DESARROLLO DEL MODULO DE ADMINISTRACIÓN Y SEGURIDAD DEL SISTEMA INTEGRADO DE INFORMACIÓN FINANCIERA DE LA UNIVERSIDAD DE NARIÑO (SIIFUN)

JUAN ANGEL SANTACRUZ LÓPEZ

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2006

DESARROLLO DEL MODULO DE ADMINISTRACIÓN Y SEGURIDAD DEL SISTEMA INTEGRADO DE INFORMACIÓN FINANCIERA DE LA UNIVERSIDAD DE NARIÑO (SIIFUN)

JUAN ANGEL SANTACRUZ LÓPEZ

Trabajo de Grado Presentado como Requisito parcial para optar al Título de Ingeniero de Sistemas

Asesor:
JAIRO ROBERTO PATIÑO
Ingeniero de Sistemas

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2006

“Las ideas y conclusiones aportadas en la tesis de grado, son responsabilidad exclusiva de su autor ”

Articulo 1° del acuerdo N° 324 de Octubre 11 de 1966, emanado del Honorable Consejo Directivo de la Universidad de Nariño.

AGRADECIMIENTOS

El autor expresa sus agradecimientos a:

Ing. Nelson Jaramillo Enríquez, Ingeniero de Sistemas, Director del departamento de Sistemas, por su colaboración y apoyo.

Fidel Zambrano, Ing de Sistemas, Gerente del proyecto. Por brindarme la oportunidad.

Jairo Patiño, Ing de Sistemas, Asesor del proyecto. por su gran ayuda.

A los compañeros del SIIFUN por el apoyo, el conocimiento y su amistad.

A todas las personas que de una u otra manera colaboraron en la realización de este proyecto.

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

Ing. Jairo Patiño
Asesor académico

_____

Ing. Franklin Eduardo Jiménez Giraldo
Jurado

San Juan de Pasto, Marzo de 2006

DEDICATORIA

A Dios, por darme vida, fortaleza, y la oportunidad.

A mi papá, porque no me dio las cosas fáciles, pero me dio el impulso.

A Ana Cecilia, Rosy, Nancy Angelita, Paola a toda mi familia y mis amigos.

A los que sin palabras me han ayudado fuertemente... David Santiago y mi mamá.

Juan Angel

CONTENIDO

		Pág.
INTRODUCCIÓN		16
TEMA		17
1.1	TITULO DEL PROYECTO	17
1.2	MODALIDAD	17
1.3	LÍNEA DE INVESTIGACIÓN	17
1.4	ALCANCE Y DELIMITACIÓN	17
2.	DESCRIPCIÓN DEL PROBLEMA	19
2.1	PLANTEAMIENTO DEL PROBLEMA	19
2.2	FORMULACION DEL PROBLEMA	19
2.3	SISTEMATIZACION DEL PROBLEMA	20
3.	OBJETIVOS	21
3.1	OBJETIVO GENERAL	21
3.2	OBJETIVO ESPECIFICO	21
4.	JUSTIFICACIÓN	22
		23
5.	ESTUDIO DE FACTIBILIDAD	23
5.1	FACTIBILIDAD TÉCNICA	23
5.1.1	Hardware	23
5.1.2	Software	25
5.2	FACTIBILIDAD ECONÓMICA	25
5.3	FACTIBILIDAD OPERATIVA	
6.	ANTECEDENTES	26
7.	METODOLOGÍA	27
8.	MARCO REFERENCIAL	29
8.1.	MARCO TEÓRICO	29
8.2	MARCO CONCEPTUAL	32
8.2.1	Arquitectura J2ee	32
8.2.1.1	Servidor de Aplicaciones	32
8.2.2	Sistema Manejador de Bases de Datos (Back – End)	33
8.2.3	Sistema Gestor de Base de Datos (Back-End)	33
9.	ESTUDIO DEL DISEÑO ETAPA 1 DEL SIIFUN.	34
		35
10.	CONTRUCCION DE LA BASES DE DATOS DEL SIIFUN	36
	MODULO ADMINISTRACIÓN	39
10.1	DICCIONARIO DE DATOS.	39
10.2	DISEÑO DE LA ESTRUCTURA GENERAL DEL SISTEMA.	39

10.2.1 Perfiles de Seguridad 39
10.3 HERRAMIENTAS TECNOLÓGICAS UTILIZADAS 39
10.3.1 Arquitectura del Software 39
10.3.2 Herramientas de Desarrollo 41

11. MANUAL DE OPERACIONES DEL SIIFUN MODULO ADMINISTRACION 41
11.1 INTERFACES 43
11.1.1 Ingreso al Sistema y Menús Principales. 44
11.1.2 Perfiles de Seguridad. 44
11.1.3 Conexión Validación De Usuarios Y Seguridad. 44
11.1.4 Ingreso A Los Diferentes Módulos del Siifun 44
11.2 DISEÑO E INTERFACES DEL MODULO ADMINISTRACIÓN DEL SIIFUN 46
11.2.1 Mapa de Navegación 48
11.2.2 Interfaz de Usuarios 49
11.2.2.1 Interfaz de Creación del Usuarios 50
11.2.2.2 Interfaz de Actualización Del Usuarios 51
11.2.3 Interfaz de Grupos 52
11.2.3.1 Interfaz de Creación de Grupos 53
11.2.3.2 Interfaz de Actualización de Grupos 54
11.2.4 Interfaz de Operaciones 55
11.2.4.1 Interfaz de Creación de Operaciones 55
11.2.4.2 Interfaz de Actualización de Operaciones 55
11.2.5 Interfaz de Cargos 56
11.2.5.1 Interfaz de Creación de Cargos 57
11.2.5.2 Interfaz de Actualización de Cargos 57
11.2.6 Interfaz de Notificaciones 58
11.2.6.1 Interfaz de Notificaciones Recibidas 58
11.2.6.2 Interfaz de Notificaciones Entregadas 59
11.2.6.3 Interfaz de Elaborar Notificaciones 60
11.2.7 Interfaz de Backups 60
11.2.8 Interfaz de Logs 61
11.2.8.1 Interfaz de Logs Listados 62

12. OPERACIÓN DEL SISTEMA POR EL USUARIO ADMINISTRADOR
12.1 CONFIGURACIONES E INGRESO DE DATOS 62

13. POLÍTICAS DE SEGURIDAD 64
13.1 DEFINICION DE POLÍTICAS DE SEGURIDAD INFORMÁTICA 64
13.2 CONTENIDO POLITICAS DE SEGURIDAD IMPLANTADAS EN EL MODULO DE ADMINISTRACION Y SEGURIDAD 64
13 GENERACION DE PROPUESTAS PARA LAS POLITICAS DE SEGURIDAD EXTERNAS AL SOFTWARE 77

14. CONCLUSIONES.

15. RECOMENDACIONES. 78

REFERENCIAS BIBLIOGRÁFICAS 79

LISTA DE FIGURAS

PAG

FIGURA 1. Mapa de Navegación 46
FIGURA 2. Interfaz de usuarios 48
FIGURA 3. Interfaz de creación del usuarios 49
FIGURA 4. Interfaz de actualización del usuarios 50
FIGURA 5. Interfaz de grupos 51
FIGURA 6. Interfaz de creación de grupos 52
FIGURA 7. Interfaz de actualización de grupos 53
FIGURA 8. Interfaz de operaciones 54
FIGURA 9. Interfaz de creación de operaciones 55
FIGURA 10. Interfaz de actualización de operaciones 55
FIGURA 11. Interfaz de cargos 55
FIGURA 12. Interfaz de creación de cargos 56
FIGURA 13. Interfaz de actualización de cargos 57
FIGURA 14. Interfaz de notificaciones 57
FIGURA 15. Interfaz de notificaciones recibidas 58
FIGURA 16. Interfaz de notificaciones entregadas 58
FIGURA 17. Interfaz de elaborar notificaciones 59
FIGURA 18. Interfaz de backups 60
FIGURA 19. Interfaz de logs 60
FIGURA 20. Interfaz de logs listados 61
62

GLOSARIO

CLIENTE-SERVIDOR es una arquitectura basada en que en los ordenadores de una red, algunos equipos se comportan como clientes (realizan petición) y otros como servidores (conceden la petición al cliente).

BASE DE DATOS es sencillamente un conjunto de tablas en las que se Almacenan distintos registros, con el fin de almacenar contenidos de una forma sistemática que nos permita clasificarlos, buscarlos y editarlos rápida y fácilmente.

SOFTWARE LIBRE se refiere a la libertad que tienen los usuarios para modificar, distribuir, estudiar, vender o cambiar el código fuente.

ARQUITECTURA DEL SOFTWARE hace relación a la estructura global del software y a la manera en que la misma, proporciona integridad conceptual al sistema. La arquitectura es la estructura jerárquica de cómo están constituidos los componentes del programa, la manera en la que interactúan sus componentes, y las estructuras de datos que los componentes van a utilizar.

FRONT-END es una arquitectura de Software en la que se desarrolla el aplicativo o se implementan las interfaces del usuario.

BACK-END es una Arquitectura de software; se denomina de esta manera, al sistema gestor de la Base de datos.

SERVIDOR se define como un computador con buena capacidad de proceso como de poder compartir recursos físicos; suministra información a las peticiones de los clientes.

HARDWARE son dispositivos electrónicos con capacidad de cálculo, dispositivos de interconexión y dispositivos electromecánicos que proporcionan una función externa del mundo real.

SOFTWARE se define como un conjunto de programas, instrucciones y lenguajes que permiten al sistema la ejecución de múltiples tareas.

INTERFAZ se entiende como un programa de computador que sirve de intermediario entre el usuario y la máquina, con el fin de facilitar la comunicación entre ellos.

NAVEGADOR: es un programa cliente que permite el acceso al servicio http en un servidor (a través de la red). El programa lee los documentos con el hipertexto y despliega el resultado en el computador del cliente.

URL es un identificador URL, permite encontrar una dirección en la red, para ello debe hacerse uso del navegador.

ADMINISTRADOR La persona que supervisa y controla el correcto funcionamiento de un sistema informático.

USUARIOS entendidos como, todas las personas que necesitan de la información del sistema e interactúan con él.

RESUMEN

Este documento muestra la información necesaria referente al desarrollo del proyecto: MODULO DE ADMINISTRACIÓN Y SEGURIDAD DEL SISTEMA INTEGRADO DE INFORMACIÓN FINANCIERA DE LA UNIVERSIDAD DE NARIÑO (SIIFUN)

El objetivo principal del proyecto es administrar y prestar seguridad al uso del SISTEMA DE INFORMACIÓN INTEGRAL Y FINANCIERO DE LA UNIVERSIDAD DE NARIÑO, para lo cual se desarrolla un sistema computarizado.

El proyecto nace de la necesidad de unificar, mantener organizada, controlada, y segura la información, a la vez de proveer de un rápido acceso al momento de manejar los recursos financieros de la universidad.

El desarrollo del proyecto permite aumentar los niveles de seguridad de la información, de igual manera protege los procesos involucrados del SIIFUN, como también da a conocer las Políticas de Seguridad internas y externas al software que se deben adoptar para proteger la información.

ABSTRACT

This document shows the necessary information with respect to the development of the project: I MODULATE OF ADMINISTRATION AND SECURITY OF THE INTEGRATED SYSTEM OF FINANCIAL INFORMATION OF THE UNIVERSIDAD DE NARIÑO (SIIFUN)
The main objective of the project is to administer and to lend security to the use of the INTEGRAL AND FINANCIAL SYSTEM OF INFORMATION OF THE UNIVERSIDAD DE NARIÑO, for that which an on-line system is developed.

The project is born of the necessity of unifying, to maintain organized, controlled, and sure the information, at the same time of providing from a quick access to the moment to manage the financial resources of the university.

The development of the project allows to increase the levels of security of the information, in a same way it protects the involved processes of the SIIFUN, as well as he/she gives to know the internal and external Politicians of Security to the software that you/they should be adopted to protect the information.

INTRODUCCIÓN

Siendo la Universidad de Nariño una institución de tan alta importancia en la región, debe contar con procesos eficaces y dinámicos que coincidan con su misión, visión y metas. Así, el área financiera, que es una de las principales dentro de la organización, necesita un sistema de información idóneo, integral y capaz de llevar a cabo las actividades que conducen a su óptimo funcionamiento. Que soporte la integridad de su información y que cuente con mecanismos de seguridad para cumplir sus objetivos.

Es una necesidad administrativa disponer de información homogénea y oportuna para la toma de decisiones, lo cual conduce al desarrollo del Sistema Integrado de Información Financiera de la Universidad de Nariño (SIIFUN) que permitirá que la entidad cumpla a cabalidad con las exigencias gubernamentales, sociales e internas.

El sistema mediante la elaboración de una única base de datos y la optimización de procesos, generará registros simultáneos a partir de una sola carga de datos, los cuales necesitan una protección en cada estación, y para todos los procesos. Es por ello que se necesita una organización y un motor de seguridad como lo es el objetivo de esta pasantía, con el fin de que se sometan todos los recursos tanto humanos como lógicos, a una administración de sus funciones y su iteración.

En este trabajo se dará soporte en el desarrollo de la administración de los usuarios del sistema, la protección de los datos y de la comunicación en la red, además se propondrán las políticas de seguridad de los procesos que queden fuera del alcance del control del sistema.

1. TEMA

1.1 TITULO DEL PROYECTO

DESARROLLO DEL MODULO DE ADMINISTRACIÓN Y SEGURIDAD DEL SISTEMA INTEGRADO DE INFORMACIÓN FINANCIERA DE LA UNIVERSIDAD DE NARIÑO (SIIFUN)

1.2 MODALIDAD

La modalidad del trabajo de grado corresponde a pasantía según acuerdo 046 del 17 de Abril del 2001 emanado por el Honorable Consejo Académico de la Universidad de Nariño.

1.3 LINEA DE INVESTIGACIÓN

El proyecto planteado se inscribe en la línea de Software y Manejo de Información.

1.4 ALCANCE Y DELIMITACION

La fase 2 del proyecto Sistema Integrado de Información Financiera de la Universidad de Nariño (SIIFUN) correspondiente al modulo de administración y seguridad comprende los siguientes ítems:

- Administración: Este módulo permite el manejo de usuarios del sistema a quienes se les dará una identificación y una clave para su ingreso. Esto permitirá monitorizar operaciones a los registros que ellos trabajen, como también la interpretación de la clase de usuarios para desplegar las interfaces de trabajo.

Para lograr este objetivo se desarrolló los siguientes sub-módulos:
Administración de Operaciones
Administración de Grupos
Administración de Usuarios
Administración de Cargos
Administración de Notificaciones

- Seguridad en la red: se establecieron los protocolos y demás herramientas que brindaran seguridad en la comunicación de la información a través de la red.

Para estos objetivos se desarrollaron los siguientes módulos:
Administración de Logs.
Administración de Backups.
Configuración de servidores de aplicación.
Configuración de protocolos de seguridad.

- Políticas de seguridad: se trabajaron mecanismos para dar seguridad dentro del sistema en la programación y la configuración de aplicaciones, y la aplicación de medidas externas para mantener el sistema protegido.

2. DESCRIPCIÓN DEL PROBLEMA

2.1 PLANTEAMIENTO DEL PROBLEMA

Actualmente no se cuenta con un sistema de información administrativa integral en la Universidad de Nariño, lo que trae consigo problemas de retrazo en la consulta actualizada y unificada de los recursos económicos. Se incorpora a este problema la falta de organización de la administración de usuarios del sistema y de la información que estos manejan, los grupos a los que estos pertenecen, y sus delimitaciones en las funciones, desde el ingreso al sistema, sus operaciones dentro de él y su salida.
En el manejo de contraseñas de usuarios, no se cuenta con modelos de encriptación de estas, como tampoco de políticas de seguridad para la administración de las mismas y su documentación.

El tratamiento descentralizado de la información, y sus procesos en los subsistemas por cada dependencia distribuidas en cedes administrativas que conforman la institución, tiene consecuencias en la poca vigilancia de las tareas de administración y seguridad. Además no se cuenta con recursos lógicos y físicos confiables para la protección de la información y la aplicación de políticas para asegurar estos bienes, que permanecen en riesgo, tanto en tiempo de ejecución de las labores en la red como en la conservación de los mismos.
El sistema actual contiene módulos de auditoria general, pero no se presta para evaluaciones de todos los procesos, debido a que no posee salidas de información eficientes para evaluaciones intuitivas, como por ejemplo: conocer a través de interfaces, quienes de los operarios del sistema realizó transacciones detalladas a los datos.

Al integrar el manejo administrativo en el SIIFUN se podrá dar confiabilidad a la información y se prestará medios seguros para su protección de manera, rápida y actualizada, así cuando se necesite evaluar el comportamiento del sistema y de su manejo, se extraigan resultados de auditoria y revisión completos a través del manejo de Logs.

2.2 FORMULACIÓN DEL PROBLEMA

¿Como suministrar organización y seguridad al SIIFUN y a los recursos que manejan las dependencias financieras de la Universidad de Nariño ?

2.3 SISTEMATIZACIÓN DEL PROBLEMA

- Qué herramientas emplear para la protección de la comunicación de la red?
- Cómo garantizar el ingreso al sistema solo del personal autorizado ?

- Cómo garantizar que el software proteja la información que circule por la red?

- Cómo garantizar que la información que se archive para historiales este bien protegida?.

- Cómo el sistema registra los movimientos de operaciones de los actores del sistema?.

- Como se puede tener información para la utilización y mantenimiento de la administración y seguridad del SIIFUN?

- Como se puede garantizar el funcionamiento de la seguridad del SIIFUN?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Desarrollar y programar el modulo de administración y seguridad del SIIFUN.

3.2 OBJETIVOS ESPECIFICOS

- Configurar una comunicación segura, con aplicaciones desarrolladas en una arquitectura orientada a la Web (navegadores cuyas versiones serán especificadas en el Estudio de Factibilidad)bajo Java y la utilización de protocolos de seguridad.

- Implementar una aplicación que permita la administración de usuarios, sus modificaciones e integrar prioridades para el manejo de los diferentes módulos del sistema.

- Aplicar sistemas de encriptación de los datos que circulan a través de la red.

- Generar políticas de seguridad para todo el sistema desde el manejo del personal que interactúa con el mismo, hasta el resguardo de la información en backup para el historial.

- Desarrollar un sistema de logs por cada operación, donde se registren las operaciones de los actores del sistema.

- Documentar el proceso de desarrollo para que el producto final tenga un buen soporte.

- Entregar un software probado exhaustivamente de tal forma que el producto final sea confiable y de calidad.

4 JUSTIFICACIÓN

El sistema de información integral maneja la información de las diferentes dependencias administrativas y financieras de la Universidad de Nariño, por lo cual, debe contar siempre con una información precisa y confiable. Esto amerita dar alta prioridad a su protección. Para ello se desarrolló el modulo de administración de usuarios y sus grupos, de seguridad y las configuraciones del sistema.

Además se necesitaron implementar normas de seguridad, que en la actualidad son pocas, y que se dirigen al cuidado externo del sistema, cuando este no pueda controlarse a través del software.

El sistema actual carece de una vigilancia de sus funciones internas y externas a él, aunque tiene módulos de auditoria pero no son suficientes porque no posee salidas de información para evaluaciones de sus funciones no prioritarias, algunas como: registrar quienes de los operarios del sistema realizó transacciones o consultas a los datos, o como también que personal puede ingresar a las dependencias administrativas. Y que estas sean presentadas en el momento en que se necesiten.

La Universidad de Nariño ha iniciado con el desarrollo de dicho sistema, la fase 1, que contempló el análisis y diseño del software, el siguiente paso es comenzar su implementación, para esto se necesitó el personal capacitado, que lleve a buen término el proyecto y entregue un producto que solucione los inconvenientes que actualmente se presentan.

5. ESTUDIO DE FACTIBILIDAD

El proyecto fue diseñado para funcionar en un ambiente de intranet en la Universidad de Nariño, pero posee la capacidad de manejo desde la red externa, porque funciona bajo un ambiente WEB. De manera que puede prestar servicios a usuarios que se encuentren en otros lugares y que por medio de Internet busquen trabajar en el SIIFUN.

Para la implementación del sistema de información, se cuenta con:

5.1 FACTIBILIDAD TÉCNICA

5.1.1 Hardware Además de los equipos y configuraciones que se mencionan a continuación, en la Universidad de Nariño se tiene instalada la infraestructura de red necesaria, para la ejecución del proyecto. Por tanto se cuenta con equipos así:

ESPECIFICACIONES EQUIPO SERVIDOR

Las siguientes especificaciones, se escogieron para los procesos de complejidad del SIIFUN y de los demás sistemas que funcionarán para la Universidad de Nariño, por su capacidad de multiproceso, alta velocidad y factibilidad en precio.

- Procesador:
  Up to four dual-core AMD Opteron processors Model 875 (2.1 GHz).
- Secondary cache (Level 2):
  1 MB Level 2 cache por base(AMD procesador Opteron Models 875 have 2 x 1 MB L2 cache - 1 MB per core)
- Capacidad de memoria:
  Up to 4 GB DDR1
  DIMM slots:
  System has 16 DIMM slots (cuatro procesadores); DDR1/333 or DDR1/400 ECC registered DIMMs (128-bit plus ECC databus).
- Red:
  Dos puerto Ethernet 10/100/1000BASE-T.

  Un puerto Ethernet dedicado 10/100BASE-T con dos puertos para encadenamiento
- Serial:
  Un puerto asincrónico RJ-45 TIA/EIA-232-F.
- SCSI:
- Bus de Expansion :
  Siete slots internos PCI-X.
- Disco interno Mass Storage:
  Up to six hot-swap Ultra320 SCSI disco (73 GB/10K RPM, 146 GB/10K RPM, 73 GB/15K RPM, 300 GB/10K RPM).

- Unidad interna de DVD: Una slim-line DVD standard.

EQUIPO CLIENTE

Los requerimientos mínimos que debe tener las estaciones de trabajo son:
- Procesador con 233 GHz
- Mother Board soporte para tarjeta de red o modem.
- Memoria de 128/256 MB
- Disco duro de 10 GB
- Tarjeta de red Ethernet 10/100 Mbps
- Teclado
- Mouse

Los requerimientos óptimos que debe tener las estaciones para que el trabajo sea eficiente son:
- Procesador con 2.0 GHz
- Mother Board soporte para tarjeta de red o modem.
- Memoria de 512 MB
- Disco duro de 40 GB
- Tarjeta de red Ethernet 10/100 Mbps
- Teclado
- Mouse

Lo anterior son las características básicas pero es recomendable la mejor dotación para un mejor desempeño del sistema.

5.1.2 Software

Sistema operativo:
- El servidor trabaja con sistema operativo SOLARIS.
- Máquina virtual: jdk1.5.0_03 (software libre).
- Servidor de aplicaciones:
  TOMCAT que maneja:
  - SERVLETS, BEANS , JSP , XML , HTML , JAVASCRIPT, AJAX,
- Herramienta para desarrollar aplicaciones e interfaces:
  MACROMEDIA DREAMWEAVER.

- Desarrollador de base de datos:
- POWER GRES
- PG-ADMIN
- Desarrollo en bases de datos POSTGRES para Windows.

- La Base de datos que se implantará finalmente:
  ORACLE. licencias adquiridas por la Universidad de Nariño.

- Configuración de la comunicación:

- Protocolo TCP-IP
- Configuración sistema operativo.
- Protocolo SSL.
- Open SSL.
- Algoritmos de encriptación.

- Navegadores Internet:
- Internet Explorer versiones 5 en adelante.
- Mozilla Firefox (1.0).
- Netscape 7.2.
- Algoritmos de encriptación.

5.2 FACTIBILIDAD ECONÓMICA

Los gastos del proyecto fueron asumidos por la Vicerrectoría Administrativa de la Universidad de Nariño y el pasante del proyecto. El proyecto es viable desde el punto de vista económico.

5.3 FACTIBILIDAD OPERATIVA

El proyecto para el desarrollo del Módulo ADMINISTRACIÓN Y SEGURIDAD DEL SIIFUN, fue propuesto ante la necesidad de organizar a los usuarios para que puedan llevar un esquema para sus trabajos, y que preste el servicio a una posterior monitorización por parte del administrador del sistema, así como también, prestar seguridad de los datos, ya que todo sistema de información debe contener normas para su protección. Por tanto cuenta con el respaldo de los directores del proyecto y de sus demás miembros, quienes se beneficiarán de el servicio que este prestará.

6. ANTECEDENTES

Los procesos del actual sistema de la información financiera de la Universidad de Nariño, se manejan de manera aislada, es decir se han llegado a crear programas específicos para procesos en particular lo cual hace que el sistema sea ineficiente en el sentido de perdida de tiempo, ambigüedad de la información, repetición de procesos en diferentes dependencias y no existe una comunicación directa entre dichas dependencias. Por ello no se ha implementado las normas de protección de la información.

Se han creado aplicativos utilizando las herramientas Informix y 4GL las cuales ya no cuentan con versiones apropiadas, entonces se hace necesario una renovación del sistema utilizando nuevas tecnologías en el manejo de la información, tanto en las etapas de análisis y diseño como en las posteriores fases de implementación.

La universidad se ha visto interesada en la implementación de un sistema con estas características, por lo cual recientemente se han realizado estudios de algunas alternativas como el sistema de información desarrollado por la Universidad de Pamplona (área administrativa) que finalmente fue rechazado por su alto costo y porque ya se había dado inicio al proyecto SIIFUN.

Debido a esto se desarrolló la fase I del proyecto correspondiente al análisis de requerimientos y diseño del Sistema Integrado de Información Financiera de la Universidad de Nariño SIIFUN, bajo la metodología RUP (Rational Unified Process) y el modelamiento Orientado a Objetos. Con el fin de optimizar el trabajo del sistema se subdividió en tres módulos: Presupuesto, Tesorería y Contabilidad.

En el análisis de requerimientos se contempló las etapas de presentación general del sistema, determinación de clientes y metas, se determinaron funciones, atributos, casos de uso, los diagramas de casos de uso, modelamiento conceptual y glosario. Y en el diseño se realizaron los diagramas de secuencia del sistema, contratos para las operaciones del sistema, diagramas de colaboración, diagramas de clases y diagramación de paquetes.

En el análisis y diseño del módulo de administración se contemplo el desarrollo de la administración de usuarios, la utilización de los logs y los campos que permiten el manejo de sesiones por parte de los usuarios del Sistema Integrado de Información Financiera de la Universidad de Nariño (SIIFUN).

7. METODOLOGÍA

La metodología a utilizar se basa en el Unified Development Process. El cual se compone de distintas iteraciones. Con esta estrategia se pretende dar respuesta a la problemática encontrada en otros procesos de desarrollo como el Modelo Estructurado, en el cual las distintas fases tienen que culminarse, de principio a fin, en su totalidad. Dado este inconveniente se desarrollo este proyecto con esta metodología.

Los objetivos y modelos utilizados en las distintas fases de las empresas, incorporan elementos del esquema conocido como Modelo Estructurado, ya que éste cuenta con estrategias que son muy eficaces para la elaboración de aplicaciones comerciales. Una vez iniciadas. Esto conduce a que ante la imposibilidad de cumplir ciento por ciento con los objetivos de una determinada fase (análisis, diseño) en un solo instante de tiempo, se tenga que estar constantemente devolviendo en el proceso a retomar decisiones de fases anteriores.

El proceso iterativo propone que se planeen ciclos con objetivos muy concretos, con una planificación de recursos adecuada y con una valoración de los riesgos coherente. Cada uno de estos ciclos aborda una parte de las actividades del flujo de trabajo, con lo cual se puede ser más efectivo en su culminación. Una vez terminado un ciclo, se efectúa una comprobación y valoración de los resultados con lo cual se planea la siguiente iteración. Esta nueva iteración, en el caso en el cual el ciclo vigente no tenga los resultados adecuados o se requiera una profundización o depuración mayor, puede determinar volver a cruzar por los mismos objetivos propuestos. Esto permite que no se aborde todo el conocimiento en un solo instante, sino que se dé a partir de un proceso pausado de reconocimiento del tema, en el cual se estructura una actividad de aprendizaje a partir de la reflexión múltiples veces del mismo contexto del proyecto.

El proceso está fraccionado en distintos pasos de un flujo de trabajo. Estos pasos corresponden a las etapas habituales del esquema del Modelo Estructurado como son: modelamiento del negocio, análisis de requerimientos, análisis y diseño de la solución, construcción, pruebas e implantación. Sin embargo, a diferencia del diseño estructurado, estas etapas se asocian con fases cuyos objetivos se obtienen a partir de varias iteraciones.

Ya que en la fase 1 del proyecto SIIFUN se realizaron las etapas de modelamiento del negocio, análisis de requerimientos, análisis y diseño de la solución, la fase 2 corresponde a la construcción de la aplicación.

Los objetivos concretos en la construcción son:

- Como objetivo principal de esta fase es implementar el diseño propuesto. Vale la pena anotar, que de acuerdo a la estrategia escogida para el proceso de desarrollo, ésta construcción se da de manera iterativa también, y en cada iteración se involucra al usuario final. Por tanto, no se pretende construir todo el proyecto en un solo instante

de tiempo sino que la implementación se hace incremento a incremento, de acuerdo a un plan previamente establecido.

- Se deben llevar a cabo un protocolo de pruebas de caja blanca y de caja negra, para cada nuevo incremento construido. De la misma manera, debe volverse a probar el software construido previamente para determinar que el nuevo incremento no modifique su comportamiento correcto. Finalmente, todo el sistema desarrollado hasta el momento, debe ser probado de manera integral a fin de poder determinar su correcto comportamiento.

En la implementación y pruebas se desarrolla el código de una manera certificada que se basa en dos aspectos:

- Actividades Técnicas:
  - Definir estándares de programación: que consiste en asimilar los idiomas aplicables al lenguaje, conocer y adecuar estándares de programación al lenguaje, Razón por la cual se realizará una capacitación en la arquitectura y lenguaje escogidos para el desarrollo de la aplicación.
  - Definir estructura de directorios basados en los diagramas de paquetes.
  - Codificación y pruebas unitarias: Revisiones de código
  - Pruebas de módulos y de sistema: Casos de prueba, procedimiento de instalación

- Documentos Entregables:
  - Código fuente.
  - Documentación.
  - Manuel de usuario.

8. MARCO REFERENCIAL

8.1. MARCO TEÓRICO

El objetivo de un sistema de información se encuentra en transformar un conjunto de datos de una organización y convertirlo en información confiable, con el fin de que puedan ser utilizados para mejores requerimientos de la organización, ayudando así, a la toma de decisiones, las cuales permitirán afrontar diferentes tipos de situaciones.

Gracias al análisis y diseño de la primera etapa del SIIFUN, se ha desarrollado los diferentes módulos que lo constituyen: MODULO DE TESORERÍA, PRESUPUESTO, CONTABILIDAD Y ADMINISTRACIÓN. Los cuales al ponerlos en marcha darán a la Universidad de Nariño un servicio integral en el manejo de su economía.

Para el manejo del SIIFUN se hizo necesario diseñar e implementar el Módulo de administración y seguridad, siendo necesario organizar y asegurar la información que se maneja en él. Tomando prototipos de otros sistemas así como también de otros criterios, se reforzó el análisis y diseño de la primera etapa del SIIFUN módulo Administración y Seguridad para lograr un desarrollo que cubra las especificaciones del mismo. Para que estos lineamientos tengan aceptación en el desarrollo se estudió la teoría de:

Arquitectura
Se definen como Tecnologías que utilizadas para el desarrollo de aplicaciones web empresariales. Que surgen frente a esta nueva demanda de aplicaciones que interconectan intra redes con el amplio mundo del Internet.

Servidor De Aplicaciones
Proporciona servicios que soportan la ejecución y disponibilidad de las aplicaciones desplegadas. Es el corazón de un gran sistema distribuido.
El estándar J2EE el servidor de aplicaciones permite el desarrollo de aplicaciones de una manera sencilla y eficiente. Una aplicación desarrollada con la esta tecnología admite ser desplegada en cualquier servidor de aplicaciones o servidor web que cumpla con el estándar. Un servidor de aplicaciones es una implementación de la especificación J2EE .

Base De Datos
Se define como un conjunto de datos informáticos, relacionados, organizados y no redundantes entre si, que se encuentran almacenados con una estructura, la cual es gestionada por un DBMS. Desde el punto de vista informático, se concibe como un sistema conformado por un conjunto de datos, almacenados en discos que permiten una fácil manipulación, además se incluyen los programas que permiten manejar esa información.

Seguridad Informática
“Podemos entender como seguridad una característica de cualquier sistema (informático o no) que nos indica que ese sistema esta libre de todo peligro , daño o riesgo, y que es en cierta manera infalible como esta característica particularizando para el caso de sistemas

operativos o redes de computadoras , es muy difícil de conseguir (según la mayoría de expertos en imposible) se suaviza la definición de seguridad y se pasa a hablar de fiabilidad(probabilidad de que un sistema se comporta tal y como se esperaba de él) mas que una seguridad; por tanto se habla de sistemas fiables en lugar de hacerlos de sistemas seguros."[1]

Políticas de Seguridad

Es un conjunto de normas que adopta una organización para mejorar la calidad de la seguridad del sistema informático, para poder así garantizar la protección de sus datos.
Entre los propósitos de las políticas de seguridad es :

- Informar a los miembros de la organización que se involucran en el sistema el deber que tienen respecto a las obligaciones .
- Facilitar guías para actuar ante posibles amenazas o problemas presentados.

Los elementos claves de las políticas de seguridad son: Disponibilidad , integridad, y confidencialidad.
De acuerdo con los nuevos ambientes que surgen en la puesta en marcha del sistema, es debido actualizar las políticas de seguridad, para ello se requiere compromiso por parte de la organización en general.

Seguridad Física

Debido a la importancia que tienen los equipos, programas, instalaciones y la información es necesario que las organizaciones tomen medidas para garantizar la seguridad, para evitar la pérdida o el daño de los mismos. "Desgraciadamente, la seguridad física es un aspecto olvidado con demasiada frecuencia a la hora de hablar en seguridad informática en general; en muchas organizaciones se suelen tomar medidas para prevenir o detectar accesos no autorizados o negaciones de servicio, pero rara vez para prevenir la acción de un atacante que intenta acceder físicamente a la sala de operaciones o al lugar donde se depositan las impresiones del sistema. Esto motiva que en determinadas situaciones un atacante se decline por aprovechar vulnerabilidades físicas en lugar de lógicas, ya que posiblemente le sea más fácil robar una cinta con una imagen completa del sistema que intentar acceder a él mediante fallos en el software. Hemos de ser conscientes de que la seguridad física es demasiado importante como para ignorarla: un ladrón que roba un ordenador para venderlo, un incendio o un pirata que accede sin problemas a la sala de operaciones nos puede hacer mucho más daño que un intruso que intenta conectar remotamente con una máquina no autorizada; no importa que utilicemos los más avanzados medios de cifrado para conectar a nuestros servidores, ni que hallamos definido una política de firewalling muy restrictiva: si no tenemos en cuenta factores físicos, estos esfuerzos para proteger nuestra información no

[1] HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 2.1. p.4

van a servir de nada".[2]

Seguridad Lógica
La seguridad lógica para garantizar la integridad, confidencialidad y disponibilidad de la información, abarca las siguientes áreas: _ Controles de acceso, la seguridad lógica, esta orientada a establecer los controles de acceso que se deben tener para proteger la información almacenada al igual que controlar el mal uso de la información, un inadecuado control de acceso lógico es una amenaza potencial para la pérdida o divulgación de la información. "La seguridad lógica se encarga de controlar y salvaguardar la información generada por los sistemas, por el software de desarrollo y por los programas en aplicación; identifica individualmente a cada usuario y sus actividades en el sistema, y restringe el acceso a datos , a los programas de uso generadle uso específico, de las redes y terminales. La seguridad lógica puede evitar una afectación de pérdida de registros, y ayuda a conocerle momento en que se produce un cambio o fraude en los sistemas".[3]

Seguridad en Comunicaciones y Redes
La seguridad de los equipos conectados a una red, la información que se almacena y comparten, es uno de los aspectos más importantes en la interconexión del sistema, pero la seguridad en la red es mucho más que evitar accesos no autorizados a los equipos y a sus datos. La protección en una red incluye el mantenimiento del entorno físico apropiado que permita un funcionamiento correcto y efectivo de la red, por lo cual es vital establecer mantenimiento preventivo periódico para evitar la pérdida de datos y minimizar los fallos en la red de datos. En un entorno de red debe asegurarse la privacidad de los datos sensibles y también las operaciones de la red de daños no intencionados o deliberados. El mantenimiento de la seguridad de la red requiere un equilibrio entre facilitar un acceso fácil a los datos por parte de los usuarios autorizados y restringir el acceso a los datos por parte de los no autorizados. Es responsabilidad del administrador crear este equilibrio.

8.2 MARCO CONCEPTUAL

Para realizar un modulo de administración y seguridad del sistema y que sea acorde con las necesidades del mismo se tuvo en cuenta las relaciones existentes entre datos y procesos, con el fin de optimizar aquellos que se relacionan directamente. En base a este estudio se resolvió la escogencia de la plataforma mas adecuada para el desarrollo de la aplicación.

En la fase de desarrollo se tiene en cuenta la ingeniería del software, como herramienta principal, porque es interesante el concepto del conocimiento del producto final que debe ser de alta calidad.

Este trabajo se desarrolló con base a la teoría necesaria en el análisis para el desarrollo e implementación de un sistema de información, cuyo objetivo principal es convertir las entradas en salidas que permitan o suministren a los usuarios finales, los medios necesarios para la gestión y toma de decisiones a través de procesos de información.
La teoría de conceptos considerada para el desarrollo es:

---
[2]HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 2.1. p.21
[3] ECHENIQUE, José Antonio. Auditoría en Informática. McGrawHill. Segunda Edición. México.p.195

8.2.1 ARQUITECTURA JAVA 2 ENTREPRISE EDITION (J2EE) Es diseñada para aplicaciones distribuidas que son construidas con base en componentes (unidades funcionales de software), los cuales interaccionan entre sí para formar parte de una aplicación J2EE. Un componente de esta plataforma debe formar parte de una aplicación y ser desplegado en un contenedor, o sea en la parte del servidor J2EE que le ofrece al componente ciertos servicios de bajo nivel y de sistema (tales como seguridad, manejo de concurrencia, persistencia y transacciones). Como se ve, J2EE no es sólo una tecnología, sino un estándar de desarrollo, construcción y despliegue de aplicaciones.

- Cliente web (contenedor de applets): Es usualmente un navegador e interactúa con el contenedor web haciendo uso de HTTP. Recibe páginas HTML o XML y puede ejecutar applets y código JavaScript.
- Aplicación cliente: Son clientes que no se ejecutan dentro de un navegador y pueden utilizar cualquier tecnología para comunicarse con el contenedor web o directamente con la base de datos.
- Contenedor web: Es lo que comúnmente denominamos servidor web. Es la parte *visible* del servidor de aplicaciones. Utiliza los protocolos HTTP y SSL (seguro) para comunicarse.

8.2.2.1 Servidor de Aplicaciones Tomcat. Tomcat es un contenedor de Servlets con un entorno JSP. Un contenedor de Servlets es un shell de ejecución que maneja e invoca servlets por cuenta del usuario. Permite implementar: APPLETS, SERVLETS, BEANS , JSP , XML , HTML , JAVA SCRIPT, AJAX.

8.2.2 Herramienta para Desarrollar Aplicaciones Macromedia Dreamweaver. Es un editor de Páginas web, creado por Macromedia. Es el programa de este tipo más utilizado en el sector del diseño y la programación web, por sus funcionalidades, su integración con otras herramientas y tiene las funciones típicas de un editor de código fuente para la web.

8.2.3 Sistema Gestor De Base De Datos. (Back – End). Los Sistemas Gestores de Bases de Datos son un tipo de software muy específico, dedicado a servir de interfaz entre las bases de datos y las aplicaciones que la utilizan.
Este es un software que permite insertar, modificar y recuperar eficazmente los datos específicos dentro de una gran masa de información compartida por muchos usuarios.
Un DBMS permite la descripción de los datos en forma separada de su utilización, es decir asegura la independencia de datos, se compone de un lenguaje de definición de datos, un lenguaje de manipulación de datos y de un lenguaje de consulta. Entre las grandes ventajas del DBMS, cabe destacar:
El DBMS, puede ser invocado desde programas de aplicación de sistemas de transacciones, escritos en lenguaje de cuarta generación , para la creación, o actualización de los datos, o de igual forma consultar a través del propio lenguaje que tienen las bases de datos, o en lenguajes de alto nivel.
Independencia física: permitir la realización de estructuras. de almacenamiento de datos en forma independiente de su estructura lógica en la realidad.

Independencia lógica: permitir una cierta independencia entre los datos vistos por las aplicaciones y la estructura lógica de ellos en la realidad.

PGADMIN: es una herramienta de propósito general para diseñar, mantener, y administrar las bases de datos de Postgres. Funciona bajo Windows 9x, XP y NT.

POSTGRES: es un servidor de base de datos relacional libre, liberado bajo la licencia BSD. Es una alternativa a otros sistemas de bases de datos de código abierto (como MySQL, Firebird y MaxDB), así como sistemas propietarios como Oracle o DB2.

ORACLE: Oracle es un sistema de administración de base de datos (o RDBMS por el acrónimo en inglés de Relational Data Base Management System), fabricado por Oracle Corporation.

9. ESTUDIO DEL DISEÑO ETAPA 1 DEL SIIFUN

Para el desarrollo del modulo administración y seguridad, se estudió el trabajo de análisis y diseño realizado en la etapa 1 del proyecto SIIFUN, de donde se extrajo los lineamientos de como construir la aplicación y la base de datos.

Cabe anotar que para entonces se desconocieron algunos cambios que solo se los tendrían en cuenta en el desarrollo del mismo. Por ello el presente trabajo contiene además de lo dispuesto en el análisis y diseño, elementos que mejoran la calidad del software final y su función en el sistema general.

10. CONSTRUCCION DE LA BASE DE DATOS DEL SIIFUN MODULO ADMINISTRACION

La base de datos del SIIFUN, fue desarrollada luego del estudio previo en el análisis (etapa 1 del proyecto SIIFUN). Donde se dejó el diseño para su posterior construcción.
Se hace referencia del esquema origen de la base de datos el documento:
Pasantía Universidad de Nariño:

SISTEMA DE INFORMACION FINANCIERA DE LA UNIVERSIDAD DE NARIÑO S.I.I.F.U.N, volúmenes 1,2 y 3 publicación 2004.

En este desarrollo, algunos lineamientos fueron cambiados e implementados porque surgieron nuevos hallazgos de tipo operacional, por consiguiente el esquema actual de la base de datos del sistema en general es diferente en su gran mayoría al que se pensaba implementar en la primera etapa. El módulo administración generó algunos cambios en su base de datos que fueron:

Tabla Usuario
Se incorporó otros campos, como son:
- Ipusuario: que identifica la estación en donde trabaja el usuario.
- fechacontraseñainicial: identifica la fecha de creación de la cuenta.
- fechacontraseñafinal: identifica la fecha de la caducidad de la contraseña del usuario.
- Activo: indica el estado del usuario en el sistema.

Tabla Grupo
Se incorporó el campo:
- serial: que indica una secuencia de identificación del grupo en su creación.

Tabla de Log
Se eliminó el campo hora y se lo integró al campo fecha para que en él se guarde estos
Se cambio el valor de la variable fecha de varchar a timestamp.

Tabla Unidad administrativa:
Se aumentaron los campos :
- conordenador : de tipo bool,
padre: de tipo varchar(2).

10.1 DICCIONARIO DE DATOS

El resultado de los cambios generados en el desarrollo del SIIFUN módulo Administración, se encuentran ilustrados en los siguientes cuadros:

DICCIONARIO DE DATOS PARA EL MODULO DE ADMINISTRACIÓN Y SEGURIDAD DEL SIIFUN

USUARIO

CAMPO	TIPO	DESCRIPCIÓN
Login	varchar(30)	Valor único para cada usuario
contrasena	varchar(30)	Única para cada usuario
identificacionusuario	int8	Cedula del usuario del sistema
Ipusuario	inet	Valor asignado a la estación de trabajo del usuario
fechacontrasenai	varchar(50)	Tiempo de inicio de la contraseña
fechacontrasenaf	varchar(50)	Tiempo de caducidad de la contraseña
Activo	bool	Valor que evalúa si una cuenta de usuario es activa

GRUPO

CAMPO	TIPO	DESCRIPCIÓN
Nombre	varchar(30)	Nombre del grupo
identificaciongrupo	int8	Identificación dada por el sistema
Seq	serial	Indica secuencia

OPERACIONES

CAMPO	TIPO	DESCRIPCIÓN
codigooperacion	varchar(40)	Identificación de las operaciones
descripcion	varchar	Nombre de la operación

CARGOSSIIFUN

CAMPO	TIPO	DESCRIPCIÓN
Codcargo	varchar(10)	Identificación de los cargos
descripcioncargo	varchar(50)	Nombre del cargo

NOTIFICACIÓN

CAMPO	TIPO	DESCRIPCIÓN
Detalle	varchar(500)	Nombre de la notificación
origen_idusuario	int8	Emisor de la notificación
fecha_ini	varchar(20)	Creación de la notificación
fecha_fin	varchar(10)	Caducidad de la notificación
Sequen	int4	valores no repetidos y secuenciales
codigonotificacion	int4	Valor asignado por el sistema
Activo	bool	Valor que evalúa si una notificación si esta activa

TIPONOTIFICACION

CAMPO	TIPO	DESCRIPCIÓN
descripciontiponotifica	varchar(50)	Nombre de los tipos de notificación
cod_tipo_notifica	Varchar(3)	Identificación de los tipos de notificación
Activo	Bool	Evalúa si esta en el sistema

RECURSOSHUMANOS

CAMPO	TIPO	DESCRIPCIÓN
identificacionusuario	int8	Cédula del usuario
nombreusuario	varchar(50)	Nombre completo del usuario
Activo	Bool	Evalúa si esta en el sistema

UNIDADADMINISTRATIVA

CAMPO	TIPO	DESCRIPCIÓN
Codigoua	varchar(2)	Identificación de las unidades administrativas
Nombre	Text	Nombre de la unidad administrativa
autonomia	Bool	-
conordenador	Bool	-
Padre	varchar(2)	REFERENCES unidadadministrativa

LOG

CAMPO	TIPO	DESCRIPCIÓN
identificacionusuario	int8	Cédula del usuario
codigooperacion	varchar(10)	Operación que realizo en el SIIFUN
Fecha	timestamp	Día, mes, año ,hora y minutos

ARCHIVONOTIFICACION

CAMPO	TIPO	DESCRIPCIÓN
Ruta	varchar(60)	Ruta y nombre del archivo de la notificación
codigonotificacion	int8	Identificación de la notificación
Activo	Bool	Si existe en el sistema

GRUPOOPERACION

CAMPO	TIPO	DESCRIPCIÓN
codigooperacion	varchar(30)	Identificación de la operación REFERENCES operaciones
identificaciongrupo	int8	Identificación del grupo REFERENCES grupo
Activo	Bool	Si existe en el sistema

USUARIOGRUPO

CAMPO	TIPO	DESCRIPCIÓN
identificacionusuario	int8	Identificación del usuario

		REFERENCES usuario
identificaciongrupo	int8	Identificación del grupo REFERENCES grupo
Activo	Bool	Si existe en el sistema

USUARIOSNOTIFICACION

CAMPO	TIPO	DESCRIPCIÓN
destino_idusuario	int8	Identificación del usuario destino
codigonotificacion	int8	Identificación de la notificación
Estado	int2	Valor de lectura de la notificación
Activo	Bool	Si existe en el sistema

USUARIOUNIDADADMINISTRATIVA

CAMPO	TIPO	DESCRIPCIÓN
identificacionusuario	int8	Identificación del usuario REFERENCES usuario
Codigoua	varchar(10)	Identificación de la unidad administrativa REFERENCES unidadadministrativa
Codcargo	varchar(10)	Identificación del cargo
Activo	Bool	Si existe en el sistema

10.1 DISEÑO DE LA ESTRUCTURA GENERAL DEL SISTEMA.

10.1.1 Perfiles de Seguridad: en todo proyecto de sistemas, en el que se maneja información, debe existir un control de seguridad sobre este, para lo cual el administrador debe asignar perfiles a cada usuario indicando que tareas del sistema puede o no realizar.
Con base a lo anterior se crearon en el sistema grupos de usuarios quienes tienen los permisos a ciertas tareas del programa. Los usuarios son dependientes de estos grupos para poder ingresar al sistema; a su vez los grupos son dependientes de las operaciones.
Así se configura, para cada dependencia y usuario los permisos de acceso.

10.2 HERRAMIENTAS TECNOLÓGICAS UTILIZADAS

En el desarrollo del SIIFUN se utilizaron las siguientes herramientas:

10.2.1 Arquitectura del Software

Arquitectura
Para el desarrollo del proyecto SIIFUN se adoptó trabajar con la arquitectura J2EE por su solidez en los siguientes aspectos:
Es un grupo de especificaciones que permiten la creación de aplicaciones empresariales, como por ejemplo acceso a bases de datos (JDBC), utilizando directorios distribuidos (JNDI), acceso a métodos remotos (RMI/CORBA), funciones de correo electrónico (JavaMail) y aplicaciones Web (JSP y Servlets), entre otras herramientas.

10.2.2 Herramientas de Desarrollo. Servidor de aplicaciones TOMCAT:

Se eligió trabajar con el servidor Tomcat por ser un administrador de aplicaciones que permite manejar, tanto el contenido estático como el dinámico.
Permite implementar: APPLETS, SERVLETS, BEANS , JSP , XML , HTML , JAVASCRIPT, AJAX,

Herramienta desarrolladora de aplicaciones MACROMEDIA DREAMWEAVER.
Por ser el programa más utilizado para la fabricación de diseños y la programación web, y por sus funcionalidades, se escogió para la implementación de las interfaces y la programación del SIIFUN, al igual porque permite la integración con otras herramientas del ambiente web.

Sistema gestor de base de datos. (back – end).
Con respecto al gestor de base de datos, se escogió en el desarrollo POSTGRES; este es un manejador bastante amplio, de fácil manejo y sobre todo de gran compatibilidad con JAVA y en general con la arquitectura J2EE.

El SIIFUN trabajará finalmente con un manejador mas robusto para base de datos como lo es ORACLE, su grandes ventajas son la eficiencia, escalabilidad y acondicionamiento flexible a la arquitectura en que se desarrolla el sistema.

POSTGRES
Se trabajó en las pruebas iniciales con este motor de base de datos, por tratarse de ser uno de los mejores que se adquiere como software libre y que tiene buena aceptación para la tecnología J2EE. Pero ya que la Universidad de Nariño adquirió las licencias de Oracle, entonces la parte final del proyecto se implantará en esta base de datos

PGADMIN
Es un proyecto de software gratuito liberado bajo la Licencia Artística. El programa esta disponible en código abierto. (Gratuito)

ORACLE
Para la etapa final de la puesta en marcha del SIIFUN se implementará la utilización de esta base de datos por sus características de excelente rendimiento, además por poseer un motor robusto para el desempeño de bases de datos empresariales.

11. MANUAL DE OPERACIÓN DEL SIIFUN -MODULO ADMINISTRACIÓN

11.1 INTERFASES

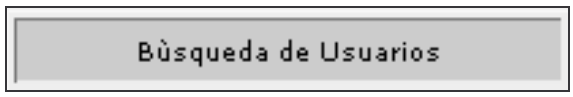
El diseño de interfaces de usuario, es el medio de comunicación entre el usuario y el sistema. Para realizar este diseño se evalúa las necesidades del usuario, que es quien requiere trabajar con la información, partiendo de este análisis se implementa un formato general en que el usuario y la máquina puedan intercambiar datos.

Para la elaboración del diseño de interfaces se creo una hoja de estilos general para todo el SIIFUN, esta se encuentra en :

(ruta del ROOT según sistema Operativo)...\siifun\utilidades\estilos\siifun\ siifun.css

Con la cual se trabajan los siguientes objetos:

- Etiquetas: utilizadas para mostrar un texto solo de lectura .

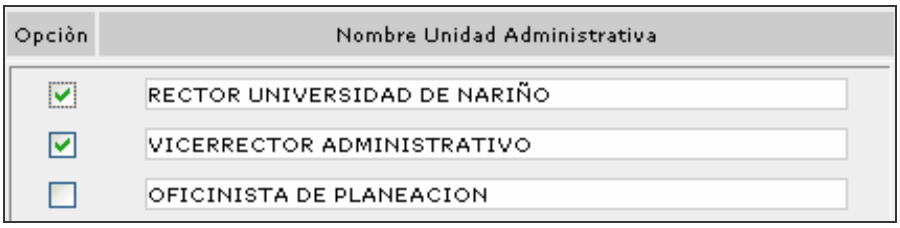


- Cajas de texto: utilizadas para ingresar datos al sistema, esta información puede ser modificada.

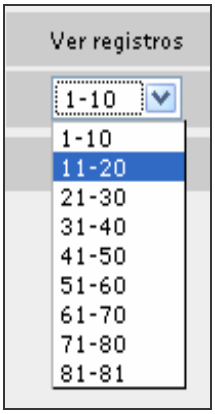
- Botones de comando: utilizados para que el programa realice una tarea.

- Botones de opción: indican al usuario que debe escoger una alternativa.

- Botones de chequeo: se utiliza para que el usuario escoger o no varias opciones.



- Combos y listas desplegables: permite mostrar un menú para que el usuario escoja una alternativa.



- Botones de calendarios: permiten citar un calendario para ingresar una fecha.

A continuación se describe el primer menú del módulo de Administración luego de que el usuario a ingresado con el login y su contraseña.

- Parte superior: cabecera que muestra los vínculos de avance, retroceso o salida del sistema.

  También esta contiene un link que se fabrica automáticamente hacia la pagina de Nuevas Notificaciones cuando al usuario le halla llegado una nueva notificación.

- En la parte izquierda, se creará un sub-menú hacia los diferentes módulos como son: (PRESUPUESTO, TESORERÍA, CONTABILIDAD Y ADMINISTRACIÓN) según los permisos que tenga el usuario.

- En la parte centro inicial se cargará un link hacia la pagina de Nuevas Notificaciones informando cuantas notificaciones sin leer posee.

- En la parte centro, se cargara el menú administrativo.

11.1.1 Ingreso Al Sistema y Menús Principales.

Para iniciar a trabajar en el sistema los usuarios deben tener su propia cuenta , la cual les va a permitir identificarse y cumplir con las funciones determinadas por los perfiles de usuario. Para ingresar deben introducir un login y un password del sistema, los cuales dan la entrada a la respectiva sesión. En caso de pérdida de login o password, su actualización o para la modificación, el usuario deberá acercarse al administrador del sistema para solucionar gestionar el proceso legal según las políticas de seguridad para estos casos.

11.1.2 Perfiles de Seguridad. El sistema permite evaluar la clase de usuario que intenta ingresar, para ello se integró en la programación, algoritmos que prestan seguridad a este proceso. Luego procede a dar permisos de acuerdo al rol que el usuario tenga en el sistema para que pueda a ingresar al modulo al que pertenece.

11.1.3 Conexión y Seguridad. Con la validación del usuario se hace la conexión a los recursos que este debe utilizar en el desarrollo de su trabajo en la sesión: Por ellos se lleva una monitorización rigurosa a todos los procesos que realice en el tiempo de trabajo.

11.1.4 Ingreso A Los Diferentes Módulos Del Siifun Para el ingreso a los diferentes módulos, el sistema entrega al usuario de manera automática diferentes interfaces que son:

11.2 DISEÑO E INTERFACES DEL MODULO ADMINISTRACIÓN DEL SIIFUN

Diseño de las páginas

Para este fin se trabajaron en tres tipos de ventanas y sus distribuciones son:

Esquema de las ventanas para los menús principales:

<table>
<tr><td colspan="3">A</td></tr>
<tr><td colspan="3">B</td></tr>
<tr><td colspan="3">C</td></tr>
<tr><td>D</td><td>E</td><td>F</td></tr>
</table>

A. Área de cabecera principal.
B. Área informativa de las notificaciones.
C. Área de información de la unidad administrativa con que trabaja el usuario en la sesión.
D. Área de links a los demás módulos del SIIFUN.
E. Área del menú principal de los Módulos.
F. Área para salidas del sistema.

Esquema de las ventanas para creación y actualización de elementos:

<table>
<tr><td colspan="3">A</td></tr>
<tr><td colspan="3">B</td></tr>
<tr><td colspan="3">C</td></tr>
<tr><td>D</td><td>E</td><td>F</td></tr>
<tr><td colspan="3">G</td></tr>
<tr><td colspan="3">H</td></tr>
</table>

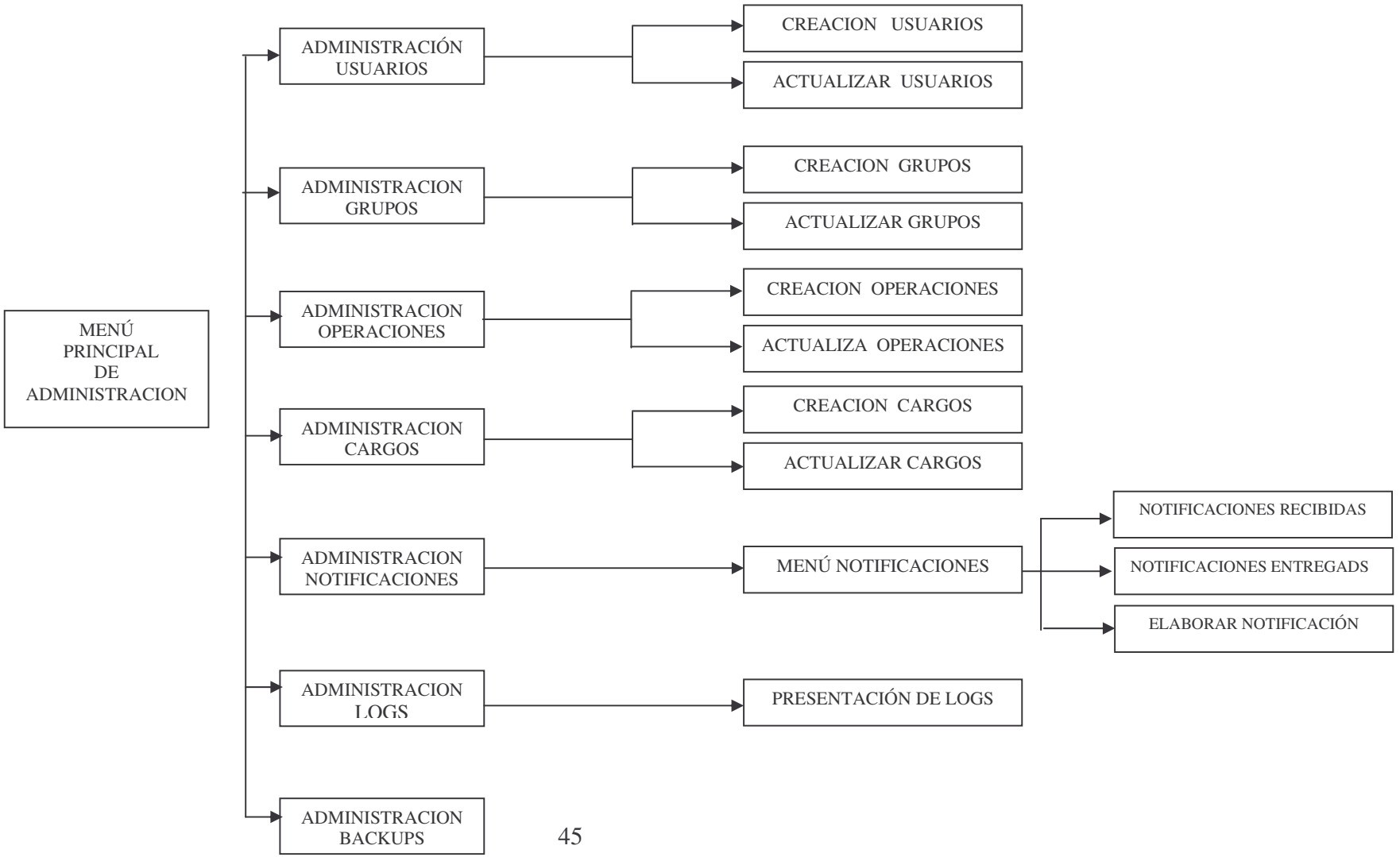
G. Área de cabecera principal.
H. Área para el Título de la página.
I. Área de trabajo: Parámetro de ingreso o lectura de datos de los elementos a consultar o ingresar.
J. Área de Titulo del listado.
K. Área para las descripciones de los nombres de los elementos.
L. Área para Otros valores.
M. Área para la presentación de la información de elementos.
N. Área de Botones para escoger las operaciones.

Esquema de los sub menús :

<table>
<tr><td>A</td></tr>
<tr><td>B</td></tr>
</table>

A. Área de cabecera principal.
B. Área de Botones para escoger las operaciones.

11.2.1 MAPA DE NAVEGACIÓN



Ventana Principal MODULO DE ADMINISTRACIÓN

Esta ventana permite el ingreso al menú de Administración, en el cual se encuentran los link de ingreso para Usuarios, Grupos Operaciones, Cargos, Notificaciones Tipo de Notificaciones, Backups y Logs.
También los link para ingresar a los demás módulos del SIIFUN, como son: Presupuesto Tesorería y Contabilidad. Y la salida del sistema.

11.2.2 INTERFAZ DE USUARIOS

Esta ventana permite al Administrador buscar el usuario para poder crear, eliminar o actualizar sus datos.

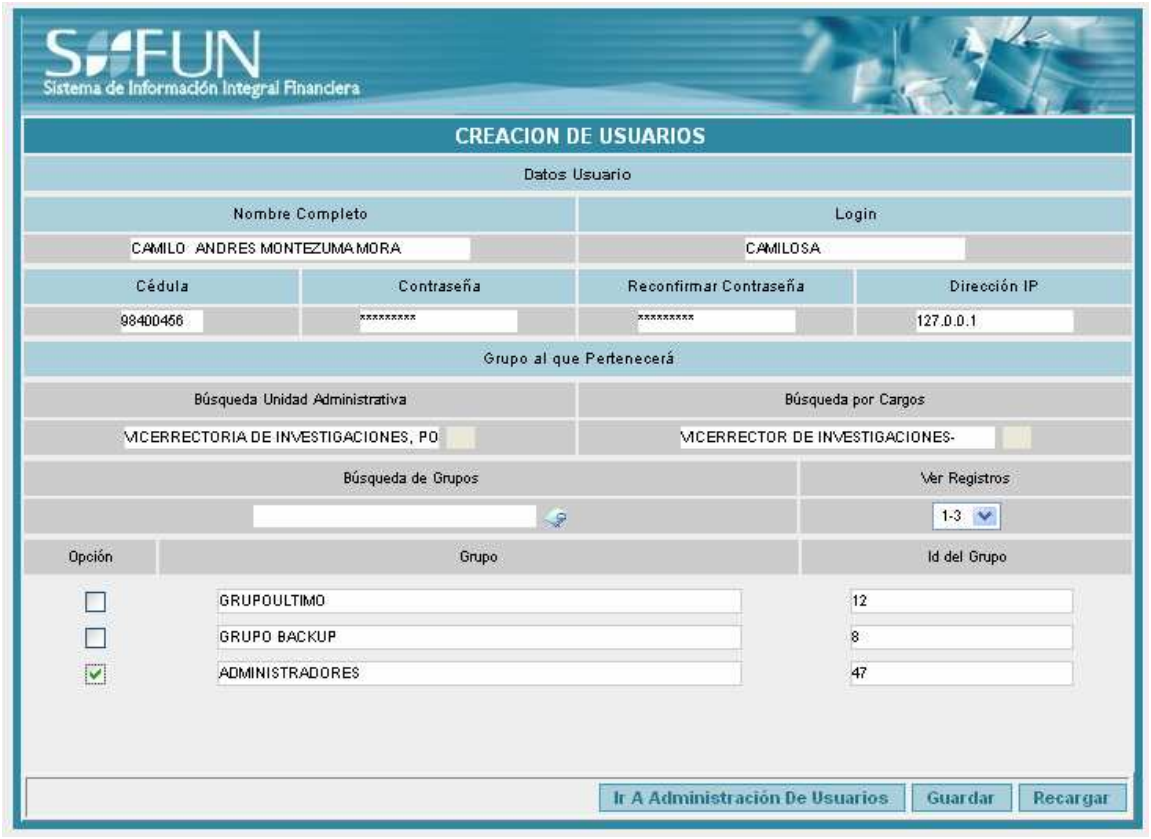
Con el botón CREAR se ingresa a la creación de usuarios.

Con el botón ELIMINAR permite eliminar al usuario después de haberlo seleccionado en la lista..

Con el botón ACTUALIZAR se ingresa a la modificación de los datos del usuario seleccionado de la lista.

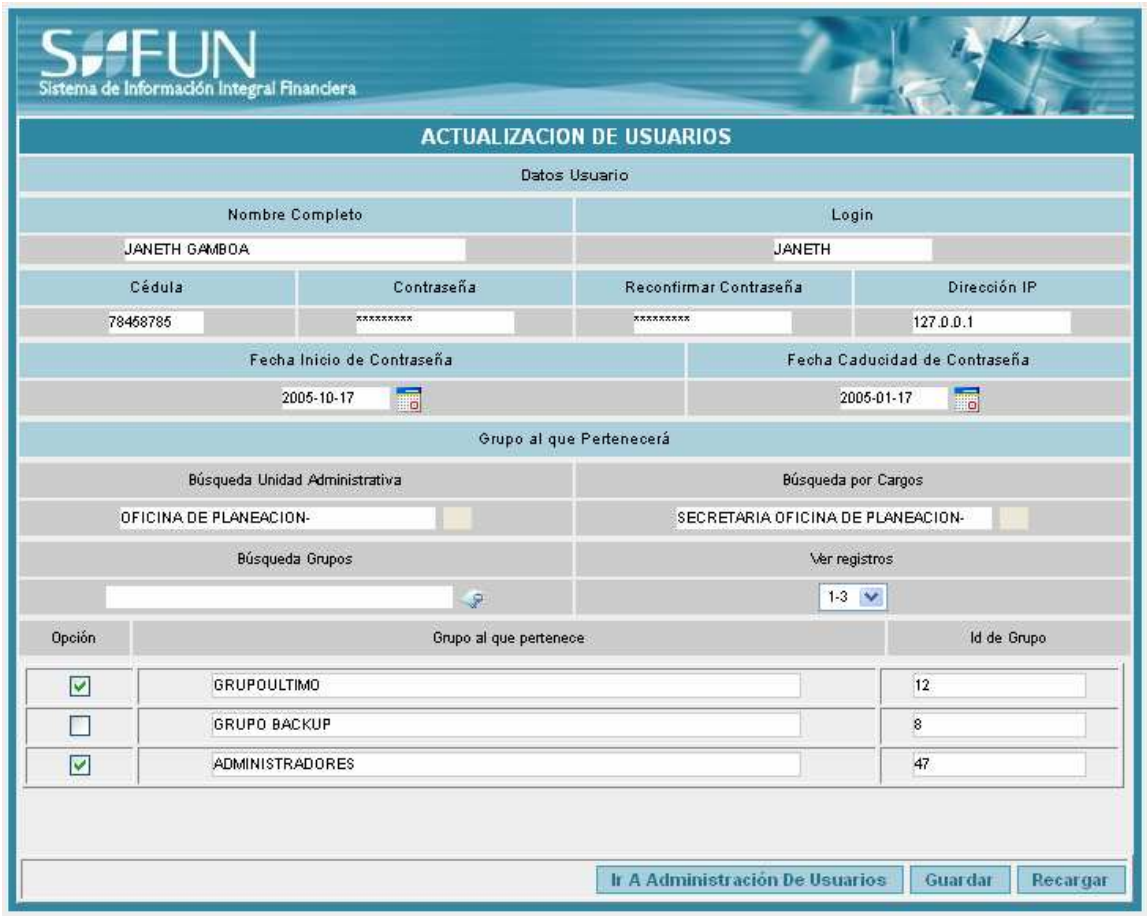
Con el botón RECARGAR se refresca esta pantalla.

11.2.2.1 INTERFAZ DE CREACIÓN DE USUARIOS



En esta interfaz se ingresa el nombre completo el login, la cédula, contraseña y su reconfirmación la dirección IP, la unidad administrativa a la que pertenece, el cargo en ella, y a los grupo que pertenecerá el usuario.

11.2.2.2 INTERFAZ DE ACTUALIZACIÓN DEL USUARIOS



En esta interfaz se modifica el nombre completo el login, la cédula, contraseña y su reconfirmación la dirección IP, la unidad administrativa a la que pertenece, el cargo en ella, y el grupo al que pertenecerá el usuario.

11.2.3 INTERFAZ DE GRUPOS

En esta ventana le permite al Administrador eliminar, actualizar o crear un nuevo grupo.
Con el botón CREAR se ingresa a la creación de grupos.
Con el botón ELIMINAR permite eliminar el grupo después de haberlo seleccionado en la lista.
Con el botón ACTUALIZAR se ingresa a la modificación de los datos del grupo seleccionado de la lista.
Con el botón RECARGAR se refresca esta pantalla.

11.2.3.1 INTERFAZ DE CREACIÓN DE GRUPOS

En esta interfaz se ingresa el nombre completo del grupo, presenta la identificación automáticamente, permite buscar en el listado de los grupos y buscar por registros, se debe seleccionar las operaciones que pertenecerán al grupo.

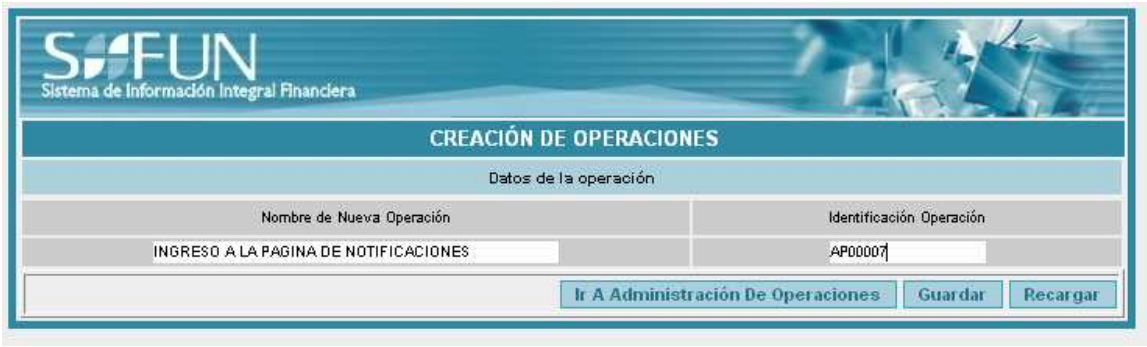
11.2.3.2 INTERFAZ DE ACTUALIZACIÓN DE GRUPOS

En esta interfaz se modifica el nombre completo del grupo, las operaciones que presenta en el listado de las operaciones las cuales pertenecerán al grupo.

11.2.4 INTERFAZ DE OPERACIONES

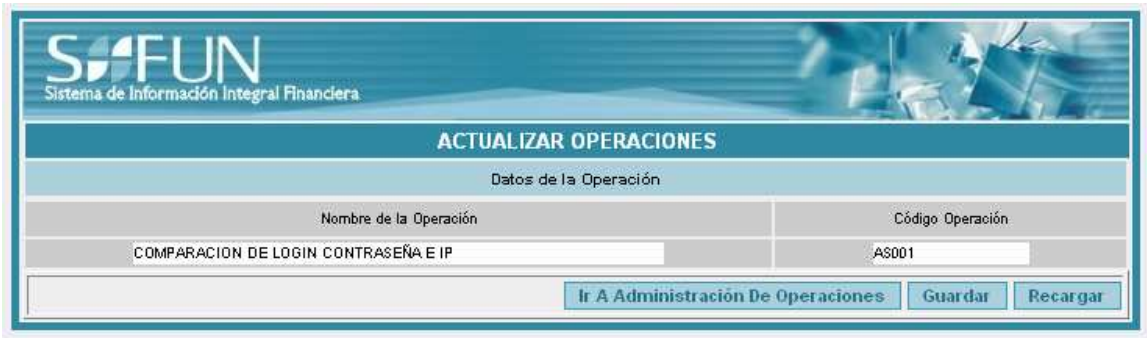
Esta interfaz permite al usuario crear las diferentes operaciones, como también eliminar o actualizar.
Con el botón CREAR se ingresa a la creación de operaciones.
Con el botón ELIMINAR permite eliminar la operación después de haberla seleccionado en la lista.
Con el botón ACTUALIZAR se ingresa a la modificación de los datos de la operación seleccionada de la lista.
Con el botón RECARGAR se refresca esta pantalla.

11.2.4.1 INTERFAZ DE CREACIÓN DE OPERACIONES



En esta interfaz se ingresa el nombre completo de la operación, se ingresa la identificación de la operación.

11.2.4.2 INTERFAZ DE ACTUALIZACIÓN DE OPERACIONES



En esta interfaz se actualiza el nombre completo de la operación.

11.2.5 INTERFAZ DE CARGOS

Esta interfaz permite crear, eliminar o actualizar la información de los cargos del SIIFUN.
Con el botón CREAR se ingresa a la creación de usuarios.
Con el botón ELIMINAR permite eliminar al usuario después de haberlo seleccionado en la lista..
Con el botón ACTUALIZAR se ingresa a la modificación de los datos del usuario seleccionado de la lista.
Con el botón RECARGAR se refresca esta pantalla.

Esta interfaz permite crear, eliminar o actualizar la información de los cargos del SIIFUN.
Con el botón CREAR se ingresa a la creación de usuarios.
Con el botón ELIMINAR permite eliminar al usuario después de haberlo seleccionado en la lista..
Con el botón ACTUALIZAR se ingresa a la modificación de los datos del usuario seleccionado de la lista.
Con el botón RECARGAR se refresca esta pantalla.

11.2.5.1 INTERFAZ DE CREACIÓN DE CARGOS

En esta interfaz se ingresa el nombre completo del cargo, la identificación de la operación es automática.

11.2.5.2 INTERFAZ DE ACTUALIZACIÓN DE CARGOS

En esta interfaz permite actualizar el nombre completo del cargo.

11.2.6 INTERFACES DE NOTIFICACIONES

Esta interfaz es un menú, que permite el ingreso a las notificaciones recibidas, a las que el usuario ha originado y a la opción de elaborar una nueva notificación.

11.2.6.1 INTERFAZ DE NOTIFICACIONES RECIBIDAS

Permite el listado de las notificaciones recibidas, en donde haciendo clic en el nombre de quien originó la notificación ingresa a la lectura de ella.

11.2.6.2 INTERFAZ DE NOTIFICACIONES ENTREGADAS

Permite el listado de las notificaciones que cada usuario ha elaborado. Y el acceso a cada una de ellas.

11.2.6.3 INTERFAZ DE ELABORAR NOTIFICACIONES

permite crear notificaciones con la opción de escoger el tipo de notificación los destinatarios, escribir el mensaje, adjuntar los archivos y enviar.

11.2.7 INTERFAZ DE BACKUPS

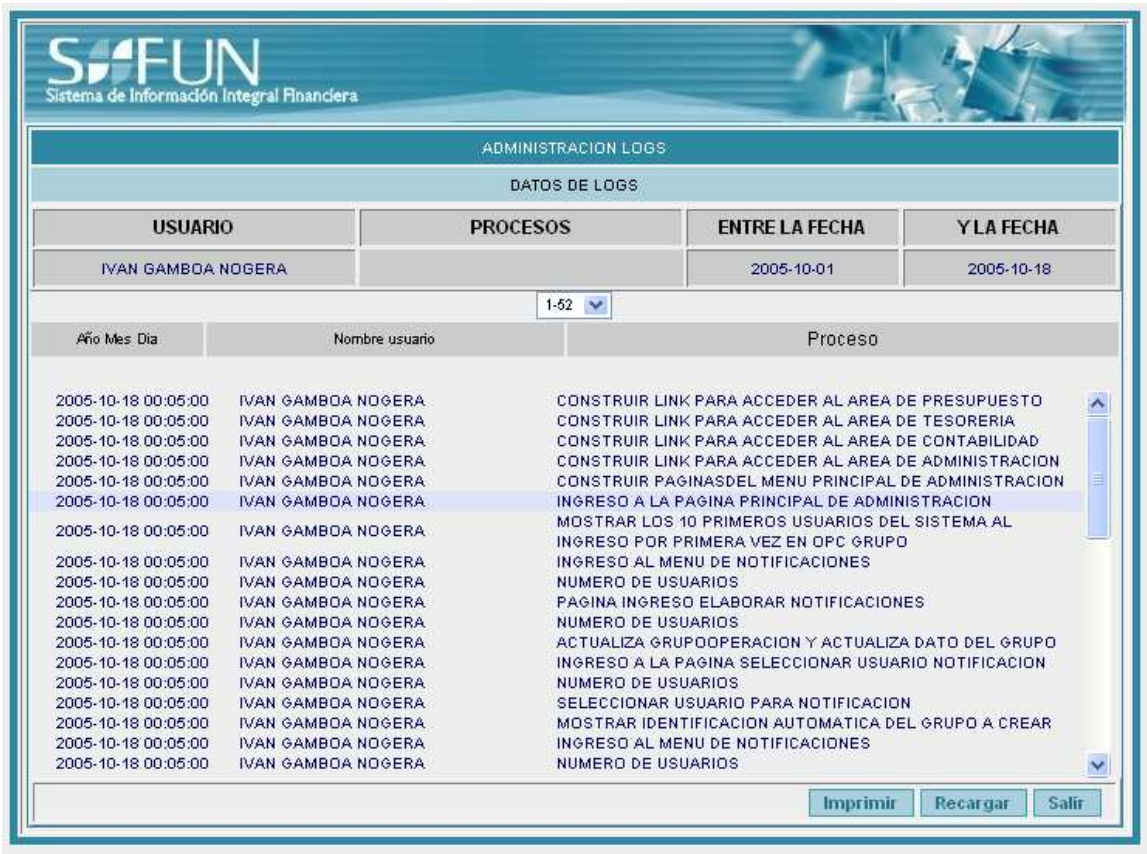
Esta interfaz permite restaurar la base de datos ingresando la fecha con su hora hasta la fecha hasta donde se quiere que se haga el Backup. Para ejecutar el proceso se presiona el botón realizar Backup SIIFUN

11.2.8 INTERFAZ DE LOGS

Esta interfaz administra los registros de los usuarios y presenta sus movimientos desde una fecha señalada hasta una fecha fin.

Con el botón buscar se escoge el usuario
Con los iconos de fecha se escogen los parámetros de inicio y fin.
Con botón operaciones se escogen las operaciones del sistema.
Con el botón RECARGAR se refresca esta pantalla.

11.2.8.1 INTERFAZ DE LOGS LISTADOS



Presenta las operaciones con fecha, nombre de usuario y proceso en que se realizó las estas tareas.

12. OPERACIÓN DEL SISTEMA POR EL USUARIO ADMINISTRADOR

12.1 CONFIGURACIONES E INGRESO DE DATOS

Configuración de Las Operaciones:

El ingreso de las operaciones se realiza en el modulo de administración en donde se pide una descripción y un código que la identifique en el sistema.

EJEMPLO:
Descripción operación: ingreso a la pagina de tesorería

Descripción operación	Código de la operación
Ingreso a la página de tesorería	PT001

Configuración De Los Grupos:

El ingreso de las operaciones se realiza en el modulo de administración en donde se pide una descripción, luego se le al grupo a crear se le asocian las respectivas operaciones.

EJEMPLO:
Descripción operación: ingreso a la pagina de tesorería

Descripción Grupo	Código del Grupo
Grupo de tesoreros	112
ok	INGRESO A LA PAGINA DE TESORERIA
ok	LINK DE TABLAS EN PAC

Configuración de Los Usuarios:

El ingreso de las operaciones se realiza en el modulo de administración en donde se pide datos del usuario , a este se le asocian las respectivos grupos a los que puede pertenecer. Automáticamente las operaciones las apropia el usuario en relación al grupo para el que fue creado.

EJEMPLO:
Descripción operación: ingreso a la pagina de tesorería

Descripción Grupo	Código del Grupo
Grupo de tesoreros	112
ok	INGRESO A LA PAGINA DE TESORERIA
ok	LINK DE TABLAS EN PAC

Al igual que la unidad administrativa a la que pertenecerá y su cargo.

Ejemplos operaciones:

Ingreso a la página de tesorería : TP001

T = páginas de tesorería o de cada modulo

P = indica las páginas en general

001 = organización en cada modulo.

TS001 =

T = páginas de tesorería o de cada modulo.
S = consulta a la base de datos.
001 = organización en cada modulo.

TE001 =

T = páginas de tesorería o de cada modulo.
E = modificación a la base de datos.
001 = organización en cada modulo.

13. POLITICAS DE SEGURIDAD

13.1 DEFINICION DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

Es una forma de comunicarse con los usuarios y los gerentes. Estas establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes en una organización.

No se trata de una descripción técnica de mecanismos de seguridad, o de una expresión legal que involucre sanciones a conductas de los empleados. Es mas bien una descripción de lo que deseamos proteger y el porque de ello.

Cada política de seguridad es consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la institución.

13.2 CONTENIDO POLITICAS DE SEGURIDAD IMPLANTADAS EN EL MODULO DE ADMINISTRACION Y SEGURIDAD.

1. SOFTWARE
1.1 Ingreso al Sistema.
1.1.1 Usuarios
1.2 Interfaces.
1.2.1 Usuarios
1.3 Encriptación
1.3.1 Datos
1.4 Desarrollo
1.4.1 Codificación

2. CONFIGURACION DE SEGURIDAD EN SERVIDOR
2.1 Servicios de aplicaciones
2.1.1 Servidor aplicaciones
2.2 Servicios de bases de datos
2.3 Servidor de base de datos

3. REGISTRO DE DATOS
3.1 Historial de procesos.
3.1.1 Logs
3.2 Lectura y escritura de backup
3.2.1 Backups

1. SOFTWARE	
Aspecto:	1.1 Ingreso al Sistema.
Elemento:	1.1.1 Usuarios.
Se tiene un control de acceso a los usuarios desde la primera interfaz.	
El sistema identifica las peticiones que el usuario hace para ingreso al mismo.	
Cuando el sistema identifica al usuario, lo valida y monitoriza con privilegios su trabajo. De lo contrario, lo rechaza.	
Las actividad de inicio de sesión están previamente analizada por el software.	
El usuario puede ingresar a la dependencia a la que pertenece previamente condicionado por el administrador.	
Las transacciones y las visualizaciones que entrega el sistema son registradas por este para funciones de auditoria.	
El usuario trabajará con valores dados por la sesión durante la existencia de esta.	
Una vez que el usuario ingresa con una nueva sesión, no se podrá conectar nuevamente desde otra terminal o la misma.	

1. SOFTWARE	
Aspecto:	1.2 Interfaces.
Elemento:	1.2.1 Usuarios.
Las interfaces son previamente analizadas para cada usuario de a cuerdo con sus facultades de operación según la función que desempeña en el sistema.	
Todo trabajo actividad que desee realizar el usuario esta previamente analizada por el software.	
El usuario puede visualizar solo lo que el software le permite, esto previamente condicionado por el administrador.	
Las transacciones y las visualizaciones que le entrega el sistema al usuario son registradas por este para funciones de auditorias.	
El manejo de ventanas que contienen mensajes para el usuario en particular, son independientes a las tareas que esté realizando, pero se ejecutan al mismo tiempo.	
Las sesiones están en permanente contacto con el servidor de aplicaciones, el cual las mantendrá en ejecución constante y no permite que se destruya si no es de manera intencionada por el usuario.	

1. SOFTWARE	
Aspecto:	1.3 Encriptación
Elemento:	1.3.1 Datos.
Se utilizan algoritmos de encriptación para variables y datos de los usuarios.	
Los datos a encriptar solo podrán ser cambiados por el usuario mismo tales como login y contraseña.	
El sistema advierte el tiempo en que las contraseñan caducan, para que el usuario cambie estos valores.	
El programa permite que el tiempo de vida de las contraseñas sea cambiado según crea el administrador.	
Las contraseñas permanecen encriptadas en las bases de datos.	

1. SOFTWARE	
Aspecto:	1.4 Desarrollo
Elemento:	1.4.1 Codificación.
Se trabajó con software libre, como también con el que la Universidad tiene licenciado.	
La codificación se encuentra comentariada. Para motivos de manejos, cambios o actualizaciones.	
El desarrollo se llevó a cabo con base al análisis y diseño de la primera etapa del SIIFUN.	
La planificación para la seguridad que ofrece el software se realizó tomando prototipos de otras entidades.	

2. CONFIGURACION DE SEGURIDAD EN SERVIDOR	
Aspecto:	2.1 Servicios
Elemento:	2.1.1 Servidor de aplicaciones
Configurar las variables de entorno.	
Establecer la conexiones a la base de datos.	
Configurar la máquina virtual con que trabajará la aplicación.	
Se configuró la jerarquía de archivos y la organización utilizada por las aplicaciones incluyendo: páginas jsp, Servlets, Beans, Java Script, Estilos, Iconos,	

carpetas de los diferentes módulos, archivos XML, librerías.
Configurar la cantidad de usuarios que pueden existir haciendo uso de las sesiones.
Activar la limpieza de memoria periódicamente.
Especificar tipos de conexiones y de sesiones.
Protección de directorios, archivos, clases, código.

2. CONFIGURACION DE SEGURIDAD EN SERVIDOR	
Aspecto:	2.2 Servicios de bases de datos
Elemento:	2.2.1 Servidor de bases de datos.
Se configuró los drive de conexiones para la aplicación.	
Validaciones a los usuarios que intentan conectarse a la base de datos	
Reutilización de conexiones a bases de datos, en lugar de abrir nuevas.	
Hacer barrido de conexiones que no abandonadas, y limpiarlas de la memoria.	
Configuración del tiempo de vida de una conexión a la base de datos por usuario en la sesión.	

3. REGISTRO DE DATOS	
Aspecto:	3.1 Historial de procesos
Elemento:	3.1.1 logs.
Se construyó las carpetas para guardar las transacciones hechas por los usuarios.	
internamente en el código del programa, se encuentra las operaciones que cada usuario realiza en el SIIFUN.	
Existe una interfaz para visualizar las mencionadas operaciones para lo concurrente a Auditorias.	
Cada visualización de pantalla es registrada en los archivos logs. Al igual que cada registro, link u operación del sistema.	
Se implanto una jerarquía para estos archivos de logs.	

El programa no permite visualizar los archivos de logs de los propios usuarios.
El programa restringe la lectura de estos archivos con permisos de usuarios.

3. REGISTRO DE DATOS	
Aspecto:	3.2 Lectura y escritura de backup
Elemento:	3.2.1 Backup.
Se construyó las carpetas para guardar las modificaciones a la base de datos hechas por los usuarios.	
De manera automática en el código del programa, se encuentra las transacciones que cada usuario realiza en el SIIFUN. Por ello por algún motivo de caída del sistema, este guarda los últimos cambios que los usuarios hayan efectuado.	
Existe una interfaz para la restauración de la base de datos. Que se puede realizar solo con permisos exclusivos del usuario administrador.	
Estos archivos son resguardados.	

13.2.1 Generación de Propuestas para las políticas de seguridad externas al software

1. ENVIRONMENT PARA EL SERVIDOR.
1.2. Requerimientos para el servidor
1.3. Environment y seguridad.

2. RED DE DATOS
2.1 Servicios
2.1.1 Recursos de Red
2.2 Servicios
2.2.1 Recursos De Red
2.3 Servicios y usuarios
2.3.1 Recursos De Red para el usuario
2.4 Servicios
2.4.1 Internet
2.5 Servicios
2.5.1 Aplicaciones en Internet
2.6 Control Lógico
2.6.1 Servidores
2.7 Control lógico
2.7.1 Acceso.

2.8 Control lógico
2.8.1 Monitoreo.

1. ENVIRONMENT PARA EL SERVIDOR	
Aspecto:	1.2 Requerimientos para el servidor
Elemento:	1.2.1 Environment y seguridad.
Configuración de corriente eléctrica es :(AC power) 90-264 V AC (47-63 Hz); 760 W máximo AC output	
operación de temperatura debe ser promedios: 5 degrees C to 35 degrees C (41 degrees F to 95 degrees F), 10% to 90% relative humidity	
Temperature: -40 degrees C to 65 degrees C (-40 degrees F to 149 degrees F), up to 93% relative humidity, noncondensing, 38 degrees C max wet bulb.	
Altitud (operating): Up to 3000 m; maximum ambient temperature is derated by 1 degree C per 500 m above 500 m.	
Altitude (nonoperating) : Up to 12,000 m.	
Acoustic noise: Less than 6.7 bels sound power in temperatura ambiente de 24 grados Centígrados.	
Regulations: - Safety: IEC60950, UL/CSA60950, EN60950 - RFI/EMC: FCC Class A, Part 15 47 CFR, EN55022, CISPR 22 - Immunity: EN55024	
Dimenciones: - Height: 133 mm (5.3 inches) - Width: 444.5 mm (17.5 inches). - Depth: 756 mm (29.8 inches) - Weight: 34 kg (75 lb.) maximum	

1 2. RED DE DATOS	
Aspecto:	2.1 Servicios
Elemento:	2.1.1 Recursos De Red
Cada funcionario es responsable de proteger la información confidencial que llegue a sus manos.	

Es responsabilidad de Centro de Informática la implementación de mecanismos de seguridad que garanticen la integridad, confidencialidad, disponibilidad de la información.
La información confidencial debe ser protegida por reglamentación o leyes internas.
El administrador de la red de datos debe mantener un control de los recursos compartidos en la red.
En caso de que los usuarios necesiten compartir datos residentes en un computador, deberán usar correo electrónico y/o Directorios públicos que sean habilitados por el Centro de Informática.
Los servicios de News, chat, Real Audio, Netmeeting, mensajeria instantánea, descarga de música y programas, deben estar bloqueados. Si algún usuario necesita utilizar alguno de estos servicios por razones de trabajo, se debe realizar una solicitud por escrito, especificando el servicio, la hora y fecha exactas en que lo va a utilizar con su respectiva justificación y visto bueno del Jefe de la Dependencia. El servicio será habilitado temporalmente y específicamente para el usuario autorizado.
Cuando un funcionario recibe una nueva cuenta de usuario, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.
La solicitud de una nueva cuenta o el cambio de privilegios debe ser realizada por escrito y ser debidamente aprobada. No debe concederse una cuenta a personas que no sean trabajadores de la Universidad de Nariño a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente en un lapso de 30 días o inmediatamente termine su trabajo.

DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA, PARA EL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO. volúmenes 1 y 2 publicación Colombia 2005. p. 91

2. RED DE DATOS [2]	
Aspecto:	2.2 Servicios
Elemento:	2.2.1 Recursos De Red
Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.	

La información que viaja a través de la red de datos debe estar encriptada mediante algún algoritmo de encriptación que esta establecido por la institución Cuando un trabajador es despedido o renuncia a la Universidad, debe desactivarse su cuenta antes de que deje el cargo.
Si no ha habido actividad en una terminal, PC o estación de trabajo durante cierto periodo de tiempo, el sistema debe automáticamente bloquear la pantalla y suspender la sesión. El periodo recomendado de tiempo es de diez minutos. El re-establecimiento de la sesión requiere que el usuario proporcione se autentique nuevamente.
Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la Universidad, pudiendo ser causal de despido. Los servidores de red y los equipos de comunicación deben estar ubicados en lugares apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos lugares y a los cuartos de cableado a personas no autorizadas.
En caso de que los usuarios necesiten compartir datos residentes en un computador, deberán usar correo electrónico y/o Directorios públicos que sean habilitados por el Centro de Informática.
Los servicios de News, chat, Real Audio, Netmeeting, mensajeria instantánea, descarga de música y programas, deben estar bloqueados. Si algún usuario necesita utilizar alguno de estos servicios por razones de trabajo, se debe realizar una solicitud por escrito, especificando el servicio, la hora y fecha exactas en que lo va a utilizar con su respectiva justificación y visto bueno del Jefe de la Dependencia. El servicio será habilitado temporalmente y específicamente para el usuario autorizado.
Cuando un funcionario recibe una nueva cuenta de usuario, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.
La solicitud de una nueva cuenta o el cambio de privilegios debe ser realizada por escrito y ser debidamente aprobada. No debe concederse una cuenta a personas que no sean trabajadores de la Universidad de Nariño a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente en un lapso de 30 días o inmediatamente termine su trabajo.

2. RED DE DATOS	
Aspecto:	2.3 Servicios y usuarios
Elemento:	2.3.1 Recursos De Red para el usuario
No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Administrador de Sistemas o el Director del Centro de Informática lo determinen necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo. Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas. Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también implica que los administradores de sistemas Unix no deben entrar inicialmente como "root", sino primero empleando su propio ID y luego mediante "set userid" o "su" para obtener el acceso como "root". En cualquier caso debe registrarse en la bitácora todos los cambios de ID. Toda cuenta queda automáticamente suspendida después de 30 días de inactividad.[3]	
Se debe contar con un servidor de autenticación que pueda validar los usuarios que hacen parte de la red de datos.	

[2] DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA, PARA EL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO. volúmenes 1 y 2 publicación Colombia 2005. p. 91

[3] Ibid p. 110

4 2. RED DE DATOS	
Aspecto:	2.4 Servicios
Elemento:	2.4.1 Internet
Los servidores de correo electrónico deben estar configurados de tal forma que permitan realizar la identificación de posibles virus en archivos adjuntos. Se deben restringir los servicios de mensajera instantánea por Internet, descarga de música, emisoras y canales de televisión. Se debe especificar claramente los servicios de Internet que serán prestados y configurar el muro de fuego para que autorice el trafico de paquetes únicamente de esos servicios. La descarga de programas por Internet debe estar restringida, este proceso de ser necesario será realizado por personal especializado que determinara que tipo de programa, licenciamiento y la viabilidad e la instalación del mismo en computadores de la	

Universidad. No ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido, así ofrezca atractivos premios o temas provocativos. Mucho menos si estos archivos tienen doble extensión.
Tomar precauciones con los contenidos de applets de Java, JavaScripts y Controles ActiveX, durante la navegación, así como los Certificados de Seguridad.
Es recomendable configurar el navegador desactivando la ejecución automática de estos contenidos. No emplear los máximos privilegios en tareas para las que no sean estrictamente necesarios.
No se debe confiar en los archivos gratuitos que se descargan de sitios Web desconocidos, ya que son una potencial vía de propagación de virus Configurar el sistema para que muestre las extensiones de todos los archivos. De ninguna manera se debe ejecutar ningún archivo con doble extensión.

[4] DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA, PARA EL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO. volúmenes 1 y 2 publicación Colombia 2005. p. 94

2. RED DE DATOS	
Aspecto:	2.5 Servicios
Elemento:	2.5.1 Aplicaciones en Internet
No contestar los mensajes SPAM, ya que al hacerlo se re-confirmará su dirección IP, ni prestar atención a los mensajes con falsos contenidos , tales como ofertas de premios, dinero, solicitudes de ayuda caritativa, advertencia de virus de fuentes desconocidas, etc.	
Tampoco se deben descargar archivos con títulos atractivos pero sospechosos, desde canales de Chat, Newsgroups, redes compartidas como KaZaa, Morpheus, BearShare, etc. o vía FTP.	
Se debe borrar y revisar constantemente los cookies, archivos temporales e historial, en la opción Herramientas, Opciones de Internet, de su navegador. Al igual que su configuración. Los correos electrónicos debe registrar una firma digital que identifique la persona que envía el mensaje.	

2. RED DE DATOS	
Aspecto:	2.6 Control Lógico
Elemento:	2.6.1 Servidores
Debe existir un plan de capacitación continuo para los funcionarios operarios del SIIFUN en la concientización sobre los temas relacionados en seguridad. Los servidores deben configurarse de forma que permitan realizar revisión de log´s del servidor, frente a los accesos al sistemas, es decir de conexiones o ingreso al sistema	
Los servidores deben configurarse de forma que permitan realizar revisión de acceso fallido al sistema, servicios o archivos.	
Los servidores deben configurarse de forma que permitan realizar revisión de log´s de accesos remotos con o sin éxito.	
Los servidores serán instalados en áreas de tipo estratégico y restringido.	
Los servicios que no sean propios de cada servidor, se ejecutaran de forma manual, únicamente con autorización el administrador del sistema. Los servidores deben estar configurados para garantizar un número mínimo de caracteres para las contraseñas y un tiempo mínimo de caducidad estipulada por el administrador. El servidor debe garantizar los privilegios iniciales que deben contener los archivos que se generen, los cuales deben corresponder a la siguiente configuración: Propietario: lectura, escritura y ejecución. Grupo de trabajo: No lectura, No escritura y No ejecución. Otros usuarios: No lectura, No escritura y No ejecución.	

2. RED DE DATOS	
Aspecto:	2.7 Control Lógico
Elemento:	2.7.1 Acceso
Se debe mantener un control sobre las cuentas de usuario que se manejan en el servidor y deshabilitar las que se encuentren fuera de uso.	

El servidor debe restringir en especial a los usuarios, que no sean tipo administrador, el acceso a los archivos del sistema, la raíz principal del mismo y archivos de configuración.

2. RED DE DATOS	
Aspecto:	2.8 Control Lógico
Elemento:	2.8.1 Monitoreo
Para la detección de ataques se debe implementar sistemas de detección de intrusos (ISD). El Centro de Informática debe contar con herramientas para monitoreo y análisis de tráfico y control de accesos a Internet (herramientas IDS, administradores de URLs, firewalls)	
Se debe incorporar programas que permitan monitorizar los paques con que va a trabajar el servidor y sus estaciones.	

Se cita a continuación el material completo de las políticas generales de seguridad del Centro De Informática de La Universidad De Nariño, lugar donde se dará el manejo y se pondrá en funcionamiento el SIIFUN. En ese documento se encuentra la documentación amplia de Auditoria y Seguridad del lugar. Para que se adopten las medidas externas que puedan afectar al software, directa o indirectamente.

DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA, PARA EL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO. volúmenes 1 y 2 publicación 2005.

14. CONCLUSIONES.

- La realización de un modulo de administración y seguridad para los sistemas de información, produce grandes mejoras en el desempeño del mismo, obteniendo como resultados procesos, eficientes y seguros en el momento del manejo de los datos. El área de trabajo del proyecto SIIFUN con sus elementos es propicia, para que toda la información que allí se maneja se encuentre controlada y organizada debido a la importancia de la misma.

- Es importante destacar que los planes y políticas deben ajustarse específicamente a los requerimientos, circunstancias y procedimientos de cada una de ellas. Concientes que el conocimiento y el manejo de la información es el recurso más importante de toda institución y que es deber de las directivas gestionar e impulsar la adquisición del mismo, se pretende realizar la Auditoría a la seguridad informática del Centro de Informática con el fin de aportar una herramienta conceptual que permita a las directivas conocer el estado actual de esta dependencia y realizar los correspondientes correctivos y mejoras a la misma según unas políticas establecidas.

- Una de las principales deficiencias del sistema que actualmente se esta utilizando en la Universidad de Nariño es la ausencia total de documentación que oriente en el desarrollo y funcionamiento de cada proceso, dificultando la operación y mantenimiento del mismo. Con el trabajo realizado se presenta parte de la solución a este problema y con la facilidad que presentan los manuales para que se brinde la posibilidad de expansión de los módulos restantes.

- Es importante que la Universidad cuente con un equipo de personas con conocimientos en seguridad informática y Auditoría, aplicados a las áreas como redes de datos, programación, quienes constantemente realicen tareas de seguimiento a las diferentes actividades que involucran el procesamiento de registros. Ya que el valor de la información es muy alto y la mejor inversión, es protegerla

15. RECOMENDACIONES.

Es de vital importancia la concientización de adoptar en la puesta en marcha del sistema, las políticas de seguridad , y que todos los usuarios entiendan que el manejo de la información y su cuidado ameritan mucha responsabilidad.

Se debe administrar los registros de logs y de backups de manera segura, y para ello se debe disponer del personal idóneo para estos procesos. Así también, mantener este material en lugares seguros y restringidos con la mejor disposición para su protección

Mantener la documentación organizada para una posterior implementación de este módulo.

Cuando el sistema se encuentre funcionando, y se conecten los usuarios por medio de la Internet, se debe estudiar métodos para la restricción de personas que quieran ingresar al sistema de manera indebida.

REFERENCIAS BIBLIOGRÁFICAS

- ALDEGANI, Gustavo miguel. Seguridad Informática MP EDICIONES Argentina, 1997.

- DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA, PARA EL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO. volúmenes 1 y 2 publicación 2005.

- Disponible en Internet: http://documentación y Tutoriales de JAVA y POSTGRES.

- Disponible en Internet: www.solotutoriales.com

- ECHENIQUE G, José Antonio. Auditoría en Informática. McGrawHill, 2001.

- HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 2.1.

- http://ingenieroseninformatica.org/recursos/tutoriales
- http://www.javaencastellano.com
- http://ainsuca.javeriana.edu.co/sidre/EAIngSoftware.htm.
- http://www.trucosdeordenador.com

- PRESSMAN, Roger S. Ingeniería de Software- Un enfoque práctico. 5 ed.
- Madrid: McGraw-Hill, 2002. 597p.

- SISTEMA DE INFORMACION FINANCIERA DE LA UNIVERSIDAD DE NARIÑO S.I.I.F.U.N, volúmenes 1,2 y 3 publicación 2004.