UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES "ACATLÁN"

ADMINISTRACIÓN DE BASES DE DATOS DEL DEPARTAMENTO DE SISTEMAS DE INFORMACIÓN DE LA FES ACATLÁN

M E M O R I A D E D E S E M P E Ñ O
QUE PARA OBTENER EL TÍTULO DE:
MATEMÁTICAS APLICADAS Y COMPUTACIÓN
P R E S E N T A:
S E R E N O G A R C I A O C T A V I O

ASESOR: Mtra. María del Carmen Gonzalez Videgaray

UNAM
CAMPUS ACATLAN

Naucalpan, Edo. de México Noviembre 2004

Agradecimientos

A mis padres

Por la paciencia que me han tenido, por cuidarme, preocuparse por mi, permitirme estudiar una carrera, por aconsejarme y servirme de guía en todos los momentos de mi vida, se los agradezco y creo que nunca podré agradecerles lo suficiente.

A mis hermanos

Por lo que me han enseñado, por los momentos que hemos pasado juntos y por recordarme el camino a seguir cuando lo había olvidado. Gracias y espero no defraudarlos.

A los amigos que he tenido

Por darme su comprensión y escucharme en mis dudas, por brindarme su amistad sin esperar nada a cambio y haberme permitido pasar un tiempo de nuestras vidas juntos.

A dos amigas que nunca olvidare

Aunque pase mucho tiempo estas dos amigas siempre tendrán un lugar especial en mi corazón Rosa por haberme dado ánimos cuando ya no podía continuar y a Margarita Mora por haber compartido su amistad conmigo, creó que será muy difícil encontrar a dos personas como ellas nuevamente, espero que se encuentren bien.

A mis compañeros de trabajo

En especial a mi líder de proyecto Rosario Rivera por su paciencia y a Sheidy por la paciencia que me tuvo y por lo que aprendí de ella.

A los buenos profesores que he tenido

Les quiero agradecer también a los profesores de los cuales he aprendido tanto, espero no haberlos molestado mucho con mis dudas, pero no era con el fin de molestarlos.

A la UNAM

Por darme la oportunidad de formar parte de su comunidad de estudiantes.

ÍNDICE

4. DISEÑO DEL SISTEMA

Introducción

Entre los diversos retos de las organizaciones actuales se encuentra manejar adecuadamente la gran cantidad de información que se genera día con día. Por lo cuál los sistemas de información basados en computadoras se han vuelto el corazón de las actividades cotidianas, pues a partir de su aparición se ha logrado almacenar, procesar y transportar la información de una manera inimaginable en otros tiempos. Aunque este avance trae consigo el problema de la seguridad informática.

La falta de medidas de seguridad informática es un problema del cual la mayoría de las empresas desconocen su magnitud, pues generalmente no se invierte ni el tiempo ni el dinero necesarios para prevenir el daño o la pérdida de la información que, como se ha mencionado es uno de los recursos más importantes que se tienen en una organización.

En la presente memoria de desempeño profesional el autor pretende mostrar su experiencia al realizar un sistema de seguridad, cuya función es la de crear y administrar cuentas de usuario, para así determinar diversos niveles de acceso a la información de los sistemas desarrollados por el Departamento de Sistemas de Información. El proyecto lleva el nombre de SISECU (**Si**stema de **Se**guridad y Control de Usuarios) y se realizó en Departamento de Sistemas de Información con lo cual se garantiza la seguridad del proyecto Atenea de la Facultad de Estudios Superiores Acatlán.

El proyecto SISECU surge a partir de los objetivos de actualizar y optimizar los sistemas de información desarrollados por el DSI (Departamento de Sistemas de Información) de la ENEP Acatlán, dicho proyecto además de actualizar los sistemas de un ambiente DOS a un ambiente Windows para aprovechar las ventajas de un ambiente gráfico,

pretenden utilizar las capacidades de un manejador de base de datos relacional para que la información sea mas confiable actualizada y segura.

Resumen de los capítulos que forman este trabajo:

Capítulo 1 Se da una introducción acerca de la importancia que tiene la información para las instituciones en la actualidad, y cómo el uso de las computadoras para procesar la información ha traído consigo un nuevo tipo de delincuencia: la "delincuencia informática".Lo que hace necesario que se empleen diversas medidas de seguridad para salvaguardar la información de una organización.

Capítulo 2 Se explican las razones por las cuales el sistema que actualmente se usa para llevar el control del personal académico de la FES Acatlán se debe remplazar, originando la creación de nuevos sistemas de información entre los que se encuentra el sistema de seguridad y control de usuarios (SISECU).

Capítulo 3 Se da una introducción al manejador de base de datos que se eligió para manipular la información referente al personal académico, dicho manejador es SQL Server. Además de mencionar el porqué dicho manejador es adecuado para almacenar la información.

Capítulo 4 Se explican los procesos que realiza el sistema, la información que almacena y manipula para funcionar y la manera de utilizar el sistema para crear y administrar las cuentas de los usuarios.

CAPÍTULO I

SEGURIDAD INFORMÁTICA

1.1 La computadora en las actividades diarias

Las computadoras son herramientas que procesan datos siguiendo instrucciones almacenadas en programas, y además tienen la capacidad de almacenar esos datos a alta velocidad, El uso que se puede dar a una computadora es muy amplio, ya que puede emplearse con fines meramente administrativos como realizar informes, llevar inventarios, etc. Hasta realizar aplicaciones multimedia (cualquier combinación de texto, gráficos, sonido, animación y vídeo que llega a nosotros por medio de una computadora) dichas características hacen que cada día más personas estén interesadas en aprender lo relativo a las computadoras.

En los inicios de la computación, las computadoras eran tan grandes y complejas que sólo las empresas importantes podían costear su operación con ayuda de personal especializado, lo cual era sumamente costoso .

A partir de los años 80 gracias al avance tecnológico de la miniaturización aparece el microprocesador, circuito integrado que rige las funciones fundamentales del ordenador, con lo que el tamaño de las computadoras tiende a ser cada vez menor, dando lugar a la aparición del ordenador personal cuyo uso se ha vuelto común.

Además, con la aparición de sistemas operativos fáciles de utilizar para los usuarios el aprender a usar una computadora se ha vuelto una labor más sencilla, logrando que personas sin muchos conocimientos al respecto puedan emplear una computadora de una manera eficaz.

Con el abaratamiento de las computadoras y de los medios de almacenamiento hoy en día, la mayor parte de los datos de una empresa están almacenados en los equipos informáticos. Por lo que cualquier problema en los sistemas de información repercute instantáneamente en la totalidad de la empresa y afecta al funcionamiento normal de la misma.

1.2 Nociones generales de seguridad

La Seguridad es una necesidad básica en algunos ámbitos. Pues desde el principio de la aparición del hombre como tal sobre la tierra, este ha tenido que adoptar una serie de precauciones y medidas para garantizar la preservación de la vida y las posesiones, tanto a nivel individual como colectivo.

La preocupación del hombre por protegerse ha dado origen a diversas invenciones. Cerraduras, puertas resistentes, ventanas selladas, trampas, cajas fuertes, sistemas de alarma y escudos, son conocidos y usados desde el principio de la civilización.

Es importante saber lo que la palabra seguridad representa, por ejemplo: El Diccionario Esencial de la Real Academia Española nos dice que seguridad es:

"Cualidad o estado de seguro.
Dicho de un mecanismo: Que asegura algún buen funcionamiento, precaviendo que este falle, se frustre o se violente. "[1]

Un concepto común sobre la seguridad es que esta se trata de la protección de bienes y personas por diversos medios, posteriormente conoceremos las medidas de seguridad que deben tenerse en cuenta para proteger la información de una institución.

[1] Diccionario Esencial de la Real Academia Española, pag. 1000

1.3 Importancia de la Información

Cuando se habla de la función informática dentro de una organización generalmente se tiende a hablar de tecnología nueva, de nuevas aplicaciones, nuevos dispositivos de hardware, nuevas formas de elaborar reportes o consultas, etc. Sin embargo se suele pasar por alto o se tiene muy implícita la base que hace posible la existencia de los anteriores elementos. Esta base es la información.

Es importante conocer el significado de la información dentro la función informática. Así, debemos saber que la información está compuesta de datos, es decir los datos son "la unidad mínima que compone cierta información." [2]

La información es definida como la "Agregación de datos que tiene un significado específico más allá de cada uno de éstos." [3]

Y tiene un sentido particular según el criterio de quien los interpreta.

Ejemplo: 2, 0, 0 y 4 son datos; y 2004 es una información, si se refiere al año.

---

[2] Fernández Calvo Rafael Glosario básico inglés-español para usuarios de Internet 4ª edición. Ed. Asociación de técnicos de informática, 2002.

[3] Fernández Calvo Rafael Glosario básico inglés-español para usuarios de Internet 4ª edición. Ed. Asociación de técnicos de informática, 2002.

Es importante conocer, que cuando la información es procesada por medio de sistemas de información, tiene diversas características, entre las que destaca:

- Se encuentra almacenada y procesada en computadoras. Para almacenar la información se pueden emplear diversos medios desde un archivo de texto, una hoja de Excel, hasta una base de datos, el escoger entre uno ú otro medio depende de las necesidades especificas que se tienen en el momento y de la tecnología disponible.

- La información puede ser confidencial para algunas personas o para otras instituciones. Existe información que puede ser pública: es decir puede ser consultada por cualquier persona; y también existe información privada; que sólo puede ser consultada y manipulada por un grupo de personas que cuentan con acceso a ella.

- La información está sujeta a ser destruida. Las compañías que quedan incapacitadas de utilizar sus sistemas de información pueden sufrir perdidas importantes e incluso fatales. Por lo que es preciso contar con medidas de prevención ante distintos riesgos, que van desde catástrofes naturales (incendios, inundaciones, etc.) hasta fallas de hardware o software, además de la destrucción accidental o intencionada de la información (descompostura de una computadora, destrucción de archivos, etc.).

- La información puede estar sujeta a robos, sabotaje o fraudes. El plagio de datos por medio del copiado no representa una desaparición física, por lo que, este tipo de acciones son difíciles de descubrir. También hay que tener especial cuidado en evitar la sustracción de los respaldos de la información, como pueden ser respaldos en CD o en discos duros. El fraude también constituye un peligro para cualquier organización, el fraude consiste principalmente en la desviación de fondos y la manipulación de información con fines personales.

Los primeros puntos nos indican que la información esta centralizada y que puede tener un alto valor y los últimos puntos nos indican que se puede provocar la destrucción total o parcial de la información, lo que afecta directamente su disponibilidad, originando retrasos que pueden resultar de un alto costo para una organización.

1.4 Delincuencia informática

El aumento en el uso de las computadoras y aplicaciones, el desarrollo de tecnologías que permiten el almacenamiento, procesamiento y transmisión de grandes cantidades de información , no sólo ha revolucionado los hábitos de trabajo y comunicación de las personas, sino que ha traído consigo un nuevo tipo de delincuencia que se ha llamado "delincuencia informática".

A continuación se muestran partes de textos que estiman la magnitud del problema de la delincuencia informática.

"Las estadísticas muestran que en Estados Unidos la delincuencia computacional es una de las actividades ilícitas más productivas, si se tiene en cuenta que los robos de bancos producen un promedio de 10,000 dólares a sus autores; las defraudaciones, 19,000 dólares y los crímenes computacionales 450,000 dólares. Según datos del F.B.I., sólo el 1% de las actividades computacionales ilícitas se detectan a tiempo, mientras sólo el 7% son denunciadas a las autoridades. Aunque el Stanford Research Institute estima en más de tres mil millones de dólares las ganancias anuales de los delitos computacionales, es difícil obtener cifras confiables, pues la mayoría de las víctimas prefiere guardar tanta discreción como sus atacantes. Pues en muchas ocasiones, las víctimas de fraude optan por resignarse a las pérdidas para evitar la posibilidad de represalias aún mayores en contra suya."[4]

[4] Graton, Pierre, Protección informática : en datos y programas; en gestión y operación; en equipos y redes; en Internet. Editorial Trillas, 1998. pag. 33.

Se considera que los delitos informáticos tienen una tendencia a aumentar, por lo que la seguridad de los sistemas de información se ha convertido en un asunto de alta prioridad para las empresas, como lo muestra el siguiente artículo de Internet..

"Los delitos informáticos en el 2001 aumentaron un 10% en Europa,..., según un estudio elaborado por la consultora IDC por encargo de la empresa EDS, especialista en soluciones tecnológicas para entornos empresariales.
En España, según el citado estudio, apenas la mitad de las compañías afirma haber puesto en marcha un plan de continuidad del negocio para casos de crisis, si bien el 90,2% considera que sus sistemas de Tecnologías de la Información (TI) son lo suficientemente seguros como para garantizar la continuación de los servicios que presta.

Según la gerente de Seguridad de EDS para España, "el tema ha dejado de ser exclusivamente una cuestión de departamento de sistemas para convertirse en un asunto estratégico", si bien Javier Atencia, experto en seguridad informática y director del programa de televisión 'Mundo Digital', dice que sólo un 10% de las empresas españolas "tienen algún tipo de seguridad informática".

El informe encargado por EDS (realizado entre 350 compañías de España, Francia, Reino Unido, Alemania, Italia y Sudáfrica de los sectores industrial, comercial y de servicios) revela que el 35,2% de las empresas entrevistadas asegura que durante 2001 tuvo problemas de delincuencia informática. De entre ellas, el 45,9% declara haber sufrido entre dos y cinco ataques (en España este indicador aumenta hasta el 56,5%) y el 15% asegura que sus sistemas informáticos han sido asaltados en más de diez ocasiones durante el último año.

Para Carmen García, gerente de Seguridad de EDS para España, Portugal e Italia, "la realidad está haciendo que la seguridad de los sistemas de información se convierta en un asunto de alta prioridad para los líderes de los gobiernos y las empresas de todos los países".

Por otro lado, entre las causas más frecuentes de los desastres en los sistemas de Tecnologías de la Información destacan los ataques por virus informáticos (78,5%), errores por parte de los usuarios (64,2%), caídas del sistema (37,5%), fraude interno y vandalismo (34%)."[5]

Los delitos de esta naturaleza son difíciles de probar, por lo que aunque se tengan sospechosos no siempre se puede comprobar su participación, como se aprecia en el siguiente párrafo de un artículo de Internet.

"En España, uno de los primeros casos en los que los Cuerpos de Seguridad del Estado intervinieron contra el delito de intrusión informática, fue el 2 de abril de 1998 en el que la Unidad de Delitos Informáticos de la Guardia Civil detuvo a 3 personas e imputó a otras 10 del grupo "Hispahack" como autores de la entrada sin autorización en diversos sistemas informáticos, entre ellos el de la NASA, la Universidad de Oxford o la Universidad Politécnica de Cataluña. Finalmente, solo uno de los acusados fue llevado a juicio y posteriormente absuelto porque no fue probado que el acusado participase en la entrada ilegal, obtención y transferencia de datos."[6]

En el mismo artículo se habla acerca de lo difícil que es cuantificar los delitos informáticos, y de los delitos más denunciados en España.

[5] http://www.belt.es/noticias/2002/02_abril/01_05/04_ataqs_informatics.htm
[6] http://www.69neuronas.com/articulos/delitos/delitos1.pdf

Estadísticas y Delitos en España durante el año 2002

"El presidente del Observatorio Español de Internet, Francisco Canals, presentó un informe en que se calculaba que aproximadamente 24000 españoles habían sufrido un fraude o estafa a través de Internet en el año 2002, aunque esta cifra es difícil cuantificarla con precisión pues los afectados raramente denuncian estos hechos en comisaría.

La mayoría de las denuncias presentadas en las comisarías españolas se refieren a portales o páginas dedicadas a la pornografía infantil.

La Guardia Civil durante el año 2002 recibió poco más de 9.000 denuncias por delitos informáticos, de los que 7.820 estaban relacionadas con la pornografía infantil, 773 por fraudes y 443 por violación de sistemas de seguridad realizadas por intrusos."[7]

[7] http://www.69neuronas.com/articulos/delitos/delitos1.pdf

1.5 Seguridad de la información

La seguridad de la información tiene como objetivo proteger los recursos de las organizaciones como son la información y el equipo, contra los diferentes delitos a los que pueden estar expuestos como el robo, la destrucción o modificación de información, fraude, etc., la seguridad de la información puede definirse como "el nombre genérico para el conjunto de herramientas diseñadas para proteger los datos."[8]

La seguridad de la información busca proteger las siguientes propiedades de la información.

Confidencialidad: Es la condición que asegura que la información no pueda ser descubierta o estar disponible por o para personas, entidades o procesos no autorizados. La información debe ser usada y manipulada únicamente por quienes tienen el derecho o la autoridad de hacerlo.

Integridad: La integridad de la información es la condición de seguridad que garantiza que la información es modificada, creada o borrada, sólo por el personal autorizado. Es decir, se busca que la información no este propensa a alteraciones no deseadas.

[8] Rodríguez Luis Angel, Seguridad de la información en sistemas de cómputo. Ventura ediciones, s.a. de c.v. pag.12

Un ejemplo de ataque a la Integridad es la modificación no autorizada de las calificaciones en un sistema escolar, o la modificación no autorizada de una cuenta bancaria. Para lograr esto las medidas de seguridad implementadas en la organización se debe eliminar toda posibilidad que los datos puedan ser modificados por intrusos.

Disponibilidad: Es la capacidad de la información de estar en el lugar, momento y forma en que es requerida por el usuario autorizado. Situación que se produce cuando se puede acceder a un Sistema de Información en un periodo de tiempo considerado como aceptable.

El disponer de la información después del momento necesario puede equivaler a la no disponibilidad. Otro caso grave es la no disponibilidad absoluta, por haberse producido algún desastre. En ese caso a medida que pasa el tiempo el impacto será mayor, hasta llegar a suponer la no continuidad de la entidad,

Conservación: Es la capacidad de evitar que la información almacenada sufra algún daño y por consiguiente su destrucción.

1.6 Medidas de seguridad

Hay diversas medidas de seguridad que deben tenerse en cuenta para que la información de una organización se encuentre segura, las cuales son:

Políticas y procedimientos: La falta de políticas y procedimientos en seguridad es uno de los problemas que enfrentan las empresas hoy día en lo que se refiere a la protección de su información frente a peligros externos e internos. Pues siempre existe la posibilidad de que existan personas deshonestas dentro de una organización que podrían, hacer mal uso de la información, sin olvidar la existencia de atacantes externos.

La políticas de seguridad son esencialmente orientaciones e instrucciones que indican cómo manejar los asuntos de seguridad y forman la base de un plan para la implantación efectiva de medidas de protección tales como: identificación y control de acceso, respaldo de datos, planes de contingencia y detección de intrusos.

Si bien las políticas varían considerablemente según el tipo de organización de que se trate, en general incluyen declaraciones generales sobre metas, objetivos, comportamiento y responsabilidades de los empleados en relación a las violaciones de seguridad. A menudo las políticas van acompañadas de instrucciones y procedimientos, por ejemplo procedimientos de contratación, abandono o transferencia de lugar de trabajo, etc..

Seguridad física: Su principal objetivo es proteger los recursos contra el robo o la destrucción accidental o intencional, incluye los controles de acceso al centro de cómputo, por ejemplo, por medio de tarjetas de identificación, condiciones del medio ambiente como temperatura, equipo contra incendios, seguridad de las computadoras, por ejemplo, control de acceso a la zona de servidores y seguridad de los respaldos de la información.

Seguridad de las comunicaciones: Existen diversas amenazas a la seguridad de las comunicaciones como la intercepción de los datos para realizar un fraude ó daño a los medios físicos de transmisión, como la destrucción de cables, etc. Se pueden realizar diversas medidas de seguridad para minimizar las amenazas como encriptar la información transferida, instalar el servidor en un lugar seguro y bien vigilado, revisar regularmente la red, etc. "Un fraude en las comunicaciones de datos representa la alteración, modificación o intercepción de mensajes con fines de lucro, mediante el uso de un sistema de comunicaciones en línea."[9]

Seguridad lógica: consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo" [10], es en este punto en donde se especifica el tipo de acceso que puede tener una persona o usuario de un sistema de información, por ejemplo se deben de especificar los privilegios para los programadores, usuarios, analistas, de acuerdo a sus funciones dentro de la organización, conjuntamente se realizan otras acciones como asignación de passwords, encriptación de archivos, restricciones de tiempo en el uso de los sistemas, etc. Cabe mencionar que se debe determinar el sistema operativo seguro para almacenar la información, un manejador de

[9] Graton, Pierre, Protección informática : en datos y programas; en gestión y operación; en equipos y redes; en Internet. Editorial Trillas, 1998. pag. 174
[10] http://www.internet-solutions.com.co/seguridadfisicaylogic.html

base de datos en donde residirá la información que cumpla con los requerimientos de seguridad que tenemos especificados y la realización de las copias de seguridad de la información.

Plan de contingencia: También llamado plan de recuperación de desastres o plan de emergencia, es una guía para la restauración rápida y organizada de las operaciones de computo después un desastre, el plan de contingencia debe ser elaborado de acuerdo con las necesidades de la organización.

Cada uno de estos puntos es independiente de los demás. Sin embargo, para aumentar la seguridad de la información es necesario que se trabaje en todos los aspectos, ya que no servirá de mucho tener una buena seguridad lógica si cualquiera puede acceder físicamente a los servidores y modificar la información, o acceder a los respaldos de la información.

El conservar adecuadamente la información no es una tarea fácil, ya que la información puede ser destruida total o parcialmente por diversas causas como catástrofes naturales destacando incendios, inundaciones, terremotos, etc, fallas de hardware o software, además de la destrucción accidental o intencionada de la información (descompostura de una computadora, destrucción de archivos, sabotaje, etc.).

El Sistema de SISECU ayudará a mejorar la seguridad lógica de los sistemas del DSI, aunque hay muchas consideraciones a tener en cuenta en su diseño.

CAPÍTULO II

ANÁLISIS DEL PROBLEMA

2.1 Facultad de Estudios Superiores Acatlán

Debido a que el sistema SISECU se realizó para la Facultad de Estudios Superiores Acatlán, en el Departamento de Sistemas de Información (DSI), con el objeto de administrar la seguridad de diversos sistemas desarrollados por el DSI, los cuales forman parte de un proyecto mayor denominado ATENEA, es importante conocer la Institución, así como determinar los diversos tipos de usuarios que debe crear y administrar la aplicación de seguridad.

La Facultad de Estudios Superiores Acatlán se encuentra ubicada en Av. Alcanfores y San Juan Totoltepec s/n, Santa Cruz Acatlán, Naucalpan Edo. de México, C.P. 53150.

El objetivo de la FES Acatlán es impartir educación superior a nivel licenciatura en las especialidades de: "Derecho, Comunicación, Matemáticas Aplicadas y Computación, Relaciones Internacionales, Arquitectura, Ciencias Políticas y Administración Pública, Diseño Gráfico, Pedagogía, Economía, Actuaría, Sociología, Ingeniería Civil, Historia, Filosofía, Enseñanza de Inglés y Lengua y Literatura Hispánicas, las cuales se ubican dentro de tres áreas de conocimiento: de las Ciencias Físico Matemáticas y de las Ingenierías; de las Ciencias Sociales; y de las Humanidades y las Artes."[16] Así como impartir estudios de posgrado y realizar diversos proyectos de investigación.

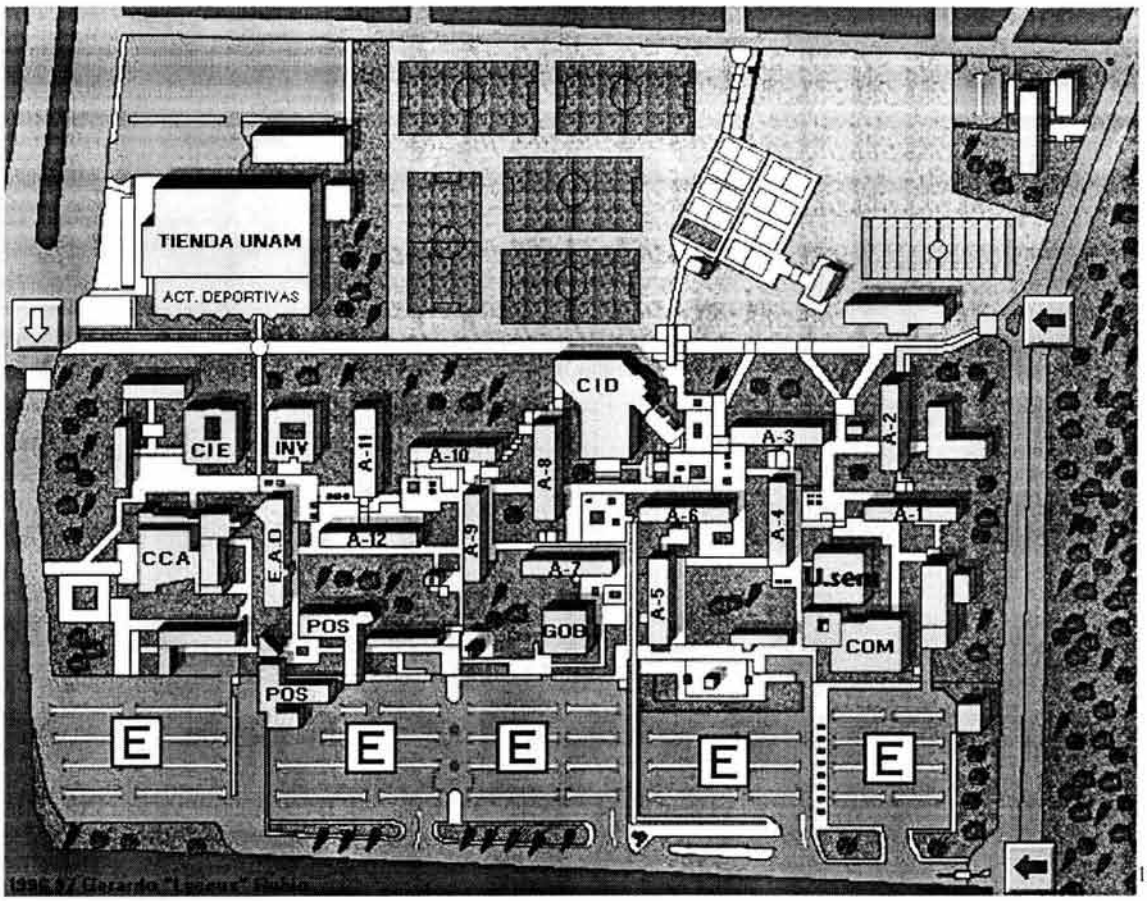
[16] Notifes Acatlán boletín informativo de la Facultad de Estudios Superiores Acatlán pag 4

Es importante tener una idea de cómo está compuesta físicamente la ENEP Acatlán, pues en todos los edificios en los que labora algún funcionario que cuente con acceso a la red de Acatlán se debe instalar el sistema SISECU, para permitir trabajar con el resto de los sistemas que forman el proyecto ATENEA.

"Acatlán está construida sobre una superficie de 30 hectáreas, con una planta física de 30 edificios que albergan un conjunto de tres edificios para Posgrado, uno para investigación y tres para 29 talleres y laboratorios; 268 aulas; construcciones especiales para los centros de Información y Documentación, de Enseñanza de Idiomas y de Desarrollo Tecnológico, la Unidad de Seminarios, el Centro Cultural Acatlán y cuatro auditorios que en su conjunto tienen un aforo de 1,500 usuarios." [17]

[17] Notifes Acatlán boletín informativo de la Facultad de Estudios Superiores Acatlán pag 3

A continuación se muestra un plano de la FES Acatlán.



[18]

[18] http://www.acatlan.unam.mx/campus/mapa/

2.2 Planteamiento del problema

Actualmente se encuentra en uso el sistema SISPA (Sistema de Personal Académico) dicho sistema se encuentra formado a su vez por otros sistemas que se encargan de administrar todo lo relacionado a la planta docente de la ENEP Acatlán, por ejemplo: realizar la captura de lo relacionado a la aplicación de los exámenes extraordinarios, como asignación de profesor, salón, etc., llevar el control de las faltas de los profesores, sacar reportes, etc., dichos sistemas están hecho para ejecutarse bajo un ambiente DOS. Los sistemas han presentado diversos problemas:

- El sistema no permite el uso del ratón, por lo que su uso no resulta fácil para muchos usuarios acostumbrados a un ambiente Windows.
- Se tuvieron algunos conflictos con el uso de la información de los sistemas que forman a SISPA, por lo que se añadieron funciones de auditoria.
- Las tablas que almacenan los datos llegan a corromperse y es necesario indexar los archivos que contienen la información periódicamente.
- El sistema SISPA no puede ejecutarse en sistemas operativos posteriores a Windows 98, por ejemplo Windows 2000, Windows XP, etc.
- El sistema SISPA está por superar su tiempo de vida útil, ya que se requiere que el sistema realice nuevas funciones y por las razones anteriormente expuestas no se considera conveniente modificar el código del sistema.

2.3 Planteamiento de la solución

2.3.1 Propuesta de solución

Se pretende la actualización y optimización de los sistemas de información de la Escuela, por lo que se propuso el proyecto específico "Sistemas Integrados de Información de Acatlán".

Objetivo general del proyecto Atenea

"Contar con bases de datos distribuidas y compartidas; actualizadas y confiables, que permitan a los usuarios autorizados conocer de forma eficiente los recursos y funcionamiento de la Escuela, además de agilizar y facilitar todo tipo de trámites y servicios."[19]

Para cumplir con el objetivo general propuesto se ha determinado que la mejor opción no es modificar los sistemas que están en uso actualmente, ya que el problema de la compatibilidad con las nuevas versiones de Windows persistiría, por lo que se pretende crear nuevos sistemas de información capaces de administrar todo lo relacionado a la planta docente de la FES Acatlán, dicho proyecto recibe el nombre de proyecto ATENEA. A continuación se menciona el objetivo de los sistemas que forman parte del proyecto Atenea en su etapa inicial, pues se pretende desarrollar más sistemas en etapas posteriores del proyecto.

A continuación se muestran los objetivos de los sistemas que forman parte del proyecto ATENEA en su primer etapa:

---

[19] Manual de proyecto Atenea año 2003 pag. 1.

Adscripciones

Administrar las adscripciones de la FES Acatlán de una forma cómoda, sencilla y eficiente la cual impactará de manera automática a los sistemas que requieran de esta información.

Extraordinarios

Realizar la captura de los exámenes extraordinarios y las modificaciones que éstos presentan durante el periodo de entrega a Secretaría General.

Grupos-materia

Realizar la captura de la planta docente (horas curriculares frente a grupo) y las modificaciones que ésta presenta durante el semestre en cuestión.

Realizar la captura del personal que tiene horas de apoyo académico (no frente a grupo) en cualquier Entidad de la Escuela.

Realizar la captura de los profesores que tienen horas de formación complementaria (frente a grupo) en las Entidades respectivas de la Escuela.

Inasistencias

Realizar la impresión de los tarjetones Tipo A, B y C que genere un profesor o trabajador académico-administrativo durante el periodo referido y capturar las inasistencias que presente en el mismo período de tiempo.

Profesor

Realizar la captura de los datos personales, domicilio, historial académica, categorías académicas, programa e informe de trabajo; generados por el profesor que se encuentre adscrito a cualquier Entidad de la Escuela, ya sea por contratación a través de nómina o por honorarios.

Propuestas de contratación

Realizar la captura de las propuestas de contratación de los profesores que cobrarán a través de nómina en las diferentes Entidades de la Escuela.

Seguridad

Administrar las funciones y responsabilidades de acceso a los sistemas que sean desarrollados por el Departamento de Sistemas. [20]

2.3.2 Objetivos del Sistema de Seguridad y Control de Usuarios

Los objetivos del sistema de Seguridad son: Administrar las diferentes bases de datos que se encuentran en el servidor, permitiendo el acceso a la información de diferentes bases de datos solamente a los usuarios autorizados.

Administrar los privilegios que los usuarios tienen en los diferentes sistemas que forman el proyecto ATENEA, para dar acceso en cada sistema a los procesos que tiene permitido el usuario.

[20] Manual de proyecto Atenea año 2003 pag. 1-2

Alcance del sistema

El sistema SISECU tiene la propiedad de identificar y dar acceso a los usuarios que ingresen a los diferentes sistemas que conforman el proyecto Atenea, el sistema será usado por los lideres de proyecto del DSI, ya que cada sistema desarrollado por el DSI para formar parte del proyecto ATENEA debe compartir la información que se tiene para evitar la duplicidad de la información, por lo que cada líder de proyecto usará el proyecto SISECU para administrar los usuarios y los permisos que estos tienen en los sistemas. El sistema realiza las siguientes tareas.

- Servir a los lideres de proyecto del DSI como una herramienta que permite la comunicación entre sistemas.
- Realizar auditorias de los procesos realizados.
- Asignar y remover privilegios para permitir el acceso a los sistemas.
- Llevar un registro de los accesos de los usuarios a los sistemas.
- Asignar y modificar las contraseñas de los usuarios.
- Administrar los roles de las aplicaciones.

2.3.3 Equipo asignado al proyecto

El jefe del departamento de sistemas de información decidió que el equipo al que pertenezco sería el encargado de realizar un sistema que pueda administrar las bases de datos del DSI, las cuentas de los usuarios que se conectan a dichas bases de datos y acceder a las diferentes aplicaciones a las que tenga acceso el usuario.

El proyecto recibió el nombre de SISECU (**Si**stema de **Se**guridad y control de Usuarios). Se eligió como herramienta para desarrollar dicho sistema el lenguaje de programación Delphi.

Delphi es una herramienta de desarrollo de programas que permite la rápida creación de aplicaciones para Windows 3.x, Windows95, Windows98, Windows2000, Windows Millenium, Windows NT. Además de que en otros proyectos había tenido la oportunidad de utilizar Delphi y determiné que con este software se podía desarrollar el sistema sin necesidad de utilizar herramientas externas, como depuradores o software para realizar reportes.

2.3.4 Conformación del equipo de trabajo.

Para llevar a cabo este proyecto se dividieron las actividades a realizar de la siguiente manera:

Laura Silva Fuertes: Jefa del Departamento de Sistemas de Información

- Creación del logotipo del sistema.
- Presentación del proyecto ante las autoridades.

Rosario Rivera Aguilar: Líder de proyecto

- Revisión y aprobación del diseño de las pantallas del sistema.
- Revisión de avances del sistema.
- Aprobación del diseño de la base de datos.

Octavio Sereno García: Analista-programador

- Llevar a cabo el análisis del sistema.
- Desarrollo del prototipo del sistema.
- Diseño de la base de datos.
- Presentación ante los distintos líderes de proyecto del sistema SISECU.
- Análisis y diseño de la base de datos.
- Diseño de las pantallas del sistema.
- Desarrollo del código del sistema.
- Capacitación de los líderes de proyecto del DSI en el uso del sistema SISECU.

María de Lourdes Trejo: Analista

- Prueba de los prototipos del sistema, para buscar errores.

CAPÍTULO III

MANEJO DE LA INFORMACIÓN

3.1 Especificaciones para usar el sistema

Para realizar un sistema es necesario conocer las necesidades de los usuarios, por lo que se realizaron diversas exposiciones de los prototipos de sistema SISECU a los lideres de proyecto del DSI, en las cuales se determinó la manera en que se debían de administrar las cuentas de los usuarios, la cuál es mediante la creación de un nombre de usuario y contraseña únicos para cada usuario y la asignación de privilegios para trabajar con los sistemas y se modificó la apariencia final del sistema, después de esto se procedió a investigar acerca de las características que debe tener un equipo de cómputo para poder instalar el sistema y la opción más conveniente para almacenar la información.

Las especificaciones técnicas mínimas para utilizar el sistema son:

- ✓ Procesador 486 DX a 80 Mhz
- ✓ 50 MB libres en disco duro
- ✓ 16 MB en memoria RAM

Se considera como recomendable que el equipo cuente con:

- ✓ Procesador Pentium 166 Mhz
- ✓ 50 MB libres en disco duro
- ✓ 32 MB en memoria RAM

Después de que el DSI realizó un censo del equipo de cómputo con el que cuentan las órganos de la FES Acatlán se encontró que: todos los órganos cuentan con al menos una computadora que supera las especificaciones recomendables. Los líderes del DSI también cuentan con al menos una computadora que supera las especificaciones recomendables.

Para la realización del proyecto ATENEA se determinó que el almacenamiento de la información en archivos ya no resulta conveniente y que la mejor opción para almacenar los datos es emplear un sistema manejador de base de datos relacional. Existen diversas herramientas que nos permiten desarrollar y administrar bases de datos relacionales de entre ellas se escogió SQL Server. Pues además de ser el mejor manejador de base de datos relacional que se ejecuta en Windows NT (el sistema operativo del servidor) es fácil de utilizar para construir y administrar bases de datos relacionales.

3.2 SQL Server

A continuación se da una breve introducción del sistema manejador de base de datos relacional SQL Server y de la manera como administra los usuarios, SQL Server 2000 es la versión que se escogió para crear y administrar las diversas bases de datos y las cuentas de usuarios que requieren los sistemas del DSI.

SQL Server es un sistema manejador de Base de Datos relacional (RDBMS) que trabaja con la arquitectura Cliente / Servidor y utiliza el lenguaje SQL para agregar, modificar o eliminar información. SQL Server está diseñado para admitir grandes volúmenes de procesamiento de transacciones (como el registro del inventario en un almacén, la contabilidad o facturación, etc.).

Base de datos Relacional

Una base de datos relacional es una base de datos en donde todos los datos visibles al usuario están organizados estrictamente como tablas de valores, y en donde todas las operaciones de la base de datos operan sobre estas tablas.

Tablas

Las tablas son el corazón de una base de datos relacional. Las tablas son una colección de datos sobre una entidad (persona, lugar, cosa, etc.) específica distribuidos en formas de filas (también llamadas registros) y columnas (también llamadas campos).

3.2.1 Arquitectura Cliente / Servidor

Para acceder a una base de datos que utiliza esta arquitectura las computadoras personales están combinadas en una red de área local junto con el servidor de base de datos (generalmente ordenadores de gran potencia) que almacenan las bases de datos. Los manejadores de Bases de Datos diseñados para emplear esta arquitectura permiten que varios usuarios hagan operaciones sobre las bases de datos al mismo tiempo, por ejemplo un usuario puede hacer una consulta al mismo tiempo que otro, situado en un lugar diferente, está introduciendo datos en la base de datos, tal como se aprecia en la Figura 2.1.

Figura 2.1 El modelo cliente /servidor

3.2.2 Funciones de un RDBMS

El RDBMS o sistema administrador de bases de datos relacionales se encarga entre otras cosas de:

- Mantener las integridad de la información en la Base de Datos.
- Asegurarse de que la información es almacenada correctamente, es decir, que las reglas que definen las relaciones entre los datos no sean violadas.
- Recuperar toda la información en un punto conocido en caso de que el sistema falle.

Redundancia de los datos

Antes de la aparición de los manejadores de base de datos la información se guardaba en archivos, ya que algunos datos eran utilizados por múltiples aplicaciones, con frecuencia se registraban los mismos datos en diversos archivos, lo que ocasiona la llamada redundancia de los datos, esto origina varios problemas que tienen que ver con la integridad de los datos.

Problemas con la integridad de los datos

"Una causa de que la integridad de los datos resulte inadecuada es la redundancia de éstos."[16] Si la información sobre una entidad es almacenada en más de un lugar es muy probable que surjan incongruencias, por ejemplo si la dirección de un alumno se almacena en cinco lugares diferentes y el alumno se cambia de domicilio, el cambio de dirección se tiene que realizar en cinco lugares diferentes. Si el cambio no se realiza en alguno de los cinco distintos lugares se tendrá información diferente en diversos lugares de la misma persona, al plantearse este proyecto se determinó compartir la información de las bases de datos para evitar la redundancia de los datos. Por ejemplo los datos de las adscripciones (clave de la adscripción, nombre de la adscripción, etc.) ya han sido capturados y validados por el sistema de Adscripciones, por lo que solamente se crea una vista de los datos que se requieren consultar, tal vista es tratada como una tabla que solamente puede ser consultada, pues los datos de las adscripciones solamente se pueden modificar usando el sistema de Adscripciones.

[16] Shakuntala Atre, Técnicas de base de datos estructuración en diseño y administración Editorial trillas, 1988. pag. 22

3.3 Seguridad en SQL Server

SQL Server valida a los usuarios con 2 niveles de seguridad; autentificación del login y validación de permisos en la Base de Datos por medio de las cuentas de usuarios y de los roles. La autentificación identifica al usuario que está usando una cuenta y verifica sólo la habilidad de conectarse con SQL Server. El usuario debe tener permiso para acceder a las Bases de Datos en el Servidor. Esto se cumple asignando permisos específicos para la Base de Datos, para las cuentas de usuario y los roles. Los permisos controlan las actividades que el usuario tiene permitido realizar en las Bases de Datos de SQL Server.

Autentificación del Usuario

Un usuario debe tener una cuenta para conectarse a SQL Server. Este reconoce 2 mecanismos de autentificación: Autentificación de SQL Server y de Windows NT. Cada uno tiene un diferente tipo de cuenta.

Autentificación de SQL Server

Cuando se usa, un administrador del Sistema de SQL Server, define una cuenta (también llamada login) y una contraseña o password para dicha cuenta. En este caso los usuarios deben suministrar tanto el login como el password cuando se conectan a SQL Server.

Autentificación de Windows NT

Cuando se usa este método, el usuario no necesita de una cuenta de SQL Server, para conectarse. Un administrador del sistema debe definir, ya sea cuentas de Windows NT o grupos de Windows NT como cuentas válidas de SQL Server.

Modo de autentificación

Cuando SQL Server está corriendo en Windows NT, un administrador puede especificar que se ejecute en uno de 2 modos posibles de autentificación:

Modo de autentificación de Windows NT: Sólo está autorizada la autentificación de Windows NT. Si este es el modo escogido los usuarios no pueden usar cuentas de SQL Server.

Modo mixto: Cuando se usa este modo de autentificación, los usuarios se pueden conectar a SQL Server con la autentificación de Windows NT o con la de SQL Server.

El determinar el tipo de autentificación es responsabilidad del administrador de las bases de datos, para el servidor que se emplea en este proyecto se determinó que la mejor opción es usar el modo de autentificación mixto, ya que si se empleara solamente la autentificación de Windows NT, para iniciar sesión en los sistemas y en el servidor el usuario se debería identificar en Windows; pero en la actualidad muchos usuarios de los sistemas comparten sus computadoras para trabajar, por lo que si dos o más usuarios comparten una misma computadora no solamente se tendría que cerrar la sesión del sistema para que otro usuario trabaje, además se debería de cerrar la sesión de Windows, si se trata de Windows xp, Windows 2000, Windows NT o superior, pero para computadoras con sistema operativo como Windows 95 y Windows 98 se tendría que reiniciar la computadora cada vez que un usuario diferente tuviera que trabajar con el sistema.

3.4 Cuentas de usuario y roles en una base de datos

Después de que los usuarios han sido autentificados, y se les ha permitido conectarse a SQL Server, deben tener cuentas en la Base de Datos. Las cuentas de usuario y los roles, identifican permisos para ejecutar acciones en la base de datos, por ejemplo, borrado, actualización o inserción de datos.

Cuentas de usuarios de la base de datos

Las cuentas de usuario utilizadas para aplicar permisos de seguridad son las cuentas de usuarios, o grupos de Windows NT o las cuentas de SQL Server. Las cuentas de usuario son específicas para cada Base de Datos.

Roles

Con el fin de mejorar los aspectos relacionados con la seguridad se ha introducido la noción de rol. Se define un rol como una colección de privilegios relacionados, que pueden ser otorgados a usuarios o a otros roles. Los roles han sido diseñados para facilitar la administración de los privilegios sobre los diversos objetos de la base de datos, como tablas, vistas, etc.

Los roles tienen las siguientes propiedades:

- Pueden ser otorgados a otros roles; pero no a sí mismos.
- Pueden ser otorgados a uno o más usuarios.
- Pueden ser habilitados o deshabilitados
- Pueden ser revocados.

3.5 La administración del RDBMS

Al emplear un manejador de base de datos se requiere que un usuario o grupo de ellos se encargue de administrar los datos de la base de datos. A la persona o grupo que se encarga de administrar la base de datos se la llama administrador de base de datos ABD (o DBA por sus siglas en inglés). El administrador de la base de datos no es el propietario de los datos sino el protector de ellos. Para el inicio de este proyecto se determinó que los administradores del servidor serían: Rosario Rivera Aguilar y Octavio Sereno García. Aunque cada líder de proyecto podrá crear las bases de datos que requiera y por medio del programa SISECU administrar las cuentas de los usuarios.

Una de las herramientas que puede emplear el DBA en el manejo y documentación de los datos es un diccionario de datos.

Un diccionario de datos es un depósito central de información, que suele representarse mediante una estructura de tablas, contiene información de las tablas que forman la base de datos, su significado, uso y forma de representación.

3.6 Introducción al lenguaje SQL

Para usar adecuadamente SQL Server es necesario conocer el lenguaje de consultas SQL, el nombre SQL es una abreviatura de Structured Query Languaje (Lenguaje de consultas estructurado). Como su nombre lo indica, SQL es un lenguaje informático el cuál está compuesto por comandos, cláusulas, operadores y funciones de agrupamiento. Estos elementos se combinan en instrucciones para crear, actualizar y manipular datos almacenados en una base de datos y más concretamente con las bases de datos relacionales.

SQL es a la vez un lenguaje fácil de aprender y una herramienta completa para manipular datos. Las peticiones sobre los datos se expresan mediante sentencias, que deben escribirse de acuerdo con ciertas reglas de este lenguaje. En el presente trabajo se da una breve introducción a este lenguaje.

"SQL es un lenguaje estándar por haberse visto consolidado por el Instituto Americano de Normas, en inglés American National Standars Institute (ANSI) y por la Organización de Estándares Internacional, en inglés Internetional Standars Organization (ISO)"[17] entre otros Institutos.

[17] R. Groff James , N. Weinberg Paul, Aplique SQL Editorial Mc-Graw-Hill 1991 pag. 9

3.6.1 Comandos SQL

Existen dos tipos de comandos SQL:

los DLL que permiten crear y eliminar bases de datos, tablas, campos e índices.

los DML que permiten generar consultas para ordenar, borrar y extraer datos de la base de datos, además de permitir añadir y modificar datos en la base de datos.

Los distintos Comandos DLL son:

Create: Utilizado para crear nuevas tablas, usuarios, roles, etc.

Drop: Utilizado para eliminar tablas, usuarios, roles, etc.

Alter: Utilizado para modificar las tablas, agregando campos o cambiando la definición de los mismos.

Los distintos Comandos DML son:

Select: Utilizado para consultar registros de la base de datos que satisfagan un criterio determinado

Insert: Utilizado para añadir datos en la base de datos.

Update: Utilizado para modificar los valores de los campos y registros especificados

Delete: Utilizado para eliminar registros de una tabla de una base de datos

3.6.2 Sentencias de selección o consultas

Las consultas son la base del lenguaje SQL. La sentencia Select, que se utiliza para expresar consultas en SQL, es la más potente y compleja de las sentencias SQL.

La sentencia Select recupera datos de una base de datos y los devuelve en forma de resultados de consulta. Consta de seis cláusulas: las dos primeras (Select y From) obligatorias y las otras cuatro opcionales.

La forma básica de la sentencia Select es:

Select {* | lista de columnas}
From {nombres de tablas [alias] }
[Where {condición}]
[Group By {columnas de agrupamiento}]
[Having {condición}]
[Order By { columna [Asc | Desc]}]

Donde la barra vertical | Indica la elección de una de las opciones que este separando. Una u otra no ambas. Los corchetes [ ] Encierran elementos opcionales de la sentencias, es decir que pueden emplearse o no dependiendo del usuario, como podemos apreciar las cláusulas Where, Group By, Having y Order By son opcionales. Las llaves { } Encierran elementos obligatorios de la sentencia que siempre deben de ser especificados.

Cláusula Select

La cláusula Select lista los datos recuperados de la base de datos. Los elementos o datos a seleccionar pueden ser columnas de la base de datos, o columnas a calcular por SQL cuando efectúa la consulta, o también el asterisco (*) para recuperar todos los campos de una tabla en particular.

La lista de columnas puede ser un simple nombre de campo (por ejemplo Sueldo). Expresiones más complejas pueden incluir operaciones matemáticas o funciones de columna (por ejemplo Venta * 0.15).

La lista de columnas debe ir separadas por comas si existen más de una (por ejemplo Nombre, Edad, Sexo).

Supongamos que tenemos una tabla Agenda compuesta de los campos Apellido, Nombre y Sexo que tiene la siguiente estructura.

Tabla Agenda

Apellido	Nombre	Sexo
Amaya Cárdenas	José Antonio	masculino
Almanza Liñan	Manuel	masculino
Amaya Galindo	Connie	femenino
Armenta Fraga	Gerardo	masculino
Cervantes Gonzalez	Juan	masculino
Cepeda Rivera	Maria Del Carmen	femenino
Gómez Cardenas	Rosa	femenino
González Rubio	Agustín	masculino
Gómez Torres	Omar	masculino
González Rivera	Maria	femenino
Rangel Galindo	Erica	femenino
Ramírez Méndez	Susana	femenino
Reyes Montanez	Margarita	femenino

Al realizar una consulta los nombres de campos pueden ir precedidos por el nombre de la tabla o su alias. Por ejemplo Agenda.Nombre o A.Nombre donde A es el alias para la tabla Agenda.

```
Select Agenda.Nombre, Agenda.Apellido
From Agenda;
```

Muestra los distintos nombres y apellidos almacenadas en la tabla Agenda.

Nombre	Apellido
José Antonio	Amaya Cárdenas
Manuel	Almanza Liñan
Connie	Amaya Galindo
Gerardo	Armenta Fraga
Juan	Cervantes Gonzalez
Maria Del Carmen	Cepeda Rivera
Rosa	Gómez Cardenas
Agustín	González Rubio
Omar	Gómez Torres
Maria	González Rivera
Erica	Rangel Galindo
Susana	Ramírez Méndez
Margarita	Reyes Montanez

Cláusula From

La cláusula From utilizada para especificar la tabla de la cual se van a seleccionar los registros. El formato de esta cláusula es:

From {nombres de tablas [alias] }

nombres de tablas puede ser uno o más nombres de tablas en la base de datos. Alias es un nombre que se usa para referirse a la tabla en el resto de la sentencia Select para abreviar el nombre original, haciendo más manejable la consulta. Por ejemplo,

```
Select A.Nombre, A.Apellido
From Agenda A;
```

es mucho más práctico y sencillo que:

```
Select Agenda.Nombre, Agenda.Apellido
From Agenda;
```

Las dos sentencias son idénticas y nos devuelven los nombres y apellidos de todos los registros que contiene la tabla Agenda.

Cláusula Where

La cláusula Where es utilizada para especificar las condiciones que deben reunir los registros que se van a seleccionar.

La cláusula Where contiene condiciones en la forma:

Where {expresión1 operador expresion2}

expresión1 y expresion2 pueden ser nombres de campos, valores constantes o expresiones. Operador es un operador relacional que une dos expresiones. Más adelante se verán los distintos operadores que se pueden utilizar.

Por ejemplo, la siguiente sentencia nos muestra el número de personas en nuestra tabla agenda cuyo sexo sea femenino.

```
Select count(*) Mujeres
From Agenda
where sexo = 'femenino';
```

Nos traerá como resultado:

Mujeres
7

Donde Mujeres es un alias que asignamos para que se muestre como encabezado en el resultado.

Al emplear la Cláusula Where cada vez que se desee establecer una condición que se refiera a un campo de tipo carácter la condición de búsqueda debe ir encerrada entre comillas simples.

Cláusula Order By

La cláusula Order By ordena los resultados de la consulta en base a los datos de una o más columnas, de acuerdo a un orden específico. Por tanto, indica como deben ordenarse los registros que se seleccionen. Tiene la forma:

```
Order By { columna [ Asc | Desc] }
```

columna puede ser el nombre de un campo, o el número de posición que ocupa la expresión de columna en la cláusula Select. Por defecto se ordenan Ascendentemente (de menor a mayor). Si se deseará ordenar de mayor a menor se empleará Desc (Descendente). Por ejemplo, para mostrar los nombres de todas las personas en nuestra tabla Agenda ordenados en forma descendente, se emplea la siguiente sentencia:

```
Select A.Nombre, A.Apellido
From Agenda A
Order by A.Nombre Desc;
```

Nombre	Apellido
Susana	Ramírez Méndez
Rosa	Gómez Cardenas
Omar	Gómez Torres
Maria Del Carmen	Cepeda Rivera
Maria	González Rivera
Margarita	Reyes Montanez
Manuel	Almanza Liñan
Juan	Cervantes Gonzalez
José Antonio	Amaya Cárdenas
Gerardo	Armenta Fraga
Erica	Rangel Galindo
Connie	Amaya Galindo
Agustín	González Rubio

Cláusula Group By

La cláusula Group By especifica una consulta sumaria. Es decir en vez de producir una fila de resultados por cada fila de datos de la base de datos, una consulta sumaria agrupa todas las filas similares en grupos específicos.

Seguido de la cláusula Group By se especifican los nombres de uno o más campos cuyos resultados se desean agrupados. La cláusula Group By tiene la forma:

Group By {columnas de agrupamiento}

columnas de agrupamiento debe coincidir con la expresión de columna utilizada en la cláusula Select. Puede ser uno o más nombres de campo de una tabla separados por coma, o una o más expresiones separadas por comas.

Supongamos que tenemos una tabla Empleado compuesta de los campos Cve_Emp, Apellido, Nombre, Sexo, Edad y Cve_Depto que tiene la siguiente estructura.

Tabla Empleado

Cve_Emp	Apellido	Nombre	Sexo	Edad	Cve_Depto
1	Amaya Liñan	Miguel	masculino	20	1
2	Almanza Galindo	Carlos	masculino	55	4
3	Amira Rubio	María	femenino	32	3
4	Armenta Fraga	Jesús	masculino	29	2
5	Cervantes González	Juan	masculino	41	3
6	Cepeda Rivera	Rosa	femenino	33	1
7	Gómez Garza	Angélica	femenino	22	2
8	González García	Ángel	masculino	41	2
9	Gómez González	Omar	masculino	37	2
10	González Rivera	Maria	femenino	26	3
11	Rangel Galindo	Margarita	femenino	29	3
12	Ramírez Méndez	Susana	femenino	35	1
13	Reyes Díaz	Liliana	femenino	42	2
14	Rico Aguilar	Claudia	femenino	19	4

Si además tenemos una tabla Departamento compuesta de los campos Cve_Depto y Departamento que tiene la siguiente estructura.

Tabla Departamento

Cve_Depto	Departamento
1	Contabilidad
2	Almacén
3	Ventas
4	Dirección

En el siguiente ejemplo realizamos una consulta que nos dice cuantos empleados están registrados en cada departamento:

```
Select cve_depto, count(*)numero_empleados
From empleado
Group by cve_depto;
```

Resultado:

cve_depto	numero_empleados
1	3
2	5
3	4
4	2

Esta sentencia nos devolverá una fila por cada departamento de empleados. Cada una de las filas contendrá la clave del departamento y el número de empleados en él.

Cláusula Having

La cláusula Having dice a SQL que incluya solo ciertos grupos producidos por la cláusula Group By en los resultados de la consulta. Al igual que la cláusula Where, utiliza una condición de búsqueda para especificar los grupos deseados. Es decir, es utilizada para especificar la condición que deben de cumplir los grupos. Sólo es válida si previamente se ha especificado la cláusula Group By.

La cláusula Having contiene condiciones en la forma:

Having {expresión1 operador expresión2}

expresión1 y expresión2 pueden ser nombres de campos, valores constantes o expresiones
operador es un operador relacional que une las dos expresiones.

La siguiente sentencia nos mostrará los departamentos que tengan al menos cinco empleados. Es decir que se excluirá del resultado a los departamentos que cuenten con menos de cinco empleados.

```
Select cve_depto, count(*)numero_empleados
From empleado
Group by cve_depto
Having count(*) >= 5;
```

Resultado:

cve_depto	numero_empleados
2	5

Enlace de dos Tablas

Los ejemplos vistos hasta el momento solo extraen datos de una única tabla y pocas cosas se podrían hacer si no se pudieran relacionar varias tablas para obtener las consultas requeridas, pues frecuentemente la información que buscamos no esté almacenada en una sola tabla. Una base de datos relacional permite seleccionar información de más de una tabla y combinar los resultados en un listado. La búsqueda combinada en más de una tabla se conoce con el término de búsqueda relacional o JOIN.

Para extraer los datos deseados deberemos de buscar un campo que contenga información común en los dos tablas, es decir, aquel por el que están relacionadas ambas tablas, los campos deben ser del mismo tipo de datos (entero, carácter, etc.), es decir deben contener el mismo tipo de datos, pero no es necesario que tengan el mismo nombre.

El Join se indica en la cláusula Where como otra condición más, utilizando cualquier operador relacional (=, <, >, <=, >=, <>). Su formato es:

Where {campo1 operador campo2 }

Por ejemplo, si se desea saber el nombre del departamento donde trabaja determinado empleado, y se intenta buscar en la tabla empleado, puede verse que no tiene una columna con el nombre de departamento; sin embargo, la tabla de departamento tiene la clave del departamento y el

nombre del departamento (cve_depto y departamento). Como las dos tablas tienen una columna en común cve_depto, es posible relacionar las dos tablas mediante la cláusula Where indicando la tabla y la columna separados por un punto. El siguiente ejemplo lista los nombres y apellidos de los empleados y a que departamentos pertenecen, ordenados por Departamento y Apellido en forma ascendente:

```
Select  D.Departamento , E.Apellido, E.Nombre
From Empleado E, Departamento D
Where E.cve_depto = D.cve_depto
order by D.departamento, E.Apellido ;
```

Resultado:

Departamento	Apellido	Nombre
Almacén	Armenta Fraga	Jesús
Almacén	Gómez Garza	Angélica
Almacén	Gómez González	Omar
Almacén	González García	Ángel
Almacén	Reyes Díaz	Liliana
Contabilidad	Amaya Liñan	Miguel
Contabilidad	Cepeda Rivera	Rosa
Contabilidad	Ramírez Méndez	Susana
Dirección	Almanza Galindo	Carlos
Dirección	Rico Aguilar	Claudia
Ventas	Amira Rubio	María
Ventas	Cervantes González	Juan
Ventas	González Rivera	Maria
Ventas	Rangel Galindo	Margarita

Enlace de más de dos tablas

SQL puede unir muchas tablas en una sola sentencia, para ello debemos efectuar el Join entre todas ellas, anteponiendo a los nombres de los campos los nombres de la tabla o de su alias, pues en caso de que algún nombre de campo se repita en alguna de las tablas y no se especifique el nombre de su tabla o alias se produce un mensaje de error en la consulta.

3.6.3 Expresiones SQL

Las expresiones se utilizan frecuentemente en las cláusulas Where, Order By y Having de las sentencias Select.

Las expresiones nos permiten utilizar operaciones matemáticas, operaciones con cadenas de caracteres y manipular fechas para construir consultas complejas.

Los elementos que compones las expresiones son:

- Nombres de campos.
- Constantes.
- Operadores de caracteres.
- Operadores numéricos.
- Operadores de fechas.
- Operadores lógicos.
- Operadores de relación.
- Funciones.

Nombres de campos

Las expresiones más comunes son los nombres de campos, que es el nombre asignado a una columna de una tabla. Se pueden combinar con otros elementos de las expresiones

Constantes

Las constantes son valores que no cambian. Por ejemplo, en la expresión Salario + 300, el valor 300 es una constante y Salario es el nombre de un campo.

Las constantes de caracteres se deben encerrar entre comillas simples(' '). Las constantes de fechas deberán estar encerradas entre comillas simples, por ejemplo, '02-AUG-1999' representa la fecha 02 de Agosto de 1999.

Operadores de caracteres

Las expresiones de caracteres pueden incluir los siguientes operadores:

Operador	Significado
+	Concatenación de caracteres

Si por ejemplo, NOMBRE contiene 'Margarita' y APELLIDOS 'Mora' al unirlos tendremos:

Valor	Resultado
NOMBRE + APELLIDOS	'Margarita Mora'

Operadores Numéricos

Son operadores usados para realizar operaciones aritméticas, se pueden utilizar los siguientes operadores:

operador	Significado
+	Suma
-	Resta
*	Multiplicación
/	División

Operadores de fechas

Las expresiones de fechas pueden incluir los siguientes operadores:

operador	Significado
+	Añade un número de días a una fecha para producir una nueva fecha.
-	Resta de un número de días a una fecha para producir una nueva fecha, o el número de días entre dos fechas.

Ejemplos:

```
'02-AUG-1999' + 10 = '12-AUG-1999'
'02-AUG-1999' – 3  = '30-JUL-1999'
```

Operadores Lógicos

Dos o más expresiones pueden ser combinadas para formar expresiones más complejas con distintos criterios. Cuando existen dos o más expresiones deben estar unidas por And, Or o Xor.

And: Es el "y" lógico. Evalúa dos expresiones o condiciones y devuelve un valor de verdad sólo si ambas son ciertas.

Or: Es el "o" lógico. Evalúa dos expresiones y devuelve un valor de verdad si alguna de las dos es cierta.

Xor: Es llamado O exclusivo. Evalúa dos expresiones y devuelve un valor de verdad si son diferentes sus valores (una es verdadera y otra es falsa), y falsa si son iguales (las dos son verdaderas, o las dos son falsas).

Not: Negación lógica. Devuelve el valor contrario de la expresión.

La siguiente consulta nos mostrará el nombre y apellido de los empleados cuya edad sea mayor a 20 y menor a 40.

```
Select Nombre, Apellido
From Empleado
Where Edad > 20 AND Edad < 40;
```

Resultado:

Nombre	Apellido
María	Amira Rubio
Jesús	Armenta Fraga
Rosa	Cepeda Rivera
Angélica	Gómez Garza
Omar	Gómez González
Maria	González Rivera
Margarita	Rangel Galindo
Susana	Ramírez Méndez

La siguiente consulta nos mostrará el nombre de todos los empleados cuya edad sea mayor a 20 y menor a 40 o su sexo sea masculino.

```
Select Nombre, Apellido
From Empleado
Where (Edad > 20 AND Edad < 40)
OR Sexo = 'masculino';
```

Resultado:

Nombre	Apellido
Miguel	Amaya Liñan
Carlos	Almanza Galindo
María	Amira Rubio
Jesús	Armenta Fraga
Juan	Cervantes González
Rosa	Cepeda Rivera
Angélica	Gómez Garza
Ángel	González García
Omar	Gómez González
Maria	González Rivera
Margarita	Rangel Galindo
Susana	Ramírez Méndez

Operadores de relación

Los operadores de relación, también llamados de comparación, sirven para separar dos expresiones, pueden ser cualquiera de los siguientes:

Operador	Significado
=	Igual a
<>	Distinto de
>	Mayor que
>=	Mayor o igual que
<	Menor que
<=	Menor o igual que
Like	Coincide con un texto determinado
Not Like	No coincide con un texto determinado
Is Null	Igual a nulo (vacío)
Is Not Null	No es nulo (no está vacío)
Between	Rango de valores entre una cota inferior y otra superior
In	Pertenencia a un conjunto de valores o ser miembro de una subconsulta

Funciones

Las funciones permiten realizar con los datos operaciones adicionales a las mencionadas anteriormente, pudiendo participar como operadores en las expresiones.

Una función obtiene un valor único que se obtiene aplicando ciertas operaciones a otros valores dados, que se llaman argumentos. Se especifican como una palabra predefinida seguida de los argumentos entre paréntesis y separados por comas.

El lenguaje SQL dispone de un conjunto de funciones que pueden usarse en las consultas. A continuación se listan algunos ejemplo de las funciones que utiliza el lenguaje SQL.

Funciones para datos de tipo carácter:

Función	Descripción
Chr	Convierte un Código ASCII en una cadena de caracteres.
Chr(65)	Devuelve la letra A.
Rtrim	Quita los blancos que existan por la derecha en una cadena.
Rtrim ('ABCD ')	Devuelve 'ABCD'.
Ltrim	Quita los blancos por la izquierda que tenga una cadena.
Ltrim(' ABCD')	Devuelve 'ABCD'.
Upper	Convierte cada letra de una cadena a mayúscula.
Upper('programa')	Devuelve 'PROGRAMA'.
Lower	Convierte a minúscula cada letra de una cadena.
Lower('HOY')	Devuelve 'hoy'.

Funciones para datos de tipo numérico

Función	Descripción
Mod	Divide dos números y devuelve el resto de la división.
Mod(13,3)	Devuelve 1.
Length	Devuelve la longitud de una cadena.
Length ('hoy')	Devuelve 3
Max	Devuelve el mayor de dos números.
Max(15,33)	Devuelve 33.
Min	Devuelve el menor de dos números.
Min(15,33)	Devuelve 15.

Funciones para datos de tipo fecha

Función	Descripción
Month	Devuelve el mes de una fecha en cifras.
Month(24-Aug-2001)	Devuelve 8
Day	Devuelve el día de una fecha.
Day(24-Aug-2001)	Devuelve 24
Year	Devuelve el año, con todas sus cifras, de una fecha.
Year(24-Aug-2001)	Devuelve 2001.

3.6.4 Creación de tablas

Para crear en SQL Server una tabla llamada departamento, que contenga los campos cve_Depto (clave del departamento) y departamento (nombre del departamento) se puede emplear la siguiente sentencia.

```
Create table departamento ( cve_depto int,
                            departamento char(30) );
```

En dicha tabla se especifica el tipo de información que cada columna va a contener. La columna cve_depto contendrá información numérica del tipo entero, departamento contendrá cadenas de caracteres con una longitud máxima de 30 caracteres.

Se procede de forma similar para crear la tabla Empleado con el comando Create Table:

```
Create Table empleado (cve_emp int,
apellido char(40),
nombre char(25),
sexo char(10),
edad int,
cve_depto int);
```

3.6.5 Destrucción de una tabla

La sentencia para destruir una tabla es Drop. El formato para destruir o borrar un tabla es

```
Drop Table {nombre de tabla}
```

tabla es el nombre de la tabla que se va a destruir o eliminar, si lo que se desea es borrar los registros de la tabla sin destruirla se utiliza el comando Delete, el cual trataremos posteriormente.

La sentencia para eliminar la tabla departamento de la base de datos es:

```
Drop Table departamento;
```

3.6.6 Sentencia Insert

La sentencia Insert se utiliza para añadir registros a las tablas de la base de datos. El formato de la sentencia para insertar un registro o fila de datos es:

```
Insert Into tabla [campo1, campo2, .., campoN]
Values {valor1, valor2, ..., valorN};
```

tabla Es el nombre de la tabla en la que se añade el registro.
Campo1, ..., CampoN es una lista opcional de nombres de campo en los que se insertarán valores en el mismo número y orden que se especificarán en la cláusula Values.

Valor1, ..., ValorN Es una lista de valores, separados por comas, para dar valor a los distintos campos del registro que se añadirá a la tabla.

Esta consulta graba en el campo1 el valor1, en el campo2 y valor2 y así sucesivamente. Hay que prestar especial atención en colocar entre comillas simples (') las cadenas de caracteres y las fechas.

Si no se especifica la lista de campos, los valores en la cláusula Values deben ser tantos como campos tenga la tabla y en el mismo orden en que se definieron al crear la tabla.

Ejemplo para añadir un registro a la tabla departamento:

```
Insert into departamento (cve_depto, departamento)
Values (3, 'Ventas');
```

Otra manera de utilizar la sentencia Insert es usarla en conjunto con la sentencia Select en vez de la cláusula Values. Si tenemos una tabla llamada SubDepartamento formada por los siguientes registros:

Cve_SubDepto	SubDepartamento
101	Administración
102	Pedidos
103	Atención a clientes
104	Subdirección

Si ejecutamos la siguiente sentencia:

```
insert into Departamento
select *
from Subdepartamento;
```

Obtenemos el siguiente mensaje:

(4 row(s) affected)

Si consultamos la información de la tabla Departamento veremos que los registros de la tabla Subdepartamento se han añadido a la tabla Departamento.

```
select *
from  Departamento;
```

Resultado:

Cve_Depto	Departamento
1	Contabilidad
2	Almacén
3	Ventas
4	Dirección
101	Administración
102	Pedidos
103	Atención a clientes
104	Subdirección

Las filas sombreadas son los registros que se añadieron después de ejecutar la sentencia Insert.

3.6.7 Sentencia Update

La sentencia Update se utiliza para cambiar el contenido de los registros de una tabla de la base de datos. Su formato es:

```
Update {nombre de tabla }
Set {Campo1 = Valor1 [, Campo2 = Valor2,
   ... CampoN = ValorN]}
[Where expresión1 operador expresion2];
```

nombre de tabla Es el nombre de la tabla a actualizar.

campo1,campo2 Es el nombre del campo o campos que se desean cambiar. En una misma sentencia Update pueden actualizarse varios campos de cada registro de la tabla.

Valor1, ...,ValorN Es una lista de valores, separados por comas, en donde cada nuevo valor se asigna al campo que le precede.

La cláusula Where sigue el mismo formato que la vista en la sentencia Select y determina que registros se modificarán, en caso de no especificarse todos los registros se modificarán.

Update no genera ningún resultado. Para saber qué registros se van a cambiar, hay que examinar primero el resultado de una consulta de selección que utilice el mismo criterio y después ejecutar la consulta de actualización.

Ejemplo para actualizar el nombre del departamento tres a Ventas Directas:

```
Update departamento
Set departamento = 'Ventas Directas'
Where cve_depto = 3;
```

Nos muestra como resultado:

(1 row(s) affected)

Si realizamos una consulta a la tabla Departamento obtendremos lo siguiente:

```
select *
from Departamento;
```

Resultado:

Cve_Depto	Departamento
1	Contabilidad
2	Almacén
3	Ventas Directas
4	Dirección
101	Administración
102	Pedidos
103	Atención a clientes
104	Subdirección

3.6.8 Sentencia Delete

La sentencia Delete se utiliza para borrar registros de una tabla de la base de datos. El formato de la sentencia es:

```
Delete {nombre de tabla }
[Where expresión1 operador expresion2];
```

nombre de tabla es el nombre de la tabla de la que se van a eliminar los registros.

La cláusula Where sigue el mismo formato que la vista en la sentencia Select y determina que registros se borrarán.

Cada sentencia Delete borra los registros que cumplen la condición impuesta o todos si no se indica cláusula Where.

Una consulta delete elimina los registros completos, no únicamente los datos en campos específicos. Una vez que se han eliminado los registros utilizando una consulta de borrado no se puede deshacer la operación. Si se desea saber qué registros se eliminarán, primero se pueden examinar los resultados de una consulta de selección que utilice el mismo criterio y después ejecutar la consulta de borrado

Ejemplo para eliminar todos los registros de la tabla empleado:

```
Delete from empleado;
```

CAPÍTULO IV

DISEÑO DEL SISTEMA

4.1 Diseño de entrada

Es importante hacer que las pantallas en las que se captura la información sean fáciles de llenar para el usuario y que sean llenadas con datos precisos, ya que estas pantallas representan el enlace que une al sistema de información con el mundo y sus usuarios.

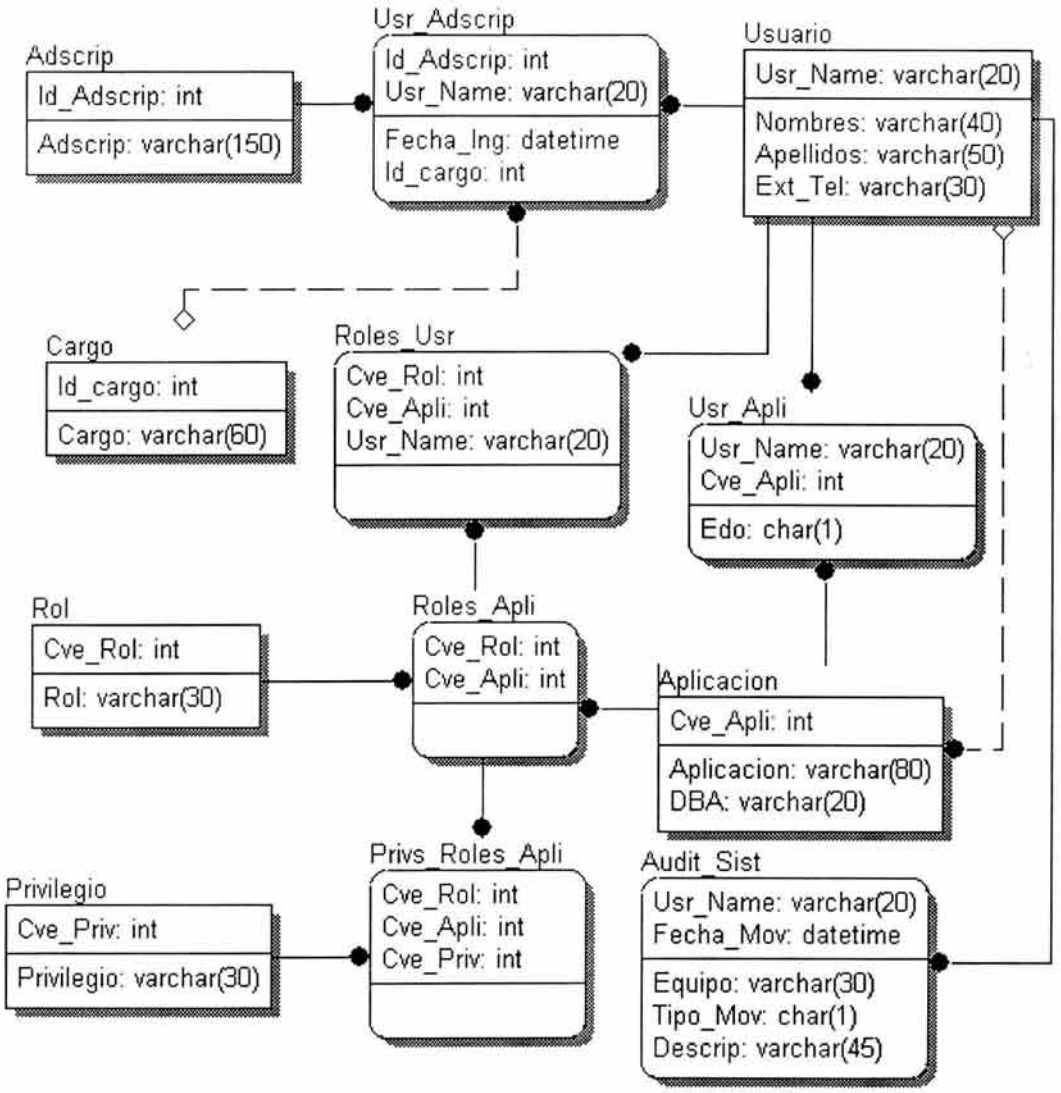
Se decidió que todas las pantallas deben ser consistentes entre sí, por ejemplo, si se emplea el término "Guardar" para salvar los datos en una pantalla, no debe de emplearse en otras el término "Salvar" para realizar la misma acción. La cantidad de datos a introducir en cada pantalla por teclado será pequeña ya que muchos datos se encontraran en catálogos y solamente se seleccionaran, para que la oportunidad de cometer errores al introducir datos sea pequeña. Las pantallas deben satisfacer el propósito para el cual fueron diseñadas sin confundir al usuario, se llenaran de arriba hacia abajo y de izquierda a derecha y los títulos de los datos requeridos se colocarán a la izquierda del dato.

Para que el llenado de los datos sea lo más preciso posible se usan validaciones para restringir los valores que puede recibir cada dato solicitado, ya sea que solo pueda recibir números, letras o algún conjunto de valores predeterminado, en muchas ocasiones el usuario podrá seleccionar el dato de un catálogo evitando así errores de captura.

4.2 Diseño de la base de datos

El diseño de una Base de Datos requiere conocer las funciones del usuario que se desean modelar, y los conceptos de Base de Datos que se usan para representar dichas funciones. Antes de diseñar una aplicación para SQL Server es importante realizar un diseño de la Base de Datos que refleje exactamente las funciones realizadas por el usuario, ya que una Base de Datos bien diseñada requiere cambios mínimos y generalmente se desarrolla con mayor eficiencia.

El siguiente modelo muestra las tablas de la base de datos propuesta, así como las relaciones entre estas. Para realizar el diagrama que se muestra a continuación se utilizó Erwin 4.0 de Computer Associates, debido a que es una herramienta fácil de usar, además de que basándose en el diagrama creado Erwin es capaz de crear las sentencias en SQL para construir la base de datos.



4.2.1 Diccionario de datos

Con base en el modelo anterior se creó la base de datos del sistema. A continuación se describe cada una de las tablas que forman la base de datos comenzando por el nombre de la tabla, una descripción del contenido de ésta, después se muestra la estructura de cada campo que compone a la tabla incluyendo su nombre, tipo, longitud y la descripción de dicho campo. Si al iniciar el campo tiene el símbolo • se trata de una clave primaria, es decir que por este campo estará ordenada la tabla, que dicha clave es única y no acepta valores nulos, sin embargo si antes del nombre esta un * significa que es una llave foránea, lo cual indica que este campo es llave primaria en otra tabla y que a través de este podemos unir ambas tablas, además se muestra un ejemplo de los datos contenidos.

Adscrip: Catalogo de las adscripciones que integran a la FES Acatlán.

Nombre del Campo	Tipo de dato	Tamaño	Requerido	Descripción
•Id_Adscrip	Entero		Si	Identificador de la adscripción
Adscrip	VarChar	150	Si	Nombre de la adscripción

Ejemplo:

Id_Adscrip	Adscrip
2	Unidad de Servicios Editoriales
3	Unidad de Servicios a la Comunidad
4	Unidad de Planeación

Aplicación: Catalogo de las aplicaciones desarrolladas por el DSI de la FES Acatlán y que se pueden llamar a través del sistema de seguridad.

Nombre del Campo	Tipo de dato	Tamaño	Requerido	Descripción
•Cve_Apli	Entero		Si	Identificador de la Aplicación
•Aplicación	VarChar	80	Si	Nombre de la Aplicación
*DBA	VarChar	20	No	Usuario encargado de la Aplicación

Ejemplo:

Cve_Apli	Aplicacion	DBA
1	Sistema de control de usuarios	seg
2	Sistema de Evaluacion en línea	rrivera
3	Sistema de Adscripción	yram
4	Profesor	atenea

Audit_Sist: Registro de las altas, bajas y modificaciones hechas en el sistema.

Nombre del Campo	Tipo de dato	Tamaño	Requerido	Descripción
•Usr_Name	VarChar	20	Si	Clave que identifica al usuario
•Fecha_Mov	Datetime		Si	Fecha del movimiento
Equipo	VarChar	30	Si	Nombre de la computadora en donde se realizó la modificación
Tipo_Mov	Char	1	Si	Tipo de movimiento realizado
Descrip	Varchar	45	No	Descripción del movimiento

Ejemplo:

Usr_Name	Fecha_Mov	Equipo	Tipo_Mov	Descrip
Atenea	02/10/2003 12:23:01	Acatlan	A	Añadió al usuario ROMJ680611
Atenea	01/10/2003 17:53:09	Acatlan	A	Añadió al usuario DEEC750724
Atenea	30/09/2003 19:34:22	Acatlan	A	Añadió al usuario OEPL481004

Cargo: Catalogo de cargos que puede tener un usuario.

Nombre del Campo	Tipo de dato	Tamaño	Requerido	Descripción
•Id_cargo	Entero		Si	Identificador del cargo
Cargo	VarChar	60	Si	Nombre del cargo

Ejemplo:

Id_cargo	Cargo
1	Servicio Social
2	Profesor
3	Líder de proyecto
4	Programador

Privilegio: Catalogo de los privilegios que existen para las diferentes aplicaciones.

Nombre del Campo	Tipo de dato	Tamaño	Requerido	Descripción
•Cve_Priv	Entero		Si	Clave del privilegio
Privilegio	VarChar	30	Si	Nombre del privilegio

Ejemplo:

Cve_Priv	Privilegio
19	Impresion
20	Exportar
21	Movimientos
22	Captura_Datos

Privs_Roles_Apli: Contiene la asociación de los roles y los privilegios asignados en cada aplicación.

Nombre del Campo	Tipo de dato	Tamaño	Requerido	Descripción
•Cve_Rol	Entero		Si	Clave del rol
•Cve_Apli	Entero		Si	Clave de la aplicación
•Cve_Priv	Entero		Si	Clave del Privilegio

Ejemplo:

Cve_Rol	Cve_Apli	Cve_Priv
1	3	16
1	4	1
1	4	2
1	4	18
1	5	1
1	5	2

Rol: Catalogo de los Roles creados para las diferentes aplicaciones.

Nombre del Campo	Tipo de dato	Tamaño	Requerido	Descripción
•Cve_Rol	Entero		Si	Clave del Rol
Rol	VarChar	30	Si	Nombre del Rol

Ejemplo:

Cve_Rol	Rol
7	Consulta
8	Capturista_Evelin
9	Programador_Evelin

Roles_Apli: Esta tabla lleva el control de los Roles que existen en cada Aplicación.

Nombre del Campo	Tipo de dato	Tamaño	Requerido	Descripción
•Cve_Rol	Entero		Si	Clave del Rol
•Cve_Apli	Entero		Si	Clave de la aplicación

Ejemplo:

Cve_Rol	Cve_Apli
1	10
2	2
3	4
5	3

Roles_Usr: Esta tabla lleva un seguimiento de los roles que tiene asignado cada usuario en las diferentes aplicaciones.

Nombre del Campo	Tipo de dato	Tamaño	Requerido	Descripción
•Cve_Rol	Entero		Si	Clave del Rol
•Cve_Apli	Entero		Si	Clave de la aplicación
•Usr_Name	VarChar	20	Si	Clave que identifica al usuario

Ejemplo:

Cve_Rol	Cve_Apli	Usr_Name
5	3	SIFL690412
5	9	SIFL690412
7	4	AAGC490717
7	4	AEFV650716

Usr_Adscrip: Esta entidad lleva el registro de la adscripción a la que pertenece un usuario.

Nombre del Campo	Tipo de dato	Tamaño	Requerido	Descripción
•Id_Adscrip	Entero		Si	Identificador de la adscripción
•Usr_Name	VarChar	20	Si	Clave que identifica al usuario
Fecha_Ing	Datetime		No	Fecha en que se da de alta el usuario
*Id_cargo	Entero		Si	Identificador del cargo que tiene el usuario

Ejemplo:

Id_Adscrip	Usr_Name	Fecha_Ing	Id_cargo
24	ROMJ680611	02/10/2003 12:23:01	2
25	DEEC750724	01/10/2003 17:53:09	2
26	OEPL481004	30/09/2003 19:34:22	2

Usr_Apli: Contiene la relación de las aplicaciones que pueden mandar llamar los usuarios.

Nombre del Campo	Tipo de dato	Tamaño	Requerido	Descripción
•Usr_Name	VarChar	20	Si	Clave que identifica al usuario
•Cve_Apli	Entero		Si	Clave de la aplicación
Edo	Char	1	No	Estado del usuario en la aplicación

Ejemplo:

Usuario	Cve_Apli	Edo.
Atenea	1	H
Atenea	3	H
GOVC620430	1	H
GOVC620430	3	H
GOVC620430	4	H
GOVC620430	5	H

Usuario: Esta tabla contiene los datos de los usuarios generados por el sistema de seguridad

Nombre del Campo	Tipo de dato	Tamaño	Requerido	Descripción
•Usr_Name	VarChar	20	Si	Clave que identifica al usuario
Nombres	VarChar	40	Si	Nombres del usuario
Apellidos	VarChar	50	No	Apellidos del usuario
Ext_Tel	VarChar	30	No	Número telefónico del usuario

Ejemplo:

Usr_Name	Nombres	Apellidos	Ext_Tel
GOVC620430	Ma. Del Carmen	Gonzalez Videgaray	
SIFL690412	Laura	Silva Fuertes	
SOAM630121	Miguel Ángel	Soto Abrego	

4.3 Diagramas de flujo

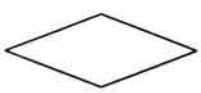
Los diagramas de flujo son probablemente la ayuda gráfica más antigua para diseñar un sistema, se utilizan para explicar los diversos procesos que formarán un sistema de una manera clara y fácil de entender utilizando pocos símbolos y conexiones entre ellos. Para comprender mejor los siguientes diagramas a continuación se explica el significado de cada símbolo utilizado en los diagramas de flujo de este trabajo.

4.3.1 Símbolos utilizados para representar los procesos

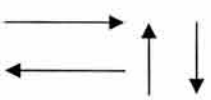
"

Terminador Indica el inicio ó fin del diagrama de flujo.

Proceso Representa los procesos realizados.



Decisión Muestra las diferentes acciones que deben realizarse si se cumple o no con una determinada acción.



Líneas de flujo Indican la secuencia entre pasos y la transmisión de información entre operaciones."[16]

[16] Henry C.Lucas, Jr. , Técnicas de informatica hoy Segunda Parte Tomo 3 Sistemas de información Editorial Paraninfo S.A., 1987. pag. 173

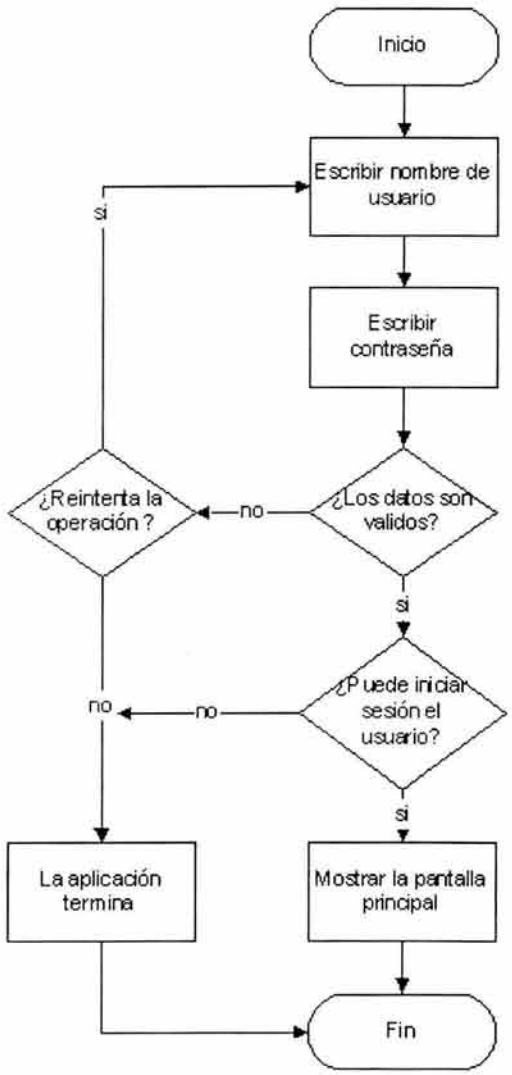
4.3.2 Diagramas de flujo de cada proceso

A continuación mencionaremos los procesos que se realizan en el sistema SISECU para administrar las cuentas de los usuarios, los diagramas muestran como realizar estos procesos de una manera general.

Identificación de usuario

Para poder acceder al sistema de seguridad el usuario debe de identificarse en el sistema, por lo que debe realizar el siguiente proceso.

Identificación de usuario



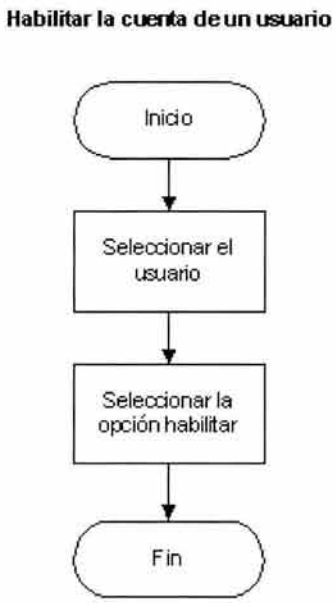
El nombre de usuario es el nombre con el que se conoce al usuario en el sistema, se puede considerar como el login de SQL Server.

Deshabilitar la cuenta de un usuario

Para evitar que un usuario inicie sesión en el sistema sin eliminarlo se debe deshabilitar su cuenta, este proceso se muestra en el siguiente diagrama.

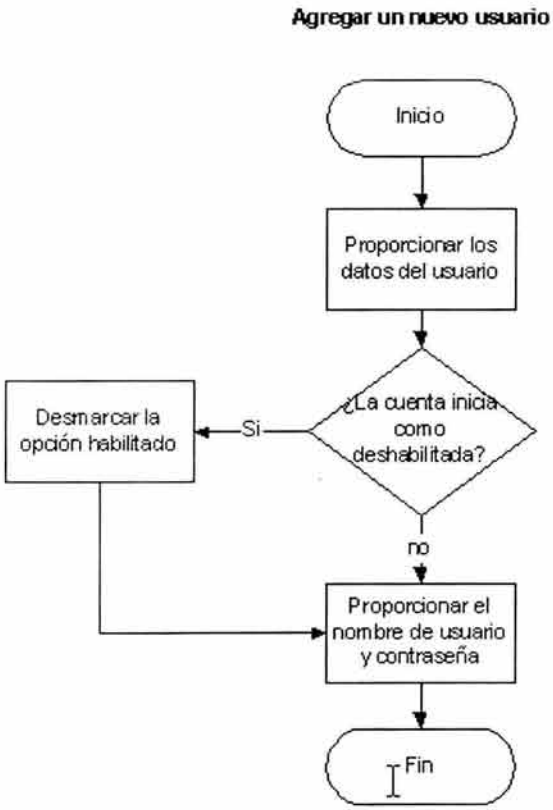
Habilitar la cuenta de un usuario

Si una cuenta de usuario se encuentra deshabilitada y se requiere habilitar dicha cuenta, se realiza el siguiente proceso.



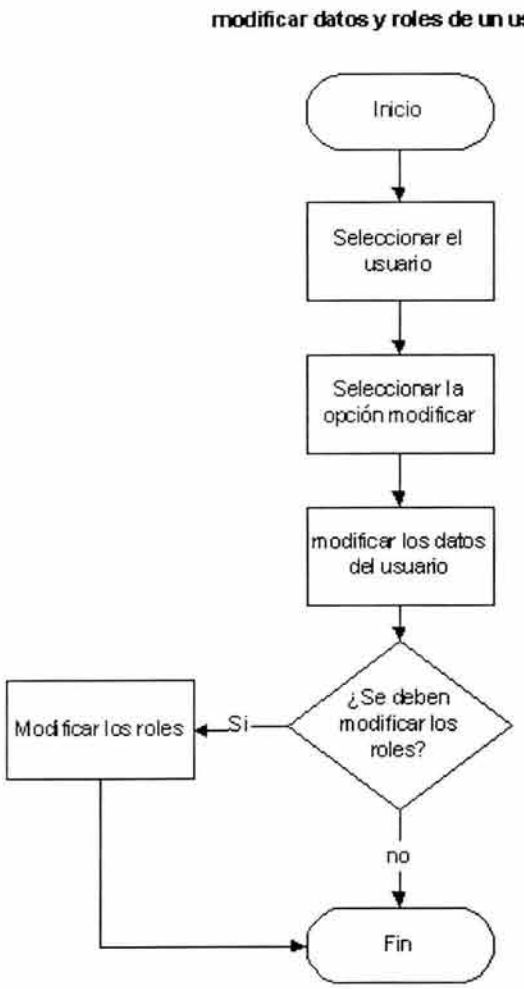
Agregar un nuevo usuario

Para añadir un nuevo usuario al sistema, siempre y cuando dicho usuario no se encuentre registrado en alguno de los sistemas del DSI, se realizan las siguientes acciones.



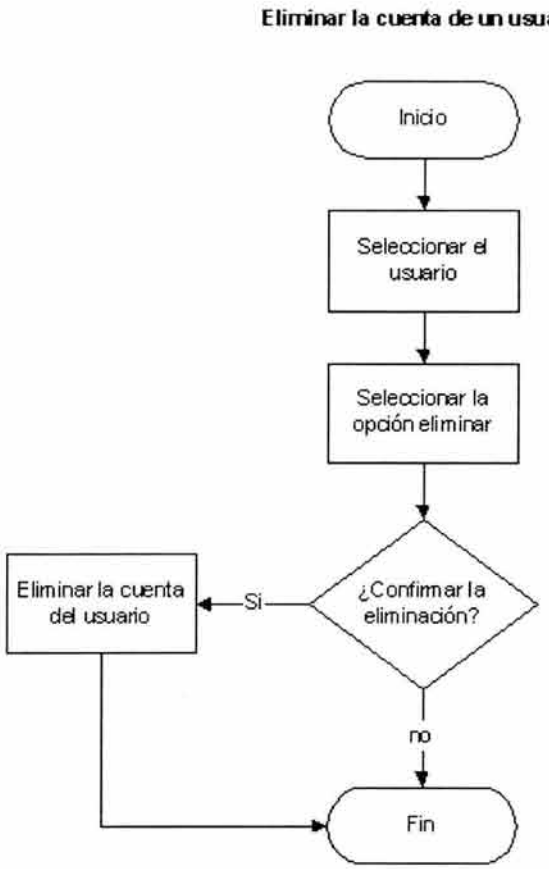
Modificar datos y Roles de un usuario

Para modificar los datos de un usuario, o modificar los roles que tiene en una aplicación se realiza el siguiente proceso.



Eliminar la cuenta de un usuario

Para eliminar la cuenta de un usuario, se realiza el siguiente procedimiento.



En este sistema todas las operaciones que implican eliminar algún dato requieren ser confirmadas.

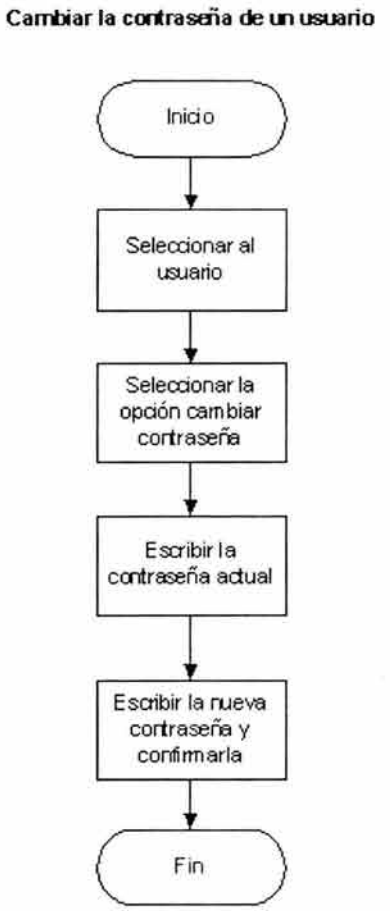
Añadir un usuario de otra aplicación

Para añadir un usuario al sistema si dicho usuario ya existe en alguno de los sistemas del DSI, se realiza el siguiente proceso.

Añadir un usuario de otra aplicación

Cambiar la contraseña de un usuario

Proceso que permite cambiar la contraseña de un usuario.



Consultar el historial de un usuario

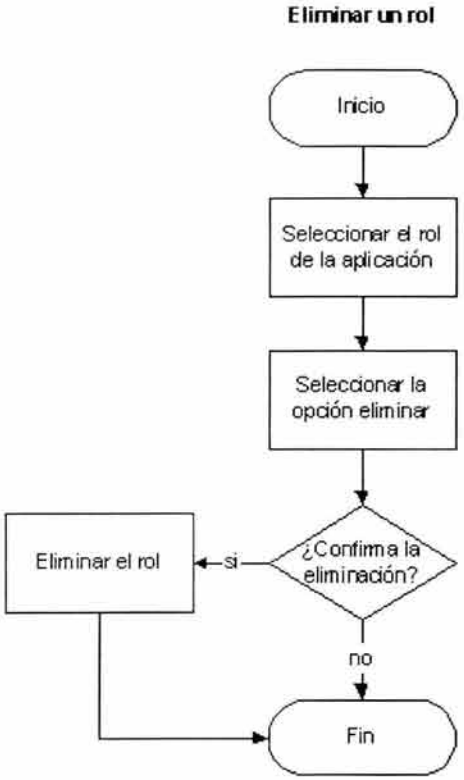
Para consultar el historial de un usuario (fecha de creación, de eliminación) para nuestra aplicación, se realiza el siguiente proceso.

Añadir un rol

Para crear un rol en una aplicación se sigue el siguiente proceso.

Eliminar un rol

Para eliminar un rol de la aplicación se realiza el siguiente proceso.

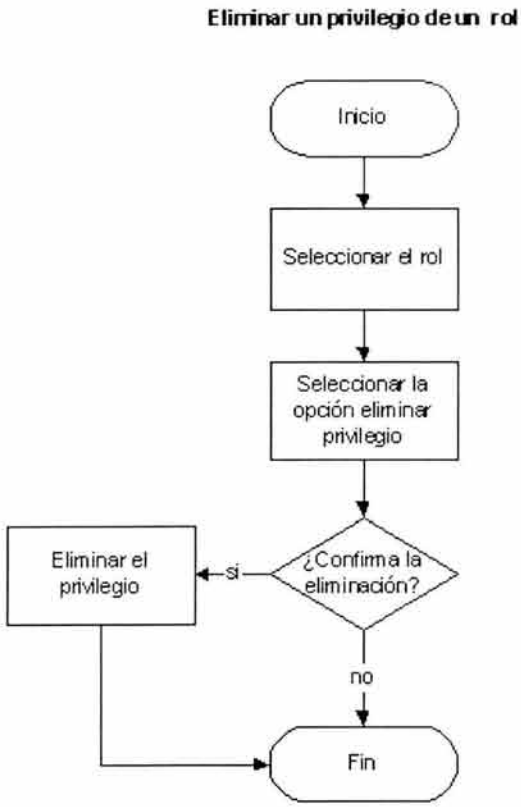


Añadir un privilegio a un rol

Para añadir un privilegio a un rol, recordemos que un rol es un conjunto de privilegios, se realiza el siguiente proceso.

Eliminar un privilegio de un rol

Para eliminar un privilegio que forma parte de un rol, se realiza el siguiente proceso.



Imprimir el reporte de usuarios

Proceso para imprimir un reporte de los usuarios.

4.4 Diseño de salida

La salida de un sistema se refiere a los resultados y a la información generada por el Sistema. Hay que tener en cuenta que para la mayoría de los usuarios la salida es la única razón para el desarrollo de un Sistema y la base para evaluar su utilidad. Se analizaron varios puntos para decidir cuales serían las salidas más apropiadas del sistema y se determinó lo siguiente.

Se necesita un reporte que muestre los usuarios de cada aplicación ordenados por nombre y los privilegios que tienen asignados y otro reporte con las mismas especificaciones ordenado por la adscripción a la que pertenecen los usuarios. Dichos informes serán presentados de forma impresa, aunque se espera añadir más reportes impresos cuando sean requeridos.

Además existen algunas consultas necesarias que no requieren ser impresas, por lo que dichas consultas solamente mostraran su resultado en pantalla.

4.5 Pantallas del sistema

A continuación se presentarán cada una de las pantallas diseñadas para el sistema de seguridad. Estas aparecerán desglosadas por menú y a su vez las pantallas contenidas dentro de cada submenú de arriba hacia abajo y de izquierda a derecha. Se explica además de la función de cada pantalla, el modo de acceso y el proceso que involucra dicha pantalla.

1 *Pantalla de identificación*

Proceso: Identificación de Usuario
Descripción: Esta pantalla sirve para que el usuario inicie su sesión, con lo cual se leen y asignan los privilegios del usuario.

Modo de uso:

1. Al mostrarse la pantalla (Fig. 1a) teclear el nombre de usuario en la primer caja de texto.
2. Teclear la contraseña correspondiente al usuario en la segunda caja de texto.
3. Accionar el botón Aceptar mediante un clic.

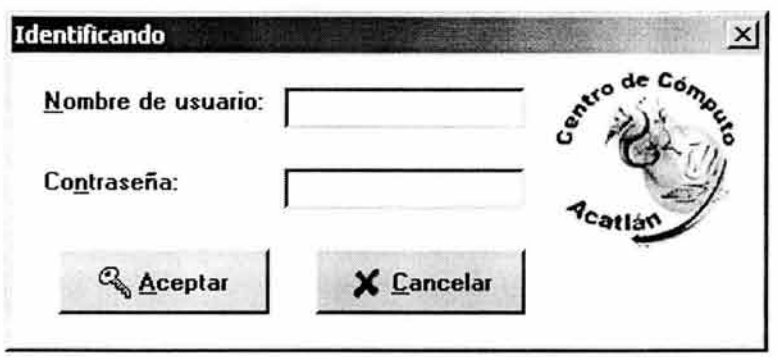


Fig. 1a

2 *Pantalla principal:*

Proceso: Permitir acceder a las pantallas que se usan para administrar las cuentas de los usuarios, llamar a otros sistemas y salir del sistema.

Descripción: Pantalla en donde se encuentra el menú principal y las opciones correspondientes al sistema.

Modo de uso:

1. Al aceptarse el nombre de usuario y la contraseña del usuario en la pantalla de identificación aparecerá la pantalla *Sistema de Seguridad y Control de Usuarios* (Fig. 2a). Al dar un clic en alguna de las opciones del menú aparecerá una lista con las opciones disponibles del menú.
2. Dar un clic en el menú de interés.

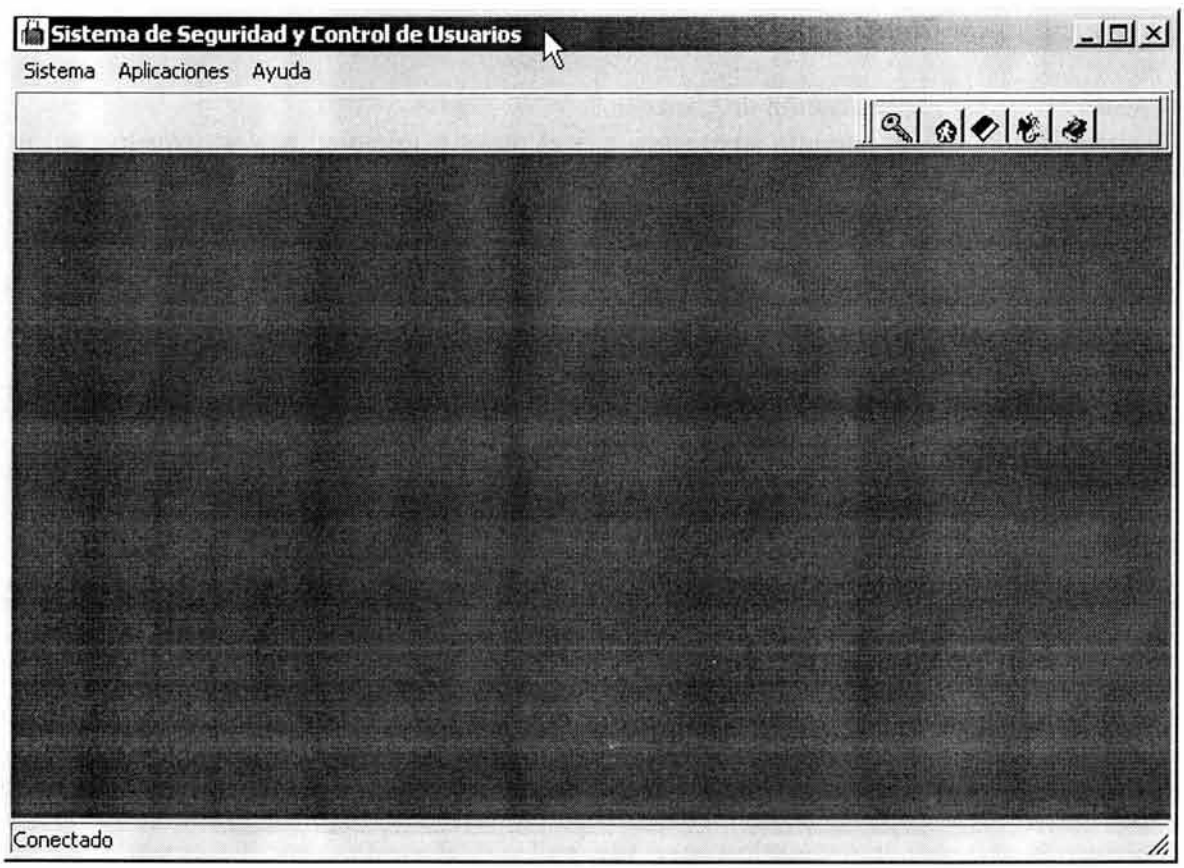


Fig. 2a

El menú principal consta de tres opciones de elección:

Sistema
Aplicaciones
Ayuda

Cada una de estas opciones y lo que contienen se describe a continuación.

Pantalla 2.1 Menú Sistema de la pantalla principal

Proceso: Presentar las opciones Cerrar Sesión o Iniciar Sesión, Mantenimiento de Usuarios, Administración de privilegios, Reporte de Usuarios y Salir.

Descripción: Este menú permite acceder a las pantallas que administran las cuentas de los usuarios, si se tienen los privilegios para realizar dichas operaciones, en caso de que no sea así las únicas opciones disponibles son: Cerrar Sesión o Iniciar Sesión y Salir.

Modo de acceso: A partir de la pantalla principal dar un clic en la opción Sistema del menú principal (Fig. 2b).

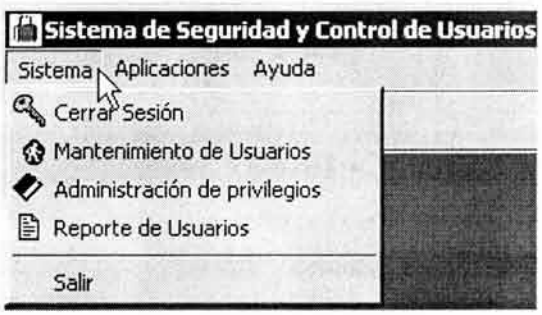


Fig. 2b

Pantalla 2.2 Menú Sistema > Cerrar Sesión

Proceso: Cerrar la sesión activa de un usuario.

Descripción: Esta opción permite cerrar una sesión que se encuentra abierta, con el fin de permitir que otro usuario trabaje con el sistema sin tener que salir del mismo, cuando se selecciona esta opción el texto del menú cambia de Cerrar Sesión a Iniciar Sesión, además de Ocultar los menús Mantenimiento de Usuarios, Administración de privilegios y Reporte de Usuarios y deshabilitar las opciones del menú Aplicaciones.

Modo de acceso: A partir de la pantalla principal dar un clic en la opción Sistema del menú principal, seleccionar Cerrar Sesión (Fig. 2c).

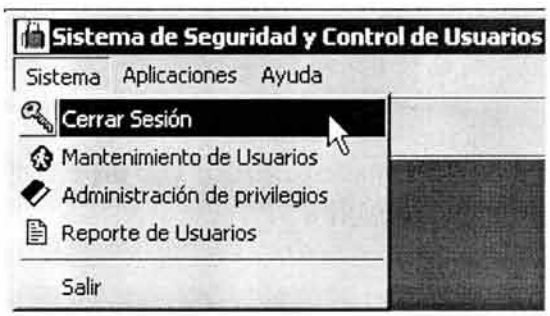


Fig. 2c

Pantalla 2.3 Menú Sistema > Iniciar Sesión

Proceso: Identificación de Usuario.

Descripción: Esta opción aparece después de cerrar una sesión, al dar clic en esta opción se muestra la pantalla de identificación de usuario, para que se inicie otra sesión en el sistema.

Modo de acceso: A partir de la pantalla principal dar un clic en la opción Sistema del menú principal, seleccionar Iniciar Sesión (Fig. 2d).

Fig. 2d

Pantalla 2.4 Menú Sistema > Mantenimiento de Usuarios

Proceso: Mostrar la pantalla *Mantenimiento de Usuarios*.
Descripción: Esta opción permite mostrar la pantalla *Mantenimiento de Usuarios*, si se tienen los privilegios necesarios.
Modo de acceso: A partir de la pantalla principal dar un clic en la opción Sistema del menú principal, seleccionar Mantenimiento de Usuarios (Fig. 2e).

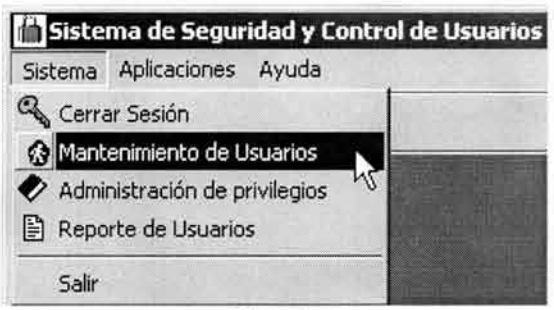


Fig. 2e

Pantalla 2.5 Menú Sistema > Administración de privilegios

Proceso: Mostrar la pantalla *Administración de privilegios*.
Descripción: Esta opción permite mostrar la pantalla *Administración de privilegios*, si se tienen los privilegios necesarios.
Modo de acceso: A partir de la pantalla principal dar un clic en la opción Sistema del menú principal, seleccionar Administración de privilegios (Fig. 2f).

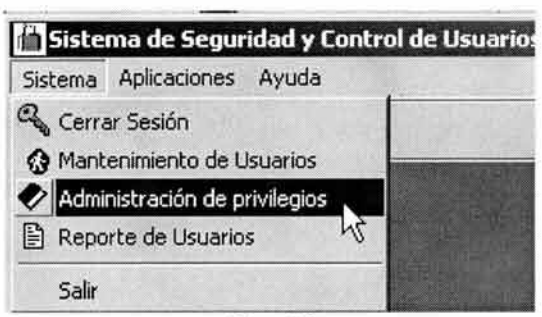


Fig. 2f

Pantalla 2.6 Menú Sistema > Reporte de Usuarios

Proceso: Mostrar la pantalla *Reporte de Usuarios*.
Descripción: Esta opción permite mostrar la pantalla *Reporte de Usuarios*, si se tienen los privilegios necesarios.
Modo de acceso: A partir de la pantalla principal dar un clic en la opción Sistema del menú principal, seleccionar Reporte de Usuarios (Fig. 2g).

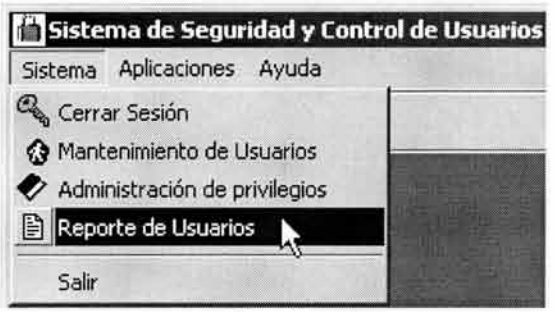


Fig. 2g

Pantalla 2.7 Menú Sistema > Salir

Proceso: Salir del sistema.
Descripción: Esta opción permite salir del sistema.
Modo de acceso: A partir de la pantalla principal dar un clic en la opción Sistema del menú principal, seleccionar Salir (Fig. 2h).

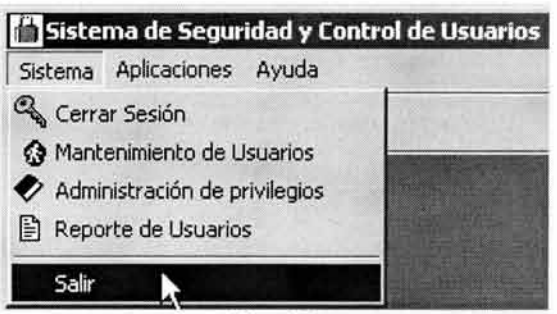


Fig. 2h

Pantalla 2.8 Menú Aplicaciones de la pantalla principal

Proceso: Permitir al usuario mandar llamar otros sistemas.

Descripción: Este menú permite mostrar los diversos sistemas desarrollados por el DSI, si se tienen los privilegios para acceder a determinado sistema la opción se muestra habilitada, en caso contrario la opción se encuentra deshabilitada (en color gris) y no se puede seleccionar.

Modo de acceso: A partir de la pantalla principal dar un clic en la opción Aplicaciones del menú principal (Fig. 2i), para mandar llamar alguna aplicación dar un clic sobre el nombre de la aplicación.

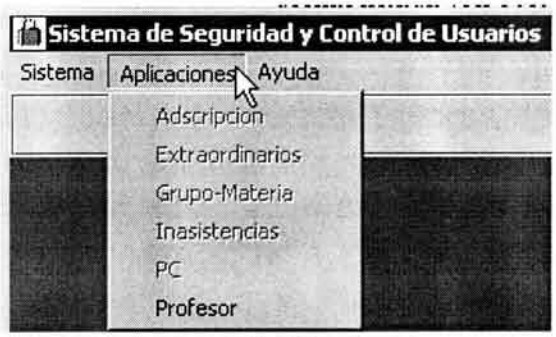


Fig. 2i

Pantalla 2.9 Menú Ayuda de la pantalla principal

Proceso: Mostrar información acerca del sistema y la ayuda en línea del mismo.

Descripción: Esta opción permite mostrar la pantalla *Acerca de* y la ayuda en línea del sistema.

Modo de acceso: A partir de la pantalla principal dar un clic en la opción Ayuda del menú principal (Fig. 2j).

Fig. 2j

Pantalla 2.10 Menú Ayuda > Acerca de

Proceso: Mostrar la pantalla *Acerca de.*

Descripción: Esta opción permite mostrar la pantalla *Acerca de*, dicha pantalla muestra información relacionada con el sistema como el nombre de la institución y el nombre del desarrollador del sistema.

Modo de acceso: A partir de la pantalla principal dar un clic en la opción Sistema del menú principal, seleccionar la opción Acerca de (Fig. 2k).

Fig. 2k

Pantalla 2.11 Menú Ayuda > Contenido

Proceso: Mostrar la ayuda en línea del sistema.

Descripción: Esta opción permite mostrar la ayuda en línea del sistema.

Modo de acceso: A partir de la pantalla principal dar un clic en la opción Sistema del menú principal, seleccionar Contenido (Fig. 2l).

Fig. 2l

Pantalla 3. *Pantalla Mantenimiento de Usuarios*

Proceso: Administración de las cuentas de usuario.

Descripción: Esta pantalla muestran las cuentas de usuario creadas y eliminadas. Se encuentra dividida en dos secciones una en la que muestra los usuarios activos y otra los usuarios eliminados, en la sección de usuarios activos se pueden realizar diversas operaciones sobre los usuarios del sistema, como agregar un usuario nuevo, modificar los datos de un usuario existente, eliminar a un usuario, agregar a un usuario que existe en el sistema pero no en nuestra aplicación, cambiar la contraseña de un usuario, deshabilitar y habilitar la cuenta de un usuario y ver el historial de los usuarios; y en la sección de usuarios eliminados solamente se puede consultar el historial de dichos usuarios.

Modo de acceso: A partir de la pantalla principal dar un clic en la opción Sistema del menú principal y seleccionar Mantenimiento de Usuarios.

Modo de uso:

3. Al mostrarse la pantalla *Mantenimiento de Usuarios* seleccionar una de las pestañas que dividen la pantalla, si se selecciona la pestaña Usuarios Activos (Fig. 3a). al dar un clic en el menú Operaciones aparecerá una lista con las opciones disponibles, si se selecciona la pestaña Usuarios Eliminados (Fig. 3b). El menú Operaciones aparecerá deshabilitado, la única operación disponible es consultar el historial de un usuario mediante el botón Historial.
4. Dar un clic en el menú o botón de interés, después de seleccionar una cuenta de usuario.

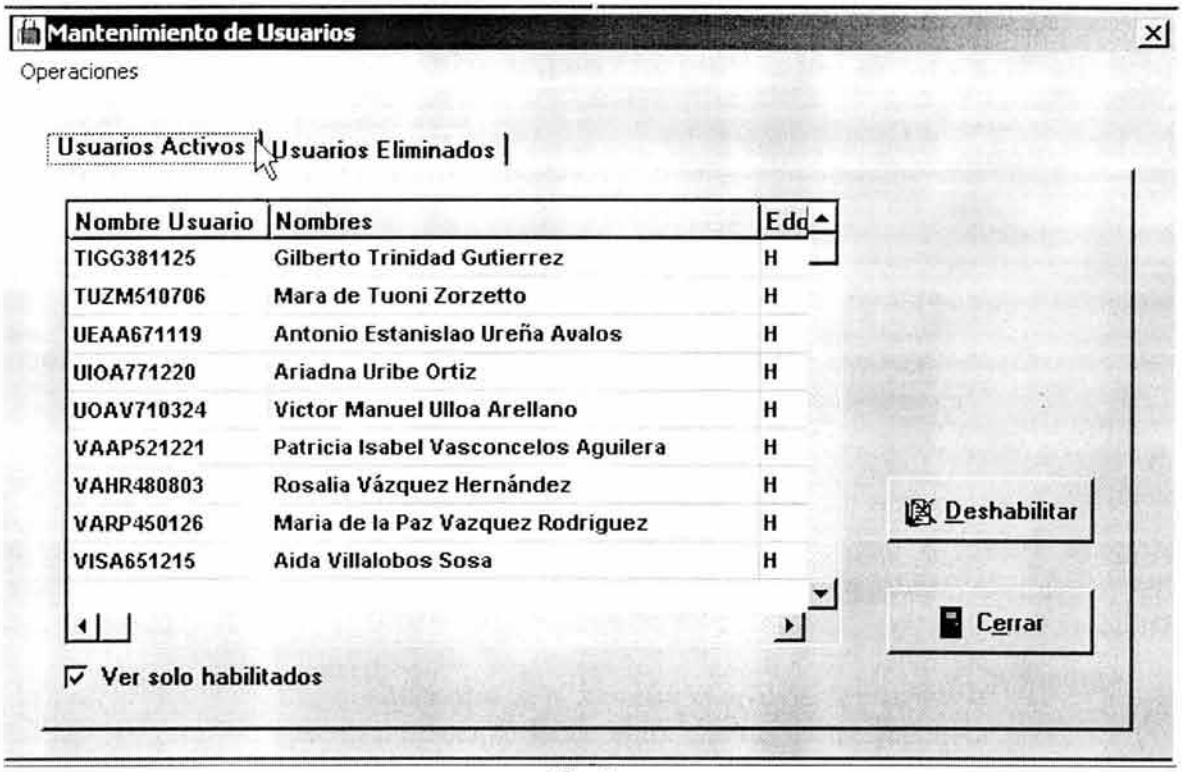

Mantenimiento de Usuarios
Operaciones
Usuarios Activos
Usuarios Eliminados
Nombre Usuario
Nombres
Edo
TIGG381125 Gilberto Trinidad Gutierrez H
TUZM510706 Mara de Tuoni Zorzetto H
UEAA671119 Antonio Estanislao Ureña Avalos H
UIOA771220 Ariadna Uribe Ortiz H
UOAV710324 Victor Manuel Ulloa Arellano H
VAAP521221 Patricia Isabel Vasconcelos Aguilera H
VAHR480803 Rosalia Vázquez Hernández H
VARP450126 Maria de la Paz Vazquez Rodriguez H
VISA651215 Aida Villalobos Sosa H
Deshabilitar
Cerrar
Ver solo habilitados

Fig. 3a

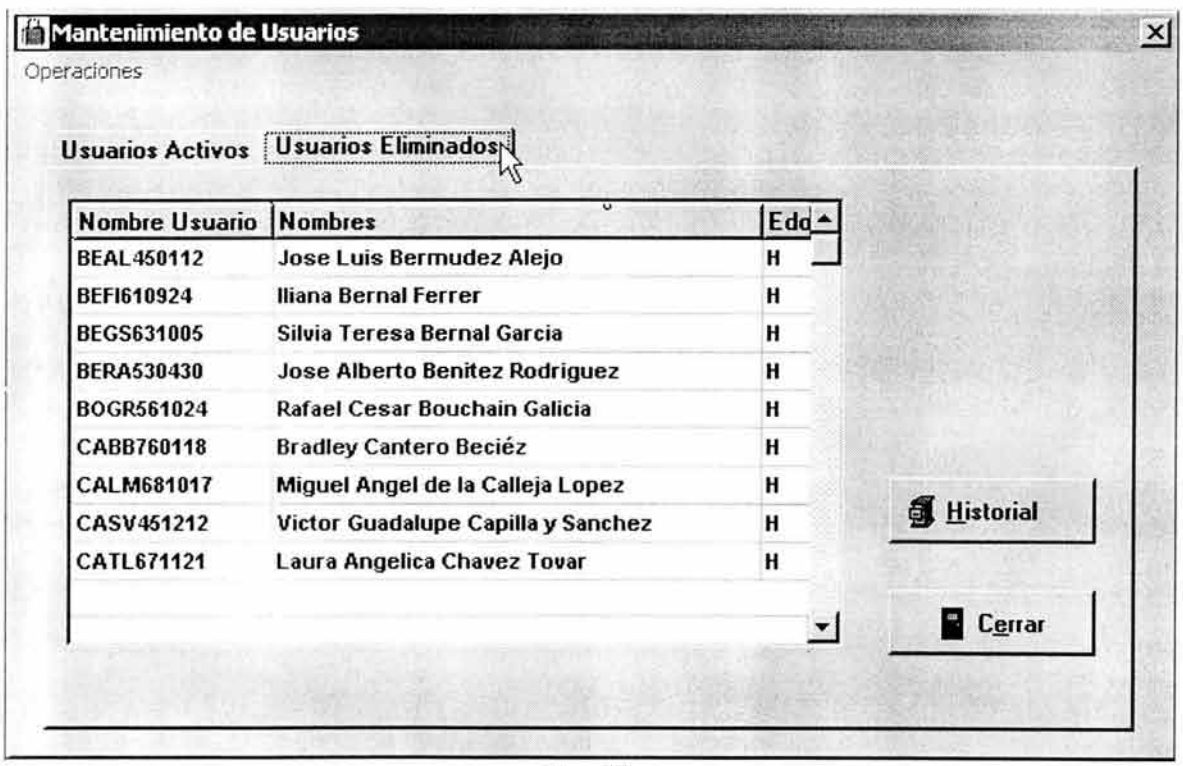

Mantenimiento de Usuarios
Operaciones
Usuarios Activos
Usuarios Eliminados
Nombre Usuario
Nombres
Edo
BEAL450112 Jose Luis Bermudez Alejo H
BEFI610924 Iliana Bernal Ferrer H
BEGS631005 Silvia Teresa Bernal Garcia H
BERA530430 Jose Alberto Benitez Rodriguez H
BOGR561024 Rafael Cesar Bouchain Galicia H
CABB760118 Bradley Cantero Beciéz H
CALM681017 Miguel Angel de la Calleja Lopez H
CASV451212 Victor Guadalupe Capilla y Sanchez H
CATL671121 Laura Angelica Chavez Tovar H
Historial
Cerrar

Fig. 3b

A continuación se describen los procesos que se pueden realizar desde la pantalla de *Mantenimiento de Usuarios*.

Pantalla 3.1 Deshabilitar usuario

1. Para deshabilitar la cuenta de un usuario se selecciona la pestaña Usuarios Activos.
2. Se selecciona la cuenta a deshabilitar (Fig. 3c), dando un clic sobre la cuenta de usuario en la cuadricula, en caso de que no se muestre la cuenta a deshabilitar puede revisarse las cuentas en la cuadricula mediante la barra de desplazamiento que se encuentra a la derecha.
3. Dar un clic en el botón Deshabilitar 

.

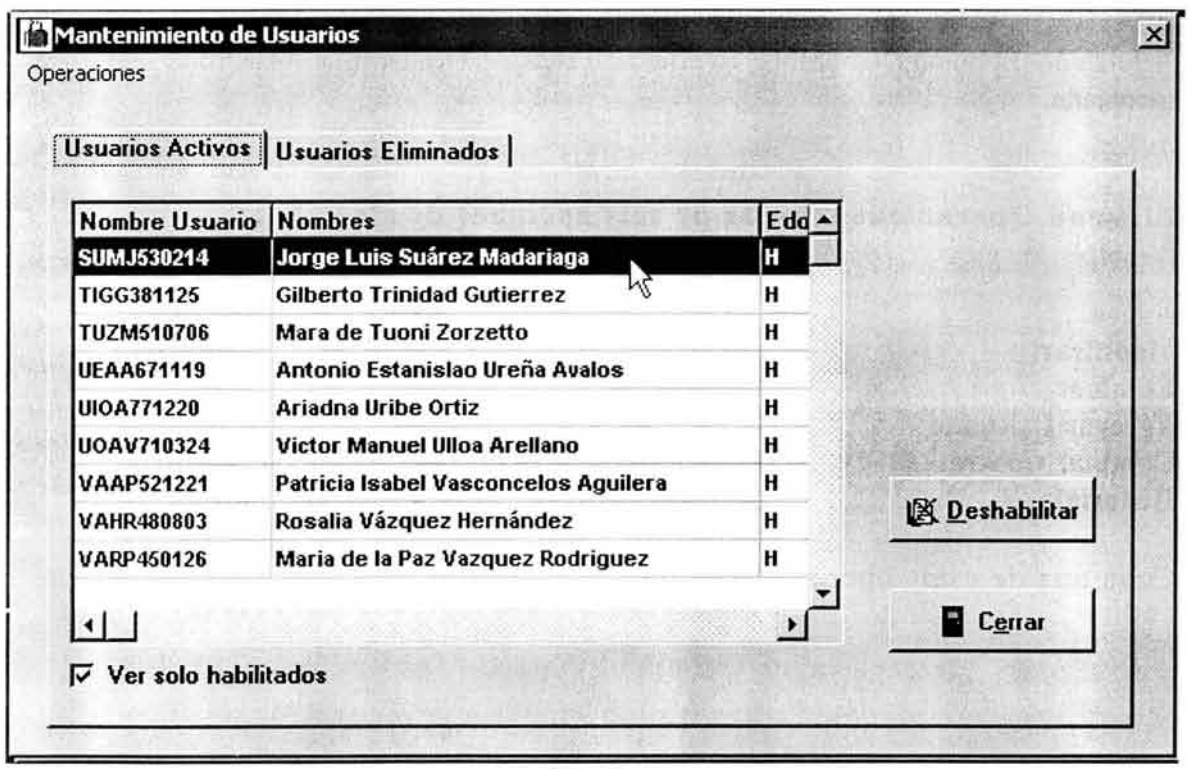


Fig. 3c

Pantalla 3.2 Habilitar usuario

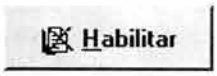
1. Para habilitar la cuenta de un usuario se selecciona la opción Usuarios Activos.
2. Para ver las cuentas de usuario deshabilitadas, la casilla Ver solo habilitados debe estar desmarcada (Fig. 3d), en caso de encontrarse marcada esta casilla (Fig. 3e), dar un clic sobre ella.
3. Se selecciona la cuenta a habilitar, dando un clic sobre la cuenta de usuario en la cuadricula, como el la figura 3c.
4. Dar un clic en el botón que ahora muestra el mensaje 

Fig. 3d

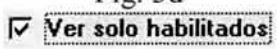


Fig. 3e

Aclaración: El botón Deshabilitar cambia su mensaje a Deshabilitar o Habilitar según sea apropiado.

El menú Operaciones consta de seis opciones de elección:

Nuevo
Modificar
Eliminar
Agregar Existente
Cambiar Contraseña
Historial

Cada una de estas opciones y lo que contienen se describe a continuación.

Pantalla 3.3 Menú Operaciones de la pantalla Mantenimiento de Usuarios

Proceso: Presentar las opciones Nuevo, Modificar, Eliminar, Agregar Existente, Cambiar Contraseña, Historial.

Descripción: Presentar diversas operaciones que se emplean para administrar las cuentas de los usuarios.

Modo de acceso: A partir de la pantalla *Mantenimiento de Usuarios* dar un clic en el menú Operaciones (Fig. 3f).

Fig. 3f

Pantalla 3.4 Menú Operaciones > Nuevo

Proceso: Mostrar la pantalla *Nuevo Usuario.*

Descripción: Esta opción permite mostrar la pantalla *Nuevo Usuario*, para mostrar la pantalla no es necesario haber seleccionado ninguna cuenta del usuario.

Modo de acceso: A partir de la pantalla *Mantenimiento de Usuarios* dar un clic en el menú Operaciones, seleccionar Nuevo (Fig. 3g), o pulsar la combinación de teclas Ctrl+N.

Fig. 3g

Pantalla 3.5 Menú Operaciones > Modificar

Proceso: Mostrar la pantalla que se encarga de la modificación de los datos y roles de un usuario.

Descripción: Esta opción permite mostrar la pantalla *Modificación del usuario*, para modificar los datos o roles de un usuario es necesario seleccionar previamente la cuenta del usuario a modificar.

Modo de acceso: En la pantalla *Mantenimiento de Usuarios* seleccionar la cuenta del usuario a modificar, dar un clic en el menú Operaciones, seleccionar Modificar (Fig. 3h), o pulsar la combinación de teclas Ctrl+M.

Fig. 3h

Pantalla 3.6 Menú Operaciones > Eliminar

Proceso: Eliminar la cuenta de un usuario.

Descripción: Esta opción permite eliminar un usuario de nuestra aplicación.

Modo de acceso: En la pantalla *Mantenimiento de Usuarios* seleccionar la cuenta del usuario a eliminar, dar un clic en el menú Operaciones, seleccionar Eliminar (Fig. 3i), o pulsar la combinación de teclas Ctrl+L.

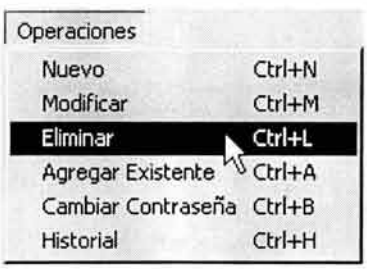


Fig. 3i

Modo de uso:

1. En la pantalla *Mantenimiento de Usuarios* seleccionar la cuenta del usuario a eliminar.
2. En el menú Operaciones, seleccionar Eliminar (Fig. 3i)
3. Confirmar o cancelar la eliminación(Fig. 3j).

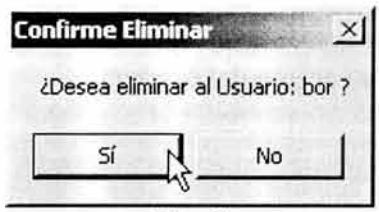


Fig. 3j

Pantalla 3.7 Menú Operaciones > Agregar Existente

Proceso: Mostrar la pantalla *Agregar Usuarios Existentes*.

Descripción: Esta opción permite mostrar la pantalla *Agregar Usuarios Existentes*, para mostrar la pantalla no es necesario haber seleccionado ninguna cuenta del usuario.

Modo de acceso: A partir de la pantalla *Mantenimiento de Usuarios* dar un clic en el menú Operaciones, seleccionar Agregar Existente (Fig. 3k), o pulsar la combinación de teclas Ctrl+A.

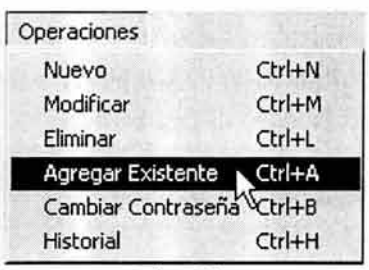


Fig. 3k

Pantalla 3.8 Menú Operaciones > Cambiar Contraseña

Proceso: Mostrar la pantalla *Cambio de Contraseña.*

Descripción: Esta opción permite mostrar la pantalla *Cambio de Contraseña*, para cambiar la contraseña de un usuario es necesario seleccionar previamente la cuenta del usuario.

Modo de acceso: En la pantalla *Mantenimiento de Usuarios* seleccionar el usuario al que se va a cambiar su contraseña, dar un clic en el menú Operaciones, seleccionar Cambiar Contraseña (Fig. 3l), o pulsar la combinación de teclas Ctrl+B.

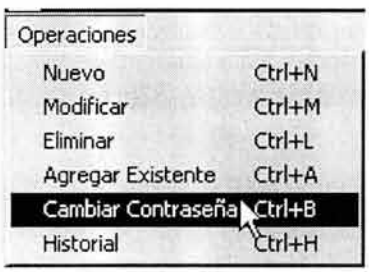


Fig. 3l

Pantalla 3.9 Menú Operaciones > Historial.

Proceso: Mostrar la pantalla *Historial del Usuario.*

Descripción: Esta opción permite mostrar la pantalla *Historial del Usuario*, en donde se puede consultar cuando ingresó el usuario al sistema, para consultar el historial de un usuario es necesario seleccionar previamente la cuenta del usuario.

Modo de acceso: A partir de la pantalla *Mantenimiento de Usuarios* dar un clic en el menú Operaciones, seleccionar Historial (Fig. 3m), o pulsar la combinación de teclas Ctrl+H.

Fig. 3m

Pantalla 4. *Pantalla Nuevo Usuario*

Proceso: Agregar un nuevo usuario.

Descripción: Esta pantalla nos permite dar de alta a un nuevo usuario en nuestro sistema. Después de llenar los datos requeridos se crea el usuario dando un clic en el botón Guardar.

Modo de acceso: A partir de la pantalla *Mantenimiento de Usuarios* dar un clic en la opción Nuevo del menú Operaciones.

Modo de uso: Para crear una nueva cuenta de usuario se realiza el siguiente procedimiento:

5. Al mostrarse la pantalla *Nuevo Usuario* (Fig. 4a). Seleccionar la Adscripción a la que pertenece el usuario en el cuadro combinado Adscripción.
6. Seleccionar el cargo del usuario en el cuadro combinado Cargo.
7. Escribir el nombre del usuario en la caja de texto Nombre(s).
8. Escribir los apellidos del usuario en la caja de texto Apellidos.
9. Escribir el teléfono del usuario en la caja de texto Extensión (El llenar esta caja de texto es opcional).
10. Marcar la casilla Habilitado, si se quiere que la cuenta se cree como habilitada.
11. Escribir el nombre de usuario (el nombre con el que se identificara ante el sistema) en la caja de texto Nombre de Usuario (Alias).
12. Escribir la contraseña del usuario en la caja de texto Contraseña.
13. Escribir la contraseña ahora en la caja de texto Confirmar Contraseña.
14. Después de capturar la información en la pantalla (Fig. 4b), dar un clic en el botón Guardar.

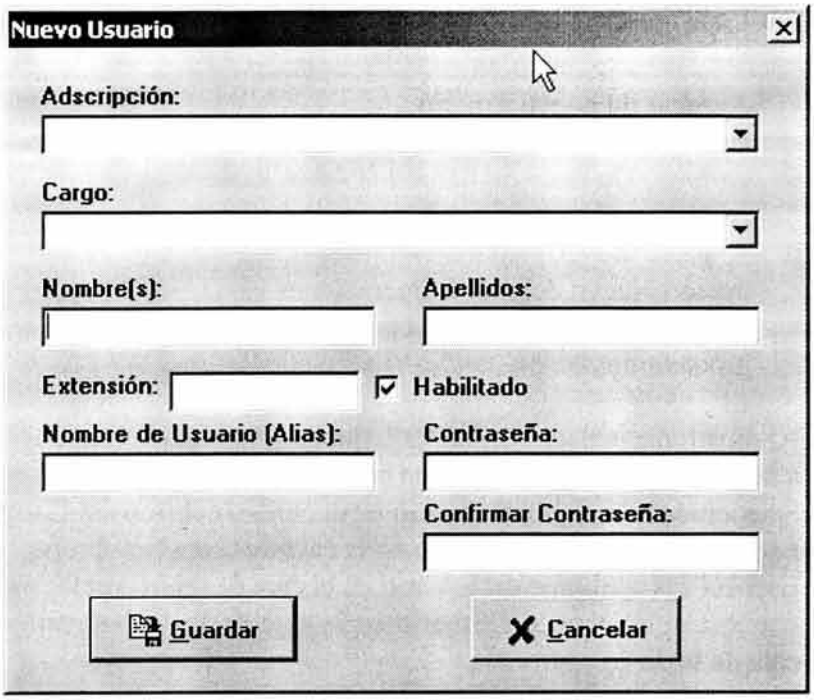

Nuevo Usuario
Adscripción:
Cargo:
Nombre(s):
Apellidos:
Extensión:
Habilitado
Nombre de Usuario (Alias):
Contraseña:
Confirmar Contraseña:
Guardar
Cancelar

Fig. 4a

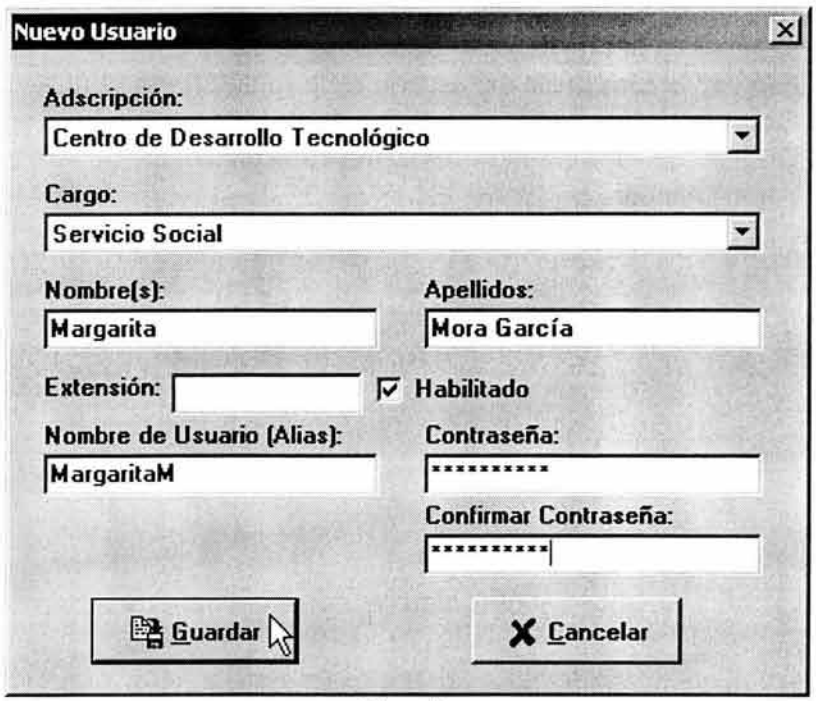

Nuevo Usuario
Adscripción:
Centro de Desarrollo Tecnológico
Cargo:
Servicio Social
Nombre(s):
Margarita
Apellidos:
Mora García
Extensión:
Habilitado
Nombre de Usuario (Alias):
MargaritaM
Contraseña:
Confirmar Contraseña:
Guardar
Cancelar

Fig. 4b

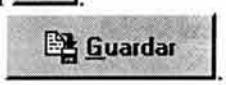
Pantalla 5. *Pantalla Modificación del usuario*

Proceso: Modificar los datos o roles de un usuario.

Descripción: Esta pantalla nos permite modificar o actualizar los datos de un usuario como la adscripción a la cual pertenece, el cargo que tiene, su número telefónico su nombre y apellidos, además de permitir cambiar su estado a habilitado o deshabilitado, pero el nombre de usuario no puede ser modificado, además nos permite asignar o quitar roles al usuario.

Modo de acceso: En la pantalla *Mantenimiento de Usuarios* seleccionar el usuario a modificar, en el menú Operaciones dar un clic en la opción Modificar.

Modo de uso: Para modificar los datos de un usuario o sus roles se realiza el siguiente procedimiento:

1. Después de mostrarse la pantalla *Modificar Usuario* (Fig. 5a). Cambiar los datos del usuario.
2. Para agregar roles al usuario se seleccionan de la lista Roles disponibles (Fig. 5b), dar un clic en el botón  .
3. Para quitarle roles al usuario se seleccionan de la lista Roles asignados (Fig. 5c), dar un clic en el botón  .
4. Dar un clic en el botón Guardar  .

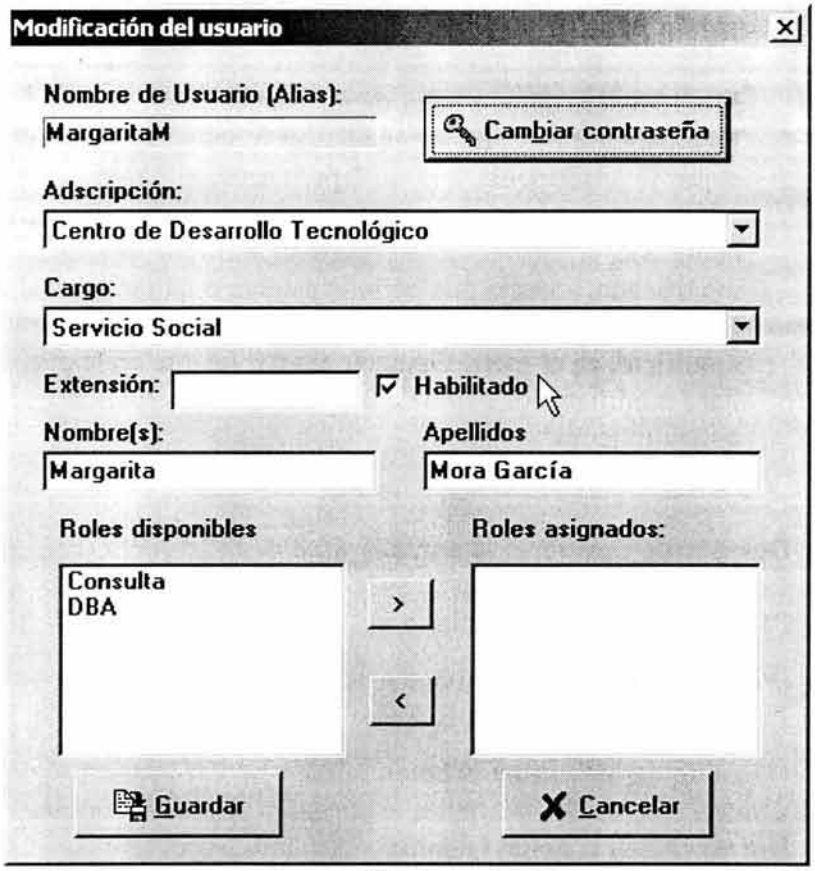


Fig. 5a

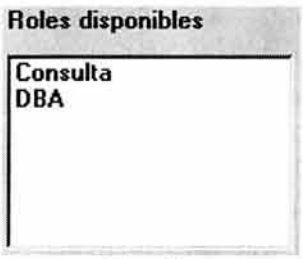


Fig. 5b

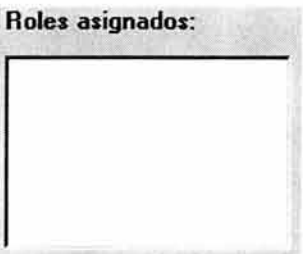
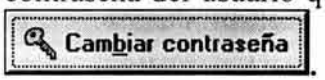


Fig. 5c

Modo de uso: Para mostrar la pantalla *Cambio de Contraseña*, para modificar la contraseña del usuario que se está modificando, dar un clic en el botón 

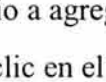
Pantalla 6. *Pantalla Agregar Usuarios Existentes*

Proceso: Añadir un usuario de otra aplicación.

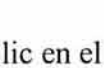
Descripción: Esta pantalla nos permite agregar a usuarios que han sido dados de alta para otra aplicación, o eliminar usuarios que tenemos dados de alta en nuestra aplicación.

Modo de acceso: En la pantalla *Mantenimiento de Usuarios*, en el menú Operaciones dar un clic en la opción Agregar Existente.

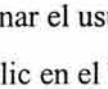
Modo de uso: Para añadir un usuario de otra aplicación se realiza siguiente procedimiento:

1. Al mostrarse la pantalla *Agregar Usuarios Existentes* (Fig. 6a). Seleccionar el usuario a agregar de la lista Usuarios externos (Fig. 6b).
2. Dar un clic en el botón 
.

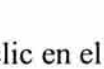
Modo de uso: Para añadir todos los usuarios de otra aplicación se realiza siguiente procedimiento:

1. Dar un clic en el botón 
.

Modo de uso: Para eliminar un usuario de la aplicación actual se realiza siguiente procedimiento:

1. Seleccionar el usuario a eliminar de la lista Usuarios actuales (Fig. 6c).
2. Dar un clic en el botón 
.

Modo de uso: Para eliminar a todos los usuarios de la aplicación actual (excepto al administrador del sistema) se realiza siguiente procedimiento:

1. Dar un clic en el botón 
.

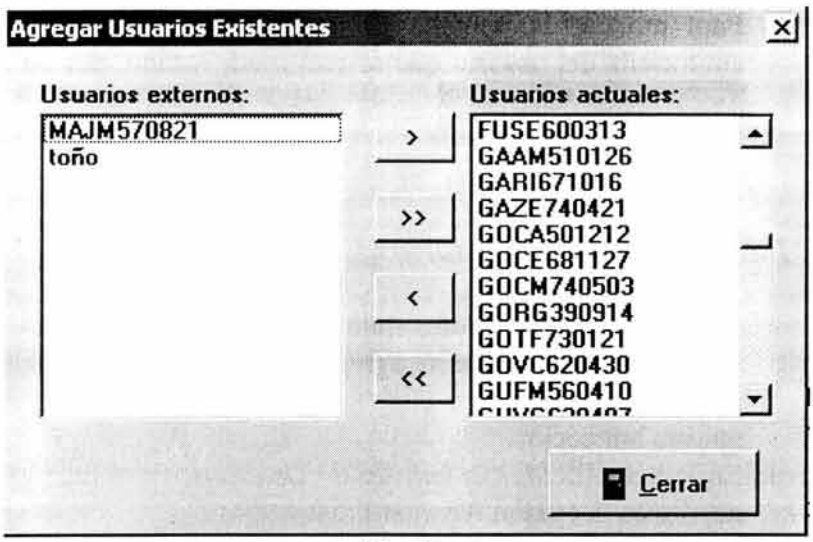


Fig. 6a

Fig. 6b

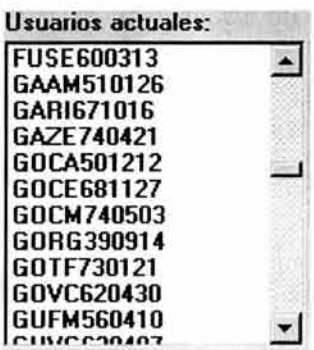


Fig. 6c

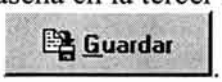
Pantalla 7. *Pantalla Cambio de Contraseña*

Proceso: Cambiar la contraseña de un usuario.

Descripción: Esta pantalla sirve para cambiar la contraseña de un usuario, para cambiar la contraseña de un usuario se necesita saber la contraseña actual del usuario, si se manda llamar a la pantalla *Cambio de Contraseña* desde la pantalla de *Mantenimiento de Usuarios* es necesario seleccionar previamente la cuenta del usuario, si se manda llamar desde la pantalla *Modificación del usuario* se cambiara la contraseña del usuario que se este modificando.

Modo de acceso: En la pantalla *Mantenimiento de Usuarios* seleccionar el usuario al que se va a cambiar su contraseña, dar un clic en el menú Operaciones, seleccionar Cambiar Contraseña (Fig. 3l), o pulsar la combinación de teclas Ctrl+B, o en la pantalla *Modificación del usuario* dar un clic en el botón Cambiar contraseña.

Modo de uso: Para cambiar la contraseña de un usuario se realiza siguiente procedimiento:

1. Al mostrarse la pantalla *Cambio de Contraseña* (Fig. 7a). Se escribe la contraseña actual en la primer caja de texto.
2. Escribir la nueva contraseña en la segunda caja de texto.
3. Escribir la nueva contraseña en la tercer caja de texto.
4. Dar un clic en el botón 

.

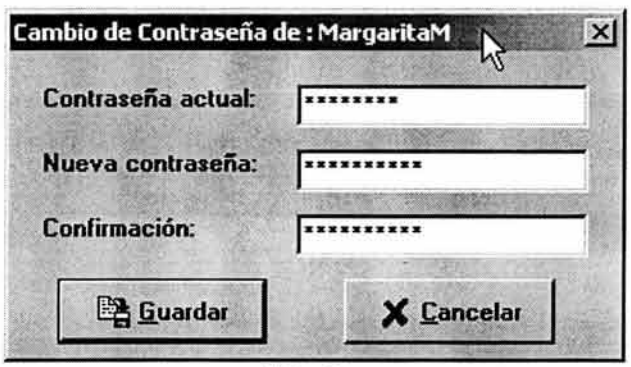


Fig. 7a

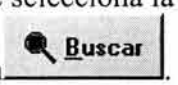
Pantalla 8. *Pantalla Historial del Usuario*

Proceso: Mostrar el historial un usuario.

Descripción: Esta pantalla muestra el Historial del Usuario, es decir cuando ingresó el usuario en nuestro o en otro sistema, para consultar el historial de un usuario es necesario seleccionar previamente la cuenta del usuario.

Modo de acceso: A partir de la pantalla *Mantenimiento de Usuarios* seleccionar el usuario dar un clic en el menú Operaciones, seleccionar Historial.

Modo de uso: Para consultar el historial de un usuario se realiza siguiente procedimiento:

1. Al mostrarse la pantalla *Historial del Usuario* (Fig. 8a). se muestra el usuario seleccionado, si se desea consulta el historial del usuario en la aplicación actual se selecciona la opción Actual.
2. Si se desea consulta el historial del usuario en todas las aplicaciones incluyendo la actual se selecciona la opción Todas.
3. Dar un clic en el botón 

.

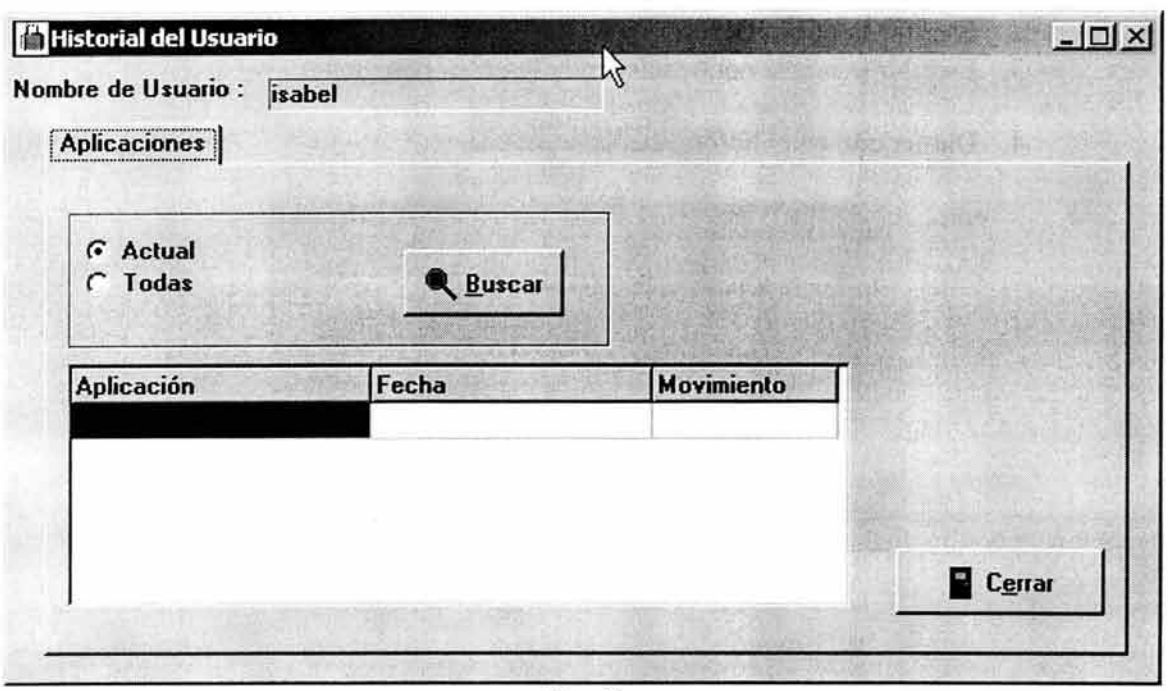


Fig. 8a

Pantalla 9. *Pantalla Administración de privilegios*

Proceso: Administrar los roles y los privilegios de la aplicación.

Descripción: Esta pantalla sirve para administrar los roles de la base de datos, realizando diversas operaciones como crear y eliminar roles y añadirles o quitarles privilegios, la pantalla se encuentra dividida en dos partes las cuales son Roles de la Aplicación y Privilegios de los roles.

Modo de acceso: A partir de la pantalla principal dar un clic en la opción Sistema del menú principal y seleccionar Administración de privilegios.

Modo de uso: A continuación se explican los procesos que pueden realizarse en la parte Roles de la Aplicación de la pantalla. Para crear un nuevo rol se realiza el siguiente proceso.

15. Al mostrarse la pantalla *Administración de privilegios* seleccionar la pestaña Roles de la Aplicación (Fig. 9a).
16. Dar un clic en el botón Nuevo, para mostrar la pantalla *Añadir Rol* (Fig. 9b).
17. En la pantalla *Añadir Rol* escribir el nombre del nuevo Rol, o seleccionamos uno de los disponibles.
18. Dar un clic en el botón Guardar para crear el rol.
19. Después de pulsar el botón Guardar la pantalla *Añadir Rol* se cierra y volvemos a la pantalla *Administración de privilegios*.

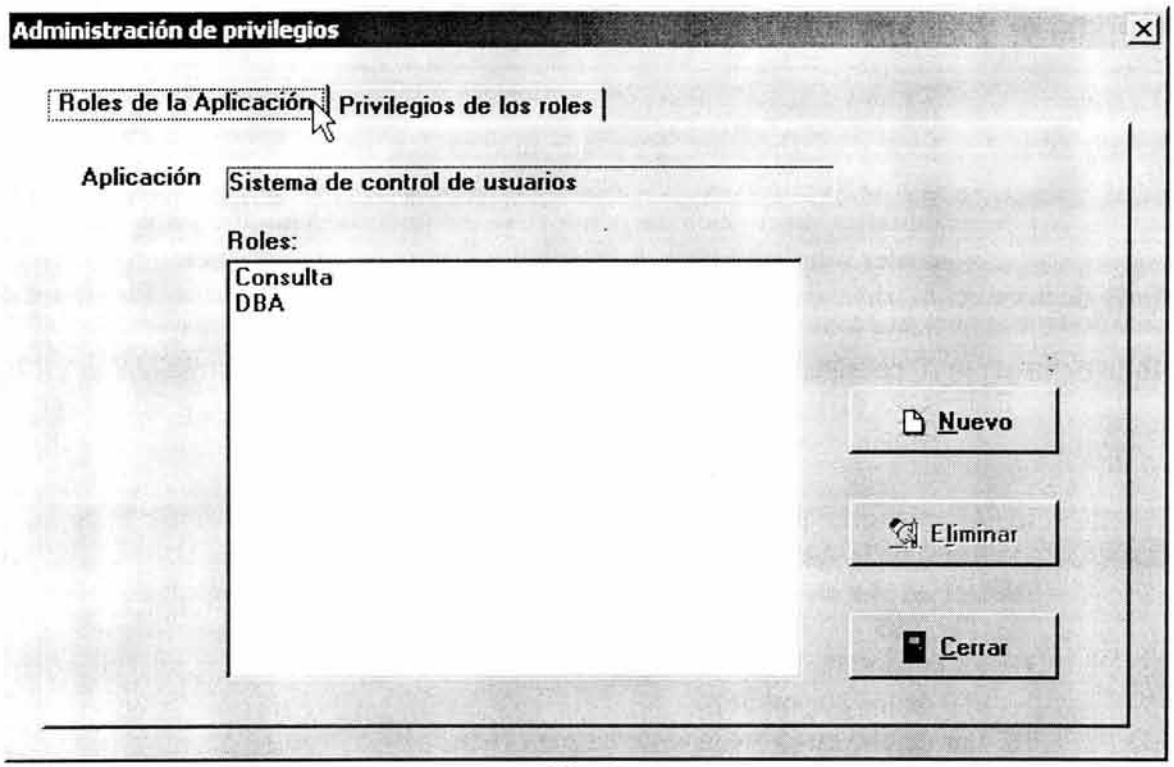


Fig. 9a

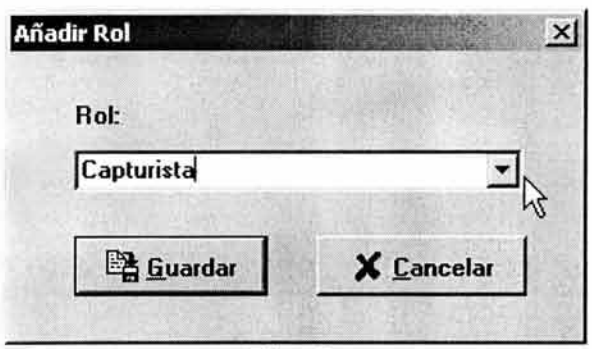


Fig. 9b

Modo de uso: Para eliminar un rol se realiza el siguiente proceso.

1. Al mostrarse la pantalla *Administración de privilegios* seleccionar la pestaña Roles de la Aplicación (Fig. 9a).
2. Seleccionar el rol a eliminar en la lista Roles.
3. Al hacer esto el botón Eliminar cambia su estado de deshabilitado a habilitado
4. Dar un clic en el botón Eliminar (Fig. 9c).
5. Confirmar la eliminación del rol (Fig. 9d).

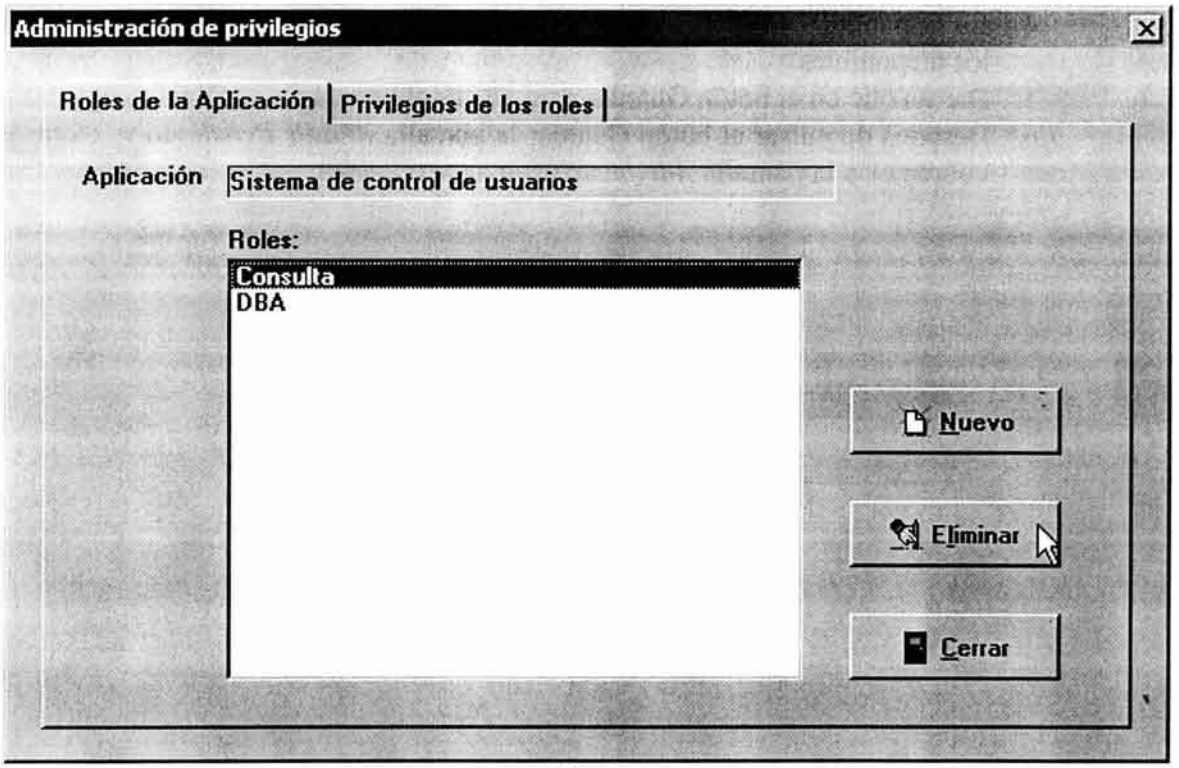


Fig. 9c

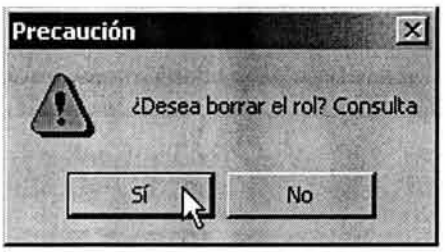


Fig. 9d

Modo de uso: A continuación se explican los procesos que pueden realizarse en la parte Privilegios de los roles de la pantalla. Para agregar un privilegio a un rol se realiza el siguiente proceso.

1. Al mostrarse la pantalla *Administración de privilegios* seleccionar la pestaña Privilegios de los roles (Fig. 9e).
2. Seleccionar el rol del cuadro combinado Rol.
3. Dar un clic en el botón Nuevo (Fig. 9f). Con lo que se muestra la pantalla *Añadir Privilegio.*

4. En la pantalla *Añadir Privilegio* escribir el privilegio, o seleccionar uno de los disponibles.
5. Dar un clic en el botón Guardar para añadir el privilegio al rol (Fig. 9g).
6. Después de pulsar el botón Guardar la pantalla *Añadir Privilegio* se cierra y volvemos a la pantalla *Administración de privilegios*.

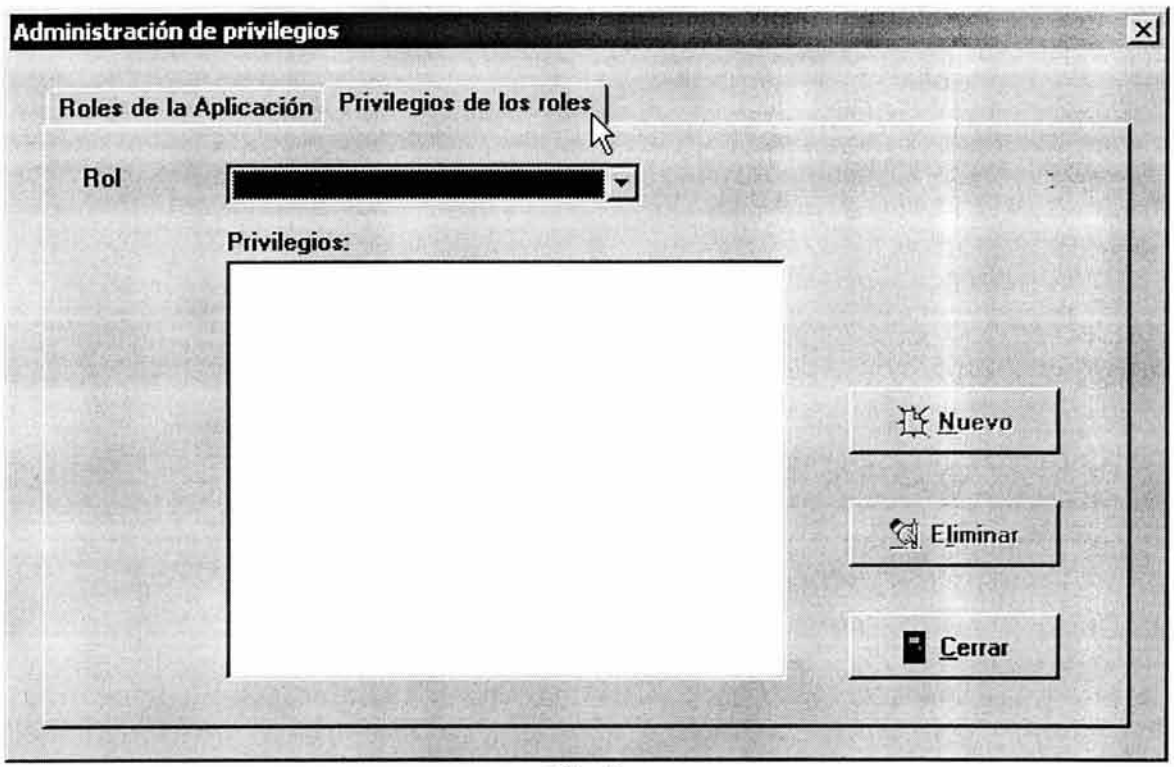


Fig. 9e

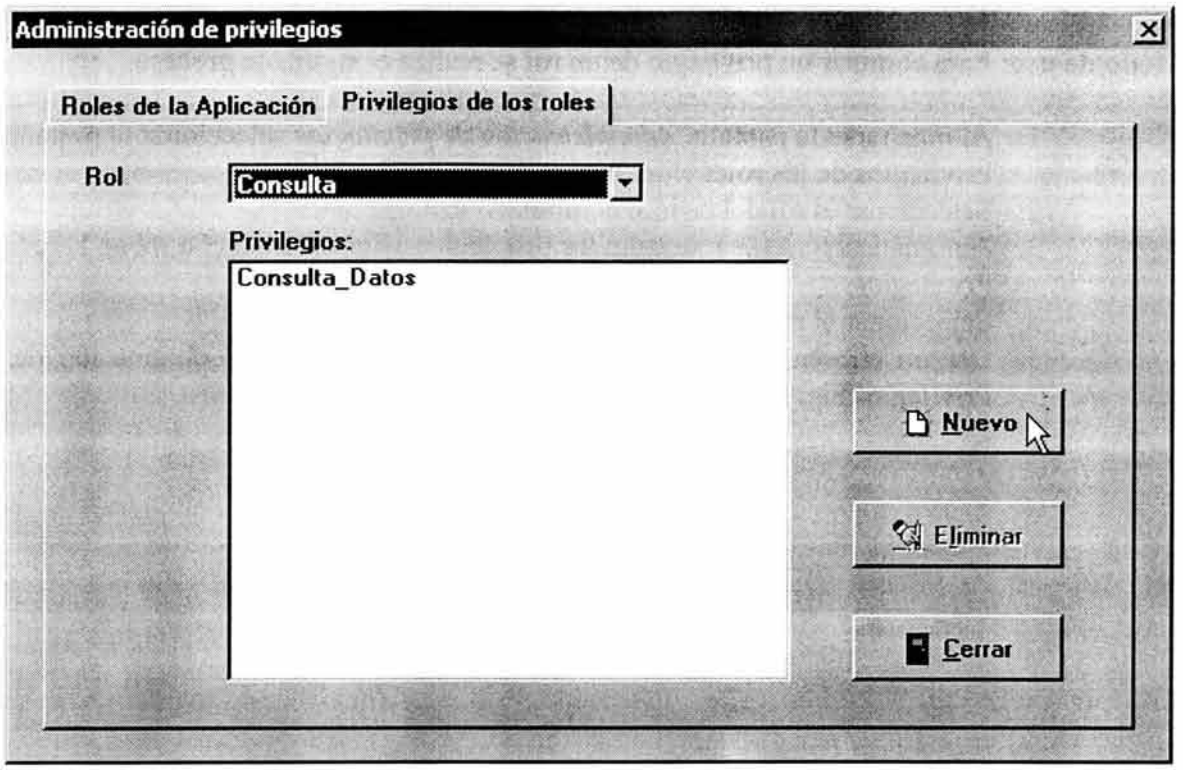

Administración de privilegios
Roles de la Aplicación
Privilegios de los roles
Rol
Consulta
Privilegios:
Consulta_Datos
Nuevo
Eliminar
Cerrar

Fig. 9f

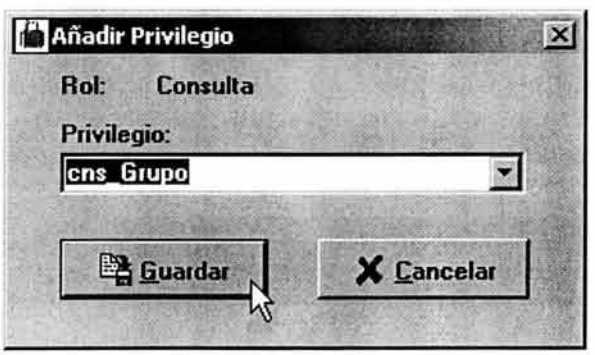

Añadir Privilegio
Rol: Consulta
Privilegio:
cns_Grupo
Guardar
Cancelar

Fig. 9g

Modo de uso: Para eliminar un privilegio de un rol se realiza el siguiente proceso.

1. Al mostrarse la pantalla *Administración de privilegios* seleccionar la pestaña Privilegios de los roles (Fig. 9e).
2. Seleccionar el rol del cuadro combinado Rol.
3. Automáticamente se muestran los privilegios asignados a dicho rol en la lista Privilegios.
4. Seleccionar el privilegio a eliminar en la lista Privilegios.
5. Dar un clic en el botón Eliminar (Fig. 9h).Confirmar la eliminación del Privilegio (Fig. 9i).

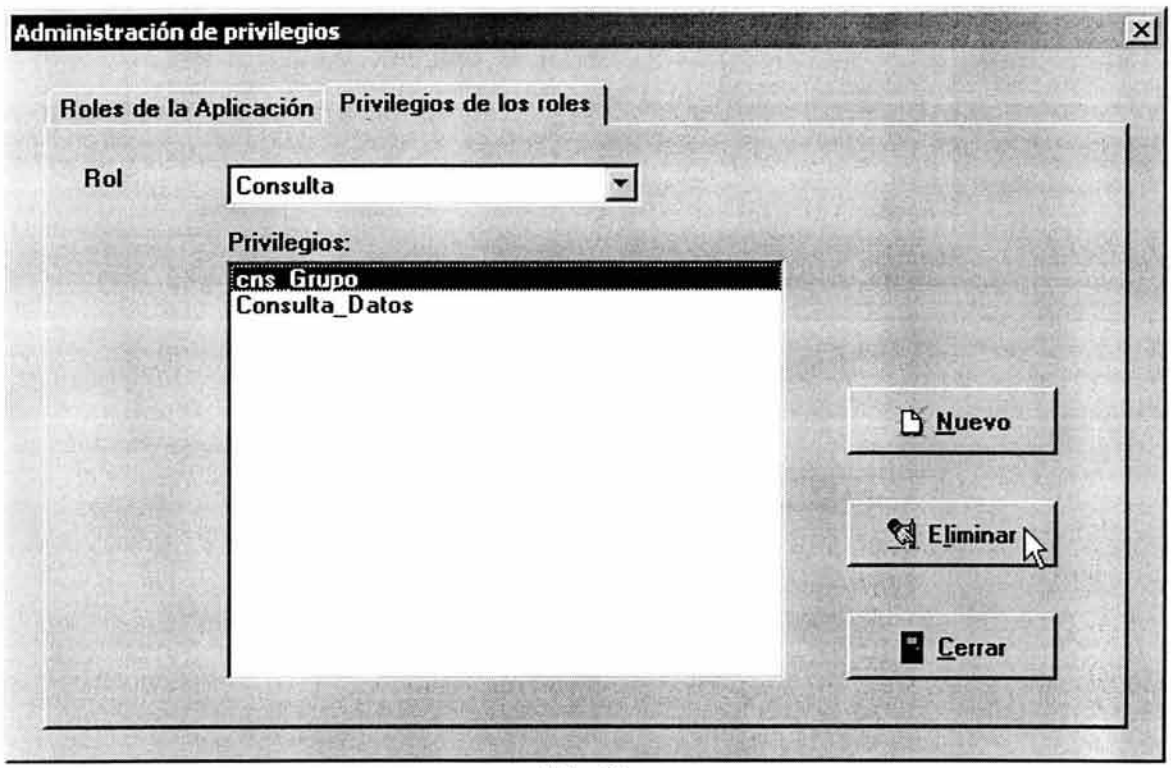


Fig. 9h

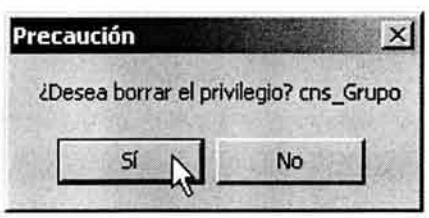


Fig. 9i

Pantalla 10. *Pantalla Impresión de reportes*

Proceso: Imprimir los usuarios que existen en el sistema.

Descripción: Esta pantalla sirve para imprimir los usuarios que tenemos dados de alta en nuestra aplicación y los roles que tienen asignados.

Modo de acceso: A partir de la pantalla principal dar un clic en la opción Sistema del menú principal y seleccionar Reporte de Usuarios.

Modo de uso:

1. Al mostrarse la pantalla *Impresión de reportes* (Fig. 10a).
2. Dar un clic en el menú Reportes.
3. Seleccionar la opción Reporte de Usuarios.
4. Al seleccionar la opción Reporte de Usuarios se despliega un submenú que tiene las opciones Ordenados por adscripción y Ordenados por nombre.
5. Seleccionar el submenú Ordenados por adscripción (Fig. 10b), o el submenú Ordenados por nombre (Fig. 10c).

Fig. 10a

Fig. 10b

Fig. 10c

Pantalla 11. *Pantalla Acerca de*

Proceso: Mostrar la pantalla *Acerca de*.

Descripción: La pantalla *Acerca de* (Fig. 11a) muestra información relacionada con el sistema como el nombre de la institución y el nombre del desarrollador del sistema.

Modo de acceso: A partir de la pantalla principal dar un clic en la opción Ayuda del menú principal, dar un clic en la opción Acerca de.

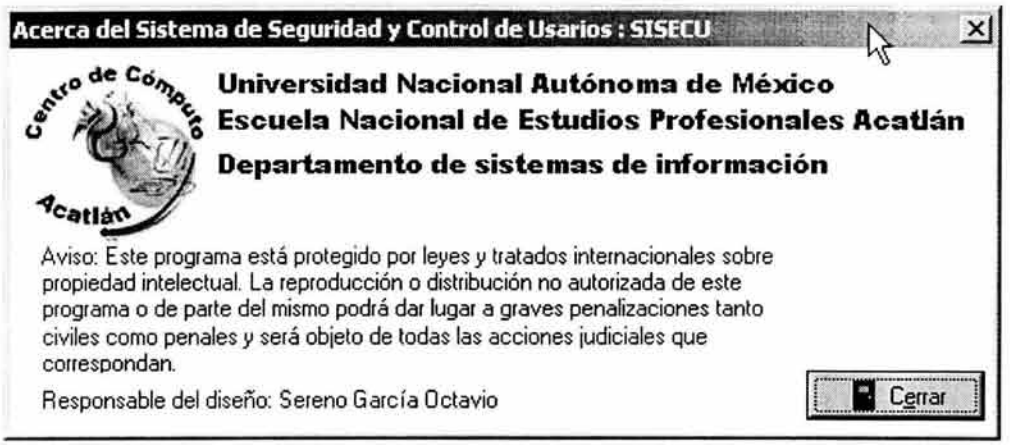


Fig. 11a

Pantalla 12. *Pantalla Temas de Ayuda: Sistema de Seguridad*

Proceso: Mostrar la pantalla *Temas de Ayuda*: Sistema de Seguridad.
Descripción: Esta pantalla muestra la ayuda en línea del sistema (Fig. 12a).
Modo de acceso: A partir de la pantalla principal dar un clic en la opción Ayuda del menú principal, dar un clic en la opción Contenido.

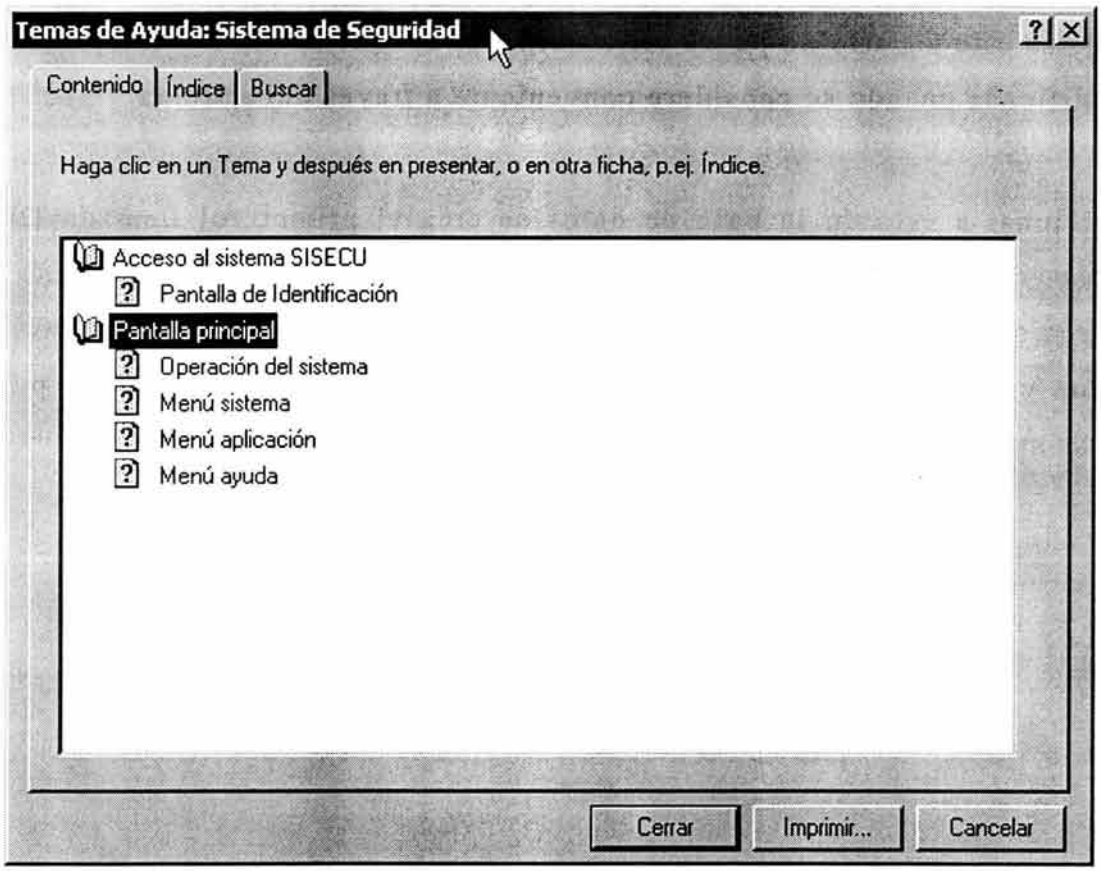


Fig. 12a

4.6 Administración del sistema

Al iniciar por primera vez el sistema se crea a un usuario el cuál tiene permisos o privilegios para crear nuevos usuarios a los que les asignará permisos a través del sistema de seguridad, dicho usuario es el administrador del sistema. Por lo que cuenta con acceso total al sistema, además este usuario no podrá ser eliminado, aunque su contraseña puede ser modificada cuando se considere conveniente a través del sistema.

Adicional a esto en la base de datos se crea el primer rol llamado DBA, dicho rol se asigna al administrador del sistema y le da acceso de seleccionar, insertar o actualizar datos en todas las tablas de la base de datos y a todas las pantallas del sistema SISECU, el administrador puede crear nuevos roles con menos permisos para asignar a los usuarios.

Conclusiones

En conclusión la informática se encuentra en una etapa de constante avance, esto trae consigo nuevas herramientas que pueden ayudar en el desarrollo de los sistemas computacionales, pero, para asegurarnos de que la información es confiable es necesario, además de utilizar dichas herramientas eficazmente, establecer medidas de seguridad para salvaguardar la información. De no hacerlo, el lugar donde se centraliza la información, con frecuencia un centro de cómputo, puede ser el activo más valioso y al mismo tiempo el más vulnerable.

El objetivo básico del Sistema de Seguridad es, como se señala al inicio de este trabajo, permitir el acceso a la información solamente a los usuarios autorizados. Dicho objetivo se ha cumplido plenamente y se han obtenido las siguientes ventajas:

- Se tiene un registro de los accesos a los sistemas por parte de los usuarios, en forma histórica y/o actualizada.
- Se pueden imprimir reportes de los usuarios y de sus privilegios asignados.
- Se ha podido especificar el acceso que tiene un usuario a la información.
- Impresión de reportes con clave codificada, que permite conocer el usuario que imprimió el reporte y la fecha de impresión.

Además hay que mencionar que el compartir la información entre las bases de datos trae consigo beneficios, como son:

- Aumento de la precisión. Pues al consultar los datos de una base para su utilización y no tener que volver a capturarlos existen menos probabilidades de capturarlos mal.
- Menor redundancia de los datos. Pues al guardar los datos en un lugar y permitir su consulta en otro se reduce el repetir información.

El desarrollar este proyecto permitió aplicar diversos conocimientos adquiridos a lo largo de la carrera, destacan principalmente los temas de programación, bases de datos, análisis y diseño de sistemas y redes de computadoras. Además de aprender que es necesario saber de antemano con que recursos de hardware y software contamos para planear la mejor manera de aprovecharlos. Se reafirmó que es importante tener una buena comunicación con los usuarios finales del sistema, para conocer exactamente cuales son sus necesidades de información y determinar como satisfacerlas.

Este sistema se encuentra aún en una etapa de cambio, ya que se pretende que en su siguiente etapa pueda realizar las asignaciones de privilegios a grupos de usuarios, pues por el momento dicho proceso se hace individualmente, con la creación de este proceso se pretende reducir el tiempo necesario para asignar privilegios en el sistema.

Bibliografía

1. Diccionario Esencial de La Real Academia Española,
   Editorial. Espasa, 2001.

2. Fernández Calvo Rafael
   Glosario básico inglés-español para usuarios de Internet 4ª edición
   Ed. Asociación de técnicos de informática, 2002.

3. Graton, Pierre
   Protección informática: en datos y programas; en gestión y operación;
   en equipos y redes; en Internet.
   Editorial Trillas, 1998.

4. Rodríguez Luis Angel
   Seguridad de la información en sistemas de cómputo
   Ventura ediciones, S.A. de C.V. 1995.

5. Shakuntala Atre,
   Técnicas de base de datos estructuración en diseño y administración
   Editorial trillas, 1988.

6. R. Groff James , N. Weinberg Paul
   Aplique SQL
   Editorial Mc-Graw-Hill, 1991.

7. Henry C.Lucas, Jr.
   Técnicas de informatica hoy Segunda Parte Tomo 3 Sistemas de información
   Editorial Paraninfo S.A., 1987.

8. Senn James A.
   Análisis y diseño de sistemas
   Ed. Mc Graw Hill, 1992.

9. Notifes Acatlán
boletín informativo de la Facultad de Estudios Superiores Acatlán.

10. Manual del proyecto Atenea año 2003.

11. http://www.belt.es/noticias/2002/02_abril/01_05/04_ataqs_informatics.htm

12. http://www.69neuronas.com/articulos/delitos/delitos1.pdf

13. http://www.internet-solutions.com.co/seguridadfisicaylogic.html

14. http://www.acatlan.unam.mx/campus/mapa/

Anexo A

Virus informáticos

Los virus informáticos son uno de los principales riesgos de seguridad para los sistemas, ya sea que estemos hablando de un usuario que utiliza la computadora de su casa para trabajar, o de un usuario que trabaja en una empresa con un sistema informático importante.

Las consecuencias de los virus pueden ser desastrosas, por ejemplo si se cambia el tipo de sangre de un paciente en un hospital, o el estado de cuenta de una empresa las consecuencias pueden ser devastadoras. Los virus se valdrán de cualquier técnica para lograr su cometido. Así, encontraremos virus muy simples que sólo se dedican a presentar mensajes en pantalla y algunos otros mucho más complejos que intentan ocultar su presencia y atacar en el momento justo.

Descripción de virus informático

Un virus informático es un programa de computadora cuya característica más relevante es que puede replicarse a sí mismo y propagarse a otras computadoras, además tiene la capacidad de causar daño como interrumpir el funcionamiento del sistema o afectar el rendimiento de las computadoras infectadas.

Antecedentes

En 1948, John von Neumann, había desarrollado un algoritmo que permitía a las líneas de código reproducirse por sí mismas. En 1949, John Von Neumann, publicó los resultados de sus investigaciones en un artículo titulado "Teoría y Organización de Autómatas Complicados".

La teoría de Von Neumann se comprobó experimentalmente en la década de los setenta, en los Laboratorios Bell de AT&T, donde se desarrolló un juego llamado Core Wars. El objetivo del juego era escribir pequeños programas capaces de destruir los programas contrarios. En 1984, el matemático A. Dewdney escribió un artículo sobre el juego.

Categorías de virus

A continuación se da una clasificación de virus, aunque hay que tener en cuenta que el tipo y cantidad de virus aumenta rápidamente con el tiempo.
Virus de Macros/Código Fuente. Se adjuntan a los programas Fuente de los usuarios y, a las macros utilizadas por: Procesadores de Palabras (Word, Works, WordPerfect), Hoja

Gusanos. Son programas que se reproducen a sí mismos y no requieren de un anfitrión, pues se "arrastran" por todo el sistema sin necesidad de un programa que los transporte. Los gusanos se cargan en la memoria y se posicionan en una determinada dirección, luego se copian en otro lugar y se borran del que ocupaban, y así sucesivamente. Esto hace que queden borrados los programas o la información que encuentran a su paso por la memoria, lo que causa problemas de operación o pérdida de datos.

Caballos de Troya. Son aquellos que se introducen al sistema bajo una apariencia totalmente diferente a la de su objetivo final; esto es, que se presentan como información perdida o "basura", sin ningún sentido. Pero al cabo de algún tiempo, y esperando la indicación programada, "despiertan" y comienzan a ejecutarse y a mostrar sus verdaderas intenciones.

Bombas de Tiempo. Son los programas ocultos en la memoria del sistema o en los discos, o en los archivos de programas ejecutables. En espera de una fecha o una hora determinadas para "explotar". Algunos de estos virus no son destructivos y solo exhiben mensajes en las pantallas al llegar el momento de la "explosión". Llegado el momento, se activan cuando se ejecuta el programa que las contiene.

Autorreplicables. Son los virus que realizan las funciones más parecidas a los virus biológicos, ya que se autorreproducen e infectan los programas ejecutables que se encuentran en el disco. Se activan en una fecha u hora programadas o cada determinado tiempo, contado a partir de su última ejecución. Un ejemplo de estos es el virus del Viernes 13, que se ejecuta en esa fecha y se borra (junto con los programas infectados), evitando así ser detectado.

Infectores del área de carga inicial. Infectan los diskettes o el disco duro, alojándose inmediatamente en el área de carga. Toman el control cuando se enciende la computadora y lo conservan todo el tiempo.

Infectores del sistema. Se introducen en los programas del sistema, para infectar todo disco que sea introducido a la unidad.

Virus Bat: Este tipo de virus empleando ordenes DOS en archivos de proceso por lotes consiguen replicarse y causar efectos dañinos como cualquier otro tipo virus. En ocasiones, los archivos de proceso por lotes son utilizados como lanzaderas para colocar en memoria virus comunes. Para ello se copian a sí mismo como archivos COM y se ejecutan.

Síntomas de infección

Son múltiples los indicios que pueden hacernos pensar que una computadora se encuentra infectada por un virus. Teniendo en cuenta que la variedad de posibles efectos que pueden derivarse de la actuación del virus es casi tan elevada como su número, nos limitaremos sólo a las manifestaciones más habituales:

Aparecen mensajes de error inusuales

Los programas ejecutan acciones de acceso a disco que anteriormente no se realizaban.

Hay menos memoria de la habitual.

La computadora se detiene de manera súbita

El ordenador se vuelve cada vez más lento y tarda más en cargar los programas: hay dificultades al leer archivos o discos.

La luz de la disquetera se mantiene encendida más tiempo de lo normal.

Desaparición de datos en los archivos

Aparición de imágenes extrañas en el monitor.

Los archivos simplemente desaparecen.

Pérdida de espacio en disco.

Se produce una variación en el tamaño de los archivos del sistema operativo.

Se modifican sin razón aparente el nombre de los ficheros.

Cómo se producen las infecciones

Los virus informáticos se difunden cuando las instrucciones o código ejecutable que hacen funcionar los programas pasan de un ordenador a otro. Una vez que un virus está activado, puede reproducirse copiándose en discos flexibles, en el disco duro, en programas informáticos legítimos o a través de redes informáticas.

Los virus funcionan, se reproducen y liberan sus cargas activas sólo cuando se ejecutan. Por eso, si un ordenador está simplemente conectado a una red informática infectada o se limita a cargar un programa infectado, no

¿Que es un antivirus?

Un antivirus es un programa de computadora cuyo propósito es combatir y erradicar los virus informáticos. Para que el antivirus sea productivo y efectivo hay que configurarlo cuidadosamente de tal forma que aprovechemos todas las cualidades que ellos poseen.

Un antivirus es una solución para minimizar los riesgos y nunca será una solución definitiva, lo principal es mantenerlo actualizado. Para mantener el sistema estable y seguro el antivirus debe estar siempre actualizado, tomando siempre medidas preventivas y correctivas y estar constantemente leyendo sobre los virus y nuevas tecnologías.

El antivirus normalmente escanea cada archivo en la computadora y lo compara con las tablas de virus que guarda en disco. Esto significa que la mayoría de los virus son eliminados del sistema después que atacan a éste. Por eso el antivirus siempre debe estar actualizado, es recomendable que se actualice una vez por semana para que sea capaz de combatir los virus que son creados cada día. También, los antivirus utilizan la técnica heurística que permite detectar virus que aun no están en la base de datos del antivirus. Es sumamente útil para las infecciones que todavía no han sido actualizadas en las tablas porque trata de localizar los virus de acuerdo a ciertos comportamientos ya preestablecidos.

El aspecto más importante de un antivirus es detectar virus en la computadora y tratar de alguna manera eliminarlo de nuestro sistema. Hay que tener en cuenta que los antivirus consumen recursos, porque al estar todo el tiempo activos y tratando de encontrar virus al instante se utiliza la memoria de la computadoras y tal vez las vuelvan un poco más lentas.

La única forma de mantener un sistema seguro de virus es mantener el antivirus actualizado, por lo que al comprar un antivirus debemos saber con que frecuencia esa empresa pone a disposición del público sus actualizaciones de las tablas de virus ya que estos son creados diariamente para infectar los sistemas, por lo que si adquirimos un antivirus cuyas tablas de virus aparezcan mensualmente no podremos actualizar nuestro antivirus con la frecuencia necesaria, se recomienda como mínimo actualizar el antivirus una vez a la semana.