ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERIA DE SISTEMAS
CARRERA INGENIERIA INFORMATICA MENCION REDES DE INFORMACION

DISEÑO DE UN ESQUEMA DE SEGURIDAD PARA LA INTRANET Y EXTRANET DEL CONESUP

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO INFORMÁTICO MENCIÓN EN REDES DE INFORMACION

CRISTINA ALEXANDRA CHAUCA CHIMBO
SAMIRA PAOLA VILLALBA LINDAO

DIRECTOR: ING. GUSTAVO SAMANIEGO

Quito, septiembre 2007

DECLARACIÓN

Nosotras, Cristina Alexandra Chauca Chimbo y Samira Paola Villalba Lindao, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Cristina Chauca Chimbo

Samira Villaba Lindao

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Cristina Alexandra Chauca Chimbo y Samira Paola Villalba Lindao bajo mi supervisión.

Ing. Gustavo Samaniego
DIRECTOR DE PROYECTO

AGRADECIMIENTO

A Dios por darnos salud y fuerza para culminar una meta.

A todas las personas que tuvieron paciencia , tiempo y voluntad para guiarnos en esta etapa de nuestras vidas.

DEDICATORIA

A mi hijo que fue uno de mis impulsos, que con su amor me tuvo paciencia.
A mis padres y a mejor amiga que me dieron el ánimo para terminar esta etapa de mi vida profesional.

Samira Villalba

A ustedes papitos queridos porque han sido la fuente de apoyo y amor incondicional.
A ti amiga por el apoyo recibido.

Cristina Chauca

CONTENIDO

DECLARACION i

CERTIFICACION ii

AGRADECIMIENTO iii

DEDICATORIA iv

CONTENIDO v

RESUMEN xii

PRESENTACION xiii

Capítulo 1 MARCO TEORICO 1

1.1 INTRANET/EXTRANET 1

1.1.1 RED 1

1.1.2 INTERNET 1

1.1.3 INTRANET 1

1.1.4 EXTRANET 2

1.2 SEGURIDADES EN REDES 4

1.2.1 LA INFRAESTRUCTURA DE LA TECNOLOGIA DE INFOMACION Y SU SEGURIDAD 4

1.2.1.1 Políticas y Procedimientos de Seguridad 6

1.2.1.2 Seguridad Física y del Entorno 6

1.2.1.3 Seguridad Perimental 6

1.2.1.4 Seguridad de Red propiamente dicha 7

1.2.1.5 Seguridad de Equipos 7

1.2.1.6 Seguridad de Aplicaciones 7

1.2.1.7 Seguridad de datos 8

1.2.2 TIPOS DE SEGURIDAD 8

1.2.2.1 Seguridad Física 8

1.2.2.2 Seguridad Lógica 8

1.2.3 PROPIEDADES DE LA SEGURIDAD INFORMATICA 8

1.2.3.1 Autenticidad 9

1.2.3.2 Integridad 9
1.2.3.3 Disponibilidad 9
1.2.3.4 Confidencialidad 9
1.2.4 BENEFICIOS DE LA SEGURIDAD 9
1.2.5 AREAS DE ADMINISTRACION DE LA SEGURIDAD 10
1.3 VULNERABILIDADES EN INTRANET/EXTRANET 10
1.3.1 TIPOS DE VULNERABILIDADES 10
1.3.2 AMENAZAS 11
1.3.3 ATAQUES 12
1.3.4 INTRUSOS 13
1.4 METODOLOGIA PARA EL DISEÑO DE SEGURIDADES EN REDES (INTRANET/EXTRANET) 14
1.4.1 ANALISIS DE RIESGO 14
1.4.2 DISEÑO DE SEGURIDADES 15
1.4.3 MANUAL DE POLITICAS 16
Capítulo 2. ANALISIS DE RIESGOS 17
2.1 RECOPILACION DE LA INFORMACION DE LA INTRANET Y EXTRANET 17
2.1.1 CONSEJO NACIONAL DE EDUCACION SUPERIOR 18
2.1.2 MISION 18
2.1.3 VISION 18
2.1.4 ORGANIGRAMA 18
2.1.5 ANALISIS FODA 19
2.1.6 IDENTIFICACION DE ACTIVOS 21
2.1.6.1 Activos Críticos 22
2.1.6.1.1 Información **22**
2.1.6.1.2 Software **23**
2.1.6.1.3 Hardware **24**
2.1.7 SEGURIDADES FISICAS 28
2.1.8 SEGURIDADES LOGICAS 28
2.1.8.1 Respaldo de datos 29

2.1.8.2 Seguridades legales 29
2.1.8.3 Mantenimiento 29
2.2 IDENTIFICACION DE VULNERABILIDADES EXISTENTES 29
2.2.1 PRINCIPALES CAUSAS DE AMENAZAS 30
2.2.2 CONSECUENCIAS DE LAS AMENAZAS 30
2.2.3 REQUERIMIENTOS DE SEGURIDAD 33
2.2.4 IDENTIFICACION DEL SISTEMA DE SEGURIDAD ACTUAL EN EL CONESUP 35
2.2.5 CREACION DE PERFILES DE AMENAZAS 37
2.2.6 IDENTIFICACION DE COMPONENTES CLAVES 42
2.2.7 EVALUACION DE VULNERABILIDADES EN LA RED 43
2.3 ANALISIS DE RESULTADOS 52
2.4 DETERMINACION DE REQUERIMIENTOS 53
Capítulo 3. DISEÑO DEL ESQUEMA DE SEGURIDAD 56
3.1 DISEÑO DE LA SEGURIDAD FISICA 56
3.1.1 AREAS SEGURAS 56
3.1.1.1 Perímetro Físico 56
3.1.1.2 Controles de acceso físico 57
3.1.1.3 Protección de oficinas 58
3.1.1.4 Aislamiento de las áreas de entrega y carga 59
3.1.2 SEGURIDAD DE LOS EQUIPOS 59
3.1.2.1 Ubicación y protección de los equipos 59
3.1.2.2 Suministros de Energía 60
3.1.2.3 Seguridad del Cableado 60
3.1.2.4 Mantenimiento de Equipos 60
3.1.2.5 Seguridad de los equipos fuera de la Institución 61
3.1.2.6 Baja o reutilización de equipos 61
3.2 DISEÑO DE LA SEGURIDAD LOGICA 61
3.2.1 DISEÑO DE LA RED 62
3.2.1.1 Metodología SAFE 62

3.2.1.1.1 Módulo Internet **63**
3.2.1.1.2 Módulo Campo **63**
3.2.1.2 Diseño de la red del CONESUP **64**
3.2.1.2.1 Módulo Internet **65**
3.2.1.2.2 Módulo Campo **66**
3.2.2 CONTROL DE ACCESO LOGICO **67**
3.2.2.1 Requerimientos para el control de acceso **67**
3.2.2.1.1 Políticas de Control de accesos **67**
3.2.2.2 Administración de accesos de usuarios **67**
3.2.2.2.1 Registro de Usuarios **68**
3.2.2.2.2 Administración de contraseñas **68**
3.2.2.2.3 Revisión de derechos de acceso de usuario **69**
3.2.2.3 Responsabilidades del usuario **69**
3.2.2.3.1 Uso de Contraseñas **69**
3.2.2.3.2 Equipos desatendidos en áreas de usuarios **70**
3.2.2.4 Control de acceso a la red **70**
3.2.2.4.1 Políticas para utilizar los servicios de red **70**
3.2.2.4.2 Enrutamiento Forzado **70**
3.2.2.4.3 Autenticación de usuarios para conexiones externas **71**
3.2.2.4.4 Control de conexión a la red **71**
3.2.2.5 Control de acceso al Sistema Operativo **71**
3.2.2.5.1 Procedimientos de conexión de PCs **71**
3.2.2.5.2 Identificación y Autenticación de los usuarios **71**
3.2.2.5.3 Sistema de administración de contraseñas **72**
3.2.2.5.4 Limitación del horario de conexión **72**
3.2.2.6 Control de acceso a las aplicaciones **72**
3.2.2.6.1 Restricción del acceso a la información **72**
3.2.2.7 Monitoreo del acceso y uso de los sistemas **73**
3.2.2.7.1 Registro de eventos **73**
3.2.2.7.2 Monitoreo del uso de los sistemas **73**
3.2.2.8 Computadores móviles y trabajo remoto **73**
3.2.2.8.1 Computadores móviles **74**

3.2.2.8.2 Trabajo remoto **74**

3.3 MANUAL DE POLITICAS Y PROCEDIMIENTOS **74**

3.3.1 POLITICAS **74**

3.3.1.1 Políticas de seguridad del hardware **74**

3.3.1.1.1 Adquisición e instalación de equipos **74**

3.3.1.1.2 Seguridad física del equipo **75**

3.3.1.1.3 Mantenimiento de equipos **75**

3.3.1.2 Políticas de seguridad del software **76**

3.3.1.2.1 Adquisición, instalación y actualización **76**

3.3.1.3 Políticas de seguridad para el control de acceso a los sistemas de información **77**

3.3.1.3.1 Acceso Físico **77**

3.3.1.3.2 Acceso a la información (archivos y documentos) **77**

3.3.1.3.3 Respaldos y Recuperación de archivos **78**

3.3.1.3.4 Acceso a los servidores de red **78**

3.3.1.3.5 Administración de usuarios **79**

3.3.1.3.6 Correo electrónico e Internet **79**

3.3.1.4 Políticas de seguridad para el desarrollo de software **80**

3.3.1.5 Políticas de seguridad para contingencia **80**

3.3.1.6 Políticas de seguridad para la capacitación del personal **81**

3.3.2 PROCEDIMIENTOS **81**

3.3.2.1 Adquisición de nuevos equipos **83**

3.3.2.2 Adquisición de partes de hardware **83**

3.3.2.3 Instalación y/o cambio físico de equipos **84**

3.3.2.4 Registro y/o actualización de los datos del equipo y sus partes **84**

3.3.2.5 Para sacar un equipo fuera de la Institución **85**

3.3.2.6 Apagado de equipos si se produce un corte de suministro eléctrico **85**

3.3.2.7 Mantenimiento Correctivo **85**

3.3.2.8 Mantenimiento Preventivo **86**

3.3.2.9 Actualización y/o instalación de software en los **87**

equipos

3.3.2.10 Adquisición y Registro del software nuevo en el departamento de Sistemas 87

3.3.2.11 Acceso al área de Servidores 88

3.3.2.12 Permisos para el acceso a los archivos 88

3.3.2.13 Respaldos de archivos, aplicaciones y bases de datos 89

3.3.2.14 Restauración de respaldos de archivos, aplicaciones y bases de datos 89

3.3.2.15 Acceso a las aplicaciones 90

3.3.2.16 Acceso a Base de datos 90

3.3.2.17 Acceso al correo electrónico e Internet 90

3.3.2.18 Acceso Remoto 91

3.3.2.19 Creación de usuarios 91

3.3.2.20 Actualización (Modificación y eliminación) de usuarios 91

3.3.2.21 Bloqueo y desbloqueo de usuarios 92

3.3.2.22 Mantenimiento de correo electrónico 92

3.3.2.23 Permisos y restricciones del acceso a páginas de Internet 92

3.3.2.24 Plan de restauración de aplicaciones y bases de datos 93

Capítulo 4. ANALISIS COSTO/BENEFICIO 94

4.1 COSTO DE EQUIPAMIENTO, INSTALACION, CONFIGURACION 94

4.2 PRESENTACIÓN Y SELECCIÓN DE PROVEEDOR EN EL MERCADO 95

4.2.1 PRESENTACION DE PROVEEDORES 95

4.2.2 SELECCIÓN DE PROVEEDORES 96

4.3 DETERMINACION DEL PRESUPUESTO PARA LA IMPLEMENTACION 96

4.4 ANALISIS COSTO/BENEFICIO 97

4.4.1 IDENTIFICACION DE BENEFICIOS 97

4.4.2 ANALISIS DE AHORRO EN COSTOS 97

4.4.2.1 Identificación de Servicios al Público, tiempo y costos 97

4.4.2.2 Resultados del ahorro en costos 99

Capítulo 5. CONCLUSIONES Y RECOMENDACIONES 101

5.1 CONCLUSIONES 101

5.2 RECOMENDACIONES 103

GLOSARIO 104

BIBLIOGRAFIA 107

ANEXO I. INVENTARIO DE EQUIPOS 108

ANEXO II. ENCUESTA DE EMPLEADOS IT 113

ANEXO III. CARACTERISTICAS Y PRECIOS DE PROVEEDORES 120

ANEXO IV. METODOLOGIA OCTAVE-OMIG (CD)

NORMA ISO 17799 (CD)

MODELO SAFE DE CISCO (CD)

RESUMEN

Hoy en día el tema de las seguridades informáticas para las pequeñas y medianas empresas evoluciona con gran rapidez en nuestro medio, siendo necesario proteger nuestra información de posibles ataques internos o externos.

El presente trabajo propone un diseño de seguridades para la Intranet y Extranet del CONESUP basados en diferentes metodologías tales como: OCTAVES, SAFE CISCO para pequeñas empresas y las NORMAS ISO 17799.

Este trabajo proporciona además un manual de políticas de seguridad y procedimientos que ayudaran a minimizar los posibles ataques a la red del CONESUP.

PRESENTACION

El presente proyecto se estructuro en cinco capítulos:

Aunque el primer capítulo trate el marco el teórico, posiblemente sea uno de los mas importantes ya que en el se intenta transmitir la idea de seguridad, que es el resultado de operaciones realizadas por personas y soportadas por tecnologías, además presenta conceptos de seguridad que serán manejados a lo largo del proyecto.

En el segundo capítulo se recopilará información de la situación actual de la empresa, se identificaran vulnerabilidades y se realizará el análisis de riesgo, una vez determinados los resultados se procederá a la determinación de requerimientos.

El diseño de seguridades tanto físicas como lógicas son desarrollados en el tercer capítulo dependiendo de los requerimientos determinados en el capítulo anterior, además se desarrollará un manual de políticas y procedimientos.

En el cuarto capítulo se recopilaran costos de equipamiento, instalación y configuración de los dispositivos a utilizarse en el nuevo de diseño de seguridad, y determinar un presupuesto para la implementación. Se describirá los requisitos que deberán presentar las empresas para ser parte de la lista proveedores del CONESUP y se concluirá con un análisis costo / beneficio que tendrá como resultado de la implementación del diseño de seguridad.

Por último en el capítulo cinco, se describirán conclusiones y recomendaciones para la aplicación del diseño y la continúa revisión de las seguridades de información en el CONESUP.

Capítulo 1. MARCO TEORICO

1.1 INTRANET / EXTRANET

1.1.1 RED

Es un conjunto de computadores autónomos interconectados entre si con el propósito de compartir recursos de procesamiento y/o almacenamiento, mantener y mejorar el desempeño de la red, reducir costos, y se constituirse en un poderoso medio de comunicación e información eficaz y eficiente para el usuario.

1.1.2 INTERNET

Es el conjunto de redes TCP/IP interconectadas entre si a nivel mundial, y en el que convergen diferentes plataformas de hardware y software, con el propósito de proporcionar información y servicios.

1.1.3 INTRANET

Un Intranet es una red TCP/IP o conjunto de redes TCP/IP interconectadas entre si al interior de una institución, empresa u organización, la misma que puede proporcionar todos los servicios de Internet y sistemas de información y aplicaciones de software para uso privado de dicha institución.

Beneficios

- Compartir y publicar información a los usuarios de la Intranet
- Crear canales de comunicación interna
- Disponibilidad de la información de acuerdo al perfil del usuario
- Optimización de recursos y reducción de costos.
- Comunicación y coordinación centralizada

Características

- Están basadas en la arquitectura cliente-servidor.
- Funciona con diferentes plataformas de Hardware y Sistemas Operativas independientemente del fabricante.
- Utiliza la familia de protocolos de comunicación TCP/IP
- Es amigable y fácil de usar.

1.1.4 EXTRANET

Es una Intranet en la que se permite el acceso restringido y controlado de la información a usuarios externos que no pertenecen a la institución u organización dueña de la Intranet. Se puede conectar de diferentes formas:

- Mediante Internet
- Por línea telefónica Dial-up (conmutada)
- Con una Línea dedicada
- Mediante una Red Celular

Permite la conexión a proveedores y/o clientes de la organización. La infraestructura de los usuarios externos no forma parte de la red física de la Intranet.

Beneficios

- Acceso a recursos e información de una red sin necesidad de estar ubicado físicamente dentro de la red.
- Acceso a servicios que brinda la empresa al proveedor y/o clientes

Características

- El acceso es controlado por perfiles a usuarios externos.
- Se permite el acceso solamente a determinadas aplicaciones e información

En la tabla 1.1. se presenta un cuadro comparativo de las características de Internet, Intranet y Extranet

	Internet	Intranet	Extranet
Acceso	Público	Privado	Restringido
Usuarios	Todo Público	Miembros de la institución o empresa	Usuarios de otras empresas que mantienen relación con la empresa dueña de la intranet
Información	Fragmentada y distribuida ampliamente	Privada	Compartida en un ambiente confiable con el fin de alcanzar determinados objetivos

Tabla 1.1 Cuadro comparativo de Internet, Intranet, Extranet

En la figura 1.1 se ilustra la interconexión ente el Internet, Intranet y Extranet

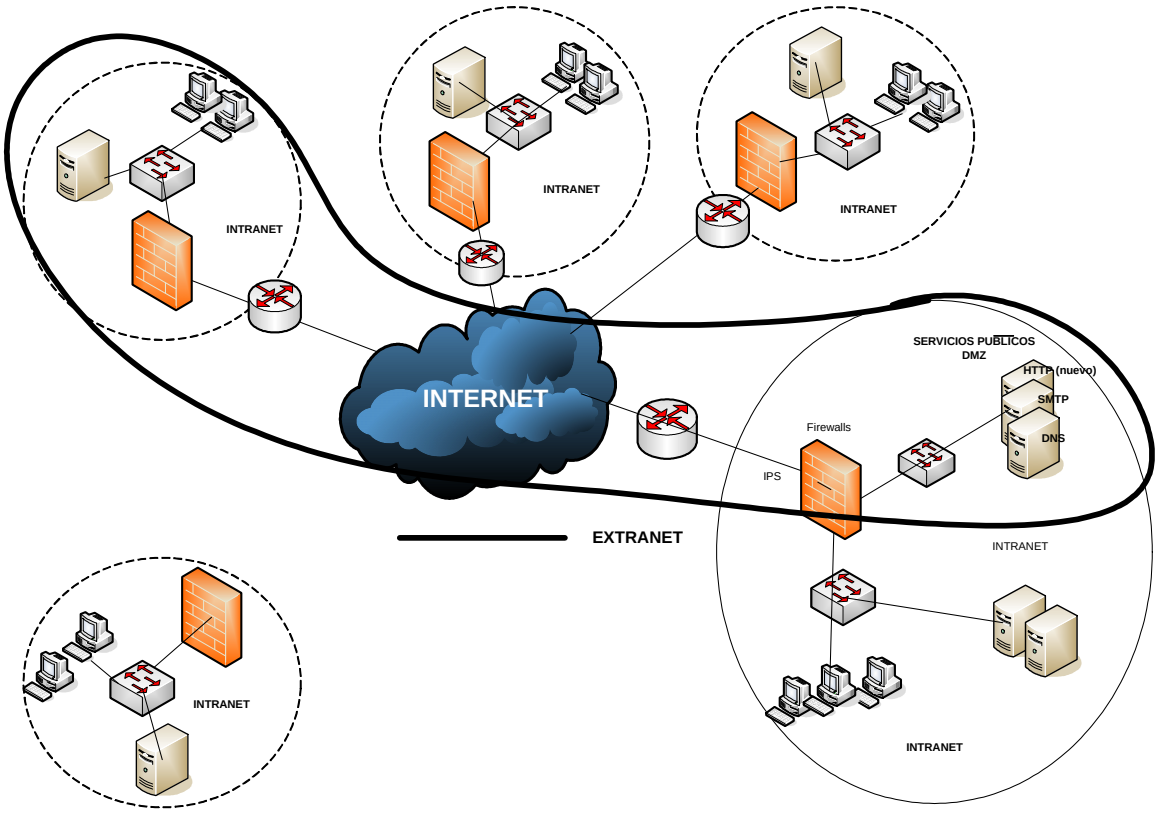

Fig. 1.1 Diagrama Internet, Intranet y Extranet (Mediante Internet)

1.2 SEGURIDADES EN REDES

La seguridad en las redes pretende minimizar la vulnerabilidad en los sistemas de información, además se puede decir, que es el conjunto de procedimientos y recursos utilizados con el fin de guardar integridad, confidencialidad, y disponibilidad en la información. De ahí que las medidas de seguridad que se implantarán deberán ser proporcionales al bien que se intente proteger.

Objetivos de las seguridades

- Proteger la información para que no sea alterada y/o divulgada personas no autorizadas.
- Minimizar los riesgos contra un determinado ataque
- Evitar la interrupción que el servicio ofrece

1.2.1 LA INFRAESTRUCTURA DE LA TECNOLOGÍA DE INFORMACIÓN Y SU SEGURIDAD

Para minimizar el riesgo de manera que se garantice un nivel aceptable de Confidencialidad, Integridad y Disponibilidad de los activos de información se tomará como referencia una Infraestructura de Tecnología de Información formada por capas donde en cada una de ellas estén involucradas personas, tecnología y operaciones. [1]

Personas

Para garantizar la seguridad de la información debe implicarse el personal. Evidentemente quien primero debe tomar conciencia de la necesidad de gestionar la seguridad de la información es la propia Dirección de la empresa. Este compromiso del personal con la seguridad se traducirá posteriormente en la adopción de políticas y procedimientos de seguridad, la asignación de funciones y responsabilidades de seguridad, la formación y concienciación del personal,

1 ALVAREZ GONZALO, C. Seguridad Informática

tanto administradores como usuarios, y la auditoria de las acciones realizadas por el personal. Es necesario implantar mecanismos de seguridad física, que exigen la colaboración de todo el personal

Tecnología

Existe una gran cantidad de soluciones técnicas de seguridad disponibles en el mercado que permiten salvaguardar la Confidencialidad, Integridad y Disponibilidad de la información, Sin embargo, sin unas políticas y procedimientos de seguridad adecuados, las medidas técnicas se implantarán mal o donde no hacen falta, sin objetivos claros y a menudo de forma inconsistente o incompleta. La tecnología, sin un sistema global de gestión de la seguridad, resulta ineficaz y produce una falsa sensación de seguridad, defraudando las expectativas generadas.

Operaciones

Sostener la seguridad de la organización requiere una serie de acciones diarias como por ejemplo mantener actualizada y comunicada la política de seguridad; gestionar la seguridad por ejemplo, con una política adecuada de actualización de parches; gestionar las contraseñas de usuarios y servidores; evaluar la seguridad de las medidas implantadas mediante auditorias y pruebas periódicas; mantener al día el plan de recuperación ante desastres.

La Infraestructura de Tecnologías de información, se subdivide en siete capas donde sobre cada una de ellas se debe implantar un mecanismo de protección. [1] Estas capas son:

1.- Políticas y Procedimientos de Seguridad.
2.- Seguridad Física y del entorno.
3.- Seguridad perimetral.
4.- Seguridad de Red
5.- Seguridad de equipos.

6.- Seguridad de Aplicaciones.
7.- Seguridad de Datos

1.2.1.1 Políticas y Procedimientos de Seguridad

Esta parte posiblemente sea la mas descuidada y desatendida de todas, siendo precisamente la mas importante, ya que constituye la piedra angular de la Seguridad.

La Dirección de la organización debería aprobar, publicar y comunicar a todos los empleados un documento de políticas de seguridad de la información. Debería establecer el compromiso de la Dirección y el enfoque de la organización para gestionar la seguridad de la información.

1.2.1.2 Seguridad Física y del Entorno

Si un intruso tiene la posibilidad de acceder físicamente a los equipos e infraestructuras de la red (al hardware), el mayor riesgo planteado es que podría dañar o robar los dispositivos junto con la información que contienen. Las medidas que se deberán adoptar son por ejemplo: control del personal que accede a los distintos recursos y dependencias; puesto de trabajo despejado, es decir, no deben quedar papeles ni disquetes ni CD ni ningún otro soporte de información sensible al alcance de un intruso físico y siempre debe activarse el bloqueo de terminal cuando éste quede desatendido mediante salvapantallas protegido por contraseña; utilización de cajas fuertes, armarios y cajoneras con llaves; rejas en las ventanas, puertas blindadas y sistemas de alarma conectados a una central para guardar los accesos exteriores; etc.

1.2.1.3 Seguridad Perimetral

El perímetro es el punto o conjunto de puntos de la red interna de confianza gestionada por la propia organización en contacto con otras redes externas no fiables, no sólo Internet. El atacante posee acceso a los servicios ofrecidos o

accesibles desde el exterior. El perímetro se protege instalando cortafuegos, redes privadas virtuales, routers bien configurados, redes inalámbricas debidamente protegidas y módems telefónicos controlados así como antivirus.

1.2.1.4 Seguridad de Red propiamente dicha

Si una persona no autorizada posee acceso a la red interna de la organización, potencialmente puede acceder a cualquier puerto de cualquier equipo o monitorizar el tráfico que circula por la red, de forma pasiva (solo de lectura) o activa (modificable). Para proteger la red de estas amenazas se puede utilizar sistemas de detección de intrusos, segmentación de redes mediante routers y switches, utilizando IPSEC y/o SSL para cifrado durante el transporte de datos, protección de redes inalámbricas.

1.2.1.5 Seguridad de Equipos

La seguridad de equipos tanto servidores como clientes implica las siguientes tareas: mantenerse al día con los parches de seguridad, desactivar todos los servicios innecesarios y mantener el antivirus activo y constantemente actualizado. El mayor riesgo es cuando el atacante puede acceder al equipo a través de vulnerabilidades en servicios del sistema operativo a la escucha. El bastionado y la aplicación de plantillas de seguridad constituyen las dos herramientas básicas para proteger equipos.

1.2.1.6 Seguridad de Aplicaciones

Las aplicaciones se protegen realizando un control de acceso mediante la sólida implantación de mecanismos de autenticación y autorización. Una medida de seguridad adicional consiste en la instalación de cortafuegos de aplicación, dedicados a filtrar el tráfico específico de distintas aplicaciones: correo (SMTP), Web (http), bases de datos, etc.

1.2.1.7 Seguridad de datos

Si un atacante ha traspasado todas las barreras anteriores y posee acceso a la aplicación, la autenticación y autorización, así como el cifrado, constituyen las tecnologías mas empleadas para proteger los datos.

1.2.2 TIPOS DE SEGURIDAD

1.2.2.1 Seguridad Física

La seguridad física está relacionada con los recursos y el espacio físico utilizados para la protección de los elementos que conforman los sistemas de información dentro de la empresa, tales como:

- Control de acceso físico a servidores y cuarto de control
- Ubicación y ambiente adecuado de los servidores y cuarto de control
- Uso correcto de PC’s

1.2.2.2 Seguridad Lógica

La seguridad lógica está relacionada con los procedimientos y recursos lógicos utilizados para proteger los sistemas de información dentro de la empresa. Tales como:

Creación de perfiles de usuarios. Es decir el acceso a la información será parcial dependiendo del perfil del usuario y utilizando contraseñas.
Utilización de algoritmos de encriptación para la transmisión de información
Utilización de sistemas de monitoreo para llevar un control sobre el acceso a los sistemas y usuarios.

1.2.3 PROPIEDADES DE LA SEGURIDAD INFORMATICA

La seguridad informática debe cuidar que no se violen las siguientes propiedades:

1.2.3.1 Autenticidad

Garantiza que una entidad es quien dice ser. El servicio de autenticidad protege del ataque de suplantación de personalidad (masquerade), es decir, que una entidad externa se hace pasar por quien no es. Este servicio puede ser utilizado de dos formas: Autenticación de una de las partes (origen o destino), o autenticación mutua

1.2.3.2 Integridad

El objetivo de esta propiedad es garantizar que los datos y recursos no han sido alterados y sean fiables. Asegura al receptor que el mensaje recibido fue el mismo que el enviado por el emisor, es decir, la información no fue añadida, modificada o sustraída. Un ataque a esta propiedad puede darse en el almacenamiento, transporte o procesamiento de la información.

1.2.3.3 Disponibilidad

El objetivo de esta propiedad es garantizar que la información y los servicios no sean interrumpidos y permanezcan accesibles en forma permanente.

1.2.3.4 Confidencialidad

El objetivo de esta propiedad es garantizar que el mensaje no sea revelado a terceras personas o personas no autorizadas, pero que si sean entendibles por el destinatario correcto.

1.2.4 BENEFICIOS DE LA SEGURIDAD

Los beneficios de un sistema de seguridad bien elaborado son inmediatos, ya que la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

Aumento de la productividad. El hecho de implementar políticas de seguridad, tales como: Acceso restringido a Internet, Uso correcto de usuarios y claves, etc; hace que el personal utilice los recursos adecuadamente logrando un aumento de la productividad.

Compromiso con la misión de la compañía.- Brinda confiabilidad al usuario final, lo cual se refleja en la buena imagen de la Institución.

1.2.5 AREAS DE ADMINISTRACIÓN DE LA SEGURIDAD

Existen tres áreas de administración de la seguridad y son:
Autenticación.- Es decir identificar al personal que pueden tener acceso a la información y servicios en la empresa.
Autorización.- Esta área de administración es la encargada de crear perfiles para que los usuarios solo puedan acceder a la información del área de trabajo que ellas dominen
Auditoria.- Esta área vigila en forma continua los servicios en producción, existen herramientas para realizar estadísticas sobre el uso y el acceso de los servicios en la red.

1.3 VULNERABILIDADES EN INTRANET / EXTRANET

La vulnerabilidad en una red es originada con errores individuales de ciertos componentes que al interactuar con varios de ellos generan inseguridad en la red.

1.3.1 TIPOS DE VULNERABILIDADES

Físicas .- Se relaciona con el espacio donde se encuentran ubicados los dispositivos de la red; por ejemplo, son vulnerabilidades las inadecuadas instalaciones de trabajo, disposición desorganizada de cables de energía y red, ausencia de recursos para el combatir incendios, etc.

En Hardware.- Son vulnerabilidades de hardware las que se relacionan con los componentes de hardware de la red. Por ejemplo el mal dimensionamiento de un equipo para las funciones que va a desarrollar, falta de equipos para plan de contingencia, defectos de fabricación de los dispositivos, etc.

En Software.- Estas vulnerabilidades están relacionadas con las aplicaciones de sistemas informáticos. Por ejemplo, instalaciones indebidas de aplicaciones a usuarios inexpertos o mal intencionados, configuraciones incompletas de los sistemas operativos, entre otros.

En la Transmisión de la Información.- Existen vulnerabilidades en la transmisión de la Información por la ausencia de sistemas de encriptación, por la elección de un sistema inadecuado para envío de mensajes de alta prioridad y por errores en los medios de transmisión.

Actualmente existen analizadores de vulnerabilidades desarrollados por expertos que identifican y definen las vulnerabilidades de una red bajo un esquema de reglas; sin embargo, el conocimiento de estas reglas puede ocasionar que personas malintencionadas realicen ataques a las redes que no tienen protección contra estas vulnerabilidades.

1.3.2 AMENAZAS

Es una condición para hacer daño o perjudicar a alguien o a la red que al tener la oportunidad viola la seguridad de la misma.

Las amenazas pueden ser:

Amenazas Naturales

Estas amenazas son relacionadas con las condiciones naturales por ejemplo, la humedad, el clima, el polvo, desastres naturales, etc; estas amenazas pueden ser

prevenidas teniendo cuidados especiales en el entorno donde se ubicarán los equipos de la red.

Amenazas Accidentales o Involuntarias

Son aquellas que aparecen en forma no premeditada, por ejemplo en operaciones indebidas de usuarios inexpertos, fallos de software, funcionamiento irregular de los sistemas, etc. Una forma de prevenir este tipo de amenazas es teniendo procedimientos para el mantenimiento de sistemas informáticos como, una revisión periódica de equipos, capacitación a usuarios para evitar errores humanos, mantenimiento de instalaciones, etc. Estos procedimientos deberán ser tomados en cuenta en una análisis de riesgos global.

Amenazas Intencionales

Estas amenazas son la participación maliciosa de un sujeto o entidad para un uso indebido de la red. Las amenazas intencionales se denominan ataques.

1.3.3 ATAQUES

Un ataque informático es la violación de la seguridad de una red (confidencialidad, integridad, disponibilidad o uso legítimo).
La información que circula por la Intranet o extranet de una empresa puede ser atacada de diferentes formas.

Interrupción o Denegación de servicio.- El intruso bloquea la transmisión de la información para que el receptor no la reciba, es decir, la degradación fraudulenta del servicio impide la realización de un proceso normal en la red. Este ataque afecta el principio de disponibilidad de la información.

Intercepción.- El emisor transmite la información al receptor, pero esta es interceptada por una tercera persona. También puede realizarse la divulgación o repetición del contenido, es decir, captura un proceso legítimo y lo repite para

producir un efecto no deseado o destinarlo a una persona no autorizado. Este ataque afecta al principio de confidencialidad.

Suplantación de identidad.- El intruso se hace pasar por el emisor generando información y transmitiéndola al receptor. Este ataque permite el acceso a la información a personas no autorizadas. Por ejemplo, se produce cuando una persona o entidad suplanta la personalidad de la otra, se enmascara para realizar una función no autorizada en la red. Este ataque afecta al principio de autenticidad de la información.

Modificación.- El intruso intercepta la información enviada por el emisor, la altera o modifica (substracción o adición del mensaje) y la trasmite al receptor, además puede reordenarla o retardarla para que se produzca un efecto no deseado y evita que esta alteración sea detectada. Este ataque afecta al principio de integridad.

1.3.4 INTRUSOS

Existen dos clases de intrusos:

Pasivo .- El intruso pasivo accede a la información confidencial que esta siendo trasmitida sin realizar ninguna modificación en ella, es decir, se dedica a monitorear la red. Los objetivos principales son la intercepción de la información y el análisis de tráfico.

La información mas importante para el intruso pasivo y que le permite intercambiar con organizaciones en competencia son: conocer al emisor y al receptor en una comunicación, conocer el volumen de tráfico y el horario mas habitual de la trasmisión de información entre las entidades.

Este intruso es muy difícil de detectar porque no ocasiona ninguna alteración a la información; sin embargo, se puede prevenir un ataque de este tipo con mecanismos de cifrado de información.

Activos.- El intruso activo altera la información que es interceptada con intenciones maliciosas.

Las personas que realizan este tipo de ataque generalmente son:

Terroristas.- Es decir, cualquier persona que ataca al sistema para causar algún daño en él, por ejemplo: borrar bases de datos o destruir sistemas de ficheros, etc.
Ex–empleados.- Es decir, personas descontentas con la organización que pueden aprovechar debilidades de un sistema que conocen, por ejemplo: insertar troyanos, bombas lógicas o simplemente conectarse al sistema como si aun trabajara para la organización

1.4 METODOLOGIA PARA EL DISEÑO DE SEGURIDADES EN REDES (INTRANET / EXTRANET)

1.4.1 ANÁLISIS DE RIESGO

Para el desarrollo del análisis de riesgo del presente proyecto se ha tomado como referencia la metodología OCTAVE OMIG Versión 2.0, adaptandolo a las necesidades de la Institución.

OCTAVE son las siglas de Operational Critical Treath, Asset, an Vulnerability Evaluation, desarrollado por Carnegie Mellon University.

Este es un método que está basado en un conjunto de criterios, las cuales definen los elementos esenciales para la evaluación del riesgo de seguridad. Las principales características de este método son:

Comprensivo.- Pues se organiza con fases y procesos.

Autodirigido.- Este método puede ejecutarlo un pequeño grupo de personas de la institución

OCTAVE comprende básicamente 3 grandes Fases:

FASE 1: Reunión de Activos – Perfiles de Amenazas.- En esta fase, se debe recoger: Información de activos existentes, requerimientos de seguridad, áreas de interés, estrategias de protección actuales y vulnerabilidades existentes.

FASE 2: Identificación de Vulnerabilidades en la Infraestructura.- Enfoca a las vulnerabilidades tecnológicas que afectan a los activos críticos y componentes de infraestructura que soportan a estos activos.

FASE 3: Define los riesgos asociados con los activos críticos. Crea planes de mitigación para esos riesgos y elabora una estrategia de plan organizacional. Los planes y estrategias son revisados y aprobados por la gerencia.

1.4.2 DISEÑO DE SEGURIDADES

Para el diseño de seguridad de la red tanto físico como lógico, el presente proyecto se basa en la metodología SAFE de CISCO para pequeñas y medianas empresas.

Safe no es una guía para diseñar redes, mas bien es una guía para asegurar las redes, ya que ellas seguirán ofreciendo todos los servicios que el usuario espera de la red.

La metodología Safe de Cisco se basa en un enfoque modular por dos motivos importantes. El primero es que la arquitectura relaciona la seguridad entre los distintos bloques funcionales de la red, y el segundo, permite al diseñador evaluar e implementar la seguridad módulo a módulo en lugar de hacerlo generalmente.

1.4.3 MANUAL DE POLÍTICAS

Para la elaboración del Manual de políticas y procedimientos se utilizó como guía la NORMA ISO 177999, tanto para la seguridad física como lógica de la red, que tratan de promover sistemas de calidad para la seguridad del usuario inclinándose al conocimiento y a la aplicación de la normalización como base de la calidad.

Capítulo 2. ANÁLISIS DE RIESGOS

Definición de Riesgo:

Es la probabilidad de que una amenaza o ataque se concrete, explote una vulnerabilidad y provoque un efecto negativo en la red.

El riesgo es mayor mientras mayor es el valor del activo y mayor su grado de exposición a amenazas.

El riesgo no puede eliminarse por completo, pero si se puede reducir.

Objetivos del Análisis de Riesgos:

- Identificar las amenazas que un sistema de información y su entorno pueden tener.
- Cuantificar las consecuencias e impacto generado por los ataques y amenazas concretados

2.1 RECOPILACIÓN DE LA INFORMACIÓN DE LA INTRANET Y EXTRANET.

Para la recopilación de la información tanto de la Intranet como Extranet, se la clasificará en dos partes; en la primera se identificará la Institución donde se desarrollará el diseño de seguridades, su misión, visión, organigrama y el análisis FODA para tener un diagnóstico de la situación actual en los diferentes ambientes (interno y externo) y que será utilizada posteriormente en la identificación de las vulnerabilidades. Y en segundo lugar se identificará los activos mediante la metodología OCTAVE, para luego realizar el análisis de riesgo.

2.1.1 CONSEJO NACIONAL DE EDUCACION SUPERIOR

Definición

El Consejo Nacional de Educación Superior es una entidad autónoma de Derecho Pública con personería jurídica, sus siglas son “CONESUP” y es el organismo planificador regulador y coordinador del Sistema Nacional de Educación Superior.

2.1.2 MISIÓN

Definir la política de Educación Superior.
Estructurar, planificar, dirigir, regular, coordinar, controlar y evaluar el Sistema Nacional de Educación Superior.

2.1.3 VISIÓN

Ser un Sistema de Educación Superior académicamente competitivo a nivel mundial.
Referente de los sistemas de Educación.
Caracterizado por su ética, autonomía, pertinencia y calidad.
Fundamentado en el crecimiento y el pluralismo.
Y por su compromiso con el desarrollo, los valores ancestrales y el respeto a la naturaleza.

2.1.4 ORGANIGRAMA

En la figura 2.1 se puede ilustra el organigrama de la Institución

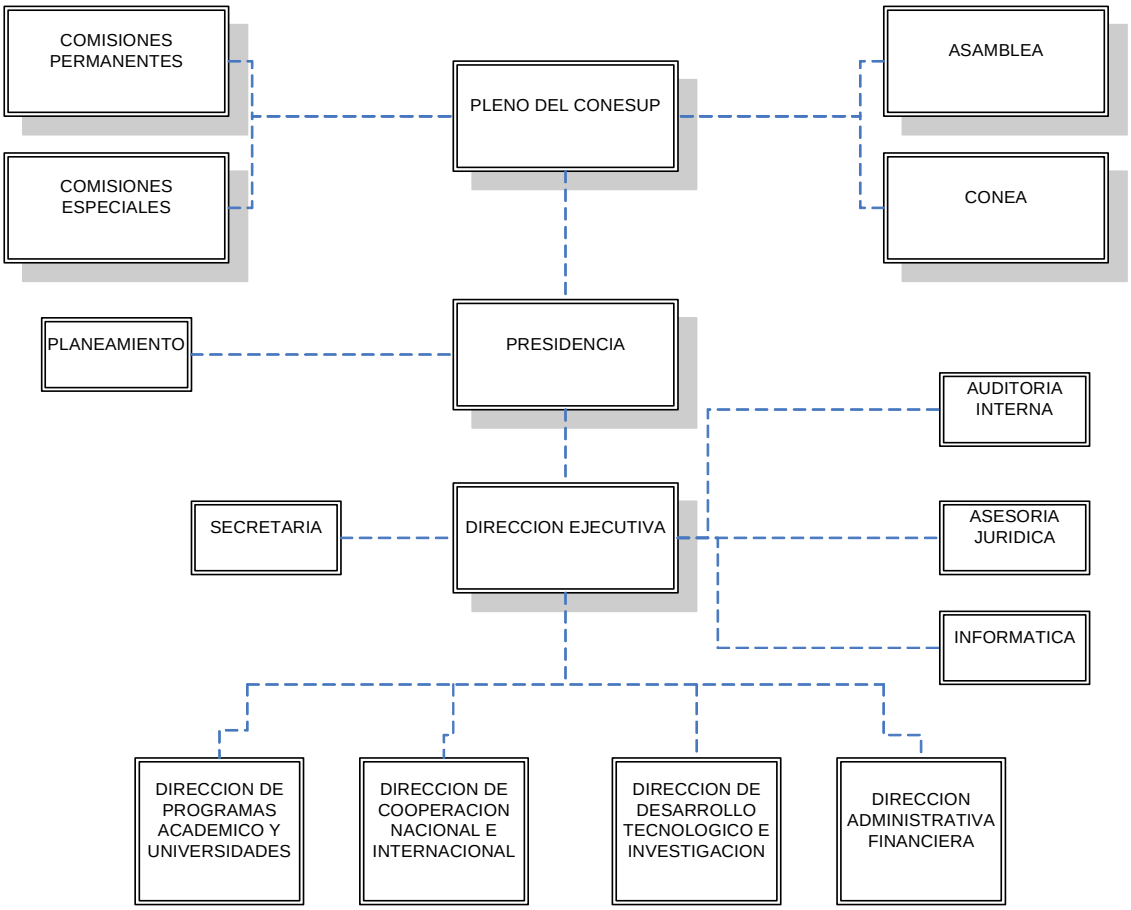

Fig. 2.1 Organigrama del CONESUP

2.1.5 ANALISIS FODA

El análisis FODA será utilizado para identificar los factores externos e internos que afectan directa o indirectamente a la Institución.

Fortalezas

Personal capacitado y con experiencia

Dinamismo en ejecución de proyectos especiales

Hardware adquirido

Apoyo de autoridades

Oportunidades

Desarrollo tecnológico
Software y hardware disponible
Convenios con otras instituciones o empresas

Debilidades

Personal a contrato
Falta de motivación
Falta de capacitación en actualización tecnológica
Variedad en plataforma en SI
Resistencia interna al cambio
Falta de coordinación entre áreas
Bajo nivel de conocimientos informáticos de usuarios internos

Amenazas

Limitación de recursos de la institución para proyectos informáticos
Cambios políticos.
Injerencia de personas ajenas a la unidad
Ocultamiento de la información

En el análisis FODA se pudo detectar que entre las debilidades se encuentran; el trabajar con personal de contrato sin establecerles políticas en la manipulación de la información ya que sin ellas existe gran riesgo de perdida y modificación de la misma; además la falta de coordinación entre áreas y los bajos conocimientos informáticos de los usuarios internos. Sin embargo podemos destacar que si existe apoyo de parte de las autoridades promoviendo la capacitación necesaria para los empleados.

FASE I

2.1.6 IDENTIFICACION DE ACTIVOS

GRUPO DE ACTIVOS	
Activos Importantes	**Descripción**
INFORMACIÓN	
Base de datos Académico	Información Académica de Universidades, Escuelas Politécnicas e Institutos. Información de Graduados de Universidades, Escuelas Politécnicas e Institutos
Base de datos Sigef	Información financiera de la Institución
Base de datos Olimpo	Información de los activos fijos de la Institución
Base de datos Regycont	Información de la documentación externa
SOFTWARE	
Sistema Académico	Aplicación que maneja la información medular del CONESUP como: Información general y académica de las Universidades, Escuelas Politécnicas e Institutos Registro de Títulos de graduados Certificación de Títulos Legalización de Firmas
Sigef	Sistema Gubernamental de Contabilidad y Finanzas con el cual se administra la contabilidad y finanzas del CONESUP
Olimpo	Sistema para la administración de activos fijos e inventario
Regycont	Sistema para el seguimiento de documentación del CONESUP
HARDWARE	
Servidor de Correo	Equipo para la administración del correo electrónico del CONESUP
Servidor PDC_CONESUP	Equipo donde se encuentra el Servidor de base de datos: Oracle 8i y SQL Server 7.0
Servidor BDC_CONESUP	File Server, Http Server
Servidor SEDNA	Equipo donde se encuentra la biblioteca virtual, foro y chat
Servidor REGYCONT	Equipo donde se encuentra la base de datos y la aplicación del registro y control de documentación
Router	Equipo mediante el cual se establece la conexión hacia el exterior de la Intranet
Switchs	Equipo mediante el cual se establece la comunicación al interior de la Intranet y son parte fundamental del backbone de la red
PCs	Estaciones de trabajo de cada usuario de la red, donde almacenan información de las actividades que desempeñan.

Laptops	Equipos utilizados en reuniones o comisiones de trabajo donde almacenan información y son utilizadas en su mayoría como estaciones de trabajo
Computadores de casa	Equipos personales utilizados para conectarse remotamente a servicios de la Intranet del CONESUP
Access Point	Componentes Wireless
OTROS ACTIVOS	
SRI, SITAC	

Tabla 2.1 Activos del CONESUP

Según lo indicado en la tabla 2.1, tenemos 3 grupos bajo los cuales se clasifican los activos del CONESUP. Dentro de cada grupo se escogerá a los activos mas críticos dentro de la Institución.

2.1.6.1 Activos Críticos

2.1.6.1.1 Información

Dentro de este grupo tenemos como principal activo a la *Base de Datos Académico*, que contiene la información medular del CONESUP, esto es: Información general de Universidades, Escuelas Politécnicas e Institutos Técnicos y Tecnológicos, que contiene, el nombre de la Institución, tipo de entidad (privada, pública), dirección, pagina web, e-mail, número telefónico, servicios, autoridades.

Además de la oferta académica que existe en cada una de ellas, como por ejemplo: Carreras de Pregrado y Postgrado, duración, modalidad, lugar, convenios.

Otra información también almacenada en la base de datos es la de graduados clasificados en: pregrado, postgrados, reconocimiento de títulos extranjeros y reconocimientos de títulos de colegios profesionales. Cada grupo contiene la siguiente información: Universidad, carrera, duración, modalidad, nombres, sexo, nacionalidad, fecha inicio y fecha fin de estudios, título de bachiller, procedencia del título de bachiller, reconocimiento de estudios superiores en años o créditos,

institución de donde viene el reconocimiento, fecha de acta de grado, No. Acta de grado, título, fecha de refrendación, No. De refrendación, Nombre de Proyecto de Tesis, Responsable del ingreso de información por parte de la Institución Educativa.

La *base de datos Sigef,* es otro activo crítico ya que en ella se almacena la información financiera de la Institución como son los salarios, dietas, gastos, cuenta contables, etc.

Otro activo crítico es la *base de datos del Regycont,* donde se almacena la información resumida de la documentación que ingresa y sale de la Institución así como su imagen.

2.1.6.1.2 Software

Dentro de este grupo tenemos como activo importante el *Sistema Académico*, mediante el cual se tiene acceso y se manipula la información de la base de datos antes descrita. Es un sistema desarrollado en la misma institución bajo la plataforma Windows y ASP.

El Sistema *Sigef* es otro activo importante ya que maneja toda la información financiera de la Institución como: Salarios, gastos y cuentas contables.

El Sistema *Regycont*, es una aplicación que se encarga del ingreso y seguimiento de la documentación externa así, como de la información que sale de la Institución.

El Sistema Olimpo, es una aplicación que administra los activos fijos de la Institución.

2.1.6.1.3 Hardware

Se considera como activos críticos de Hardware a los equipos que son importantes en el procesamiento, almacenamiento y transmisión de la información crítica descrita anteriormente.

- **Servidores**

En la tabla 2.2 se describen las características y funciones de cada Servidor

TOTAL	MODELO	CARACTERISTICAS	FUNCION
2	COMPAQ PROLIANT ML 370	Procesador:800 Mhz Memoria: 1 GB Disco: SCSI 72 y 18 GB	**PDC_CONESUP (BDD)** -Servidor de base de datos: Oracle 8i y SQL Server 7.0 -DNS -Sigef (BDD y Aplicación) -Olimpo (BDD y Aplicación) -Sistema Academico (BDD) **SEDNA** -File Server -Mail Server -Http Server -Seguridad
3	CLON	Procesador: 1600 MHz Memoria: 1 GB Disco: 80, 20 y 32 GB	**BDC_CONESUP (**Http Server-File Server) -Sistema Academico (Aplicación) **CORREO** -Print Server -Apache -MySQL -Correo Electrónico **REGYCONT** -Servidor de base de datos y Aplicación del Regycont -File Server

Tabla 2.2 Descripción de Servidores

- **Router**

  CISCO 1751

<u>Características</u>

- 32 MB Flash
- 64 MB DRAM
- Cisco IOS IP Software Feature
- Funcionalidades de voz
- Interfaces WAN son incluídas por separado

- **Switchs**

  3COM

Características

- 24 ports 10/100 Mbps Nway auto-negociables
- Auto MDI-II/MDI-X ports (todos los puertos son Up-link con cualquier cable)
- Integrate address Look-Up Engine, supports up to 8 K absolute MAC address
- 2.5 Mb internal RAM for frame buffering
- Modo de Transmisión Full/Half duplex para cada Puerto (200 Mbps)
- Tazas Wire-speed filtering/forwarding
- Control de flujo IEEE 802.3x flow para modo Full-duplex
- Control de flujo Back pressure para modo Full-duplex
- Método Store-and-forward switching
- Extensive front-panel diagnostic LEDs
- 5 años de garantía

- **CABLEADO**

  UTP Categoría 5e

- **PCs.**

Según el inventario realizado (Ver Anexo I), se resume lo siguiente:

Se cuenta con 80 equipos personales dentro de la Intranet en Quito. Adicionalmente existen 5 equipos fuera de la ciudad y desde los cuales se tiene acceso a los recursos de la Intranet.
El 90% de los usuario almacenan la información en los respectivos discos duros de los equipos a su cargo. Estos discos duros tienen una capacidad de almacenamiento de alrededor de 40 GB.
El 80%, esto es 60 equipos, tienen licencias para el sistema operativo, aplicaciones y herramientas de oficinas.
Los equipos personales son Clones, con sistema operativo Windows 2000 Proffesional, con 512 MB en RAM, 40 GB en Disco duro como mínimo.
Utilizan como aplicaciones principales: Office 2000 Proffesional, Winzip, Internet Explorer

- **Portátiles**

Según el inventario realizado (Ver Anexo I) se concluyó que:

Existen 15 computadores portátiles, cada uno configurado para acceder a la red de la intranet
El 90% de los equipos son utilizados como maquinas de escritorio y adicionalmente son empleados para reuniones o comisiones de trabajo fuera de la institución
En la mayoría de discos duros se almacena información institucional por utilizarlas como equipos personales

- **Servicio de Web Hosting**

Además de los equipos que se encuentran en la intranet, se tiene un Web hosting en el exterior, ubicado en los Estados Unidos donde se encuentra almacenadas

algunas aplicaciones como: La pagina web del CONESUP, Proyectos de Investigación, Recepción de Archivos, Foro, además se cuenta con un espacio para bases de datos. En el siguiente resumen dado por los técnicos del servidor se detalla la seguridad con la que cuenta.

El servidor cuenta con un sistema operativo Unix FreeBSD, en el caso de existir algún servicio innecesario es removido del sistema para disminuir el numero de programas que necesitarían seguridad. Los puertos que son comúnmente usados por los hackers para atacarlos son protegidos por firewalls.
Todos los password son cambiados con palabras seguras, no adivinables.

El software que es usado en el sistema es actualizado o parchado apropiadamente contra las vulnerabilidades de seguridad cuando son descubiertos.

Los técnicos monitorean activamente los servicios de alerta de seguridad, los servidores ejecutan scripts o cgis bajo el usuario nobody en lugar de utilizar la propia cuenta de usuario, así no se tendrá acceso a los archivos sensitivos de las cuenta, en caso de que los scripts lleguen a estar comprometidos.

Mientras la cuenta esta en el servidor no hay otros usuarios compartiendo dicha cuenta, en servidores compartidos usted puede asegurar sus archivos de otros usuarios removiendo el grupo de acceso y ejecutando scripts a través de wrappers.

En los servidores se ejecutan programas de seguridad para detectar programas sospechosos, si uno es descubierto se envía mensajes a los técnicos para revisar los servidores de esta manera la actividad en la red es monitoreada.

Si existe un programa sospechoso, un alto numero de paquetes o trafico grande se notifica a un técnico para la revisión. Las reglas del firewall pueden ser configuradas para bloquear dicho tráfico desde los servidores.

Las colas de emails también son monitoreadas y los trabajos muy grande en la cola son notificados para protección contra explosiones de scripts o spams .
La red misma es totalmente cambiada de tal manera que el tráfico del servidor no pueda ser olfateadas por otro servidor. El trafico de datos se realiza mediante con fibra óptica a los proveedores.

Para cualquier scripts o aplicación que se necesite instalar el propietario es el responsable de la instalación, no se provee parches de seguridad o auditorias al software instalado por el usuario.

2.1.7 SEGURIDADES FÍSICAS

Las instalaciones físicas del CONESUP, consisten en un edificio y una casa de dos pisos consecutivos, los cuales son custodiados por guardias, las habitaciones donde se encuentran los servidores tienen acceso restringido y se encuentran cerradas generalmente con llave que posee el administrador de la red.
Se cuenta con una unidad UPS que provee energía eléctrica en caso de un cese de fluido eléctrico a los servidores, con el objeto de salvaguardar los equipos y los datos de posibles daños.

2.1.8 SEGURIDADES LÓGICAS

Cada usuario posee un USERNAME y PASSWORD tanto para el personal técnico como para los operarios de los terminales.

El administrador del sistema, en este caso el responsable del proceso de informática, es quien crea las cuentas a cada usuario, la misma que esta formada de la siguiente manera:

napellido
Donde:
n= primera letra del primer nombre
apellido= primer apellido

Para seguridad de los datos y de la red de posibles accesos no deseados se posee un firewall a nivel lógico o de software: INET SERVER con LINUX

2.1.8.1 Respaldo de datos

Se realiza un doble respaldo diario de las BDDs y se copian a dos servidores distintos (al propio servidor y a uno alterno)

2.1.8.2 Seguridades legales

La institución no cuenta con todas las licencias requeridas por la ley, ya que solo se tienen 70 licencias para Microsoft Windows y existen alrededor de 80 terminales con este producto.

2.1.8.3 Mantenimiento

El mantenimiento de los equipos y de la infraestructura informática en general es correctivo, es decir, se lo aplica solamente cuando un equipo necesita una reparación o existe un problema determinado. No se realizan mantenimientos preventivos.

2.2. IDENTIFICACIÓN DE VULNERABILIDADES EXISTENTES

Luego de la identificación de activos, se debe identificar las áreas preocupantes
Siguiendo con los procedimientos de OCTAVE, se debe identificar las amenazas de los activos, las áreas que son afectadas, sus causas y consecuencias.

2.2.1 PRINCIPALES CAUSAS DE AMENAZAS

Acción deliberada y/o accidental por parte de personas.- Este grupo incluye a personas que son parte del CONESUP así como a personas que no pertenecen a el, quienes pueden tomar acción deliberada sobre los activos.

Problemas del Sistema.- Estos problemas son por ejemplo defectos de hardware, defectos de software, no disponibilidad de los sistemas, virus, código malicioso, y otros problemas relacionados.

Otros Problemas.- Estos son problemas que están fuera de algún control. Esto puede incluir desastres naturales.

2.2.2 CONSECUENCIAS DE LAS AMENAZAS

- Revelación u Observación de información sensitiva
- Modificación de información importante o sensitiva
- Destrucción o pérdida de la información, hardware o software importante.
- Interrupción de acceso a la información, software, aplicaciones o servicios

A continuación, en la tabla 2.3 se detalla las amenazas y sus consecuencias para cada activo, tanto de información, así como de hardware y software para luego realizar el respectivo análisis.

ACTIVO	CAUSAS DE AMENAZAS			CONSECUENCIA			
	Acciones deliberadas y/o accidentales por parte de personas	**Problemas de sistemas**	**Otros Problemas**	**Revelación**	**Modificación**	**Destrucción y/o pérdida**	**Interrupción**
INFORMACIÓN							
Base de datos Académico	X	X		X	X	X	X
Base de datos Olimpo	X	X		X	X	X	X
Base de datos Sigef	X	X		X	X	X	X
Base de datos del Regycont	X	X		X	X	X	X
HARDWARE							
Servidor de Correo	X	X				X	X
Servidor PDC_CONESUP	X	X				X	X
Servidor BDC_CONESUP	X	X				X	X
Router		X				X	X
Switchs		X				X	X
Servidor SEDNA	X					X	X
Servidor REGYCONT	X	X		X		X	X
SOFTWARE							
Sistema Académico	X	X		X	X	X	X
Regycont	X	X		X	X	X	X
Sigef	X	X		X	X	X	X
Olimpo	X	X		X	X	X	X

Tabla 2.3 Causas de Amenaza y sus consecuencias para cada activo

Análisis tabla 2.3

Información

Como muestra la tabla 2.3, la Información tiene como fuente de amenaza la acción deliberada y/o accidental de personas que se encuentran dentro o fuera del CONESUP, debido a que muchos usuarios confían sus contraseñas a otras personas. Adicionalmente no existe mucha seguridad en las oficinas y los usuarios dejan aplicaciones abiertas, entre los mas frecuentes podemos encontrar el Sistema Regycont y el Sistema Académico. Esto puede ocasionar la revelación, modificación o perdida de la información.

Hardware

Una amenaza para el hardware, es el robo de portátiles y por ende el robo de la información existente en dichos equipos.

Se puede tener también Problemas de Sistemas debido a hardware defectuoso de fábrica.

Adicionalmente el hardware está expuesto a otro tipo de amenazas como desastres naturales, cortocircuitos.

Como consecuencia de estas amenazas se tiene la suspensión del servicio que brindan las aplicaciones del CONESUP

Software

Una fuente de amenaza para el Software del CONESUP, son básicamente los problemas del Sistema. Dentro de los problemas del sistema se describe lo siguiente:

- Cuellos de botella
- Códigos Maliciosos
- Retardos en las Aplicaciones
- Aplicaciones no disponibles
- Condiciones de lazos mal elaborados en las aplicaciones por ejemplo los reportes en el Sistema Académico.

Como consecuencia de estas amenazas, se tiene la interrupción del servicio de las aplicaciones del CONESUP

2.2.3 REQUERIMIENTO DE SEGURIDAD

En la tabla 2.4 se identifica los requerimientos de seguridad para los activos críticos.

ACTIVO	REQUERIMIENTO DE SEGURIDAD
INFORMACION	
Base de datos Académico	Disponibilidad Acceso a la información es requerida 24/7 Integridad Los nuevos ingresos y la modificación deben ser realizados por personas autorizadas Confidencialidad Puede ser conocido
Base de datos Regycont	Disponibilidad Acceso a la información 24/5 Integridad Esta información debe ser manejada por personas autorizadas de cada área Confidencialidad Solamente el área puede conocer la información respectiva
Base de datos Olimpo	Disponibilidad Acceso a la información 24/5 Integridad Debería ser administrada por personal autorizado Confidencialidad Solo conocido para personal autorizado
Base de datos Sigef	Disponibilidad Acceso a la información 24/7 Integridad Debería ser administrada por personal autorizado Confidencialidad Solo conocido para personal autorizado
HARDWARE	
Servidor de Correo Servidor PDC_CONESUP Servidor BDC_CONESUP Servidor SEDNA Servidor REGYCONT Router Switchs	Disponibilidad Acceso a la información 24/7 Integridad Administrado solo por el personal de sistemas Confidencialidad No aplica
SOFTWARE	
Sistema Académico	Disponibilidad Acceso a la información 24/7 Integridad Solo manipulado por el personal autorizado

	Confidencialidad Solo conocido por personal autorizado
Sigef	Disponibilidad Acceso a la información 24/7 Integridad Solo manipulado por el personal autorizado Confidencialidad Solo conocido por el personal autorizado
Olimpo	Disponibilidad Acceso a la información 24/7 Integridad Solo manipulado por el personal autorizado Confidencialidad Solo conocido por el personal autorizado
Sistema Regycont	Disponibilidad Acceso a la información 24/7 Integridad Solo manipulado por el personal autorizado Confidencialidad Solo conocido por el personal autorizado

Tabla 2.4 Requerimientos de seguridad de cada activo

Según la tabla 2.4, se resume lo siguiente :

Información

Disponibilidad

Las bases de datos deben estar disponibles las 24/7, por consultas o por trabajos fuera de horario.

Integridad

Todos los ingresos y modificaciones deben ser realizados por personas autorizadas de las áreas correspondientes.

Confidencial

Solamente la base de datos Académico puede ser visualizada por el publico, las demás por el personal autorizado.

Hardware

Disponibilidad

El hardware tiene que estar disponible todo el tiempo de manera que permita el funcionamiento optimo de la red.

Integridad

Solo puede ser administrado por el departamento de sistemas.

Confidencialidad

No aplica

Software

Disponibilidad

Las aplicaciones tienen que estar disponible las 24/7 para brindar los diferentes servicios al público.

Integridad

Las actualizaciones o modificaciones a los sistemas deben ser realizados por el departamento de informática.

Confidencialidad

Conocido solo por el departamento de informática.

2.2.4 IDENTIFICACIÓN DEL SISTEMA DE SEGURIDAD ACTUAL EN EL CONESUP

Según la encuesta realizada al personal de IT en el CONESUP (Ver Anexo II), se han obtenido los siguientes resultados:

No hay conocimiento de la seguridad de los sistemas de información y por ende no existe documentación de la misma.
Existen estrategias de seguridad basadas en los objetivos del CONESUP, sin embargo éstos no son documentados ni revisados periódicamente.

El CONESUP no da a conocer sobre la responsabilidad que el personal debe tener con la seguridad de la información, pues en los contratos laborales no existe una cláusula que indique aquello. Adicionalmente existe poco interés para invertir en soluciones de seguridad.

No existe ninguna documentación sobre políticas de seguridades, ni un plan de contingencia en la organización.

No existen políticas de seguridad ni procedimientos para controlar el acceso físico al personal, al hardware o dispositivos de comunicación, cabe mencionar que por esta falta de políticas ya se ha tenido perdidas.

Existe un control de activo (hardware y equipos de oficina) por parte del departamento administrativo. No existe un plan para el mantenimiento de equipos tanto para hardware y software, cada equipo que llega a tener problemas es reparado en ese momento.

Los respaldos de la información sensitiva se guardan en otra maquina dentro de la misma organización.

Cada usuario cuenta con una password para el ingreso al SO, y para algunas aplicaciones que manejan información sensitiva.

El monitoreo de la red y el firewall son revisados frecuentemente por el administrador, uno de los problemas que tiene la organización es que no cuenta con equipos modernos en cuestión de servidores y por esta razón hay cuellos de botella.

No existen procedimientos para el manejo de vulnerabilidades, ni un actual diseño de la arquitectura de seguridad y topología de la red en la empresa.

2.2.5 CREACION DE PERFILES DE AMENAZAS

Siguiendo con el modelo del Octave, se procederá con un estudio de amenazas por accesos de los actores humanos, entre ellos:

Acceso a la Red.- Es decir, cuando se amenaza a un activo critico utilizando la red en una forma accidental o deliberadamente.

Acceso Físico.- Cuando se amenaza a un activo critico desde el espacio físico mediante un actor humano

Problemas del sistema.- Cuando se amenaza a un activo crítico mediante problemas de software, hardware o alguna aplicación por ejemplo: Defectos de software, virus, caídas del sistema, defectos de hardware.

Otros problemas.- Cuando la amenaza de un activo crítico, se encuentra en desastres naturales, problemas con tercerizadoras, problemas de telecomunicaciones, problemas de proveedores.

A continuación, en las siguientes tablas se analizará los problemas que ocasiona el actor humano tanto interno como externo con los diferentes accesos que cuenta.

Activo (bien)	Interno (actor)							
	Accidental (motivo)				Intencional (motivo)			
	Disponibilidad	Modificación	Perdida / Destrucción	Interrupción	Disponibilidad	Modificación	Perdida / Destrucción	Interrupción
	(consecuencia)				(consecuencia)			
INFORMACION								
Base de datos Académico		X	X			X	X	
Base de datos Sigef		X	X			X	X	
Base de datos Olimpo		X	X			X	X	
Base de datos Regycont		X	X			X	X	
SOFTWARE								
Sistema Académico	X			X	X			X
Sigef	X			X	X			X
Olimpo	X			X	X			X
Regycont	X			X	X			X
HARDWARE								
Servidor de Correo	X			X	X			X
Servidor PDC_CONESUP	X			X	X			X
Servidor BDC_CONESUP	X			X	X			X
Router	X			X	X			X
Switchs	X			X	X			X
Servidor SEDNA	X			X	X			X
Servidor REGYCONT	X			X	X			X

Tabla 2.5 Actores humanos Internos usando el acceso a la Red

Activo (bien)	Externo (actor)							
	Accidental (motivo)				Intencional (motivo)			
	Disponibilidad	Modificación	Perdida / Destrucción	Interrupción	Disponibilidad	Modificación	Perdida / Destrucción	Interrupción
	(consecuencia)				(consecuencia)			
INFORMACION								
Base de datos Académico				X			X	X
Base de datos Sigef				X			X	X
Base de datos Olimpo				X			X	X
Base de datos Regycont				X			X	X
SOFTWARE								
Sistema Académico	X			X	X			X
Sigef	X			X	X			X
Olimpo	X			X	X			X
Regycont	X			X	X			X
HARDWARE								
Servidor de Correo	X				X			
Servidor PDC_CONESUP	X				X			
Servidor BDC_CONESUP	X				X			
Router	X				X			
Switchs	X				X			
Servidor SEDNA	X				X			
Servidor REGYCONT	X				X			

Tabla 2.6 Actores humanos Externos usando el acceso a la Red

Activo (bien)	Interno (actor)							
	Accidental (motivo)				Intencional (motivo)			
	Disponibilidad	Modificación	Perdida / Destrucción	Interrupción	Disponibilidad	Modificación	Perdida / Destrucción	Interrupción
	(consecuencia)				(consecuencia)			
INFORMACION								
Base de datos Académico		X				X		
Base de datos Sigef		X				X		
Base de datos Olimpo		X				X		
Base de datos Regycont		X				X		
SOFTWARE								
Sistema Académico	X		X	X	X		X	X
Sigef	X		X	X	X		X	X
Olimpo	X		X	X	X		X	X
Regycont	X		X	X	X		X	X
HARDWARE								
Servidor de Correo	X				X			
Servidor PDC_CONESUP	X				X			
Servidor BDC_CONESUP	X				X			
Router	X				X			
Switchs	X				X			
Servidor SEDNA	X				X			
Servidor REGYCONT	X				X			

Tabla 2.7 Actores humanos Internos usando el acceso Físico

Activo (bien)	Externo (actor)							
	Accidental (motivo)				Intencional (motivo)			
	Disponibilidad	Modificación	Perdida / Destrucción	Interrupción	Disponibilidad	Modificación	Perdida / Destrucción	Interrupción
	(consecuencia)				(consecuencia)			
INFORMACION								
Base de datos Académico		X	X			X	X	
Base de datos Sigef		X	X			X	X	
Base de datos Olimpo		X	X			X	X	
Base de datos Regycont		X	X			X	X	
SOFTWARE								
Sistema Académico			X	X			X	X
Sigef			X	X			X	X
Olimpo			X	X			X	X
Regycont			X	X			X	X
HARDWARE								
Servidor de Correo	X		X	X	X		X	X
Servidor PDC_CONESUP	X		X	X	X		X	X
Servidor BDC_CONESUP	X		X	X	X		X	X
Router	X		X	X	X		X	X
Switchs	X		X	X	X		X	X
Servidor SEDNA	X		X	X	X		X	X
Servidor REGYCONT	X		X	X	X		X	X

Tabla 2.8 Actores humanos Externos usando el acceso Físico

Análisis de las amenazas cuando los actores humanos accesan a la red y al espacio físico

Según la tablas 2.5, 2.6, 2.7 y 2.8 se resume que puede haber una modificación o pérdida de la información en las bases de datos causada por actores internos y externos de la organización. Actualmente se cuenta con una seguridad básica para el ingreso a los equipos que consisten en claves o perfiles de usuarios, pero no existe un documento donde se identifiquen las prácticas de seguridad para el personal, tales como: Políticas de passwords, que no se divulgue información sensitiva, asegurar la información del cual ellos son responsables, etc.

Con respecto a los sistemas, la mayoría accesa a la información de las base de datos y por contar con servidores de poca capacidad existe en muchas ocasiones cuellos de botella lo que ocasiona que la aplicación sea interrumpida o no este disponible.

Con respecto al hardware, muchas veces se interrumpe el trabajo debido a algún daño en el equipo. No existe un plan de mantenimiento, uno de los problemas mas frecuentes es la fuente de poder que deja de funcionar, en varias ocasiones hasta quema los demás dispositivos, lo que retrasa como mínimo un día de trabajo.

A continuación, las tablas 2.9 y 2.10 se refieren a otros actores que afectan a los activos

D=Disponibilidad
M=Modificación
P=Perdida
I=Interrupción

Activo (bien)	Actores															
	Defectos de Software				Virus				Caídas del Sistema				Defectos de hardware			
	Consecuencias															
	D	M	P	I	D	M	P	I	D	M	P	I	D	M	P	I
INFORMACION																
Base de datos Académico	x			x	x		x	x	x			X	x			x
Base de datos Sigef	x			x	x		x	x	x			X	x			x
Base de datos Olimpo	x			x	x		x	x	x			X	x			x
Base de datos Regycont	x			x	x		x	x	x			X	x			x
SOFTWARE																
Sistema Académico	x			x	x			x	x			X	x			x
Sigef	x			x	x			x	x			X	x			x
Olimpo	x			x	x			x	x			X	x			x
Regycont	x			x	x			x	x			X	x			x
HARDWARE																
Servidor de Correo													x			x
Servidor PDC_CONESUP													x			x
Servidor BDC_CONESUP													x			x
Router													x			x
Switchs													x			x
Servidor SEDNA													x			x
Servidor REGYCONT													x			x

Tabla 2.9 Actores - Problemas del sistema

Activo (bien)	Actores															
	Desastres naturales				Problemas con tercerizadoras				Problemas de telecomunicaciones				Problemas con proveedores			
	Consecuencias															
	D	M	P	I	D	M	P	I	D	M	P	I	D	M	P	I
INFORMACION																
Base de datos Académico			x			x	x		x			X				x
Base de datos Sigef			x			x	x		x			X				x
Base de datos Olimpo			x			x	x		x			X				x
Base de datos Regycont			x			x	x		x			X				x
SOFTWARE																
Sistema Académico			x		x			x	x			X				x
Sigef			x		x			x	x			X				x
Olimpo			x		x			x	x			X				x
Regycont			x		x			x	x			X				x
HARDWARE																
Servidor de Correo			x		x											x
Servidor PDC_CONESUP			x		x											x
Servidor BDC_CONESUP			x		x											x
Router			x		x											x
Switchs			x		x											x
Servidor SEDNA			x		x											x
Servidor REGYCONT			x		x											x

Tabla 2.10 Actores –Otros problemas

Análisis de las amenazas cuando el actor son los problemas del sistema y otros

Según las tablas 2.9 y 2.10 los principales problemas son las infecciones por virus o por troyanos, aunque la organización cuenta con un antivirus (AVG Edition Free), la mayoría de veces no ha sido lo suficiente para arreglar el equipo. Otro problema que ocasiona la pérdida de información es el daño de discos duros.
Los problemas con proveedores han sido mínimos sin embargo han retrasado el trabajo cuando los equipos nuevos ingresan con alguna falla.
Dentro de los contratos laborales no existe ninguna cláusula para que las personas tercerizadas, se responsabilicen del uso de la información.

FASE II

2.2.6 IDENTIFICACION DE COMPONENTES CLAVES

Luego de la creación de perfiles de amenazas se identifico a cada activo con un valor de importancia dependiendo del daño que causarían si se perdiera dicho activo. El valor de importancia varia de 1 a 5, donde: 1 es de menor importancia y 5 el de mayor importancia.

En la tabla 2.11 se indica el activo y su importancia

ACTIVO	IMPORTANCIA
Información	5
Hardware	4-3-2
Software	3-2

Tabla 2.11 Activo y el valor de su importancia

La Información tiene una importancia de 5 ya que en ella se encuentran las bases de datos, respaldos de las mismas, contraseñas de los usuarios.
El Hardware tiene una importancia de:

- 4 para Servidores
- 3 para Pcs
- 2 para Routers, Switches y Hubs.

El Software tiene una importancia de 3 para el Software de aplicación y programas fuentes, y un valor de 2 para Sistemas operativos e información de los usuarios.

2.2.7 EVALUACION DE VULNERABILIDADES EN LA RED

Actualmente la Institución cuenta con la topología estrella. En la figura 2.2 se ilustra la red actual del CONESUP.

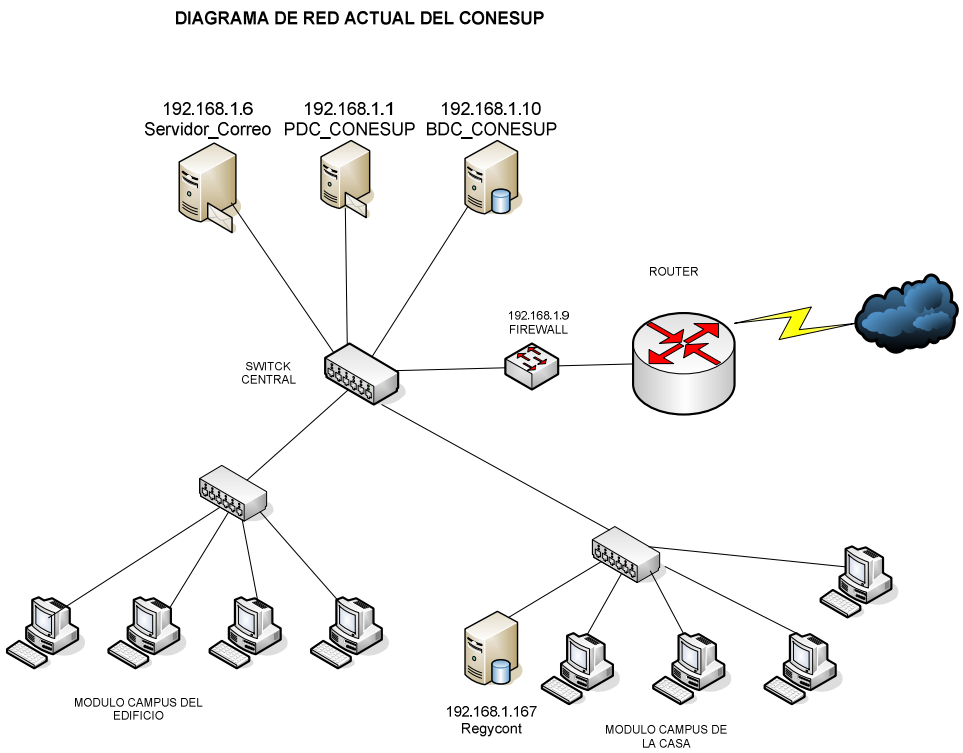

Fig. 2.2 Diagrama de Red actual del CONESUP

Para la evaluación de vulnerabilidades se utilizo tres herramientas distintas: NMAP, NESSUS y LANGUARD N.S.S 8.0, obtenidas del Internet gratuitamente, sin embargo la última herramienta es una versión de prueba por ser comercial.

Estas pruebas fueron realizadas desde una máquina de la misma red, a los servidores y equipos de la red:

A continuación en la tabla 2.11 se detalla la clasificación de las IPs para toda la red

	Rango de IPs	
Servidores	192.168.1.1	192.168.1.10
Pcs	192.168.1.11	192.168.1.119
VPN (no utilizadas)	192.168.1.220	192.168.1.250

Tabla 2.11 Rango de IPs

En la tabla 2.12, se describe a cada servidor con su IP, función y sistema operativo

NOMBRE	**IPs**	**FUNCION**	**SISTEMA OPERATIVO**
PDC_CONESUP	192.168.1.1	Servidor de Base de datos y Motor de Base de datos	WINDOWS NT 4.0
	192.168.1.4	Firewalls (Guayaquil)	LINUX
CORREO	192.168.1.6	DHCP, File Server, Printer Server	WINDOWS NT 4.0
NS1 - KYPUS	192.168.1.9	Firewalls (Software y Hardware), DNS y Correo	LINUX
BDC_CONESUP	192.168.1.10	Servidor Web (IIS), File Server	WINDOWS NT 4.0
RRUIZ	192.168.1.167	Regycont (Bdd y aplicación), Pc, Servidor de desarrollo de la pagina web del CONESUP	WINDOWS 2000

Tabla 2.12 Descripción de Servidores

La tabla 2.12 se muestra que mas de un servidor tiene las mismas funciones, es decir, existen dos servidores File Server así como de bases de datos. Según las entrevistas realizadas al departamento de sistemas estos casos se dieron por el crecimiento de la red y por colapsar los servidores que no tenían mucha capacidad.

NMAP

Esta herramienta permite conocer los puertos abiertos y protocolos disponibles de una determinada máquina, los siguientes gráficos son los resultados obtenidos en el rango de IPs de los servidores.

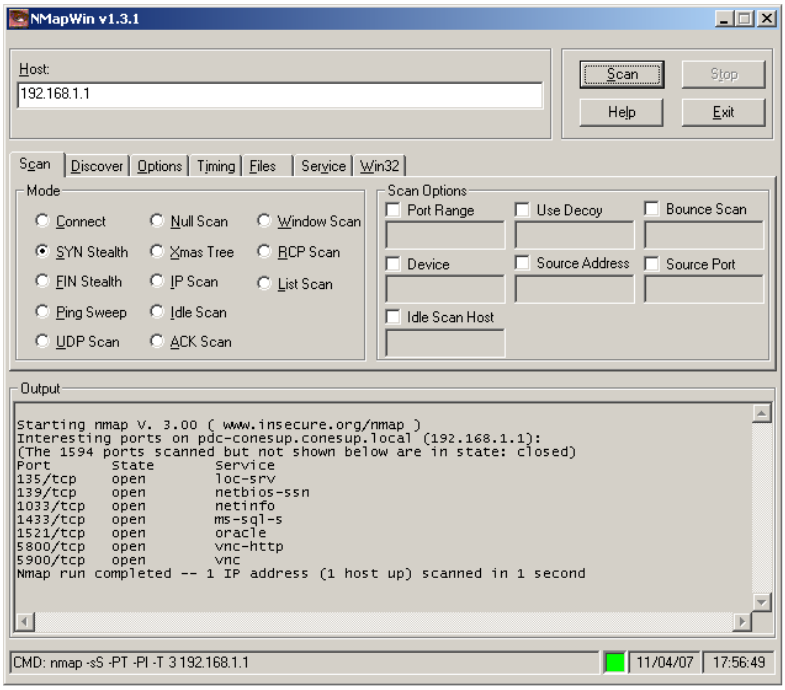

Fig. 2.3 Escaneo del Servidor 192.168.1.1 - PDC_CONESUP

En la figura 2.3 se muestra que el servidor de base de datos tiene abierto los puertos para el acceso remoto (vnc) y el puerto 135 que ha sido utilizado por hackers como agujero para entrar a los ordenadores, esto hace que sea el servidor vulnerable a ataques.

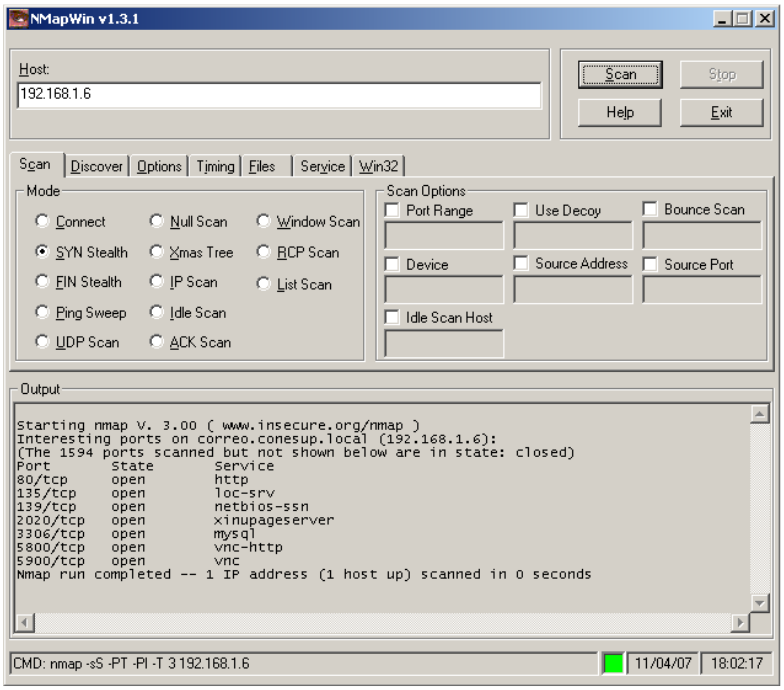

Fig. 2.4 Escaneo del servidor 192.168.1.6 - CORREO

En la figura 2.4 se observa que el servidor CORREO igual que el PDC_CONESUP tiene el puerto 135 abierto vulnerable a un ataque, además el puerto mysql , http, vnc abiertos que no cumplen con la función que tiene el servidor.

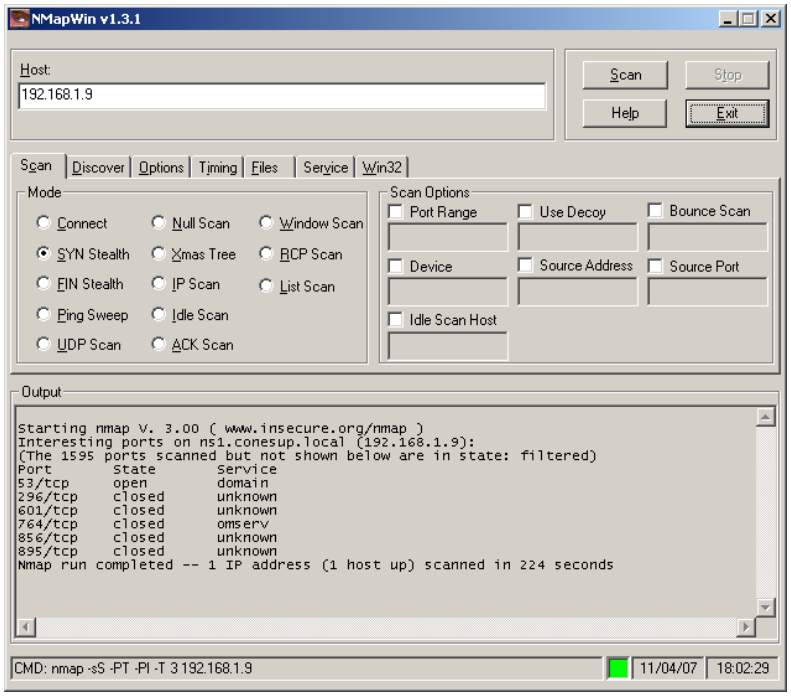

Fig. 2.5 Escaneo del servidor 192.168.1.9 – KYPUS

En la figura 2.5 se muestra el escaneo del servidor 192.168.1.9 donde se puede observar el puerto 53 abierto que le corresponde a la función que tiene el servidor de DNS, además es el firewalls y el servidor de correo.

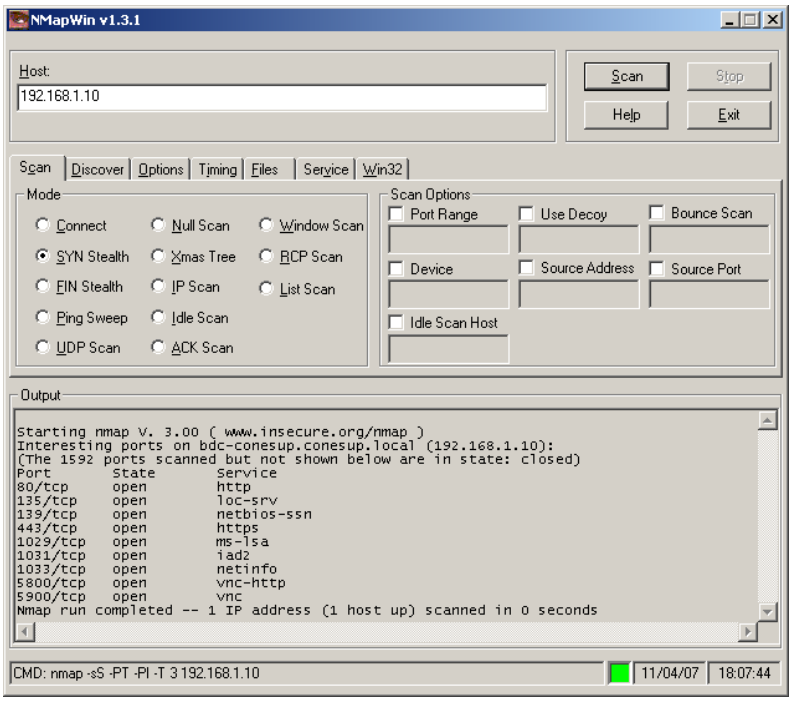

Fig. 2.6 Escaneo del servidor 192.168.1.10 – BDC_CONESUP

La figura 2.6 muestra el resultado del escaneo al servidor BDC_CONESUP, según las funciones que cumple este servidor es aceptable que los puertos 80 y 443 estén abiertos por el servidor Web, pero no el puerto 135 por lo que existe vulnerabilidad a través de este puerto.

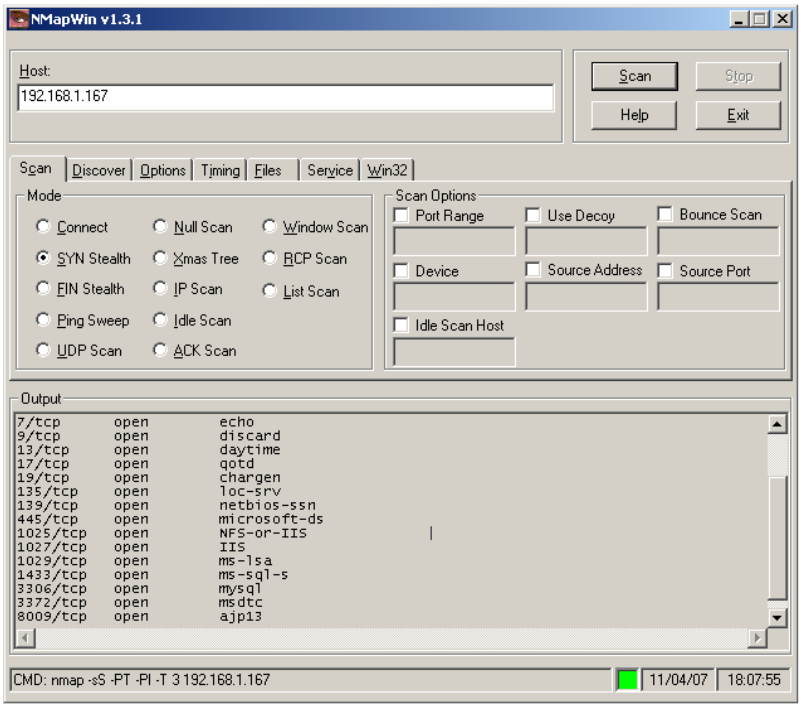

Fig. 2.7 Escaneo al PC 192.168.1.167

La figura 2.7 muestra el resultado del escaneo al PC 192.168.1.167 con la herramienta Nmap, este equipo tiene algunas funciona como: servidor Regycont, Servidor Web local del sitio Web del CONESUP, realiza conexiones remotas al web hosting ubicado en los Estados Unidos para realizar tareas programadas en dicho servidor y es utilizada como una estación de trabajo. Los puertos que debe tener abierto para cumplir con las funciones anteriormente mencionadas sería el de mysql, sql, http, ftp sin embargo el puerto 135 se encuentra abierto lo que hace vulnerable al equipo.

NESSUS

La herramientas NESSUS, muestra la información mas completa de los equipos como: Puertos abiertos, notas de seguridad, advertencias de seguridad, agujeros, sistemas operativos, parches instalados, el nivel de riesgo de la vulnerabilidad además de dar una solución a ese riesgo como por ejemplo la instalación de nuevos parches.

La tabla 2.13 permite conocer en el rango de los servidores sus vulnerabilidades

IPs	Puertos Abiertos	Notas de Seguridad	Advertencias de Seguridad	Agujeros
192.168.1.1	16	51	9	6
192.168.1.4	4	10	0	0
192.168.1.6	12	54	20	9
192.168.1.9	6	14	2	1
192.168.1.10	10	50	8	6
192.168.1.167	20	41	0	8

Tabla 2.13 Vulnerabilidades en los Servidores

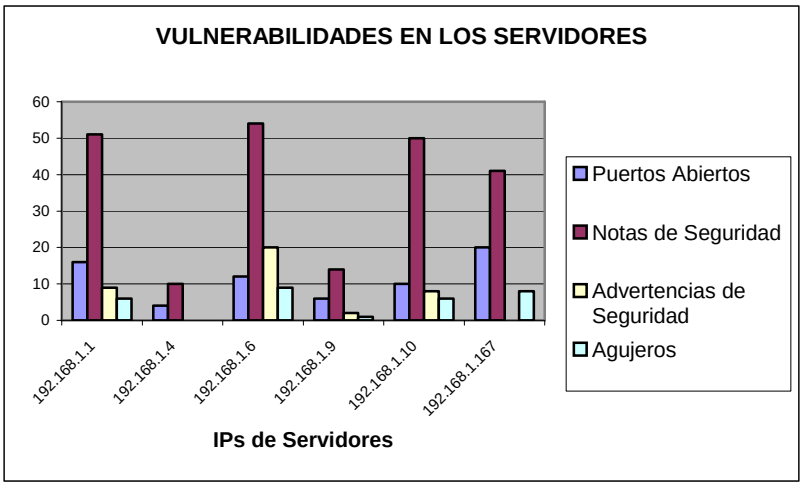

Fig. 2.8 Vulnerabilidades en los Servidores

En la figura 2.8 permite conocer el nivel de riesgo que tiene cada servidor tiene según las vulnerabilidades encontradas.

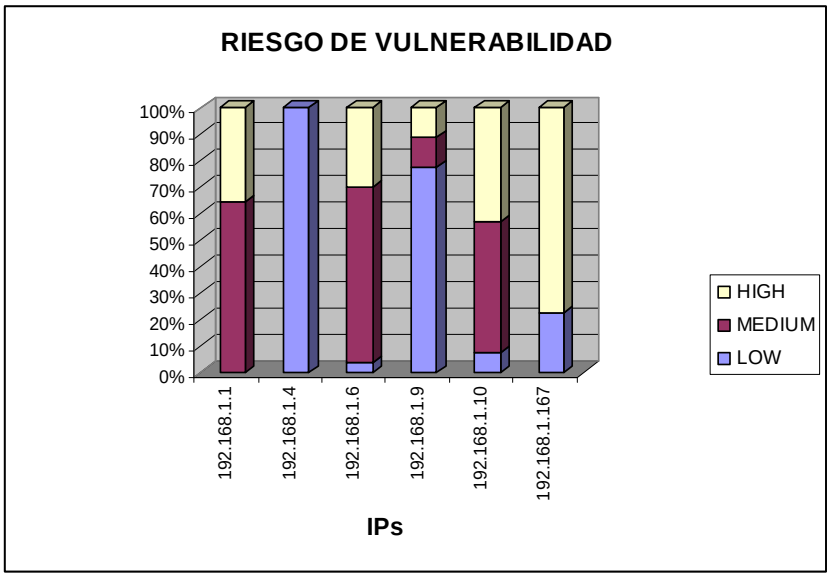

Fig. 2.9 Riesgo de las Vulnerabilidades en los Servidores

En la figura 2.9 muestra el porcentaje de vulnerabilidades encontradas en 79 equipos dentro de rango de IPs 192.168.1.11 a 192.168.1.250

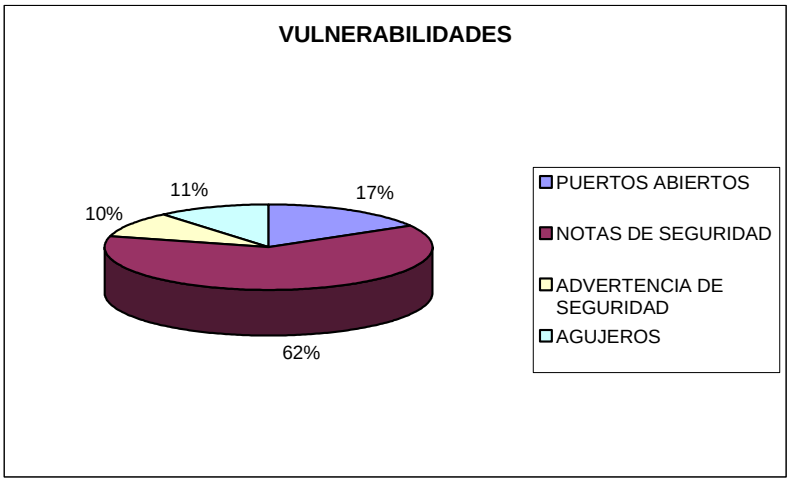

Fig. 2.10 Vulnerabilidades en PCs

En la figura 2.10 se ilustra las vulnerabilidades de la red tales como : los puertos abiertos, notas de seguridad, advertencia de seguridad y agujeros

LANGUARD N.S.S. 8.0

LANGUARD es una herramienta comercial, el software utilizado en esta evaluación es una versión prueba por esta razón tiene limitaciones en el escaneo de todos los equipos.

A continuación en las figuras 2.11 y 2.12 se presentan los resultados del escaneo de los servidores y las vulnerabilidades encontradas.

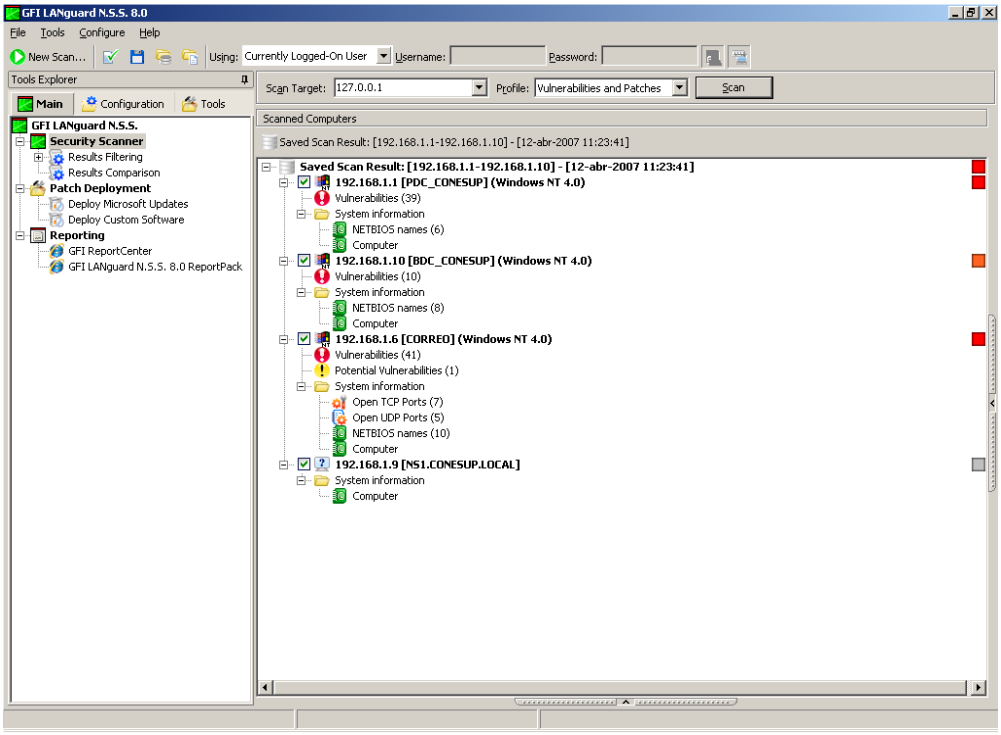

Fig 2.11 Vulnerabilidades en los Servidores

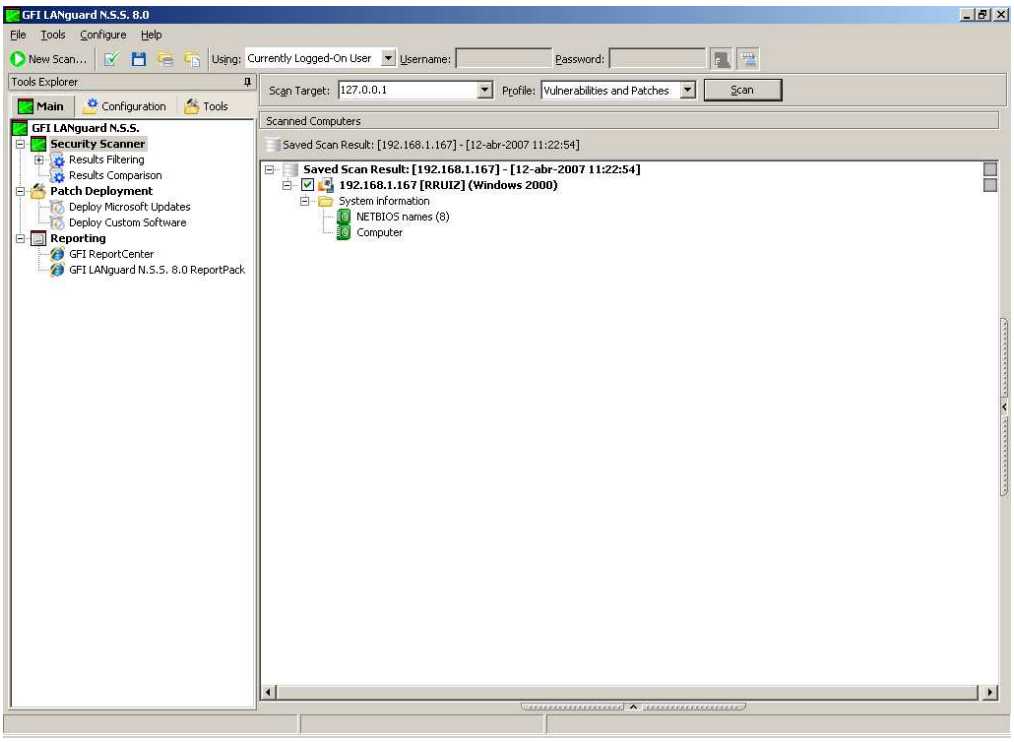

Fig 2.12 Vulnerabilidad en Servidores

En la figura 2.13 se muestra el resultado de 25 equipos que fue el máximo para escanear por ser una versión prueba.

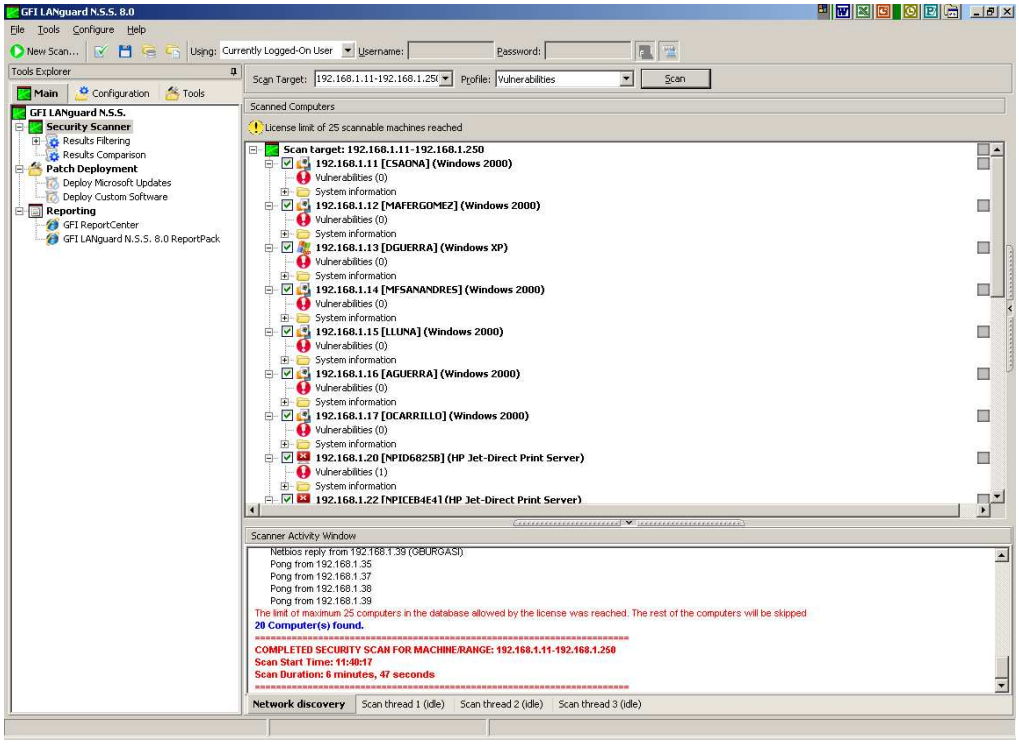

Fig. 2.13 Escaneo de 25 Pcs

FASE III

2.3 ANALISIS DE RESULTADOS

Según las evaluaciones realizadas de las vulnerabilidades encontradas en los servidores en el punto anterior se puede indicar que los servidores no solo tienen abierto los puertos que le corresponden dependiendo a su función sino que existen agujeros por donde pueden ser atacados, además por tener servidores de poca capacidad, se han improvisado en otros servidores las mismas funciones.

No existen manuales de procedimientos ni políticas de seguridad que guíen al usuario en el manejo de aplicaciones, manejo de la información, esto ha ocasionado la perdida de información tanto en forma accidental así como deliberada lo que ha generado retraso en el trabajo. Además no se cuenta con un plan de mantenimiento para equipos, en donde se tenga presente la actualización de aplicaciones y sistemas operativos, y la revisión del hardware para prevenir posibles daños en el mismo de forma periódica.

No existe un adecuado control para el acceso físico a los departamentos, esto ocasiona que el trabajo sea interrumpido para atender consultas de personas externas a la Institución.

En la actualidad las oficinas del CONESUP ubicadas en las diferentes ciudades del país (Guayaquil, Loja, Cuenca, Riobamba y Manabí) dependen de la disponibilidad de la red en la que están conectadas; por ejemplo, la oficina de Guayaquil está ubicada dentro de la Universidad de Guayaquil y depende de la disponibilidad de la red de la Universidad para conectarse al servidor ubicado en Quito. Además cuando existen problemas en los servidores de Quito la atención de las oficinas remotas se ve interrumpida.

2.4 DETERMINACION DE REQUERIMIENTOS

Adquisición y organización de Servidores en una sola área

Descripción: Debido al incremento de usuarios en la red y por la seguridad de la misma, se deben adquirir servidores que soporten los servicios actuales; cada servidor cumplirá con máximo dos funciones para que no colapse, todos los servidores deberán estar ubicados en una sola área con sus respectivas seguridades
Prioridad= Alta

Desarrollar políticas para el acceso físico a los departamentos de la Institución

Descripción: Para evitar que el trabajo sea interrumpido por personas no autorizadas especialmente en áreas de procesamiento de datos se deben implementar políticas para el ingreso a estas áreas.
Prioridad= Alta

Desarrollar políticas de seguridad de acceso físico a los equipos

Descripción: Debido a la falta de políticas para el acceso físico a los equipos se han originado problemas tales como pérdida de información y pérdida o daño de dispositivos de hardware
Prioridad= Alta

Manual de políticas y procedimientos para el acceso y manejo de la información

Descripción: Se debe realizar un manual de políticas y procedimientos para el manejo de la información, donde se responsabilice al usuario del uso de ella así como de su almacenamiento seguro.
Prioridad: Alta

Desarrollar políticas para respaldos de la información

Descripción: Es necesario contar con políticas que aseguren los respaldos o backup de la información sensitiva y que asegure la pronta recuperación de información si es necesario .
Prioridad: Media

Desarrollar un Plan de Contingencia

Descripción: Se debe contar con un plan de contingencia con el fin de asegurar la recuperación de los sistemas de información ante un desastre natural o actos mal intencionados, además para reducir la probabilidad de pérdidas en un nivel mínimo aceptable.
Prioridad: Media

Plan para el Mantenimiento preventivo de Equipos

Descripción: Se debe contar con un plan para el mantenimiento de equipos para prevenir posibles daños de fuentes de poder, daños de discos duros, o la infección de virus, además, contar con los sistemas operativos y aplicaciones actualizadas
Prioridad: Baja

Capacitación de usuarios

Descripción: Planificar una capacitación a los usuarios para el uso de las aplicaciones existentes así como de las herramientas actualizadas para que puedan desempeñar mejor su trabajo.
Prioridad: Baja

Documentación de los Sistemas de Información y de procedimientos para el manejo de la información

Descripción: Se requiere que cada aplicación desarrollada en el Dpto. de Sistemas tenga su respectiva documentación es decir, manual de usuario, manual de instalación y manual de programación. Además se requiere que cada procedimiento para el manejo de información en las áreas de procesamiento de datos sea documentado completa y adecuadamente.
Prioridad: Media

Desarrollar un diseño de seguridad para la Intranet que minimice el riesgo de un ataque

Descripción: Se requiere diseñar un esquema de seguridad para la Intranet para mejorar su rendimiento y minimizar el riesgo de un ataque
Prioridad: Alta

Capítulo 3 DISEÑO DEL ESQUEMA DE SEGURIDAD

3.1 DISEÑO DE LA SEGURIDAD FISICA

Para realizar el diseño de seguridad tanto Física como Lógica y para el manual de políticas y procedimientos se siguieron los lineamientos de la norma ISO 17799.

Los objetivos de la seguridad física:

- Proteger los activos del T.I. del CONESUP de los riesgos de desastres naturales y/o actos accidentales o mal intencionados.
- Minimizar la pérdida de información y garantizar la recuperación de la misma.
- Asegurar que las condiciones ambientales sean las más favorables para el buen funcionamiento de los equipos.

3.1.1 AREAS SEGURAS

Objetivo Principal: Proteger físicamente contra el acceso no autorizado o daño a la información de los sistemas a todos los departamentos del CONESUP especialmente donde se procesan datos sensibles.

3.1.1.1 Perímetro Físico

El área de los servidores debe ser cerrada desde el piso real hasta el techo real contando con una ventilación adecuada y sus respectivas instalaciones eléctricas, donde el acceso solo será para las personas autorizadas tales como administradores de las aplicaciones, bases de datos y red

El departamento de Sistemas junto con el departamento Administrativo deberán crear normas a seguir para acceder y modificar al hardware. Cada empleado será responsable de sus computadores personales y no se permitirá que personas no

autorizadas a los sistemas de información tengan acceso a los computadores sin autorización. Cualquier modificación del hardware será registrado por la persona encargada de los activos fijos previo a la comprobación de fallo o problemas de funcionamiento con el hardware por parte del departamento de Sistemas.

El acceso a los diferentes departamentos deberá ser controlado en primera instancia por la guardia de seguridad y segundo por la secretaria de cada departamento en horas laborables; en horas no laborables no ingresará ninguna persona no autorizada a los departamentos.

3.1.1.2 Controles de acceso físico

El área de información debe estar ubicada al ingreso del edificio y de la casa, de tal manera que todos los usuarios que requieran información para algún trámite la obtenga en esta área y así evitar que pasen a otro departamento si no es necesario.

Toda persona externa que ingrese a la institución por motivos específicos y/o autorizados deberá registrar su información en un documento: nombre, hora de ingreso, departamento al que se dirige y además el guardia deberá retener algún documento de identidad.

La información sensible como: respaldos de datos y códigos fuentes de los sistemas de información desarrollado en el CONESUP será almacenada en un lugar de condiciones ambientales adecuadas, lejos de canalizaciones de agua y energía, se utilizaran archivadores ignífugos y su acceso solo será permitido por las personas autorizadas en este caso al departamento de sistemas y alguna autoridad de la Institución.

3.1.1.3 Protección de oficinas

Cada departamento deberá contar con un acceso principal con cerradura, el responsable del cuidado del edificio cerrará cada acceso principal con llave luego de que todo el personal del área se haya retirado, además deberá revisar las ventanas que se encuentren también cerradas.

Se debe instalar un sistema de detección de intrusos en todas las puertas y ventanas accesibles y que será activado después de cerrar los departamentos.

Las áreas donde se procesan datos tales como Registro de Títulos y el departamento de Sistemas, no deben ser accesibles al público todo el tiempo; deberá definirse un horario para la atención al cliente en el caso de Registro de Títulos; el ingreso de llamadas telefónicas también deberá restringirse a un determinado horario.

El área donde se almacena la información sensible, deberá estar ubicado en un lugar que no este expuesto al acceso público.

Cada departamento debe tener un extintor de CO2 o espuma para que el personal pueda sofocar cualquier pequeño incendio si existiere.

Debido a que el hardware de cada usuario esta desprotegido por estar en los puestos de trabajo, el departamento de Sistemas deberá organizar a los sistemas para que los usuarios finales puedan acceder a su información a través de la red local y trabajar directamente en los servidores de ficheros y servidores de aplicaciones y así mantener a los datos importantes de la Institución a salvo de errores o manipulaciones del hardware.

3.1.1.4 Aislamiento de las áreas de entrega y carga

La bodega del CONESUP donde se encuentra toda clase de suministros de oficina debe contar con un listado de personas o proveedores autorizados para el acceso a la misma.

La bodega del CONESUP debe contar con un acceso exterior a la institución para que en la entrega de los suministros el personal externo no acceda a otros departamentos para dicha entrega.

3.1.2 SEGURIDAD DE LOS EQUIPOS

Objetivo Principal: Proteger físicamente a los equipos para reducir toda clase de daño, pérdida o acceso no autorizado a los datos y que ocasionen la interrupción a las actividades de la Institución

3.1.2.1 Ubicación y protección de los equipos

En cada departamento los equipos deberán ser ubicados en lugares que no afecten al mismo, por ejemplo no cerca de ventanas donde puedan ser afectados por la lluvia, polvo o por robo.

El CONESUP pondrá políticas sobre comer, beber o fumar cerca de las instalaciones de los equipos especialmente en el área de procesamiento de información.

Se deberá realizar por los menos dos veces al año un monitoreo de las condiciones ambientales en los departamentos especialmente en los de procesamiento de datos para prevenir cualquier problema en los equipos.

3.1.2.2 Suministros de Energía

El área de los servidores debe contar con un UPS para asegurar el trabajo continuo hasta que el generador de energía sea activado.

El edificio y la casa del CONESUP contará con una puesta a tierra para proteger de rayos a los equipos.

El edificio y la casa del CONESUP contaran con un suministro de energía para cada uno, así mismo la caja donde se encuentran los interruptores de energía deben ser colocados en lugares fuera del alcance de personas externas para que no se ocasionen alguna interrupción de energía al edificio y a la casa

3.1.2.3 Seguridad del Cableado

El cableado de red debe estar protegido por conductos como canaletas y ubicados en lugares que no obstruyan el paso a las personas para evitar daños al cable y que se vean interrumpidos los servicios de red.

Las instalaciones de cableado eléctrico deberá ser independiente del cableado de red para evitar interferencias.

3.1.2.4 Mantenimiento de Equipos

El departamento de Sistemas del CONESUP, debe contar con un plan de mantenimiento preventivo de equipos que será calendarizado por departamentos, para evitar que el trabajo se vea interrumpido por falla de algún hardware del equipo y que exista pérdida de información.
El departamento de Sistemas del CONESUP, llevara una bitácora de daños mas frecuentes en los equipos para estar prevenidos de futuros problemas con los mismos.

El departamento de sistemas deberá contar con un sistema de backups distribuidos para asegurar la información sensitiva de los usuarios finales replicando los backups entre el edificio y la casa, es decir, replicar los datos del servidor principal de archivos a otro secundario y éste deberá contar con las seguridades respectivas para los servidores.

3.1.2.5 Seguridad de los equipos fuera de la Institución

Los equipos que se encuentran ubicados en las oficinas del CONESUP en las distintas ciudades del país (Guayaquil, Cuenca, Loja, Manabí y Riobamba) tendrán un responsable si algo pasará con ellos.

El CONESUP debe contar con una cobertura de seguros para los equipos portátiles dentro y fuera de la institución. En el caso de viaje el equipo será llevado como equipaje de mano.

3.1.2.6 Baja o reutilización de equipos

Los equipos que serán sustituidos por otros deberán ser formateados y configurados nuevamente para el nuevo usuario después de sacar los respaldos respectivos, con el fin de que no exista información del antiguo dueño.

3.2 DISEÑO DE LA SEGURIDAD LOGICA

Los objetivos de la Seguridad lógica son:

- Definir y controlar los permisos y accesos a los programas y archivos
- Asegurar que los datos sean utilizados por el proceso adecuado y con los procedimientos correctos
- Asegurar que los datos y programas que no correspondan a un departamento sean modificados por los usuarios de dicho departamento
- Asegurar que la información trasmitida sea recibida por el destinatario al cual fue enviada.

- Asegurar que la información recibida sea la misma que fue transmitida

3.2.1 DISEÑO DE LA RED

Para el diseño de la seguridad de la red se consideró la arquitectura de seguridad de SAFE de CISCO y se centra en las amenazas que pueden surgir y en los medios para combatirlas.

3.2.1.1 Metodología SAFE

La metodología SAFE trabaja en módulos y tiene dos ventajas fundamentales: la primera es relacionar la seguridad entre los bloques funcionales de la red y además permite realizar una evaluación e implementación de la seguridad módulo a módulo.

Como se trata de una empresa pequeña se tomó como guía a Safe para pequeñas empresas. Dentro de este diseño sólo existen dos módulos: Módulo de Internet y Módulo de Campo.

Acontinuación, en la figura 3.1 se ilustra el modelo SAFE para pequeñas empresas

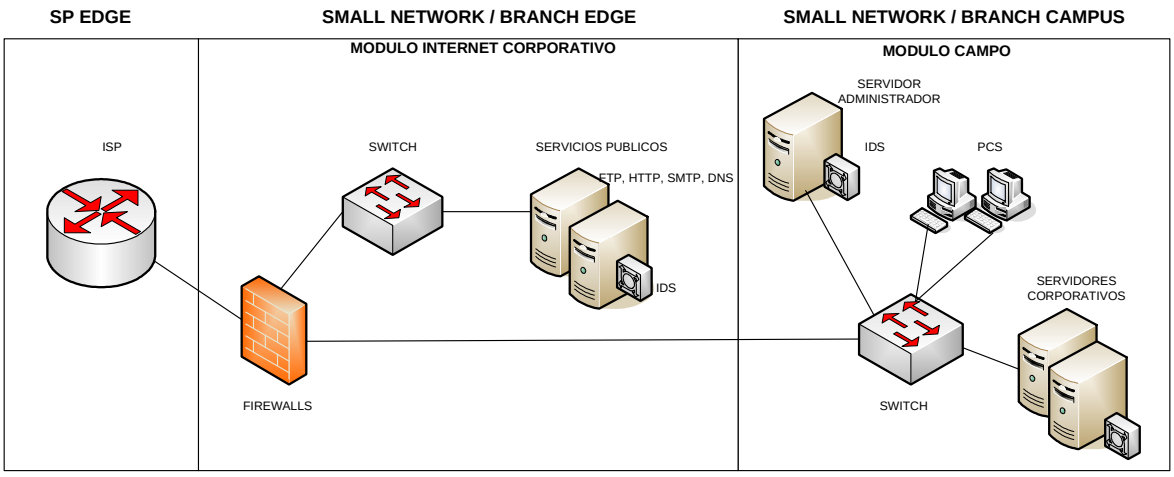

Fig. 3.1 Diseño de seguridad de Safe para pequeñas empresas

3.2.1.1.1 Módulo Internet

Este módulo proporciona a los usuarios internos los servicios de Internet, así mismo a los usuarios externos acceso a los servicios públicos de la DMZ, sin embargo no existe el servicio de comercio electrónico.
Dentro de los componentes principales estan:

- Servidor SMTP
- Servidor DNS
- Servidor FTP/HTTP
- Dispositivos IDS/IPS
- Firewalls / Firewalls router
- Switch L2

Dentro de las amenazas que combate están:

- Acceso no autorizado
- Ataques a la capa de aplicación
- Virus y Trojanos
- Ataques de contraseñas
- Denegación de servicios
- Ataques de falsificación
- Rastreadores de paquetes
- Reconocimiento de la red
- Abuso de confianza
- Redireccionamiento de puertos.

3.2.1.1.2 Módulo Campo

Este módulo está formada por las estaciones de trabajo, servidores internos, servidor de administración y se puede combinar switch simples con switchs de capa 2
Dentro de los dispositivos principales estan:

- Switch L2
- Servidores corporativos
- Estaciones de Trabajo
- Host administrador

Dentro de las amenazas que combate estan:

- Rastreadores de paquetes
- Virus
- Acceso no autorizado
- Ataques a la capa de aplicación
- Abuso de confianza
- Redireccionamiento de puertos

Directrices del Diseño

Las principales funciones del switch de campo son conmutar el trafico de producción y administración, proporcionar conectividad a los servidores corporativos y de administración así como a los usuarios, además del IDS que permitirá conocer si alguien no autorizado esta tratando de ingresar a la red.

3.2.1.2 Diseño de la red del CONESUP

La figura 3.2 muestra el Diseño de las seguridades lógicas de la red CONESUP basada en la arquitectura de SAFE de CISCO

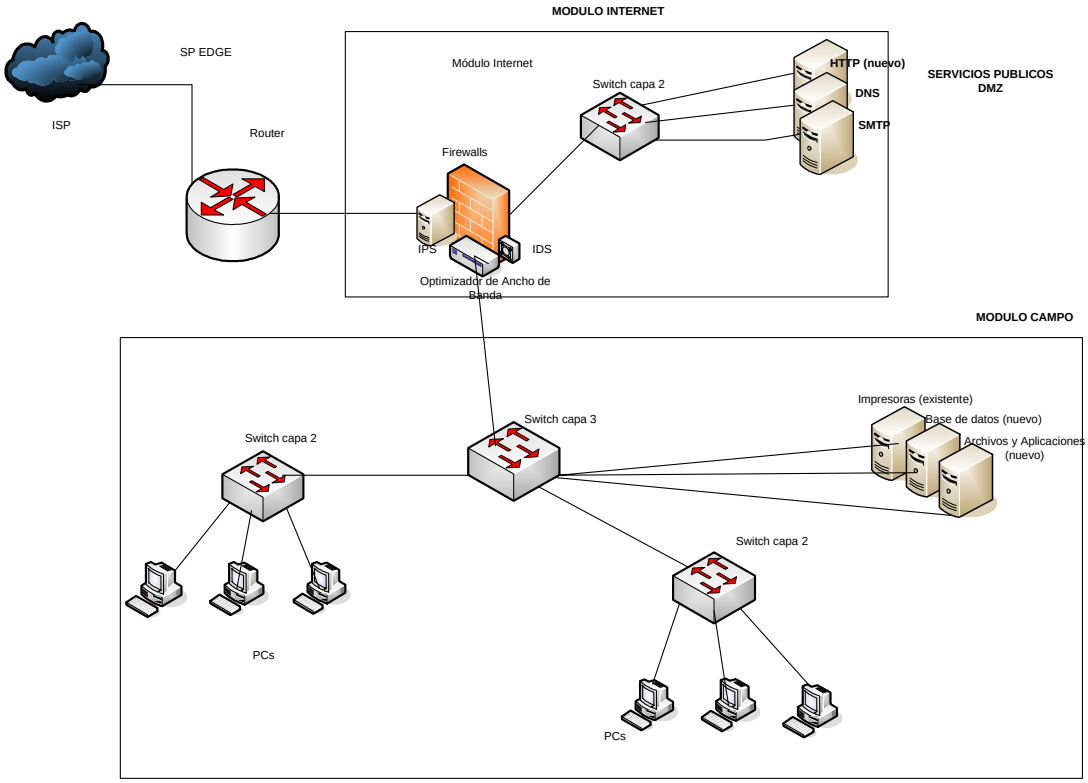

Fig. 3.2 Diseño de seguridad de la Red del CONESUP

3.2.1.2.1 Modulo Internet

Dentro del Módulo de Internet se necesitarán los siguientes dispositivos:

- Router[1]
- Firewalls[1]
- IDS[2]
- IPS[2]
- Optimizador de Ancho de banda[2]
- Servidor HTTP[1]
- Servidor SMTP[1]
- Servidor DNS[1]
- Servidor FTP[1]
- Switch capa 2[1]

[1] Ver características en el Anexo III
[2] Viene incluido en el Firewall

3.2.1.2.2 Modulo Campo

Dentro del Módulo de Campo se necesitarán los siguientes dispositivos:

- Servidor de base de datos[1]
- Servidor de Aplicaciones y Archivos[1]
- Servidor de Impresoras (Se configurará en un clon ya existente)
- 2 Switch capa 2[1]
- Switch capa 3[1]
- PCs[3]

A continuación en la tabla 3.1 se describe las funciones para los nuevos equipos del diseño propuesto.

EQUIPO	FUNCION
Servidor de Base de Datos (nuevo)	Cuenta con 4 discos, predominara la bdd de Sql Server y como secundaria Oracle
Servidor de Aplicaciones y Archivos (nuevo)	Cuenta con 4 discos. Aplicaciones: Regycont, Sigef, Olimpo Archivos: Usuarios
Servidor http	Sistema Académico
Servidor de Impresoras	Uno existente solo para ese servicio

Tabla 3.1 Servidores con la función que desempeñan

Nota: El servidor Sedna, se reemplazará con el firewalls que cuenta con un IPS e IDS y optimizador de ancho de banda.

[1] Ver características en el Anexo III
[3] No se compraran PCs, se utilizaran las existentes

3.2.2 CONTROL DE ACCESO LOGICO

3.2.2.1 Requerimientos para el control de acceso

Objetivo Principal: Controla el acceso a la información mediante requerimientos de seguridad, además de políticas de autorización y difusión de la información

3.2.2.1.1 Políticas de Control de accesos

El Conesup deberá definir y documentar políticas de acceso para cada sistema de información dependiendo de los requerimientos de seguridad para el acceso.

Las políticas de acceso deberán estar relacionadas con la clasificación de información para cada departamento

El departamento de Sistemas deberá ubicar a cada usuario bajo un perfil dependiendo de la categoría del puesto de trabajo.

El departamento de Sistemas documentará dentro de las políticas de acceso que esta permitido y que no, que debe imponerse y que reglas serán optativas o condicionales, como por ejemplo, páginas web y servicios de red.

3.2.2.2 Administración de accesos de usuarios

Objetivo Principal: Impedir el acceso no autorizado a los sistemas de información implementando procedimientos de asignación para el acceso a estos sistemas. Dentro de estos procedimientos se deberá tomar en cuenta desde el inicio de un nuevo usuario hasta la finalización del mismo cuando ya no requiera acceso a los sistemas de información.

3.2.2.2.1 Registro de Usuarios

El departamento de Sistemas creará para cada usuario un identificador personal para el acceso de cada sistema, esto permitirá que cada usuario sea responsable por sus acciones.

El departamento de Sistemas verificará que el usuario tenga permisos para el uso del sistema de información, además debe contar con la autorización del Director del departamento para el acceso del sistema al usuario requerido.

Para el soporte técnico de los sistemas desarrollados por terceros, el departamento de sistemas les permitirá el acceso al sistema de información luego de haber sido autorizado el ingreso para dicho soporte por el departamento Administrativo.

El departamento Administrativo deberá notificar al departamento de Sistemas cuando un usuario es cambiado a otra área y de funciones o si el usuario ya no trabajará en la Institución. El departamento de Sistemas deberá cancelar los permisos de acceso a los sistemas de información que no le competen inmediatamente a la notificación. Se revisará periódicamente las cuentas de usuarios para revisar si ya no están en servicio y no se utilizará cuentas de usuarios ya existentes para asignarlos a nuevos usuarios.

El departamento de Sistemas deberá asignar los privilegios mínimos a cada usuario dependiendo de la necesidad de uso de los sistemas

3.2.2.2.2 Administración de contraseñas

Se responsabilizará a cada usuario por mantener su password o contraseña en secreto.

El departamento de Sistemas proporcionará al usuario nuevo o al usuario que olvidó su clave, una contraseña provisional. Esta contraseña provisional será

dada personalmente al usuario, sin hacer uso de correos electrónicos o de terceras personas.

3.2.2.2.3 Revisión de derechos de acceso de usuario

El departamento de Sistemas deberá realizar una revisión a los derechos de acceso de los usuarios por lo menos cada 6 meses y después de que algún usuario se haya cambiado a otro departamento y de funciones, para que no existan privilegios concedidos sin la respectiva autorización.

3.2.2.3 Responsabilidades del usuario

Objetivo Principal: Concientizar a los usuarios su responsabilidad para el acceso a los sistemas de información, entre ellas el uso de las contraseñas y la seguridad de los equipos que están bajo su cargo.

3.2.2.3.1 Uso de Contraseñas

El empleado deberá mantener su contraseña en secreto, no registrarla en papeles a la vista de otros usuarios o compartirlas a los compañeros, en tal caso se las deberá almacenar en lugares seguros.

El empleado deberá cambiar su contraseña cada 3 meses para mayor seguridad y si hubiere sido revelada se notificará al departamento de sistemas inmediatamente para realizar el cambio.

La contraseña tendrá un mínimo de 6 caracteres, no se utilizará palabras relacionadas con nombres, fechas de nacimiento, cédulas de identidad, números telefónicos, además todos los caracteres no podrán ser totalmente numéricos o totalmente alfabéticos, sin embargo serán fáciles de recordar.

La contraseña provisional será cambiada al iniciar por primera vez una sesión en la red.

3.2.2.3.2 Equipos desatendidos en áreas de usuarios

Los usuarios deberán garantizar la protección de sus equipos cuando se encuentren desatendidos por medio de un protector de pantalla con clave o el cierre de su sesión.

3.2.2.4 Control de acceso a la red

Objetivo Principal: Garantizar la seguridad de los servicios de red tanto interna como externa, evitando interfaces inadecuadas entre la Institución y otras organizaciones, protegiendo la red y los servicios de red con mecanismos de autenticación y con controles de acceso a los usuarios para el uso de los servicios de información.

3.2.2.4.1 Políticas para utilizar los servicios de red

El departamento de sistemas deberá crear políticas y procedimientos para el acceso de los usuarios a los servicios de red dependiendo del perfil de cada usuario.

3.2.2.4.2 Enrutamiento Forzado

El departamento de Sistemas deberá aplicar reglas para evitar que los usuarios escojan rutas fuera de la trazada entre su computador personal y los servicios de red a los que tienen acceso tales como conexiones automáticas de los puertos al firewall , imponer el uso del firewall a todos los usuarios externos a la Institución que necesiten tener acceso a nuestra red, además controlar las comunicaciones autorizadas internas a externas o viceversa mediante firewalls.

3.2.2.4.3 Autenticación de usuarios para conexiones externas

El departamento de sistemas deberá usar una técnica de autenticación a los usuarios externos, en este caso a los técnicos de las oficinas ubicadas en algunas ciudades del país y que se encuentran dentro de una red que esta afuera del control de la seguridad de la Institución, que acceden al Sistema Académico y de Registro de títulos.

3.2.2.4.4 Control de conexión a la red

El departamento de Sistemas deberá implementar políticas de acceso para limitar las conexiones de los usuarios a las aplicaciones que están dentro y fuera de la Institución a través de un firewall, por ejemplo, el correo electrónico y transferencia de archivos en ambas direcciones.

3.2.2.5 Control de acceso al Sistema Operativo

Objetivo Principal: Controlar el acceso no autorizado a los computadores y a los recursos de los mismos utilizando una identificación del usuario, un registro de los accesos exitosos y fallidos y restringir el tiempo de conexión de los usuarios

3.2.2.5.1 Procedimientos de conexión de PCs

El departamento de sistemas implementará procedimientos para la conexión a los computadores personales con el fin de minimizar las oportunidades de ingresos no autorizados a ellos.

3.2.2.5.2 Identificación y Autenticación de los usuarios

Cada usuario contará con un identificador único que constará de un usuario y password

3.2.2.5.3 Sistema de administración de contraseñas

El departamento de sistemas deberá controlar que exista una buena administración de contraseñas y que estas a su vez sean mantenidas y seleccionadas por los usuarios. Dentro de esta administración se debe:
Imponer que cada usuario cambio en determinada fecha su contraseña
Mantener un registro de contraseñas de por lo menos 12 meses anteriores para que no se repitan las contraseñas seleccionada por los usuarios.
Ocultar la contraseña en pantalla cuando es ingresada
Modificar la contraseña de algún software adquirido luego de su instalación.

3.2.2.5.4 Limitación del horario de conexión

Cada perfil de usuario contará con un determinado horario de conexión para el acceso a los servicios de información y de red dentro de las horas laborables.

3.2.2.6 Control de acceso a las aplicaciones

Objetivo Principal: Evitar el acceso no autorizado de la información contenida en los sistemas de información. El acceso a los sistemas de aplicación deben ser bajo las políticas de acceso a los usuarios dependiendo del perfil de cada uno además no deberán comprometer a otros sistemas con los que comparten recursos de información.

3.2.2.6.1 Restricción del acceso a la información

El usuario final no deberá conocer las funciones o la información de los sistemas de aplicación a las que no este autorizado el acceso.

El departamento de sistemas registrará y controlará los derechos de los usuarios a la información por ejemplo, de lectura, de escritura, de ejecución y control total.

Toda información mostrada en pantalla como reporte será solo la información que el usuario este autorizado a acceder y así mismo se envíe dicha información a las personas autorizadas.

3.2.2.7 Monitoreo del acceso y uso de los sistemas

Objetivo Principal: Detectar actividades no autorizadas, además permitirá medir la eficacia de los controles adoptados con las políticas de acceso.

3.2.2.7.1 Registro de eventos

Se deberá llevar y almacenar por un período determinado un registro de auditoría que contará con su respectiva seguridad y que deba contener la identificación del usuario, fecha y hora de inicio y terminación, registro de intentos exitosos y fallidos del acceso al sistemas y a los datos para posibles investigación de algún fraude, para esto todos los computadores tendrán una configuración sincronizada de relojes.

3.2.2.7.2 Monitoreo del uso de los sistemas

El departamento de sistemas deberá monitorear el uso de los sistemas de información con el fin de controlar que solo los usuarios que tengan autorización a ella sean los que estén utilizándolas.

3.2.2.8 Computadores móviles y trabajo remoto

Objetivo Principal: Garantizar la seguridad de la información cuando se utilice computadores móviles o instalaciones de trabajos remotos.

3.2.2.8.1 Computadores móviles

El departamento de sistemas implementará políticas para el manejo de computadores móviles o portátiles donde deberá incluir protección física, controles de acceso y protección contra virus.

3.2.2.8.2 Trabajo remoto

El departamento de sistemas deberá desarrollas políticas e implementar la protección para el acceso al trabajo remoto de usuarios que deban trabajar fuera de la Institución, además este trabajo deberá ser autorizado y controlado.

3.3 MANUAL DE POLITICAS Y PROCEDIMIENTOS

3.3.1 POLITICAS

3.3.1.1 Políticas de seguridad del hardware

3.3.1.1.1 Adquisición e instalación de equipos

La adquisición de nuevos equipos será revisada y analizada por el departamento de Sistemas para justificar el pedido.

La instalación de los equipos será realizada por el departamento de sistemas siguiendo los procedimientos para la configuración e instalación de los programas permitidos en la empresa y en conocimiento del departamento de Activos fijos para asignar a un responsable del activo.

Todo cambio de hardware nuevo en los computadores personales se realizará únicamente por fallo del mismo y solo el departamento de sistemas autorizará la compra previo a una revisión del problema de mal funcionamiento además será

registrado en un documento, esta política también será aplicada para las oficinas externas del Conesup.

3.3.1.1.2 Seguridad física del equipo

El usuario responsable del equipo deberá notificar al departamento de sistemas y al departamento de activo fijo si el equipo será asignado a otra persona, ubicado en otra área o parte de el será reemplazado por un hardware nuevo.

En los contratos a tercerizados deberá existir una cláusula donde exista un procedimiento de protección de activos (hardware), además un procedimiento si el activo ha sido afectado ya sea por pérdida o modificación.

Todo equipo que sale de la institución debe contar con la respectiva autorización del jefe del departamento y llenar un formulario donde indique el tiempo que estará afuera de la institución, motivo y responsable del equipo, además notificar al departamento de sistemas si el equipo es un computador para proceder a las seguridades del equipo ya establecidas.

Las portátiles deberán estar aseguradas por alguna empresa externa.

Todo equipo que sale de la institución debe contar con la respectiva autorización del jefe del departamento y llenar un formulario donde indique el tiempo que estará afuera de la institución, motivo y responsable del equipo, además notificar al departamento de sistemas si el equipo es un computador para proceder a las seguridades del equipo ya establecidas.

3.3.1.1.3 Mantenimiento de equipos

El departamento de sistemas estará a cargo del mantenimiento preventivo de los servidores y computadoras personales además será realizado cada seis meses previo a una calendarización y deberá ser registrado en una bitácora.

Cualquier problema de falla del equipo deberá reportarse inmediatamente al departamento de sistemas porque podría ocasionar pérdida de la información o interrupción de los servicios.

El departamento de sistemas estará a cargo del mantenimiento correctivo de los equipos y de la red supervisado por el Jefe de Sistemas.

El personal que realice pasantías en el departamento de Sistemas estará bajo la supervisión del jefe del departamento para realizar algún tipo de mantenimiento de equipos.

El departamento de sistemas se responsabilizará de mantener la adecuada instalación de la infraestructura de red.

3.3.1.2 Políticas de seguridad del software

3.3.1.2.1 Adquisición, instalación y actualización

El departamento de sistemas será quien instale software adicional a los equipos si es necesario para el usuario.

El departamento de sistemas será el encargado de la actualización de software y de los parches de seguridad periódicamente.

Todo software que se necesite comprar para el departamento de sistemas tendrá su previa justificación y aprobación de las autoridades para su adquisición.

Todo software adquirido será registrado en el departamento de activo fijo

3.3.1.3 Políticas de seguridad para el control de acceso a los sistemas de información

3.3.1.3.1 Acceso Físico

Los equipos deberán estar ubicados bajo condiciones que ofrezcan seguridad física, eléctricas y además que permitan el acceso físico sin ninguna restricción al personal del departamento de sistemas

El departamento de sistemas será quien tenga acceso al cuarto de servidores sin ninguna restricción y en caso urgente pueden acceder las autoridades de la empresa.

3.3.1.3.2 Acceso a la información (archivos y documentos)

Las portátiles serán protegidas por software de control de acceso, antivirus y firewalls para evitar que cuando salgan de la institución no regresen con problemas de mal manejo y borren programas, virus o software no deseado.

El departamento de sistemas no será responsable de la información personal de los usuarios que se encuentre en los discos duros de cada computador.

Si el usuario detectara la presencia de algún virus en el equipo, deberá notificar inmediatamente al departamento de sistemas y desconectar al equipo de la red hasta solucionar el problema.

Cada usuario deberá cerrar la sesión en su computador personal cuando no lo este utilizando.

Se deberá responsabilizar al personal de contrato sobre el manejo de información a través de sus contratos.

3.3.1.3.3 Respaldos y Recuperación de archivos, aplicaciones y bases de datos

El departamento de sistemas será responsable para realizar los backups de la información almacenada en las portátiles

El departamento de sistemas garantizará la seguridad de la información de los usuarios que se encuentra almacenada en los servidores de archivos, servidores de bases de datos, servidores de aplicaciones.

El departamento de sistemas será quien garantice la protección de la información asegurando su integridad, disponibilidad de acuerdo a sus normas establecidas.

El departamento de sistemas garantizara la seguridad de las bases de datos, los respaldo de las mismas y la restauración si hubiera la necesidad.

3.3.1.3.4 Acceso a los servicios de red

El acceso del personal a los servicios de red y de la información en horas no laborables será con previa autorización del responsable del área y coordinado con el departamento de sistemas para asignar los permisos.

El departamento de sistemas será quien otorgue permisos a los empleados para el acceso a la información y los servicios de la red dependiendo de su perfil.

El departamento de sistemas será quien controle que el acceso a la red y a la información este disponible y no sea interrumpido las 24 horas del día, los 365 días del año.

El departamento de sistemas será quien asegure la disponibilidad de los servicios para los usuarios de acceso remoto, con previa autorización de las autoridades.

El departamento de sistemas se responsabilizará de la administración de las IPs públicas y privadas.

El departamento de sistemas será quien realice el monitoreo de la red y si encontrara alguna actividad sospechosa ocasionado por un computador personal, lo desconectará de la red hasta solucionar el problema.

El departamento de sistemas se responsabilizará de la administración, operación y correcto funcionamiento de los servicios de red.

3.3.1.3.5 Administración de usuarios

El departamento de sistemas será quien cree la cuenta al nuevo usuario en la red con su respectiva identificación y autenticación.

Cada usuario en su primer ingreso podrá cambiar su contraseña que será única e intransferible, es decir, queda prohibido que el usuario comparta su contraseña a los compañeros.

El departamento de sistemas administrara el tiempo útil de la clave.

El departamento de sistemas creará cuentas temporales con el respectivo control de acceso y dependiendo al perfil solicitado.

El departamento de sistemas será quien elimine las cuentas de las personas que ya no laboran en la institución.

El departamento de sistemas será quien modifique las cuentas de los usuarios con previa autorización del jefe del departamento solicitante.

3.3.1.3.6 Correo electrónico e Internet

El departamento de sistemas será quien administre la información que ingresa por el correo electrónico.

El departamento de sistemas será quien controle la navegación de los usuarios y limite el acceso a páginas de internet que no tienen ningún vínculo con las funciones de la empresa.

El departamento de sistemas definirá que tamaño de archivos podrá enviar y recibir cada usuario dependiendo de las normas del departamento.

El usuario no abrirá correo electrónico enviado por un remitente que no conoce, no responderá el mensaje ni mucho menos ejecutará archivos adjuntos en dichos correos.

3.3.1.4 Políticas de seguridad para el desarrollo de software

Todo Software desarrollado en el departamento de sistemas tendrá su respectiva documentación (manual de usuario, instalación y programación).

Todo software desarrollado en el departamento de sistemas deberá seguir una metodología con sus respectivas normas y procedimientos seleccionados por el departamento de sistemas.

Toda modificación de algún software deberá tener su pedido formal dando su justificación y estará guiada por el Jefe de Sistemas.

3.3.1.5 Políticas de seguridad para contingencia

El departamento de sistemas debe contar con planes de contingencia que pueda garantizar la recuperación de la información por algún desastre sin el mayor número de perdidas y a un bajo costo.

Para el caso de un colapso total de aplicaciones o de bases de datos, se deberá definir un procedimiento de restauración de los respaldos de las mimas.

3.3.1.6 Políticas de seguridad para la capacitación del personal

El departamento de sistemas deberá contar con un plan de capacitación al personal de la empresa del software existente.

El departamento de sistemas deberá tener la posibilidad de capacitarse en lenguajes para el desarrollo de software, nuevas aplicaciones que faciliten el trabajo de los usuarios, de administración de la red y mantenimiento de equipos y red

3.3.2 PROCEDIMIENTOS

En la tabla 3.2 se muestra las políticas de seguridad con sus respectivos procedimientos

POLITICAS	PROCEDIMIENTOS
POLITICAS DE SEGURIDAD DEL HARDWARE	
Adquisición e instalación de equipos	• Adquisición de nuevos equipos • Adquisición de partes de hardware • Instalación y/o cambio físico de equipos • Registro y/o actualización de los datos del equipo y sus partes
Seguridad Física	• Para sacar un equipo fuera de la Institución • Apagado de equipos si se produce un corte de suministro eléctrico
Mantenimiento de equipos	• Mantenimiento Correctivo • Mantenimiento Preventivo
POLITICAS DE SEGURIDAD DEL SOFTWARE	
Adquisición, instalación y actualización	• Actualización y/o instalación de software en los equipos

	• Adquisición y registro del software nuevo en el departamento de Sistemas
POLITICAS DE SEGURIDAD PARA EL CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACION	
Acceso Físico	• Acceso al área de Servidores
Acceso a la Información (archivos y documentos)	• Permisos para el acceso a los archivos
Respaldos y Recuperación de archivos, aplicaciones y bases de datos	• Respaldos de archivos, aplicaciones y bases de datos • Restauración de respaldos de archivos, aplicaciones y bases de datos
Acceso a los servicios de red	• Acceso a las aplicaciones • Acceso a Base de datos • Acceso al correo electrónico e internet • Acceso Remoto
Administración de usuarios	• Creación de usuarios • Actualización (modificación y eliminación) de usuarios • Bloqueo y desbloqueo de usuarios
Correo electrónico e Internet	• Mantenimiento de correo electrónico • Permisos y restricciones del acceso a páginas de internet
POLITICA DE SEGURIDAD PARA EL DESARROLLO DE SOFTWARE	
Seguridad para el Desarrollo de Software	• Metodologías establecidas por el departamento de Sistemas para el Desarrollo de Software
POLITICA DE SEGURIDAD PARA CONTINGENCIA	
Seguridad para Contingencia ante desastres	• Plan de restauración de aplicaciones y bases de datos.

	• Plan de contingencia
POLITICA DE SEGURIDAD PARA LA CAPACITACION DEL PERSONAL	
Seguridad para la Capacitación del personal	• Plan de Capacitación

Tabla 3.2 Políticas y procedimientos

A continuación se describen los procedimientos:

3.3.2.1 Adquisición de nuevos equipos

1. El Jefe de Sistemas recibe el requerimiento del nuevo equipo por parte del jefe solicitante.
2. El Jefe de Sistemas analiza el requerimiento y pasa al departamento financiero un memorando del pedido con las especificaciones del equipo
3. El departamento financiero revisa si hay presupuesto. Si hay presupuesto envía la solicitud al departamento de adquisiciones.
4. En el departamento de adquisiciones solicita proformas a tres empresas del grupo de proveedores.
5. El departamento de adquisiciones escoge la mejor opción y envía la solicitud al departamento financiero para la compra
6. El proveedor entrega el equipo al jefe de adquisiciones y este a su vez al departamento de sistemas
7. El departamento de sistemas asigna un técnico para que pruebe el funcionamiento del equipo y lo configure
8. El técnico entrega el equipo al usuario correspondiente.

3.3.2.2 Adquisición de partes de hardware

1. El jefe del departamento de sistemas recibe la solicitud para revisar el equipo por alguna falla.
2. El Jefe de Sistemas asigna a un técnico para que revise el requerimiento
3. El técnico identifica el problema y que se necesita reemplazar.

4. El técnico genera una solicitud de material y equipos con la características técnicas para la adquisición.
5. El Jefe de Sistemas envía esta solicitud al departamento administrativo para su autorización y compra.
6. El departamento de adquisición entrega el material y equipo al departamento de sistemas.
7. El técnico revisa el material y equipo recibido y reemplaza el anterior
8. El técnico prueba el funcionamiento del equipo
9. El técnico entrega el equipo al usuario correspondiente

3.3.2.3 Instalación y/o cambio físico de equipos

1. El Jefe de Sistemas recibe el requerimiento del jefe solicitante
2. El Jefe de Sistemas asigna a un técnico para analizar el requerimiento
3. El técnico identifica si es instalación o cambio físico de equipos
4. El técnico verifica si existen instalaciones de red y eléctricas en el lugar a ubicar el equipo
5. Si no existen las instalaciones siga el siguiente numeral caso contrario vaya al numeral 7
6. El Jefe de Sistemas solicita al departamento de adquisiciones que se realizan las instalaciones eléctricas y de red a la empresa que presta estos servicios.
7. El técnico realiza el cambio o movimiento del equipo.

3.3.2.4 Registro y/o actualización de los datos del equipo y sus partes

1. El técnico de sistemas una vez configurado el equipo entrega al usuario correspondiente.
2. El técnico indica la entrega del equipo y el cambio realizado al departamento de activos
3. El jefe de activos asigna a una persona para que registre los datos del equipo en un formulario y almacenarlo en una base de datos.

4. El jefe de activos imprime el formulario y hace firmar al usuario responsable del equipo.

3.3.2.5 Para sacar un equipo fuera de la Institución

1. El Jefe de Sistemas recibe el requerimiento por parte del jefe solicitante
2. El Jefe de Sistemas asigna a un técnico para que analice el requerimiento
3. El técnico respalda la información del equipo
4. El técnico instala todos las aplicaciones de seguridad para el equipo
5. El técnico entrega el equipo al usuario
6. El usuario ya puede salir de la Institución con el equipo

3.3.2.6 Apagado de equipos si se produce un corte de suministro eléctrico

En caso de producirse un corte de suministro eléctrico el personal deberá realizar los siguiente:

1. Si el corte de energía dura mas de 10 minutos el personal deberá apagar sus computadores
2. Si el corte de energía dura mas tiempo que la capacidad del UPS el Jefe de Sistemas deberá apagar los servidores, antes que el UPS se apague

Cuando se restablezca la energía eléctrica, el personal procederá de la siguiente manera:

1. El Jefe de Sistemas encenderá los servidores
2. Luego de 5 minutos cada usuario encenderá sus equipos.

3.3.2.7 Mantenimiento Correctivo

1. El Jefe de Sistemas asigna al técnico para que ejecuten el mantenimiento correctivo
2. El técnico recibe el requerimiento del usuario responsable del equipo
3. Se pide que el conserje encargado del piso traslade el equipo al área de sistemas.

4. Si el equipo tiene garantía siga el numeral 9, caso contrario siga el siguiente numeral.
5. Si el equipo requiere de partes continúe con el siguiente numeral caso contrario vaya al 8
6. El técnico solicita al departamento de adquisiciones mediante formulario el hardware requerido
7. El departamento de adquisiciones entrega el hardware al técnico
8. El técnico procede a la reparación del equipo y siga en el numeral 11
9. El técnico reporta y entrega el equipo a la empresa proveedora para que solucione el problema
10. La empresa una vez solucionado el problema entrega el equipo al técnico
11. El técnico revisa que el equipo que este en correcto funcionamiento
12. Si al equipo se le han cambiado algunas partes, el técnico deberá reportarlo al departamento de adquisiciones para que procedan a la actualización en la base de datos de acuerdo al registro de activos.
13. El técnico entrega el equipo al usuario y hace firmar el documento de recibido en buen funcionamiento.

3.3.2.8 Mantenimiento Preventivo

1. El Jefe de Sistemas comunica a los directores de los departamentos las fechas que se ejecutara el mantenimiento a las computadoras
2. El Jefe de Sistemas asigna a los técnicos para realizar el mantenimiento de acuerdo al cronograma establecido
3. El personal técnico realiza el mantenimiento preventivo en cada escritorio del usuario.
4. El técnico apaga y destapa el equipo.
5. El técnico quita el polvo interno del equipo con una aspiradora
6. El técnico asegura todas las tarjetas internas del equipo
7. El técnico cierra el equipo
8. Limpia el teclado, el mouse, monitor, cpu y unidades de dispositivos magnéticos
9. El técnico enciende el equipo y comprueba su funcionamiento

10. El técnico solicita una firma por parte del usuario de recibir el equipo.

3.3.2.9 Actualización y/o instalación de software en los equipos

1. El Jefe de Sistemas recepta el requerimiento por parte del Director solicitante
2. El Jefe de Sistemas asigna a un técnico para que realice el análisis del requerimiento
3. El técnico determina si es actualización o instalación de nuevo software, si es actualización siga con el siguiente numeral caso contrario al 5
4. El técnico pide al Jefe de Sistemas permisos de acceso mediante IP a las páginas del fabricante de software para actualizarlas en línea, pase al numeral 9
5. El técnico revisa en el registro de software si existe el software requerido, si no existe pase al siguiente numeral, caso contrario pase al numeral 9
6. El técnico informa al Jefe de Sistemas que no se cuenta con el software requerido
7. El Jefe de Sistemas pide al departamento de adquisiciones que compren adjuntando un justificativo
8. El departamento de adquisiciones entrega el software al Jefe de Sistemas y esta a su vez al técnico
9. El técnico instala el software a la máquina del usuario solicitante
10. El técnico prueba el funcionamiento del software
11. El Técnico entrega el equipo al usuario solicitante, adjuntando el documento de entrega y recepción con los datos actualizados.

3.3.2.10 Adquisición y Registro del software nuevo en el departamento de Sistemas

1. El Jefe de Sistemas recibe el requerimiento del director solicitante o del técnico del departamento de sistemas
2. El Jefe de Sistemas analiza el requerimiento

3. El Jefe de Sistemas justifica el requerimiento y envía la solicitud al departamento de adquisiciones.
4. El departamento de adquisiciones envía el pedido al departamento financiero para que aprueben el presupuesto
5. Una vez aprobado el presupuesto el departamento de adquisiciones realiza la compra.
6. El departamento de adquisiciones entrega el software al departamento de sistemas previo al registro del software en el departamento de activos
7. El Jefe de Sistemas asigna a un técnico para que registre el software en sus activos y realiza copias de seguridad del software
8. El técnico almacena los CDs originales en una caja de seguridad
9. El técnico instala el software en las maquinas solicitantes .

3.3.2.11 Acceso al área de Servidores

Cuando existe un problema o chequeo rutinario del cableado de datos y/o eléctrico

1. El Jefe de Sistemas solicita al departamento de adquisiciones para que emita una orden de trabajo al servicio técnico contratado para este trabajo.
2. El Jefe de Sistemas acompaña al personal de servicio técnico durante la revisión que realiza en las instalaciones del cuarto de servidores.
3. Una vez terminado la revisión por parte de la empresa externa, el Jefe de Sistemas valida el trabajo realizando las pruebas de funcionamiento respectivas
4. El Jefe de Sistemas notifica al departamento de adquisiciones los resultados del trabajo para que se proceda al pago.

3.3.2.12 Permisos para el acceso a los archivos

1. El Jefe de Sistemas recibe el requerimiento de un director solicitante para solucionar problemas de los sistemas desarrollados por proveedores externos.

2. El Jefe de Sistemas solicita al departamento de adquisiciones que se procede a emitir una orden de trabajo para la empresa externa
3. El Jefe de Sistemas proporciona el permiso para el acceso a los archivos requeridos por parte del personal técnico de la empresa externa.
4. Una vez realizado el trabajo por la empresa externa, el jefe de sistema realiza las validaciones necesarias para verificar el buen funcionamiento
5. El Jefe de Sistemas notifica los resultados al departamento de adquisiciones para que proceda el pago respectivo.

3.3.2.13 Respaldos de archivos, aplicaciones y bases de datos

1. El Jefe de Sistemas asigna a un técnico para realizar los respaldos de la información de la empresa (archivos, aplicaciones, bases de datos)
2. El Jefe de Sistemas concede los permisos al técnico para realizar los respaldos
3. El Jefe de Sistemas define que información debe ser respaldada y su periodicidad dependiendo de la criticidad.
4. El técnico antes de realizar los respaldos etiqueta las cintas magnéticas de acuerdo al formato escogido por el departamento de sistemas
5. El técnico procede a realizar los respaldos
6. El técnico realiza un reporte del contenido de las cintas magnéticas
7. El técnico procede al almacenamiento de las cintas dependiendo de la periodicidad del respaldo:
8. Si es semanal el respaldo se almacenará en una caja fuerte
9. Si es mensual el respaldo se almacenará en un banco.

3.3.2.14 Restauración de respaldos de archivos, aplicaciones y bases de datos

1. El Jefe de Sistemas asigna a un técnico para que realice la restauración de los respaldos
2. Si el backup a restaurar se encuentra guardado en el banco, el Jefe de Sistemas solicitara al departamento de adquisiciones que gestione la salida del backup del banco

3. Si el backup a restaurar se encuentra almacenado localmente, el Jefe de Sistemas entrega al técnico el backup a restaurar.
4. El técnico procede a restaurar el backup solicitado y realiza las validaciones respectivas

3.3.2.15 Acceso a las aplicaciones

1. El Jefe de Sistemas recibe el requerimiento por parte del director solicitante
2. El Jefe de Sistemas crea el perfil para el acceso a la aplicación
3. El Jefe de Sistemas asigna a un técnico para instalar y configurar el equipo del usuario con la aplicación requerida.
4. El técnico realiza las pruebas correspondientes del funcionamiento de la aplicación

3.3.2.16 Acceso a Base de datos

1. El Jefe de Sistemas recibe el requerimiento del director solicitante
2. El Jefe de Sistemas crea los perfiles de usuario para el acceso requerido
3. El Jefe de Sistemas asigna a un técnico para que configure e instale el software cliente en el equipo del usuario para el acceso a la base de datos
4. El técnico realiza pruebas de funcionamiento para el acceso a la base de datos requerida.

3.3.2.17 Acceso al correo electrónico e Internet

1. El Jefe de Sistemas recibe el requerimiento del director solicitante
2. Si es acceso a correo electrónico siga el siguiente numeral caso contrario siga el numeral 4
3. El Jefe de Sistemas verifica si la cuenta de correo esta creada si no lo esta crea la cuenta.
4. El Jefe de Sistemas asigna a un técnico para que configure el acceso a Internet en el equipo de usuario

5. El técnico realiza las pruebas respectivas para verificar el funcionamiento del servicio

3.3.2.18 Acceso Remoto

1. El Jefe de Sistemas recibe el requerimiento del director solicitante
2. El Jefe de Sistemas analiza el requerimiento
3. El Jefe de Sistemas comunica mediante memorando si el requerimiento es aprobado o negado con su justificativo. Si es aprobado siga con el siguiente numeral.
4. El Jefe de Sistemas configura la cuenta de usuario de acuerdo a las políticas de acceso a los usuarios a los servicios de red
5. El Jefe de Sistemas entrega la contraseña del usuario al jefe solicitante del acceso remoto

3.3.2.19 Creación de usuarios

1. El Jefe de Sistemas recibe el requerimiento por parte del director solicitante
2. El Jefe de Sistemas crea al usuario y asigna el perfil y grupo que le corresponde a dicho usuario dependiendo del área y cargo.
3. La contraseña es temporal hasta que ingrese por primera vez en la red y le pida cambiar.
4. La contraseña será única e intransferible
5. La longitud de la contraseña será máximo de 6 caracteres
6. La contraseña debe contener por lo menos un carácter especial, un carácter numérico, un carácter alfabético mayúscula.
7. No se utilizará palabras de nombres comunes personales o fechas significativas.

3.3.2.20 Actualización (Modificación y eliminación) de usuarios

1. El Jefe de Sistemas recibe el requerimiento del director solicitante

2. Si es modificación siga el siguiente numeral, si es eliminación de cuenta siga el numeral 4
3. El Jefe de Sistemas procede a realizar las modificaciones requeridas a la cuenta del usuario solicitante siga el numeral 5
4. El Jefe de Sistemas procede a eliminar la cuenta
5. El Jefe de Sistemas notificará al director solicitante que el requerimiento ha sido realizado.

3.3.2.21 Bloqueo y desbloqueo de usuarios

1. El Jefe de Sistemas recibe la petición de bloqueo por parte del director solicitante, esto podría suceder por los siguiente motivos: vacaciones, comisiones de servicio fuera de la institución por mas de un día, otros
2. El Jefe de Sistemas bloquea la cuenta del usuario
3. El Jefe de Sistemas recibe la petición para desbloqueo de una cuenta por parte del director solicitante
4. El Jefe de Sistemas desbloquea la cuenta del usuario

3.3.2.22 Mantenimiento de correo electrónico

1. El Jefe de Sistemas realizará un monitoreo periódico en forma semanal para identificar los siguientes eventos:
    a. Correos tipo spam y los URL que los genera.
    b. Tamaño de mensajes mayor a 10 MB de las cuentas de usuarios
2. Una vez identificada los URL que generan correos tipo spam, el Jefe de Sistemas los agregará a las listas negras en el servidor de correo.
3. Una vez identificadas las cuentas con tamaño mayor a 10 MB, el Jefe de Sistemas notifica al usuario de dicha cuenta para que tome las acciones correctivas.

3.3.2.23 Permisos y restricciones del acceso a páginas de Internet

1. El Jefe de Sistemas recibe la solicitud del Director solicitante

2. Si es permiso de acceso para páginas Web siga el numeral 4 , caso contrario siga el siguiente numeral
3. El Jefe de Sistemas agrega en la lista de páginas no permitidas del firewall, el URL solicitante siga numeral 7.
4. El Jefe de Sistemas valida técnicamente si el acceso a la página solicitada no provoca problemas en la red tales como: alto consumo de ancho de banda, descargas trojanos, virus, gusanos, etc
5. Si es aprobada siga al siguiente numeral caso contrario ir al numeral 7.
6. El Jefe de Sistemas agrega el URL solicitado en la lista de acceso permitido del firewall
7. El Jefe de Sistemas notifica al director que el requerimiento se ha realizado, si no fue aprobado el acceso al URL solicitado adjunta la justificación técnica respectiva.

3.3.2.24 Plan de restauración de aplicaciones y bases de datos

1. El Jefe de Sistemas identifica la magnitud del daño en la pérdida de la información (aplicaciones o bases de datos)
2. Si el daño incluye equipo pase al numeral 3 caso contrario al 4
3. El jefe de sistemas instala y configura un equipo de las mismas características al dañado o un equipo que soporte la información a restaurar.
4. Para la restauración de la aplicación o de las bases de datos se sigue el procedimiento 3.3.2.14 sobre la Restauración de respaldos de archivos, aplicaciones y bases de datos

Capítulo 4. ANALISIS COSTO/BENEFICIO

4.1 COSTO DE EQUIPAMIENTO, INSTALACIÓN, CONFIGURACIÓN

El siguiente cuadro presenta los costos de equipamiento, instalación y configuración de los equipos que se utilizarán en el diseño de seguridades de la red.

En la tabla 4.1 se muestra los equipos que serán utilizados en el diseño con el costo promedio de 3 empresas que proporcionaron proformas.

	EQUIPAMIENTO	INSTALACION	CONFIGURACION
MAQUINARIAS Y EQUIPOS			
1 UPS	5211.24		
1 ROUTER	2020.07		
1 FIREWALL	3666.66	766.66	
3 SWITCH CAPA 2	5259.78		
1 SWITCH CAPA 3	3784.82		
1 IPS	943.30		
TODO EL CABLEADO	8160.00		
2 SERVIDORES ARC	13648.78		
2 SERVIDORES BDD	33990.82		
120 LICENCIAS ANTIVIRUS	7560.00		
TOTAL	**84245.47**	**766.66**	
INSTALACIONES			
Se utilizaran la mismas instalaciones de cableado y eléctrico			
CAPACITACION			
En Equipos	1000.00		
SUMINISTROS Y MATERIALES DE OFICINA			
Materiales	200.00		
TOTAL			**86212.13**

Tabla 4.1 Equipamiento y su costo

Ver Anexo III. Precios de Proveedores

4.2 PRESENTACIÓN Y SELECCIÓN DE PROVEEDOR EN EL MERCADO

4.2.1 PRESENTACION DE PROVEEDORES

Para la presentación de proveedores, el CONSEJO NACIONAL DE EDUCACIÓN SUPERIOR CONESUP en cumplimiento de lo dispuesto por los Art 51 y 52 del Reglamento a la Ley Codificada de Contratación Pública y del Instructivo para calificación, Listado y Registro de Proveedores de la Institución, realizan una invitación a las personas naturales y/o jurídicas para registrarse como proveedores de bienes, ejecución de obras y prestación de servicios, para que acrediten su capacidad y solvencia. Además, adjuntan un listado de los siguientes documentos a presentar hasta determinado tiempo:

a) Certificado de existencia legal y cumplimiento de obligaciones otorgado por la Superintendencia de Compañías, para personas jurídicas constituidas en el Ecuador.
b) Fotocopias de la cédula de ciudadanía y papeleta de votación del Representante Legal
c) Registro único de Contribuyentes actualizado
d) Certificado de la Contraloría General del Estado de no constar en el registro de contratista incumplidos.
e) Carta de presentación en la que se especifiquen los bienes o servicios que ofrece, además se señalará el domicilio con la dirección exacta, calle, número, piso, oficina y números telefónicos, fax, etc
f) Escritura de Constitución debidamente Inscrita en el Registro Mercantil
g) Balances aprobados por la Superintendencia de Compañías, actualizados a la fecha de presentación de los documentos
h) Registro de accionistas actualizado.

Las personas naturales deberán cumplir con lo estipulado en los literales b,c,d,e.
Los proveedores calificados confirmarán la vigencia de los documentos presentados, en caso de variaciones deberán actualizarlos.

4.2.2 SELECCIÓN DE PROVEEDORES

Una vez recibidas las ofertas de los proveedores, se reúne la Comisión de Adquisiciones y escoge a los proveedores con las mejores ofertas dependiendo de los siguientes aspectos:

a) Cumplimiento de las características técnicas de las ofertas
b) Costo
c) Calidad – Marca
d) Forma de Pago
e) Garantías técnicas y tiempo de las mismas
f) Si es único proveedor en el mercado ecuatoriano

4.3 DETERMINACIÓN DEL PRESUPUESTO PARA LA IMPLEMENTACION

Una vez determinado el costo de equipamiento valorado en $84.245,47 (OCHENTA Y CUATRO MIL DOSCIENTOS CUARENTA Y CINCO DOLARES AMERICANOS CON CUARENTA Y SIETE CENTAVOS).

El costo de la instalación de $766,66 (SETECIENTOS SESENTA Y SEIS DOLARES AMERICANOS CON SESENTA Y SEIS CENTAVOS) que corresponde al firewall, las instalaciones de cableado y eléctrico se utilizaran las existentes.

La capacitación de equipos con un costo de $1000,00 (MIL DOLARES AMERICANOS) que corresponden al Router y Firewall, y $200.00 (DOSCIENTOS DOLARES AMERICANOS) para suministros de oficina.

Se concluye que el proyecto tiene un costo total aproximado de : $86.212,13 (OCHENTA Y SEIS MIL DOSCIENTOS DOCE DOLARES AMERICANOS CON TRECE CENTAVOS),

4.4 ANÁLISIS COSTO/BENEFICIO

El Consejo Nacional de Educación Superior es una institución pública que presta servicios sin fines de lucro, por tanto para el análisis Costo/Beneficio se determinaron tres aspectos fundamentales para identificar el beneficio del nuevo diseño de Red:

- Ahorro de tiempo
- Ahorro en costos
- Disponibilidad de Servicio

4.4.1 IDENTIFICACIÓN DE BENEFICIOS

- Reducir los tiempos asociados a la realización de las tareas y funciones que utilizan la Intranet y Extranet del CONESUP
- Mantener una alta disponibilidad de los sistemas de información para que el servicio no se interrumpa.
- Incrementar el número de transacciones por tiempo.
- Mayor productividad de personal
- Ahorro en costos

4.4.2 ANÁLISIS DE AHORRO EN COSTOS

4.4.2.1 Identificación de Servicios al Público, tiempo y Costos:

Para el análisis de ahorro en costos se identifico tres procesos que tienen mayor prestación de servicios del CONESUP entre ellos: Area Académica, Registro de Títulos y Certificación.

En la tablas 4.2, 4.3 y 4.4 se muestran los tiempos de procesamiento y el valor de cada trámite, tanto en la situación actual como en la estimada y lo que se ahorraría.

- *Area Académica*

	Situación Actual		Situación Estimada		Ahorro	
Servicio	Tiempo de procesamiento	Costo (USD)	Tiempo de procesamiento	Costo (USD)	Tiempo de procesamiento	Costo (USD)
Registro de Carreras Pregrado y Postgrado	10 min	2,10	5 min	1,05	5 min	1,05
Informes sobre creación de Universidades	3 meses	6.219,90	2.5 meses	5.183,25	0.5 meses	1063,65
Informes sobre creación de Carreras y Postgrados	3 horas	25,89	2 horas	17,26	1 hora	8,63

Tabla 4.2 Situación actual, situación estimada y su ahorro del Area Académica

- *Registro de Títulos (Por Trámite)*

	Situación Actual		Situación Estimada		Ahorro	
Servicio	Tiempo de procesamiento	Costo (USD)	Tiempo de procesamiento	Costo (USD)	Tiempo de procesamiento	Costo (USD)
Revisión de Archivos	20 min	1,80	15 min	1,35	5 min	0,45
Correo Electrónico: Devolución de archivos o cartas de conformidad a las universidades	5 min	0,45	2 min	0,18	3 min	0,27
Espera de documentos y Revisión de documentos con los archivos	3 días	136,08	2 días	90,72	1 día	45,36
Subida a la base de datos del CONESUP a los graduados	10 min	0,90	5 min	0,45	5 min	0,45
COSTO DEL PROCESO POR TRAMITE		139,23		92,70		46,53

Tabla 4.3 Situación actual, situación estimada y su ahorro del Area de Registro de Títulos

- *Certificación*

	Situación Actual		Situación Estimada		Ahorro	
Servicio	Tiempo de procesamiento	Costo (USD)	Tiempo de procesamiento	Costo (USD)	Tiempo de procesamiento	Costo (USD)
Certificados de registro de Título	15 min	9,00	10 min	6,00	5 min	3,00
Legalización de Firmas en Títulos	10 min	3,00	5 min	1,50	5 min	1,50
Legalización de Firmas de documentos	10 min	3,00	5 min	1,50	5 min	1,50
Certificados de Constar o no en Registro de Títulos	1 día	4,00	4 horas	2,00	4 horas	2,00

Tabla 4.4 Situación actual, situación estimada y su ahorro del Area de Certificación

4.4.2.2 Resultados del ahorro en costos

Número de trámites promedio al mes	Ahorro
Académico	
30 Registros de Carreras Pregrado y Postgrado	31,50
80 Informes sobre creación de Carreras y Postgrados	690,40
Registro de Títulos	
120 Trámites	5.583,60
Certificación (Ventanillas)	
100 Certificados de registro de Título	300,00
80 Legalización de Firmas en Títulos	120,00
80 Legalización de Firmas de documentos	120,00
40 Certificados de Constar o no en Registro de Títulos	80,00
Total mensual de ahorro	**6.925,50**

Tabla 4.5 Resultados del ahorro en costos

Como resultado del análisis en la tabla 4.5, el presente proyecto de diseño de Red valorado por $86.212,13 estaría recompensado en 13 meses con el ahorro en los servicios en dinero y tiempo de servicio.

Capítulo 5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Los problemas que se han producido en la red interna del CONESUP, han sido por no contar con un manual de políticas de seguridad y procedimientos que permitan que los procesos sean optimizados en tiempo y costo.

- El desconocimiento de la importancia de la seguridad de la información ha ocasionado que mucha de ella sea mal manejada modificada y eliminada.

- La falta de un plan estratégico previo a la salida de un nuevo servicio al público, ha ocasionado que la red actual se sature y genera demora en los tiempos de respuesta.

- El crecimiento de la Institución en cuanto al personal se refiere , ha generado que se incrementen servicios en servidores que ya tienen una función específica.

- El manual de políticas permitirá al administrador de la red mantener la integridad, confidencialidad y disponibilidad de información en la Institución.

- El proceso para elaborar un diseño de seguridad de red esta basado en el uso de varias metodologías para las diferentes etapas tales como: Análisis Situación Actual (OCTAVE), Diseño de seguridad de Red (SAFE) y Manual de políticas y procedimientos (ISO 17799), lo cual nos permitió conocer nuevas conceptos.

- Las políticas y procedimientos descritos en el presente trabajo tendrán un buen resultado siempre y cuando los Directores y los Jefes responsables

de los procesos los acepten y practiquen concientizando a los empleados sobre su importancia.

5.2 RECOMENDACIONES

- Considerando que mientras exista un avance tecnológico, la seguridad de la información puede tener mas amenazas; por tanto se recomienda que el manual de políticas sea revisado y actualizado periódicamente

- Se recomienda que antes de sacar un nuevo servicio al público y/o incremente personal se realice un plan estratégico donde se considere la seguridad de la información, la infraestructura de red y requerimientos tecnológicos.

- Se recomienda desarrollar un plan de contingencias para el respaldo y recuperación de la información en caso de desastres

- Se recomienda que el Departamento de Sistemas defina metodologías específicas para el desarrollo de software y se estandarice el procedimiento.

GLOSARIO

ACCESO. Situación en la que un usuario hace uso de la información contenida en los sistemas

BACKUP.- Copia de seguridad o Copia de respaldo de datos

BASE DE DATOS. Colección de datos almacenadas en un dispositivo de almacenamiento de acceso directo.

CERTIFICACIONES DE TITULO. Documento donde consta el nombre del profesional, su cédula, el título y el nivel al que pertenece, además el número y fecha de Registro dado por el Conesup.

FIREWALL. Elementos utilizado en las redes de computadoras (hardware o software) para controlar las comunicaciones permitiéndolas o negándolas

HARDWARE. Componentes físicos de una computadora, incluyendo el procesador, memoria, dispositivos de entrada/salida y discos.

IDS. Intrusion Detection System. Es un programa usado para detectar accesos desautorizados a un computador o a una red.

INFORMACION. Conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno

IPS. Intrusion Prevention System. Hardware o Software que busca anomalías a nivel de sistema operativo, monitorean la actividad del sistema de archivos

JEFE DE SISTEMAS. Persona que tiene a su cargo la responsabilidad de administrar el área de tecnología.

OCTAVE. Operational Critical Treath, Asset, an Vulnerability Evaluation. Es un método basado en un conjunto de criterios, las cuales definen los elementos esenciales para la evaluación del riesgo de seguridad.

POLITICA. El conjunto de ordenamiento y lineamientos enmarcados en los diferentes instrumentos jurídicos y administrativos de la institución que rigen la función informática.

PROCEDIMIENTO. Modo de ejecutar determinadas acciones que suelen realizarse de la misma forma, con una serie común de pasos claramente definidos, que permiten realizar una ocupación o trabajo correctamente

REGISTRO DE TITULOS. Es un proceso mediante el cual se asigna a través del sistema Académico, un número único que valida autenticidad del título profesional de una persona.

REGYCONT. Sistema informático que se utiliza para registrar y realizar un seguimiento de la documentación externa recibida.

ROUTER. Enrutador o emcaminador, que direcciones paquetes de una dirección a otra.

SERVIDOR. Nodo de Computadora que consiste de un dispositivo de discos de almacenamiento compartido en un LAN; almacena aplicaciones de software y los archivos de los usuarios que son accesados remotamente.

SIGEF. Sistema informático que permite realizar transacciones, registros financieras y almacenarlas en una base de datos.

SISTEMA ACADEMICO. Sistema informático que permite el registro y la manipulación de las carreras de pregrado y postgrado de las Universidades, Escuelas Politécnica e Institutos Técnicos y Tecnológicos, además de la información general de cada institución y la información de profesionales

SOFTWARE. Colección de instrucciones lógicas usando un lenguaje de programación que la CPU de la computadora puede interpretar para llevar a cabo una tarea específica.

SWITCH CAPA 2. Dispositivo electrónico de interconexión de redes de computadores que opera en capa 2 del modelo OSI (nivel de enlace de datos), transfiere datos de un segmento a otro de acuerdo con la dirección MAC de destino de los datagramas en la red

SWITCH CAPA 3. Dispositivo de múltiples redes de nivel 3 y encaminador de paquetes entre las redes con funciones de encaminamiento o routing

UPS. Sistema de alimentación ininterrumpida. Es un dispositivo que, gracias a su batería de medio puede proporcionar energía eléctrica tras un apagón existente en la red eléctrica.

VIRUS INFORMATICO. Programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario

BIBLIOGRAFIA

- ALVARES MARAÑON, Gonzalo; PEREZ GARCIA, Pedro Pablo. Seguridad informática para empresas y particulares. McGrawHill. Carmelo Sánchez González. Madrid, 2004.

- CARRACEDO GALLARDO, Justo. Seguridad en Redes Telemáticas. McGrawHill. Concepción Fernández Madud. Madrid. 2004.

- MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. Hackers 3, Secretos y soluciones para la seguridad de redes. McGrawHill. Carmelo Sánchez González. Madrid, 2002.

- NORMA ISO 177999

- http://www.uv.es/~sto/cursos/icssu/html/ar01s04.html. Abril 2007

- http://www.segu-info.com.ar/fisica/seguridadfisica.htm . Junio 2007

- http://es.tldp.org/Manuales-LuCAS/doc-como-seguridad-fisica/COMO-seguridad-fisica.html . Junio 2007

- http://www.cert.org/octave/. Julio 2007

- http://www.gfihispana.com/downloads/downloads.aspx?pid=lanss&lid=es

- http://www.nessus.org/

- ALBERTS, Christopher, DOROFEE, Audrey, STEVENS, James, WOODY, Carol, “Lista de documentos guía del método OCTAVE-S”, Carnegie Mellon University , Software Engineering Institute, Pittsburgh, PA, Enero 2005, se encuentran comprimidos en http://www.sei.cmu.edu/community/octave-s/OCTAVE-s.zip

ANEXO I

INVENTARIO DE EQUIPOS Y PORTATILES

REPORTE ACTIVOS FIJOS - Clase de Activo

Tipo de Activo: EQUIPOS, SISTEMAS Y PAQUETES INFORMATICOS
SubTipo de Activo: EQUIPO PARA PROCESAMIENTO ELECTRONICO DE DATOS
Clase de Activo: C.P.U.

Código	Descripción	Fecha de Adquisición	Valor CH	MARCA	MODELO	Número de Serie	Custodio 1
007-09-005-0912	CPU CLON INGEINCON	22/05/2002	753.00		MIDITORRE	2002-057	GUERRA LEON DANILO HUMBERTO
007-09-005-0922	CPU	10/12/2004	500.00	COMPAQ		3D07FQRIDOMA	JARRIN PINOS GABRIELA ALEXANDRA
007-09-005-0933	CPU- CLON	10/12/2004	450.00			0796	ALBUJA GUAMAN MARCELO GEOVANNY
007-09-005-0936	CPU	10/12/2004	200.00	COMPAQ	47XMAX	F808BK620078	BODEGA
007-09-005-0944	CPU	10/12/2004	400.00				BODEGA
007-09-005-0952	CPU CLON	01/09/2002	573.00			635L4-048-1	BURGASI JACOME HERIBERTO GERMAN
007-09-005-0964	CPU -CLON	18/12/2001	676.00			690	CARRILLO GILER JORGE EDUARDO
007-09-005-0967	CPU CLON	01/09/2002	573.00			635L4-045-1	CUENCA NAVARRETE IVAN DANILO
007-09-005-0977	CPU	30/07/2002	742.00				BONILLA PALACIOS MARCO
007-09-005-0985	CPU CLON	30/07/2002	742.00			772	VERDESOTO GARCIA MARIA ELENA
007-09-005-0992	CPU CLON	01/09/2002	573.00			635LA-043-1	CABEZAS JARRIN MARCELO EDUARDO
007-09-005-0994	CPU	10/12/2004	200.00			300	GALARZA YANEZ YOLANDA DEL PILAR
007-09-005-1003	CPU	10/12/2004	200.00	COMPAQ	DESKPRO	F926CCK41205	BODEGA
007-09-005-1010	CPU CLON	02/09/2002	573.00			63524054-1	CALVOPIÑA MOLINA JOSE AUGUSTO
007-09-005-1013	CPU CLON	07/12/2001	624.00			585	BODEGA
007-09-005-1023	CPU CLON	19/06/2002	754.00	INGEINCO	MIDITORRE	2002-0067	AGUILAR MOSCOSO CESAR ANDRES
007-09-005-1028	CPU CLON	01/09/2002	573.00			635L4-056-1	CASTELO LEON MIGUEL ANGEL
007-09-005-1033	CPU CLON	06/07/2001	624.00			574	BODEGA
007-09-005-1040	CPU CLON	10/12/2004	450.00			777	GUANOQUIZA DAVID
007-09-005-1044	CPU	10/12/2004	100.00	COMPAQ	DESKRPO	F738BK522029	BODEGA
007-09-005-1048	CPU SP CLON	01/09/2002	573.00			6365L4-050-1	FERAUD MORAN MARIA CONSUELO
007-09-005-1058	CPU CLON	10/12/2004	400.00			635L4-046-1	TERAN CANO FABIAN EDUARDO
007-09-005-1061	CPU CLON	01/09/2002	573.00			635L4-051-1	BUSTILLOS NOBOA ROBERTO VINICIO
007-09-005-1065	CPU SUPER	01/09/2002	573.00	POWER		635L4-044-1	LATORRE TAPIA LUIS FERNANDO
007-09-005-1074	CPU	10/12/2004	200.00	COMPAQ	DESKPRO	F007DCZ41769	BODEGA
007-09-005-1084	CPU CLON	25/03/2002	676.00			743	GOMEZ VELASQUEZ SEGUNDO RICARDO
007-09-005-1085	CPU CLON	10/12/2004	200.00			387	BODEGA
007-09-005-1094	CPU	10/12/2004	100.00	INTER INSIDE		16070029	BODEGA
007-09-005-1100	CPU	10/12/2004	400.00	INTER INSIDE		388	BODEGA
007-09-005-1106	CPU CLON	01/09/2002	574.00				GONZALEZ PALACIOS TONNY ELIOT

REPORTE ACTIVOS FIJOS - Clase de Activo

Tipo de Activo: EQUIPOS, SISTEMAS Y PAQUETES INFORMATICOS
SubTipo de Activo: EQUIPO PARA PROCESAMIENTO ELECTRONICO DE DATOS
Clase de Activo: C.P.U.

Código	Descripción	Fecha de Adquisición	Valor CH	MARCA	MODELO	Número de Serie	Custodio 1
007-09-005-1117	CPU	10/12/2004	200.00	COMPAQ	DESKPRO	F805BK620226	LUZURIAGA ZURITA MEDARDO ANIBAL
007-09-005-1129	CPU	10/12/2004	700.00	COMPAQ	DESKPRO	6035FR4ZQ616	ALLAUCA AMAGUAYA EDGAR GONZALO
007-09-005-1134	CPU PROLIAN	10/12/2004	2,000.00		ML-370	D049FD61K315	GUERRA LEON DANILO HUMBERTO
007-09-005-1139	CPU CLON	22/05/2002	753.00		MIDITORRE ATX	2002-158	GUERRA LEON DANILO HUMBERTO
007-09-005-1142	CPU CLON	30/07/2002	742.00		SERVIDOR	851	GUERRA LEON DANILO HUMBERTO
007-09-005-1153	CPU	10/12/2004	500.00	COMPAQ	DESKPRO	F007DCZ41043	MARTINEZ MORA JORGE FERNANDO
007-09-005-1156	CPU	10/12/2004	150.00	IBM	SERVER 310	553D80R	BODEGA
007-09-005-1159	CPU CLON	10/12/2004	450.00			737	ZAMBRANO SUAREZ RAMIRO JULIAN
007-09-005-1162	CPU	10/12/2004	400.00	COMPAQ		F926CCK41201	BODEGA
007-09-005-1196	CPU	10/12/2004	10.00	IBM	250	MS70112623152	BODEGA
007-09-005-1197	CPU	10/12/2004	10.00	COMPAQ	PROSIGNIA	6412HJP20057	BODEGA
007-09-005-1208	CPU CLON	07/06/2001	622.00			577	GUERRA LEON DANILO HUMBERTO
007-09-005-1212	CPU	10/12/2004	200.00	COMPAQ	DESKPRO	F007DCZ41035	BODEGA
007-09-005-1220	CPU CLON	30/07/2002	742.00			78	VILLARROEL OCAÑA ANDRES
007-09-005-1227	CPU CLON	12/12/2001	676.00			694	HERRERA RIVADENEIRA HIPATIA DEL RO
007-09-005-1229	CPU SP	10/12/2004	400.00			635S4-047-01	BODEGA
007-09-005-1236	CPU CLON	06/07/2001	622.00			576	BODEGA
007-09-005-1243	CPU	10/12/2004	400.00	COMPAQ	DESKPRO	F020DW441275	BODEGA
007-09-005-1248	CPU CLON	25/03/2002	676.00			742	SEMPERTEGUI ARPI KARLA ALEXANDRA
007-09-005-1253	CPU CLON	01/09/2002	573.00			635L4-052-1	MONAR MORA SUSANA JUDITH
007-09-005-1257	CPU	10/12/2004	400.00			0579	BODEGA
007-09-005-1263	CPU	10/12/2004	140.00		16070029		BODEGA
007-09-005-1278	CPU	10/12/2004	200.00	COMPAQ	DESKPRO	F825BQ340033	BODEGA
007-09-005-1282	CPU	10/12/2004	500.00	COMPAQ	DESKPRO	FO20DW441237	SAONA GUTIERREZ CARLOS EDUARDO
007-09-005-1296	CPU CLON	25/03/2002	676.00			747	RAMIREZ VERDESOTO SILVANA MARIUX
007-09-005-1305	CPU CLON	17/07/2001	624.00			584	BODEGA
007-09-005-1309	CPU CLON	10/12/2004	400.00			301	BODEGA
007-09-005-1312	CPU	01/05/2002	753.00	SUPER POWER	MIDITORRE	2002-066	BODEGA
007-09-005-1323	CPU	01/06/2001	623.00			573	BODEGA
007-09-005-1330	CPU CLON	30/06/2002	742.00		SERVIDOR	776	ENCALADA ALVAREZ SOLEDAD NARCISA

REPORTE ACTIVOS FIJOS - Clase de Activo

Tipo de Activo: EQUIPOS, SISTEMAS Y PAQUETES INFORMATICOS
SubTipo de Activo: EQUIPO PARA PROCESAMIENTO ELECTRONICO DE DATOS
Clase de Activo: C.P.U.

Código	Descripción	Fecha de Adquisición	Valor CH	MARCA	MODELO	Número de Serie	Custodio 1
007-09-005-1335	CPU CLON	01/09/2002	573.00			0635N4-049-1	PEREZ VALLEJO SANDY GIOVANNA
007-09-005-1342	CPU CLON	30/07/2002	742.00			795	MACAS RUIZ JOSE EVARISTO
007-09-005-1348	CPU CLON	12/12/2001	676.00			693	BODEGA
007-09-005-1349	CPU	10/12/2004	400.00			635L4053-1	HERMOZA GUERRA CARLOTA GULNARA
007-09-005-1356	CPU	10/12/2004	200.00	COMPAQ		FOO7DCZ41447	BODEGA
007-09-005-1361	CPU	30/07/2002	742.00	SAMSUNG		771	BODEGA
007-09-005-1372	CPU CLON	06/07/2001	624.00			575	BODEGA
007-09-005-1377	CPU CLON	10/12/2004	400.00			586	REYES SARRIA SYBIL ROCIO
007-09-005-1420	CPU	10/12/2004	300.00	COMPAQ	DESKPRO	F007DCZ41896	BODEGA
007-09-005-1425	CPU CLON	10/12/2004	400.00			302	TORRES REYES ANA MARIA
007-09-005-1432	CPU	10/12/2004	200.00	COMPAQ		FOO7DCZ41440	SAN ANDRES ALVAREZ MARIA FERNANI
007-09-005-1438	CPU	10/12/2004	200.00	COMPAQ	DESKPRO	F007DCZ41449	BODEGA
007-09-005-1447	CPU CLON	10/12/2004	400.00			0760	GUANOQUIZA DAVID
007-09-005-1450	CPU	10/12/2004	200.00	COMPAQ	DESKPRO	F825BQ340023	BODEGA
007-09-005-1461	CPU	10/12/2004	300.00	INTIL INSIDE	CERERON	4161	BODEGA
007-09-005-1469	CPU CLON	10/12/2004	400.00			587	BODEGA
007-09-005-1474	CPU	10/12/2004	200.00	COMPAQ	DESKJET	F007DCZ41112	CHICAIZA ANCHALUIZA EDWIN MANUEL
007-09-005-1481	CPU	10/12/2004	200.00	COMPAQ	DESKPRO	F007DCZ41036	BODEGA
007-09-005-1489	CPU CLON	10/12/2004	450.00			793	ROMERO IBARRA JORGE MARIO
007-09-005-1494	CPU CLON	10/12/2004	400.00			691	MOREIRA VELASQUEZ DARIO
007-09-005-1495	CPU	10/12/2004	450.00		ATX	361	GOMEZ AYALA MARIA FERNANDA
007-09-005-1505	CPU	10/12/2004	200.00	COMPAQ		F007DCZ41805	BODEGA
007-09-005-1511	CPU	10/12/2004	200.00	COMPAQ	DESKPRO	F805BK620801	BODEGA
007-09-005-1517	CPU	10/12/2004	300.00	COMPAQ		FOO7DCZ41912	BODEGA
007-09-005-1519	CPU	10/12/2004	200.00	COMPAQ	DESKPRO	F007DCZ41597	ZAPATA BUSTAMANTE WILSON EDUARD
007-09-005-1524	CPU	10/12/2004	150.00	COMPAQ	DESKPRO	F800B8K620240	ZAPATA BUSTAMANTE WILSON EDUARD
007-09-005-1574	CPU CLON	07/03/2003	525.00				SOLIS RECALDE MARIO LENIN
007-09-005-1579	CPU CLON	07/03/2003	525.00				GUERRA LEON DANILO HUMBERTO
007-09-005-1584	CPU CLON	07/03/2003	525.00				MERCHAN ORTIZ MARIA EUGENIA
007-09-005-1589	CPU CLON	07/03/2003	525.00				MOREJON MANGUI HOLGUER BOLIVAR

REPORTE ACTIVOS FIJOS - Clase de Activo

Tipo de Activo: EQUIPOS, SISTEMAS Y PAQUETES INFORMATICOS
SubTipo de Activo: EQUIPO PARA PROCESAMIENTO ELECTRONICO DE DATOS
Clase de Activo: COMPUTADOR

Código	Descripción	Fecha de Adquisición	Valor CH	MARCA	MODELO	Número de Serie	Custodio 1
007-09-010-0960	COMPUTADOR PORTATIL	09/09/2002	1,995.00	IBM	TRINK PAD		BODEGA
007-09-010-0987	COMPUTADOR	10/12/2004	500.00	COMPAQ ARMADA 175(		3J97CFQSW2D-R	BODEGA
007-09-010-1001	COMPUTADOR PORTATIL	10/12/2004	800.00	COMPAQ	ARMADA E 500	AEST3900T4X20DC1298	CRESPO ZALAMEA ANDRES ROBERTO
007-09-010-1012	COMPUTADOR PORTATIL	08/10/2002	2,000.00	TOSHIBA	2400-S251	62018220P	CARRILLO GILER JORGE EDUARDO
007-09-010-1077	COMPUTADOR PORTATIL	10/12/2004	800.00	COMPAQ 2920B	ARMADA E500	3J11FMZ1C91D	BODEGA
007-09-010-1078	COMPUTADOR DE MANO	10/12/2004	400.00	HEWLETT PACKARD	JORNADA 690	SJ03040068	BODEGA
007-09-010-1079	COMPUTADOR PORTATIL	10/12/2004	800.00	COMPAQ	ARMADA 1750	3J9ACJ23S046	BODEGA
007-09-010-1202	COMPUTADOR	10/12/2004	50.00	COMPAQ	2820D	7308HDJ50066	BODEGA
007-09-010-1203	COMPUTADOR	10/12/2004	20.00	COMPAQ	2820D	7333HDJ51670	BODEGA
007-09-010-1217	COMPUTADORA PORTATIL	10/12/2004	500.00	COMPAQ	2900C	V724BQGN1905	BODEGA
007-09-010-1430	COMPUTADOR DE MANO	10/12/2004	400.00	HEWLETT PACKARD	JORNADA-690	SG02900253	BODEGA
007-09-010-1431	COMPUTADOR DE MANO	10/12/2004	400.00	HEWLETT PACKARD	JORNADA-690	SG03000100	BODEGA
007-09-010-1484	COMPUTADOR PORTATIL	10/12/2004	800.00	COMPAQ	ARMADA 1750	BJ9ACJ23S26J	CABEZAS JARRIN MARCELO EDUARDO
007-09-010-1600	COMPUTADOR PORTATIL	31/03/2003	1,754.00	COMPAQ		1V2CLDL2B45B	BUSTILLOS NOBOA ROBERTO VINICIO
007-09-010-1935	COMPUTADOR PORTATIL	05/05/2004	1,652.63	HP EVO	NX9010	CNF4130FK5	MEDINA ACOSTA MARIO WILDEMBER
007-09-010-2021	COMPUTADOR PORTATIL	25/01/2005	1,560.00	HP	COMPAQ9010	CNF4330NCY	RUIZ ZURITA RUBEN ALFREDO
007-09-010-2045	COMPUTADOR PORTATIL	15/11/2005	1,312.49	GATEWAY	CX2610	7155901001075	VEGA DELGADO ARMANDO GUSTAVO
007-09-010-2048	COMPUTADOR	15/12/2005	2,372.00	SONY VAIO	VGN-TX650FP	261990404100366	TONON PEÑA LUIS ENRIQUE
007-09-010-2051	COMPUTADOR PORTATIL	11/02/2006	2,354.00	SONY VAIO	PCG-4FIP	J0016MVX	GUERRA LEON DANILO HUMBERTO
007-09-010-2052	COMPUTADOR PORTATIL	28/07/2006	1,032.00	TOSHIBA	M100-SP1011	56168589K	CABEZAS JARRIN MARCELO EDUARDO
007-09-010-2053	COMPUTADOR PORTATIL	28/07/2006	1,032.00	TOSHIBA	M100-SP1011	56168646K	MERCHAN ORTIZ MARIA EUGENIA
007-09-010-2054	COMPUTADOR PORTATIL	28/07/2006	1,032.00	TOSHIBA	M100-SP1011	56168724K	CARRILLO GUZMAN OSWALDO WLADI
007-09-010-2055	COMPUTADOR PORTATIL	28/07/2006	739.03	NOTEBOOK ECS	EM-G320125	96F61000061Q54800110	AVILA LOOR MANUEL
007-09-010-2056	COMPUTADOR PORTATIL	28/07/2006	945.00	NOTEBOOK DELL	15JS531	0DK344-70166-65F03QM	LATORRE TAPIA LUIS FERNANDO
007-09-010-2057	COMPUTADOR PORTATIL	09/04/2007	1,739.00	HP	NX-6320	CNU6450V76	ORDOÑEZ CHAVEZ MARIA MILAGROS
			26,989.15				

ANEXO II

ENCUESTA DE EMPLEADOS IT

Encuesta de empleados IT

PRACTICAS	ESTAS PRACTICAS SON USADAS POR LA ORGANIZACION		
CONOCIMIENTO DE SEGURIDAD Y ADIESTRAMIENTO			
Los miembros del personal entienden sus roles de seguridad y responsabilidades?. Es ésta documentada y verificada?	SI	NO	DESCONOCE
Existen adecuadas experiencias internas para todos los servicios soportados, mecanismos y tecnologías (ej. Login, monitorio o encriptacion), incluyendo sus operaciones seguras, es documentada y verificada?	SI	NO	DESCONOCE
El conocimiento de la seguridad, entrenamiento, y recordatorios periódicos son provistos para todo el personal. Se documenta lo que el personal entiende y la conformidad se verifica periódicamente.	SI	NO	DESCONOCE
ESTRATEGIAS DE SEGURIDAD			
Las estrategias del negocio de la organización rutinariamente incorporan consideraciones de seguridad	SI	NO	DESCONOCE
Las estrategias de seguridad y las políticas se basan en las estrategias del negocio de la organización y metas	SI	NO	DESCONOCE
Las estrategias de seguridad, metas y objetivos son documentados y son rutinariamente revisados, actualizados y comunicados a la organización	SI	NO	DESCONOCE
ADMINISTRACIÓN DE LA SEGURIDAD			
La administración designa suficiente fondos y recursos a actividades de seguridades de información	SI	NO	DESCONOCE
Los roles de la seguridad y responsabilidades son definidas para todo el personal en la organización	SI	NO	DESCONOCE
Los contratos de la organización y las practicas de terminación del contrato para el personal toma en cuenta problemas de seguridad en la información	SI	NO	DESCONOCE
La administración de los riesgos de seguridad de la información incluyen: Riesgos de acceso a la seguridad de la información Toman acciones para mitigar riesgos de la seguridad de la información	SI	NO	DESCONOCE

La gerencia recibe y actúa sobre reportes de rutina que resumen situaciones relacionadas con la seguridad de la información (auditorias, logs, riesgos y valoraciones de vulnerabilidades)	SI	NO	DESCONOCE
REGULACIONES Y POLÍTICAS DE SEGURIDAD			
La organización tiene un conjunto comprensivo de documentación de las políticas actuales que son periódicamente revisadas y actualizadas.	SI	NO	DESCONOCE
Existe un proceso de documentación para la administración de políticas de seguridad que incluya: Creación Administración (incluyendo las revisiones periódicas y actualizaciones) Comunicaciones	SI	NO	DESCONOCE
La organización tiene un proceso de documentación para evaluar y asegurar la satisfacción con las políticas de seguridad en la información , leyes aplicables y regulaciones, y requerimientos de seguridad	SI	NO	DESCONOCE
La organización asegura uniformemente estas políticas de seguridad	SI	NO	DESCONOCE
ADMINISTRACIÓN COLABORATIVA DE LA SEGURIDAD			
La organización tiene políticas y procedimientos para protección de la información cuando trabaja con organizaciones externas (ej. Proveedores, colaboradores, subcontratistas, o socios), incluyendo: Protección de la información que pertenece a otras organizaciones Entendimiento de las políticas de la seguridad y procedimientos de organizaciones externas Límites de acceso a la información por parte del personal externo	SI	NO	DESCONOCE
La organización ha verificado que los servicios de seguridad externos, mecanismos y tecnologías reunen sus necesidades y requerimientos	SI	NO	DESCONOCE
PLANIFICACIÓN DE LA CONTINGENCIA / RECUPERACIÓN DE DESASTRES			
Un análisis de operaciones, aplicaciones y datos críticos se ha realizado	SI	NO	DESCONOCE
La organización a documentado, revisado y probado: La continuidad del negocio o planes de operación de emergencia Planes de recuperación de desastres	SI	NO	DESCONOCE

Planes de contingencia para responder a las emergencias			
La contingencia, recuperación de desastres y planes de continuación del negocio consideran acceso físico y electrónico y de controles	SI	NO	DESCONOCE
Todo el personal esta: Consciente de la contingencia Recuperación del desastre, y planes para continuar el negocio Entiende y esta capacitado con sus responsabilidades	SI	NO	DESCONOCE
SEGURIDADES FÍSICAS Y PROCEDIMIENTOS			
Los planes para facilitación de seguridad y procedimientos para salvaguardar las premisas, edificios y algunas áreas de acceso restringido son documentadas y probadas	SI	NO	DESCONOCE
Existen políticas documentadas para manejar visitantes	SI	NO	DESCONOCE
Existen políticas documentadas para el control físico de hardware y software	SI	NO	DESCONOCE
CONTROL DE ACCESO FISICO			
Existen políticas y procedimiento para controlar el acceso físico a las áreas de trabajo y hardware (computadora, dispositivos de comunicación, etc) y software	SI	NO	DESCONOCE
Las estaciones de trabajo y otros componentes que permiten acceso a información sensitiva estan físicamente protegido para prevenir accesos no autorizados	SI	NO	DESCONOCE
MONITOREO Y AUDITORIA DE SEGURIDAD FISICA			
Se guardan los archivos de mantenimiento para documentar las reparaciones y modificaciones de componentes físicos	SI	NO	DESCONOCE
Una acción individual o grupal con respecto a los controles de los dispositivos físicos se considera	SI	NO	DESCONOCE
Los archivos de auditoria y mantenimiento son rutinariamente examinados para buscar anomalías y tomar acciones correctivas de ser necesario.	SI	NO	DESCONOCE
ADMINISTRACIÓN DE RED Y SISTEMAS			
Existen documentados y probados planes de seguridad para salvaguardar los sistemas y las redes	SI	NO	DESCONOCE
La información sensitiva es protegida por almacenamiento seguro (backup almacenamiento fuera del lugar)	SI	NO	DESCONOCE
La integridad del software instalado es regularmente verificada	SI	NO	DESCONOCE

Todos los sistemas están actualizados y con las respectivas revisiones, parches y con las recomendaciones propuestas de seguridad	SI	NO	DESCONOCE
Existen planes documentados y probados del respaldo de datos para backups de software y datos. Todo el personal entiende sus responsabilidad en estos planes	SI	NO	DESCONOCE
Los cambios en el hardware y software para el IT son planificados controlados y documentados	SI	NO	DESCONOCE
El personal miembro de la IT sigue procedimientos cuando se emiten, cambian y expiran los passwords de usuarios, cuentas y privilegios. Identificación única de usuario es requerida para todos los sistemas de información incluyendo usuarios tercerizados Los usuarios y cuentas por defecto han sido removidas del sistema	SI	NO	DESCONOCE
Solamente servicios necesarios corren en los sistemas, todos los servicios innecesarios han sido removidos	SI	NO	DESCONOCE
HERRAMIENTAS DE ADMINISTRACIÓN DE SISTEMAS			
Las herramientas y mecanismos para asegurar sistemas y la administración de redes son usados, y son rutinariamente revisados y actualizados o reemplazados	SI	NO	DESCONOCE
MONITOREO Y AUDITORIA DE LAS SEGURIDADES DEL IT			
Los sistemas y monitoreo de redes y herramientas de auditorio son rutinariamente usados por la organización. Las actividades inusuales son atacadas con políticas apropiadas y procedimientos	SI	NO	DESCONOCE
Firewalls y otros componentes de seguridad son periódicamente auditados para saber si están de acuerdo con la política	SI	NO	DESCONOCE
AUTENTICACIÓN Y AUTORIZACIÓN			
Los controles de acceso apropiado y autenticación de usuarios (permiso de archivos, configuración de redes) consistentes con las políticas son usados para restringir el acceso a usuarios a la información, sistemas sensitivos, servicios y aplicaciones específicas, y conexiones de red	SI	NO	DESCONOCE
Existen políticas documentadas para establecer y dar por terminado los derechos y acceso a la información ya sea de individuos o grupos	SI	NO	DESCONOCE
Métodos o mecanismos son provistos para asegurar que la información sensitiva no haya sido accesada, alterada o destruida de alguna manera inautorizada. Estos métodos y	SI	NO	DESCONOCE

mecanismos son periódicamente revisados y verificados			
ADMINISTRACIÓN DE LAS VULNERABILIDADES			
Existen conjuntos de documentos o procedimientos para manejar las vulnerabilidades incluyendo: Seleccionar herramientas de evaluación de vulnerabilidades, checklist y scripts Mantenerse actualizado con el conocimiento de los tipos de vulnerabilidades y ataques Revisión de las fuentes de información o anuncios de vulnerabilidades, alerta de seguridades y noticias Identificación de los componentes de la infraestructura a ser evaluados Planificación de evaluación de vulnerabilidades Interpretación y respuesta a los resultados Almacenamiento y mantenimiento seguro de los datos vulnerables	SI	NO	DESCONOCE
Los procedimientos del manejo de vulnerabilidades son periódicamente revisados y actualizados	SI	NO	DESCONOCE
Las variaciones de las vulnerabilidades tecnológicas son realizadas sobre un período base y las vulnerabilidades son direccionadas cuando se las verifica	SI	NO	DESCONOCE
ENCRIPTACIÓN			
Controles de seguridad apropiados son usados para proteger información sensitiva mientras esta almacenada y durante la transmisión (ej. Encriptación de datos, infraestructura de clave publica, tecnología de vpns)	SI	NO	DESCONOCE
Protocolos de encriptación son usados cuando se administran sistemas remotamente: ruteadores y firewalls	SI	NO	DESCONOCE
ARQUITECTURA DE SEGURIDAD Y DISEÑO			
Los sistemas de arquitectura y diseño para los sistemas nuevos y revisados incluye las siguientes consideraciones Estrategias de seguridad, políticas y procedimientos Histórico de compromisos de seguridad Resultados de valoración de riesgos de seguridad	SI	NO	DESCONOCE
La organización mantiene diagramas actualizados que muestren la arquitectura de seguridad y la topología de la red de la empresa	SI	NO	DESCONOCE
MANEJO DE INCIDENTES			

Existen procedimientos documentados para identificar, reportar y responder a incidentes sospechosos de seguridad y violaciones	SI	NO	DESCONOCE
Los procedimientos del manejo de incidentes son periódicamente probados verificados y actualizados	SI	NO	DESCONOCE
Existen procedimientos de políticas documentadas para trabajar con agencias legales	SI	NO	DESCONOCE
PRACTICAS GENERALES DEL PERSONAL			
Los miembros del personal siguen buenas practicas de seguridad tales como Aseguran la información del cual ellos son responsables No divulgan información sensitiva a otros (resistencia a la ingeniería social) Tienen la habilidad adecuada para usar información tecnológica, hardware y software Usan buenas practicas para los passwords Entienden y siguen las políticas de seguridad y regulaciones Reconocen y reportan incidentes	SI	NO	DESCONOCE
Todo el personal en todos los niveles de responsabilidades implementan sus roles asignados y la responsabilidad para la seguridad de la información	SI	NO	DESCONOCE
Existen procedimientos documentados para autorizaciones y vigilancia de todo el personal (incluyendo personal tercerizado) el cual trabaja con información sensitiva o el cual trabaja donde la información recibe	SI	NO	DESCONOCE

ANEXO III

CARACTERISTICAS Y PRECIOS DE PROVEEDORES

CARACTERÍSTICAS Y PRECIOS DE PROVEEDORES

UPS

Descripción: SmartOnline SU10KRT3U – SU10KRT3UHV (6kVA & 10kVA)

Características:	
Output Capacity (VA/Watts)	10000/7000
Backup Time (typical Minutes) Half/Full load	20/8+
Rack Space	3U (power module) 3U (battery module)
Runtime (minutes) with additional external battery modules	5 battery (156/74)

Costo:

EMPRESA	PRECIO
A	6.920,00
B	7.750,00
C	5.650,90
PROMEDIO	**6.774,30**

Descripción: Powerware 9140 7500VA OL UPS-IEC309-60A C19 6U

Características:	
Rango de Potencia	10kVA/8kW y 7.5kVA/6 kW Entrada Monofásico/Salida Monofásica Entrada Trifásica/Salida monofásica (Versión manual elegible en HW)
Entrada de Tensión Nominal	1/1:230Vac (200-240 Vac) 3/1: 400/230Vac
Salida de Tensión Nominal	208 o 230 Vac, auto-sensitivo (200-240Vac)
Frecuencia	50/60 Hz (auto-sensitivo)
Configuración	Online, doble-conversión; rackmount en 6U incluyendo baterias

Costo:

EMPRESA	PRECIO
A	4.035,85
B	3.477,75
C	3.520,95
PROMEDIO	**3.678,19**

ROUTER

Descripción: CISCO 1841 WIC DSU T1 V2 IP BASE

Características:	
Fabricante	Cisco
Arquitectura de Red Compatible	Ethernet-10 Mbps Twisted Pair (10BaseT), Ethernet-100Mbps Two-Pair (100BaseTX), Gigabit Ethernet-1000Mbps (1000BaseTX)
Número de puertos	4
Características Generales	DHCP Client Functionality, Integrated Firewall, IP Routing, IPSec, NAT, Uplink, VoIP
Memoria Flash Instalada	32 MB
Protocolos de Red	DHCP, DNS, FTP, http, SMTP, SNMP, TCP/IP, TELNET
Memoria principal instalada	128 MB
Velocidad	1 Gbps

Costo:

EMPRESA	PRECIO
A	2.061,25
B	1.943,98
C	2.054,98
PROMEDIO	**2.020,07**

FIREWALLS

Descripción: Kypus Server Appliance Model 500-250 usuarios

Características:	
From Factor	1U Rackmount Server
Network Interfaces	Two Ethernet autosensing 10/100/1000 Base T
Port	Trunking and Fallover
Processor	Intel Pentium4 2.8Ghz FSB 533 Mhz
RAM Memory	1Gbytes up 2 Gbytes DDR266
Flash Memory	128 Mb
Power Supply	200 Watts, Auto-switching 100/240 AC power
Software	Propietary Linux Embedded O.S. (KOS), Firewall Web Caching proxy

	with Content Filtering, Application Control (P2P), Mall Server with spam and virus cheking, DNS, FTP, LDAP, IDS/IPS, DHCP, SNMP, Webmail, VPN (IPSec and PPTP) File and Print Server, Smart Reports, Bandwidth control (QoS) Web Server with Virtual Host support 1 año de actualizaciónes, antivirus y listas negras

Costo:

EMPRESA	PRECIO
A	2.950,00
B	3.050,00
C	5.000,00
PROMEDIO	**3.666,66**

INSTALACIÓN Y CAPACITACION DEL FIREWALL

Costo:

EMPRESA	PRECIO
A	900,00
B	600,00
C	800,00
PROMEDIO	**766,66**

SWITCH CAPA 2

Descripción: CISCO CATALYST 2960 24 10/100 + 2 10/100/1000 LAN - BASE

Características:	
Fabricante	Cisco
Arquitectura de Red	Ethernet – 100 Mbps Two-Pair (100BaseTX) Ethernet – 10Mbps Twisted Pair (10BaseT) Gigabit Ethernet – 1000 Mbps (1000BaseTX)
Número de Puertos	24
Características Generales	Auto-Negotiation, Auto-Sensing Per Device, Flow Control, Rack-mountable, Stackable, Uplink
Modo de comunicación	Full – Duplex

	Half – Duplex
Memoria principal instalada	64 MB
Tipo de Switch	LAN Switch
Velocidades	10, 100, 1000 Mbps

Costo:

EMPRESA	PRECIO
A	1.043,33
B	1.150,29
C	1.050,99
PROMEDIO	**1.081,53**

Descripción: 3Com 3CR17402-91 Switch 3848

Características:	
Fabricante	3Com
Arquitectura de Red	Ethernet, Fast Ethernet, Gigabit Ethernet
Número de Puertos	48

Costo:

EMPRESA	PRECIO
A	2.618,75
B	2.093,75
C	2.562,50
PROMEDIO	**2.425,00**

SWITHC CAPA 3

Descripción: 3Com Switch 5500G-EI 24 Port 10/100/1000

Características:	
Fabricante	3Com
Arquitectura de Red	Ethernet, Fast Ethernet, Gigabit Ethernet
Número de puertos	24
Características Generales	Autonegociable Alimentación en línea
Sistema Operativo	Sistema operativo de 3Com, compartido con los 3Com Switch 8800, 7700 y Router 6000
Administración de 3Com	3Com Network Supervisor, 3Com Network Director, 3Com Enterprise Management Suite

Herramientas de depuración de red	Tracker DHCP, helper UDP, traceroute mirroring de puerto 1 a 1 (solo unidad independiente)
Fuente de alimentación integrada	50/60 Hz AC; entrada a 90-240 VAC soporta múltiples modos de alimentación: sólo AC, AC y DC y sólo DC
Velocidad	10/100/1000 Mbps

Costo:

EMPRESA	PRECIO
A	3.712,00
B	3.836,23
C	3.806,23
PROMEDIO	**3.784,82**

IPS

Descripción: 3Com XS RTR IPS 2Su Tipping Point

IPS continuamente limpia la red de tráfico malicioso, incluyendo gusanos, virus, trojanos, spyware, amenazas de VoIP

Costo:

EMPRESA	PRECIO
A	954,26
B	925,73
C	949,93
PROMEDIO	**943,30**

CABLEADO

Descripción: Cableado categoría 6

Características:	
Generales	Específicas para crosstalk y ruido 10 Base-T, 100Base-TX, 1000Base-TX
Performances	Hasta 250 Mhz

Costo:

EMPRESA	PRECIO POR INSTALACIÓN DE PUNTO
A	45,00
B	100,00
C	60,00
PROMEDIO	**68,33**

SERVIDORES PUBLICOS

Descripción: HP PROLIANT ML370 G5 5U RACK MOUNTABLESERVER

Características:	
Fabricante	Hewlett Packard
Tipo de procesador	Intel Xeon Dual - Core
Memoria instalada	2 GB
Número máxima de procesador/instalados	2/1
Velocidad	2.33
Número de slots de memoria	2
Sockets de memoria	DIMM
Memoria máxima del sistema	64 GB
Driver Controllers	IDE/EIDE Drive Array (Raid) Serial ATA
Tamaño de cache	4 MB
Velocidad del Bus	1.33 Mhz
System Chipset	Intel 5000 P chipset
Número de Discos	4
Soporta Raid	Raid 0, 1, 5

Costo:

Empresa	Precio
A	7.048,75
B	6.788,75
C	6.644,68
PROMEDIO	**6.827,39**

SERVIDORES DE BASE DE DATOS Y APLICACIONES - ARCHIVOS

Descripción: (2) HP ML570 G4 3.4 GHZ HIGH PERFORMANCE RACK SERVER

Características:	
Fabricante	Hewlett Packard
Tipo de procesador	Intel Xeon Dual - Core
Memoria Estándar	2 GB
Tipo de memoria	PC2-3200 DDR2
Storage Controller	HP Smart P400 Controller
Cache Procesador	16 MBL3
Memoria máxima del sistema	64 GB
Max front side Bus	800 Mhz
Networking	HP Dual embedded NC371i Multi-function Gigabit network adapter
Rack height	6 U
Número de Discos	4
Max Internal Drivers	18

Costo:

EMPRESA	PRECIO
A	17.122,50
B	17.223,75
C	16.640,00
PROMEDIO	**16.995,41**

ANTIVIRUS

Descripción: Symantec Norton Antivirus

Costo:

EMPRESA	PRECIO
A	54,00
B	60,00
C	75,00
PROMEDIO	**63,00**