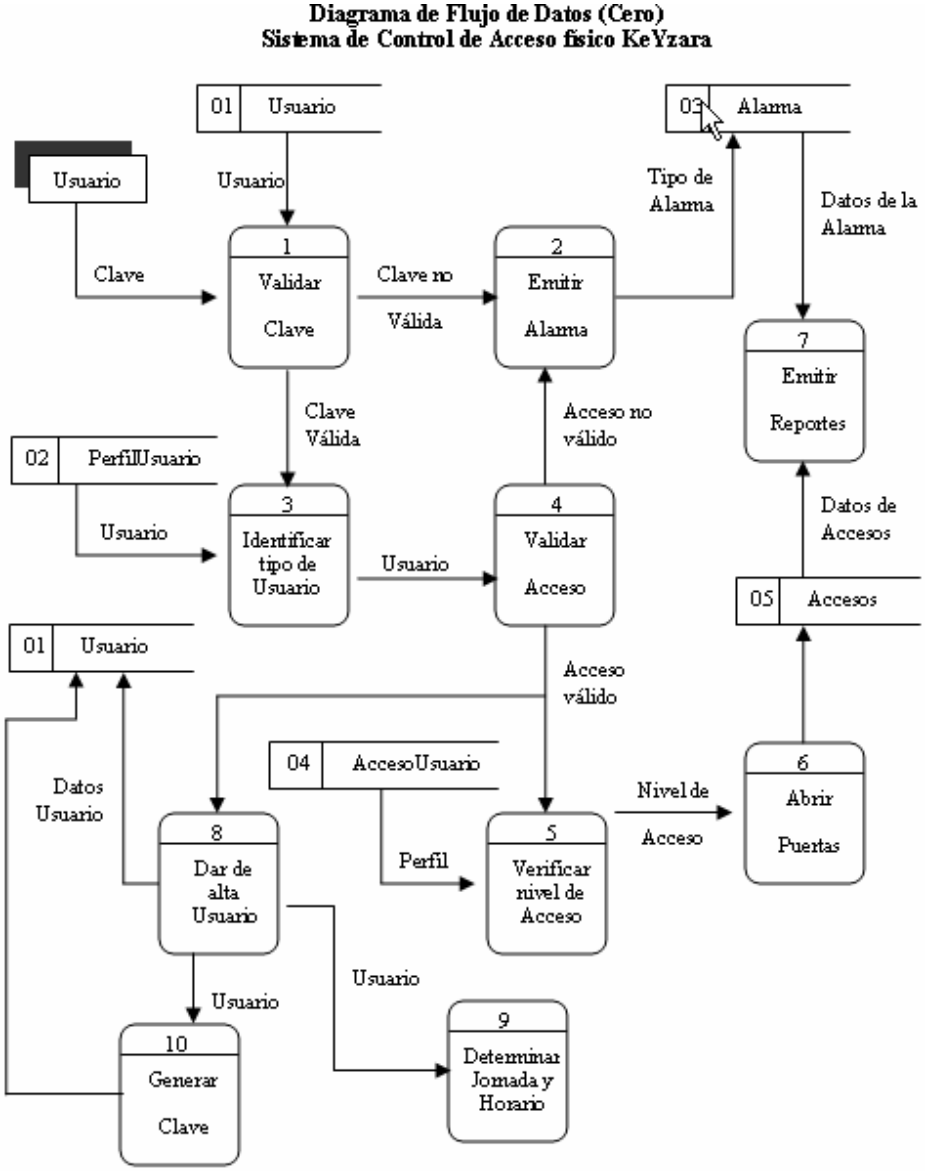


Fig.3.6 Diagrama de Flujo de Datos (Cero) del sistema KeYzara.

3.2 Diseño de la Base de Datos

Uno de los retos en el diseño de la base de datos es el de obtener una estructura estable y lógica tal que:

- El sistema de base de datos no sufra de anomalías de almacenamiento.
- El modelo lógico pueda modificarse fácilmente para admitir nuevos requerimientos.

Una base de datos implantada sobre un modelo bien diseñado tiene mayor esperanza de vida aun en un ambiente dinámico, que una base de datos con un diseño pobre. En promedio, una base de datos experimenta una reorganización general cada seis años, dependiendo de lo dinámico de los requerimientos de los usuarios. Una base de datos bien diseñada tendrá un buen desempeño aunque aumente su tamaño, y será lo suficientemente flexible para incorporar nuevos requerimientos o características adicionales.

3.2.1 Normalización

3.2.1.1 Primera forma normal (1FN)

Se considera que una relación se encuentra en la primera forma normal cuando cumple lo siguiente:

1. Las celdas de las tablas posean valores simples y no se permiten grupos ni arreglos repetidos como valores, es decir, contienen un solo valor por cada celda.
2. Todos los ingresos en cualquier columna (atributo) deben ser del mismo tipo.
3. Cada columna debe tener un nombre único, el orden de las columnas en la tabla no es importante.

4. Dos filas o renglones de una misma tabla no deben ser idénticas, aunque el orden de las filas no es importante.
5. Las columnas repetidas deben eliminarse y colocarse en tablas separadas.

El evento de asignar una clave de usuario implica que debe haberse establecido un perfil de usuario; la Fig.3.7 muestra la relación entre la tabla usuario y perfil que ejemplifica lo citado anteriormente.

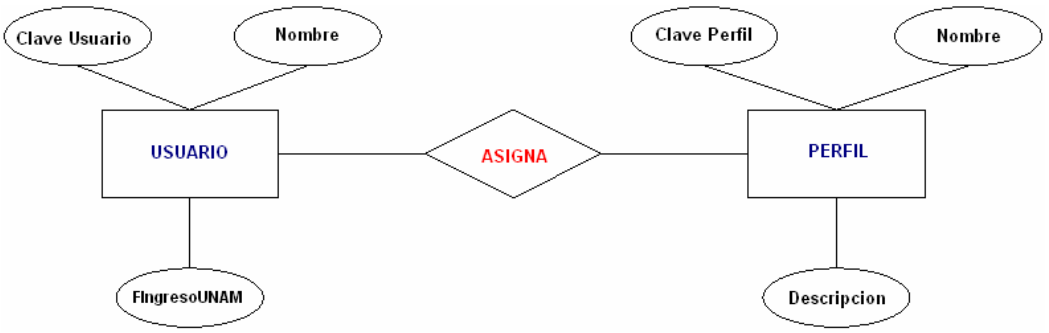


Fig.3.7 Representación gráfica de 1FN.

Tablas de catálogo: Son todas aquellas tablas en donde se almacenan los diferentes datos que puede tener una entidad.

Tablas de sistema: Son aquellas entidades que relacionan a tablas catálogo, principalmente son las tablas centrales en la base de datos.

El primer paso para el diseño de la base de datos fue identificar las entidades requeridas para la recolección y procesamiento de los datos; para esta definición fue necesario analizar la problemática a resolver. Con este análisis las tablas definidas son:

Usuario: En esta tabla se almacenan los datos personales de los usuarios registrados en el sistema junto con la fecha en el que fue registrado y el responsable que lo dio de alta. Ver Fig.3.8.

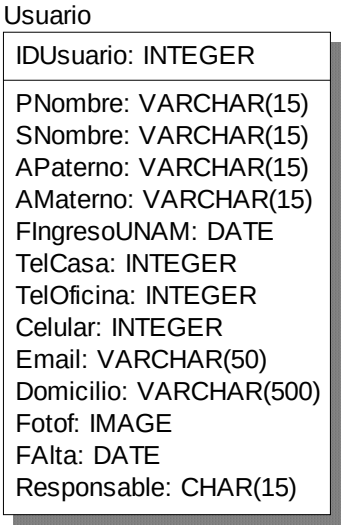


Fig.3.8 Tabla Usuario.

Perfil: Catálogo que contiene todos los perfiles permitidos dentro del sistema y que hasta el momento están definidos tres de ellos: Usuario, Propietario y Administrador. Ver Fig.3.9.

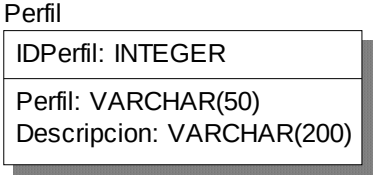


Fig.3.9 Tabla Perfil.

Área: Catálogo que contiene todas las diferentes áreas que existen dentro del Departamento de Computación de la Facultad de Ingeniería. Ver Fig. 3.10.

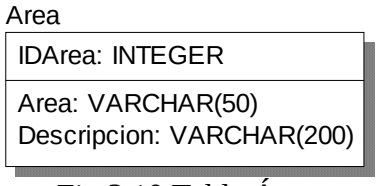


Fig.3.10 Tabla Área.

Status: Catálogo que contiene el estado en el que se encuentra el usuario dentro del sistema es decir si esta activo o inactivo. Ver Fig.3.11.

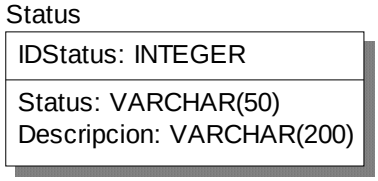


Fig.3.11 Tabla Status.

Nombramiento: Catálogo que contiene todos los diferentes nombramientos que están definidos dentro del Departamento de Computación de la Facultad de Ingeniería. Ver Fig.3.12.

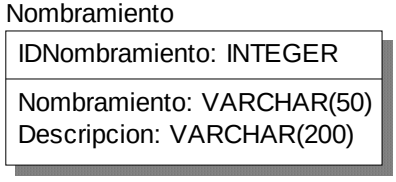


Fig.3.12 Tabla Nombramiento.

Mes: Catálogo que contiene un identificador por cada uno de los meses del año junto con su descripción, es decir, su nombre. Ver Fig.3.13.

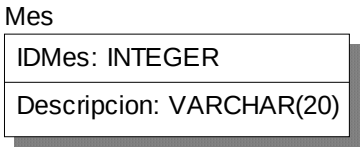


Fig.3.13 Tabla Mes.

Semestre: Catálogo que contiene toda la información relacionada a un semestre por su nombre, periodo y estado ya sea activo o inactivo. Ver Fig.3.14.

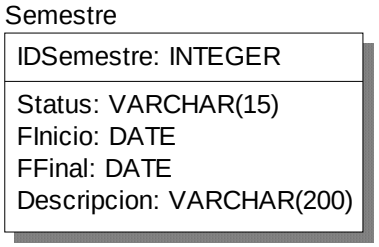


Fig.3.14 Tabla Semestre.

DiaNoLaboral: Catálogo de días no laborables considerados por el Departamento de Computación de la Facultad de Ingeniería. Ver Fig.3.15.

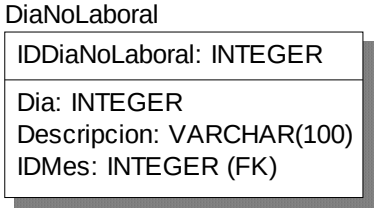


Fig.3.15 Tabla DiaNoLaboral.

ClaveUsuario: Tabla que contiene todas las diferentes claves que permiten el acceso al sistema KeYzara. Ver Fig.3.16.

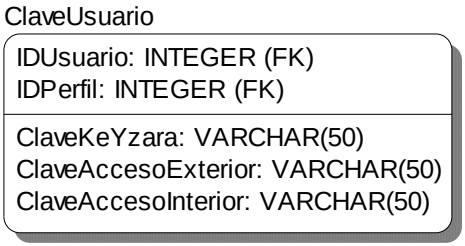


Fig.3.16 Tabla ClaveUsuario.

PerfilUsuario: Tabla que contiene la información que define a un usuario por perfil, área, nombramiento y status. Ver Fig.3.17.

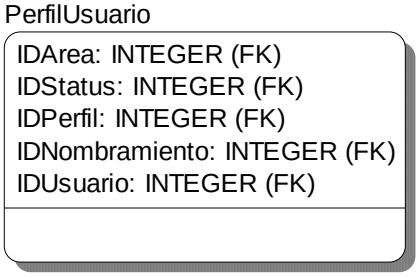


Fig.3.17 Tabla PerfilUsuario.

DiaHoraLaboral: Tabla que contiene la información correspondiente a la jornada y horario que un usuario tiene acceso al sistema KeYzara. Ver Fig.3.18.

Fig.3.18 Tabla DiaHoraLaboral.

DiaExtraordinario: Tabla que guarda la relación de días que un usuario tiene permitido accesar al sistema KeYzara siendo días no laborables. Ver Fig.3.19.

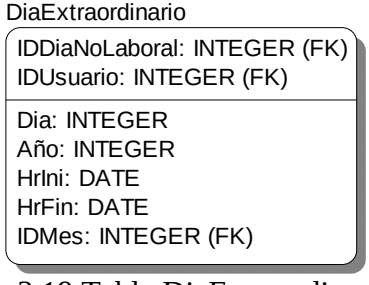


Fig.3.19 Tabla DiaExtraordinario.

3.2.1.2 Segunda forma normal (2FN)

Para definir formalmente la segunda forma normal requerimos saber que es una **dependencia funcional:** Consiste en edificar que atributos dependen de otro(s) atributo(s). Ver Fig. 3.20.

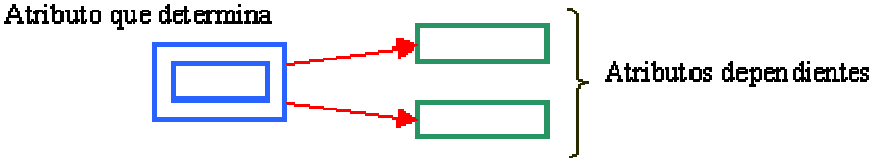


Fig. 3.20 Representación gráfica 2FN.

Definición formal: Una relación R está en 2FN si y solo si está en 1FN y los atributos dependen funcionalmente de la llave primaria. Una relación se encuentra en segunda forma normal, cuando cumple con las reglas de la primera forma normal y todos sus atributos que no son llaves, dependen por completo de está. De acuerdo con está definición, cada tabla que tiene un atributo único como llave primaria, esta en segunda forma normal.

La segunda forma normal se representa por dependencias funcionales como lo muestra la Fig.3.21, la tabla Usuario almacena a todas las personas autorizadas, de las cuales cada una de ellas tiene una clave única que los identifica.

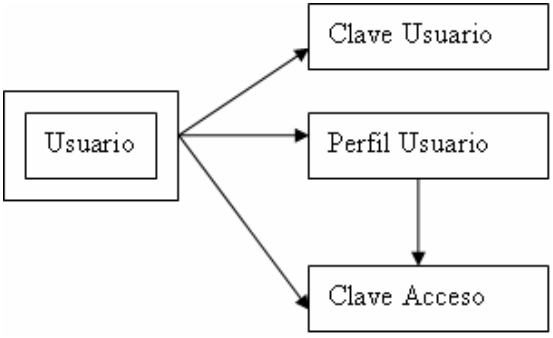


Fig. 3.21 Dependencias funcionales.

Nótese que las llaves primarias están representadas con doble cuadro, las flechas nos indican que de estos atributos se puede referenciar a los otros atributos que son funcionalmente la llave primaria.

3.2.1.3 Tercera forma normal (3FN)

Para definir formalmente la 3FN necesitamos definir **dependencia transitiva:** En una afinidad (tabla bidimensional) que tiene por lo menos 3 atributos (A,B,C) en donde A determina a B**,** B determina a C pero no determina a A.
Dependencia formal: Una relación R está en 3FN si y solo si esta en 2FN y todos sus atributos no primos dependen no transitivamente de la llave primaria.
Consiste en eliminar la dependencia transitiva que queda en una segunda forma normal, en pocas palabras una relación esta en tercera forma normal si está en segunda forma normal y no existen dependencias transitivas entre los atributos; nos referimos a dependencias transitivas cuando existe más de una forma de llegar a referencias a un atributo de una relación. Por ejemplo, consideremos el siguiente caso:

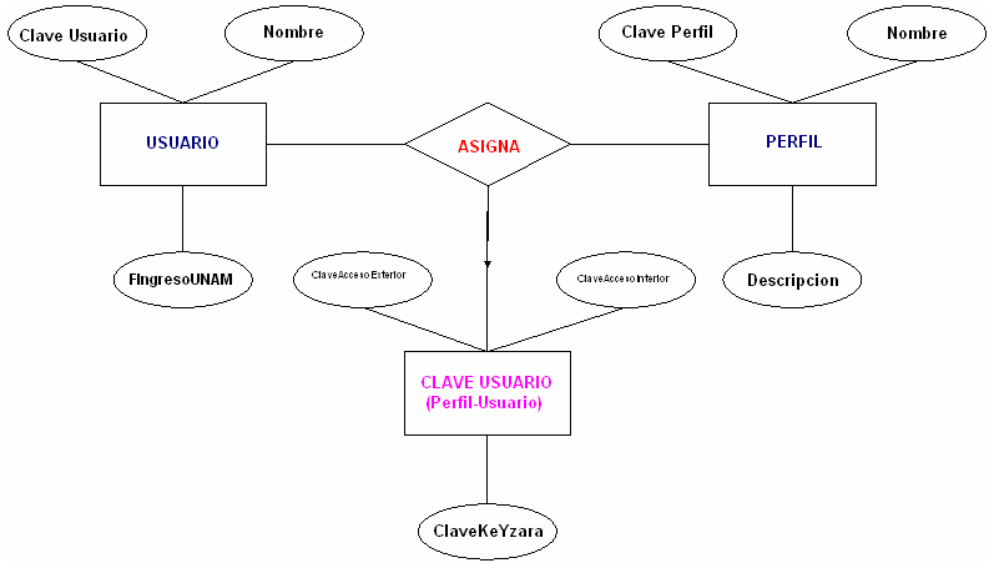


Fig.3.22 Diagrama usuario-claveusuario-perfil

La Fig.3.22 muestra la relación usuario-claveusuario-perfil, pero en especial consideremos al elemento usuario, gráficamente la podemos representar de la siguiente manera.

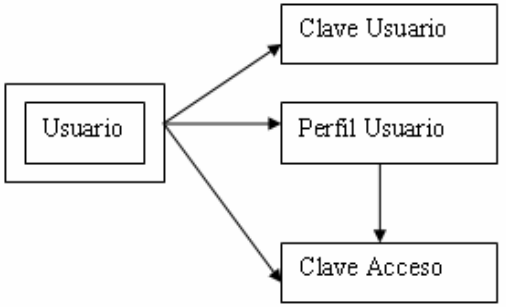


Fig. 3.23 Relación en segunda forma normal

La Fig.3.23 muestra a la relación en segunda forma normal, los atributos llave están indicados en doble cuadro indicando los atributos que dependen de dichas llaves, sin embargo, en la llave Usuario tiene como dependientes a 3 atributos en el cual la clave acceso puede ser referenciado por dos atributos: Usuario y PerfilUsuario, (existe dependencia transitiva), esto se soluciona al aplicar la tercer forma normal que consiste en eliminar estas dependencias separando los atributos, por lo tanto tenemos:

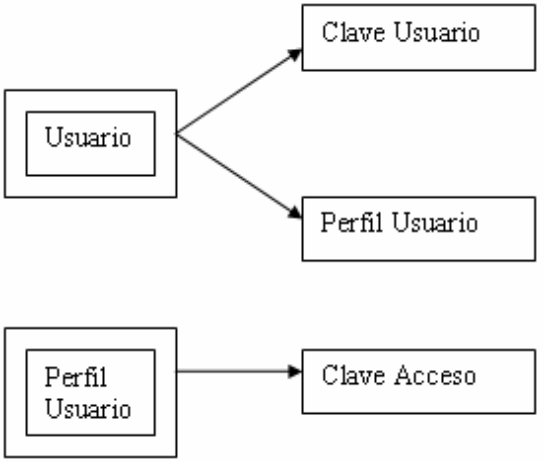


Fig.3.24 Diagramas en tercera forma normal

La Fig.3.24 muestra la eliminación de las dependencias, finalmente la dependencia transitiva se rompió al separar los atributos que dependen directamente de la llave primaria, es decir, en este diagrama en tercera forma normal tenemos a dos dependencias por separado, por un lado tenemos al elemento Usuario y sus atributos ClaveUsuario y PerfilUsuario; y por otro PerfilUsuario con el atributo ClaveAcceso.

Una vez definidas las tablas en 1FN, se aplico la 2FN en donde aparecieron dependencias transitivas como en el ejemplo anterior, por lo que fue necesario aplicar 3FN, es así como el diseño final de la base de datos quedo de la siguiente manera, Ver Fig.3.25.

3.2.2 Diagrama Entidad-Relación

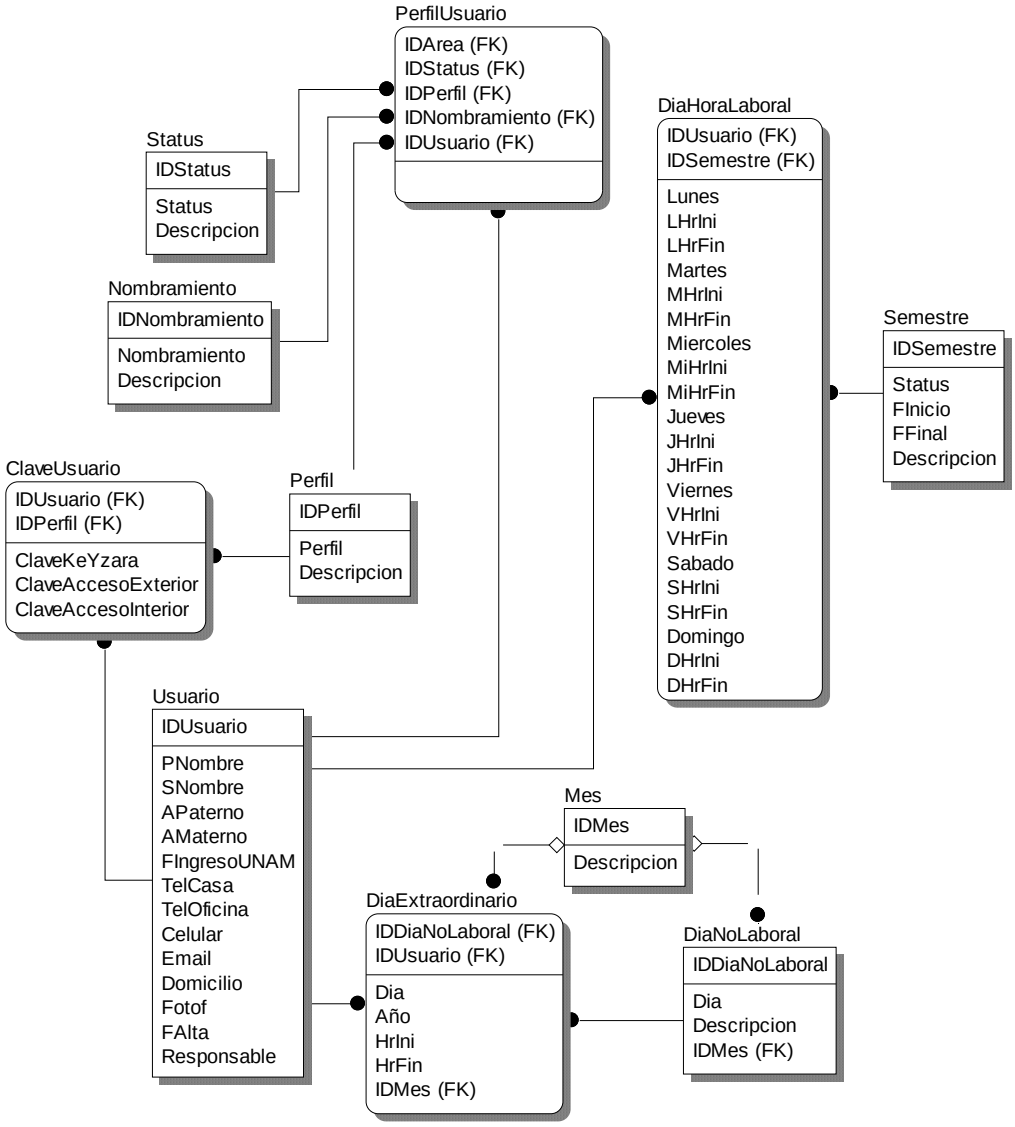


Fig.3.25 Diagramas Entidad-Relación del sistema KeYzara.

3.2.3 Diccionario de Datos

Usuario

Nombre	Null?	Tipo	Descripción
IDUsuario	Not Null	integer	Clave del usuario.
PNombre		varchar(15)	Primer nombre del usuario.
SNombre		varchar(15)	Segundo nombre del usuario.
APaterno		varchar(15)	Apellido paterno del usuario.
AMaterno		varchar(15)	Apellido materno del usuario.
FIngresoUNAM		date	Fecha de ingreso a la UNAM del usuario.
TelCasa		integer	Teléfono de casa del usuario.
TelOficina		integer	Teléfono de oficia del usuario.
Celular		integer	Número de celular del usuario.
Email		varchar(50)	Correo electrónico del usuario.
Domicilio		varchar(500)	Domicilio del usuario.
Foto		image	Foto del usuario.
FAlta		date	Fecha de alta del usuario en el sistema KeYzara.
Responsable		varchar(15)	Nombre del administrador que dio de alta un usuario.

Perfil

Nombre	Null?	Tipo	Descripción
IDPerfil	Not Null	integer	Clave del perfil de usuario.
Perfil		varchar(50)	Nombre del perfil de usuario. (Administrador,

Descripción		varchar(200)	Propietario y Usuario) Descripción del perfil de usuario.

Área

Nombre	Null?	Tipo	Descripción
IDArea	Not Null	integer	Clave de área.
Área		varchar(50)	Nombre de área.
Descripcion		varchar(200)	Descripción del área.

Status

Nombre	Null?	Tipo	Descripción
IDStatus	Not Null	integer	Clave de status.
Status		varchar(50)	Nombre de status.
Descripcion		varchar(200)	Descripción del status.

Nombramiento

Nombre	Null?	Tipo	Descripción
IDNombramiento	Not Null	integer	Clave del nombramiento.
Nombramiento		varchar(50)	Nombre del nombramiento.
Descripcion		varchar(200)	Descripción del nombramiento.

Mes

Nombre	Null?	Tipo	Descripción
IDMes	Not Null	integer	Clave del mes.

Descripcion	varchar(20)	Nombre del mes.

Semestre

Nombre	Null?	Tipo	Descripción
IDSemestre	Not Null	integer	Clave del semestre.
Status		varchar(15)	Status del semestre.
FInicio		date	Fecha de inicio del semestre.
FFinal		date	Fecha de fin del semestre.
Descripcion		varchar(200)	Descripción del semestre.

DiaNoLaboral

Nombre	Null?	Tipo	Descripción
IDDiaNoLaboral	Not Null	integer	Clave del día no laboral.
Dia		integer	Número de día.
Descripcion		varchar(100)	Descripción del día no laboral.
IDMes	Not Null	integer	Clave del mes.

ClaveUsuario

Nombre	Null?	Tipo	Descripción
IDUsuario	Not Null	integer	Clave de usuario.
IDPerfil	Not Null	integer	Clave del perfil.
ClaveKeYzara		varchar(50)	Clave de acceso al sistema KeYzara sólo para el administrador y propietario.
ClaveAccesoExterior		varchar(50)	Clave de acceso exterior.
ClaveAccesoInterior		varchar(50)	Clave de acceso interior.

PerfilUsuario

Nombre	Null?	Tipo	Descripción
IDArea	Not Null	integer	Clave de área.
IDStatus	Not Null	integer	Clave de status.
IDPerfil	Not Null	integer	Clave de perfil.
IDNombramiento	Not Null	integer	Clave de nombramiento.
IDUsuario	Not Null	integer	Clave del usuario.

DiaHoraLaboral

Nombre	Null?	Tipo	Descripción
IDUsuario	Not Null	integer	Clave de usuario.
IDSemestre	Not Null	integer	Clave de semestre.
Lunes		boolean	Día laboral-Lunes.
LHrIni		date	Hora de inicio del lunes laboral.
LHrFin		date	Hora de fin del lunes laboral.
Martes		boolean	Día laboral-Martes.
MHrIni		date	Hora de inicio del martes laboral.
MHrFin		date	Hora de fin del martes laboral.
Miercoles		boolean	Día laboral-Miércoles.
MiHrIni		date	Hora de inicio del miércoles laboral.
MiHrFin		date	Hora de fin del miércoles laboral.
Jueves		boolean	Día laboral-Jueves.
JHrIni		date	Hora de inicio del jueves laboral.
JHrFin		date	Hora de fin del jueves

		laboral.
Viernes	boolean	Día laboral-Viernes.
VHrIni	date	Hora de inicio del viernes laboral.
VHrFin	date	Hora de fin del viernes laboral.
Sabado	boolean	Día laboral-Sábado.
SHrIni	date	Hora de inicio del sábado laboral.
SHrFin	date	Hora de fin del sábado laboral.
Domingo	boolean	Día laboral-Domingo.
DHrIni	date	Hora de inicio del domingo laboral.
DHrFin	date	Hora de fin del domingo laboral.

DiaExtraordinario

Nombre	Null?	Tipo	Descripción
IDDiaNoLaboral	Not Null	integer	Clave del día no laboral.
IDUsuario	Not Null	integer	Clave de usuario.
Dia		integer	Número de día.
Año		integer	Número de año.
HrIni		date	Hora de inicio del día extraordinario.
HrFin		date	Hora de fin del día extraordinario.
IDMes	Not Null	integer	Clave del mes.

CAPÍTULO 4

FUNCIONALIDADES DEL SISTEMA

Este capítulo tiene como objetivo describir la estructura y las principales funcionalidades con las que cuenta el sistema KeYzara.

En el presente capítulo se hará referencia a el Apéndice A, el cual contiene sugerencias para un mejor funcionamiento del sistema KeYzara.

4.1 Sistema KeYzara - Inicio

Para poder acceder a la aplicación y mantener un control de las entradas y cambios que se realicen, es necesario iniciar una sesión ingresando el usuario y clave en la pantalla que se muestra a continuación: Fig.4.1.

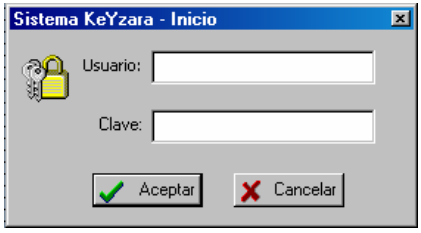


Fig.4.1. Pantalla de inicio

Cabe mencionar que los únicos perfiles con autorización para ingresar a la aplicación son el Propietario y Administrador. (Ver Apéndice A; A.1).

4.2 Estructura principal de la aplicación

Al iniciar una sesión en el sistema KeYzara, se desplegará la pantalla principal la cual se muestra en la Fig.4.2.

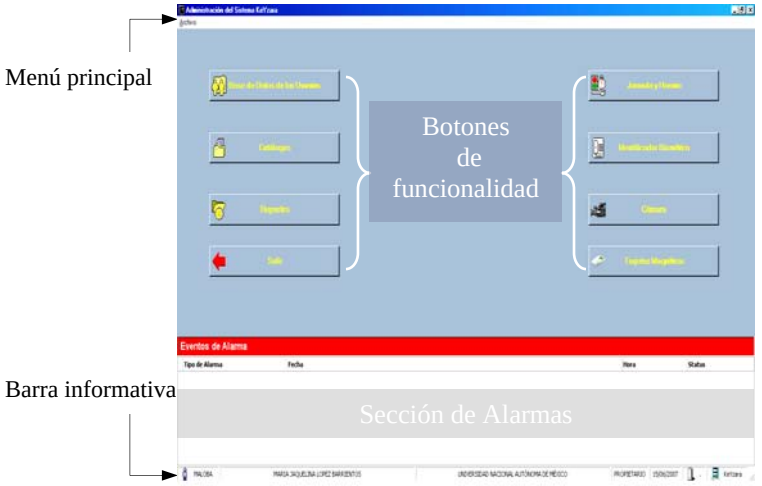


Fig.4.2. Pantalla principal del sistema KeYzara.

4.3 Botones de Funcionalidad

4.3.1 Base de Datos de los Usuarios

En esta sección se agregan, modifican o eliminan datos de usuarios, así como se puede generar un reporte con todos los usuarios registrados. (Ver Apéndice A; A.2.1)

La pantalla principal que manipula el catálogo de usuarios se muestra a continuación: Fig.4.3.

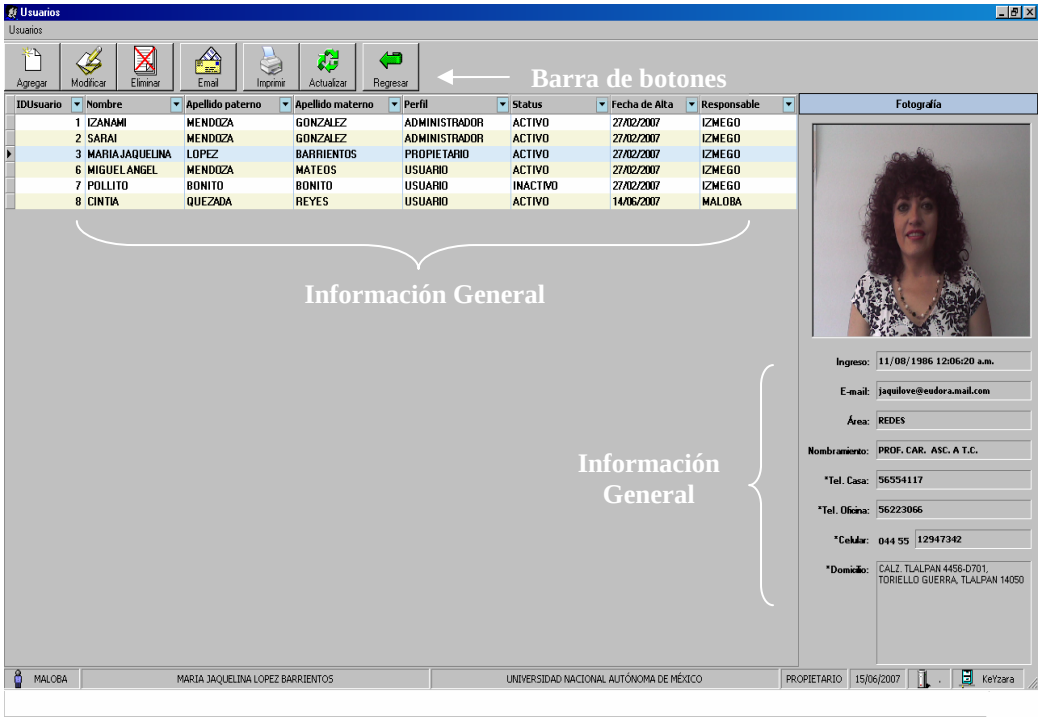


Fig.4.3. Pantalla principal de la base de datos de los usuarios.

La funcionalidad resumida de cada uno de los botones que aparecen en la pantalla de la Fig.4.3 se muestra a continuación (véase la tabla 4.1) y enseguida se describe cada uno de ellos.

Botón	Funcionalidad
	Muestra la pantalla de captura de información para un nuevo usuario.

Botón	Funcionalidad
	Muestra la pantalla donde los datos de un usuario pueden ser modificados.
	Elimina el registro completo de un usuario.
	Envía el usuario y claves generadas durante el registro.
	Imprime el reporte de todos los usuarios registrados.
	Refresca los datos procesados en la pantalla principal.
	Cierra la pantalla.

Tabla 4.1. Funcionalidad de los botones de la pantalla base de datos de los usuarios.

Agregar: Para agregar un usuario al sistema, la información requerida se divide en tres secciones: Información general, Información adicional e Información opcional (véase la figura 4.4). Para que el registro se concluya es obligatorio que la información general y adicional sea proporcionada mientras que la información opcional, puede o no ser incorporada.

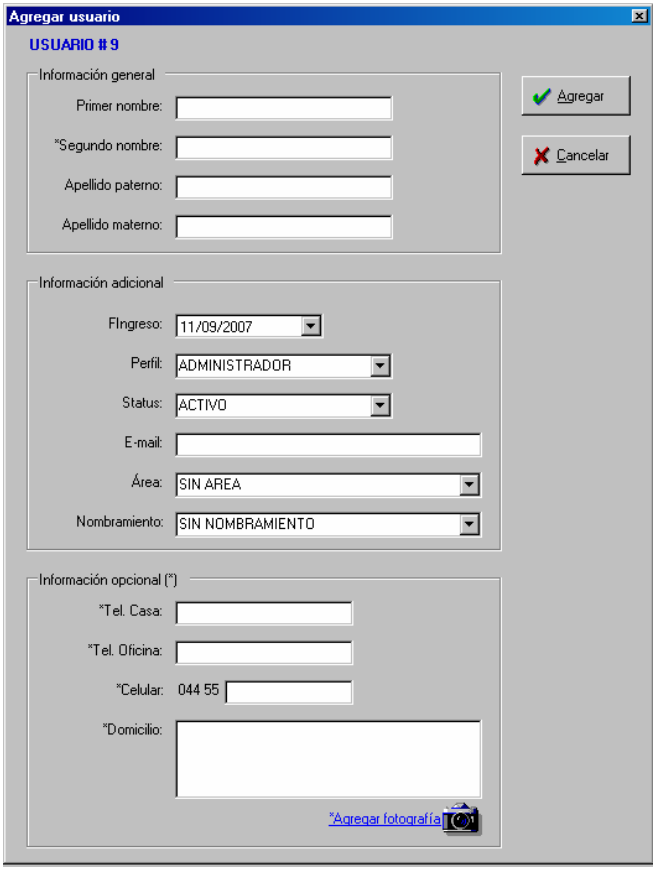


Fig.4.4. Pantalla para ingresar los datos de un nuevo usuario.

Para que el Administrador del sistema KeYzara ubique con mayor facilidad a los usuarios registrados se puede incorporar su fotografía al sistema.

Agregar fotografía: El procedimiento para agregar o modificar la fotografía de un usuario consiste solamente en seleccionar la ubicación o ruta del archivo fotográfico, visualizar la imagen y si es la deseada confirmamos dando un click en el botón Agregar como se muestra en la Fig.4.5. En caso contrario tenemos la opción de cancelar en la parte inferior de la pantalla.

Fig.4.5 Pantalla para visualizar e ingresar una imagen a un nuevo usuario.

Modificar: Para poder modificar los datos o fotografía de un usuario, primeramente hay que seleccionar el usuario y posteriormente dar un click en el botón Modificar. Aparecerá una pantalla con los datos cargados y correspondientes al usuario seleccionado listos para poder editarlos como se muestra en la figura 4.6.

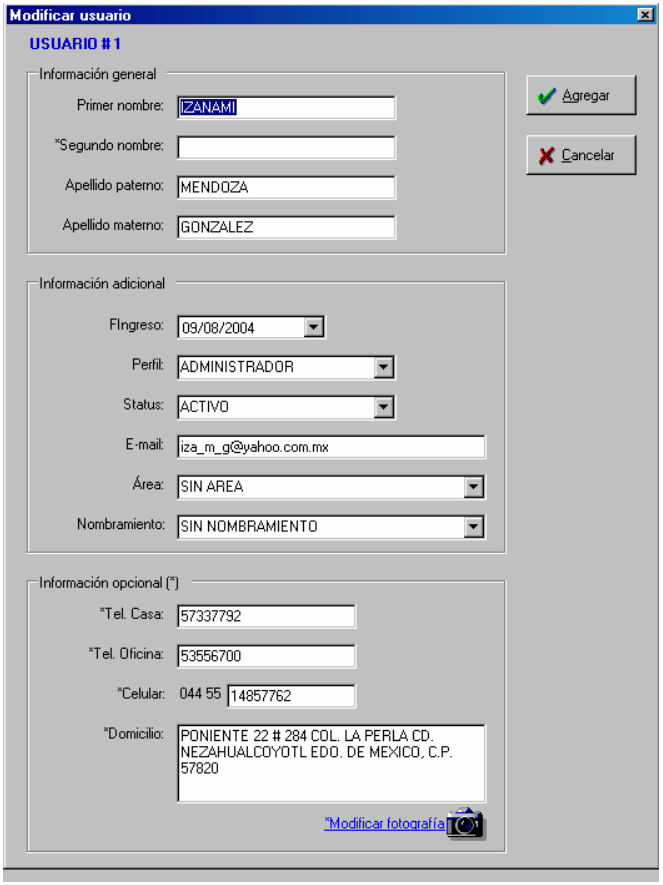


Fig.4.6 Pantalla para modificar los datos de un usuario.

Eliminar: Para eliminar hay que seleccionar el usuario, dar click en el botón eliminar y por último confirmar el mensaje de advertencia antes de realizar el borrado. Ver Fig.4.7.

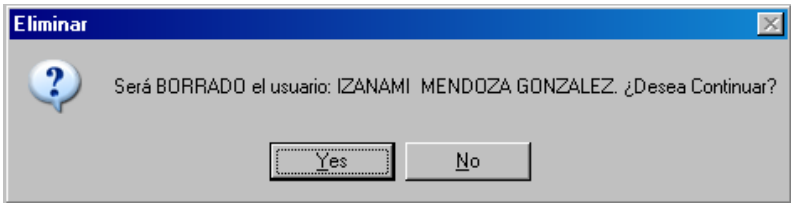
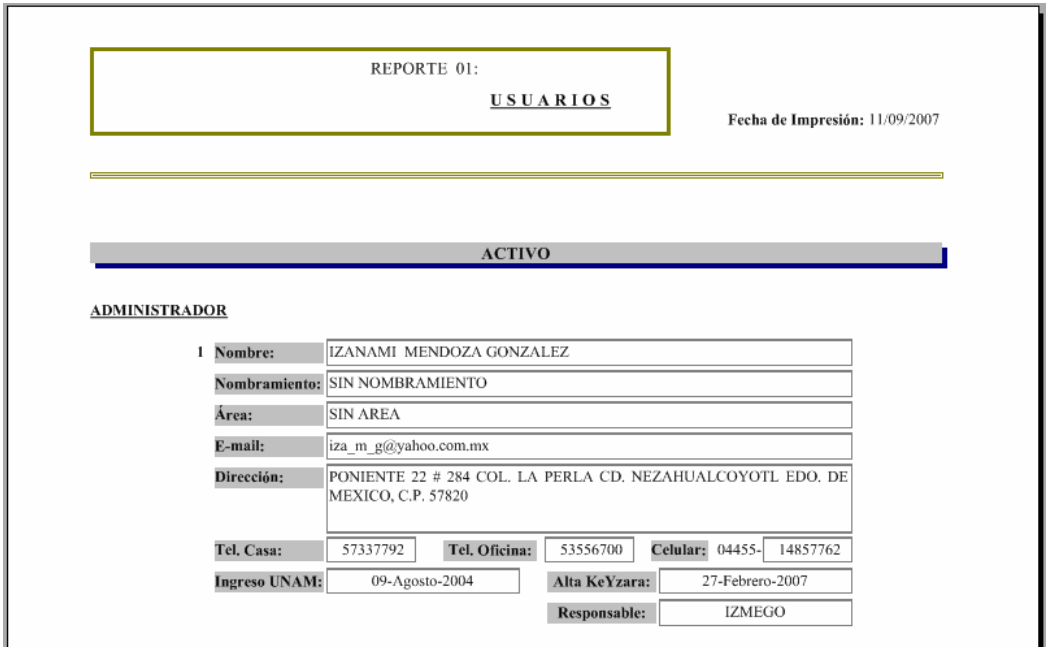


Fig. 4.7 Mensaje de confirmación antes de borrar un usuario de la base de datos.

Imprimir: Se puede visualizar e imprimir un reporte con todos los datos de los usuarios registrados en el sistema. Ver Fig.4.8.



REPORTE 01:

USUARIOS

Fecha de Impresión: 11/09/2007

ACTIVO

ADMINISTRADOR

1	**Nombre:**	IZANAMI MENDOZA GONZALEZ				
	Nombramiento:	SIN NOMBRAMIENTO				
	Área:	SIN AREA				
	E-mail:	iza_m_g@yahoo.com.mx				
	Dirección:	PONIENTE 22 # 284 COL. LA PERLA CD. NEZAHUALCOYOTL EDO. DE MEXICO, C.P. 57820				
	Tel. Casa:	57337792	**Tel. Oficina:**	53556700	**Celular:**	04455-14857762
	Ingreso UNAM:	09-Agosto-2004	**Alta KeYzara:**	27-Febrero-2007		
			Responsable:	IZMEGO		

Fig.4.8 Visualización del reporte correspondiente a los usuarios.

4.3.2 Catálogos

En esta sección se agregan, modifican o eliminan los datos correspondientes a cada catálogo, así como se puede generar un reporte con la información registrada. Ver Fig.4.9.

Los catálogos con los que se cuenta son los siguientes: Área, Días no laborables, Nombramiento, Perfil usuario y Semestre. Ver Fig.4.9.

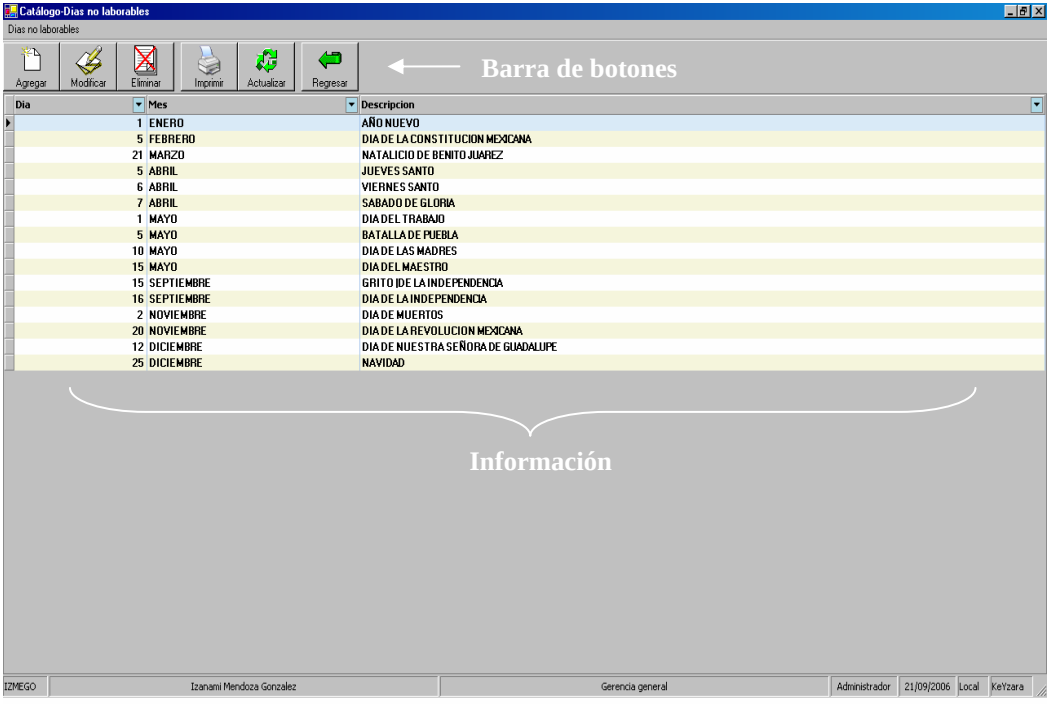


Fig. 4.9 Pantalla principal de los catálogos.

La funcionalidad resumida de cada uno de los botones que aparecen en la pantalla de la figura 4.9 se describe a continuación (véase la tabla 4.2):

Botón	Función
	Muestra la pantalla de captura de información para agregar datos a un catálogo.
	Muestra la pantalla donde los datos de un catálogo pueden ser modificados.
	Elimina la información seleccionada de un catálogo.
	Imprime el reporte de los catálogos: Área, Días no laborables, Nombramiento, Perfil usuario y Semestre.
	Refresca los datos procesados en la pantalla principal.
	Cierra la pantalla.

Tabla 4.2. Funcionalidad de los botones de la pantalla principal de los catálogos.

Agregar: Para agregar información a un catálogo hay que proporcionar los datos requeridos en la pantalla y dar click en el botón Aceptar, ver Fig.4.10.

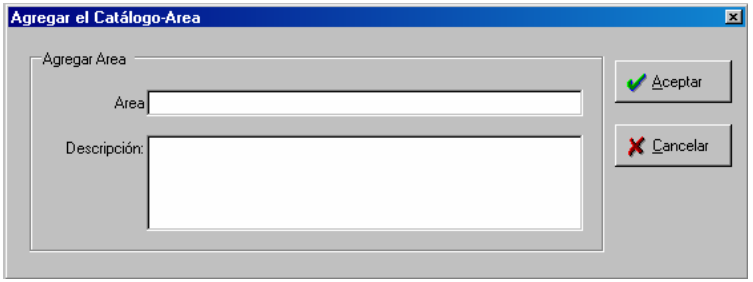


Fig.4.10 Pantalla para ingresar los datos de un nuevo catálogo.

Modificar: Para poder modificar los datos de un catálogo, primeramente hay que seleccionar el registro que se quiere modificar y posteriormente dar un click en el botón Modificar. Aparecerá una pantalla con los datos cargados y correspondientes al registro seleccionado, listos para poder editarlos. Ver Fig.4.11.

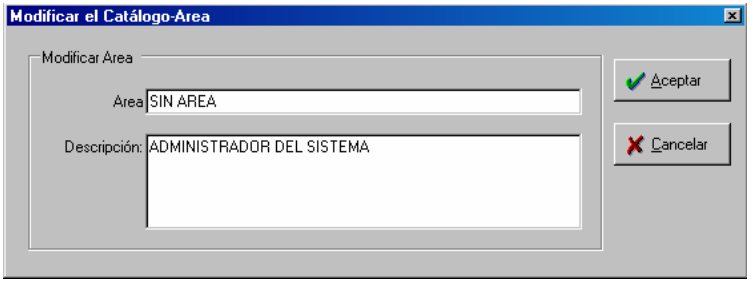


Fig.4.11 Pantalla para modificar los datos de un catálogo.

Eliminar: Para eliminar hay que seleccionar un registro, dar click en el botón eliminar y por último confirmar el mensaje de advertencia antes de realizar el borrado. Ver Fig.4.12.

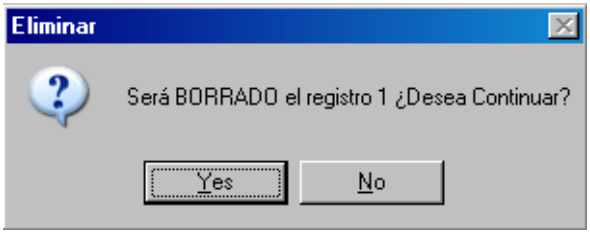
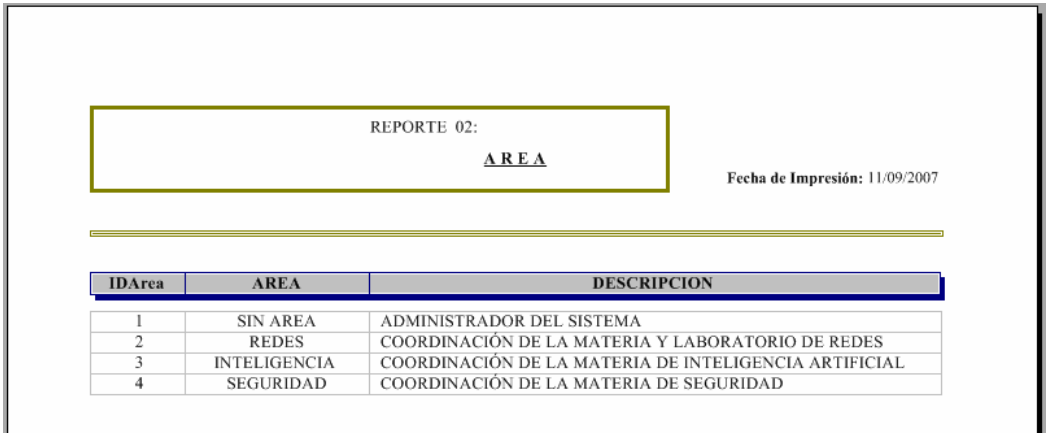


Fig. 4.12 Mensaje de confirmación antes de borrar un catálogo de la base de datos.

Imprimir: Se puede visualizar e imprimir un reporte con los datos correspondientes al catálogo que se está trabajando. Ver Fig.4.13.



REPORTE 02:

A R E A

Fecha de Impresión: 11/09/2007

IDArea	AREA	DESCRIPCION
1	SIN AREA	ADMINISTRADOR DEL SISTEMA
2	REDES	COORDINACIÓN DE LA MATERIA Y LABORATORIO DE REDES
3	INTELIGENCIA	COORDINACIÓN DE LA MATERIA DE INTELIGENCIA ARTIFICIAL
4	SEGURIDAD	COORDINACIÓN DE LA MATERIA DE SEGURIDAD

Fig. 13 Visualización del reporte correspondiente a los catálogos.

4.3.3 Jornada y Horario

En esta sección se asigna la jornada y horario por cada usuario que se encuentre registrado en el sistema KeYzara incluyendo o no días no laborables. Ver Fig.4.14.

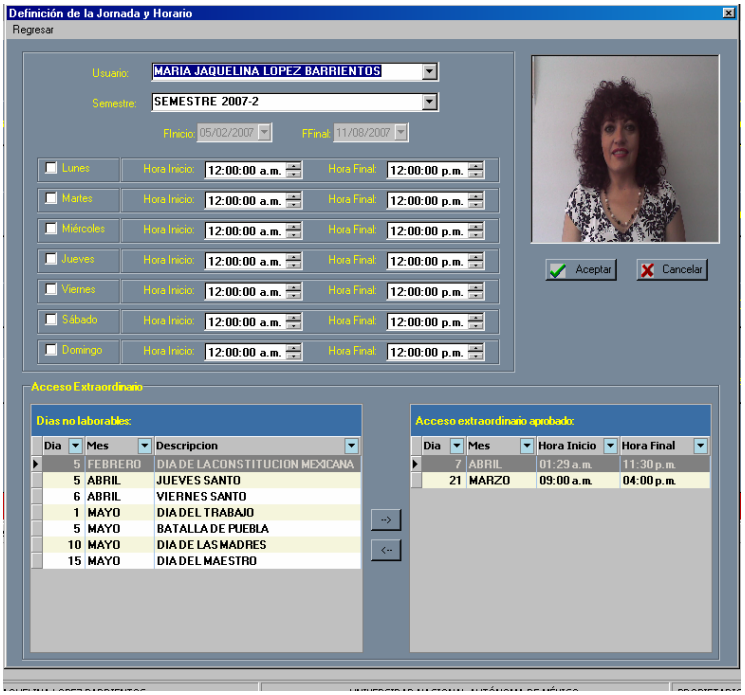


Fig.4.14 Pantalla principal para asignar una jornada y un horario a un usuario.

Acceso extraordinario: Para otorgar acceso a los usuarios en días no laborables basta con seleccionar el día en el recuadro de los días no laborables y agregarlo al acceso extraordinario aprobado. Al momento de agregarlo aparecerá una pantalla para definir el horario de acceso sólo para ese día como se aprecia en la Fig.4.15.

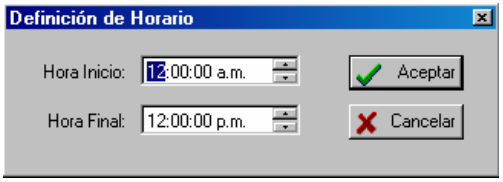


Fig. 4.15 Pantalla para definir un horario a un usuario.

CAPÍTULO 5

TECNOLOGÍA A FUTURO

En el presente capítulo, se hablará del futuro de la tecnología de los dispositivos que emplea el Sistema KeyZara, ya que esta avanza a pasos agigantados.

5.1. Tecnología a futuro

El futuro es la tecnología biométrica ya que llaves, tarjetas, pasaportes y códigos de seguridad podrían pasar a ser cosas del pasado a medida que la tecnología biométrica hace de nuestros cuerpos las únicas contraseñas que necesitamos.

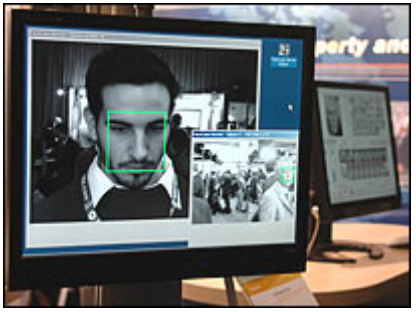


Fig.5.1. Algunos sistemas seleccionan rostros en una multitud.

Los sistemas biométricos -los cuales identifican a una persona por sus rasgos físicos o de comportamiento intrínsecos - están siendo rápidamente diseñados y utilizados en muchos aspectos de nuestra vida cotidiana.

La tecnología biométrica utiliza principalmente el reconocimiento de rasgos faciales, del iris o del dedo. Sin embargo, otros sistemas utilizan desde las venas en la mano de un individuo hasta la forma en que éste habla.

El Reino Unido es uno de 27 países vinculados al *US Visa Waiver Program*, un programa estadounidense que exime de la necesidad de obtener visa a los ciudadanos de algunas naciones.

El gobierno estadounidense exige como parte de ese programa que todos los pasaportes emitidos después del 26 de octubre de 2006, deben tener un chip con los detalles del portador del documento además de un identificador biométrico como la fotografía digital del dueño del pasaporte.

5.2 Alta Tecnología

Las autoridades afirman que esta medida busca en primer lugar evitar el fraude en la obtención de pasaportes. Bajo este programa, un funcionario de seguridad comparará la fotografía digital con la foto física y el portador del documento.

Sin embargo, ya está disponible la tecnología para que las revisiones sean automáticas.

Un pasajero mirará hacia una cámara en un punto de control fronterizo. A partir de este procedimiento una computadora elaborará un mapa de puntos clave de su rostro, que luego serán comparados con aquellos puntos claves o rasgos únicos, almacenados en el chip que contiene su pasaporte. Este proceso confirmará la identidad de la persona.

Fig. 5.2. La tecnología biométrica es utilizada por las fuerzas militares estadounidenses.

Éste es sólo un ejemplo de cómo la tecnología biométrica está siendo aplicada.

Las compañías especializadas están desarrollando tecnología para ser utilizada en múltiples situaciones, desde equipos portátiles hasta la entrada a edificios, la vigilancia callejera y la "guerra contra el terror".

La entrada a edificios u oficinas mediante tecnología biométrica, que obviaría la necesidad de carnets, tarjetas de identidad o llaves de los empleados y el riesgo de que éstos se extravíen, sean robados o utilizados incorrectamente- es uno de los principales aspectos en que trabaja la industria.

La tecnología bidimensional del rostro es utilizada en los pasaportes biométricos.

En segundos, un sistema identifica 40.000 puntos en el rostro sobre la base de rasgos geométricos faciales, la inclinación de la nariz, entre otros, con el fin de crear una imagen en tres dimensiones, que posteriormente es almacenada junto con los datos personales del individuo y los permisos de acceso.

5.3 Clave bancaria: las venas de la mano

En Japón, más de 16.000 oficinas bancarias y 16.400 cajeros automáticos cuentan con un nuevo sistema de identificación de lectura biométrica el patrón de las venas de la palma de la mano que, al estar dos o tres milímetros bajo la epidermis, son una clave infalsificable, más precisa que las huellas dactilares o el iris ocular, ya de por sí seguros.

Las investigaciones demuestran que el patrón de las venas es único para cada individuo, incluso en el caso de gemelos idénticos, y que éste permanece inalterable desde que el individuo se encuentra en el feto materno hasta su muerte. Asumir una falsa identidad falsificando las venas es extremadamente difícil, ya que la sangre tiene que estar fluyendo para registrar la imagen o patrón.

La firma Fujitsu, alma máter de este proyecto, ofrece esta revolucionaria tecnología también para el control de acceso a edificios de alta seguridad, identificación de clientes o aplicaciones bancarias. En España, la entidad bancaria "La Caixa", con 7.000 cajeros y 8,9 millones de tarjetas emitidas, va a llevar a cabo la prueba piloto.

La cultura de las tarjetas invade el mundo hasta el punto de que una persona con mucho efectivo en el bolsillo despierta recelo. Y, como los expertos lo saben, estrujan el cerebro para lanzar novedades ayudados por las últimas tecnologías, desde la adquisición de entradas de cine por el móvil hasta tarjetas con lector incorporado para comprar sin abrir el monedero.

Las nuevas tecnologías nos hacen ser cada día más perezosos y ya no sólo pretendemos tener una tarjeta en el bolsillo, sino hacer uso de ella sin abrir el monedero o comprar una entrada de cine por Internet sin tener que hacer cola. Sin problema; porque la misma entidad bancaria, en colaboración con Movistar, está poniendo en marcha un nuevo sistema para pequeños pagos, y una adaptación de nuestro móvil para adquirir las entradas de cine mediante un lector especial a distancia.

"Del sofá de tu casa, al cine, sin colas innecesarias" podría denominarse esta campaña, consistente en comprar la entrada por Internet, teléfono, o en un cajero automático y solicitar que se nos remita un código de barras de dos dimensiones al móvil mediante un SMS.".

La pantalla del móvil, dirigida a un lector habilitado para este fin, valida la entrada y el cliente puede pasar de inmediato a ver su película preferida, iniciativa que se plantea con la idea futura de que sirva para todo tipo de espectáculos.

¿Ciencia- ficción? No, tan sólo nuevas tecnologías. Lectores de tarjetas en cada comercio, desarrollados por Visa, que ya están siendo paulatinamente instalados y que en un breve plazo de tiempo tendrán todos los establecimientos, sin ningún coste inicial ni para el cliente ni para el propietario de la tienda.

Así, se sustituye la lectura de la banda magnética de la tarjeta por la radiofrecuencia y, con tan sólo mantener el monedero o la tarjeta frente a un dispositivo, los datos son leídos por la última tecnología de radiofrecuencia, denominada Near Field Communication. Los datos se transmiten

inmediatamente y el cliente sabe que la operación es correcta porque se enciende una luz y se emite un pitido desde el lector de tarjetas.

5.4. Mecanismos portátiles

El reconocimiento facial también puede ser utilizado para observar a distancia a individuos, como por ejemplo en multitudes, clubes o reuniones públicas.

Algunos sistemas seleccionan rostros en una muchedumbre y los comparan con los rasgos almacenados en una base de datos.

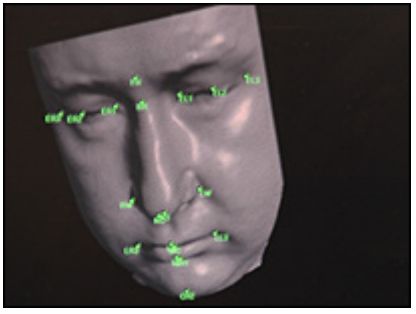


Fig. 5.4. Las imágenes en tres dimensiones pueden ser elaboradas y almacenadas en segundos.

El sistema de reconocimiento facial está siendo utilizado en casinos en Europa para identificar clientes indeseados e incluso a adictos a los juegos de azar que desean ser detenidos cuando la tentación de apostar se hace incontrolable.

Asimismo, las fuerzas estadounidenses desplegadas en Irak, Afganistán, Pakistán, Bosnia, Cuba y otras zonas en conflicto, ya están utilizando equipos

portátiles de reconocimiento de iris como mecanismos para fichar e identificar sospechosos.

Ante el auge de este tipo de tecnología, la biométrica será utilizada cada vez más en operaciones policivas y también en aspectos de la vida cotidiana.

Esta tecnología debe ser fácil y posible de utilizar y el usuario también tiene que estar dispuesto a utilizarla.

Se recomienda que esta tecnología sea adoptada con el paso del tiempo y con la familiaridad que adquiera el usuario con la biométrica al sistema KeyZara. Será algo parecido al proceso de *adaptación tras la incorporación del chip y la clave de seguridad en las tarjetas.*

CONCLUSIONES

El sistema de seguridad desarrollado proporciona la confidencialidad, integridad y disponibilidad de la información ya que por medio de los dispositivos con los que interactúa (Lector de huella dactilar, lector de tarjeta, cámara de video y los candados desarrollados) se tiene un adecuado control de acceso de los usuarios según sus intereses, para ello considera criterios establecidos que le permitan otorgar o denegar dicho acceso, lleva un control del uso del sistema a base de reportes diarios en casos de incidencias y de horarios y fechas de entrada y salida del personal a fin de identificar situaciones de riesgo y emitir alarmas de seguridad.

Debido a lo antes mencionado puede ser utilizado también como un sistema de control de asistencia y puntualidad del personal, así como también de horas extras laborables de cada elemento de la empresa, para facilitar el control de bonos por cumplimiento, puntualidad y compromiso con la empresa, si es que ésta lo desea.

Ya que la tecnología de software con la que está implementado el sistema KeYzara es Microsoft .Net, el tiempo de vida estimado del sistema será aproximadamente de tres a cuatro años, porque esta tecnología está en auge por el momento y se considera que por muchos años más. Por otro lado, se recomienda la actualización de los dispositivos de control de acceso en un periodo no más de dos años, debido a que como se mencionó en el Capítulo 5 la tecnología biométrica está avanzando rápidamente, aunque por los altos costos

aún no ha llegado al país, pero se estima que dentro de este periodo de tiempo contemos con ella.

El sistema de software desarrollado tiene la posibilidad de escalamiento a una versión Web, para una mejor administración del sistema desde cualquier ciudad del interior de la república u incluso otro país.

ANEXO A

RECOMENDACIONES

Este anexo tiene como objetivo describir las recomendaciones sugeridas para el buen funcionamiento del sistema KeYzara.

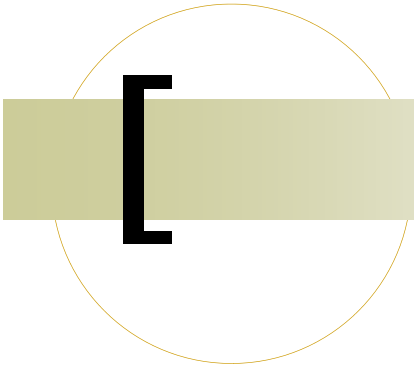
A.1 Inicio Sistema KeYzara

Ya que los únicos perfiles con autorización para ingresar a la aplicación son el Propietario y Administrador; se recomienda que las contraseñas de cada uno de estos usuarios sean distintas.

A.2 Botones de Funcionalidad

A.2.1 Base de Datos de los Usuarios

Se recomienda la actualización continua de los datos así como de las fotografías de usuarios en un periodo de 6 meses. Para que el Administrador del sistema KeYzara ubique con mayor facilidad a los usuarios registrados.



GLOSARIO

GLOSARIO DE TERMINOS

Este glosario contiene la definición de los conceptos mencionados a lo largo de los cinco capítulos que conforman este trabajo de tesis.

A

Administrador
Usuario que posee todos los permisos realizar todas las actividades dentro de un sistema de software.

Amenaza
Se representa a través de una persona, una circunstancia o evento, un fenómeno o una idea maliciosa, las cuales pueden provocar daño cuando existe una violación de la seguridad.

Asociaciones
Es la unión o enlace de dos o más entidades, las cuales se encuentran dentro del enlace del sistema y por ello el sistema debe mantener, correlacionar o desplegar información.

Atacante
También llamado perpetrador, oponente o persona que se entromete en un sistema informático.

Ataque
Realización de una amenaza. Necesita, para efectuarse, tres elementos: motivación, capacidad y oportunidad. Tienen varios objetivos incluyendo el fraude, la extorsión, el robo de información, la venganza o simplemente el desafío de penetrar un sistema.

Ataque pasivo
El atacante no altera en ningún momento la información, es decir, únicamente la observa, escucha, obtiene o monitorea mientras está siendo transmitida.

Ataque activo
Implican algún tipo de modificación de flujo de datos transmitido (modificación de la corriente de datos) o la creación de un falso flujo de datos (creación de una corriente falsa).

Autenticación
Es uno de los servicios más fáciles de comprender. Es simplemente: "verificar" la identidad.

B

Base De Datos
Es un conjunto de datos relacionados entre sí con un objetivo común. Es un conjunto de datos integrados y generalizados, estructurados.

C

Campo
Conjunto de datos de un mismo tipo.

Catálogo
Lista clasificada de los objetos de un tema determinado.

CCTV
Circuito Cerrado de Televisión.

Confidencialidad
Es la capacidad de asegurar que solo las personas autorizadas tienen acceso a algo.

Control de acceso
Determina qué usuario está autorizado para usar un recurso de manera requerida.

Criptoanálisis
Es una rama de la criptología. Se refiere a la ruptura o derrota de la criptografía, es decir, es el proceso que intenta descubrir el texto o la clave, la estrategia utilizada por el criptoanalista depende de la naturaleza del esquema de cifrado y de la información que tenga disponible.

Criptoanalista
(Puede ser un intruso) cuya tarea es descriptar la información transmitida por el canal. Tiene un total conocimiento para las técnicas usadas para encriptar y descriptar.

Criptografía
Es una rama de la criptología (kryptós =escondido, oculto; graphé = grafía, escritura) es el arte y la ciencia de transformar la información, es decir, es la encargada del diseño de procedimientos, controlados por una clave, para cifrar o enmascarar una determinada información de carácter confidencial.

Criptografía asimétrica o de clave pública
Los métodos asimétricos son aquellos en los que la clave de cifrado es diferente a la de descifrado. En términos generales, la clave de cifrado es conocida por todo el público, mientras que la de descifrado sólo es conocida por el usuario.

Criptografía simétrica o de clave secreta
Los métodos simétricos son aquellos en los que la clave de cifrado es la misma que la clave de descifrado. Para ello, es necesario que la clave únicamente sea conocida por el emisor y el receptor.

Criptología
Campo que trata con las comunicaciones seguras.

D

Dato
Es la unidad mínima de información, puede representar hechos, ideas o conceptos, que pueden ser reunidos y representados electrónicamente en forma digital.

DES (Data Encryption Standard)
Es un algoritmo de cifrado de bloque, donde la longitud de bloque es de 64 bits y la longitud de la clave es de 56 bits, si el texto es más grande entonces se procesa en bloques de 64 bits.

DFD
Diagrama de Flujo de Datos

DIFFIE – HELLMAN
El primer algoritmo de clave pública que define la criptografía de clave pública. El propósito del algoritmo es habilitar a los dos usuarios para intercambiar una clave secreta de manera más segura que puede ser utilizada para el subsecuente cifrado de mensajes. El algoritmo sólo se limita al intercambio de claves.

Disponibilidad
Se cumple si las personas autorizadas pueden acceder a la información deseada cuando lo requieran y tantas veces como sea necesario.

E

Entidad
Persona, departamento, organización u otro sistema de información que provee datos al sistema y/o recibe datos del sistema.

Escalabilidad
Capacidad de un sistema para soportar más carga de trabajo, usualmente debida al aumento de usuarios que lo utilizan

Escudo
Es una técnica, procedimiento o cualquier otra medida que reduzca la vulnerabilidad

F

Fraude
Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete.

H

Hacker
Experto informático especialista en entrar en sistemas ajenos sin permiso, generalmente para mostrar la baja seguridad de los mismos o simplemente para demostrar que es capaz de hacerlo.

I

IDEA (Internacional Data Encryotion Algorithm)
Es un cifrado de bloque simétrico, está diseñado par ser más seguro que el DES contra los ataques de fuerza bruta y diferentes tipos de criptoanalistas.

Información
Elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales.

Integridad
Proveer controles que aseguran que el contenido de los datos no haya sido modificado, y que la secuencia de los datos se mantenga durante la transmisión.

Intruso
Que se ha introducido sin derecho

K

Key clave de acceso
Una clave de acceso es una combinación de letras, números y signos que debe teclearse para obtener acceso a un programa o partes de un programa determinado, un terminal u ordenador personal, un punto en la red, etc. Entre las recomendaciones más habituales a la hora de elegir una clave de acceso, está el no utilizar nombres pertenecientes a familiares o amigos, fechas concretas (nacimiento, aniversario), nombres de mascotas, o palabras con significado (clave, acceso, etc.). Los expertos aconsejan utilizar una combinación de letras, números y signos («h+gy7/6t», por ejemplo) que debe cambiarse con relativa frecuencia.

Ll

Llave
Campo a partir del cual se pueden inferir otros campos de una tabla, por lo que, cada tupla debe estar asociada con una llave que permita su identificación.

Llave Alterna
(AK, Alternate Key). Atributo o conjunto de atributos que pueden ser seleccionados en un futuro como parte de la PK o incluso sustituirla.

Llave Candidata
Atributo o conjunto de atributos que son susceptibles de ser elegidos como PK.

Llave Foránea
(FK, Foreing Key).Atributo o conjunto de atributos que en la tabla padre forman la llave primaria y en la tabla hija son un atributo más y en algunas casos con la relación fuerte forman parte de la llave primaria.

Llave Primaria
(PK, Primary Key). Atributo o conjunto de atributos que permiten identificar de manera única cada renglón dentro de la tabla.

M

Modelo Relacional
Modelo lógico de una BD. Una BD relacional es aquella cuyos usuarios la perciben como un conjunto de tablas.

N

No repudio
Previene a los emisores o a los receptores de negar un mensaje transmitido. Se aplica al problema de la denegación falsa de la información que se recibe de otros o de la que uno ha enviado a otros. Los servicios de no repudio suministran pruebas que pueden ser demostradas a una tercera entidad.

Normalización
Es una técnica que se utiliza para comprobar la validez de los esquemas lógicos basados en el modelo relacional, ya que asegura que las relaciones (tablas) obtenidas no tengan datos redundantes.

P

Pirata informático
Es aquél que hace uso de los recursos libres y / o de pago que pueden ser movidos a través de las vías de la información que conforman internet, telnet, ftp (entre otras) para beneficio propio, que puede ser lucrativo o de otro tipo.
Por extensión, se considera pirata informático a quien hace uso de software que no ha adquirido en forma legal o a los costos formales.

Portabilidad
Posibilidad de ejecutar las aplicaciones desarrolladas en cualquier sistema operativo y/o máquina del mercado.

Propietario
Dueño de una aplicación o software y en la cual no tiene limitaciones.

R

Registro
Conjunto de datos pertenecientes a una misma entidad. El registro consta de campos, cada campo tiene una longitud definida, por lo tanto los registros son de longitud fija.

Rendimiento
Beneficio, producto o utilidad que produce algo.

Requerimiento
Característica que se desea que posea un sistema o un software.

RSA
Es uno de los primeros esquemas de clave pública. El algoritmo está basado en la dificultad para realizar factorizaciones de números largos. RSA es un bloque cifrador en el cual el texto original y el texto cifrado son enteros entre 0 y n – 1 para cualquier n.

S

Seguridad
Aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial.

Seguridad informática
Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Servicio de seguridad
Es aquel que mejora la seguridad de un sistema de información y el flujo de la información de una organización.

Sistema biométrico
Los cuales identifican a una persona por sus rasgos físicos o de comportamiento intrínsecos.

Sistema Manejador de Bases de Datos (DBMS)
Es un conjunto de programas que controla la organización, almacenamiento, recuperación, seguridad e integridad de los datos en una base haciendo uso de algún modelo de datos.

T

Tablas
Dentro del enfoque relacional es conocida como entidad de dos dimensiones (columna, renglón). Es una estructura de almacenamiento bidimensional, formada por tuplas (registros, renglón) y atributos (columnas, campos).

Tecnología biométrica
Utiliza principalmente el reconocimiento de rasgos. Examina rostros, huellas digitales y otras características físicas para confirmar las identidades individuales.

Tipos de Relaciones
Las relaciones sirven para poder utilizar datos procedentes de otras tablas como si formaran parte de la tabla en la que se esté trabajando.

U

Usuario
Persona que posee el derecho de utilizar un sistema que no es de su propiedad con ciertas limitaciones.

V

Vulnerabilidad
Es una debilidad que puede ser explotada para violar la seguridad.

BIBLIOGRAFÍA

1. Apuntes de seguridad informática de M.C. Ma. Jaquelina López Barrientos.

2. R. Elmasri, S.B. Navathe ***"Sistemas de Bases de Datos. Conceptos fundamentales"*** , Segunda Edición, Addison-Wesley Iberoamericana, 1997.Tercera Edición en 1999 (en inglés, por Addison-Wesley)

3. Pfleeger S., ***"Ingeniería de Software, Teoría y Práctica"*** - Primera Edición - Editorial Prentice Hall - 2002.

4. http://news.bbc.co.uk/hi/spanish/international/newsid_6089000/6089152.stm

5. http://www.mygnet.net/articulos/seguridad/763/index.php

6. https://pid.dsic.upv.es/C1/Material/Documentos%20Disponibles/Introducci%C3%B3n%20Proceso%20de%20Desarrollo%20de%20SW.doc

7. http://www.syscom.com.mx/Productos/Monitoreo_Seguridad/lectoras_tarjetas_teclados.htm

8. http://www.kimaldi.com/productos/sistemas_biometricos/control_de_accesos_biometrico/terminal_biometrico_de_control_de_acceso_y_presencia_kimaldi_kreta2_fp

9. http://www.vivotek.com/products_ip7131.htm