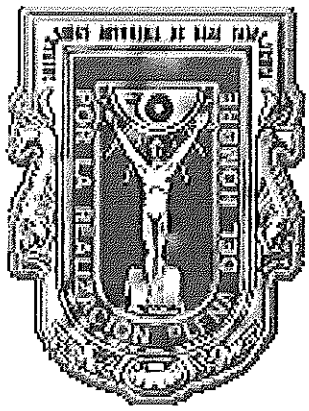
UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE CIENCIAS



SISTEMA GLOBAL DE SEGURIDAD

Memoria de Servicio Social Profesional
que como requisito parcial para obtener el título de

Licenciado en Ciencias Computacionales

presenta:

JESÚS GERARDO VÉLEZ REYNAGA

Ensenada, B.C. **Septiembre 2000**

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE CIENCIAS

SISTEMA GLOBAL DE SEGURIDAD

MEMORIA DE SERVICIO SOCIAL PROFESIONAL

QUE PRESENTA

JESÚS GERARDO VÉLEZ REYNAGA

APROBADA POR:

M.C. ALBERTO LEOPOLDO MORÁN Y SOLARES
PRESIDENTE DEL JURADO

OC. JUDITH ISABEL LUNA SERRANO
SECRETARIO

M.A.I OMAR ÁLVAREZ XOCHIHUA
1ER. VOCAL

Agradecimientos

Gracias a Dios por darme la vida y la fuerza para culminar mis estudios de licenciatura.

Gracias a mis Padres por su amistad, cariño y apoyo incondicional.

Gracias a mi hermana Myrna por brindarme motivación y ayuda para culminar con este trabajo.

Gracias a Leopoldo Morán y Judith Luna, por su amistad, ejemplo y por todos los conocimientos y experiencias profesionales que compartieron conmigo.

Gracias a la Facultad de Ciencias y a los docentes de esta institución por todos los conocimientos que me transmitieron.

Gracias a cada uno de mis compañeros que de alguna manera contribuyeron para lograr terminar mis estudios.

Resumen

de la memoria de servicio social profesional de JESÚS GERARDO VÉLEZ REYNAGA
presentado como requisito parcial
para la obtención del título de
Licenciado en Ciencias Computacionales.

Ensenada , Baja California, México. Septiembre 2000

Sistema Global de Seguridad

Resumen aprobado:

La educación superior enfrenta nuevos retos debido a los avances en las tecnologías de computación y telecomunicaciones, con esquemas nuevos como la educación a distancia. Uno de tales retos es la seguridad e integridad de la información que se maneja en apoyo del proceso de enseñanza-aprendizaje en línea. Este trabajo desarrolla el Sistema Global de Seguridad (SGS) para el sistema Material de Apoyo Docente en Línea (MADL). Se propone un esquema mediante el establecimiento e implementación de políticas de seguridad y la definición de dominios o alcances, establezca los privilegios de acceso de los usuarios y provea un ambiente de seguridad computacional para ser aplicado en los nuevos modelos de educación en línea de la Licenciatura en Ciencias Computacionales. El SGS está implementado en Java, utilizando una arquitectura cliente-servidor y tecnologías como JDBC y Servlets. La aplicación ha sido probada con éxito sobre diversas plataformas.

M.C. ALBERTO LEOPOLDO MORÁN Y SOLARES.
Director del trabajo

CONTENIDO

FIGURAS

TABLAS

I. INTRODUCCIÓN

En este fin de siglo el surgimiento de nuevas formas de comunicación y de tecnologías de información avanzadas, ofrecen emocionantes oportunidades para desarrollar novedosas y variadas formas de enseñanza, aprendizaje y cooperación. Muchas universidades utilizan los ambientes basados en Internet como el soporte de las actividades de enseñanza/aprendizaje (Collins, 99; Organista et al, 2000).

El potencial que ofrecen las redes de computadoras – especialmente Internet y WWW – en la educación, capacitación y entrenamiento, ha estimulado la investigación en sistemas integrados de enseñanza/aprendizaje, además de proporcionar material educativo multimedia, planificar, evaluar y orientar las actividades de los alumnos, para que cuenten con un desarrollo más amplio. Este es un campo de reciente creación (1990), del cual se prevée un gran desarrollo en la próxima década.

Dentro de este campo existe una línea bien definida – denominada aprendizaje colaborativo soportado por computadora (Computer-Supported Collaborative Learning) – dedicada a la creación de ambientes virtuales cooperativos y colaborativos para realizar a distancia y/o soportar las diversas actividades de enseñanza y aprendizaje que se llevan a cabo en las instituciones educativas (Ayala et. al, 1996). El aprendizaje colaborativo es especialmente útil en dominios complejos, en los que es difícil asimilar conocimiento de

manera individual. Dos ejemplos sencillos de trabajos que se han realizado respecto a este tema y que se encuentran disponibles a través del WWW son los que presentan la Universidad de Hawaii (http://leahi.kcc.hawaii.edu/org/occ) y el Colegio Comunitario de Cerro Coso, CA. (http://www.cc.cc.ca.us/cconline/default.html).

En la actualidad existe disponible a través de la red una gran cantidad de información que forma parte de sistemas que apoyan cada una de estas nuevas modalidades, sin embargo, también existen usuarios que hacen mal uso de estos recursos, especialmente, de la información que está contenida en esos sitios. Por esta causa, es usual que para poder acceder a ésta sea necesario que el usuario tenga que pasar por uno o más mecanismos de seguridad, como una identificación válida dentro del sistema antes de poder tener acceso a los recursos (Russel et. al, 1997).

La Facultad de Ciencias propone, a través de este programa, el desarrollo de un Sistema Global de Seguridad para el sistema Material de Apoyo Docente en Línea (MADL), para ser introducido en los nuevos modelos de los cursos que se imparten en la Universidad Autónoma de Baja California (UABC).

II. ANTECEDENTES

El material de apoyo docente es importante en el proceso enseñanza-aprendizaje en los diversos cursos que se imparten en las diferentes carreras de la UABC. Las modalidades en que se prepara y presenta el material varía de curso en curso, dependiendo de la carrera a la que pertenezca, siendo éste teórico, práctico o ambos. La modalidad tradicional es la presentación en forma de "notas del curso", las cuales, a su vez, forman un paquete y que se distribuyen en forma de copias a los participantes del mismo.

En 1998, se contempló la idea de desarrollar un sistema de cómputo el cual permitiera a los usuarios de esta universidad accesar a las notas de cursos, así como a artículos relacionados a estos, además el estudiante tendría la opción de autoevaluar sus conocimientos a través de este sistema. Este sistema comenzó a realizarse a mediados de 1999 con el nombre de "Material de Apoyo Docente en Línea" (MADL) con apoyo interno de la UABC.

El proyecto MADL consiste en el desarrollo e instrumentación de un sistema que dé soporte tanto a alumnos como maestros de la UABC los cursos impartidos en la institución.

El MADL es útil tanto para el alumno como para el maestro, ya que puede ser un punto de referencia para ambos. Por ejemplo, si el alumno, por algún motivo perdió parte de la clase o simplemente no pudo asistir a ella, los apuntes de esta clase estarán disponibles para él, en cualquier momento y a cualquier hora, además podrá realizar autoevaluaciones de su aprendizaje. Por lo tanto, el maestro ya no tendrá que dar la clase de nuevo, lo que implica cierta ganancia en tiempo, y el alumno contará con mayor información y le apoyará de mejor manera en la clase del día siguiente. De ninguna manera el MADL pretende sustituir la labor del maestro, al contrario, el MADL es una herramienta más para que el maestro imparta su clase, pudiendo dejar tareas, ejercicios o investigaciones sobre apuntes que se encuentren en él.

El objetivo del sistema MADL es el apoyar el proceso de aprendizaje de los alumnos, mediante la creación de un ambiente de trabajo colaborativo, vía Internet.

Antes de realizar una propuesta concreta para llevar a cabo el proyecto de Material de Apoyo Docente en Línea (MADL), se entrevistó a estudiantes y maestros de esta universidad, con el fin de conocer cual era su punto de vista en cuanto a la existencia de este tipo de herramientas y a su disponibilidad (acceso al sitio y buen entendimiento del material en cuanto a la claridad y calidad de su información).

Población Seleccionada

Se entrevistó a estudiantes y maestros de la unidad Ensenada, así como también a investigadores del CICESE, para así obtener una muestra sin tendencias ideológicas y además que permitiera conocer la postura de las personas que de alguna forma están vinculadas y podrían utilizar la herramienta MADL.

Se seleccionó una población estadística aleatoria, donde se entrevistó a diez alumnos por cada carrera o maestría que se cursa en esta casa de estudios y a cinco docentes por Escuela, Facultad o Institución. Esto dió como resultado una muestra donde $n_1 = 130$ alumnos y $n_2 = 35$ docentes

Es importante mencionar que se elaboraron dos cuestionarios diferentes (anexo A y B), para alumnos y maestros e investigadores, por ser poblaciones diferentes y obtener datos más significativos sobre las necesidades del sistema a desarrollar.

Resultados Obtenidos de las Encuestas

Los resultados que se obtuvieron mediante las encuestas a estudiantes, maestros e investigadores se muestran en los anexos C y D respectivamente.

Interpretación de Resultados

Con base en los resultados obtenidos mediante las encuestas aplicadas, e

interpretando estos resultados, se considera que un Material de Apoyo Docente en Línea debe:

1. Permitir al usuario un acceso rápido a la información, ya sea en tiempo como en el método de búsqueda que se utilice.
2. Encontrarse fácilmente a disposición del usuario, es decir, que siempre existan máquinas suficientes para prestar el servicio al usuario.
3. Ser fácil de entender y de controlar por parte del usuario.
4. Proporcionar información actualizada y de calidad.
5. Presentar al usuario la información de una manera clara, estructurada, consistente y sencilla.
6. Cumplir con el cometido de reforzar el contenido temático de algún curso o tema en particular.
7. Presentar la información en el formato adecuado según el contenido temático de la materia, para de esta manera facilitar que el estudiante entienda de una manera clara dicho contenido.
8. Permitir incorporar en él, otros cursos o tutoriales que sean de utilidad para los usuarios.
9. Permitir la interacción entre usuarios para que estos realicen comentarios, intercambien ideas y aclaren dudas con otros usuarios del mismo sistema.

Propuesta

El esquema que se propuso para llevar a cabo el Sistema de Material de Apoyo Docente en Línea consta de seis módulos, los cuales son mencionados a continuación:

Banco de Notas de Curso

Este Módulo almacenará la información referente a cada una de las materias que serán contempladas dentro del sistema. Dicha información consistirá de notas de cursos, artículos, ejemplos, etc. Además, ésta será presentada con ayuda de gráficas y en algunos casos audio y video.

Banco de Reactivos y Exámenes

Este módulo contendrá herramientas de evaluación sobre los temas concernientes a alguna materia en particular, las cuales servirán para que el alumno pueda evaluar sus conocimientos sobre el tema consultado.

Foro de Discusión Fuera de Línea

Este módulo permitirá el intercambio de opiniones entre los usuarios del sistema, para que puedan hacer comentarios o aclarar dudas sobre el contenido de la clase o del material didáctico consultado.

Control de Usuarios

Este módulo controlará el acceso de los diferentes usuarios dentro del sistema, asignándoles distintos derechos, para así tener un control adecuado sobre los accesos y los recursos que utilizan.

Sistema de Interfaz entre las Bases de Datos y el WWW

Este módulo se utilizará para establecer el enlace entre cada una de las bases de datos y la interfaz del usuario, encargándose de tomar la petición desde la interfaz del usuario y con esto permitir el acceso a las bases de datos para así obtener la información requerida y posteriormente presentarla al usuario.

Interfaz del Usuario

Este módulo se encargará de presentar al usuario un ambiente amigable, el cual presente la información de una manera clara, además de permitir un acceso sencillo y rápido a ésta.

Una vez detectados los módulos anteriores, se decidió descomponer el sistema en varios subsistemas los cuales se muestran en la siguiente figura:

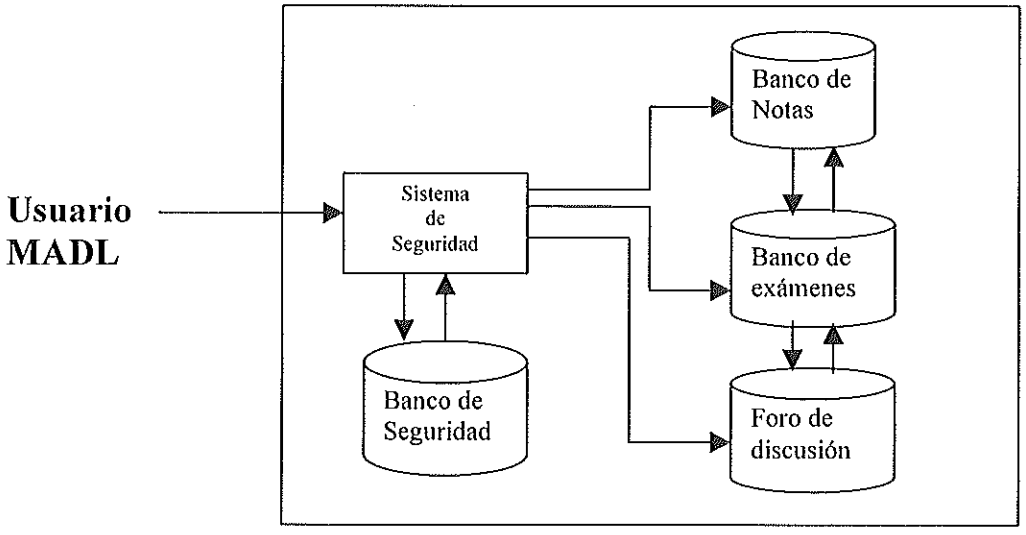


Figura 1. Arquitectura del sistema MADL

Esta descomposición del sistema es debido a que existen dos módulos (Interfaz del Usuario e Interfaz entre la Base de Datos y el WWW) que se incluyen dentro del desarrollo de cada uno de los subsistemas anteriores.

El propósito del presente trabajo es desarrollar el Sistema Global de Seguridad. Es importante mencionar que aunque cada uno de los módulos serán elaborados de manera independiente, también es cierto que durante el análisis y el diseño, los desarrolladores de cada uno de los sistemas tendrán que compartir información referente a la transferencia de datos entre los distintos módulos que constituyen al sistema MADL.

3.1 Propuesta para el desarrollo del Módulo SGS

Se propone que el sistema cuente con un primer nivel de seguridad, el cual se encargará de controlar el acceso de los usuarios a cada uno de los bancos de datos del sistema, esto se hará por medio de la asignación de derechos a cada uno de los usuarios. Dichos derechos consisten en asignarle un dominio o alcance al usuario, permitiendo el acceso a las diferentes recursos dentro del sistema.

Una vez que el usuario haya accesado los bancos de datos, éstos se encargarán de verificar el dominio al que pertenece el usuario, otorgándole los derechos que le correspondan dentro de ellos, Ejemplos de estos derechos son: lectura, escritura, eliminación de información, etc..

III. OBJETIVOS

Objetivo general

Desarrollar un sistema de seguridad que permita mantener la integridad de la información que se encuentre almacenada en el sistema de Material de Apoyo Docente en Línea (MADL). Así como, elaborar un mecanismo que permita monitorear las acciones de los usuarios dentro del mismo por medio de dominios o alcances).

Objetivos específicos

- Definir una clasificación de los diferentes tipos de usuarios.
- Asignarle a los usuarios un tipo de dominio, para permitir el acceso a la información y el monitoreo de estos en áreas específicas dentro del sistema.
- Proteger la información almacenada en el sistema por medio de políticas de seguridad.

IV. METODOLOGÍA

Para el desarrollo del presente trabajo se ha decidido aplicar los principios de la ingeniería de software como lo señala Pressman (1997) y Fairley (1994) para el ciclo de desarrollo de software. También se recurrió metodo evolutivo de desarrollo de software el cual consiste en desarrollar versiones sucesivas, en el cual las características de funcionalidad del producto se distribuyen como metas a alcanzar (funcionalidad a integrar) a través del tiempo de desarrollo. Esto es, cada intervalo fijo de tiempo, se va obteniendo una nueva versión que incluye la funcionalidad de la versión anterior, más la nueva funcionalidad especificada, así como la corrección de errores y defectos (Mc Connell, 1996). La siguiente figura muestra el proceso de desarrollo utilizando este ciclo de vida.

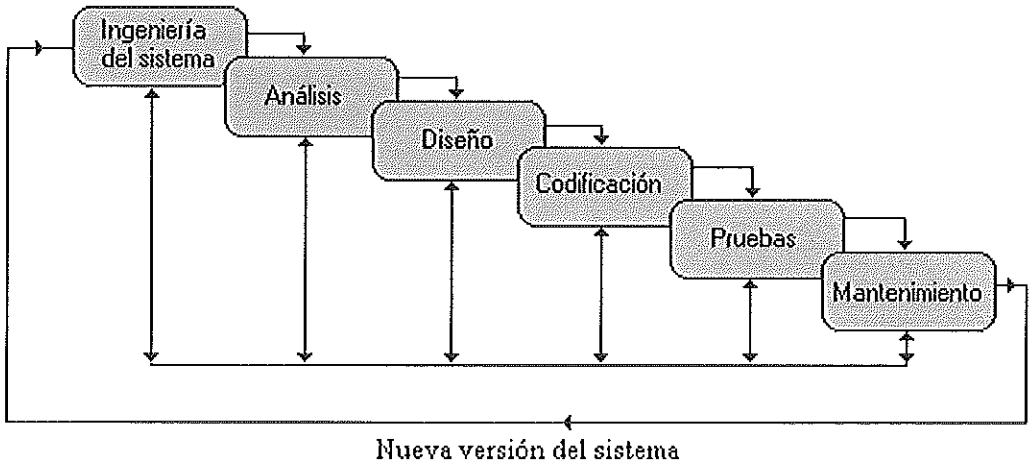


Figura 2. El ciclo de vida de versiones sucesivas

La Metodología OMT fue utilizada para desarrollar el modelado del Sistema Global de Seguridad debido a que ésta permite construir un modelo de un dominio de aplicación y después agrega detalles de implantación a él durante el diseño del sistema. Además, esta herramienta cuenta con una notación gráfica para representar los conceptos de orientación a objetos, lo cual facilita en gran medida la comprensión del problema tratado (Rumbaugh et al., 1991).

Finalmente, para lograr modelar el banco de datos que utiliza el Sistema Global de Seguridad, se decidió aplicar el modelo Entidad-Relación tal y como lo especifica Kroenke (Kroenke, 1996).

Algunos de los pasos que se siguieron dentro del ciclo de desarrollo fueron:

1. Análisis Orientado a Objetos
2. Diseño de Sistemas y diseño de Objetos
3. Modelado de la base de datos
4. Implementación.
    a. Desarrollo de la base de datos
    b. Desarrollo del interfaz del usuario
    c. Desarrollo del interfaz WWW-BD

V. DESARROLLO

5.1 Análisis y diseño del sistema

5.1.1 Modeldo de Objetos

El primer paso dentro de la metodología OMT para el proceso de análisis y diseño de un sistema se encuentra el modelado de objetos, éste consiste en describir la estructura estática de los objetos en un sistema y sus relaciones. El modelo de objetos contiene diagramas de objetos. Un diagrama de objetos es un grafo cuyos nodos son clases de objetos y cuyos arcos son relaciones entre clases.

El diagrama de objetos elaborado para este proyecto es el que se muestra a continuación:

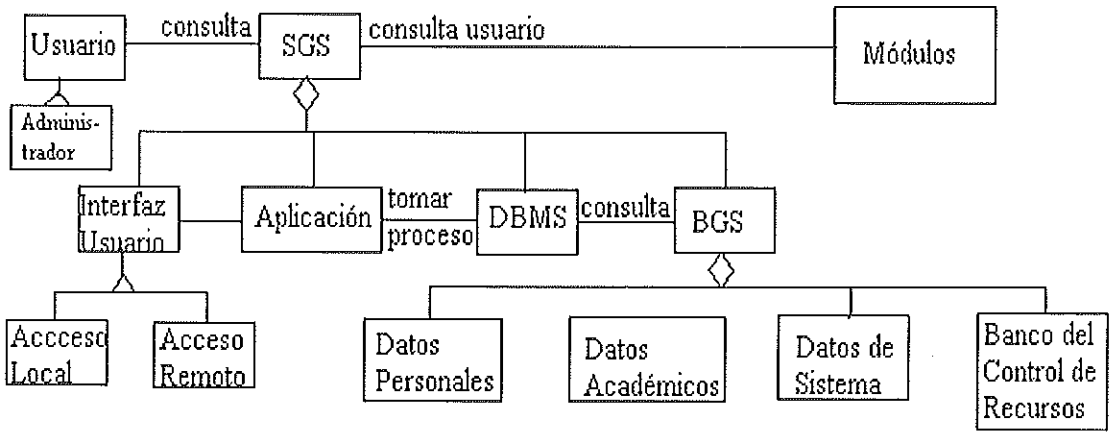


Figura 3. Diagrama de Objetos del Sistema Global de Seguridad

Usuarios

Se encarga de permitir al usuario solicitar el acceso al sistema, así como permitirle a este interactuar con las aplicaciones propias de este sistema.

Administrador

Se encarga de permitir al Administrador solicitar el acceso al sistema, así como de permitirle a este trabajar con las aplicaciones existentes en este sistema.

Sistema Global de Seguridad (SGS)

Se encargará de controlar el acceso de los usuarios al sistema, así como también proporcionar algunos servicios de seguridad a los distintos módulos que integran el mismo.

Interfaz Usuario

Se encarga de presentar de manera clara y sencilla la información solicitada por el usuario, así como también permitirle a éste un método de búsqueda adecuado, de tal manera que tenga un rápido acceso a la información.

DBMS

Es el encargado de proporcionar al sistema los datos requeridos para el buen funcionamiento del mismo. Dicho de otro modo, el DBMS accesará la información

almacenada en las distintas bases de datos, para posteriormente presentar la información al sistema.

Aplicación

Este será el encargado de realizar las tareas relacionadas con las conexiones y desconexiones dentro del sistema, además de vincular la información proporcionada por la interfaz al DBMS.

Banco de Control de Recursos (BCR)

Este banco de datos contiene información acerca de los diversos usuarios que se encuentren en ese momento dentro del sistema. Dicha información será el nombre de usuario(nickname) del alumno, docente, etc., el tiempo que tiene dentro del sistema, el recurso utilizado y tiempo en el recurso utilizado.

Datos Personales del Usuario (DPU)

En este banco de datos se almacena la información referente a los datos personales del usuario. Estos datos consisten en: nombre del usuario, dirección, teléfono, edad, sexo, e-mail y ciudad de residencia.

Datos Académicos del Usuario (DAU)

En este banco de datos se concentra la información relacionada a los datos académicos del usuario, por ejemplo: Unidad académica, facultad o escuela a la que pertenece, carrera y grado de estudio.

Datos del Sistema del Usuario (DSU)

Dentro de este banco de datos se almacenan los datos relacionados con el uso del sistema por parte del usuario, estos datos serán: nivel de acceso, recurso utilizado, nickname, password.

5.1.2 Modelo Dinámico

Como segundo paso en el análisis se tiene que elaborar un modelo dinámico, el cual describe los aspectos del sistema que cambian conforme pasa el tiempo. El modelo dinámico es usado para especificar e implantar los aspectos de control de un sistema. Para realizar el modelo dinámico según Rumbaugh (op cit) se deben seguir los siguientes pasos: creación de escenarios, elaboración de trazos de eventos y elaboración de diagramas de estado.

A continuación se presentan los escenarios y trazos de eventos elaborados para este sistema:

5.1.2.1 Escenarios y Diagramas de Trazos de eventos

Escenario 1.- Conexión del usuario al sistema

1. El sistema inicializa y espera solicitud del usuario.
2. El sistema recibe la solicitud.
3. El sistema devuelve la pantalla de login.
4. El usuario escribe su nombre y clave.
5. El sistema envía la información al DBMS para ser verificada.
6. El DBMS accesa a la información de la base de datos.
7. El DBMS recibe de la base de datos la información solicitada.
8. El sistema recibe la información verificada, la cual es válida.
9. El sistema acepta los datos y crea el contexto de la sesión
10. El banco de control de recursos indica al sistema que la operación fue satisfactoria.
11. El sistema envía al usuario una pantalla de bienvenida.

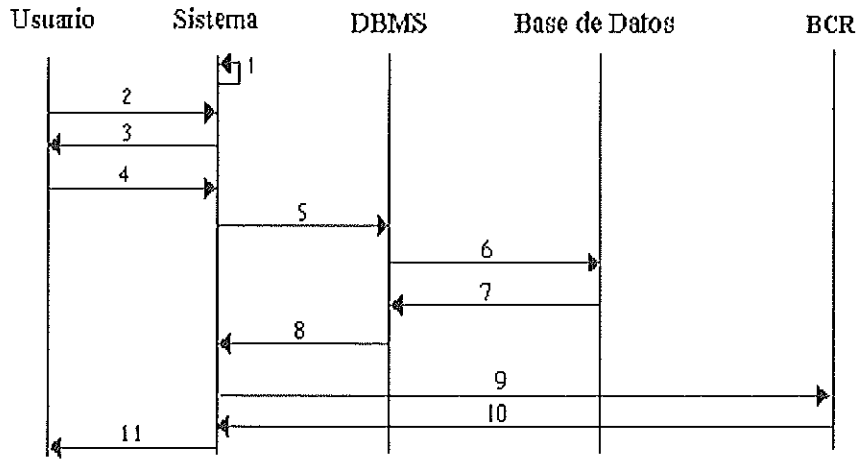


Figura 4. Trazo de eventos que muestra el proceso de conexión del usuario al sistema

Escenario 2.- El sistema monitorea a los usuarios del sistema

1. El administrador accesa a la opción de monitoreo del SGS.
2. El sistema solicita al DBMS el nombre de los usuarios que se encuentran en sistema o módulo específico.
3. El DBMS accesa la información de la base de datos.
4. El DBMS recibe la información solicitada.
5. El sistema recibe la información
6. El sistema despliega la información al administrador

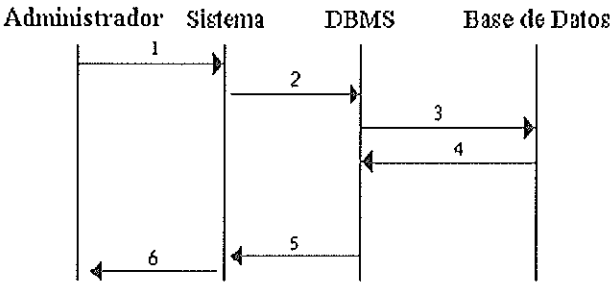


Figura 5.- Trazo de eventos que muestra como el sistema monitorea a los usuarios dentro del sistema.

Escenario 3.- El usuario se cambia de recurso dentro del sistema

1. El usuario termina la sesión con el módulo.
2. El sistema recibe la terminación de uso del módulo y además recibe los datos del usuario.
3. El sistema accesa al DBMS para verificar la información recibida del módulo.
4. El DBMS accesa la información de la base de datos.

5. El DBMS recibe la información solicitada.
6. El sistema recibe la información verificada, la cual es válida.
7. Muestra pantalla de módulos.
8. El sistema recibe la respuesta de selección del usuario para un nuevo módulo a consultar.
9. El sistema accesa al nuevo módulo.
10. El sistema recibe mensaje de aceptación del módulo.
11. El nuevo módulo envía pantalla de bienvenida al usuario.
12. El sistema envía los nuevos datos del usuario al DBMS.
13. El DBMS modifica el Banco de Control de Recursos (BCR).
14. El DBMS recibe mensaje de aceptación.
15. El sistema recibe mensaje de verificación.

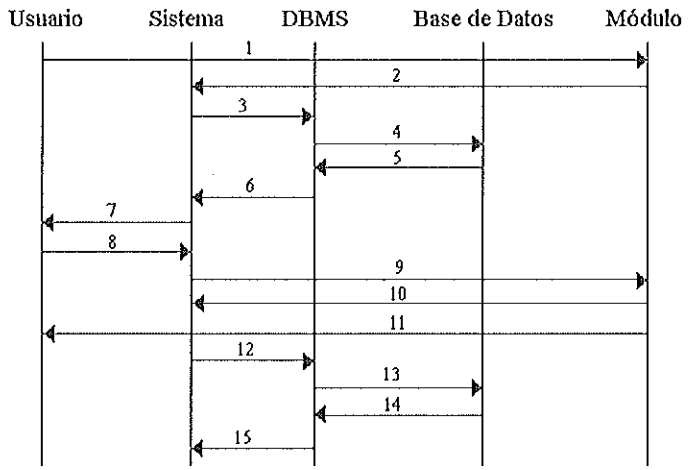


Figura 6. Trazo de eventos que muestra como cambiar de recurso dentro del sistema.

Escenario 4.- Altas en el SGS

1. El usuario selecciona la opción de *altas*.
2. El sistema despliega pantalla correspondiente a la opción de *altas*.
3. Se introducen los datos del nuevo usuario.
4. Se verifica la validez de los datos.
5. El sistema pide al DBMS que registre estos datos.
6. El DBMS accesa a la base de datos para dar de alta los datos del nuevo usuario.
7. La base de datos registra los datos y envía un mensaje al DBMS.
8. El DBMS regresa los resultados de la operación al sistema.
9. El sistema informa al usuario que la información ha sido almacenada.

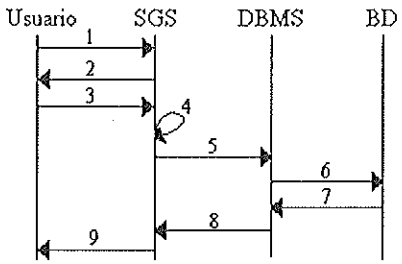


Figura 7. Trazo de eventos que muestra como dar de alta a un usuario dentro del sistema

Escenario 5.- Bajas en el SGS

1. El usuario selecciona la opción de *bajas*.
2. El sistema despliega pantalla correspondiente a la opción de *bajas*.
3. Se introducen los datos del usuario a eliminar.
4. El sistema solicita al DBMS que localice a este usuario.
5. El DBMS accesa a la base de datos para buscar los datos del usuario.

6. Se termina proceso de búsqueda.
7. Se informa al sistema que los datos fueron localizados.
8. El sistema despliega los datos a eliminar.
9. El usuario confirma la operación.
10. El sistema informa al DBMS que elimine al usuario.
11. El DBMS borra todos los datos concernientes al usuario.
12. Se envía al sistema la confirmación del proceso
13. Se informa al usuario que los datos han sido eliminados de la base de datos.

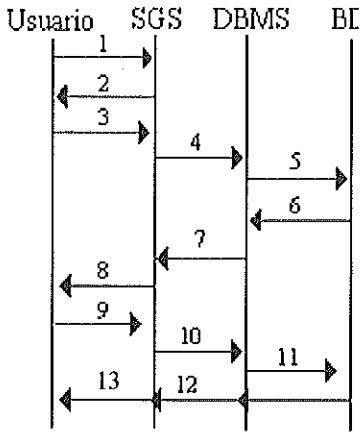


Figura 8. Trazo de eventos que muestra como dar de baja a un usuario dentro del sistema

Escenario 6.- Modificaciones en el SGS

1. El usuario selecciona la opción de *modificaciones*.
2. El sistema despliega la pantalla correspondiente a la opción de *modificaciones*.
3. Se selecciona el usuario a modificar.
4. El sistema solicita al DBMS que localice a este usuario.
5. El DBMS accesa a la base de datos para buscar los datos del usuario.

6. Se termina proceso de búsqueda.
7. Se informa al sistema que los datos fueron localizados.
8. El sistema despliega los datos del usuario a modificar.
9. El usuario modifica los datos.
10. El sistema informa al DBMS que algunos datos del usuario fueron cambiados.
11. El DBMS modifica la información necesaria en la base de datos.
12. Se informa al sistema que los datos fueron actualizados.
13. El sistema informa al usuario la actualización de los datos.

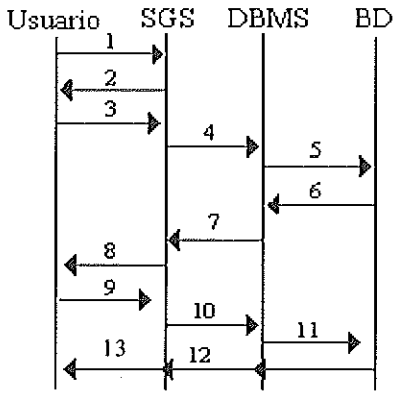


Figura 9. Trazo de eventos que muestra como hacer una modificación dentro del sistema

Escenario 7.- Consultas en el SGS

1. El usuario selecciona la opción de *consultas*.
2. El sistema despliega pantalla correspondiente a la opción de *consultas*.
3. Se selecciona el usuario a consultar.
4. El sistema solicita al DBMS que localice a este usuario.
5. El DBMS accesa a la base de datos para buscar los datos del usuario.

6. Se termina proceso de búsqueda.
7. Se informa al sistema que los datos fueron localizados.
8. El sistema despliega los datos encontrados.

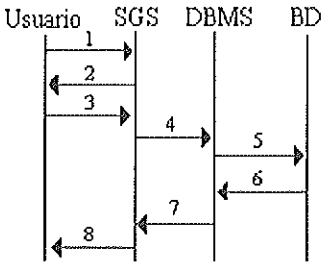


Figura 10. Trazo de eventos que muestra como hacer una consulta dentro del sistema

Una vez diseñados los escenarios y trazos de eventos para el sistema, se procedió a elaborar los diagrama de estados para las principales clases involucradas en nuestro sistema. Estos diagramas son utilizados para especificar e implantar los aspectos de control de un sistema.

5.1.2.2 Diagrama de Estados

Diagrama General de la clase Usuario

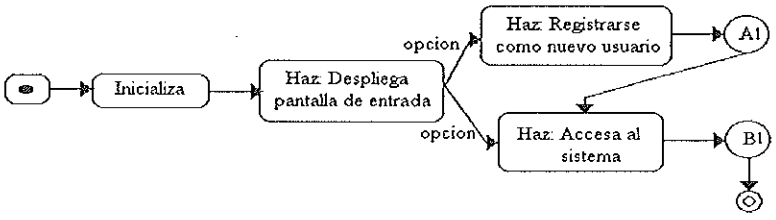


Figura 11. Diagrama de estados que muestra el diagrama general del Usuario.

Diagrama de Altas (A1)

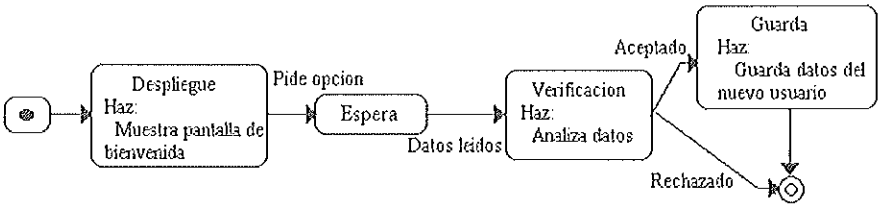


Figura 12. Diagrama de estados que muestra el trabajo realizado por el SGS al momento que se dá de alta a un nuevo usuario.

Diagrama de Acceso al Sistema (B1)

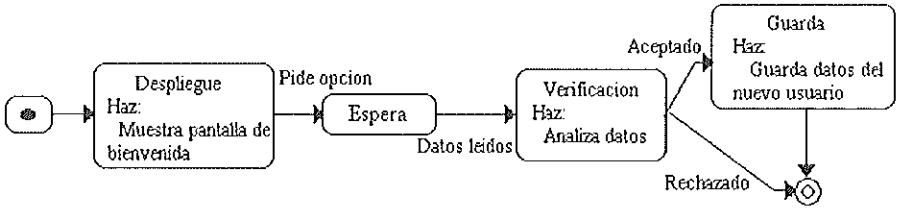


Figura 13. Diagrama de estados que muestra el trabajo realizado por el objeto SGS para la conexión del usuario al sistema

Diagrama General de la clase Administrador

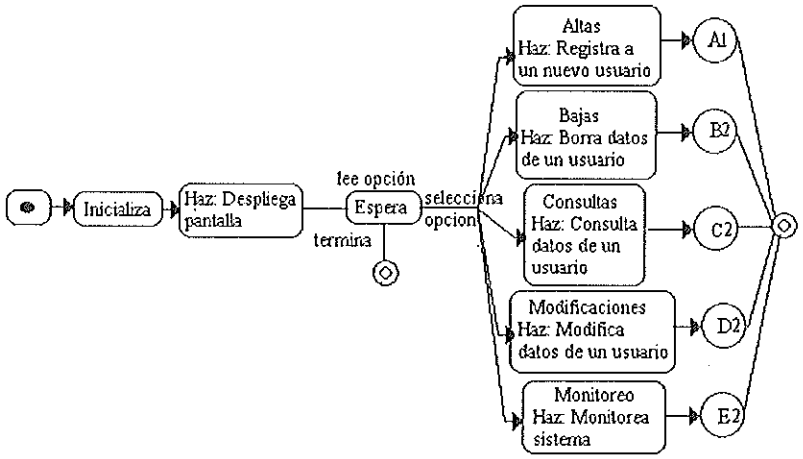


Figura 14. Diagrama de estados que muestra el diagrama general del Administrador.

Diagrama de Bajas (B2)

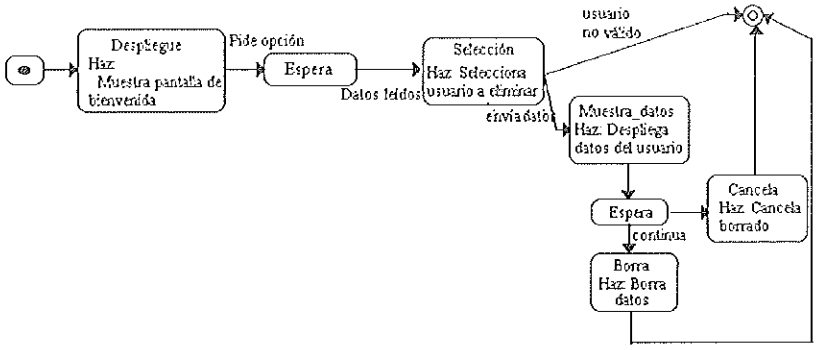


Figura 15. Diagrama de estados que muestra el trabajo realizado por el Administrador al momento que se da de baja a un usuario.

Diagrama de Consultas(C2)

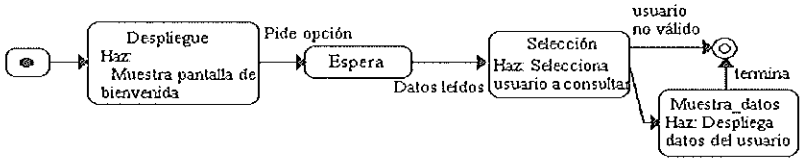


Figura 16. Diagrama de estados que muestra el trabajo realizado por el SGS al momento consultar a un usuario.

Diagrama de Modificaciones (D2)

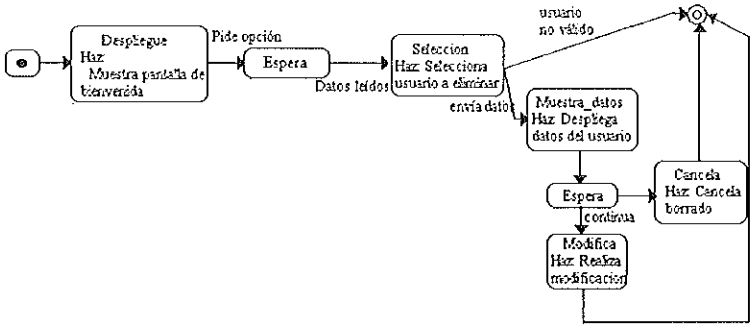


Figura 17. Diagrama de estados que muestra el trabajo realizado por el SGS al momento de modificar la información de un usuario.

Diagrama de Monitoreo (E2)

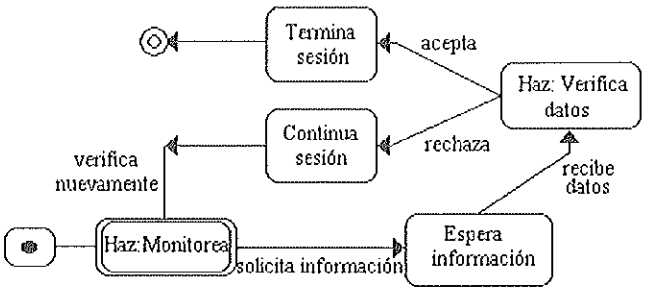


Figura 18. Diagrama de estados que muestra el trabajo realizado por el SGS al momento de monitorear a los usuarios dentro del sistema.

Manejador de Base de Datos (DBMS)

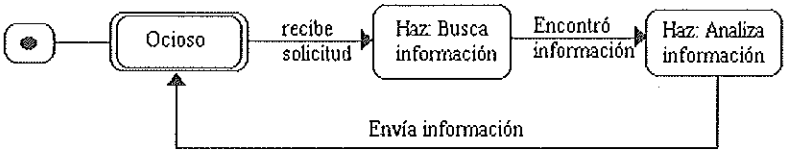


Figura 19. Diagrama de estados que muestra el trabajo realizado por el DBMS para la conexión del usuario al sistema

5.1.3 Modelo Funcional

El *modelo funcional* describe las transformaciones de los valores de los datos dentro de un sistema. El modelo funcional contiene diagramas de flujo de datos. Un diagrama de flujo de datos representa un cálculo. Un diagrama de flujo de datos es un grafo cuyos nodos son procesos y cuyos arcos son flujos de datos.

A continuación se muestran los digramas de flujo de datos elaborados para este sistema:

Diagrama General de la clase Usuario

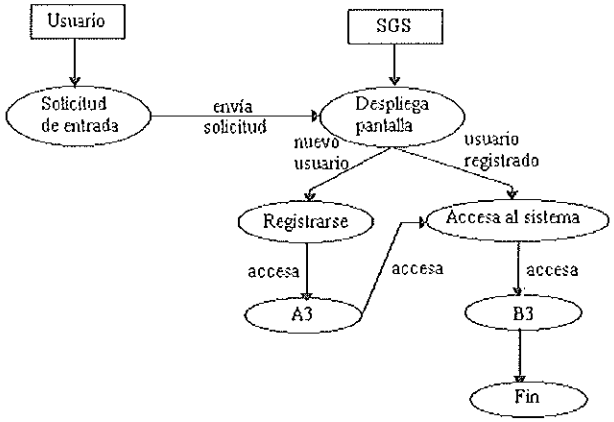


Figura 20. Diagrama de flujo de datos del usuario.

Diagrama de Alta (A3)

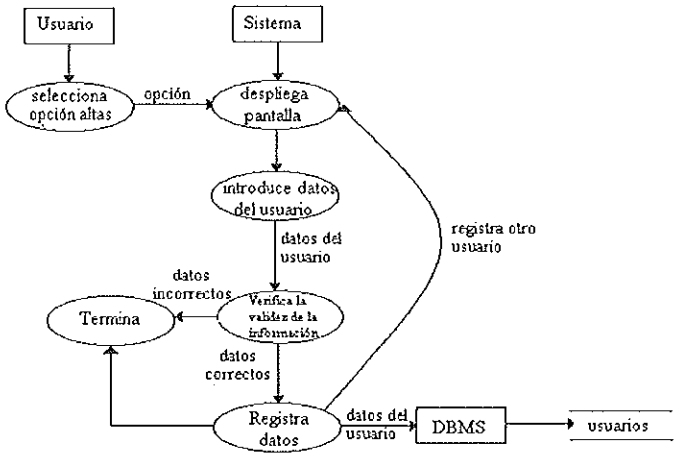


Figura 21. Diagrama que muestra el flujo de datos al momento de que el sistema da de alta a un nuevo usuario.

Diagrama de Acceso al Sistema

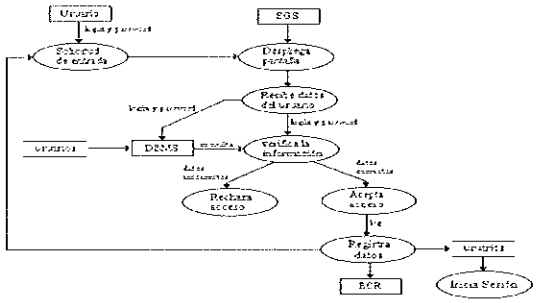


Figura 22. Diagrama que muestra el flujo de datos al momento de que el usuario establece la conexión con el sistema.

Diagrama General de la clase Administrador

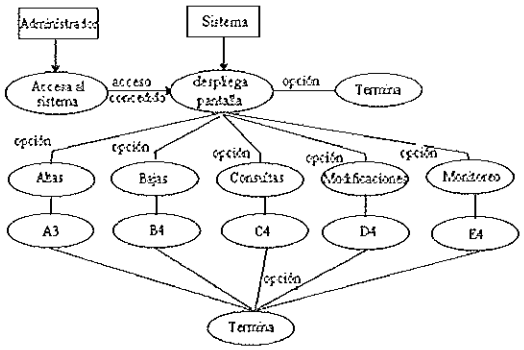


Figura 23. Diagrama de flujo de datos general del administrador.

Diagrama de Bajas (B4)

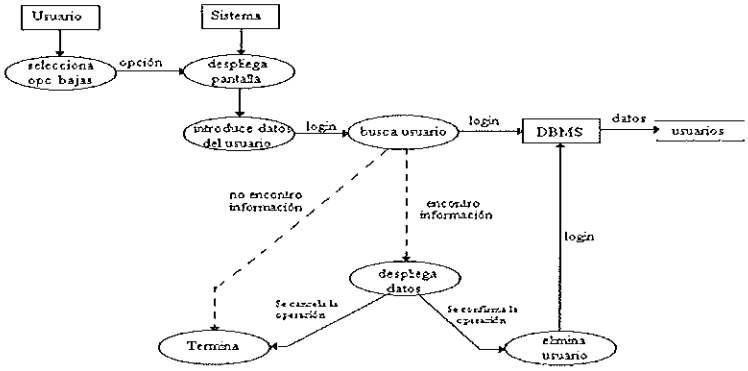


Figura 24. Diagrama que muestra el flujo de datos al momento de que el sistema da de baja a un usuario.

Diagrama de Consultas (C4)

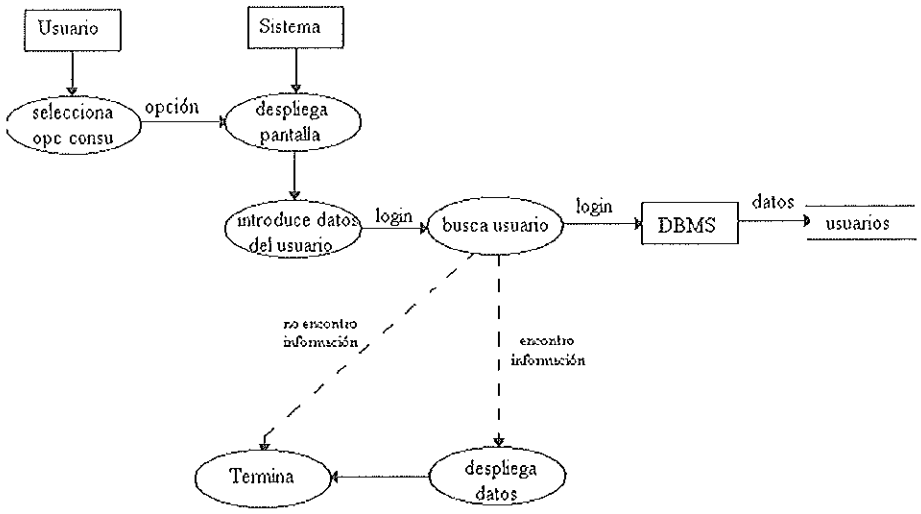


Figura 25. Diagrama que muestra el flujo de datos al momento que el sistema consulta la información de un usuario.

Diagrama de Modificaciones (D4)

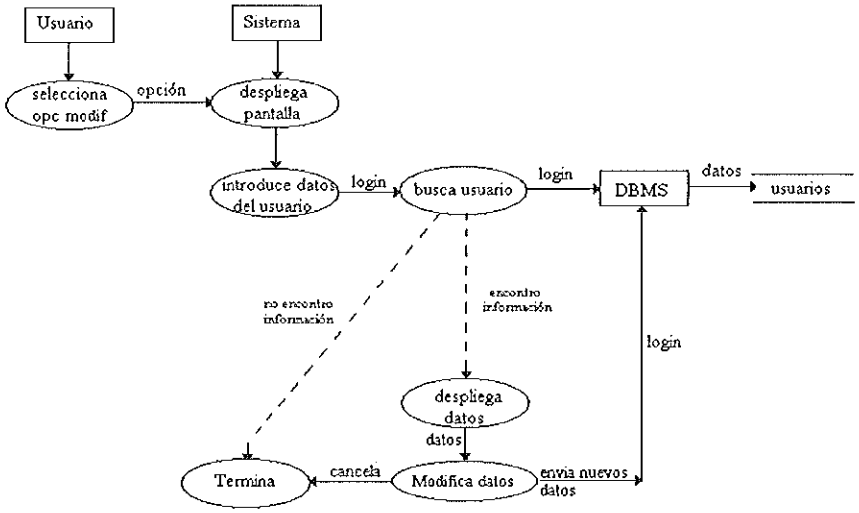


Figura 26. Diagrama que muestra el flujo de datos al momento de que el sistema modifica los datos de un usuario.

Diagrama de Monitoreo (E4)

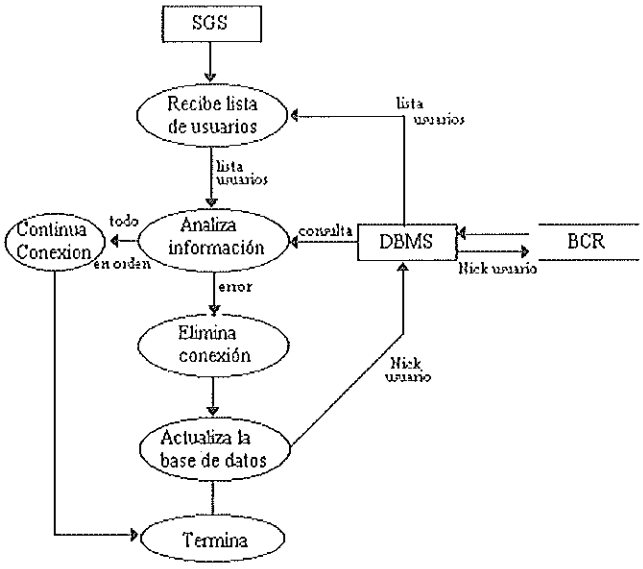


Figura 27. Diagrama que muestra el flujo de datos al momento de que el sistema monitorea a los usuarios que se encuentran dentro del sistema.

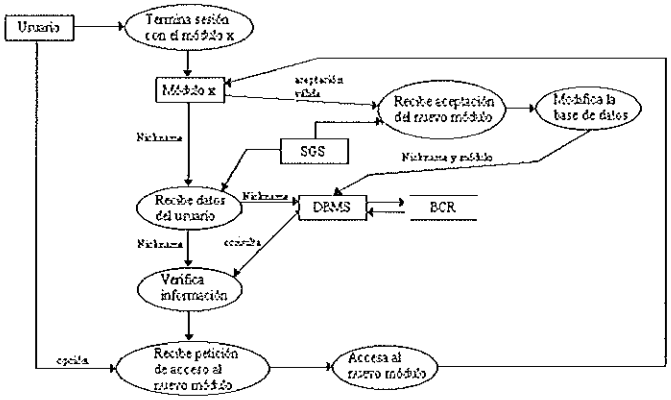


Figura 28. Diagrama de flujo de datos que muestra como el usuario solicita acceso a otro modulo dentro del sistema.

5.2 Esquema de Seguridad

Es necesario hacer notar que para el éxito de un esquema de seguridad es vital el apoyo proporcionado por parte del *cuerpo directivo, propietario de los recursos, etc.*, para que las políticas y procedimientos se han llevadas a cabo.

También los usuarios deben conocer el uso adecuado de los sistemas de cómputo y saber cómo protegerse a sí mismos de accesos no autorizados. Debe crearse una cultura de seguridad, haciendo ver a los recursos humanos involucrados, los riesgos a los que se está expuesto al participar en este tipo de ambiente.

Se considera la *seguridad física,* que se basa en mantener seguros el servidor y dispositivos asociado a él, para evitar cualquier acción que pudiera comprometerlos, por ejemplo, accesos a consola o al equipo del servidor, y factores ambientales. Algunas recomendaciones respecto a la seguridad física son:

- Proteger las computadoras contra el fuego, humo, polvo y temperaturas extremas.
- Protegerlas contra descargas o variaciones en la alimentación eléctrica.
- Mantener las computadoras alejadas de comida y bebida.

Es importante considerar que la *Seguridad en el Servidor*, también abarca proteger dispositivos, directorios y archivos contra usos o accesos no autorizados, ya sea por intrusos o por los mismos usuarios. En el caso en el que el usuario pretenda accesar

directamente al SGS, el sistema cuenta con el *login* y *password,* que se encargan de autorizar los accesos. El único usuario que tendrá acceso directo al SGS será el administrador.

Por último, pero no menos importante, la *Seguridad en la Red*, que tiene como objetivo limitar o restringir las actividades desde sitios remotos. Como se ha mencionado con anterioridad, el acceso al sistema se da por medio del servidor FCIENCIAS, al cual se encuentra conectado el servidor CIMARRON, así que la seguridad en la red es controlada principalmente por el servidor FCIENCIAS. Por otra parte, el SGS cuenta con la opción de monitorear las cuentas de los usuario que actualmente se encuentren accesando al MADL, dando como resultado información sobre tiempos de entrada, duración en cada uno de los módulos, duración total en el sistema, y datos generales de los usuarios, entre otros. El monitoreo será realizado por el administrador del SGS.

5.3 Políticas y procedimientos

Las políticas de seguridad son documentos que describen, principalmente, la forma adecuada de uso de los recursos de un sistema de cómputo, las responsabilidades y derechos que tanto usuarios como administradores tienen y que especifican qué hacer ante un incidente de seguridad (Russel et. al, 1997).

Mientras las políticas indican el *qué*, los procedimientos indican el *cómo*. Los procedimientos son los que nos permiten llevar a cabo las políticas. Algunos ejemplos que requieren la creación de un procedimiento son:

- Otorgar una cuenta,
- Dar de alta a un usuario,
- Localizar una computadora,
- Manejar un incidente de seguridad,
- Respaldar o restaurar información,

entre otros

Para que esto sirva de algo, las políticas deben ser:

- Apoyadas por los directivos
- Únicas
- Claras
- Concisas
- Bien estructuradas
- Servir de referencia
- Por escrito
- Dadas a conocer
- Entendidas por los usuarios
- Mantenerse actualizadas
- Supervisadas

Las políticas son parte fundamental de cualquier esquema de seguridad eficiente. Como administradores, aminoran los riesgos y permiten actuar de manera rápida y acertada en caso de haber una emergencia de cómputo. Como usuarios, indican la manera adecuada de usar un sistema, indicando lo que puede hacerse y lo que debe evitarse en un sistema de cómputo (Russel op cit).

Al diseñar un esquema de políticas de seguridad es conveniente que se divida el trabajo en varios campos con el fin de establecer las políticas asociadas a cada uno de estos, por ejemplo: *cuentas, contraseñas, control de acceso, uso adecuado de recursos, administración del sistema, seguridad física.*

5.4 Definición de políticas de seguridad y procedimientos

Las políticas de seguridad propuestas para el desarrollo del sistema son las siguientes:

Política #1.- Control de acceso al sistema

Es el primer nivel de seguridad, el cual ofrece un mecanismo para el control de acceso al sistema por parte de los usuarios, se concentra en contestar ¿Quién está autorizado a entrar al sistema (*log in*)? y ¿Cómo decidir si el usuario es un usuario legítimo del sistema?.

El mecanismo que se está utilizando en este caso es que el usuario debe introducir un identificador único (login), seguido por una clave (password) asociada a este identificador. Este identificador es típicamente un nombre, iniciales o un número de cuenta asignado por el administrador del sistema.

Otras de las políticas de seguridad a este respecto, son las siguientes:

- No existirán cuentas para visitantes anónimos (guest).
- No habrá identificadores (login) sin su respectiva clave de acceso (password).
- Sólo será permitida, a la vez, una sesión por cada usuario.
- No se permitirá el acceso físico a la máquina servidor a cualquier usuario.

Política #2.- Control de acceso a la información (Dominios o alcances)

Este es el segundo mecanismo que se utilizó para la realización del sistema. Es el que se encarga de monitorear el acceso a los datos almacenados en el mismo, es decir, ¿quién puede leer tus archivos? y ¿quién puede cambiar o borrar tus archivos?.

Para poder lograr este nivel de seguridad, se dividió el control de acceso a la información por medio de dominios o alcances, los cuales definen qué puede o no hacer el usuario en cada uno de estos niveles. Los dominios o alcances quedaron de la siguiente manera:

- Administradores (super usuario)
- Administradores del Banco de Notas de Cursos
- Administradores del Banco de Reactivos y Exámenes

- Usuarios ordinarios

Política #3.- Proteger los passwords almacenados

Cada sistema necesita mantener secretos sus datos de autentificación y éste no es la excepción. Los passwords son almacenados en una archivo dentro de la base de datos y este archivo es accesado solamente en circunstancias especiales: cuando un usuario nuevo es registrado, cuando un usuario desea entrar al sistema ó cuando se desea modificar el perfil de un usuario. El mecanismo seleccionado para proteger las claves almacenadas en el sistema fue mediante la encriptación de esta información.

Política #4.- Mecanismo para identificar el uso correcto de los recursos

Otra de las políticas establecidas fue la de monitorear a los usuarios que estén dentro del sistema, para asegurar que el usuario accede sólo a los recursos que tiene derecho y en caso extremo, detectar cualquier irregularidad lo más pronto posible.

Política #5.- Plan diario para el administrador del sistema

Aún en sistemas de alta seguridad, ésta no se mantiene de manera automática, es decir, un sistema por más seguro que sea si no se le da el seguimiento y mantenimiento correcto por parte del administrador, tarde o temprano va a tener problemas en su confiabilidad.

Por esta razón, se ha optado por proponer las siguientes tareas para su realización diaria:

- Realizar monitoreos tanto de las actividades de los usuarios, como del estatus de los recursos que utilizan.
- Realizar respaldos periódicos de la información.

5.5 Análisis de riesgos sobre las políticas de seguridad establecidas

Una de las principales razones para crear una política de seguridad, es precisamente asegurar que el sistema será difícil de corromper y por ende más confiable, por esto, la elaboración de un análisis de riesgos es de suma importancia para la evaluación de las políticas de seguridad establecidas.

Este análisis consiste en determinar ***qué se necesita proteger, de qué o de quién se necesita protegerlo (amenazas) y cómo va a protegerse***. Lo anterior se obtiene a través del ejercicio de establecer cuáles son los posibles riesgos y realizar un ordenamiento de los mismos de acuerdo a un nivel de prioridad.

Identificación de lo que se quiere proteger

- Hardware.- Computadoras, líneas de comunicación.
- Software.- Sistema Operativo, Manejador de Base de Datos, Servidor de Web, programas que permiten la comunicación por la red.
- Datos.- Durante la ejecución, almacenamiento en línea, respaldos, bases de datos.

Amenazas a tales recursos del sistema

- Hardware.- Que sufra alguna descompostura por uso inadecuado de personas externas o internas al sistema.
- Software.- Problemas con la prestación de los servicios de WWW, Base de datos o de los sistemas de comunicación.
- Datos.- Que usuarios internos o externos al sistema logren de alguna manera corromper la información, convirtiéndola en información no confiable o no útil.

Cómo se va a proteger

- Hardware.- Se piensa proteger mediante la instalación de dispositivos específicos de protección (UPS, reguladores de voltaje y supresores de picos de corriente, etc.) y mediante la ubicación del equipo en un espacio reservado para su uso específico con acceso controlado.
- Software.- Será protegido a través de políticas y procedimientos de administración por parte del personal responsable del buen funcionamiento del servidor.
- Datos.- Serán protegidos por medio de la autentificación de usuarios, por la asignación de dominios para el acceso, y por medio de respaldos periódicos.

5.6 Análisis y diseño de la base de datos

El modelo Entidad-Relación (Kroenke, 1996) se basa para su diseño en algunas estructuras comunes, como lo son:

Entidades.- Una entidad es algo que puede identificarse en el ambiente de trabajo de los usuarios, es algo importante para los usuarios del sistema que se va a desarrollar.

Atributos.- Las entidades tienen atributos o, en ocasiones se les llaman propiedades, que describe las características de una entidad.

Identificadores.- Las ocurrencias de una entidad tienen nombres que las identifican con el fin de reconocer una ocurrencia en particular. Un identificador puede ser único de tal manera que sólo identificará a una sola ocurrencia, en cambio, si no lo es, el valor identificará a un conjunto de éstas.

Relaciones.- Las entidades pueden asociarse una con otra en relaciones. El modelo E-R contiene clases de relaciones y ocurrencias de relaciones. Las clases de relaciones son asociaciones entre las clases de entidades y las ocurrencias de relaciones son asociaciones entre las ocurrencias de entidades.

Una vez mencionadas las características principales del módelo E-R, se explican cada uno de los pasos que se siguieron para desarrollar el modelado de datos para este sistema.

Definición de Entidades

Las entidades que se han detectado dentro del SGS son las siguientes:

- Usuario
- Módulo externo
- Banco de Control de Recursos (BCR)
- Datos del sistema (DS)
- Datos personales del usuario (DPU)
- Datos académicos del usuario (DAU)
- Datos académicos de Estudiantes.
- Datos académicos de Egresados.
- Datos académicos de Docentes.

Definición de las Relaciones existentes

Como primer punto, se menciona la relación *Usuario-Módulo Externo.* Esta relación es necesaria para que el usuario pueda tener acceso tanto al Sistema Global de Seguridad en el caso de los administradores, como al banco de notas de cursos y al banco de reactivos y exámenes.

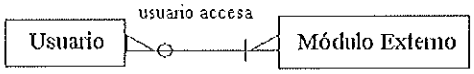


Figura 29. Relación existente entre la tabla usuario y módulo externo

La relación entre estas dos entidades es de muchos a muchos (M:N), ya que un usuario puede accesar varios módulos y un módulo puede o no, ser accesado por uno o muchos usuarios.

También se debe considerar las relaciones entre *Usuario, Datos personales y Datos académicos*. Esto es importante porque un usuario que accesa al sistema deberá tener en el registro al menos sus datos personales, académicos y los datos del sistema. La relación *Usuario-Datos personales* deberá ser de muchos a uno (N:1), ya que una persona que accese al sistema podrá tener varias cuentas, por ejemplo, una persona que administre el sistema podrá tener dos cuenta, una de ellas sería con los derechos de administrador y la otra sería como usuario ordinario. Por otro lado, la relación *Usuario-Datos del sistema* deberá ser de uno a uno (1:1), ya que cada cuenta tendrá su restricción particular. Por último queda indicar que la relación *Usuario-Datos Acádemicos* será de muchos a uno (N:1).

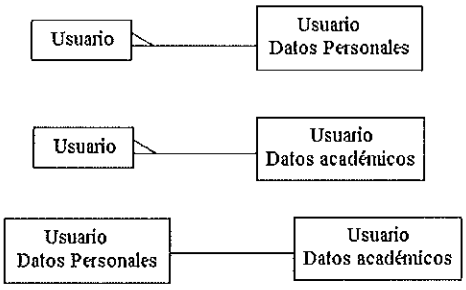


Figura 30. Relación existente entre la tabla usuario y datos, personales y datos académicos.

También se puede observar que la entidad *Usuario Datos Académicos* tiene tres entidades subtipo, *Estudiantes, Egresados y Docentes*, esto es así porque un usuario debe pertenecer solamente a uno de estos tres dominios para accesar a nuestro sistema, esto indica, que estas tres entidades subtipo son mutuamente excluyentes.

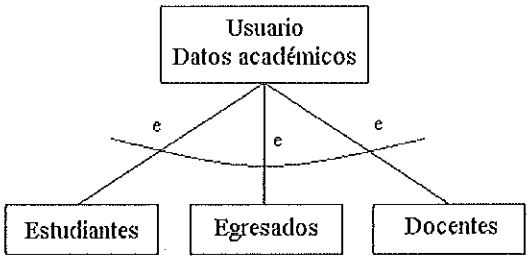


Figura 31. Relación existente entre las tabla datos académicos, estudiantes, egresados y docentes

Una última relación involucra a las entidades *Módulo externo* y *Banco de Control de Recursos*, esta relación es de muchos a uno (N:1), ya que varios módulos pueden estar haciendo peticiones sobre alguna información a dicho banco de datos. Esta relación servirá para mantener el control de los recursos que estan siendo utilizados en dicho momento por los usuarios.

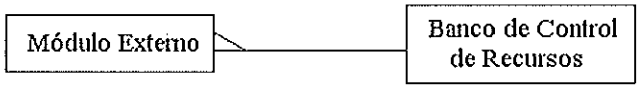


Figura 32. Relación existente entre las tabla módulo externo y banco de control de recursos.

Por otra parte es importante mencionar que la entidad *Banco de Control de Recursos* se relaciona con las entidades *Usuario*, *DPU*, *DAU* de uno a muchos (1:N) con cada una de ellas, esto es así, porque en algunas ocasiones será necesario que el *Banco de Control de Recursos* consulte alguna de esta información para un determinado usuario.

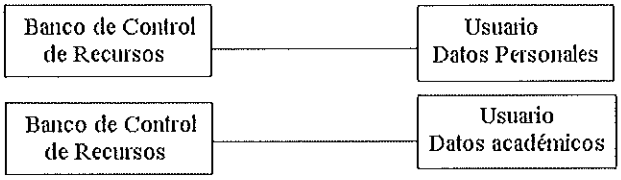


Figura 33. Relación existente entre las tablas datos personales, datos académicos y banco de control de recursos.

Tablas desarrolladas

A continuación se mencionan tanto las tablas a utilizar como cada uno de los campos que en ellas se encuentran.

La primer tabla que se menciona es la de usuarios:

Tabla I.- Descripción de la tabla usuario

Usuario
Login_id
Derechos_id
Password

En esta tabla se encuentran todos los datos del sistema relacionados con un usuario en particular, tales datos son su *login*, el tipo de derechos que este usuario posee y el *password* asignado a dicho usuario. El *login* será único para cada usuario, así que servirá como llave primaria para relacionar la tabla de usuarios con la tabla de datos personales. El *password* servirá como clave o contraseña y por último, el campo

Derechos_id direccionará directamente a la información concerniente al nivel de acceso con el que cuenta dicho usuario.

Tabla II.- Descripción de la tabla Derechos

Derechos
Derechos_id
Descripción

Esta tabla contiene la información de cada uno de los niveles de acceso disponibles para este sistema y solamente consiste de dos campos, el primero es un identificador para diferenciar cada uno de los niveles de seguridad y un segundo campo el cual sirve para dar una breve descripción de dicho identificador.

Tabla III.- Descripción de la tabla Datos Personales

Datos Personales
Login_id
Nombre
Apellido
Dirección
Teléfono
C.P.
Ciudad
Estado
Pais
E-mail

Como se puede observar en la tabla anterior, el sistema almacenará los datos personales de los usuarios, los cuales servirán para que en algún momento puedan ser localizados y obtenidos con una mayor facilidad. Aquí la llave primaria será el campo *login_id.*

Tabla IV.- Descripción de la tabla *Datos Academicos*

Datos Academicos
Clave_id
Login_id
Universidad
Unidad académica
Escuela

Ahora, como se mencionó anteriormente en el modelo relacional, el usuario tendrá también almacenados en los registros sus datos académicos. En primer lugar se tendrá la *clave_id* que contendrá la clave del docente ó la matrícula del estudiante o egresado dependiendo el caso, y el *login_id* como llaves primarias, también contará con los siguientes campos: universidad, unidad académica y escuela.

Es importante mencionar que los datos contenidos en esta tabla (datos académicos) serán complementadas por una de las tres tablas siguientes*: Estudiantes, Egresados y Docentes*. Esto se hizo con el fin de mantener un registro bien estructurado acerca de las personas que visitan el sistema y así poder tener estadísticas confiables. Las tablas se muestran a continuación:

Tabla V.- Descripción de la tabla *Estudiante*

Estudiantes
Clave_id
Carrera
Semestre

Tabla VI y VII.- Descripción de las tablas *Egresados* y *Docentes*.

Egresados
Clave_id
Carrera
Fecha de Egreso
Titulado

Docentes
Clave_id
Grado

Como se puede observar estas tablas estarán relacionadas con la tabla de datos académicos mediante *clave_id*, mencionados con anterioridad. Además de contener algunos datos específicos para cada tipo de usuario académico.

A continuación se presenta la tabla de Banco de Control de Recursos (BCR) que servirá para almacenar el *login_id, recurso_id y TEntrada*. Es decir, aquella información relacionada con el usuario que actualmente se encuentre dentro del sistema. El *login_id* se utilizará, como se ha mencionado con anterioridad, para relacionar estos datos con los datos personales y académicos. El *recurso_id* se encargará de relacionar esta tabla con la tabla de recursos disponibles para ese usuario en particular. El campo *TEntrada* contendrá la hora en que el usuario ingreso al sistema.

Tabla VIII.- Descripción de la tabla de Control de Recursos

BCR
Login_id
Recurso_id
TEntrada

Ahora, se mencionará la tabla de *recursos*, que se encuentra formada por los campos *recurso_id y descripción*. Esta tabla corresponde a la entidad Módulo externo la cual existe en el modelado de datos.

Tabla IX.- Descripción de la tabla *Recursos*

Recursos
Recurso_id
Descripción

Por último, se mencionará que las tablas *IPs, Estadisticas* y *Int-Login-Recurso*, son requeridas para la generación de reportes estadísticos acerca del uso de cada uno de los recursos que integran el sistema MADL. Los campos contemplados en cada una de estas tablas pueden ser observados a continuación:

Tabla X.- Descripción de la tabla *IP's*

IPs
Login_id
IPAddress

Tabla XI.- Descripción de la tabla *Estadisticas*

Estadisticas
Login_id
Fecha
HoraEntrada
HoraSalida
IPAddress

Tabla XII.- Descripción de la tabla *Int-Login-Recurso*

Int-Login-Recurso
Login_id
Recurso_id
Fecha
HoraEntrada

5.7 Instalación y configuración del equipo de cómputo requerido

Para el desarrollo del presente trabajo se requirió instalar el sistema operativo Windows NT Server 4.0 y algunos de los sistemas que se encuentran dentro del conjunto de herramientas que conforman el MS BackOffice. Se recurrió a esta plataforma debido a un requerimiento realizado por el administrador del proyecto.

Una vez definido esto, se llevó a cabo la instalación de dicha plataforma, así como algunas otras herramientas tales como un servidor WWW, un manejador de bases de

datos, compiladores para el desarrollo del sistema y software necesario para las máquinas cliente. Para llevar a cabo esta tarea, se asignó equipo de cómputo que está conformado actualmente de seis computadoras. También fue necesario contar con una subred propia de tal manera que ésta fue definida como dominio propio de la plataforma.

La realización de esta labor arrojó como resultado la instalación de dos Servidores Windows NT los cuales recibieron el nombre de CIMARRON y CORAL, el primero es el servidor primario y actualmente controla el dominio llamado CIMARRONES y el segundo es utilizado como servidor de respaldo para los casos en que el servidor primario experimente alguna falla en su funcionamiento. También se instaló una estación de trabajo NT (Windows NT Workstation) y tres máquinas cliente con el sistema operativo Windows 95.

Una vez hecha la instalación de cada uno de los servidores, se instalaron tanto el servidor WWW como el manejador de base de datos necesarios. El servidor WWW instalado fue el Java Web Server 2.0, debido a que este soporta el manejo de servlets, en cuanto al servidor de base de datos se apegó a los requerimientos establecidos y se optó por el MS SQL server versión 6.5 el cual viene incluido en el grupo de herramientas del Backoffice.

5.8 Desarrollo del interfaz WWW-BD

Para el desarrollo del interfaz del usuario y de la conexión entre las aplicaciones y la base de datos se utilizó el lenguaje Java y sus especificaciones de conectividad con bases de datos (JDBC) y aplicaciones del lado del servidor (Servlets). La arquitectura utilizada se muestra a continuación (Sridharan, 1997).

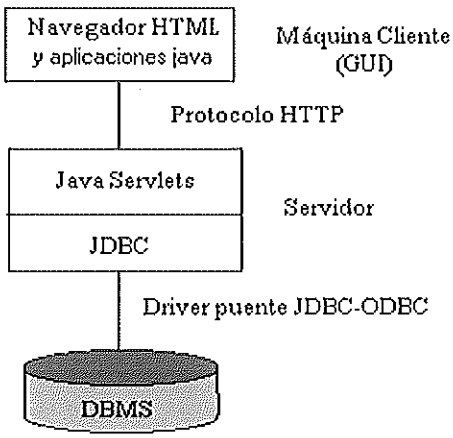


Figura 34. Diagrama que muestra la arquitectura utilizada para la conexión entre el interfaz del usuario y el manejador de base de datos.

5.9 Desarrollo de la Base de Datos

El sistema de base de datos fue desarrollado utilizando el Manejador de Base de datos (DBMS) SQL Server 6.5 de Microsoft. Este manejador facilitó la implantación de algunas políticas de seguridad, las cuales son mencionadas a continuación:

Política #1a.- Creación de diferentes bases de datos

Esta nace a raíz de la necesidad de mantener independientes los diferentes módulos que conforman el sistema MADL, para que cada uno de ellos administre la

información que le compete, con el fin de que si en algún momento la seguridad de un módulo se viera comprometida, los demás no se vean tan afectados.

Política #2a.- Creación de un dominio para cada tipo de usuario

Dentro de la base de datos correspondiente al módulo de seguridad, fueron asignados dominios o alcances para cada tipo de usuario, es decir, se les asignan privilegios que le permiten desempeñar un rol específico (administrador del sistema, administrador de subsistema o usuario ordinario). Es importante mencionar que los privilegios que se le asignan definen la capacidad del usuario para acceder a la información que solicita.

VI. RESULTADOS

Para el desarrollo de este sistema se establecieron tres tipos de políticas de seguridad, 1) las controlan el acceso al mismo, 2) las que protegen la información almacenada en el sistema y 3) las que permiten salvaguardar la integridad física del equipo de cómputo. Para cumplir con el primer tipo de política, se estableció un mecanismo tradicional, en donde el usuario tiene que introducir al sistema un identificador único y una clave asociada a éste, de esta manera el sistema podrá verificar la información y conocer si el usuario es válido o no. También se establecieron distintos tipos de usuarios, los cuales son: *Administrador (super-usuario), Administrador del BNC, Administrador del BRETA* y *Usuario ordinario*. Para proteger la información almacenada en la base de datos, se han implementado tres políticas de seguridad, la primera permite definir el dominio o alcance que tendrá cada tipo de usuario dentro del sistema, la segunda ofrece un mecanismo para verificar que los recursos son utilizados correctamente por cada uno de los usuarios y la tercera política se refiere a la dedicación que debe tener el administrador del sistema para éste, es decir, que monitoree los recursos utilizados periodicamente y que respalde constantemente la información almacenada. Por último se mencionará que se han instalado dispositivos específicos como UPS y reguladores de voltaje para proteger el equipo de cómputo requerido, además se destinó un espacio reservado para la ubicación de este equipo, con el fin de mantener el acceso controlado al mismo.

Se recurrió a la metodología OMT como herramienta principal para el análisis y diseño del sistema, el resultado de este ejercicio concluyó con la obtención de un modelo de objetos en donde se pueden apreciar cada una de las clases que conforman el sistema, un módelo dinámico en donde se aprecian los eventos existentes entre cada uno de los objetos utilizados y un diagrama funcional en donde se nos permite conocer cual será el flujo de datos dentro del sistema.

El Sistema Global de Seguridad utiliza una arquitectura cliente-servidor de tipo lógico distribuído y ha sido desarrollado utilizando el lenguaje Java como herramienta principal de desarrollo, así como algunas de sus aplicaciones como JDBC y Servlets. Este sistema se encuentra implementado bajo una plataforma Windows NT.

VII. DISCUSIÓN

Hoy en día los sistemas de seguridad son una parte fundamental de cualquier aplicación, pretendiento con estos que el sistema no interrumpa sus servicios por daños ocasionados por parte de los usuarios, además, que la información almacenada en dicha aplicación sea confiable en todo momento, garantizando las características de privacidad e integridad de la misma, así como la disponibilidad de los recursos.

Con respecto a las políticas de seguridad establecidas para este sistema, primero se mencionarán aquellas que controlan el acceso al mismo. El mecanismo que se utiliza es el esquema tradicional donde se tiene un par (identificador público, clave secreta asociada). Este esquema garantiza que sólo usuarios que especifiquen una pareja (identificador, clave) válida son los que tendrán acceso al mismo. Un requerimiento adicional para este, es que las claves asociadas deben ser protegidas, por ejemplo usando encriptación (Rusell et. al, 1992). En cuanto a la protección de la información almacenada en el sistema, se han establecido ciertas políticas de seguridad las cuales permiten al manejador de base de datos denegar cualquier acceso a la información a aquellos usuarios que no tienen privilegios de administrador, en los casos donde el sistema maneje información delicada a través del cliente, por ejemplo claves de usuarios o información de exámenes, se ha considerado la encriptación de información. Ha este mecanismo para resguardar la información se añaden las políticas mencionadas respecto

a mantener el buen funcionamiento del equipo de cómputo necesario para operar el sistema.

Respecto a la negativa de aceptar usuarios visitantes anónimos (guest) al sistema es por el hecho de que el usuario puede enmascarase en el anonimato para producir algún tipo de problema, además, esto no permitiría tener un monitoreo individual adecuado de cada uno de los usuarios que se encuentren dentro del mismo, así como de los recursos que están utilizando. Esto lleva a la siguiente política, donde para casos específicos de acceso a recursos (como los exámenes en línea), donde sólo se permitirá una sesión por usuario a la vez, con el fin de que el usuario no pueda estar haciendo el examen de un tema en particular en una sesión y en otra estar viendo las notas asociadas a esta evaluación, además, al restringuir al usuario a una sola sesión, permite al sistema realizar un monitoreo más eficaz de los recursos que están siendo utilizados en ese momento por el usuario.

Se considera que la clasificación de los diferentes tipos de usuarios que existen dentro del sistema, así como los niveles de acceso asignado a cada uno estos satisface los requerimientos de manera adecuada, ya que esto ha permitido mantener el control de los roles que le corresponden a cada uno de estos y de los recursos que están utilizando mediante un adecuado monitoreo de los mismos. Esta política de seguridad es utilizada también por otros sistemas aplicados a la enseñanza en línea tales como BlackBoard (http://www.blackboard.net) y Virtual-U (http://www.vlei.com). Una de las principales

diferencias ente el sistema propuesto en este documento y estos sistemas, es que tanto blackboard como Virtual-U, delegan la seguridad al sistema operativo sobre el que se ejecutan (Unix, Windows NT, etc.), es decir, confían plenamente en los mecanismos de seguridad que les puede brindar la plataforma en donde están instalados, mientras que el SGS proporciona además un nivel propio de seguridad.

Los modelos de seguridad utilizados, fueron seleccionados después de hacer una investigación con respecto a los distintos modelos de seguridad y a los requerimientos establecidos para este sistema. Los modelos seleccionados son ampliamente utilizados, y dos de los ejemplos más importantes de su utilización son Kerberos (Atkins, et al, 1996) y Satan (Freiss, 1997). Kerberos se basa en un modelo ampliamente probado con niveles tanto de autentificación como de autorización para el permitir el acceso a los usuarios. Mientras que para el monitoreo de los recursos del sistema, con la finalidad de encontrar posibles anomalías en el uso por parte de los usuarios, se utiliza el modelo basado en auditorías utilizado por Satan.

Específicamente el sistema ha sido desarrollado con base en un modelo cliente/servidor de tipo *lógico distribuido*, el cual permite dividir las aplicaciones (programas) entre un cliente y un servidor. Comúnmente, una aplicación con interfaz gráfica de usuario (GUI) reside del lado del cliente y es la encargada de dirigir o controlar el flujo de datos de la aplicación, mientras las aplicaciones lógicas están del lado del servidor, primordialmente para ejecutar las políticas de seguridad y el manejo de la base

de datos. Los procesos entre el cliente y el servidor se mantienen en comunicación mediante una capa intermedia de funcionalidad llamada *Middleware*, la cual ofrece un nivel conveniente de seguridad al momento de accesar la información almacenada en la base de datos (modelo de 3 capas o *three-tier*) (Graham, 1997).

Las principales ventajas de este diseño se mencionan a continuación:

- La arquitectura cliente-servidor permite al usuario accesar de manera fácil y rápida la información o aplicaciones requeridas, aún cuando sólo parte de la aplicación (el cliente) resida de su lado.
- La arquitectura permite que los mecanismos de acceso puedan ser distribuidos y a la vez mantener los mecanismos de almacenamiento y control centralizados.
- La arquitectura cliente-servidor brinda un ambiente flexible para el desarrollo de nuevas aplicaciones (Jenkins, et al, 1996). Si se mantiene el interfaz entre cliente y servidor, se pueden realizar modificaciones y extensiones a cada uno de ellos por separado, disminuyendo la complejidad de esta tarea.

Por otro lado, Java fue el lenguaje seleccionado para el desarrollo de las aplicaciones del lado del servidor (aquellas que accesan a la informacion en la base de datos), y para el desarrollo de la interfaz gráfica de usuario del lado del cliente.

Las principales ventajas que proporciona utilizar esta herramienta para la implementación se mencionan a continuación:

- Java proporciona características que hacen de él uno de los lenguajes de programación más adecuados para desarrollar un sistema como el presente, tales características incluyen: portabilidad o independencia de plataforma, robustez, orientación a objetos, además de que proporciona herramientas específicas para conectividad con bases de datos (*Java Database Conectivity* –JDBC) y desarrollo de interfaces gráficas de usuario (*Swing – Java Foundation Classes* – JFC) (Vanderburg et al, 1997).
- Java es un lenguaje diseñado con el objetivo de ser usado bajo un esquema cliente-servidor o de sistemas distribuidos bajo redes de telecomunicaciones de cobertura amplia como Internet (Horstmann et al, 1997). Proporciona de manera estándar bibliotecas de componentes y especificiones especializadas para ello, tales como *Applets y Servlets.*

VIII. CONCLUSIONES Y TRABAJO FUTURO

Aún cuando el sistema todavía se encuentra en un proceso de desarrollo, con un avance estimado del 90%, ha permitido realizar pruebas de funcionalidad a los módulos existentes (mecanismo de acceso al sistema y monitoreo de uso de recursos) obteniéndose resultados adecuados. Incluso esto se ha realizado considerando diferentes plataformas tales como Windows NT y Linux (el cliente) sin experimentar problemas en ninguno de los casos.

Con base en las pruebas realizadas (por módulos, de integración y de sistema), se considera que la combinación seleccionada de:

- Modelo de Seguridad: Control de acceso en dos niveles (Autentificación y Autorización) y Monitoreo por Auditorías.
- Arquitectura: Cliente-Servidor lógico distribuido y en 3 capas.
- Tecnología de Comunicación: Internet y el WWW.
- Lenguaje y Herramientas: Java, JFC, JDBC y Servlets.

fue adecuada para el desarrollo del SGS y para satisfacer las necesidades del MADL. Sin embargo, es necesario completar la funcionalidad del sistema y realizar la validación del mismo en términos de operación en un ambiente real de utilización. Actualmente se está trabajando en la elaboración del plan de trabajo para esta siguiente fase.

Para concluir con la presente versión falta completar la parte de encriptación de la información, aunque en estos momentos se están desarrollando otras aplicaciones que le darán mayor funcionalidad al sistema.

IX. BIBLIOGRAFÍA

Russell, D. y G.T. Gangemi Sr. 1997.Computer Security Basics. O'Reilly.

Pressman. 1997. Engineering Systems. Fourth Edition.

Fairley. 1994. Ingeniería del Software. Addisson-Wesley.

Rumbaugh, J., Blaha, Premerlani, Eddy, Lorensen.1991.Object-Oriented Modeling and Design. Prentice Hall.

Korth, H., A. Silberschatz. 1993. Fundamentos de las bases de datos. McGraw-Hill.

Kroenke, D. 1996. Procesamiento de Bases de Datos: Fundamentos, Diseño e Implementación. Prentice-Hall. 55-75 pag.

Sridharan, P. 1997. Advanced Java Networking. Prentice Hall. E.U. 205-256 pag.

Atkins, D., P. Buis, C. Hare, R. Kelley. 1996. Internet Security *Professional Reference*. New Riders publishing. E.U. 535 pag.

Freiss, M. 1998. Protecting networks with Satan. O'Reilly. E.U.

Jenkins, N. et, al., 1996. Client/Server unleashed. First Edition. Sams Publishing. E.U. 7-19 pag.

Horstmann, C., G. Cornell. 1997. Core Java fundamentals. volume 1. Prentice Hall. E.U. 6-7 pag.

Siyan K., C. Hare. 1995. Internet Firewalls and Network Security. New Riders publishing. E.U.90-114, 123-128, 137 pag.

Graham, H., R. Cattell, M. Fisher. 1997. JDBC Database Access with Java. A Tutorial and Annotated Reference. Addisson Wesley. E.U.

Vanderburg G., et al. 1997. Maximum Java 1.1. First Edition. Sams Publishing. E.U. 377-398 pag.

Ayala & Yano 96, Ayala, G. & Yano, Y. Communication Languages and Protocols in an agent- based collaborative learning environment. In Proceedings of the 1996 IEEE International Conference on Systems, Man and Cybernetics, Vol.3, pp. 2078-2087.

Collis, B. Collis. 1999. Applications of Computer Communications in Education: An Overview. IEEE Communications Magazine, N3, 1999.

Mc Conell, S. 1996. Rapid Development. McGraw Hill.

Organista J., Backoff E. 2000. El uso de internet en el proceso enseñanza-aprendizaje: opinión de los estudiantes de educación superior. CEAD 2000. Ensenada, México.

Páginas de Internet

BlackBoard (http://www.blackboard.net)

Virtual-U (http://www.vlei.com).

X. ANEXOS

GLOSARIO

API: Application Programming Interface.

BCR: Bano de Control de Recursos.

BD: Base de Datos.

BNC: Banco de Notas de Cursos.

BREA: Banco de Reactivos y Exámenes.

CASE: Computer Assistance Software Engieneering.

CECUUE: Centro de Cómputo Universitario Unidad Ensenada.

CGI: Common Gateway Interface.

CICESE: Centro de Investigación Científica y de Enseñanza Superior de Ensenada.

DAU: Datos Académicos del Usuario.

DBMS: DataBase Management System.

DPU: Datos Personales del Usuario.

DSU: Datos de Sistema del Usuario.

GUI: Graphical User Interface.

HTML: HyperText Markup Language.

HTTP: HyperText Transfer Protocol.

IIO: Instituto de Investigaciones Oceanológicas.

JDBC: Java DataBase Connectivity.

JDK: Java Development Kit.

JFC: Java Foundation Classes.

JVM: Java Virtual Machine.

LAN: Local Network Area.

MADL: Material de Apoyo Docente en Línea.

OMT: Object Modeling Technique.

RPC: Remote Process Call.

SGS: Sistema Global de Seguridad.

SQL: Structured Query Language.

UABC: Universidad Autónoma de Baja California.

WAN: World Area Network.

WWW: World Wide Web.

UPS: Uninterruptible Power Supply.

CEAD: Congreso de Educación Abierta y a Distancia.

ANEXO A. CUESTIONARIO PARA ESTUDIANTES.

1.- ¿Consideras que la Universidad te proporciona los recursos (libros, Internet, asesorías) necesarios para encontrar información acerca de una materia en particular?

Sí ( ) No ( )

2.- Cuando necesitas profundizar sobre algún tema, ¿Qué recursos utilizas con mayor frecuencia? Enumérese en orden de prioridad.

( ) Material de biblioteca
( ) Internet
( ) Notas
( ) Consultas a maestros (Asesorías)

3.- Al navegar por Internet, ¿Encuentras fácilmente temas relacionados con las materias que estas cursando?

Sí ( ) No ( )

4.- De las siguientes opciones, ¿Qué tipo de información te gustaría encontrar sobre alguna de tus materias?

( ) Conceptos Básicos
( ) Ejemplos
( ) Artículos de revistas
( ) Cuestionarios
( ) Notas de cursos

5.- Una vez encontrada la información, ¿ Su formato te facilita la comprensión de la misma?

Sí ( ) No ( )

6.- ¿En qué formato te gustaría encontrar la información?

( ) Texto ( ) Audio ( ) Otro

( ) Video ( ) Imágenes Especifica _____

7.- En los sitios visitados a través de Internet ¿Haz encontrado foros de discusión sobre algunas de las materias que cursas actualmente?

Sí ( ) No ( )

8.- ¿Consideras útil el que se desarrolle un sistema en línea para una materia en particular, que cuente con un foro de discusión, y cuya información sea presentada en los formatos de páginas HTML's, Audio y Video? y ¿Por qué?

Sí ( ) No ( )

ANEXO B. CUESTIONARIO PARA MAESTROS E INVESTIGADORES.

1.- Cuando busca información referente a un tema, ¿considera que esta información es clara y precisa?

Sí ( ) No ( )

2.- ¿Considera que la información proporcionada dentro del curso que imparte, es suficiente para el buen entendimiento del mismo?

Sí ( ) No ( )

3.- ¿ Qué requisitos cree usted que debe tener un sistema de apoyo en línea para los estudiantes?

4.- ¿Qué resultados esperaría usted de una herramienta como lo es el Sistema de apoyo en línea?

5.- ¿Es frecuente que sus alumnos le comenten que es difícil encontrar información sobre algún tema?

Sí ( ) No ( )

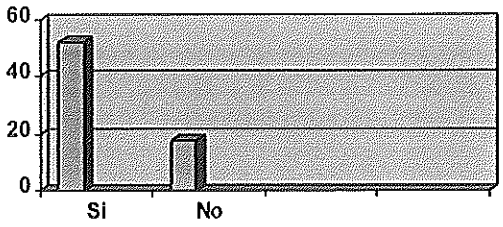
6.- ¿En que formato le gustaría que apareciera la información?

HTML ( ) Audio ( )

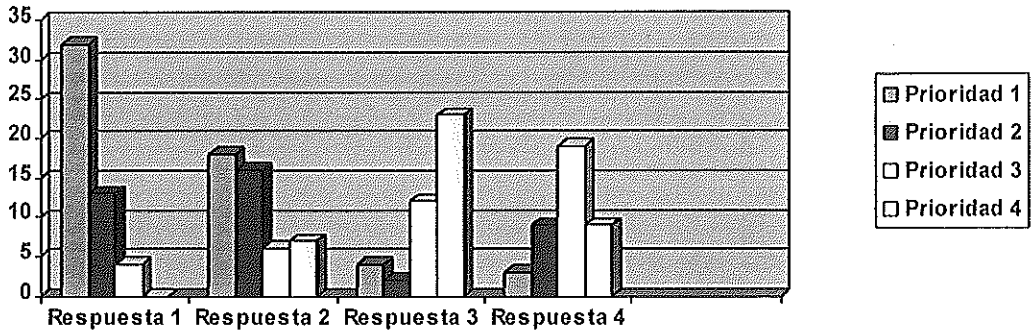
Video ( ) Gráficos ( )

ANEXO C. RESUMEN DE RESPUESTAS DEL CUESTIONARIO PARA ALUMNOS.

Pregunta 1: ¿Consideras que la Universidad te proporciona los recursos (libros, Internet, asesorías) necesarios para encontrar información acerca de una materia en particular?

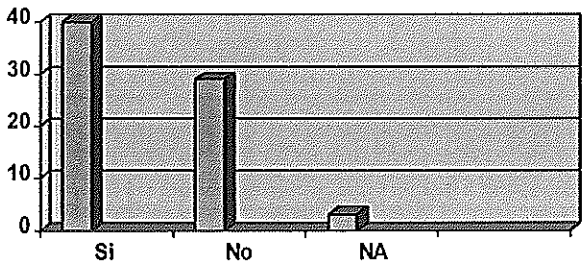


Pregunta 2: Cuando necesitas profundizar sobre algún tema, ¿qué recursos utilizas con mayor frecuencia? Enumérese en orden de prioridad.



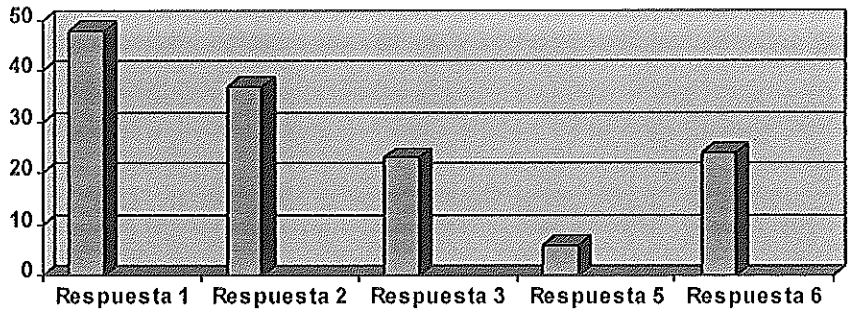
Respuesta 1→ Material de Biblioteca.
Respuesta 2→ Internet.
Respuesta 3→ Notas.
Respuesta 4→ Asesorías.

Pregunta 3: Al navegar por Internet, ¿Encuentras fácilmente temas relacionados con las materias que estás cursando?



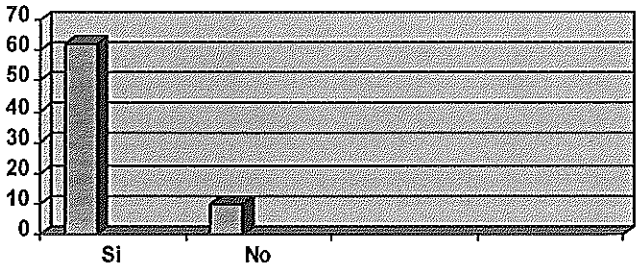
NA→ No aplica

Pregunta 4: De las siguientes opciones, ¿qué tipo de información te gustaría encontrar sobre alguna de tus materias?

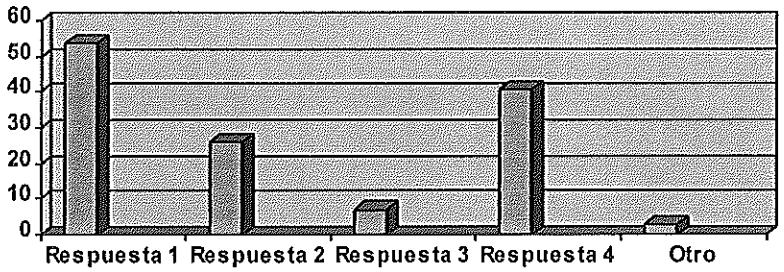


Respuesta 1→ Conceptos Básicos.
Respuesta 2→ Ejemplos.
Respuesta 3→ Artículos.
Respuesta 4→ Cuestionarios.
Respuesta 5→ Notas de cursos.

Pregunta 5: Una vez encontrada la información, ¿ Su formato facilita la comprensión de la misma?

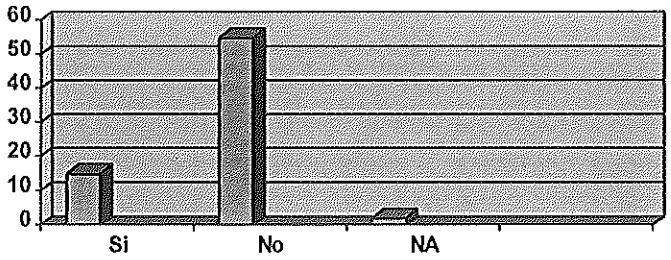


Pregunta 6: ¿En qué formato te gustaría encontrar la información?



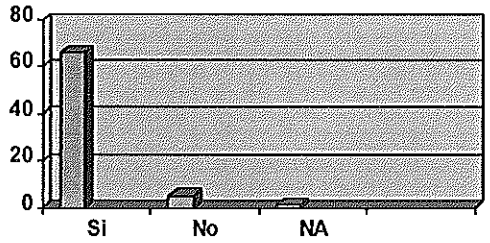
Respuesta 1→ Texto.
Respuesta 2→ Video.
Respuesta 3→ Audio.
Respuesta 4→ Imágenes.
Respuesta 5→ Otro.

Pregunta 7: En los sitios visitados a través de Internet ¿Haz encontrado foros de discusión sobre algunas de las materias que cursas actualmente?



NA→ No aplica

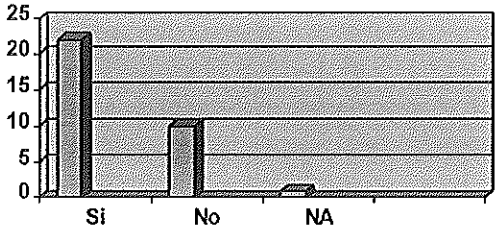
Pregunta 8: ¿Consideras útil el que se desarrolle un sistema en línea para una materia en particular, que cuente con un foro de discusión, y cuya información sea presentada en los formatos de páginas HTML's, Audio y Video? y ¿Por qué?



NA→ No aplica

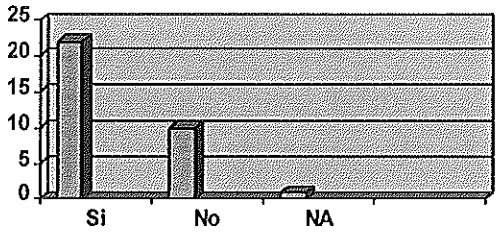
ANEXO D. RESPUESTA DEL CUESTIONARIO DE MAESTROS E INVESTIGADORES.

Pregunta 1: Cuando busca información referente a un tema, ¿considera que esta información es clara y precisa?



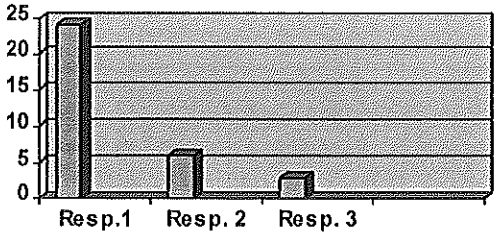
NA→ No aplica

Pregunta 2:¿Considera que la información proporcionada dentro del curso que imparte, es suficiente para el buen entendimiento del mismo?



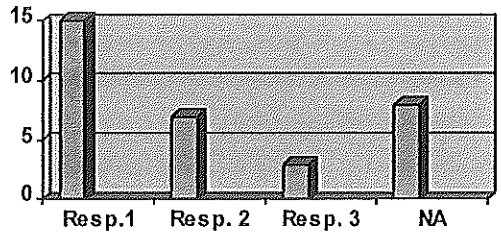
NA→ No aplica

Pregunta 3: ¿ Qué requisitos cree usted que debe tener un sistema de apoyo en línea para los estudiantes?



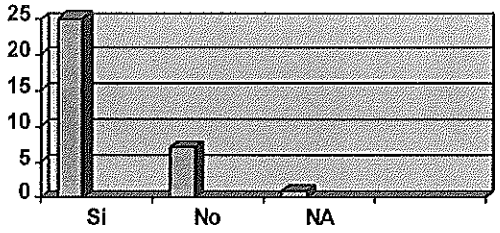
Respuesta 1→ Claridad en la información y rápido acceso.
Respuesta 2→ Proporcionar información actualizada.
Respuesta 3→ Proporcionar una variedad de temas.
NA→ No aplica

Pregunta 4: ¿Qué resultados esperaría usted de una herramienta como lo es el Sistema de apoyo en línea?



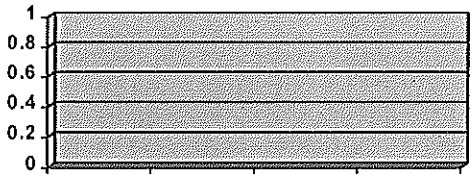
Respuesta 1→ Aclarar dudas.
Respuesta 2→ Mantenerse actualizado.
Respuesta 3→ Evitar pérdida de tiempo.
NA→ No aplica

Pregunta 5: ¿Es frecuente que sus alumnos le comenten que es difícil encontrar información sobre algún tema?



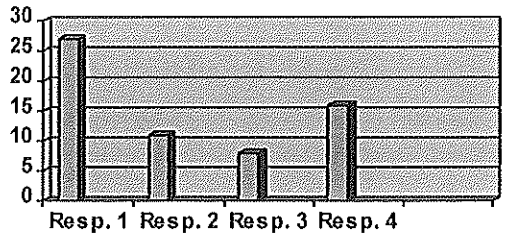
NA→ No aplica

Pregunta 6: De las materias que usted imparte, ¿cuál le gustaría que se incluyera en este sistema?



NA→ No aplica (las personas que contestaron esta pregunta, lo hicieron diciendo que la materia que ellos impartían).

Pregunta 7: ¿En que formato le gustaría que apareciera la información?



Respuesta 1→ Html
Respuesta 2→ Video
Respuesta 3→ Audio
Respuesta 4→ Gráficas
NA→ No aplica