



UNIVERSIDAD DE ORIENTE
NÚCLEO DE SUCRE
ESCUELA DE CIENCIAS
DEPARTAMENTO DE MATEMÁTICAS
PROGRAMA DE LA LICENCIATURA EN INFORMÁTICA

DESARROLLO DE UN PLAN DE GESTIÓN DE LOS SERVICIOS
TELEINFORMÁTICOS DEL PROGRAMA DE LA LICENCIATURA EN
INFORMÁTICA, DEPARTAMENTO DE MATEMÁTICAS, ESCUELA DE CIENCIAS, NÚCLEO
DE SUCRE, UNIVERSIDAD DE ORIENTE.

(Modalidad: Investigación)

Malvina José González Mistage

TRABAJO DE GRADO PRESENTADO COMO REQUISITO PARCIAL
PARA OPTAR AL TÍTULO DE LICENCIADA EN INFORMÁTICA

CUMANA, 2010

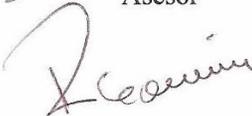
DESARROLLO DE UN PLAN DE GESTIÓN DE LOS SERVICIOS
TELEINFORMÁTICOS DEL PROGRAMA DE LA LICENCIATURA EN
INFORMÁTICA, DEPARTAMENTO DE MATEMÁTICAS, ESCUELA DE
CIENCIAS, NÚCLEO DE SUCRE, UNIVERSIDAD DE ORIENTE.

(Modalidad: Investigación)

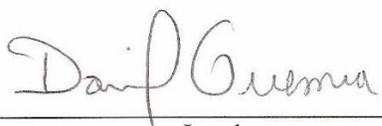
APROBADO POR:



Prof. Hugo Marciano
Asesor



Jurado



Jurado



INDICE

ÍNDICE	iii
DEDICATORIA	i
AGRADECIMIENTO	ii
LISTA DE CUADROS	iii
LISTA DE FIGURAS	iv
RESUMEN	v
INTRODUCCIÓN	1
CAPÍTULO I	4
PLANTEAMIENTO DEL PROBLEMA	4
1.1 Planteamiento del Problema	4
1.2 Alcance y Limitaciones	5
1.2.1 Alcance	5
1.2.2 Limitaciones.....	6
CAPÍTULO II	7
MARCO REFERENCIA	7
2.1 MARCO TEÓRICO	7
2.1.1 Antecedentes Investigación	7
2.2 MARCO METODOLÓGICO	44
2.2.1 Metodología de la investigación	44
2.2.2 Nivel de investigación.	45
2.2.3 Tipo de investigación.....	45
2.2.4 Técnicas de recolección de datos.....	45
2.2.4 Metodología del área aplicada	46
CAPÍTULO III	49
DESARROLLO	49
3.1 Determinación de las necesidades de la planificación.....	49

3.2 Recopilación de Información relevante	51
3.2.1 Análisis de herramientas para el monitoreo de red	51
3.2.2 Análisis de las herramientas para la documentación de red	52
3.3 Identificación de los requisitos	54
3.4 Diseño del modelo de planificación para la gestionar la red	60
3.5 Documentación de la red	63
3.6 Monitoreo de red	65
3.6.1 Análisis del tráfico de la red	73
3.7 Definición de las políticas de red.....	77
3.7.1 Seguridad Lógica.	78
3.7.2 Seguridad Física.....	84
3.8 Definición del plan de gestion	87
CONCLUSIONES	104
RECOMENDACIONES	105
BIBLIOGRAFÍA	106
ANEXOS.....	109
HOJA DE METADATOS.....	172

DEDICATORIA

El esfuerzo y dedicación realizada en este largo recorrido lleno de tropiezos y dedicación va dirigido a:

Dios y a la Virgen del Valle

mis padres

mis hermanos, Rafael, Herminia y Antonio

mis queridos sobrinos

mis amigas de siempre Yamilet e Ysmenia

mis compañeros de estudio, Jacqueline, Mercedes, Nakary, Angel y Carlos
Cruz

AGRADECIMIENTO

La culminación de este trabajo se ha realizado gracias al esfuerzo y dedicación de muchas personas que colaboraron de forma directa e indirectamente para hacer posible este trabajo. Es por ello que quiero expresar mis más sincero y humildes agradecimientos a todos ellos es especial a:

La ilustre Universidad de Oriente

La Coordinación del Programa de la Licenciatura en Informática por su apoyo a la realización de este trabajo.

Profesor y asesor Hugo Marcano, por su dedicación y valiosa contribución para la culminación de este trabajo. Gracias!.

El profesor Daniel Geremia, quien permitió y aportó todo lo que estuvo a su alcance.

Los técnicos y administradores del Laboratorio de Informática especialmente a Antonio, por su entrega y colaboración.

LISTA DE CUADROS

Tabla 1. Tabla comparativa de herramientas de monitoreo de red	51
Tabla 2. Tabla comparativa de herramientas para inventario de red	52
sistema actual de	59
Tabla 3 Resumen información monitoreada	74
Tabla 4 Resumen del Plan de gestión para la red del Programa de la Licenciatura en Informática	102
Tabla N° 5 . Normas o métricas para evaluar plan de gestión de la red del Programa de la Licenciatura en Informática.....	103

LISTA DE FIGURAS

Figura 1. Diagrama de flujo de datos del sistema actual de administración de la red del programa de la licenciatura en informática.....	57
Figura 3. Diagrama de flujo de datos expandido del proceso 1.0 del sistema actual de Administración de la red del programa de la licenciatura en informática ...	59
Figura 4. Diagrama de datos del sistema propuesto para la administración de los servicios de red del programa de la licenciatura en informática.....	61
Figura 5. Diagrama de datos expandido del sistema propuesto para la administración de los servicios de red del programa de la licenciatura en informática	62
Figura 6. Diagrama Lógico de la estructura de red del programa de la licenciatura en informática.....	65
Figura 7. Página de inicio de la aplicación Wireshark	66
Figura 8. Página de inicio para capturar trafico con la aplicación Wireshark...	68
Figura 9. Pagina de captura de tráfico con la aplicación Wireshark	69
Figura 10. Pagina de captura de tráfico con la aplicación Wireshark	70
Figura 11. Pagina de captura de tráfico con la aplicación Wireshark	71
Figura 12. Pagina de captura de tráfico con la aplicación Wireshark	72
Figura 13. Pagina para filtrar información con la aplicación Wireshark.....	73
Figura 14. Pagina se selección del filtro usando la aplicación Wireshark.....	73
Figura 15 . Cantidad de trafico monitoreado.....	75
Figura 16 Tasa se transferencia monitoreada	76

RESUMEN

Dado el continuo crecimiento de las redes y el auge tecnológico en las últimas décadas, ha surgido la necesidad de buscar herramientas que apoyen la gestión de redes de forma integrada y automática. En el presente trabajo se desarrolló un plan de gestión para los servicios teleinformáticos de la red del Programa de la Licenciatura en Informática del núcleo de Sucre de la Universidad de Oriente, el cual permite a los administradores de red realizar labores de gestión a la red local. Para la elaboración del plan de gestión se implementó la metodología Métrica[1], la cual permitió determinar las necesidades de planificación e identificar los requisitos, para ello fue necesario realizar entrevista que proporcionaron la información sobre los procesos que se ejecutaban en la red, lo que ayudó a conocer las actividades de administración y a determinar los requisitos necesarios tomándose en cuenta las áreas funcionales para la gestión de redes (configuración, avería, desempeño y seguridad) . Esto permitió diseñar un plan de gestión para la red del Programa de la Licenciatura de Informática, que permitiera mejorar los procesos de administración, se propusieron procesos como monitoreo, documentación automatizada, políticas de seguridad, entre otras como actividades primordiales para gestionar la red. Para el diseño también se tomó en cuenta la administración de red que implementa el programa Networking Cisco, el cual ayudó a determinar cómo debe implementarse la documentación y proporcionar seguridad a la red en estudio. El desarrollo de este plan de gestión permitió mejorar los servicios que se ofrecen en la red y proporcionar herramientas de gestión que apoyen las funciones que cumplen los administradores y técnicos de la red, brindando a los usuarios una red eficiente, óptima y segura.

INTRODUCCIÓN

El surgimiento de las nuevas tecnologías y la necesidad del ser humano de comunicarse, han permitido el incremento en el uso y desarrollo de las redes de comunicación, haciéndolas indispensables para las empresas e instituciones [2].

Las redes fueron desarrolladas inicialmente para compartir dispositivos costosos pero a medida que fueron creciendo se crearon nuevas ventajas que permitieron mejorar su funcionamiento dificultando el mantenimiento de las misma, lo que estimulo la necesidad de gestionar las redes, es decir, controlar los recursos que la componen en función de desempeño, capacidad, utilización, diagnostico y planificación [3].

La gestión de redes está definida como un conjunto de técnicas que tienden a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada [3]. La administración de redes es la herramienta necesaria para mantener una red en óptimo funcionamiento. Sin embargo, en la actualidad existen redes que han sido puestas en funcionamiento ignorándose su proceso de administración, produciendo ineficiencia y bajos niveles de rendimiento en sus servicios, así como poca disponibilidad para sus usuarios. Tal como ocurre en la red que funciona en el edificio de matemáticas para el Programa de la Licenciatura en Informática del Núcleo de Sucre de la Universidad de Oriente.

En el Programa de la Licenciatura en Informática del núcleo de Sucre de la universidad de oriente están centralizadas todos los aspectos académico – administrativo de la carrera de la Licenciatura en Informática. Su sede está ubicada en el edificio de matemática y tiene como función velar por la formación académica de sus estudiantes. La licenciatura en informática cuenta con una red de computadoras

que comprende oficinas administrativas y docentes, además de cuatro laboratorios que ofrecen distintas herramientas, aplicaciones y servicios para desarrollar actividades prácticas del pensum de estudio.

Dentro de los servicios que se ofrecen en la red en estudio se tienen: el préstamo de equipos, impresión de documentos, servicio de internet, etc. El presente trabajo de grado busca mejorar los servicios que se ofrecen en la red en estudio, para lograrlo se desarrolló un plan de gestión que se adapte a las necesidades que presenta la red.

Para desarrollar el plan de gestión que garantice una red funcional, con una planeación adecuada y propiamente documentada que aporte beneficios a los usuarios del Programa de la Licenciatura en Informática se buscó obtener un marco referencial que respondiera a las necesidades de la institución y de sus usuarios.

En la elaboración del plan de gestión se analizaron las necesidades de información de los procesos de gestión de red, con el fin de definir los requisitos generales y obtener modelos conceptuales de información que recopilen todo los requisitos que sean considerado necesario para diseñar el modelo de planificación que permitiera gestionar la red de forma óptima y eficiente; Dentro de las necesidades se encontraron: conocer el tráfico que circula por la red, documentación de la red, dispositivos de red como servidores, políticas de seguridad, entre otras.

Tomado en cuenta los procesos actuales y las necesidades de la red en estudio se diseñó un modelo de gestión que permitiera un mejor control y administración de la red del Programa de la Coordinación de la Licenciatura de Informática, que proporcionara mayor seguridad a los usuarios en cuanto acceso y almacenamiento de información y disponibilidad de los recursos. Además, dado que la estructura detallada de la red quedaría guardada en una documentación clasificada, sería fácil

resolver problemas de unidades particulares con base a los registros de similares características.

Una vez diseñado el modelo de gestión se dio inicio a los procesos de gestión, como son los de monitoreo del tráfico, documentación de la red y definición de políticas de seguridad, los cuales son herramientas indispensables para mantener un mejor control sobre los dispositivos y así brindar un mejor servicio a los usuarios de la red.

La estructura del presente trabajo se divide de la siguiente manera:

Capítulo I. Presentación: En esta sección se describe la situación actual de la red del programa de la licenciatura en informática. Se expresa la problemática planteada, los alcances y las limitaciones.

Capítulo II. Marco Referencial. En este capítulo se presentará los antecedentes que apoyen la investigación así como los antecedentes de la organización. Además se presenta una visión general de los aspectos teóricos involucrados con gestión de redes.

Capítulo III. Desarrollo: Suministrar una descripción de los objetivos que fueron planteados para desarrollar el plan de gestión de la red del programa de la licenciatura en informática.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 Planteamiento del Problema

La plataforma de red instalada en la Coordinación de la Licenciatura en Informática de la Universidad de Oriente del Núcleo de Sucre no cuenta con ningún proceso de gestión que suministre un nivel de control sobre los dispositivos que la conforman, razón por la cual se presentan una serie de problemas relacionados con la falta de administración de la red, la cual deben ser atendidos y solucionados para así apoyar las labores de gestión.

Dentro de los problemas que se presentan se tiene:

Retrasos en el diagnóstico de fallas debido a la ausencia de procesos de observación que permitan conocer el comportamiento o desempeño de la red para así detectar y corregir fallas que ayuden a brindar un mejor control para el funcionamiento de la red.

Documentación deficiente de la red que impide brindar información detallada y estado operativo de los dispositivos que conforman la red.

Ausencia de políticas de seguridad para el control de acceso y recuperación de información ante un evento crítico, generando así una red insegura a los usuarios.

La falta de dispositivos indispensable para el buen funcionamiento de una red, como son los servidores de nombre de dominio (*Domain Name System*, DNS) los cuales aportarían una mayor seguridad y disponibilidad de la red.

Con la finalidad de lograr mejoras significativas en los niveles de servicios ofrecidos a la comunidad universitaria se hace necesario el desarrollo de un plan de gestión para la red del Programa de la Licenciatura en Informática que permita solucionar los problemas presentados y así brindar un mejor servicio a los usuarios de la red, mejorando el tiempo de respuesta y diagnosticando las fallas a tiempo.

1.2 Alcance y Limitaciones

1.2.1 Alcance

El presente trabajo de grado esta centralizado en el desarrollo de un plan de gestión para la red del Programa de la Licenciatura de Informática, lo cual ayudará a los administradores y técnicos a establecer un nivel de control sobre los dispositivos que conforman la red, proporcionando una red operativa, segura y eficiente a sus usuarios.

El desarrollo del plan de gestión para los servicios teleinformáticos de la red del Programa de la Licenciatura en Informática permitirá:

Mejorar la operatividad de la red a través de mecanismos apropiados para el control, monitoreo y suministros de los recursos.

Hacer mejor uso de la red y utilizar mejor los recursos.

Conocer el estado (activo/inactivo) de los dispositivos que operan en la red en estudio.

Conocer el comportamiento de la red a través del monitoreo del trafico, para así

establecer estándar de rendimiento que sirvan como línea de base para comparar y generar alarmas en caso de que se produzca un evento crítico.

Obtener información de los dispositivos que conforman la red y mantener un registro de fallas y reparaciones que contribuyan al rápido y efectivo acomodo del dispositivo.

Los usuarios contarán con una red segura que cumplan con políticas y mecanismos de seguridad.

1.2.2 Limitaciones

Dentro de los obstáculos que se presentaron en la ejecución del presente trabajo de grado se encuentra la falta de información de la estructura de la red en estudio, la cual no fue planificada en el momento de su creación, razón por la cual no se cuenta con un diseño lógico y físico que brinde conocimiento de cómo está estructurada. Para enfrentar esta limitante se hizo un levantamiento de información sobre la estructura de la red que permitió obtener información necesaria para el desarrollo del plan de gestión de la red.

Otra limitación es la dependencia que existe en la red del Programa de la Licenciatura en Informática con el Departamento de Computación Académica, la cual es la encargada de brindar la conexión a la red, lo que restringe el control de algunos servicios ofrecido en la red.

CAPÍTULO II

MARCO REFERENCIA

2.1 Marco Teórico

2.1.1 Antecedentes Investigación

Existen numerosas compañías internacionales y nacionales de diversos sectores de la industria, incluyendo instituciones educativas, gubernamentales, financieras, telecomunicaciones, salud, producción de alimentos, ingeniería, producción de energía y fabricación, entre otras, que han utilizado herramientas para gestionar redes.

A continuación se listan algunas estas empresas

Universidad Central de Venezuela (UCV) [4]

En búsqueda de lograr mejoras significativas en los niveles de servicio ofrecidos a la comunidad universitaria por parte de la Dirección de Informática, así como disminuir el esfuerzo en las tareas de corrección de fallas por parte de los administradores de sistemas y administradores de redes, la Dirección de Informática de la Universidad Central de Venezuela (UCV) necesito asegurar la calidad y gestión en el nivel de servicio ofrecido al usuario final, para lo cual implanto una herramienta de gestión, específicamente para este caso una suite de soluciones agrupadas bajo la marca NetworkIT de Computer Associates, que le permitió a la Dirección de Informática realizar labores de gestión a la red local de esta dependencia y a los dispositivos de comunicación ubicados en toda la red de datos de la Universidad Central de Venezuela;

La implementación de esta herramienta permitió realizar un monitoreo

centralizado de la red de datos de la Universidad Central de Venezuela, y así mejorar los tiempos de respuestas, diagnosticar comportamientos anormales y ahorrar costos.

Ministerio de Finanzas [5]

La Oficina de Informática del Ministerio de Finanzas presentaba una serie de problemas de gestión de red que debieron ser atendidos y solucionados de forma eficiente, para así apoyar la labor de las unidades administrativas que conforman este Ministerio, dentro de los problemas encontrados se puede mencionar:

Retrasos en los tiempos de atención de las solicitudes de servicios de los usuarios y al diagnóstico de las fallas.

Desactualización del inventario de hardware y software, debido a los constantes cambios de versiones y actualización tecnológica en las distintas unidades del Ministerio.

Falta de una herramienta de monitoreo de red centralizada para la infraestructura de red de telecomunicaciones tanto en su sede principal como en sus sedes remotas.

Falta de control de licencias de software.

Aumento de la cantidad de computadores personales en el Ministerio de Finanzas, distribuidos en todas sus direcciones, lo cual ha incrementado los problemas y elevado los costos del soporte técnico.

Todo esto produjo que la Oficina de Informática se decidiera a adquirir una herramienta de gestión de red que permite garantizar un control de inventario,

licencias, monitoreo constante de la red y mejora en los tiempos de respuestas y diagnóstico de fallas.

Para la selección de la herramienta se realizaron estudio del mercado, donde se evaluaron los beneficios técnicos y económicos de las herramientas así como el costo de la inversión. Se solicitaron varias propuestas a empresas especializadas en el área de gestión, donde se pudiera evaluar el éxito o beneficio que la herramienta que ofertaban ha traído a los clientes que las han instalado. Basándose en el estudio costo/beneficio, se seleccionó a SMS (System Management Server) de Microsoft como software de gestión para el Ministerio.

Electricidad de Caracas [6]

Dada la creciente infraestructura de comunicación de La Electricidad de Caracas (EDC), la implantación de aplicaciones y sistemas cada vez más complejos y vitales tales como Servicio SAP, control remoto para emulación de terminales en puntos de pago y gerentes, mensajería y principalmente debido a niveles de servicios ofrecidos a los clientes de dichas aplicaciones, el Departamento Infraestructura, Operaciones y Soporte de Tecnología de Información de la EDC, decidió implantar una herramienta de gestión de red que permitio de manera interactiva detectar fallas y que adicionalmente permitio determinar la raíz del problema de manera rápida y eficiente, logrando inclusive realizar acciones automatizadas que puedan restaurar las fallas, minimizando así la indisponibilidad de las redes de la EDC. Para este caso especifico se implanto Tivoli como la herramienta para realizar el monitoreo en la EDC dada las características del producto, el cual se acopla a las múltiples plataformas coexistentes en la red de la EDC.

2.1.2 Antecedentes Organización

La Universidad de Oriente (UDO) fue Creada el 21 de noviembre de 1.958, mediante decreto Ley N° 459 dictado por la junta de gobierno presidida por el Dr. Edgar Sanabria, la cual planteo la creación de una universidad moderna con nueva orientación, adaptada a la realidad social, cultural y económica de la comunidad oriental [7].

El 12 de octubre de 1959 se inician en el país los estudios formales de ciencias marinas con la puesta en marcha del Instituto Oceanográfico con el cual también inicio actividades en el núcleo de sucre de la universidad de Oriente. Pero es hasta el 12 de febrero de 1960 donde comienza sus funciones académicas propiamente dicha con 120 estudiantes de los cursos básicos para las carreras de matemáticas, física química y biología; Posteriormente y de forma paulatina se instalaron los núcleos de Monagas, Bolívar, Anzoátegui y Nueva Esparta.

En su concepción la UDO se define como un sistema de educación Superior al servicio del país con objetivos comunes a las demás universidades venezolanas y del mundo. No obstante, es única en su género, experimental y autónoma, innovadora en la creación de la unidad profesional de Cursos Básicos, la departamentalización, los lapsos semestrales, el sistema de unidades de créditos, los cursos intensivos, etc., desarrollando investigación científica, docencia y extensión en todos los aspectos del conocimiento, que contempla sus programas educativos de pre y postgrado. Es casi una antítesis de la universidad tradicional cuyo campus tiene su sede en los núcleos universitarios ubicados en los Estados Anzoátegui, Bolívar, Monagas, Nueva Esparta, y Sucre, asumiendo así la responsabilidad de la educación Universitaria y desde su inicio motor fundamental del desarrollo integral en toda la región insular nororiental y sur del país, en función de las condiciones posibilidades y tendencias de desarrollo de cada uno de los Estados Orientales donde funcionan [7].

El Núcleo de Sucre está representada por autoridades encargadas de velar por el funcionamiento del núcleo como son : Decano, Coordinador Académico, Coordinador Administrativo, Director de Escuela de Ciencias, Director de Escuela de Ciencias Sociales, Director de Escuela de Humanidades y Educación, Director de Escuela de Administración y Director de Instituto Oceanográfico.

La Universidad de Oriente - Núcleo de Sucre, ofrece una gran cantidad de carreras de diversas áreas para la profesionalización de los Bachilleres provenientes de todo el Oriente y el resto del país. Estas carreras están agrupadas en cuatro (4) escuelas conformadas por: la Escuela de Ciencias, la Escuela de Administración y Contaduría, Escuela de Ciencias Sociales y la Escuela de Humanidades y Educación.

Dentro de las distintas carreras que conforman al Núcleo de Sucre de la UDO se cuenta con la carrera de licenciatura en Informática, la cual se originó tomando en cuenta el auge en el crecimiento y penetración de la computación en las distintas áreas productivas del país, lo cual provoco una gran demanda de profesionales en esta área, que llevó a estudiar la posibilidad de crear una carrera para esta profesión.

Teniendo en cuenta que se contaba con el recurso humano y los equipos necesarios para formar profesionales de esta área, La universidad de oriente en consejo universitario de fecha 13 de julio de 1989 acordó aprobar el Programa de la Licenciatura en Informática para la Escuela de Hotelería y Turismo del Núcleo de Nueva Esparta. Posteriormente se aprobó para los demás núcleos de la universidad de oriente.

El Programa de la Licenciatura en Informática comienza formalmente sus actividades en el núcleo de sucre en el primer semestre de 1993 con dos secciones y 85 estudiantes en las instalaciones del Departamento de Matemáticas y está adscrito a la Escuela de Ciencias de la Universidad.

Actualmente el programa de la Licenciatura en Informática se encuentra representada por un coordinador que tiene la función velar por el funcionamiento administrativo y académico del Programa, además posee una matrícula de más de 800 estudiantes y ha formado a más de cien profesionales especializados en el área de computación capaces de diseñar, desarrollar y aplicar programas de aplicación a cualquier sector productivo.

2.1.3 Área de Estudio

Este trabajo se ubica dentro del área de las redes de telecomunicaciones ya que son utilizados principios y conceptos relacionados con las redes.

Las redes son definida como un grupo de computadoras conectadas mediante cables u otro medio, las cuales son capaces de comunicarse entre si y compartir recursos [8].

En sus inicios, el desarrollo de las redes y los avances tecnológicos proporcionaron beneficios a empresas que desarrollaban tecnologías propias, pero a medida que las redes se fueron expandiendo se dificulto el intercambio de información entre tecnologías que usaban reglas propietarias diferentes. La necesidad interconectar sistemas de distintos propietarios provoco la estandarización de la arquitectura de redes.

En informática, la arquitectura de redes es definida como la forma de organización de una red, este tipo de organización es la que estructura la gestión, el tratamiento y vaciado de los datos [9].

La arquitectura de redes se refiere a la descripción de una red mediante la combinación de **estándares** y **protocolos**, en otras palabras define las reglas de una red y cómo interactúan sus componentes [10]. Las arquitecturas de redes más importantes

son, en la actualidad, la correspondiente a los protocolos OSI (*Open system Interconncetion*) y TCP/IP (*Transmisión Control Protocol/Internet Protocol*).

Modelo OSI

El modelo referencial para la interconexión de sistemas abiertos OSI, fue desarrollado por la Organización Internacional de Estándares (ISO) bajo la norma ISO 7489 y esta definido como un modelo de niveles para un entorno de sistemas abiertos, donde un proceso que se ejecuta en una computadora puede comunicarse abiertamente con un proceso similar en otra computadora [11].

El modelo OSI está dividido en siete capas:

Capa Física: define las características físicas de la interfaz, los componentes y conectores mecánicos, los aspectos eléctricos, valores binarios que representan niveles de tensión, y los aspectos fundamentales como los que se incluyen el establecimiento, mantenimiento y liberación del enlace físico.

Capa de Enlace de Datos: define las reglas para el envío y recepción de información a través de la conexión física entre dos sistemas. Se encarga de codificar y formar bloques de datos (tramas) para la transmisión, incluyendo sincronización, control de errores y control de flujo necesarios.

Capa de Red: se relaciona con los procedimientos de transmisión y conmutación de datos y permite la independencia de las capas superiores de las tecnologías utilizadas para el envío de datos. Es responsable del establecimiento, mantenimiento y finalización de las conexiones.

Capa de Transporte: proporciona un alto nivel de control para transferir en

forma transparente los datos entre los puntos extremos. Provee mecanismos para el control de errores y el manejo de prioridades. Ofrece servicios orientados a la conexión de los servicios finales. Controla la secuencia de paquetes, regula el flujo del tráfico y reconoce los paquetes duplicados.

Capa de Sesión: coordina el intercambio de información entre aplicaciones. Establece, administra y finaliza las sesiones (conexiones) entre aplicaciones que cooperan entre sí.

Capa de Presentación: se encarga de la sintaxis y semántica de la información que se transmite, provee independencia a los procesos de aplicaciones de las diferencias en la representación de los datos.

Capa de Aplicación: se utiliza para definir una serie de aplicaciones que gestionan transferencia de archivos, sesiones de terminales e intercambio de mensajes. En este nivel residen los procesos de red que realiza un usuario suministrándole el acceso al ambiente de red.

Este modelo fue creado con el objetivo de interconectar sistemas de cualquier fabricante. Aunque este intento no se ha culminado de manera satisfactoria, ha cumplido su función y objetivos, a pesar de existir detalles de implantación específicos de cada plataforma que ocasionan que no se puede aplicar completamente el modelo, como por ejemplo, las funciones de redes de comunicación, la transparencia de los protocolos de las diferentes capas del modelo y las funciones de gestión.

TCP/IP

Esta arquitectura recibe el nombre de dos de sus protocolos más importantes: el Protocolo de Control de Transporte (TCP) y el Protocolo Internet (IP) y es en la

actualidad la arquitectura de red que posee mayor aplicación práctica. Este conjunto de protocolos representa la base de comunicación sobre la cual se sustenta Internet, y su éxito se debe a varias razones, entre ellas:

Estándares de protocolos abiertos, independientes de cualquier hardware y sistema operativo.

Independencia del modelo de red, permitiendo que TCP/IP integre varias clases de redes.

Utiliza un esquema común de direccionamiento, que permite que cualquier dispositivo TCP/IP se identifique de forma única entre todos los dispositivos pertenecientes a la red.

La arquitectura está definida por cuatro capas:

Capa de Acceso: representa el nivel inferior en la jerarquía de TCP/IP y se encarga de suministrar la capacidad de intercambiar los datos entre los elementos de una red. Debe conocer los detalles básicos de la red a fin de darles el formato correcto a los datos que están siendo transmitidos.

Capa de Red: representa el segundo nivel y consiste en los procedimientos requeridos para el servicio de envío de paquetes de un nodo a otro atravesando diferentes redes, por lo que su función principal es proveer funciones de enrutamiento. El protocolo más importante en esta capa es el protocolo Internet (IP), el cual se encarga de definir la unidad básica de transmisión (datagrama), define el esquema de direccionamiento, suministra la información entre la capa de acceso y la capa de transporte, enruta datagramas hacia nodos remotos y realiza la fragmentación y ensamblaje de los datagramas.

Capa de Transporte: los dos protocolos más importantes son el Protocolo de Control de Transmisión (TCP) y el Protocolo de Datagrama de Usuario (UDP).

TCP proporciona un envío confiable de los datos, implementa mecanismos de detección y corrección de errores de extremo a extremo, se ocupa de mantener la secuencia de cuáles bytes son enviados y recibidos. La unidad de información intercambiada es el segmento. Provee una conexión lógica de extremo a extremo entre entidades de nivel superior, por lo que TCP está orientado a conexión.

UDP es un protocolo orientado a datagramas no confiable y no orientado a conexión. Permite que las aplicaciones intercambien mensajes a través de la red con un mínimo de información de control del protocolo.

Capa de Servicio de Aplicación: representa el cuarto y último nivel, contiene los protocolos que proporcionan servicio de usuario y que permiten compartir recursos de la red y acceso remoto, como son: TELNET, FTP, SMTP.

Debido principalmente a la funcionalidad de esta arquitectura, se han desarrollado diferentes protocolos, además de los propuestos inicialmente, que aplican a cada una de las capas del modelo.

El éxito de los modelos mencionados, especialmente el modelo TCP/IP, radica en el

esfuerzo realizado para interconectar sistemas de distintos fabricante. El modelo TCP/IP constituye la arquitectura de red más utilizada, puesto que es la base sobre la que se sustenta un gran porcentaje de las redes que conforman Internet.

Sin embargo, la interconexión de sistemas no proporciona únicamente beneficios, sino que también genera dificultades para controlar los recursos que

componen la red, la cual se vuelve una tarea más complicada cuando se integran en un mismo sistema diferentes plataformas operativas y fabricantes de dispositivos en una misma red, es así como surge la necesidad de gestionar redes.

2.1.4 Area de Investigacion

Gestion de redes

El término gestión (en inglés management) en general comprende los procesos de planeamiento, conducción, seguimiento y evaluación de un conjunto de decisiones y acciones, con el objeto de buscar la solución de distintos problemas y al mismo tiempo para lograr determinados objetivos de una organización o individuo [12].

La gestión es un eslabón intermedio entre la planificación y los objetivos concretos que se pretenden alcanzar

El desarrollo acelerado de las tecnologías de redes, aunado a la coexistencia de productos de diferentes proveedores, hacen que la gestión de redes sea cada vez más compleja. Por esta razón, las empresas y los propios proveedores de tecnología se han visto en la necesidad de implantar sistemas que faciliten la gestión. Los administradores necesitan, a un nivel bastante básico, que un sistema de gestión sea capaz de llevar a cabo ciertas funciones.

La siguiente lista muestra algunas de las tareas o aplicaciones más importantes:

Configurar: Inicializar (set-up) equipos y sistemas, fijar parámetros y definir interrelaciones entre los dispositivos.

Operar: Monitorear la utilización de la red y realizar funciones de contabilidad.

Mantener: Actuar frente a fallas y congestión.

Controlar acceso: Definir los tipos de accesos permitidos y los mecanismos de seguridad.

Planificar: Evaluar las necesidades futuras para garantizar la calidad de servicio.

Las redes y los sistemas de procesamiento distribuido son de vital importancia en empresas de todo tipo. Ahora bien, una red grande no puede ser instalada y gestionada por el esfuerzo humano únicamente.

La complejidad requiere el desarrollo de un plan que permita gestionar redes automatizadas.

La urgencia por la necesidad de gestionar redes se incrementa cada vez y la dificultad de proveer tales herramientas también aumenta, si la red incluye equipos de múltiples fabricantes.

La gestión de redes comprende un conjunto de tareas humanas y automatizadas que soportan la creación, operación y evolución de una red.

Importancia de la gestión de red

El adecuado empleo de las tecnologías de gestión de red permite:

Asegurar un servicio casi continuo a los usuarios finales, caracterizado por la disponibilidad y rápida respuesta, sin que estos se vean afectados por el crecimiento y complejidad de las redes y los cambios de tecnología, aumentando su

satisfacción.

Incrementar la productividad de operación de una red con el empleo de la mejor tecnología de redes, recursos humanos adecuados, procedimientos de trabajo probados y herramientas integradas que automaticen las operaciones de gestión, mejorando la eficiencia, la disponibilidad y el rendimiento de las redes.

Aumentar la relación calidad/costo en el diseño de las redes y reducir la necesidad de recursos humanos en la operación de la red.

Requerimientos para gestionar una red

Recurso Humano: Son los responsables del buen funcionamiento de la red y de su gestión. Su calificación y experiencia son claves para el éxito.

Procedimientos de Trabajo: Secuencia de pasos, tareas y directrices que permiten realizar una gestión de redes eficiente, sistematizando y organizando el trabajo de administración con el objetivo de hacerlo más proactivo que reactivo.

Desarrollo Tecnológico: Comienza con el propio diseño de la red y se manifiesta en su continua operación, optimización y expansión. El desarrollo tecnológico se debe tener en cuenta tanto en el diseño, instalación y puesta a punto de una red, como durante la vida útil de la misma. Debe contemplar la modernización continua en el hardware, el incremento acelerado en el ancho de banda de transmisión, un mayor número de servicios que incluyen las aplicaciones multimedia, surgimiento de nuevos protocolos, desarrollo de las redes virtuales, uso de sistemas operativos distribuidos, aplicación de técnicas de conmutación y desarrollo de técnicas de optimización de tráfico.

Causas por las que es necesaria la gestión de red

Los sistemas de información son imprescindibles y están soportados sobre las redes.

La información manejada tiende a ser cada día mayor y a estar más dispersa.

En la mayoría de los sistemas de redes existen productos y servicios de múltiples fabricantes los cuales incorporan diversas tecnologías que provocan un constante aumento de la complejidad de los recursos gestionados, tanto en cantidad como en heterogeneidad.

Los usuarios cada día son más exigentes.

Existen mayor número de nodos y más dispersos.

Sistema de Gestión

Un Sistema de Gestión es una colección de herramientas para el monitoreo y control de redes, con el fin de realizar actividades de seguimiento y control de los recursos de una red [12].

Existe gran diversidad de sistemas de gestión de redes, que refleja en gran medida la diversidad de equipos y servicios de telecomunicaciones existentes. Podemos clasificar los sistemas de gestión de acuerdo a los servicios de comunicación y por la cantidad de gestores.

Por Servicios de comunicación.

Sistemas de Gestión de equipos de comunicaciones. Son sistemas desarrollados por fabricantes para gestionar sus propios equipos.

Sistemas de Gestión de redes de comunicaciones. Son sistemas desarrollados por empresas en el área de las telecomunicaciones para gestionar los servicios que ofrecen.

Sistemas de gestión de arquitecturas de computadoras. Sistemas desarrollados por fabricantes de computadoras para controlar los dispositivos y protocolos que conforman los sistemas de comunicación, ajustándose a su arquitectura.

Sistemas de Gestión de redes de área local. Sistemas desarrollados para gestionar redes de área local.

Sistemas de Gestión normalizados. Sistemas desarrolladas para gestionar redes de acuerdo a las normas establecidas y dependiendo del protocolo que se utilizan. Para redes de protocolo OSI se usa la gestión OSI y para redes TCP/IP se utiliza gestión SNMP.

Por la cantidad de gestores

Sistemas de gestión centralizada. Sistemas que poseen solo un gestor de red.

Sistemas de gestión distribuidos. Sistemas que poseen varios gestores con acceso limitado con un gestor central que controla todos los recursos de la red.

Para una organización con gran número de diversidad de equipos, la gestión de todos ellos se traduce en la necesidad de tener varios sistemas de gestión diferentes.

La operación y control de una red con gran número de sistemas de gestión puede llegar a ser una tarea muy compleja por lo que las organizaciones requieren sistemas de gestión integrados para controlar todos los recursos de comunicaciones.

Se han desarrollado sistemas que integran la gestión de dispositivos diversos tales como módems, multiplexores, conmutadores, etc.

Estos sistemas disminuyen la necesidad de sistemas de gestión diferentes para cada tipo de dispositivo pero solamente gestionan una marca de dispositivos, por lo que el usuario sigue dependiendo de una marca concreta.

Los fabricantes de computadores han desarrollado también sus propios sistemas de gestión (Cisco, IBM, UNISYS, etc.); sin embargo actualmente todos ellos están en fase de implementación de sistemas de gestión basados en normas aceptadas internacionalmente.

En el momento actual la integración de diversos sistemas de gestión es un requisito fundamental en las organizaciones. Para llegar a ello se requiere un entendimiento en tres niveles:

Definición de recursos gestionados. Los diferentes sistemas gestionan los mismos recursos pero no exactamente los mismos parámetros de cada uno, ni de la misma manera.

Definición de las operaciones a realizar sobre ello. De la misma manera los diferentes sistemas de gestión realizan distintas operaciones sobre recursos de comunicaciones similares.

Protocolos de comunicación utilizados. Para poder realizar transferencias de información entre sistemas de gestión diferentes es imprescindible utilizar protocolos comunes.

Actualmente existen dos tendencias en cuanto a normas para la implementación de sistemas de gestión integrados:

Gestión SNMP (Simple Network Management Protocol) para redes TCP/IP. Estas normas de gestión están surgiendo en el marco de Internet y se explicarán en detalle más adelante.

Gestión OSI (CMIP-CMISE) que surge como esfuerzo de estandarización de la gestión en el marco del Modelo de Referencia para Interconexión de Sistemas Abiertos.

La gestión OSI es mucho más compleja que la gestión SNMP y aún no están terminadas todas las normas. La gestión SNMP es más sencilla y existen implementaciones de diversos fabricantes.

Aspectos funcionales de un sistema de gestión de red

Con la introducción del modelo OSI de siete capas propuesta por la Organización Internacional de Normas (ISO, *International Standard Organization*) tomado como base para la normalización abierta, se planteó la posibilidad de establecer criterios y procedimientos para la gestión de las redes.

En OSI se hace una clasificación de las funciones de gestión de la red en 5 áreas funcionales básicas, para así facilitar el diseño e implantación de los sistemas de gestión [12]. Estas funciones deberían ser parte de todo sistema de gestión inicial, con

previsión para implantar funciones adicionales en el futuro:

Gestión de configuración: La gestión de configuración ofrece mecanismos para la gestión de los elementos de la red (también denominados entidades u objetos), que se encuentran bajo el control del sistema de gestión.

Se deberá contar con las posibilidades para realizar tareas como las siguientes:

Modificar la configuración de los equipos y dispositivos que funcionan en la red.

Inicializar objetos, apagarlos, ó ponerlos fuera de servicio.

Recopilar datos sobre el estado de los dispositivos que funcionan en red en forma periódica o no (por ejemplo, a petición del supervisor de la red).

Proveer los servicios y recursos que se requieran para satisfacer la demanda de tráfico.

Como ejemplo de las actividades relacionadas con los puntos antes expuestos, se tiene:

Conexión o desconexión de servicio a los usuarios.

Establecimiento de opciones para las rutas alternas en caso de fallas.

Habilitación de configuraciones según la hora del día.

Instalación de software o de datos remotamente.

Gestión de averías: Tiene que ver con la detección, aislamiento y corrección de operaciones anormales de la red. Una falla o alarma es el indicador de un desperfecto potencial o real que podría suscitarse como consecuencia de un evento, siendo el evento un cambio de estado producido en algún punto del dominio bajo gestión.

Un evento puede generar el accionamiento de múltiples alarmas, pero el sistema de gestión debe tener la capacidad de discernir y presentar la multitud de alarmas como una sola alarma que identifica el problema en cuestión. El sistema de gestión debe tener la capacidad de permitir la configuración y reconfiguración de estas relaciones entre alarmas y eventos, según la preferencia de la empresa operadora de la red, o en función de los cambios producidos en la estructura de la misma. Asimismo, el bloque de funciones de eventos debería tener la capacidad de registrar todos los eventos, pero presentando sólo los mensajes relevantes que conciernen a los diferentes niveles de administración.

Gestión de desempeño: Tiene que ver con la evaluación del comportamiento de la red. Se encarga de recoger datos estadísticos, mediante el monitoreo, que puedan servir de base tanto para la planificación a largo plazo, como para los pronósticos de tendencias a corto plazo.

El monitoreo de la calidad de funcionamiento de la red exige mantener registros de entidades y estados, con el fin de detectar posibles problemas (por ejemplo congestión), así como efectuar el ajuste de los recursos de la red en respuesta a las tendencias observadas. Por lo tanto a partir de estos datos o registros se podrán realizar estimaciones de la calidad de servicio (QoS, Quality of Service).

Otra función puede ser la utilización de los datos históricos para pronosticar fallas en los equipos y enlaces con el fin de aplicar medidas de mantenimiento

preventivo para aumentar la disponibilidad de la red.

Gestión de seguridad: La gestión de seguridad se divide en tres rubros tales como:

La seguridad física: que tiene que ver con la seguridad de los equipos y de las edificaciones donde ellos residen.

La seguridad de acceso: que se ocupa de permitir el acceso por parte de los usuarios autorizados y controlar lo que les está permitido hacer.

La seguridad de datos: que involucra el resguardo de los datos contra daños, intencionales o no.

Gestión de contabilidad: Se trata del conjunto de funciones que permite la identificación de los recursos utilizados y la cuantificación de los costos para el eventual cobro a los usuarios en virtud de la utilización hecha de los servicios y de los recursos de la red. En las redes públicas la gestión de contabilidad participa en la elaboración de las facturas para los clientes y en el seguimiento de los pagos.

Elementos de un Sistema de Gestión de Red

En general, los sistemas de gestión de red constan de ciertos elementos que le permiten lograr sus objetivos en cuanto a las actividades de gestión. Sin embargo, se pueden encontrar definiciones distintas de acuerdo a la exactitud y a la profundidad con que se desee conocer este aspecto tan resaltante de los sistemas de gestión de red. A continuación se describen los elementos que básicamente conforman un sistema de gestión de red:

Estación de Gestión. Estación de gestión es el módulo que funciona como una interfaz administrador/sistema de gestión.

Agente. Es el equipamiento lógico de gestión que reside en el objeto gestionable, el cual se encarga de responder a las solicitudes tanto de información como de acción que requiere la estación de gestión, además de proporcionar información que no se ha solicitado por dicha estación (por ejemplo alarmas) de manera no simultánea.

Base de datos de información de Gestión. Conocida también como MIB (Management Information Base, Base de Información de Gestión), constituida por una colección de objetos, los cuales representan variables de datos que describen aspectos importantes del agente en cuestión, además de representar las características de los elementos de la red. Esta base de datos, le permite a la estación de gestión la ejecución de las actividades de monitoreo dándole acceso a el valor de los objetos MIB.

Protocolo de Gestión. Su función principal es permitir la conexión entre los agentes y la estación de gestión; estos poseen propiedades que permiten llevar a cabo ciertas operaciones: habilitar una estación de gestión para que recupere el valor de un objeto de un agente, habilitar una estación de gestión para que modifique el valor de los objetos de un agente y habilitar a un agente para que notifique a la estación de gestión con respecto a un evento significativo.

Existen varios protocolos para gestionar redes y su uso depende del tipo de red en el que es implementado, por ejemplo: Para redes **TCP/IP**, el protocolo utilizado es **SNMP** (*Simple Network Management Protocol*, Protocolo Simple de Gestión de Red) y para redes basadas en el modelo **OSI**, el protocolo utilizado es **CMIP** (*Common Management Information Protocol*, Protocolo de Información de Gestión Común), las

redes basadas en **TCP/IP** y **OSI**, existe una nueva versión de **SNMP** conocida como **SNMPv2**.

Patrones para la administración de infraestructura compleja de hardware, software y herramienta de gestión.

Existen unas series de estándares que son más que un patrón o buena práctica, que se caracteriza por no haber sido consensuada ni legitimada por un organismo de estandarización. Por el contrario, se trata de una norma generalmente aceptada y ampliamente utilizada por iniciativa propia de un gran número de interesados.

Estos estándares denominados de facto son desarrollados por consenso y compromiso de mejores prácticas discutidas por grandes grupos de individuos de varias organizaciones como OGC – Office of Government Commerce para ITIL, ISACA – *Information Systems Audit and Control Association* para COBIT, Universidad Carnegie Mellon para CMMi).

Administrar una infraestructura compleja de hardware, software y herramientas de gestión con la inserción de metodologías como ITIL, Cobit y CMMI, son exigencias complejas de presentar y explicar a equipos gerenciales que buscan disminuir el riesgo operacional como mantra corporativo.

Afortunadamente, son cada vez más las empresas conscientes de esta problemática que se deciden a adoptar procedimientos basados en enfoques con las mejores prácticas, normalizados de forma oficial por diversas organizaciones en marcos de actuación de impecabilidad para la gestión de Tecnología de información (TI). Las alternativas incluyen ITIL, Cobit y CMMI entre otras.

ITIL (*Information Technology Infrastructure Library* o Librería de

Infraestructura de tecnologías de Información)

ITIL [13] son las siglas de una metodología desarrollada a finales de los años 80 por iniciativa del gobierno del Reino Unido, específicamente por la Oficina de Gobierno de Comercio Británico (OGC).

Esta metodología es aceptada para la gestión de servicios de Tecnologías de Información tanto para el sector público como el privado. Estas mejores prácticas están basadas en experiencias adquirida con el tiempo en determinada actividad, y que son soportadas bajo un esquema de organización compleja y bien definida que busca apoyo en herramientas de evaluación e implementación.

Objetivo de usar ITIL. ITIL como metodología propone el establecimiento de estándares que nos ayuden en el control, operación y administración de los recursos (ya sean propios o de los clientes). Plantea hacer una revisión y reestructuración de los procesos existentes en casos de que estos lo necesiten (si el nivel de eficiencia es bajo o que haya una forma más eficiente de hacer las cosas), lo que nos lleve a una mejora continua.

Otra de las cosas que propone es que para cada actividad que se realice se debe hacer la documentación pertinente, ya que esta puede ser de gran utilidad para otros miembros del área, además de que quedan asentados todos los movimientos realizados, permitiendo así que toda persona esté al tanto de los cambios.

Formas de uso de ITIL. ITIL postula que el servicio de soporte, la administración y la operación se realiza a través de cinco procesos:

Manejo de incidentes

Manejo de problemas

Manejo de configuraciones

Manejo de Cambios

Manejo de entregas

Procesos de manejo de incidentes. Su objetivo primordial es restablecer el servicio lo más rápido posible para evitar que el cliente se vea afectado, y sin percibir ninguna falla, ya sea grande o pequeña que pueda presentar el sistema. A este concepto se le llama disponibilidad, es decir que el usuario o cliente pueda tener acceso al servicio y no percibir alguna interrupción del sistema. Para este proceso se maneja cuatro pasos básicos que son: propiedad, manejo, manejo de secuencias y comunicación.

Procesos de manejo de problemas. El objetivo de este proceso es prevenir y reducir al máximo los incidentes, y esto nos lleva a una reducción en el nivel de incidencia. Por otro lado nos ayuda a proporcionar soluciones rápidas y efectivas para asegurar el uso estructurado de recursos. En este proceso lo que se busca es tener pleno control del problema, esto se logra dándole un seguimiento y un monitoreo al problema.

Procesos de manejo de configuraciones. Su objetivo es proveer con información real y actualizada lo que se tiene configurado e instalado en cada sistema del usuario o cliente.

Este proceso es complejo, ya que se mueve bajo cuatro vértices que son: administración de cambios, administración de liberaciones, administración de

configuraciones y la [administración](#) de procesos diversos.

Procesos de control de cambios. Tiene como objetivo reducir los riesgos tanto técnicos, económicos y de tiempo al momento de la realizar cambios. Este diagrama se hace difícil de seguir ya que en esta etapa se produce una fase de monitoreo que permita determinar que los objetivos no han sufrido desviaciones.

Procesos de manejo de entregas. Su objetivo es planear y controlar exitosamente la instalación de software y hardware bajo tres ambientes: ambiente de desarrollo, de pruebas controladas y ambiente real.

COBIT (Objetivos de Control para tecnología de información y tecnologías relacionadas)

El COBIT es un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso.

Las siglas COBIT significan Objetivos de Control para Tecnología de Información y Tecnologías relacionadas (*Control Objectives for Information Systems and related Technology*). El modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (*Information Systems Audit and Control Association*).

La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

El COBIT es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT y que abarca controles específicos de IT desde una perspectiva de negocios.

Un modelo COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado..

COBIT, lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de tecnología. Vinculando tecnología informática y prácticas de control, el modelo COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes. Está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

El conjunto de lineamientos y estándares internacionales conocidos como COBIT, define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro “dominios” principales, los cuales son: Planificación y organización, adquisición e implantación, Soporte y Servicios y Monitoreo.

Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda. Estos dominios y objetivos de control facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. Asimismo, se deben tomar en cuenta los recursos que proporciona la tecnología de información, tales como: datos, aplicaciones, plataformas tecnológicas, instalaciones y recurso humano

CMMI

CMMI representa la fusión de un conjunto de modelos orientados a la mejora de procesos de ingeniería del software, ingeniería de sistemas, desarrollo de productos y adquisición de aplicaciones. Creado en 1991 por el *Software Engineering Institute* (SEI) como CMM y posteriormente actualizado como CMMI en 2002, está orientado a la garantía de calidad del software, y a la acreditación de empresas desarrolladoras de software en función del nivel de madurez de sus procesos de producción.

Su implementación aumenta la fiabilidad del software producido, la visibilidad de los procesos de producción y soporte, la reusabilidad de componentes, y como resultado de la combinación de este tipo de mejoras, disminuye los costes de producción y mantenimiento de las aplicaciones.

Los aspectos claves del modelo son, por un lado, la clasificación de las organizaciones en maduras e inmaduras y, luego, la prescripción del camino a seguir por una organización inmadura para evolucionar y convertirse en una organización madura.

El modelo entiende por organización inmadura aquella que lleva adelante sus

proyectos sin una definición previa de los procesos a seguir. Estos proyectos frecuentemente sobrepasan sus presupuestos y tiempos de terminación debido a que son iniciados con estimaciones poco realistas, sin una planificación adecuada, y son llevados adelante sin ningún tipo de gestión. En general estos proyectos no terminan o terminan con una disminución importante en la calidad esperada del producto.

Por organizaciones maduras el modelo entiende a aquellas que desarrollan sus proyectos en forma planeada. El logro de los objetivos del proyecto son asignados al cumplimiento de las reglas preestablecidas. Los presupuestos asignados y el tiempo previsto son los necesarios porque se parte de estimaciones metódicas y basadas en datos de proyectos previos, con roles y responsabilidades bien definidos.

Para que una organización se convierta en madura debe evolucionar con el tiempo alcanzando sucesivos niveles de madurez.

El modelo CMM identifica los siguientes niveles de madurez:

Nivel de Madurez 1 - Inicial – ausencia total de procesos definidos.

Nivel de Madurez 2 - Repetible – procesos de administración establecidos para lograr el seguimiento de los costos, tareas y funcionalidad. La disciplina está dada por la repetición en proyectos con aplicaciones similares.

Nivel de Madurez 3 - Definido – Además de las definiciones del nivel anterior, son incorporadas actividades de administración de ingeniería en forma documentada, estandarizada e integradas en una familia de procesos normalizados de la organización. Los proyectos utilizan una versión adaptada de esas normas para su desarrollo.

Nivel de Madurez 4 - Administrado – se llevan adelante los proyectos en forma controlada con métricas que permiten mediciones confiables de los procesos y productos.

Nivel de Madurez 5 - Optimizado – incluye la mejora continua de procesos a partir de la comparación y análisis de mediciones sucesivas de los proyectos.

El modelo CMMI incorpora al modelo por niveles de madurez de las organizaciones una vista de niveles de capacidad por área de procesos. La misma está orientada a incluir los casos en los cuales las organizaciones necesitan una capacidad diferenciada por área de proceso debido a los objetivos de sus negocios.

Estos niveles de capacidad son caracterizados genéricamente de la siguiente manera:

Nivel de Capacidad 0 – Incompleto: área de proceso sin objetivos.

Nivel de Capacidad 1 – Ejecutada: objetivos específicos del área de proceso son satisfechos.

Nivel de Capacidad 2 – Administrada: área de proceso institucionalizada a partir de una política organizacional de uso de los procesos.

Nivel de Capacidad 3 – Definida: área de proceso institucionalizada a partir de un proceso definido.

Nivel de Capacidad 4 – Cuantitativamente Administrada: área de proceso institucionalizada a partir de una política organizacional de la administración cuantitativa de procesos.

Nivel de Capacidad 5 – Optimizada: área de proceso institucionalizada a partir de la optimización de sus procesos.

La implementación de un proceso de mejoras según el modelo CMMI está compuesto de las siguientes fases:

Inicio, en esta fase se relevan los procesos, tareas, actividades y activos con que cuenta la organización, así como las políticas generadas por la conducción de la organización. El método que **CMMI** propone para la realización de este relevamiento es **SCAMPI** (*Standard CMMI Assessment Method for Process Improvement*). Consiste de un conjunto estructurado de actividades tales como entrevistas, revisión de documentos, presentaciones y análisis de respuestas a cuestionarios. El resultado de esto es la obtención de las fortalezas y debilidades, sobre las cuales se elaborará el **Plan de Mejoras**. El objetivo de esta fase es determinar las fortalezas, debilidades y oportunidades de mejora de la organización. Todo esto conducido por los objetivos de negocio de la organización.

Diseño, basados en las debilidades y fortalezas encontradas en el SCAMPI se elabora el *Process Improvement Plan* (PI Plan) y los *Action Plan* (PAs).

Piloto, de acuerdo a los objetivos planteados en cada PATs (*Process Action Team*) y al producto resultante de su trabajo (proceso, tarea, actividad, estándares), se capacita a los miembros del grupo del proyecto piloto y se prueba las prácticas correspondientes.

Implementación, en esta fase se extiende al resto de la organización las prácticas llevadas adelante en todos y cada uno de los proyectos piloto.

Implementar un programa de mejora requiere de la cooperación y coordinación

de todos los niveles de gerencia y subordinados

Dentro de las ventajas y desventajas que ofrecen estos patrones tenemos:

Ventajas

.-La organización TI desarrolla una estructura más clara, se vuelve más eficaz, y se centra más en los objetivos de la organización.

.-La administración tiene un mayor control, se estandarizan e identifican los procedimientos, y los cambios resultan más fáciles de manejar.

.-La estructura de procesos en IT proporciona un marco para concretar de manera más adecuada los servicios de *outsourcing*.

.-A través de las mejores prácticas se apoya al cambio en la cultura de TI y su orientación hacia el servicio, y se facilita la introducción de un sistema de administración de calidad.

.-Las mejores prácticas proporciona un marco de referencia uniforme para la comunicación interna y con proveedores.

Desventajas

Dentro de las ventajas que presentan estas metodologías se tienen:

.-Tiempo y esfuerzo necesario para su implementación.

.-Que no se dé el cambio en la cultura de las áreas involucradas.

.-Que no se vea reflejada una mejora, por falta de entendimiento sobre procesos, indicadores y como pueden ser controlados.

.-Que el personal no se involucre y se comprometa.

.-La mejora del servicio y la reducción de costos puede no ser visible.

.-Que la inversión en herramientas de soporte sea escasa. Los procesos podrán parecer inútiles y no se alcancen las mejoras en los servicios.

Modelo de Gestión OSI & Metodologías de estándares

Tanto las metodologías de estándares (ITIL, Cobit, CMMI) como la de modelo de gestión OSI proporcionan procesos de administración que permiten mejorar los servicios TI.

Las metodologías estándares proporcionan una serie de procesos que tiene como objetivo:

.-Alinear los servicios de TI con las necesidades actuales y futuras de sus usuarios.

.-Mejorar la calidad de los servicios TI.

.-Reducir los costos de los servicios

.-Actuar en conformidad a las leyes y normas.

Dentro de cada metodologías de estándares se encuentran incluidas de distintas formas procesos que abarca las áreas funcionales del modelo de gestión de red, dentro de los cuales se puede mencionar el de configuración, monitoreo y planificación de los servicios, entre otros.

Las metodologías de estándares proporcionan una gestión más completa en relación a servicios integrados, no solo gestionas servicios de TI si no que se integran a los objetivos de cada empresa o institución con el fin de mejorar las áreas de TI desde el punto de vista corporativo o institucional, mientras que el modelo OSI se enfoca más a la gestión de redes como tal.

Herramientas de Gestión

En la actualidad existen una gran variedad de herramientas de gestión que dan apoyo a las actividades de gestión de red. Las herramientas de redes están clasificadas en grupos:

Equipos de pruebas de cableado: Son dispositivos manuales que se conectan a la red para realizar diagnósticos de la capacidad de transmitir señales por los cables de la red. De esta manera se determinan si el comportamiento de un cable se ajusta a los estándares de cables, como la Categoría 5, además se conoce si existen: cruces de cables, abertura en uno de los hilos, rotura de cable, longitud excesiva del cable o conector mal instalados entre otros.

Equipo de pruebas y monitorización de sistemas de transmisión en multiplexores. Son equipos utilizados para monitorizar las señales de transmisión analógica, permitiendo así conocer el nivel de la señal, la relación ruido/señal, distorsión armónica, nivel del ruido y atenuación de la frecuencia.

Monitores de red. Son terminales que poseen determinados programas, que le permiten generar estadísticas del funcionamiento mediante la captura de datos, además de facilitar la monitorización de señales en las interfaces. Los monitores de red permiten:

.-Generas estadísticas para cada Terminal de la red y los errores que se generan.

Genera estadística en tiempo real e histórico.

Determinar el ancho de banda que se utiliza.

Generar estadísticas globales del tráfico, número de errores, bytes transmitidos y recibidos.

Analizadores de red. Son computadoras con programas especiales que permiten mostrar estadísticas del tráfico de la red mientras se están capturando los datos, como el número de paquetes por segundos. La información generada permite determinar cuánto tráfico genera cada sistema de red o protocolo y así determinar el ancho de banda de red que usa una aplicación o un usuario.

Analizadores de protocolo. Son programas que se usan para verificar el funcionamiento de los protocolos, tienen como función capturar las tramas a través de filtros definidos por el usuario y comprobar el funcionamiento de los sistemas de comunicación. Dentro de las funciones que realizan estos analizadores se tiene:

Captura de las tramas de forma sofisticada mediante filtros definibles por el usuario, para obtener solamente aquellas que no pueden ser útiles para resolver el problema.

Decodificación de los protocolos de forma clara, separando la información de cada uno de los niveles, interpretando el significado dentro de la comunicación, de cada una de las tramas del canal que ha intercambiado.

Disposición de un amplio rango de protocolos para decodificar, por lo menos que tenga los generalmente más usados y la posibilidad de que el usuario defina otros nuevos protocolos.

Las herramientas de gestión son muy útiles para los ingenieros, técnicos y administradores de red, ya que por medio del monitoreo se permite encontrar y solucionar variados y complejos problemas.

Dentro de las variadas herramientas que permiten capturar y analizar los datos que circulan por la red, se encuentran: Iris, Wireshark y Sniffer Portables entre otros, los cuales son herramientas que permiten conocer cómo funcionan los protocolos de comunicación de la red para así poder diagnosticar y resolver problemas causados por fallas o congestión. A continuación se conocerá de forma breve las distintas características que ofrecen las herramientas antes mencionadas.

Iris [16].

Es un analizador de tráfico de red desarrollado por *eEve Digital Security*, uno de los principales desarrolladores de seguridad de red, Iris es un analizador de tráfico sofisticado y fácil de usar, permite examinar el funcionamiento interno de la red, realizar trabajos de investigación que detecten violación de seguridad y resolver problemas de rendimiento de forma rápida y fácil.

Las características más interesantes de Iris son:

Decodificación de protocolos. Se puede analizar el tráfico en la red en un formato simple de entender y se pueden producir distintos reportes gráficos.

Reconstrucción de paquetes. Se pueden reconstruir las sesiones Web y se pueden simular cookies para entrar en sitios Web protegidos con contraseña, para así evaluar la seguridad de la red de una organización.

Supervisión del correo y mensajería electrónica. Esta facilidad puede complementar los procedimientos para que se haga un uso correcto y racional de los medios electrónicos de comunicación por parte de los empleados.

Filtrado de tráfico. Se pueden usar reglas o criterios para filtrar los paquetes que se van a capturar, por ejemplo dirección MAC, dirección IP, palabra clave, puerto, capa del protocolo, etc. Los filtros permiten buscar un tipo de contenido específico y rastrear patrones de tráfico que puedan corresponder a un virus o a información confidencial de la empresa.

Manipulación y forjado de paquetes (spoofing): Se pueden crear paquetes a la medida o modificar paquetes previamente capturados para luego enviarlos a la red. Esta facilidad se puede utilizar para probar un firewall y asegurarse de que bloquea y filtra los paquetes correctamente. También permite evaluar la capacidad de soportar una carga elevada por parte de un sistema o de un servidor y simular ataques de negación de servicio (DoS).

Registro de intentos de conexión: Se puede capturar y registrar la evidencia de intrusiones en la red, reconstruyendo cada movimiento que un atacante haya hecho.

Sniffer Portable.

Anteriormente llamado Sniffer Pro [17], es un programa comercial que permite determinar, localizar y analizar de forma automática problemas que afectan el rendimiento de la red, monitorizando y analizando un conjunto de protocolos. Dentro de sus características podemos mencionar:

Principales características y ventajas

Rápida detección y solución de problemas

Cuenta con una interfaz del usuario fácil de utilizar que se puede emplear en varias topologías para proporcionar una rápida captura de datos y presentación de informes

Gráficos avanzados en tiempo real

Proporciona un mapa del tráfico de la red y una matriz de los usuarios que más tráfico generan en la red.

Muestra la tabla de hosts para identificar de manera inmediata los usuarios que utilizan más ancho de banda

Muestra información sobre la distribución de los protocolos en uso, las aplicaciones que funcionan con el Protocolo de Internet (Internet Protocol, IP), y los procesos que utilizan de transporte con Internetwork Packet Exchange (IPX)

Una planificación precisa de la red

Monitoriza y muestra el uso de la red a lo largo del tiempo Hace posible el

seguimiento del uso diario de la red para planificar de manera efectiva su cambio y crecimiento.

Proporciona informes estadísticos globales, como el tráfico, los errores, la distribución del tamaño en el segmento, así como su información detallada sobre su uso

Wireshark [18].

Es una herramienta de código fuente abierto, antiguamente conocida como ethereal, es un analizador de protocolos utilizado para analizar y solucionar problemas en redes de comunicación para desarrollo software disponible en diferentes plataformas tanto para Unix y como para Windows, y además puede mostrar paquetes capturados por otros programas y guarda las captura en diferentes formatos, también puede filtrar paquetes por muchos paquetes y seleccionarlos basándose en filtros. Wireshark es una herramienta compatible con más de 480 protocolos y tiene una interfaz muy flexible y además muestra el tráfico que pasa por una red con varias opciones como son la decodificación de los paquetes para ver sus opciones y significado de manera más amigable con opción a crear filtros y estadísticas.

2.2 Marco Metodológico

2.2.1 Metodología de la investigación

A continuación se describe como se llevo a cabo la investigación y comprende el tipo de investigación y el marco metodológico utilizado con el fin de explicar los pasos que se llevaron a cabo para el desarrollo del presente proyecto.

La metodología que permitió llevar a cabo la investigación se encuentra

enmarcada dentro de los siguientes criterio [19]:

2.2.2 Nivel de investigación.

Por su naturaleza, esta investigación fue de carácter descriptivo, la cual se aplico en el

campo de la informática, especialmente en el área de las comunicaciones. Su propósito se centro en describir las características fundamentales de los servicios que presta la red y de los recursos que la conforman.

Para el desarrollo de la investigación se utilizaron criterios sistematizados que pusieron de manifiesto las principales características de los servicios y recursos que conforman la red, para así conocer su funcionamiento y comportamiento.

2.2.3 Tipo de investigación

La estrategia que se adopto para el desarrollo del sistema propuesto fue dada por una investigación de campo. Los datos fueron recolectados de manera directa en los laboratorios de informática y oficinas administrativas y docentes pertenecientes al Programa de la Licenciatura en Informática del Núcleo de Sucre de la Universidad de Oriente.

2.2.4 Técnicas de recolección de datos

Las técnicas de recolección de datos que fueron usadas para el desarrollo del proyecto fueron:

La observación directa, la cual se realizo en el área del laboratorio de informática, con el fin de conocer los procesos actuales en desarrollo.

Las entrevistas no estructuradas, las cuáles fueron aplicadas a los administradores de la red, con el fin de conocer cuáles son los requerimientos necesarios para realizar el diseño.

La investigación documental, la cual ayudo a recolectar información sobre el tema en estudio.

2.2.4 Metodología del área aplicada

El proceso de investigación se desarrollo a través de la metodología MÉTRICA [19] y fue complementada con el capítulo de administración de red del Programa de la Academia Networking Cisco [20].

Las Cuatro primeras fases a cumplir representan la fase de planificación de la metodología MÉTRICA, las siguientes fases están conformadas por los aspectos que rigen la administración de la red.

Las fases a cumplir son las siguientes:

Etapa 1. Determinación de las necesidades de la planificación. A través de las diferentes técnicas de recolección de datos y de entrevistas se identificaron los objetivos estratégicos que apoyaron el plan de gestión, así como su alcance y los factores críticos que se consideraron importantes para la planificación de la gestión de red.

Etapa 2. Recopilación de información relevante. En esta fase se recopilaron y analizaron todos los antecedentes que pudieran afectar los procesos involucrados en el desarrollo del plan de gestión, para lograr esto se seleccionaron fuentes de

información y documentación relacionada a la gestión de red, la cual sirvió como estudio previo al desarrollo de la planificación.

Etapa 3. Identificación de los requisitos. Para cumplir esta fase se estudiaron los procesos actuales que maneja la red, para esto fue necesario llevar a cabo sesiones de trabajo con administradores y usuarios de la red que permitieron analizar de cada proceso, sus fortaleza, debilidades, oportunidades y amenazas , permitiendo así tener una visión global de los recursos con que se cuenta e identificar los requisitos. Se elaboró un modelo de información que represente a los procesos, con sus entidades implicadas y sus relaciones.

Etapa 4. Diseño del modelo de planificación para la gestión de la red. Una vez identificados los requisitos se logró definir los procesos que darán soporte a la gestión de redes, para ello se analizaron los procesos actuales con los requerimientos encontrados en la fase anterior, tomando en cuenta la infraestructura tecnológica con que se cuenta y estableciendo formas de gestionar la red que responda a las necesidades de la misma.

Etapa 5. Documentación de la red. Con la información encontrada en las fases anteriores se dio inicio al proceso de administración, comenzado con la documentación de la red, para la cual se busco apoyo de software que permitiera documentar la infraestructura de la red y obtener información de los activos de hardware (Switches, Router, impresoras, servidores, ordenadores) y software que se conforman la red.

Etapa 6. Definición de las políticas de red. Esta fase se especifico como debe estar protegida la red contra el acceso no autorizado, esto tiene que ver con las políticas de seguridad, tales como longitud mínima de las contraseñas, antigüedad máxima de la contraseña, contraseñas exclusivas, entre otras. También se determino

el método para proteger y recuperar información ante una pérdida.

Etapas 7. Monitoreo de la red. A través de la monitorización se logró evaluar el funcionamiento de la red, para lo cual se definieron los recursos a gestionar y las herramientas de gestión que cumplieron con los requisitos de información y la arquitectura tecnológica. De esta forma se obtuvo un diagnóstico acerca del comportamiento de la red, la cual fue evaluada. Así se conoció el grado de utilización de los recursos y el nivel de cumplimiento de los servicios de usuarios, lo cual ayudó a diagnosticar, eliminar e informar sobre fallas de los equipos y componentes de la red o de los servicios utilizados.

CAPÍTULO III. DESARROLLO

3.1 Determinación de las necesidades de la planificación

El primer paso a cumplir fue determinar las necesidades que se tienen para planificar el plan de gestión, para lo cual se efectuaron entrevistas no estructurada a los administradores de la red, por ser considerados la principal fuente de información para conocer las necesidades existentes.

A través de estas entrevistas se pudo conocer la red en estudio, en la cual se encontró con una red que presenta una diversidad en equipos y sistemas, y que no cuenta con ningún servidor, las estaciones de trabajo están conectadas a través de dispositivos que permiten solo compartir recursos.

Como protocolo de comunicación se utiliza TCP/IP índice

Los servidores DNS no existen, las cuentas de usuario eran creadas por el administrador en un equipo específico para un usuario específico, lo cual limitaba la disposición de la máquina y hacía tediosa la tarea del administrador al tener que crear varias veces una misma cuenta en distintos equipos, por esta razón se crearon dos cuentas para uso de la red, la de administrador que posee los privilegios de un administrador y la de usuario que es usada por todos los estudiantes con privilegios limitados, poniéndose en riesgo la seguridad de la red.

Los sistemas de escritorio son utilizados bajo una plataforma mixta.

El estado actual en que se encuentra la red en estudio produce problemas para

administrarla, ya que no se cuenta con las herramientas necesarias para tal función; lo que produce entre otras cosas:

1. Falta de conocimiento del tráfico que circula por la red
2. Ausencia de políticas de seguridad
3. Falta de información de la estructura y dispositivos de la red.
4. Retardo en el diagnóstico y corrección de algún evento imprevisto.

Las causas que han originado estos problemas es la falta de procesos o herramientas que den apoyo a los administradores para brindar un control y buen funcionamiento de los servicios de red, para lo cual se deberá contar con herramientas que permita a los administradores:

1. El diagnóstico y corrección de fallas de los recursos
2. Conocer y mantener actualizada toda la información del hardware de cada equipo que se instala en la red.
3. Visualizar y conocer estadísticas de la red o de algún equipo especial para medir y evaluar su comportamiento que ayude a determinar si requiere ser actualizado o realizar algún cambio de equipo.
4. Detectar eventos que representan la ocurrencia de un problema y por lo tanto, la interrupción de un servicio.
5. Contar con un sistema que permita generar estadística, reportes y gráficas

que sirvan para la evaluación de la red, servidores, estaciones de trabajo o impresoras.

3.2 Recopilación de Información relevante

Teniendo en cuenta los problemas encontrados y las causas que lo producen, se consulto material bibliográfico, sitios y páginas Web que ayudaran aportar información relevante para el desarrollo del plan de gestión, dentro de la cual se consideraron las necesidades tecnológicas indispensables para gestionar la red en estudio, determinándose necesario la implantación de herramientas de gestión de redes que apoyen la actividades de administración de la red, específicamente la de monitoreo y documentación de red; Esto amerito estudiar distintos software que permitiera determinar cuál de ellas se adaptaba mejor a la red en estudio.

3.2.1 Análisis de herramientas para el monitoreo de red

Para el monitoreo de la red se compararon tres analizadores de red, se estudiaron los requerimientos funcionales y técnicos necesarios para la red en estudio, en la tabla n° 1 se observa el resultado de la comparación de las herramientas analizadas.

Tabla 1. Tabla comparativa de herramientas de monitoreo de red

Requisitos Funcionales	Analizadores		
	Sniffer Portable	Wireshark	Iris
Debe funcionar con Windows XP	✓	✓	✓
Debe generar reporte estadísticos del trafico	✓	✓	✓
Debe generar	✓	✓	✓

información sobre el uso del ancho de banda			
Permite monitorear la red y hacer diagnóstico	✓	✓	✓
Debe identificar problemas de rendimientos	✓	✓	✓
Requisitos Técnicos			
Portabilidad	✓	✓	✓
Funcionalidad	✓	✓	✓
Confiabilidad	✓	✓	✓
Facilidad de uso	✓	✓	✓
Eficiencia	✓	✓	✓

3.2.2 Análisis de las herramientas para la documentación de red

Para la Documentación de red se estudiaron otro tres software conocidos en el mercado, ellos fueron: Aida32 , Everest Corporation Edition y el Total Network Inventory los cuales tienen como objetivo analizar los componentes de una red y dar a conocer toda una información detallada sobre el hardware, software y configuración de la red;

Se analizaron los requerimientos necesarios para ser implantados en la red en estudio, en la tabla n° 2 se puede observar los resultado obtenido de la comparación realizada.

Tabla 2. Tabla comparativa de herramientas para inventario de red

Requisitos Funcionales	Analizadores
-------------------------------	---------------------

	Aida32	Everest Corporation Edition	Total Network Inventory
Debe funcionar con Windows XP	✓	✓	✓
Debe generar información de software	✓	✓	✓
Debe generar información de hardware	✓	✓	✓
Permite generar reportes	✓	✓	✓
Requisitos Técnicos			
Portabilidad	✓	✓	✓
Funcionalidad	✓	✓	✓
Confiabilidad	✓	✓	✓
Facilidad de uso	✓	✓	✓
Eficiencia	✓	✓	✓

De la evaluación técnica se obtuvo como resultado que las tres herramientas estudiadas para documentar la red en estudio cumplen con los requerimientos técnicos. Esto lleva a considerar el aspecto económico, en el cual se encontró que la herramienta Aida32 es la única que no genera costo de licencia y que además sustenta la promulgación del Decreto 3.390 sobre Uso de Software Libre en la Administración Pública, publicado en Gaceta Oficial N° 38.095, de fecha 28 de diciembre de 2004, en la cual se exige a la Administración Pública Nacional empleará prioritariamente Software Libre desarrollado con Estándares Abiertos, en sus sistemas, proyectos y servicios informáticos

3.3 Identificación de los requisitos

Conociendo la problemática y las necesidades que presenta la red en estudio, se dio inicio a la fase de identificación de requisitos, en el cual se estudiaron y conocieron los procesos que se ejecutan para gestionar la red, se realizaron sesiones de trabajo con administradores, técnicos y usuarios (docentes y estudiantes) que proporcionaron toda la información necesaria para identificar los requisitos que ayuden a desarrollar el plan de gestión de la red en estudio.

La red del Programa de la Licenciatura en Informática tiene como objetivo compartir recursos e intercambiar información de manera eficiente, a fin de satisfacer la creciente demanda de servicios y productos de información, que permitan el desarrollo teórico-práctico académico de sus estudiantes.

La red cuenta con distintas salas de computación que brindan a los usuarios los recursos necesarios para desarrollarse como profesionales en el área de la informática.

La red es gestionada por un administrador de red el cual tiene como objetivo mantener la red operativa, eficiente y segura. El administrador de red realiza distintas tareas para cumplir sus funciones, dentro de las cuales se puede mencionar:

Instalación Hardware: el proceso de instalación consiste como su nombre lo dice en instalar el hardware y configurarlo para que estos estén operativos a sus usuarios, este proceso es realizado sin llevar una documentación donde se informe las características del hardware y los elementos instalados.

Creación de cuentas: la creación de cuentas no es más que el proceso de asignar una cuenta con su clave o *password* a un usuario, con la cual el usuario podrá

hacer uso de los servicios que presta la red. Cabe destacar que actualmente no se crean cuentas pues la red solo trabaja con dos cuentas: la del administrador y la de usuario que es usada por los estudiantes adscrito a la coordinación de informática.

Reservación de equipos: los usuarios deben reservar los equipos para hacer uso de ellos, para cumplir esto, el usuario debe chequear que la maquina o equipo esté disponible y una vez verificada la disponibilidad reservar el equipo el día y en la hora necesaria o disponible para el usuario.

Préstamo de Equipo: préstamo de equipo es simplemente disfrutar los servicios de la red que fueron reservados con anticipación.

Préstamo de equipo de Multimedia: préstamo de equipo de multimedia es simplemente reservar los equipos de multimedia con anticipación.

Impresión de documentos: los usuarios pueden hacer uso de las impresoras de la red para obtener documentos impresos, para lo cual deben informar al administrador del documento que desean imprimir para que este pueda dar paso a la impresión del mismo. Actualmente este servicio no está en funcionamiento.

Mantenimiento: en la red del Programa de la Licenciatura en Informática se realiza mantenimiento al final de cada semestre, el cual consiste en limpiar los discos duro con el fin de que no quede ningún tipo de información y prepara los equipos para realizar el proceso de inscripción.

Reparación: las fallas que presentan los equipos son reparados una vez que estos presentan problemas al usuario el cual es el informante de los problemas que presenta el equipo. Las reparaciones son realizadas sin llevar un registro de las fallas presentadas ni las soluciones aplicadas.

Para comprender mejor los procesos que se ejecutan para administrar la red fue necesario definir en detalle cómo se realizan los distintos procesos de administración.

En la Figura 1 se puede observar el diagrama de flujo de datos que representa los distintos procesos de administración.

En la Figura 2 y 3 se muestra el diagrama de flujo de datos expandido del mismo proceso.

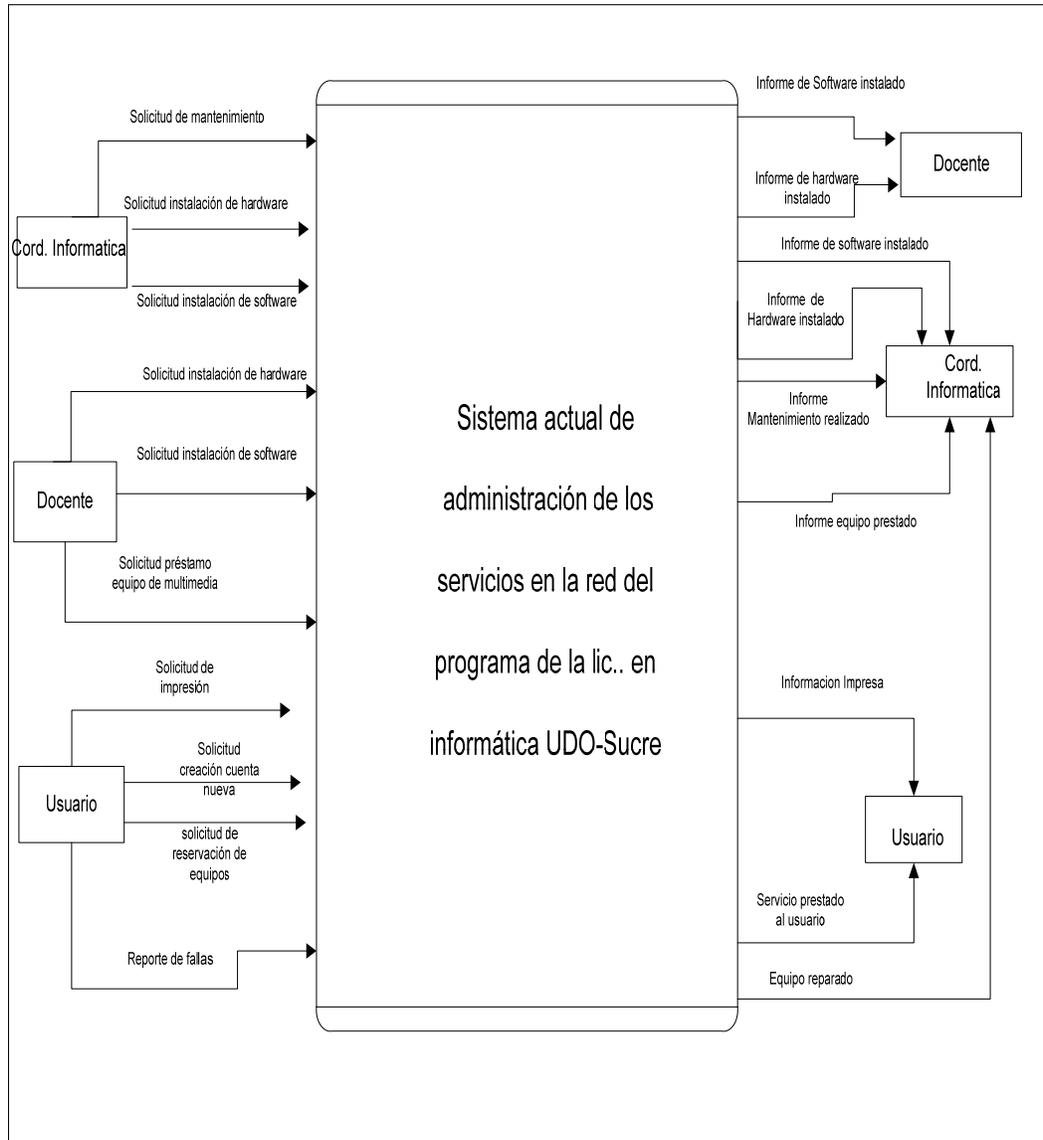


Figura 1. Diagrama de flujo de datos del sistema actual de administración de la red del programa de la licenciatura en informática

Para comprender y explicar el funcionamiento actual de los procesos de administración que se llevan a cabo en la red del programa de la licenciatura en informática es conveniente realizar una descripción de los procesos y los flujos de datos, las cuales son explicadas en etalle en el apéndice A.

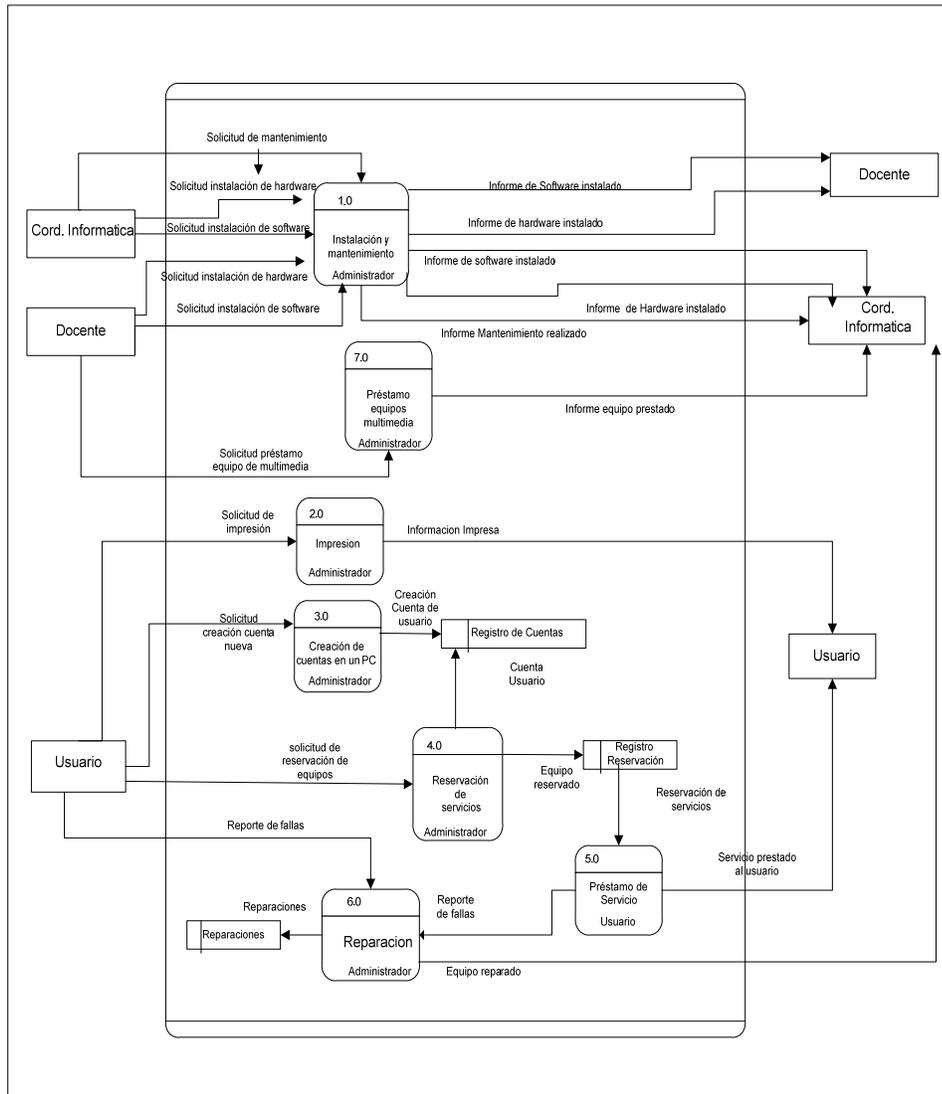


Figura 2. Diagrama de flujo de datos expandido del sistema actual de administración de la red del programa de la licenciatura en informática

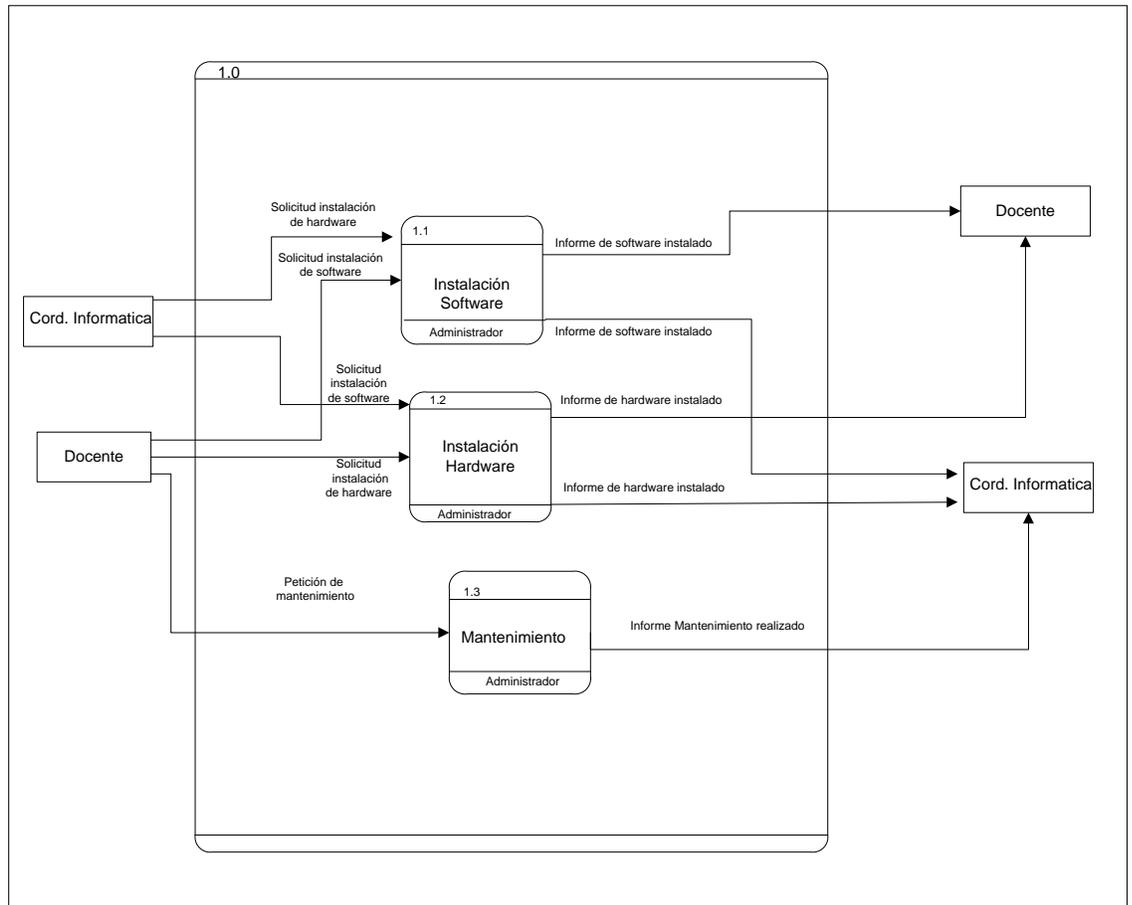


Figura 3. Diagrama de flujo de datos expandido del proceso 1.0 del sistema actual de Administración de la red del programa de la licenciatura en informática

De acuerdo a lo aportado en las entrevistas, el administrador no cuenta con las herramientas necesarias, tanto de hardware como de software, para cumplir sus funciones, lo cual permite determinar algunos requisitos necesarios para mejorar la gestión de la red, ellos son:

Establecer mecanismos modernos para la creación de cuentas de usuarios

Crear políticas de seguridad que brinden un servicio seguro y eficiente a los usuarios

Tener conocimientos de los elementos que conforman la red, así como sus configuraciones y componentes.

Conocer el comportamiento de la red

Mejoras en los procesos de instalación y configuración de hardware

Perfeccionar los procesos de mantenimiento de red

Documentar procesos como los de instalación, configuración y mantenimiento que puedan sufrir algún equipo

3.4 Diseño del modelo de planificación para la gestión de la red.

Para diseñar el modelo de planificación se tomo en cuenta los procesos actuales y las necesidades existentes para gestionar la red de forma eficiente y segura, esto permitió diseñar un modelo de planificación que integrara herramientas de gestión de red y equipos básicos para obtener una red eficaz.

El modelo de planificación fue desarrollado tomando en cuenta cuatro de las cinco áreas funcionales de la gestión de red, las cuales son: configuraciones, averías, desempeño y seguridad.

Para el modelo de planificación a diseñar se propusieron procesos de gestión que permitieran gestionar el desempeño de la red, las fallas y reparaciones, así como las configuraciones e instalaciones de los equipos que la conforman. Dentro de estos procesos se encuentran el de monitoreo, inventario, configuraciones y averías.

En la Figura 4 y 5 se puede observar el diagrama de datos que representa el plan

propuesto para gestionar la red del Programa de la Licenciatura en Informática y el diagrama expandido respectivamente.

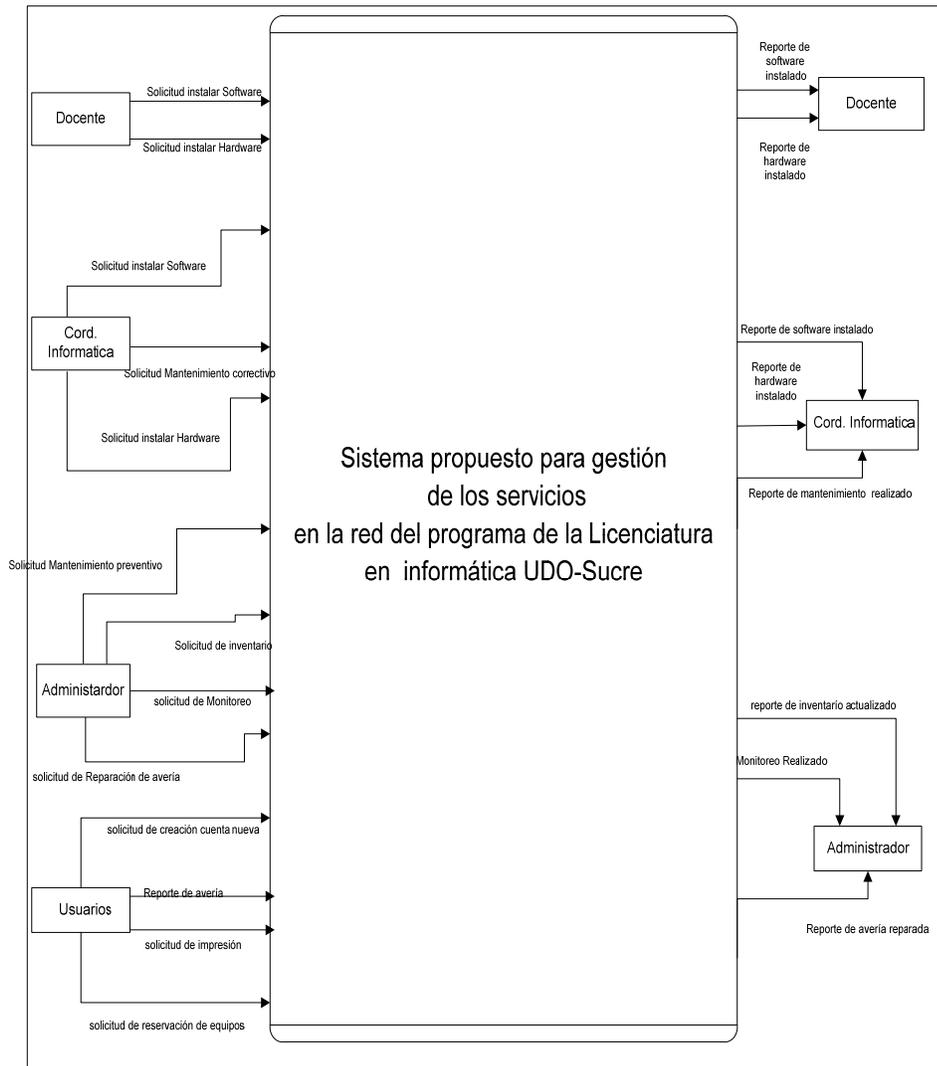


Figura 4. Diagrama de datos del sistema propuesto para la administración de los servicios de red del programa de la licenciatura en informática

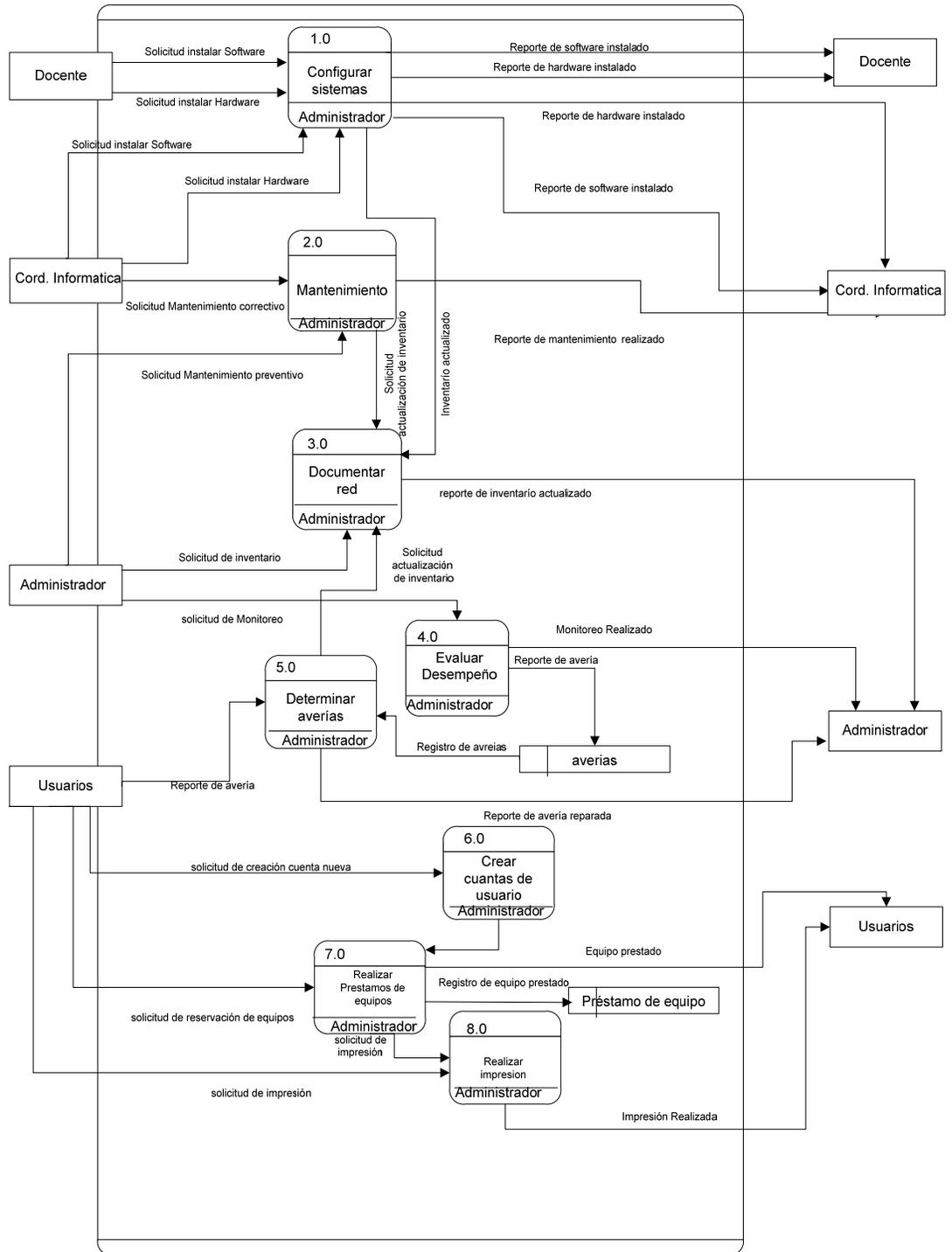


Figura 5. Diagrama de datos expandido del sistema propuesto para la administración de los servicios de red del programa de la licenciatura en informática

3.5 Documentación de la red

Para la documentación de red se compilo toda la información necesaria para definir la estructura lógica y física de la red en estudio, para ello se recolecto información a través de la observación directa para conocer los distintos dispositivos que conforma la red, así como estructura lógica y física que nos permita conocer como están dispuesto los dispositivos y elementos que conforman la red del Programa de la Licenciatura en informática.

La red del Programa de la Licenciatura en Informática recibe conexión del centro de computación académica la cual tiene como misión planificar, coordinar y supervisar todas aquellas actividades relacionadas con el diseño, administración, mantenimiento y actualización tanto de la Red Teleinformática como los Servicios que ésta provee, a la comunidad universitaria. La conexión que recibe esta red es a través de una fibra óptica, la cual es conectada a un switch Catalyste Cisco de 12 puertos, que a su vez se conecta con otros switch y concentradores, formando una topología estrellas que permite conexión a las distintas oficinas y salas del Programa de la Licenciatura en Informática.

En el programa de la Licenciatura en Informática cuenta con 4 sala de computación: la sala 1, sala 2, sala de multimedia y sala de enseñanza virtual, las cuales son usadas por usuarios para investigación, aplicaciones y realizar practica de estudio.

Para comprender mejor como se encuentra lógicamente conectada la red se presenta a continuación un diagrama lógico de la red en estudio.

La definición de la estructura lógica no es suficiente para documentar la red, es necesario realizar una documentación más profunda que permita conocer a fondo

cada dispositivo que conforma la red, para lo cual se busco apoyo en herramientas que facilitaran el inventario de la red.

El software que cumplió con los requisitos necesarios para la red en estudio fue Aida32; Para la implantación de esta herramienta fue necesario configurar un servidor que permitiera poner en funcionamiento el software, una vez configurado el servidor e instalado el software se dispuso a realizar el inventario, el cual arrojó toda la información necesaria, tanto de hardware como de software para que el administrador obtenga mejor conocimiento y mayor control de los recursos con que se cuenta y así prestar un servicio más eficaz.

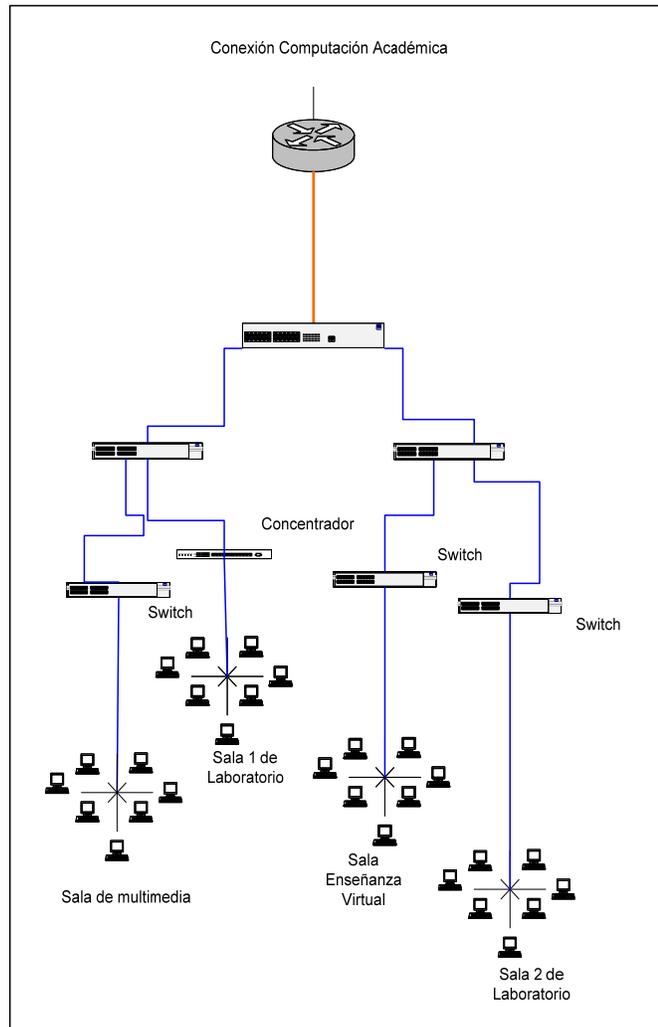


Figura 6. Diagrama Lógico de la estructura de red del programa de la licenciatura en informática

En el apéndice C se puede ver la información (hardware-software) obtenida a través de Aida32 de cada máquina que conforma la red del Programa de la Licenciatura. En Informática.

3.6 Monitoreo de red

En esta fase se evaluó el comportamiento de la red, para lo cual se busco ayuda en herramientas que permitieron conocer la información que circula en la red en

estudio.

En la fase de recopilación de información relevante se determino Wireshark como la herramienta que mejor se adaptaba a la red, la cual fue instalada en un servidor configurado provisionalmente, ya que la red no posee servidor alguno. Una vez instalado Wireshark se dio inicio a la monitorización de la red. Para poder conocer y analizar la información que circula por la red, fue necesario conocer y aprender a utilizar esta herramienta.

Instalada y operativa la herramienta, se dio inicio al uso de la misma. Al iniciar Wireshark nos encontramos con la siguiente ventana:

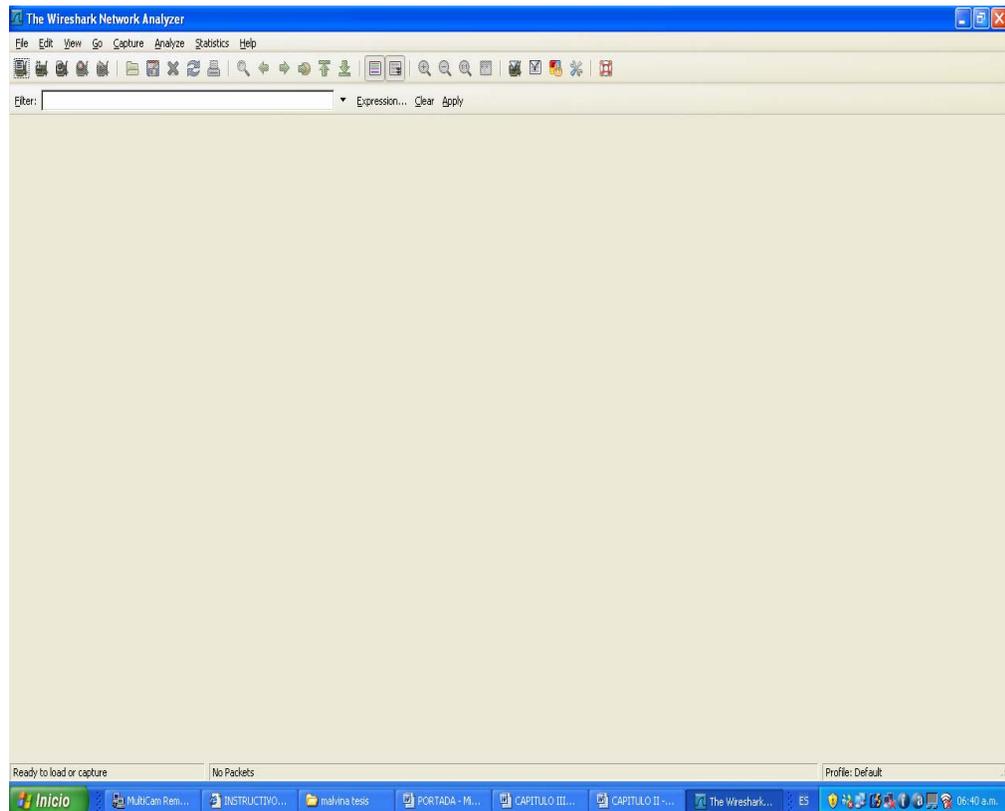


Figura 7. Página de inicio de la aplicación Wireshark

En esta ventana se observa claramente las siguientes opciones en la barra de menú:

File: este menú contiene elementos de menú para abrir y releer ficheros de captura, guardar ficheros de captura, exportar bytes, imprimir ficheros de captura, y salir de Wireshark.

Edit: este menú contiene elementos de menú para encontrar una trama, marcar una o más tramas, establecer referencias de tiempo y establecer las preferencias (cortar, copiar y pegar no están actualmente implementados).

View: este menú contiene elementos de menú para modificar opciones de visualización,

Ampliar/reducir la fuente de los paneles, colorear tramas, expandir todas las tramas, colapsar todas las tramas, mostrar un paquete en una ventana aparte, y recargar el fichero de captura actual.

Go: este menú contiene elementos de menú para desplazarse entre las tramas.

Capture: este menú permite iniciar y detener capturas, y crear filtros de captura.

Analyze: este menú contiene elementos de menú para seleccionar y filtrar paquetes coincidentes, seguir una sesión TCP, crear filtros de visualización, habilitar o deshabilitar la disección de protocolos, y configurar decodificadores especificados por el usuario.

Statistics: Este menú contiene elementos de menú para obtener un resumen de los paquetes que han sido capturados, mostrar estadísticas de jerarquía de protocolos, gráficos de entrada/salida, listas de conversaciones y hosts, tiempos de respuestas y

distintos análisis de protocolos particulares.

Help: este menú permite mostrar los plugins cargados, contiene el elemento de menú *About Ethereal...* y acceso a alguna Ayuda básica.

Para dar inicio a la monitorización y obtener información en la red, debemos seleccionar la opción “capture”, una vez que se haga click aquí aparecerá la siguiente ventana:

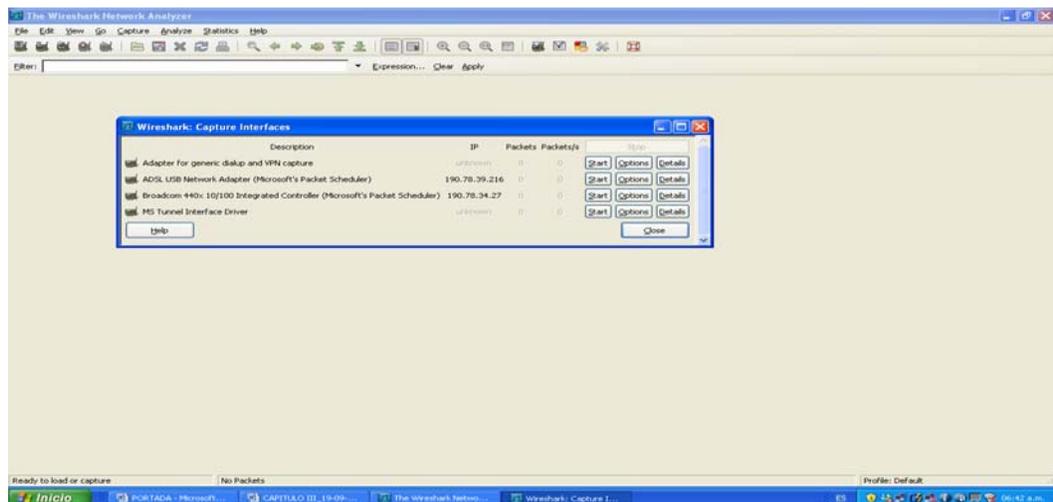


Figura 8. Página de inicio para capturar tráfico con la aplicación Wireshark

En esta ventana se seleccionará la tarjeta de red y se hará click en el botón “start”, una vez hecho esto empezara a capturar toda la información que circula por la red. Y aparecerá una ventana como la que se muestra a continuación:

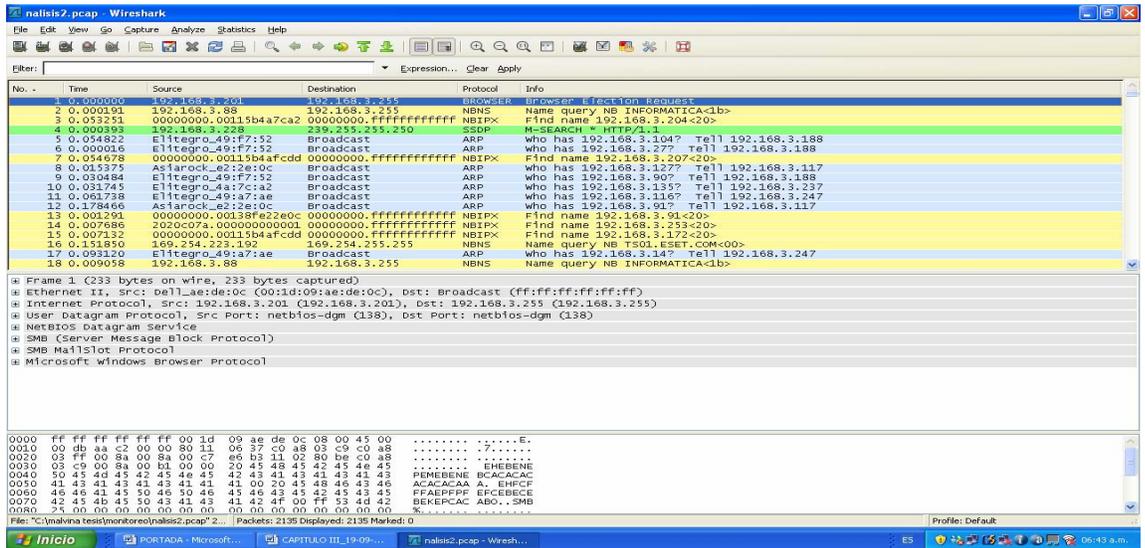


Figura 9. Pagina de captura de tráfico con la aplicación Wireshark

El monitoreo de red se realizó por cinco días consecutivo en un lapso de 6 horas diarias aproximadamente.

Para comprender mejor la información obtenida es necesario conocer que significan las salidas que emiten el monitoreo. La Figura 9 muestra las distintas salidas que emite el monitoreo.

En esta ventana se observan tres zonas de datos. La primera es la zona de listado de los paquetes capturados con información del Numero de Frame, tiempo en segundos de la captura, Origen, Destino, protocolo involucrado y por último un campo de información extra que previamente Wireshark a decodificado

La segunda zona muestra los datos del Frame capturado. En este caso Frame 194 o captura 194 (las enumera secuencialmente) que nos da información de todos los protocolos involucrados en la captura, además muestra información completa de la trama capturada. Tamaño total, etc.

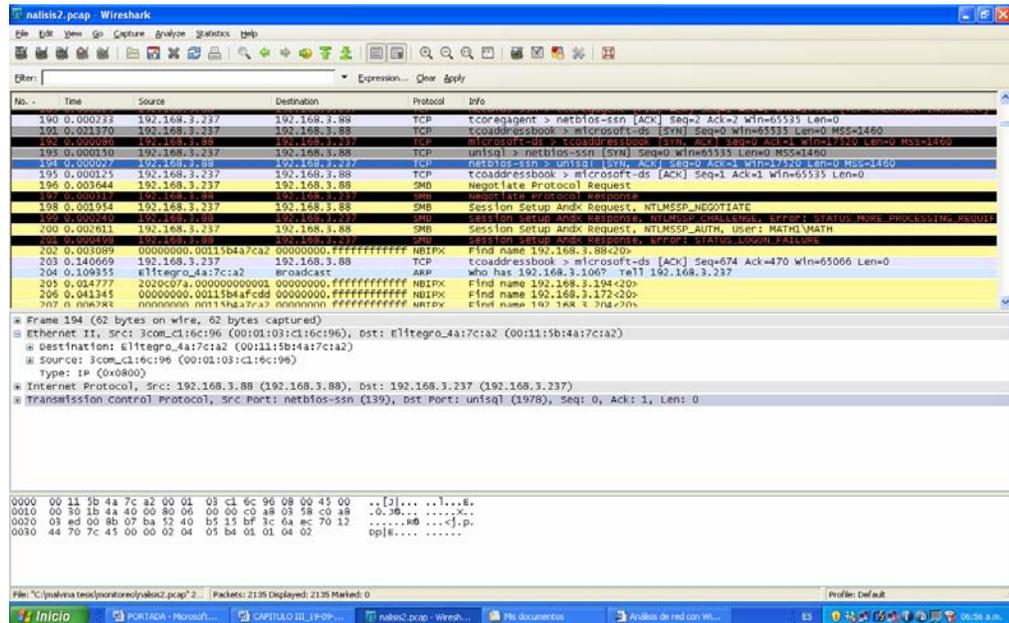


Figura 10. Pagina de captura de tráfico con la aplicación Wireshark

A continuación Ethernet II que nos muestra la cabecera Ethernet II que a su vez pertenece a la capa de enlace de datos:

0000 00 11 5b 4a 7c 92 00 01 03 c1 6c 96

Nos muestra parte de la cabecera de la trama Ethener II, en este caso:

Destino 6 bytes 00 11 5b 4a 7c 92 : MAC destino
Origen 6 bytes 00 01 03 c1 6c 96 : MAC origen
Tipo 2 bytes 08 00 : protocolo que viaja en la parte de datos de la trama en este caso
IP. 0x0800.

A continuación se observa **Internet Protocol** con los datos de la cabecera del datagrama IP:

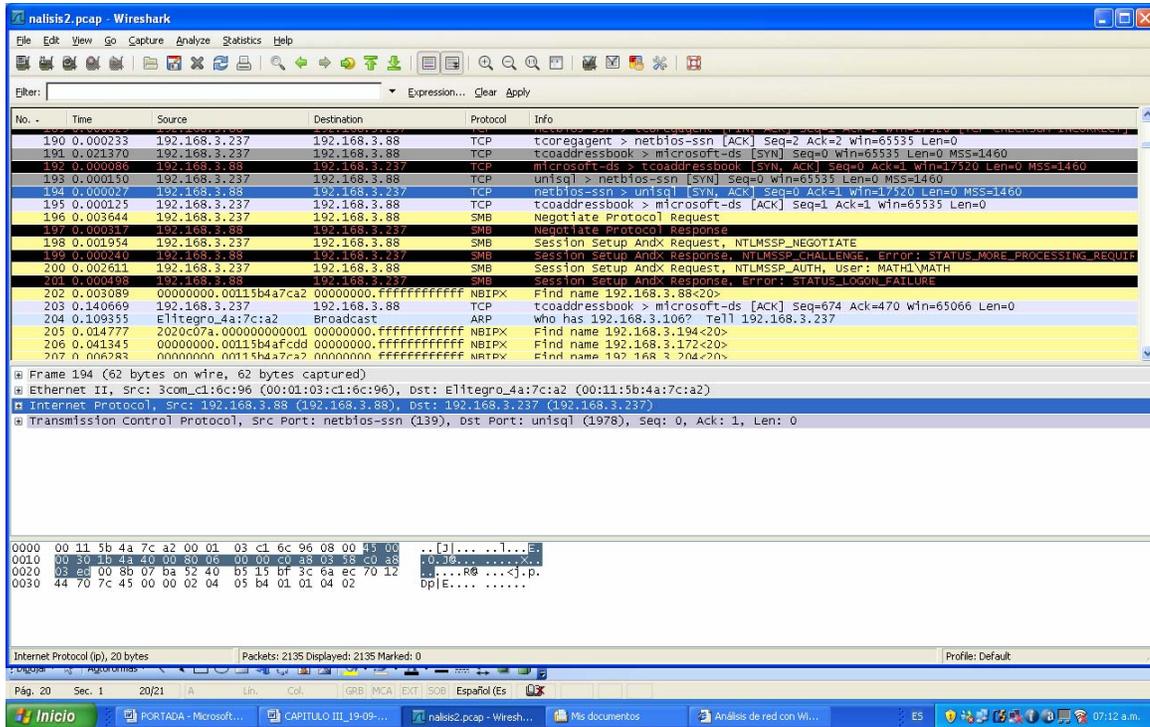


Figura 11. Pagina de captura de tráfico con la aplicación Wireshark

Después se encuentra con **Transmission Control Protocol. (TCP)**. (ver Figura N° 11)

Se trata del **Segmento TCP**. Protocolo involucrado en esta captura.

Como ya hemos visto, tenemos información del **Puerto de origen, destino, número de secuencia**, etc.

Y para finalizar se tiene **TCP Segment Data**, con todo el contenido del campo Data del segmento TCP.

Como se puede observar las salidas que produce el monitoreo es bastante amplia, para lo que existe la posibilidad de filtrar la información o paquetes que nos interesa analizar, para esto se selecciono los paquetes involucrados con la capa de aplicación (ftp, http, dns, etc).

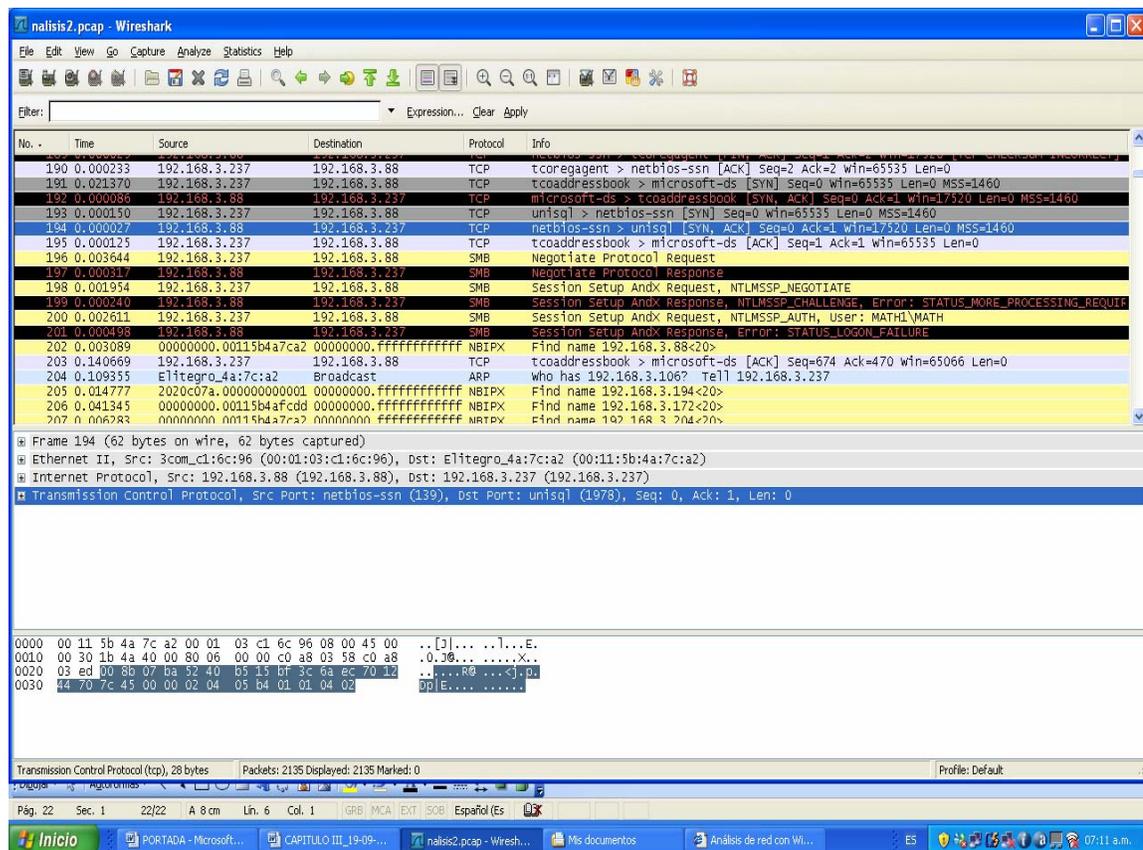


Figura 12. Pagina de captura de tráfico con la aplicación Wireshark

Para filtrar la información del monitoreo se selecciono la opción **Analyze/Display Filters**, como se muestra en la Figura 12. En esta pantalla se puede observar distintos tipos de filtrados que se deseen aplicar de acuerdo a lo que se quiere saber. Para el análisis de nuestro estudio se selecciono **TCP only**, el cual produjo la información que muestra la Figura 13.

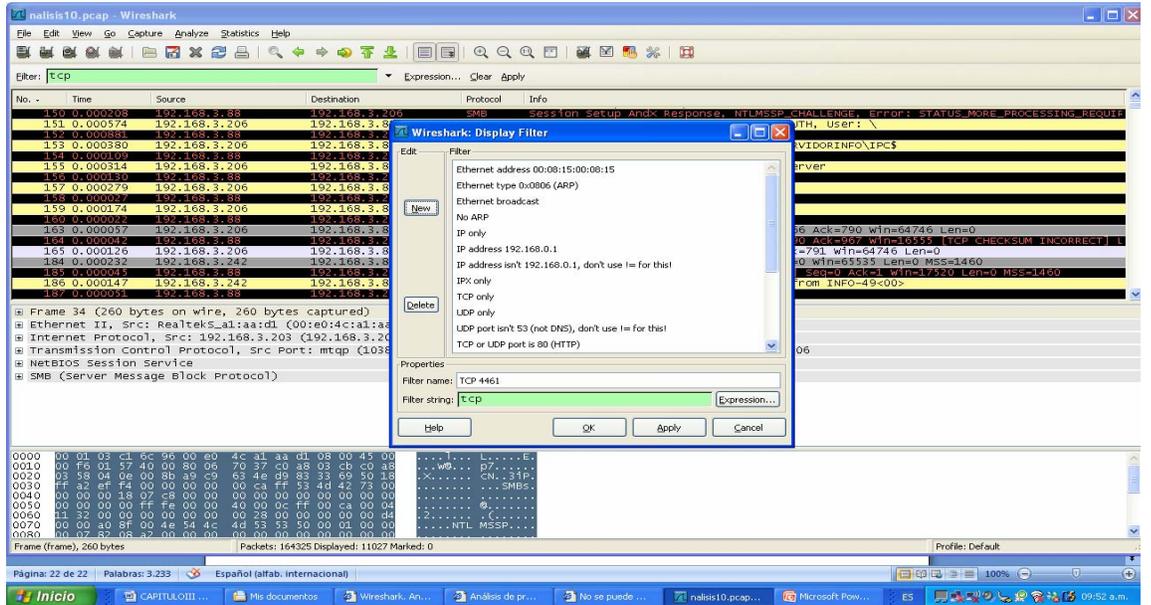


Figura 13. Pagina para filtrar información con la aplicación Wireshark

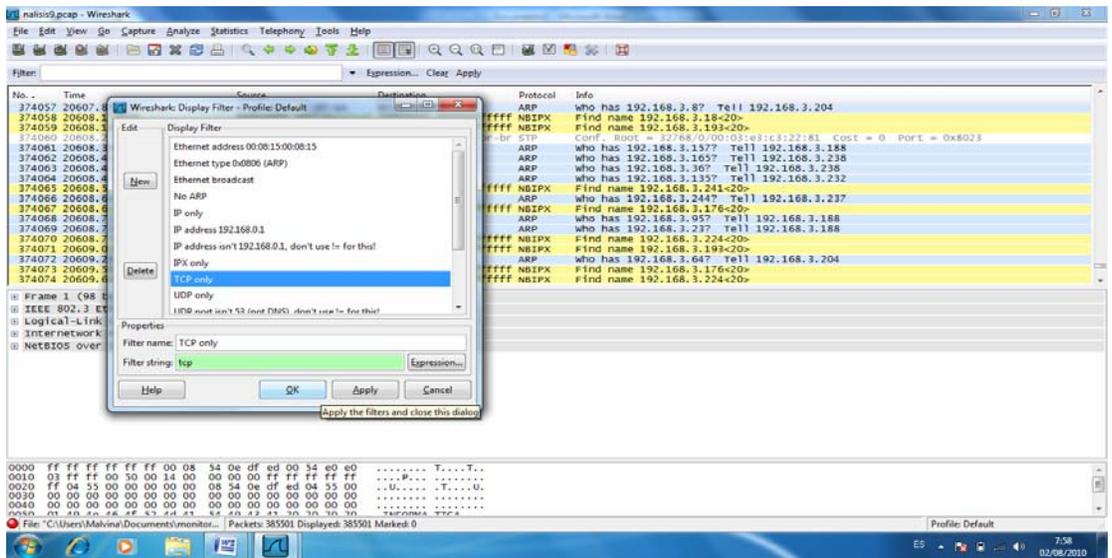


Figura 14. Pagina se selección del filtro usando la aplicación Wireshark

3.6.1 Análisis del tráfico de la red

El análisis del tráfico de la red permitió conocer la cantidad de información que circula por la red así como la velocidad de transferencia que circula por el canal de

transmisión.

El monitoreo se realizo en un periodo de cinco días durante cinco horas aproximadamente, para esto fue necesario la instalación un servidor provisional en el cual se instalo la herramienta *Wireshar* que permitió realizar un seguimiento y análisis de los protocolos a través de la captura de paquetes en tiempo real.

El desempeño de la red se determino a través de parámetros como: cantidad de tráfico, tasa de transferencia y porcentaje de utilización.

A continuación se muestra un resumen de la información obtenida a través de *wireshar*.

		Periodo de análisis (días)				
Trafic						
o de red		1	2	3	4	5
bytes		15,281	104,72	19,424	23,252	23,182
por sec		56	019	19	74	34
Mega			5158,2	1096,7	1612,6	1223,2
bytes		729,8	12	5	78	52
Paquet		16432		21682	25990	26358
es		5	385501	6	6	3

Tabla 3 Resumen información monitoreada

En la tabla 3 se puede observar la información capturada durante los cinco días de monitoreo, la cual sirvió para analizar y graficar el trafico de la red (ver grafica 13 y 14).

A través de las graficas se puede observar que el cuarto día de monitoreo hubo una aumento considerable de la cantidad de información que se transfirió; el cual se produjo por problemas de conectividad que presento la red. Esto se pudo evidenciar a través de otros parámetros ya establecidos que permitieron conocer la existencia de un problema de red relacionado con pérdidas de paquetes o segmentos.

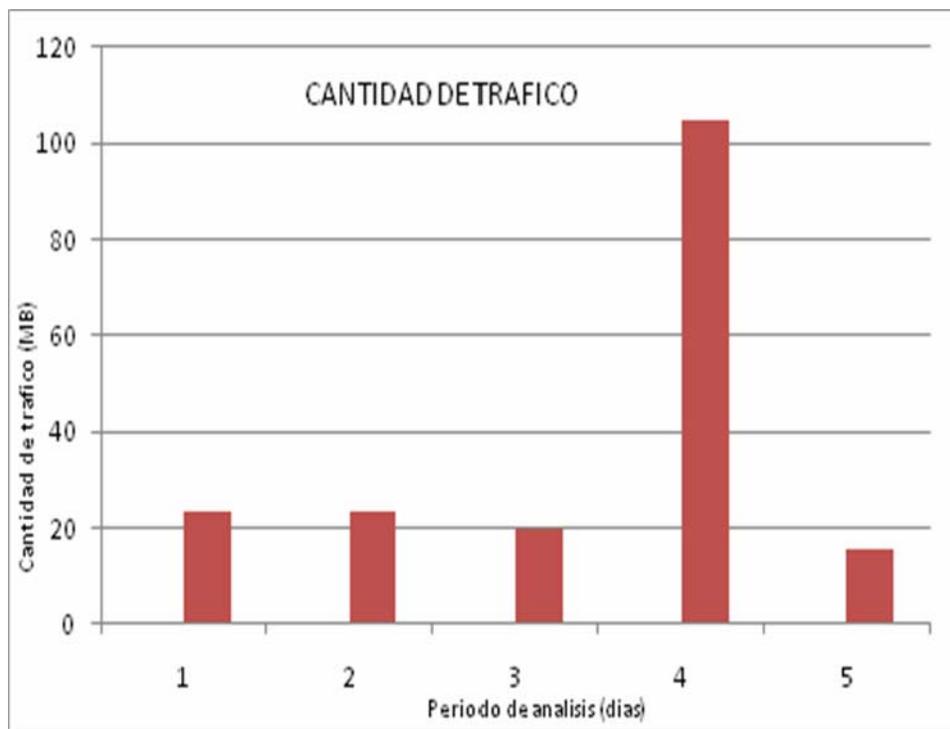


Figura 15 . Cantidad de trafico monitoreado

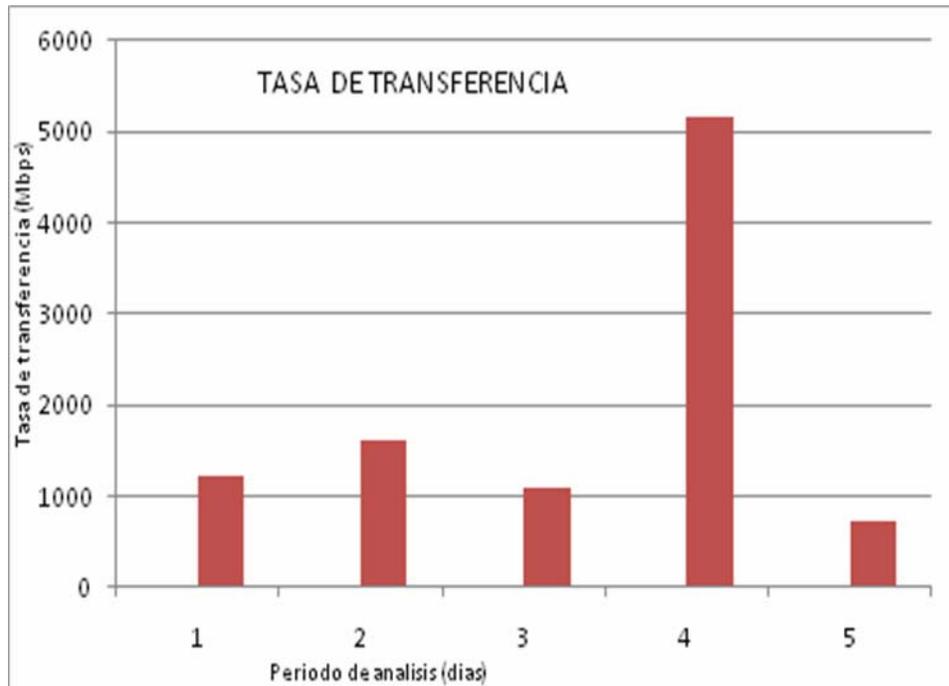


Figura 16 Tasa se transferencia monitoreada

Los siguientes parámetros permiten cuantificar y por consiguiente realizar una mejor gestión de la evaluación de la red:

- .- TCP *previous segment*
- .- Dup ACK
- .- TCP Retransmission

Las cuales permiten conocer la existencia de un problema de red en relación a perdidas de paquetes o segmentos, lo que puede producir una retransmisión de segmento o paquete perdido.

TCP Previous segmento lost nos indica que un segmento TCP anterior ha fallado. Un TCP Dup ACK puede deberse a un desorden de paquetes que hace que el receptor provoque un ACK duplicado ante un segmento que no sigue la secuencia normal. Puede deberse también debido a la pérdida de algún segmento de datos. Al recibir segmentos no ordenados, se genera ACKs duplicados, se reenvía nuevamente el mismo ACK (acuse de recibo), es decir nuevos requerimientos para recibir el segmento de forma correcta.

El problema también puede deberse a incremento de tiempo en la transmisión del paquete, retraso del paquete, con lo que se espera nuevos ACKs duplicados.

TCP *Retransmission* ocurre, explicado de forma muy básica, cuando el cliente no obtiene respuesta a un requerimiento y vuelve a reintentarlo.

En resumen podemos decir que cuando ocurre un TCP Previous segment lost se indica que durante el curso de transferencia de datos, un paquete se ha perdido o tarda en ser transmitido. En respuesta, el cliente envía un paquete TCP Dup ACK al servidor, solicitando que el paquete perdido sea enviado nuevamente. El cliente seguirá enviando ACKs duplicados hasta que sea atendida la petición.

Cuando se pierde algún segmento de datos tanto por errores del canal o por problemas de congestión TCP recibe segmentos fuera de orden y en consecuencia genera ACK duplicados. Puede ser consecuencias de picos de retardo o desorden de paquetes. Podemos decir entonces que los ACKs duplicados son síntomas también de un problema en la red. Cuando se reciban 3 ACKs duplicados es entonces cuando aparece el mecanismo de *Fast Retransmit* o Retransmisión rápida que vemos en las capturas que consiste en la retransmisión de segmento perdido.

3.7 Definición de las políticas de red

En esta fase se definieron las políticas de seguridad que debe resguardar la red del Programa de la Licenciatura en Informática, para ello se implemento la metodología que sigue la academia Cisco para administrar redes.

De acuerdo a esta academia la seguridad de redes debe estar enfocada al control de acceso y a la recuperación de datos.

La seguridad de acceso esta relacionada a la seguridad lógica y física que posee la red.

3.7.1 Seguridad Lógica.

La seguridad logica define el esquema para el control de acceso y seguridad de los atos y aplicaciones de la red y contempla todo aquello que tenga que ver con la administración de usuarios (niveles de acceso, perfiles, administración de claves de acceso, etc.), así como el control de aplicaciones, entre otros.

Para proporcionar seguridad logica a la red en estudio se definio como principal politica de seguridad la creación de cuentas de usuarios, la cual proporciona mecanismos de identificación y autenticación del usuario y la validación de los derechos y privilegios de éstos sobre los recursos de la red. Este esquema de acceso fue definido de acuerdo a los requerimientos de información de cada usuario.

Cada usuario identificado en el sistema va a tener ciertas cualidades y características que van a definir sus posibilidades de acceso y utilización de los recursos disponibles en la red.

Estos permisos de acceso a la red deben ser otorgados según su condicion de usuario (estudiante, administrador o docente) y las necesidades de cada uno.

Para los permisos de accesos se tomara en cuenta:

1. Las aplicaciones estándares están disponibles para que todos los usuarios las puedan ejecutar en cualquier momento; sin embargo, existen aplicaciones especiales que sólo algunos usuarios podrán acceder. Si el usuario necesita alguna de estas aplicaciones hay que otorgarle los accesos correspondientes.

2. Si el usuario solicita acceso a directorios comunes en un grupo, (una vez confirmada su autorización), según lo especificado en el grupo correspondiente, le autorizarán los derechos necesarios sobre dicho directorio.

Se creara una cuenta de usuario cuando este requiera integrarse a red para usar los servicios que esta ofrece, para ello de debera:

1. Definir el perfil del usuario y proceder a crearlo, según los requerimientos de éste.

2. Habilitar la cuenta para el acceso a la red, asignando el usuario, al (a los) grupo(s) necesario(s), para que pueda hacer uso de los recursos que necesita.

Dependiendo de los requerimientos practico- teorico que requiera cada usuarios de la red y para mantener la seguridad y la integridad de los datos y aplicaciones, se deben establecer perfiles de usuarios que regulen el acceso a la red y la utilización de los recursos de ésta.

Dentro de las politicas de acceso definida se determino:

1. El acceso de los usuarios a los servicios de la red se hará a través del mecanismo de autenticación mediante la identificación del usuario (*username*) y una palabra clave (*password*).

2. Sólo tendrán acceso a la red los usuarios a quienes les sean asignados su cuenta de usuarios. Esta asignación se hará a aquellos estudiantes o docentes pertenecientes al programa de la licenciatura en informática y que requieran hacer uso de los servicios de la red

3. Sólo será permitida una cuenta por usuario.

4. El nombre del usuario (*username*) estarán conformados por un código: las primeras letras del nombre y el apellido y una cifra de tres dígitos.

5. Los *usernames* definirán los derechos y privilegios que tendrán los usuarios en la red, así como los recursos y servicios que podrán utilizar.

6. Una vez realizado con éxito la creación de cuentas, el usuario deberá ser ubicado automáticamente en su directorio de trabajo, en el cual se encontrará todos sus archivos .

7. Los usuarios podrán hacer uso de cualquiera de los equipos de la red, pero respetando el número máximo de conexiones simultáneas a la red permitidas por usuario que es de una (1).

8. Debe existir un directorio público, sobre el cual todos los usuarios tienen todos los derechos y donde estos usuarios podrán colocar archivos de datos que deseen compartir con otros usuarios.

9. Los privilegios de los usuarios sobre los directorios y archivos del sistema operativo y de las aplicaciones deberán ser mínimos para evitar que éstos puedan modificar o borrar algún archivo; sólo tendrán acceso a los directorios de sistemas de las aplicaciones existentes en los servidores para lectura y así poder ejecutar las aplicaciones.

La definición de grupos de usuarios se hará de acuerdo a las áreas educativas del programa de la licenciatura en informática y a las aplicaciones que se instalen, tomando en cuenta:

1. Existirá un grupo por cada materia práctica/teórica de la Licenciatura Informática, al cuál debe pertenecer cada estudiante de dicho programa. Con la asignación de los usuarios a esos grupos se permitirán servicios comunes y la posibilidad de compartir datos entre ellos.

2. Para las funciones de administración de los sistemas operativos, manejadores de bases de datos y las aplicaciones, existirán grupos definidos por cada una de las funciones asociadas. Estos grupos poseerán características y derechos para permitir a sus miembros la realización de las tareas asociadas con sus funciones.

3. A medida que sean incorporadas más aplicaciones a la red, éstas deben ser definidas para los usuarios y los grupos para las cuales estén destinadas.

4. Para cada aplicación de bases de datos existirá un grupo definido con los atributos y derechos sobre directorios necesarios para poder acceder dicha aplicación, desde el punto de vista del sistema operativa.

5. Cada usuario perteneciente a un grupo, dependiendo de sus características puede tener distintos niveles de seguridad sobre las aplicaciones, acceso a red y entorno gráfico.

. La permisología de cada uno de los usuarios se realizará mediante la asignación de los usuarios a los grupos correspondientes, evitando así la asignación individual de derechos a cada uno de los usuarios.

7. Existirá un usuario Administrador para cada servidor. Este usuario será el encargado de administrar los parámetros y otorgar las permisologías a los usuarios para acceder a las aplicaciones .

Los usuarios tendra por defecto las siguiente restricciones:

El número de conexiones concurrentes será limitado y el número máximo de conexiones concurrentes permitidas será de una (1).

Para cada usuario nuevo que sea definido deberá crearse un directorio raíz (home), donde el usuario podrá colocar sus datos personales

Es obligatorio que todo usuario en la Red tenga asignado un password como medida de seguridad para el acceso a la red.

Es obligatorio el cambio periódico de los password y los usuarios deberá hacer cambios por claves únicas.

Esto quiere decir que cuando un usuario debe cambiar su clave, no podrá usar las anteriormente empleadas.

Se permitirán sólo tres (3) intentos no exitosos de conexión a la red.

En relación a los servicios de red, se debe asegurar que los usuarios que hagan

uso de ellos, utilicen adecuadamente estos servicios de acuerdo a las restricciones establecidas.

Se debe procurar reducir al mínimo los servicios que no sean necesarios en la red y documentar la política implementada por servicio.

Uno de los servicios que se encuentran activos en la red son: correo electrónico e Internet.

Políticas para el uso de correo electrónico

El usuario deberá cerrar su sesión de este servicio al culminar la sesión de trabajo.

Toda información contenida en el correo electrónico del usuario será de su responsabilidad.

El usuario será responsable de la información que sea enviada con su cuenta, por lo cual se asegurará de no mandar SPAMS de información, ni de mandar anexos que pudieran contener información nociva para otro usuario como virus o pornografía.

Queda prohibida la activación de más de una sesión de este servicio por usuario o código.

Políticas para el uso de Internet

Toda conexión hacia este servicio deben efectuarse a través de los firewalls o cortafuegos disponibles para tal fin; por lo tanto, las conexiones por modems o tarjetas similares quedan prohibidas, a menos que estén expresamente autorizadas.

Cuando se efectúen servicios de FTP (File Transfer Protocol) los archivos bajados deben ser pasados por procesos de antivirus antes de ser utilizados.

No deberá enviarse información confidencial hacia Internet a través de las redes de la institución, amén que esté expresamente autorizado y protegido con los servicios exigidos de seguridad.

El administrador de la red debe garantizar la implantación de mecanismos de encriptación para información confidencial que se envíe hacia Internet.

Para evitar problemas de virus informáticos y horas de trabajo en la reconfiguración o servicio, se prohíbe la instalación de programas y la modificación de los programas, paquetes y configuraciones ya instalados en las estaciones o red.

Se debe impedir que las direcciones IP (sólo alias o sobrenombres), protocolos (sólo traducción) y contraseñas o password (reusables) transiten a través del firewall.

Está totalmente prohibido bajar o consultar información e imágenes pornográficas.

En caso de requerir algún software nuevo o la modificación de alguno ya instalado, favor de solicitarlo al docente o al coordinador de la materia respectiva para que este haga la solicitud respectiva al administrador de la red.

3.7.2 Seguridad Física.

La seguridad física permite asegurar el acceso únicamente al personal autorizado a las áreas donde se encuentran ubicados los equipos de procesamiento y transmisión de datos, así como también vigilar que el ambiente de seguridad donde se encuentren ubicados los datos sea lo más adecuado y seguro posible.

La seguridad física debe ser implementada eficientemente para reducir el riesgo resultante del acceso no autorizado a los equipos de procesamiento y

transmisión de datos. Únicamente debe ser permitido el acceso a personal autorizado y todo acceso de visitantes debe ser aprobado por el Coordinador de Seguridad y monitoreado por el Administrador de ella.

Los procesos relacionados con la seguridad física de las instalaciones de procesamiento de datos son:

Sólo tendrá acceso a las áreas restringidas el personal encargado de la Administración.

El control de acceso físico a los cuartos de computación donde se encuentran los equipos de la red lo ejercerá el Coordinador del programa de la licenciatura en informática, otorgando acceso al administrador de la red que requieran realizar sus funciones.

Cualquier persona que requiera entrar al cuarto de cableado deben estar debidamente autorizados y supervisado por la coordinación.

Se consideran áreas restringidas: Cuartos de cableado de la red, Salas de servidores y cualquier lugar donde se encuentren dispositivos de red.

Sólo tendrán acceso a áreas restringidas aquellas personas que para cumplir sus funciones requieran entrar a ellas.

Controles de planta física

El acceso a el cuarto de cableado llevarse de la manera más estricta posible.

La mayoría de los equipos de computación y de telecomunicaciones deben encontrarse en un ambiente con condiciones óptimas de temperatura, humedad y

polvo para garantizar el buen funcionamiento y prolongar el tiempo de vida útil de los mismos.

Es recomendable que cualquier equipo que se instale sea colocado en el Centro de Cómputo debido a que en éste ya se han dispuesto controles ambientales de comprobada funcionalidad.

Cualquier lugar donde vayan a ser instalados equipos para la Red, debe ser acondicionado para garantizar el buen funcionamiento de los equipos y minimizar el riesgo de fallas que afecten a los usuarios y los servicios de la Red.

Debe mantenerse un inventario de los equipos de computación para llevar un control de los equipos y dispositivos que están siendo destinados a los servicios de la red.

Debe mantenerse un inventario estricto del software y hardware.

Es recomendable conectar cada servidor a una unidad de suministro de electricidad ininterrumpida (*Uninterruptible Power Supply UPS*), para proveer energía de respaldo si el suministro comercial falla.

El propósito de adoptar medidas de seguridad en redes es proteger la red contra intrusos, prevenir el uso no autorizado de los sistemas y proteger la información de los usuarios de la red. Esto se resume en el diseño de una política de seguridad, que refleje los resultados de la evaluación de la seguridad de la red y esté complementada por la selección de herramientas que ayuden a mantener la inviolabilidad de la misma. Sin embargo, es necesario tener presente que con estas herramientas no se esta libre de posibles ataques.

3.8 Definición del plan de gestión

De acuerdo a la metodológica Métrica, el plan de acción debe definir los proyectos y acciones a llevar a cabo para implementar, en nuestro caso, la gestión de redes, según las necesidades y el diseño propuesto para gestionar las redes de la Licenciatura en Informática.

En la Tabla N°4 se describe en forma breve el plan de gestión para la red del Programa de la Licenciatura en Informática. En este plan se detallan las tareas y funciones que deben ser ejecutadas para gestionar la red.

Dentro de las actividades y/o funciones de administración de redes que se determinaron para gestionar la red del Programa de la Licenciatura en Informática se encuentran: configuración, desempeño, mantenimiento, averías, documentación y seguridad.

Configuración

El objetivo de configuración es lograr un manejo adecuado de los recursos de hardware y software. En base al área funcional de configuración que propone el modelo OSI para la gestión de redes se propusieron mecanismo tanto para la instalación de hardware como de software que permitieran realizar estas configuraciones tomando en cuenta las necesidades y topología de la red. De igual forma las instalaciones deben ser realizadas por personal técnico capacitado para tal función. Dentro de los procesos a seguir para las configuraciones se determino:

Hardware

La instalación de algún hardware debe ser realizada por personal técnico capacitado para tal función, dentro de las tareas de instalación de hardware debe

contemplar la agregación, sustitución o reemplazo de alguna pieza.

Las instalaciones de hardware podrán hacerse en algunos de los siguientes casos:

Incorporación de equipos nuevos

Reparación o sustitución de algún equipo o pieza

Antes de cualquier instalación se deberá realizar un estudio previo para asegurará que el equipo o parte a ser instalada sea compatible con los componentes existen en la red.

La fecha de ejecución de la instalación debe ser programada así como su tiempo de duración

Notificar de forma anticipada a los usuarios

Documentar cada instalación y cambio que sufra cualquier equipo o componente de la red.

Software

Las instalaciones de software podrán hacerse cuando se incorporación algún equipo o cuando sea necesario actualizar o sustituir de algún software y en caso de que algún usuario necesite una aplicación que no esté instalada, en tal caso deberá solicitar tal instalación al administrador de la red.

Antes de cualquier instalación de software se debe:

Asegurar que la memoria y almacenamiento sean suficientes para instalar el

software

Verificar las versiones actuales y las que se pretende instalar sean compatibles.

Realizar respaldo de configuraciones

En cualquier caso, sea por nueva instalación, actualización o reparación de algún equipo de

deberá documentar cada instalación, así como los cambios que sufra cualquier equipo o componente de la red.

Desempeño

Esta actividad permite recolectar y analizar el tráfico que circula por la red para determinar su comportamiento y permita tomar decisiones pertinentes al comportamiento de la red.

El modelo de gestión de redes OSI nos proporciona un área funcional para gestionar el desempeño, el cual tiene que ver con la evaluación del comportamiento de la red, razón por la cual se determino el uso de herramientas que permitieran realizar un monitoreo que le permitiera al administrador o encargado de la red observar y recolectar información referente al comportamiento de la red en aspectos como:

Característica de tráfico.

A través de cualquier herramienta (para este caso de estudio se utilizo wireshark) se puede detectar los diferentes tipos de tráfico que circulan por la red, con el fin de obtener datos sobre los servicios de red (http, ftp, etc) que son más utilizados

y de esta forma establecer un patrón en cuanto al uso de la red.

Transmisión y recepción de información

Conocer los elementos de red que tiene mayor solicitud como servidores, estaciones de trabajo puertos y servicios. Una vez capturado el tráfico se podrá analizar la información recolectada y se recomienda interpretarla para determinar el comportamiento de la red y así tomar decisiones adecuadas que permitan mejorar su desempeño, para esto se debe tomar en cuenta:

Para el análisis del comportamiento de la red se debe tomar en cuenta los siguientes parámetros:

Tasa de transferencia; velocidad de transmisión que pasa por una línea de comunicación.

Cantidad de Tráfico: cantidad de información promedio que se transfiere por el canal de comunicación.

Porcentaje de Utilización: relación entre el tráfico medido al tráfico máximo que el puerto puede administrar.

Conociendo la tasa de transferencia y la cantidad de tráfico promedio que circula por la red del programa de la Licenciatura en Informática se puede crear líneas base que nos permitan tener una idea de los que circula regularmente por la red, y detectar de forma rápida alguna anomalía cuando estas líneas base no se encuentren dentro de los rangos frecuentes.

De igual forma el porcentaje de utilización será adecuado mientras se encuentre por debajo del 65%, lo cual indica que la red es estable y se puede mantener operativa independientemente de la cantidad de usuarios que se conecten a ella.

Además se debe tener por regla general que si se produce una pérdida de paquetes o segmento, automáticamente se realiza un reordenación de los mismo, en caso de que esto ocurra se debe esperar hasta 3 ACKs duplicados, de lo contrario existiría pérdida de paquetes y generaría problemas de congestión en la red. Por regla general:

.-Solo esperar hasta 3 ACKs duplicados.

.-Uno o dos ACKs duplicados indica una reordenación de los segmentos.

.-Tres o más ACKs duplicados indica que se perdió el paquete.

Mantenimiento

El mantenimiento propuesto por el área funcional de desempeño, nos permite aplicar medidas que logren aumentar la disponibilidad de la red, es por ello que en esta actividad se propone conocer las condiciones de operatividad de los equipos, así como reconocer si existe la necesidad de reparar o reemplazar un equipo, antes de que se presente una falla.

El mantenimiento debe realizarse de forma preventiva para anticipar cual falla o problemas que pueda presentar cualquier dispositivo de la red.

El mantenimiento correctivo se realizara cuando se presente la falla o el problema con el equipo.

Averías

Las averías tiene que ver con la detección, aislamiento y corrección de

operaciones normales de la red, el plan de gestión tiene la capacidad de permitir configurar y reconfigurar los dispositivos que presenten fallas o cambios en la estructura de la red. Dentro de los pasos a seguir se determino:

1. El administrador de red deberá realizar de forma periódica un mantenimiento a los equipos que conforman la red.

2. El mantenimiento debe realizarse de forma programada con el fin de no afectar a los usuarios y debe servir para realizar inspecciones, tanto de funcionamiento como de seguridad, ajustes, reparaciones, limpieza con la finalidad de evitar posibles averías o fallas en situaciones futura.

3. El mantenimiento preventivo se realizara en un periodo de seis meses (o al final de cada semestre) esto ayudara a determinación las condiciones operativas, de durabilidad y de confiabilidad de un equipo , y reducir los tiempos que genera un mantenimiento correctivo.

4. En caso de producirse una falla o avería en los equipos se deberá realizar un mantenimiento correctivo, el consiste en repara un equipo que ha presentado fallas.

5. Las reparaciones deben ser ejecutadas una vez que se ha generado una falla y atendidas de forma inmediata por el administrador para restablecer la situación o minimizar el impacto que puede causar a la red.

6. Dentro del proceso de reparación se debe determinar el origen de la falla y realizar pruebas de diagnósticos (física, lógica y medición).

7. Las fallas pueden depender de la tecnología de red, dentro de los mecanismos de recuperación de fallas a nivel de red se tienen: Recarga del sistema, Reemplazo

de recursos, Instalación de software y Cambios en la configuración.

8. Una vez detectada y reparada la falla se deberá actualizar el inventario y realizar la documentación de la falla presentada con el proceso de solución aplicado a dicha falla.

Documentación

El objetivo de realizar inventario a la red es el de conocer los elementos que posee la red y llevar un historial de cada problema y solución que presenta algún equipo de la red.

El administrador de la red deberá realizar inventario de los equipos cada vez que sea instalado un equipo y cuando se realice alguna reparación o sustitución de partes en algunos de ellos, esto con la finalidad de mantener información actualizada sobre los componentes que conforman la red así como su configuración. El inventario debe mantenerse actualizado con los registros de mantenimientos o reparaciones que sufra cada equipo o dispositivos.

El inventario debe contener información como; Diagramas indican la disposición lógica y física de los dispositivos, La disposición del cableado físico, Longitud del cable, Tipo de terminación para el cable, Ubicación de cada tomacorriente o conexión y Esquema de rotulación de cada punto de red, software instalados, fallas presentadas y soluciones aplicadas en cada caso.

Seguridad

La gestión de seguridad del modelo de gestión de redes está dividida en tres rubros: seguridad física, seguridad lógica y seguridad de datos, lo que nos indica que

el plan de gestión deben proveer un marco referencial de cómo deben actuar los usuarios y administradores de la red para prestar una mayor seguridad, para ellos se determinaron políticas de acceso, así como los deberes y prohibiciones en materia de seguridad.

Las siguientes instrucciones están dirigidas a todos los usuarios que usan los servicios de la red del programa de la licenciatura en informática, a los fines de incorporar en sus rutinas de trabajo.

1. Todos los activos de información, manejados a *través* de la red, deberán ser protegidos de manipulación, alteración, revelación, destrucción y de cualquier hecho, accidental o no, que altere la integridad de los mismos.

2. Todos los usuarios de la red serán responsables de administrar la seguridad, según los lineamientos internos establecidos, y de crear los mecanismos de control de acceso a la información por ellos manejada. La coordinación de la licenciatura serán los responsables de desarrollar la conciencia de seguridad en la institución.

3. Los administradores de la red será responsable de identificar y proteger todos los activos de información que están dentro del área asignada a ellos, para su control y administración, y de implantar las prácticas de seguridad en su área de adscripción.

4. Todos los usuarios de la red deberán considerar las prácticas de seguridad al momento de generar los activos de información, así como también al momento de manipular los mismos, a fin de resguardarlos y garantizar su confidencialidad e integridad.

5. La coordinación de la licenciatura serán los responsables de desarrollar los criterios de actuación del personal en materia de seguridad, así como también de diseñar los mecanismos o procedimientos de control que garanticen la salvaguarda de

los activos de información, a los fines de llevar a cabo las políticas recomendadas y poder monitorear el cumplimiento de las mismas.

A continuación se presenta un conjunto de instrucciones, desarrolladas para resguardar la seguridad de la información que maneja la red. Estas instrucciones van dirigidas fundamentalmente a los usuarios y administradores de la red, con el fin de dar seguridad de la red.

1. Modificar periódicamente las claves personales asignadas por el administrador para tener acceso a la red.

2. Acatar todos los criterios y lineamientos de almacenamiento y respaldo de datos. Velar por el buen funcionamiento de los equipos que le sean asignados o usados en las distintas salas de computacion.

3. Mantener respaldada y guardada, en un lugar seguro, la información que haya sido clasificada como de alto riesgo o confidencial que se encuentre bajo su responsabilidad, así como los medios de almacenamiento, manuales y listados de información.

4. Cerrar la sesion una vez finalizada la sesion de trabajo.

5. Notificar de inmediato al administrador de la red, cuando exista la sospecha o se descubra que su información ha sido manipulada sin autorización.

6. Reportar al administardor cualquier desperfecto, modificación de la configuración o instalación de programas que afecten al equipo.

7. Seguir las instrucciones emitidas por la coordinacion sobre la estructura de directorios

en los discos fijos.

Para prevenir ataques de virus se debe:

1. Revisar periódicamente el sistema (discos fijos, memoria RAM), con un programa antivirus aprobado por la coordinacion para la detección de posibles virus informáticos.

2. Al detectar o sospechar la existencia de virus informáticos en el equipo, reportarlo al administrador de red.

3. Revisar cualquier dispositivos (*pendrive*, CD, DVD, etc), que vayan a ser utilizados en alguna de las unidades de los equipos de la red, a fin de asegurar que no contenga ningún virus informático.

4. No continuar usando los equipos de la red cuando sospeche la existencia de virus informáticos y abstenerse de tomar medidas para la eliminación de los mismos.

Para evitar situaciones que comprometan la seguridad de la red, los usuarios no deben:

1. Divulgar la clave personal de la red , que le esté asignada para el acceso a los servicios de la red.

2. Realizar la instalación de cualquier programa o aplicación en las estaciones de trabajo, sin la autorización de la coordinacion .

3. Instalar programas ilegales (sin licencia) en los equipos de computación de la red.

4. Acceder a la red con las claves de acceso y equipos asignados a otros usuarios sin su previa autorización.

5. Comer, beber o fumar mientras esté utilizando los equipos de computación de la empresa o dentro de las instalaciones de computación.

6. Usar los equipos de computación de la red para la ejecución de juegos informáticos.

7. Realizar copias no autorizadas de programas instalados en su computador.

8. Instalar programas o aplicaciones en los directorios de datos de los servidores.

9. Utilizar los equipos de computación e información de la red para fines distintos a los cuales están destinados.

Con el fin de no comprometer la seguridad de la red, todos los administradores de red deben:

1. Mantener en estricto grado de confidencialidad las cuentas y las claves de acceso de los administradores y de los usuarios.

2. Realizar periódicamente respaldos de la información contenida en los directorios de datos de los servidores, con las aplicaciones seleccionadas y bajo los criterios establecidos, y realizar continuamente pruebas de recuperación de la información.

3. Guardar los medios de almacenamiento y respaldo de los datos de los usuarios, manuales y listados de información en un lugar seguro, y definir un

esquema de respaldo de la información así como los lugares alternativos donde se realizarán los respaldos.

4. Documentar las configuraciones de los equipos servidores, dispositivos, programas, aplicaciones, así como también cualquier cambio efectuado en las mismas.

5. Mantener actualizada la bitácora con las actividades diarias de cada servidor de la red, reflejando la operación realizada y la persona responsable.

6. Notificar por escrito al Coordinador, sobre cualquier cambio, problema o incidente de seguridad que ocurra en la red.

7. Definir los perfiles de usuario de acuerdo con los requerimientos de éstos y asegurarse de que puedan acceder a todas las aplicaciones solicitadas y a sus datos.

8. Realizar inducción a todo el personal de la red acerca de las medidas de la seguridad de activos de información.

9. Asegurar que todos los programas, aplicaciones, sistemas operativos, equipos y dispositivos instalados o conectados a la red, posean funciones de seguridad acordes con los requerimientos de los usuarios.

Para prevenir posibles ataques de virus se debe:

1. Revisar periódicamente la memoria de los servidores de la red (discos fijos, RAM), con un programa antivirus.

2. Evaluar y proponer alternativas de automatización y actualización de las facilidades para la detección y eliminación de virus informáticos de los servidores.

3. Implementar mecanismos que aseguren la integridad de los datos e informaciones de los usuarios en la red.

4. Definir, diseñar, e implementar procedimientos de verificación, eliminación y recuperación de la información en caso de incidentes de virus informáticos.

a evitar situaciones que comprometan la seguridad de la red, los administradores de la red no deben:

1. Copiar archivos de datos en los directorios de aplicaciones del servidor.

2. Copiar o instalar programas o aplicaciones en los discos de datos de los usuarios de la institución.

3. Facilitar la información o el acceso a ella a alguna persona, ajena o interna a la institución, que no esté autorizada para conocer o utilizar dicha información.

4. Acceder a la información de los usuarios almacenada en los discos de los servidores de la red.

Para hacer cumplir estas instrucciones de debera:

1. Divulgar y asesorar las normas y políticas existentes sobre el uso y manejo de los recursos, desde el más alto nivel operativo, y apoyar en la concientización de los usuarios para que actúe con conocimiento de causa en el tratamiento que debe darse a dichos recursos.

2. Mantener un programa de motivación y adiestramiento para la difusión de las normas y políticas existentes relacionadas con la seguridad de la información, hardware, software y cualquier documento considerado propiedad de la red.

3. Ejecutar y hacer cumplir las políticas de seguridad.

4. Velar porque los usuarios de la red cumpla, en forma optima, los procedimientos y normativas establecidos para la seguridad de activos de información.

5. Velar porque, al finalizar de cada jornada de trabajo, todos los equipos sean apagados.

6. Canalizar las acciones necesarias, en caso de que los usuario infrinja alguna norma o políticas existentes.

En cuanto a las medidas a tomar en caso de incumplimiento de las Políticas de Seguridad establecida, se deberá:

1. Determinar la identidad del infractor o de los infractores.

2. Determinar si el infractor es de origen interno o externo a la red.

3. Identificar si la violación ocurrió por negligencia personal, accidente o error, ignorancia de la política.

4. En caso de no disponer de las pruebas necesarias para inculpar al infractor se le permitirá continuar con su conducta hasta obtener la información suficiente y así aplicar las sanciones.

5. En caso de contar con las pruebas necesarias, se procederá a detener las acciones del infractor y aplicar las sanciones.

6. Los usuarios, sean estudiantes o docentes, que violen o incumplan las normas o políticas y procedimientos establecidas serán sometidos a las sanciones.

Para concluir, es importante no solo cumplir con el plan de gestión planteado, si no evaluarlo constantemente para así determinar su buen funcionamiento y brindar un servicio óptimo y funcional a sus usuarios, es por ello que es importante determinar parámetros o métricas que permitan evaluar cómo se desarrolla el plan de gestión.

A continuación se presenta una tabla (ver tabla n° 5) la cual identifica las métricas a utilizar con sus indicadores y procesos donde deben evaluarse para determinar el funcionamiento de los servicios que se desarrollan en la red del Programa de la Licenciatura en informática.

Tabla 4 Resumen del Plan de gestión para la red del Programa de la Licenciatura en Informática

Definición	Objetivo	Actividades	Calendario	Pa
Configuración	Lograr un manejo adecuado de los recursos de hardware y software	Verificar requerimientos de instalación	Antes de cualquier instalación	Ad
		Programar instalación	Cuando se necesite instalar dispositivo	
		Configurar e instalar recursos (hardware- software)	Cada vez que ingrese un dispositivos nuevo o cuando el equipo requiera	
		Documentar las configuraciones	Cada vez que se instale un hardware - software	
Desempeño	Esta actividad permite recolectar y analizar el tráfico que circula por la red para determinar su comportamiento y permita tomar decisiones pertinentes al comportamiento de la red.	Monitorear trafico de red	Diariamente	Ad
		Analizar Monitoreo	Diariamente	
		Tomar acciones sobre monitoreo	Cada vez que sea necesario	
Mantenimiento	Determinar las condiciones operativas de los dispositivos y/o recuperar posibles fallas	Determinar operatividad de los dispositivos (mantenimiento preventivo)	al final de cada semestre	Ad
		Reparar fallas (mantenimiento correctivo)	cuando se presenten averías en dispositivos	
		Analizar fallas presentadas	Cada vez que se presente una avería	
		Actualizar documentación		
Averías	Determinar el origen de una falla y reparar la avería	Determinar origen de la falla	Al reportarse fallas o cuando el monitoreo lo presuma	Ad
		Realizar pruebas de diagnostico	Cuando se presente la falla	
		Realizar pruebas a nivel de red	Cuando se presente la falla	
		Reparar las averías		
		Actualizar Documentación	cada vez que ocurra una avería y su reparación	
Documentación	El objetivo de documentar la red es el de conocer los elementos que posee la red y llevar un historial de cada problema y solución que presenta algún equipo de la red.	Documentar hardware- software de cada dispositivos	al ingresar despóticos nuevo	Ad
			al final de cada semestre	
Seguridad	El objetivo es proveer un marco referencial de cómo deben actuar los usuarios y administradores de la red para prestar una mayor seguridad y dar a conocer los deberes y prohibiciones en materia de seguridad	crear cuentas de usuarios	Al ingresar estudiantes nuevo	Ad
		instalar y/o actualizar antivirus	siempre	Ad usua
		Hacer cumplir normas de seguridad	Diariamente	Ad usua

Tabla N° 5 . Normas o métricas para evaluar plan de gestión de la red del Programa de la Licenciatura en Informática.

Normas o Patrones para gestión de redes		Indicador	Descripción
OSI			
	Detección de virus	Número de veces detectados	porcentajes de virus detectados y eliminados oportuna mente
	Ataques prevenido	Numero de ataques prevenidos	porcentajes de ataques prevenidos
	tiempo de respuesta a los ataques	horas	tiempo promedio de restauración del sistema a partir de un incidente
	Averías	Numero de reclamos	Determina la cantidad de averías validas reportadas por los usuarios
	Tiempo de respuesta averías	horas	Tiempo que transcurre desde que se determina una avería hasta que se encuentre activo y disponible para su uso
ITIL			
	Reclamos de averías	Numero de reclamos	Mide la cantidad de reclamos en funcionamiento del servicio de la red
	Tiempo de respuesta a los reclamos	Horas	Tiempo de repuesta que transcurre desde que se inicia el reclamo hasta que sea solucionado el problema
	Violación normas de seguridad	Número de veces que viole una norma de seguridad	Porcentaje de violaciones de las normas de seguridad
COBIT			

	Jerarquía de protocolo	numero paquetes	mide en porcentaje el uso de protocolos detectados en la captura
	retardo en los paquetes	Previous segment	Métricas que miden el retardo en el trafico
	paquetes perdidos	acks duplicate	miden los paquetes perdidos en el trafico

CONCLUSIONES

El desarrollo de un plan de gestión para la red del Programa de la Licenciatura en Informática permite mejorar la disponibilidad y desempeño de la red, logrando de una manera sencilla conocer los dispositivos que conforman la red así como su comportamiento a través del monitoreo de los dispositivos.

Aida32 fue una de las herramientas para la gestión de red que fueron implementadas en la red del Programa de la Licenciatura en Informática y que permitió brindar un control de los activos de la institución, como software y hardware instalado así como conocer futuras actualizaciones a realizar, complementando y apoyando de esta manera los servicios ofrecidos por la coordinación del programa de la licenciatura en informática.

Wireshark es otra herramienta de gestión para el monitoreo de red que permitió conocer el tráfico de la red y apoyar las funciones de los administradores y técnicos.

Para culminar la implantación de herramientas de gestión de red permite incrementar substancialmente la prevención, detección y restablecimiento de los servicios, lo cual se traduce en satisfacción a los usuarios.

RECOMENDACIONES

Dados los resultados y el alcance de este trabajo, la Coordinación del Programa de la Licenciatura en Informática deberían propiciar y buscar situaciones que les permitan ir mejorando, cada vez más, la gestión de los servicios informáticos de la red. Para ello se recomienda la adquisición de dispositivos como servidores de red que permitan gestionar los procesos de forma óptima.

La gestión de redes es una herramienta fundamental en el desempeño y buen funcionamiento de la red, por ellos se recomienda realizar actualizaciones de herramientas que puedan prestar mayores beneficios en concordancia con los recursos con que cuenta la institución.

Con la finalidad de complementar las políticas de seguridad recomendadas y reforzar la seguridad de las redes de la red en estudio, se recomienda la implementación del firewall, el cual permite proteger la red contra logins no autorizados del mundo exterior y previene de intrusos que pretendan acceder la red privada. El firewall funciona principalmente bloqueando los accesos desde afuera hacia el interior de las redes, pero permite a los usuarios internos comunicarse libremente con el exterior.

BIBLIOGRAFÍA

- 1 Ministerio Administraciones Públicas (2005). Metodología de planificación de sistemas de información. España. URL: <http://www.csi.maap.es/csi/pg5m41.htm#3>
- 2 Stolz, K. (1995). Todo a cerca de... redes de computación. Editorial Prentice Hall Hispanoamericana, México, 518 pp.
- 3 Mendillo V. 2003."Gestión de redes", CD-ROM N° 1.Universidad Central de Venezuela, Caracas -Venezuela.
- 4 Ortega W. 2000. "Implantación de una herramienta de gestión en la electricidad de Caracas. Trabajo de grado. Facultad de Ingeniería. Universidad Central de Venezuela. Comisión de Postgrado.
- 5 Franco. A. 2002 . Aplicación de una Herramienta de gestión Networking en la red de datos de la UCV. Caso de estudio: Dirección de Informática. Facultad de Ingeniería. Universidad Central de Venezuela.
- 6 López M. 2002. "Selección e Implantación de un sistema de Gestión de Red en el Ministerio de Finanzas" .Trabajo de pregrado. Departamento de Ingeniería. Universidad Central de Venezuela. Caracas.
- 6 Universidad de Oriente Venezuela. 2007. Reseña histórica. http://www.udo.edu.ve/index.php?option=com_content&task=view&id=10&menunav=serv

- 7 Zacker, C. 2002. Manual de referencia redes (Primera Edición). Editorial McGraw Hill.Mexico.1046 pp.
- 8 Diccionario de Informática .2001. Editorial Cultural .Madrid-España.
- 9 “Capitulo 3: Redes de Telecomunicaciones”. (2002) Enciclopedia Técnico en Telecomunicaciones. Tomo I. Editorial cultural 186 pp.
- 10 GS comunicaciones. 1997. Telecomunicaciones de redes de Datos. Editorial McGraw Hill .DF. Mexico. 193 pp.
- 11 Aula Virtual Universidad de Oriente. Licenciatura en Informática: Gestión de redes. URL: <http://aulavirtual.sucre.udo.edu.ve/course/category.php?id=6>
- 12 Eeye Digital Security. Productos : Network Security Traffic Analyzer. URL: <http://www.eeye.com/html/products/iris/index.html>.
- 13 Soporte Remoto México. Artículos. en URL: http://www.soporteremoto.com.mx/help_desk/articulo04.html.
- 14 .Monografias.com. Administración y finanzas: en que consiste cobit. En URL: <http://www.monografias.com/trabajos38/cobit/cobit.shtml>
- 15 Wikipedia La enciclopedia Libre. Capability Maturity Model Integration. En URL: http://es.wikipedia.org/wiki/Capability_Maturity_Model_Integration

- 16 McAfee. Protección de Redes McAfee. en : URL:
http://www.nai.cl/es/products/sniffer/network/sniffer_portable_hs.htm
- 17 Wireshark. About Wireshark. URL: <http://www.wireshark.org/about.html>
- 18 Arias, F. (1997). El proyecto de investigación guía para su elaboración (Segunda edición). Editorial Episteme, Caracas, 107 pp.
- 19 Consejo superior administración electrónica. Servicios y productos / Metrica .
en URL : <http://www.csi.map.es/csi/metrica3/index.html>
- 20 Cisco System, INC (2002). Academia Networking system: Guía de 2do
Semestre (segunda Edición). Editorial Pearson Educación. Madrid 736 pp.

ANEXOS

APÉNDICE A

Descripción de los Procesos actuales

Referencia:1.0

Proceso: Instalación y mantenimiento.

Descripción: El proceso de instalación y mantenimiento está a cargo del administrador, el es encargado de instala equipos y software con previa autorización del coordinador de la Licenciatura en Informática, proceso que se realiza sin ningún control ni registro de los software y/o hardware instalados. En la red del programa de la licenciatura en informática se realiza un mantenimiento correctivo al comienzo de cada semestre, esto con el fin de limpiar las maquinas de información innecesaria y preparar las maquinas para el proceso de inscripción de los estudiantes de la coordinación

Usuario: Administrador

Flujos de Entrada: Solicitud Instalación Hardware

Solicitud Instalación de software

Solicitud de mantenimiento

Flujos de Salida: Informe de hardware Instalado

Informe de software Instalado

Informe de mantenimiento realizado

Referencia: 2.0

Proceso: Impresión

Descripción: Permite que los usuarios pueden hacer uso de la impresora anticipándole el uso de la misma al administrador el cual será el responsable de

entregar el documento al usuario.

Usuario:

Flujos de Entrada: Solicitud de impresión

Flujos de Salida: Impresión realizada

Referencia: 3.0

Proceso: Creación de cuentas en una PC.

Descripción: Permite a los usuarios de la licenciatura en informática, crear una cuenta que les de acceso a los servicios que brinda la red, esta cuenta es creada por el administrador en una maquina determinada, ya que no existe ningún servidor DNS.

Usuario: Administrador

Flujos de Entrada: Solicitud creación de cuenta nueva

Flujos de Salida: Cuenta de usuario

Referencia: 4.0

Proceso: Reservación de Equipos

Descripción: Este proceso les concede al usuario la ventaja de reservar el equipo con antelación, en la cual debe verificar que la maquina donde fue creada la cuenta de usuario este disponible, este proceso se realiza de forma manual.

Usuario: Administrador

Flujos de Entrada: Solicitud reservación de de equipo

Cuenta de usuario

Flujos de Salida: Reservación de equipo

Referencia: 5.0

Proceso: Préstamo de Equipos.

Descripción: Proceso que brinda el uso de los equipos a los usuario, el cual debió haber reservado su equipo con antelación, el administrador deberá dar permiso al usuario que reservo en caso que este no llegue puede prestarlo a otro usuario que lo necesite en ese momento.

Usuario: Estudiantes

Flujos de Entrada: Reservación de equipo

Flujos de Salida: Equipo prestado

Reporte de falla

Referencia: 6.0

Proceso: Reparación

Descripción: Proceso que permite realizar reparaciones de equipos de la red que hayan sido notificadas por el usuario al administrador en el momento en que estas se producen. Estas reparaciones se hacen de forma informal, no se tiene registro alguna que contenga información del equipo y tampoco se registra las causas de las fallas ni las soluciones realizadas a la misma.

Usuario: Administrador

Flujos de Entrada: Reporte de falla

Flujos de Salida: Reparaciones

Reporte de equipo reparado

Referencia: 7.0

Proceso: Préstamo de Equipos de Multimedia.

Descripción: La red posee equipos de multimedia, los cuales son prestados a los docentes con el fin de ser utilizados en su cátedras, para ser utilizados deben reservar el equipo con antelación. Este proceso se realiza de forma manual.

Usuario: Administrador

Flujos de Entrada: Solicitud préstamo de equipo multimedia

Flujos de Salida: Informe de equipo prestado

Descripción de Flujo de Datos

Para poder comprender y explica el funcionamiento de cada proceso es conveniente realizar una descripción detallada de cada uno de ellos:

Nombre: Solicitud de Instalación de Hardware

Descripción: Contiene información de la solicitud hecha por la coordinación de informática al administrador y es usada para instalar hardware.

Origen: Coordinación Informática

Destino: Proceso 1.0 (Instalación y mantenimiento)

Nombre: Informe de Hardware Instalado

Descripción: contiene información del hardware que fue instalado.

Origen: Proceso 1.0 (Instalación y mantenimiento)

Destino: Coordinación Informática

Nombre: Solicitud de Instalación de Software

Descripción: Contiene información del software a instalar la cual es usada por el administrador para realizar la instalación.

Origen Coordinación Informática

Destino: Proceso 1.0 (Instalación y mantenimiento)

Nombre: Informe de Software Instalado

Descripción: Contiene información del software instalado.

Origen: Proceso 1.0 (Instalación y mantenimiento)

Destino: Coordinación Informática

Nombre: Solicitud de Instalación de Hardware

Descripción: Solicitud que hace el Docente al administrador para instalar cualquier hardware necesario para dictar su cátedra.

Origen: Docente

Destino: Proceso 1.0 (Instalación y mantenimiento)

Nombre: Informe de Hardware Instalado

Descripción: participación que hace el administrador al docente para informar que el hardware ha sido instalado

Origen: Proceso 1.0 (Instalación y mantenimiento)

Destino: Docente

Nombre: Solicitud de Instalación de Software

Descripción: Solicitud que hace el Docente al administrador para instalar cualquier software necesario para dictar su cátedra.

Origen : Docente

Destino: Proceso 1.0 (Instalación y mantenimiento)

Nombre: Informe de Software Instalado

Descripción: participación que hace el administrador al docente para informar que el software ha sido instalado

Origen: Proceso 1.0 (Instalación y mantenimiento)

Destino: Docente

Nombre: Solicitud de Préstamo de Equipo Multimedia

Descripción: Solicitud que hace el Docente al administrador para pedir prestado el equipo de multimedia.

Origen: Docente

Destino: Proceso 7.0 (Préstamo de equipos de multimedia)

Nombre: Reporte de Equipo Multimedia prestado

Descripción: Informe que debe entregar el administrador a la coordinación para reportar el préstamo de los equipos de multimedia.

Origen: Proceso 7.0 (Préstamo de equipos de multimedia)

Destino: Coordinación Informática

Nombre: Solicitud de Creación de cuenta nueva

Descripción: Solicitud que hace el usuario al administrador para solicitar una cuenta de usuario para usar los servicios que brinda la red.

Origen: Usuario

Destino: Proceso 3.0 (Creación de cuentas en un PC)

Nombre: Solicitud de Reservación de Equipo

Descripción: Contiene información de la cuenta del usuario y es usada para reservar el equipo y disponer de los servicios de la red.

Origen: Usuario

Destino: Proceso 4.0 (Reservación de equipo)

Nombre: Solicitud de Impresión

Descripción: Contiene información del documento que se desea imprimir

Origen: Usuario

Destino: proceso 2.0 (impresión)

Nombre: Impresión Realizada

Descripción: Impresión realizada y entregada al usuario.

Origen: proceso 2.0 (impresión)

Destino: Usuario

Nombre: Reporte de Falla

Descripción: Es la información que el usuario emite al administrador de la red cuando se presenta algún problema mientras usa los servicios de la red.

Origen: Usuario

Destino: proceso 6.0 (reparaciones)

Nombre: Informe equipo Reparado

Descripción: Contiene información de la fallas que fueron reportada por el usuario al administrador.

Origen: proceso 5.0 (préstamo de equipo)

Destino: proceso 6.0 (reparaciones)

Nombre: Solicitud de Mantenimiento

Descripción: Contiene información del mantenimiento que debe hacerse a la red.

Origen: Coordinación Informática

Destino

Nombre: Reporte de Mantenimiento Realizado

Descripción: Contiene información del mantenimiento de equipos.

Origen: Coordinación Informática

Destino: Proceso 1.0 (Instalación y mantenimiento)

Nombre: Cuenta de Usuario

Descripción: Contiene información de la cuenta de usuario la cual es usada para hacer uso de los servicios de la red..

Descripción: Origen: Proceso 3.0 (creación de cuentas en un pc)

Destino: Registro cuentas de usuarios

Nombre: Cuentas de Usuario

Descripción: información de la cuenta de usuario, la cual sirve para que el usuario haga uso de los servicios de la red

Origen: Registro cuentas de usuarios

Destino: proceso 4.0 (reservación de equipos)

Nombre: Reservación de Equipo

Descripción: Información que contiene el equipo reservado por el usuario.

Origen: proceso 4.0 (reservación de equipos)

Destino: Registro Reservación

APÉNDICE B

Descripción de los Procesos Actuales

Referencia: 1.1

Proceso: Configurar sistemas

Descripción: Permite instalar y configurar hardware y software

Flujos de Entrada: Solicitud Instalación Hardware

Solicitud Instalación de software

Flujos de Salida Reporte de Hardware Instalado

Reporte de Software Instalado

Solicitud de actualización de inventario

Referencia: 1.2

Nombre: Mantenimiento de la red

Descripción: Permite conocer las condiciones operativas de los dispositivos para prevenir posibles fallas y realiza reparaciones al presentar de averías en los dispositivos.

Flujos de Entrada: Solicitud de mantenimiento correctivo

Solicitud de mantenimiento preventivo

Flujos de Salida Solicitud de actualización de inventario

Reporte de mantenimiento realizado

Referencia: 1.3

Proceso: Documentar la red

Descripción: Permite conocer y llevar un control de los activos informáticos, tanto hardware como software, que conforman la red, además de ofrecer un servicio preventivo y correctivo.

Flujos de Entrada: Solicitud de actualización de inventario

Solicitud de inventario

Flujos de Salida Reporte inventario Realizado

Referencia:1.4

Proceso: Evaluar desempeño

Descripción: Permite conocer el comportamiento de la red, el grado de utilización de los recursos y el nivel de cumplimiento de los servicios de usuarios con la finalidad de diagnosticar, eliminar e informar sobre fallas de los equipos y componentes de la red o de los servicios utilizados.

Flujos de Entrada: Solicitud de monitoreo

Flujos de Salida Monitoreo Realizado

Reporte de Averías

Referencia: 1.5

Proceso: Determinar averías

Descripción: Permite detectar el origen de fallas presentadas en los equipos y documentar las soluciones y problemas presentados.

Flujos de Entrada: Solicitud de reparación de falla

Reporte de falla

Registro de averías

Flujos de Salida Reporte de falla reparada

Referencia:2.0

Proceso: Realizar Impresión

Descripción: Permite al usuario realizar impresiones desde cualquier equipo perteneciente a la red.

Flujos de Entrada: Solicitud de impresión

Flujos de Salida: Impresión Realizada

Descripción

Referencia:3.0

Proceso: Crear cuentas de usuarios

Descripción: Permite crear cuentas de usuarios en un servidor de Nombre de dominio

Flujos de Entrada: Solicitud de creación de cuenta nueva

Flujos de Salida Cuenta de usuario

Referencia 4.0

Proceso: Realizar préstamo de Equipo

Descripción: Proceso que permite al usuario usar cualquier equipo, el cual debió haber sido reservado con antelación.

Flujos de Entrada: Solicitud préstamo de equipo

Cuenta de usuario

Flujos de Salida Reservación de equipo

Solicitud de impresión

Informe equipo prestado

Referencia: 5.0

Proceso: Realizar préstamo Equipo de Multimedia

Descripción: La red posee equipos de multimedia, los cuales son prestados a los docentes con el fin de ser utilizados en su cátedras, para ser utilizados deben reservar el equipo con antelación. Este proceso se realiza de forma manual.

Flujos de Entrada: Solicitud préstamo equipo de multimedia

Flujos de Salida Reporte de equipo de multimedia prestado

Descripción de Flujo de Datos Actuales

Para poder comprender y explica el funcionamiento de los Flujos de Datos de

los procesos propuestos es conveniente realizar una descripción detallada de cada uno de ellos:

Nombre: Solicitud de Instalación de Hardware

Descripción

Origen: Docente

Destino: Proceso 1.1 (instalación)

Nombre: Informe de Hardware Instalado

Descripción

Origen: Proceso 1.1 (instalación)

Destino: Docente

Nombre: Solicitud de Instalación de Software

Descripción

Origen: Docente

Destino: proceso 1.1 (instalación)

Nombre: Informe de Software Instalado

Descripción

Origen: proceso 1.1 (instalación)

Destino: docente

Nombre: Solicitud de Instalación de Hardware

Descripción

Origen: Coordinación Informática

Destino: Proceso 1.1 (instalación)

Nombre: Informe de Hardware Instalado

Descripción

Origen: Proceso 1.1 (instalación)

Destino: Coordinación Informática

Nombre: Solicitud de Instalación de Software

Descripción

Origen: coordinación Informática

Destino: proceso 1.1 (instalación)

Nombre: Informe de Software Instalado

Descripción

Origen: proceso 1.1 (instalación)

Destino: coordinación Informática

Nombre: Solicitud de Préstamo de Equipo Multimedia

Descripción

Origen: Docente

Destino: Proceso 5.0 (préstamo de equipo de multimedia)

Nombre: Reporte de Equipo Multimedia prestado

Descripción

Origen: Proceso 5.0 (préstamo de equipo de multimedia)

Destino: Docente

Nombre: Solicitud de Creación de cuenta nueva

Descripción: Contiene información del usuario la cual es usada para crear una cuenta con la que podrá acceder a los servicios de la red

Origen: Usuario

Destino: proceso 3.0 (Servidor DNS)

Nombre: Solicitud de préstamo de Equipo

Descripción: Contiene información del equipo a prestar.

Origen: Usuario

Destino: Proceso 4.0 (Préstamo de equipo)

Nombre: Solicitud de Impresión

Descripción: contiene información del documento que se desea imprimir.

Origen: Usuario

Destino: Proceso 2.0 (Servidor de impresión)

Nombre: Impresión Realizada

Descripción: Documento impreso.

Origen: Proceso 2.0 (Servidor de impresión)

Destino: Usuario

Nombre: Reporte de Falla

Descripción

Origen: Usuario

Destino: Proceso 1.5 (Reparación)

Nombre: Solicitud de Mantenimiento preventivo

Descripción

Origen: Administrador

Destino: Proceso 1.2 (mantenimiento)

Nombre: Solicitud de Mantenimiento correctivo

Descripción:

Origen: Coordinación Informática

Destino: Proceso 1.2 (mantenimiento)

Nombre: Reporte de Mantenimiento Realizado

Descripción: Contiene información del mantenimiento que se hizo.

Origen: Proceso 1.2 (mantenimiento)

Destino: Coordinación Informática

Nombre: Cuenta de Usuario

Descripción: Posee información de la cuenta de usuario la cual es usada para que el usuario utilice los servicios de la red.

Origen: Registro Cuenta Usuario

Destino: Proceso 4.0 (Préstamo de equipo)

Nombre: Solicitud de Inventario

Descripción: Contiene información

Origen: Administrador

Destino: Proceso 1.3 (Inventario)

Nombre: Reporte de inventario Actualizado

Descripción: Contiene información de los equipos que conforman la red con sus componentes y reparaciones realizada.

Origen: Proceso 1.3 (inventario)

Destino: Administrador

Nombre: Solicitud de Monitoreo

Descripción: Contiene información

Origen: Administrador

Destino: Proceso 1.4 (Monitoreo)

Nombre: Reporte de Monitoreo Realizado

Descripción: Contiene información del tráfico de la red el cual es usada para evaluar el comportamiento de la red.

Origen: Proceso 1.4 (monitoreo)

Destino: Administrador

APÉNDICE C

INFO 36

Ordenador:

Sistema operativo	Microsoft Windows XP Professional
Service Pack del Sistema Operativo	Service Pack 2
Internet Explorer	7.0.5730.11
Nombre del sistema	INFO-37 (INFO-37)
Nombre de usuario	Estudiantes
Nombre de dominio	INFO-37

Placa base:

Tipo de procesador	Intel Pentium 4, 1800 MHz (4.5 x 400)
Nombre de la Placa Base	VIARAMA U8668 (Pro) (3 PCI, 1 AGP, 1 CNR, 2 SDR DIMM, 2 DDR DIMM, Audio, Video, LAN)
Chipset de la Placa Base	VIA VT8751 Apollo P4M266
Memoria del Sistema	247 MB (PC2100 DDR SDRAM)
Tipo de BIOS	Award (08/04/03)

Puerto de comunicación de Puerto de comunicaciones (COM1)

Puerto de comunicación de Puerto de impresora (LPT1)

Monitor:

Tarjeta gráfica S3 ProSavageDDR (86c420)

Acelerador 3D S3 SuperSavageDDR

Multimedia:

Tarjeta de sonido VIA AC'97 Enhanced Audio Controller

Almacenamiento:

Disquetera de 3 1/2 Unidad de disquete

Disco duro SAMSUNG SV0411N (40 GB, 5400 RPM, Ultra-ATA/133)

Disco duro USB 2.0 Flash Disk USB Device

Lector óptico ATAPI-CD ROM-DRIVE-56MAX (56x CD-ROM)

Particiones:

C: (NTFS) 20198 MB (14358 MB libre)

Dispositivos de entrada:

Teclado Teclado estándar de 101/102 teclas o
Microsoft Natural PS/2 Keyboard

Ratón Mouse compatible PS/2

Red:

Dirección IP 192.168.3.176
principal

Dirección MAC 00-E0-4C-A2-59-FA
principal

Tarjeta de Red Adaptador Fast Ethernet compatible VIA
(192.168.3.176)

Dispositivos:

Impresora Detectando automáticamente HP DeskJet
930C/932C/935C en J_PARRA

Impresora Detectando automáticamente HP LaserJet
6P en ELIZABETH

Dispositivos USB Dispositivo de almacenamiento masivo
USB

Propiedades de la BIOS:

Vendedor	Phoenix Technologies, LTD
Versión	6.00 PG
Fecha de salida	08/04/2003
Tamaño	256 KB
Dispositivos de arranque	Floppy Disk, Hard Disk, CD-ROM, ATAPI ZIP, LS-120
Funciones disponibles	Flash BIOS, Shadow BIOS, Selectable Boot, EDD
Standards soportados	DMI, APM, ACPI, ESCD, PnP
Posibilidades de expansión	PCI, AGP, USB

Sistema operativo

Propiedades del Sistema Operativo:

Nombre del Sistema Operativo	Microsoft Windows XP Professional
Nombre de código del Sistema Operativo	Whistler
Idioma del Sistema Operativo	Español (alfabetización internacional)
Tipo de núcleo del Sistema Operativo	Uniprocessor Free
Versión del Sistema	5.1.2600 (WinXP Retail)

Operativo	
Service Pack del Sistema Operativo	Service Pack 2
Fecha de instalación del Sistema Operativo	15/05/2008
Carpeta Raíz del Sistema Operativo	C:\WINDOWS

Información sobre la licencia:

Propietario registrado	WinuE
Organización registrada	Windows uE
Procesadores cubiertos por la licencia	2
Identificación del producto	55274-640-4350801-23362
Clave del producto	B3P7V-Q2WTH-CRK4R-YHJRF-39H4M

Sesión actual:

Nombre del sistema	INFO-37
Nombre de usuario	Estudiantes
Nombre de dominio	INFO-37
Tiempo transcurrido desde que inició el ordenador	4218 seg (0 días, 1 horas, 10 min, 18 seg)

Versión de los componentes:

Common Controls	6.00
Internet Explorer	7.0.5730.11
Outlook Express	6.00.2900.2180 (xpsp_sp2_rtm.040803-2158)
Windows Media Player	11.0.5721.5145 (WMP_11.061018-2006)
Internet Information Services	Ninguno
Novell Client	Ninguno
DirectX	4.09.00.0904 (DirectX 9.0)
OpenGL	5.1.2600.2180 (xpsp_sp2_rtm.040803-2158)
ASPI	Ninguno

Database Drivers:

MDAC	2.81.1117.0 (xpsp_sp2_rtm.040803-2158)
ODBC	3.525.1117.0 (xpsp_sp2_rtm.040803-2158)
MySQL Connector/ODBC	Ninguno
Oracle Client	Ninguno
PsqlODBC	Ninguno
Sybase ASE ODBC	Ninguno
Borland Database Engine	3.00

Funciones del Sistema Operativo:

Versión de depuración	No
Versión DBCS	No
Domain Controller	No
Seguridad	No
Red presente	Sí
Sesión remota	No
Modo Seguro	No
Procesador lento	No
Terminal Services	No

Impresoras

[Detectando automáticamente HP DeskJet 930C/932C/935C en J_PARRA]

Propiedades de la impresora:

Nombre de la impresora	Detectando automáticamente HP DeskJet 930C/932C/935C en J_PARRA
Impresora predeterminada	No
Punto compartido	No compartido
Puerto de impresión	de \\J_PARRA\HPDeskJe

Controlador de impresora	HP DeskJet 930C/932C/935C (v5.00)
Nombre del dispositivo	Detectando automáticamente HP D
Procesador de impresora	WinPrint
Página de separación	Ninguno
Disponibilidad	2:00 - 2:00
Prioridad	1
Trabajos de impresión en cola	0
Estado	Desconocido

Propiedades del papel:

Tamaño del papel	Letter, 8.5 x 11 in
Orientación	Foto
Calidad de impresión	300 x 300 dpi Color

Fabricante de la impresora:

Nombre de la empresa	Hewlett-Packard Company
Información sobre el producto	http://www.hp.com/united-states/consumer/gateway/printing_multifunction.html

[Detectando automáticamente HP LaserJet 6P en ELIZABETH
(Por defecto)]

Propiedades de la impresora:

Nombre de la impresora	Detectando automáticamente HP LaserJet 6P en ELIZABETH
Impresora predeterminada	Sí
Punto compartido	No compartido
Puerto de impresión	\\ELIZABETH\HPLaserJ
Controlador de impresora	HP LaserJet 6P (v5.00)
Nombre del dispositivo	Detectando automáticamente HP L
Procesador de impresora	WinPrint
Página de separación	Ninguno
Disponibilidad	2:00 - 2:00
Prioridad	1
Trabajos de impresión en cola	0
Estado	Desconocido

Propiedades del papel:

Tamaño del papel A4, 210 x 297 mm

Orientación Foto

Calidad de impresión 600 dpi Mono

Fabricante de la impresora:

Nombre de la empresa Hewlett-Packard Company

Información sobre el producto http://www.hp.com/united-states/consumer/gateway/printing_multifunction.html

Programas instalados

Programa	Versión	Tamaño
µTorrent	1.7.7	Desconocido
Adobe Reader 8.1.0 - Español [español - españa (alfabetización tradicional)]	8.1.0	53.9 MB
AIDA32 v3.93		Desconocido
avast! Antivirus	4.8	72.5 MB
AVG Free 8.0		Desconocido

Borland C++ 5.01		233.7 MB
Compresor WinRAR		3.9 MB
Corman Lisp 2.51	2.51.0000	32.0 MB
DAMN NFO Viewer		
Setup	2.10	417.0 KB
Dev-C++ 5 beta 9 release (4.9.9.2)		Desconocido
HashTab Shell Extension 1.11 for x32	1.11 for x32	324.0 KB
Java(TM) 6 Update 2	1.6.0.20	134.9 MB
K-Lite Codec Pack 3.3.0 Standard	3.30	20.6 MB
LINGO 5.0		12.6 MB
Macromedia Director MX 2004		59.6 MB
MATLAB 6.5		Desconocido
Microsoft .NET Framework 1.1 [español (alfabetización internacional)]	1.1.4322	Desconocido
Microsoft .NET Framework 1.1		Desconocido
Microsoft .NET Framework 2.0 with Security Updates		70.5 MB
Microsoft .NET Framework 2.0 with Security	2.0.50727	Desconocido

Updates

Microsoft Compression Client Pack 1.0 for Windows XP	1	Desconocido
Microsoft Internationalized Domain Names Mitigation APIs		Desconocido
Microsoft National Language Support Downlevel APIs		Desconocido
Microsoft Office Professional Edition 2003 [español (alfabetización internacional)]	11.0.7969.0	340.6 MB
Microsoft SQL Server 7.0		Desconocido
Microsoft User-Mode Driver Framework Feature Pack 1.0		Desconocido
Microsoft Visual C++ 2005 Redistributable	8.0.56336	Desconocido
NOD32 FiX v2.1		45.0 MB
QT Lite 1.1.1	1.1.1	37.8 MB
Real Alternative 1.52 Lite	1.52	14.6 MB
Reproductor de Windows		6.2 MB

Media 11		
Revisión para Windows XP (KB935448)	1	Desconocido
Shockwave Player	10.2.0.022	11.7 MB
Synchro plus SimTraffic		Desconocido
6		
TaskSwitchXP	2.0.11	1.0 MB
TORA (C:\Archivos de programa\vbTora98) #3		853.8 MB
TORA (C:\Archivos de programa\vbTora98) #4		853.8 MB
TORA (C:\Archivos de programa\vbTora98)		642.9 MB
TORA		Desconocido
TuneUp Utilities 2007	6.0.2200	26.4 MB
Unlocker 1.8.5	1.8.5	228.0 KB
Windows Internet Explorer 7	20061107.210142	1.5 MB
Windows Live installer	12.0.1202.0516	Desconocido
Windows Live Sign-in Assistant	4.100.313.1	1.2 MB
Windows Media Format 11 runtime		6.2 MB
Windows Media Format 11 runtime		Desconocido
Windows Media Player		Desconocido

11

XPize 4.6 Lite

4.6 Lite

Desconocido

Licencias

Programas	Clave del producto
Macromedia Director	DRD100-55139-55964-06583
Microsoft Internet Explorer	B3P7V-Q2WTH-CRK4R- YHJRF-39H4M
Microsoft Office Professional Edition 2003	GWH28-DGCMP-P6RC4- 6J4MT-3HFDY
Microsoft Windows	B3P7V-Q2WTH-CRK4R- YHJRF-39H4M

Antivirus

Descripción de la aplicación	Versión de la aplicación	Fecha de la Base de datos de los virus	Virus conocidos
Avast	4.8	?	?

INFO 37

Ordenador:

Sistema operativo	Microsoft Windows XP Professional
Service Pack del Sistema Operativo	Service Pack 2
Internet Explorer	7.0.5730.11
Nombre del sistema	INFO-37 (INFO-37)
Nombre de usuario	Estudiantes
Nombre de dominio	INFO-37

Placa base:

Tipo de procesador	Intel Pentium 4, 1800 MHz (4.5 x 400)
Nombre de la Placa Base	VIARAMA U8668 (Pro) (3 PCI, 1 AGP, 1 CNR, 2 SDR DIMM, 2 DDR DIMM, Audio, Video, LAN)
Chipset de la Placa Base	VIA VT8751 Apollo P4M266
Memoria del Sistema	247 MB (PC2100 DDR SDRAM)
Tipo de BIOS	Award (08/04/03)

Puerto de comunicación de Puerto de comunicaciones (COM1)

Puerto de comunicación de Puerto de impresora (LPT1)

Monitor:

Tarjeta gráfica S3 ProSavageDDR (86c420)

Acelerador 3D S3 SuperSavageDDR

Multimedia:

Tarjeta de sonido VIA AC'97 Enhanced Audio Controller

Almacenamiento:

Disquetera de 3 1/2 Unidad de disquete

Disco duro SAMSUNG SV0411N (40 GB, 5400 RPM, Ultra-ATA/133)

Disco duro USB 2.0 Flash Disk USB Device

Lector óptico ATAPI-CD ROM-DRIVE-56MAX (56x CD-ROM)

Particiones:

C: (NTFS) 20198 MB (14358 MB libre)

Dispositivos de entrada:

Teclado Teclado estándar de 101/102 teclas o
Microsoft Natural PS/2 Keyboard

Ratón Mouse compatible PS/2

Red:

Dirección IP 192.168.3.176
principal

Dirección MAC 00-E0-4C-A2-59-FA
principal

Tarjeta de Red Adaptador Fast Ethernet compatible VIA
(192.168.3.176)

Dispositivos:

Impresora Detectando automáticamente HP DeskJet
930C/932C/935C en J_PARRA

Impresora Detectando automáticamente HP LaserJet
6P en ELIZABETH

Dispositivos USB Dispositivo de almacenamiento masivo
USB

Sistema operativo

Propiedades del Sistema Operativo:

Nombre del Sistema Microsoft Windows XP

Operativo	Professional
Nombre de código del Sistema Operativo	Whistler
Idioma del Sistema Operativo	Español (alfabetización internacional)
Tipo de núcleo del Sistema Operativo	Uniprocessor Free
Versión del Sistema Operativo	5.1.2600 (WinXP Retail)
Service Pack del Sistema Operativo	Service Pack 2
Fecha de instalación del Sistema Operativo	15/05/2008
Carpeta Raíz del Sistema Operativo	C:\WINDOWS

Información sobre la licencia:

Propietario registrado	WinuE
Organización registrada	Windows uE
Procesadores cubiertos por la licencia	2
Identificación del producto	55274-640-4350801-23362
Clave del producto	B3P7V-Q2WTH-CRK4R-YHJRF-39H4M

Sesión actual:

Nombre del sistema	INFO-37
Nombre de usuario	Estudiantes
Nombre de dominio	INFO-37
Tiempo transcurrido desde que inició el ordenador	4218 seg (0 días, 1 horas, 10 min, 18 seg)

Versión de los componentes:

Common Controls	6.00
Internet Explorer	7.0.5730.11
Outlook Express	6.00.2900.2180 (xpsp_sp2_rtm.040803-2158)
Windows Media Player	11.0.5721.5145 (WMP_11.061018-2006)
Internet Information Services	Ninguno
Novell Client	Ninguno
DirectX	4.09.00.0904 (DirectX 9.0)
OpenGL	5.1.2600.2180 (xpsp_sp2_rtm.040803-2158)
ASPI	Ninguno

Database Drivers:

MDAC	2.81.1117.0 (xpsp_sp2_rtm.040803-2158)
ODBC	3.525.1117.0 (xpsp_sp2_rtm.040803-2158)

MySQL Connector/ODBC	Ninguno
Oracle Client	Ninguno
PsqlODBC	Ninguno
Sybase ASE ODBC	Ninguno
Borland Database Engine	3.00

Funciones del Sistema Operativo:

Versión de depuración	No
Versión DBCS	No
Domain Controller	No
Seguridad	No
Red presente	Sí
Sesión remota	No
Modo Seguro	No
Procesador lento	No
Terminal Services	No

Impresoras

[Detectando automáticamente HP DeskJet 930C/932C/935C en J_PARRA]

Propiedades de la impresora:

Nombre de la impresora	Detectando automáticamente HP DeskJet 930C/932C/935C en J_PARRA
Impresora predeterminada	No
Punto compartido	No compartido
Puerto de impresión	\\J_PARRA\HPDeskJe
Controlador de impresora	HP DeskJet 930C/932C/935C (v5.00)
Nombre del dispositivo	Detectando automáticamente HP D
Procesador de impresora	WinPrint
Página de separación	Ninguno
Disponibilidad	2:00 - 2:00
Prioridad	1
Trabajos de impresión en cola	0
Estado	Desconocido

Propiedades del papel:

Tamaño del papel	Letter, 8.5 x 11 in
------------------	---------------------

Orientación Foto
Calidad de impresión 300 x 300 dpi Color

Fabricante de la impresora:

Nombre de la empresa Hewlett-Packard Company
Información sobre el producto http://www.hp.com/united-states/consumer/gateway/printing_multifunction.html

[Detectando automáticamente HP LaserJet 6P en ELIZABETH
(Por defecto)]

Propiedades de la impresora:

Nombre de la impresora Detectando automáticamente HP LaserJet 6P en ELIZABETH
Impresora predeterminada Sí
Punto compartido No compartido
Puerto de impresión de \\ELIZABETH\HPLaserJ
Controlador de impresora de HP LaserJet 6P (v5.00)
Nombre del dispositivo Detectando automáticamente HP L

Procesador de impresora	de	WinPrint
Página de separación	de	Ninguno
Disponibilidad		2:00 - 2:00
Prioridad		1
Trabajos de impresión en cola	de	0
Estado		Desconocido

Propiedades del papel:

Tamaño del papel	del	A4, 210 x 297 mm
Orientación		Foto
Calidad de impresión	de	600 dpi Mono

Fabricante de la impresora:

Nombre de la empresa	de la	Hewlett-Packard Company
Información sobre el producto		http://www.hp.com/united-states/consumer/gateway/printing_multifunction.html

Programas instalados

Programa	Versión	Tamaño
µTorrent	1.7.7	Desconocido
Adobe Reader 8.1.0 - Español [español - española (alfabetización tradicional)]	8.1.0	53.9 MB
AIDA32 v3.93		Desconocido
avast! Antivirus	4.8	72.5 MB
AVG Free 8.0		Desconocido
Borland C++ 5.01		233.7 MB
Compresor WinRAR		3.9 MB
Corman Lisp 2.51	2.51.0000	32.0 MB
DAMN NFO Viewer Setup	2.10	417.0 KB
Dev-C++ 5 beta 9 release (4.9.9.2)		Desconocido
HashTab Shell Extension 1.11 for x32	1.11 for x32	324.0 KB
Java(TM) 6 Update 2	1.6.0.20	134.9 MB
K-Lite Codec Pack 3.3.0 Standard	3.30	20.6 MB
LINGO 5.0		12.6 MB
Macromedia Director MX 2004		59.6 MB

MATLAB 6.5				Desconocido
Microsoft .NET Framework 1.1 [español (alfabetización internacional)]		1.1.4322		Desconocido
Microsoft .NET Framework 1.1				Desconocido
Microsoft .NET Framework 2.0 with Security Updates				70.5 MB
Microsoft .NET Framework 2.0 with Security Updates		2.0.50727		Desconocido
Microsoft Compression Client Pack 1.0 for Windows XP		1		Desconocido
Microsoft Internationalized Domain Names Mitigation APIs				Desconocido
Microsoft National Language Support Downlevel APIs				Desconocido
Microsoft Office Professional Edition 2003 [español (alfabetización internacional)]		11.0.7969.0		340.6 MB
Microsoft SQL Server 7.0				Desconocido

Microsoft User-Mode Driver Framework Feature Pack 1.0			Desconocido
Microsoft Visual C++ 2005 Redistributable	8.0.56336		Desconocido
NOD32 FiX v2.1			45.0 MB
QT Lite 1.1.1	1.1.1		37.8 MB
Real Alternative 1.52 Lite	1.52		14.6 MB
Reproductor de Windows Media 11			6.2 MB
Revisión para Windows XP (KB935448)	1		Desconocido
Shockwave Player	10.2.0.022		11.7 MB
Synchro plus SimTraffic 6			Desconocido
TaskSwitchXP	2.0.11		1.0 MB
TORA (C:\Archivos de programa\vbTora98) #3			853.8 MB
TORA (C:\Archivos de programa\vbTora98) #4			853.8 MB
TORA (C:\Archivos de programa\vbTora98)			642.9 MB
TORA			Desconocido
TuneUp Utilities 2007	6.0.2200		26.4 MB
Unlocker 1.8.5	1.8.5		228.0 KB

Windows Explorer 7	Internet	20061107.210142	1.5 MB
Windows Live installer		12.0.1202.0516	Desconocido
Windows Live Sign-in Assistant		4.100.313.1	1.2 MB
Windows Media Format 11 runtime			6.2 MB
Windows Media Format 11 runtime			Desconocido
Windows Media Player 11			Desconocido
XPize 4.6 Lite		4.6 Lite	Desconocido

Licencias

Programas	Clave del producto
Macromedia Director	DRD100-55139-55964-06583
Microsoft Internet Explorer	B3P7V-Q2WTH-CRK4R-YHJRF-39H4M
Microsoft Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY
Microsoft Windows	B3P7V-Q2WTH-CRK4R-YHJRF-39H4M

Antivirus

Descripción de la aplicación	Versión de la aplicación	Fecha de la Base de datos de los virus	Virus conocidos
Avast	4.8	?	?

INFO 38

Ordenador:

Sistema operativo		Microsoft Windows XP Professional
Service Pack del Sistema Operativo		Service Pack 2
Internet Explorer		7.0.5730.11
Nombre del sistema	del	INFO-38 (INFO-38)
Nombre de usuario	de	Estudiantes
Nombre de dominio	de	INFO-38

Placa base:

Tipo de procesador de Intel Pentium 4, 1800 MHz

Nombre de la Placa Base de la VIARAMA U8668 (Pro) (3 PCI, 1 AGP, 1 CNR, 2 SDR DIMM, 2 DDR DIMM, Audio, Video, LAN)

Chipset de la Placa Base de la VIA VT8751 Apollo P4M266

Memoria del Sistema de 224 MB

Tipo de BIOS de Award (08/04/03)

Puerto de comunicación de Puerto de comunicaciones (COM1)

Puerto de comunicación de Puerto de impresora (LPT1)

Monitor:

Tarjeta gráfica de S3 Graphics ProSavageDDR (Microsoft Corporation) (32 MB)

Acelerador 3D de S3 SuperSavageDDR

Monitor de Samsung SyncMaster 501s/551s/551v/MagicSyncMaster CM151A (HCGW816285)

Multimedia:

Tarjeta de VIA AC'97 Enhanced Audio Controller

sonido

Almacenamiento:

Disquetera de 3 1/2	Unidad de disquete
Disco duro	ST340015A (40 GB, 5400 RPM, Ultra-ATA/100)
Lector óptico	ATAPI-CD ROM-DRIVE-56MAX (56x CD-ROM)

Particiones:

C: (NTFS)	29996 MB (26240 MB libre)
-----------	---------------------------

Dispositivos de entrada:

Teclado	Teclado estándar de 101/102 teclas o Microsoft Natural PS/2 Keyboard
Ratón	Mouse compatible PS/2

Red:

Dirección IP principal	192.168.3.202
Dirección MAC principal	00-E0-4C-A2-67-37
Tarjeta de Red	Adaptador Fast Ethernet compatible VIA (192.168.3.202)

Sistema operativo

Propiedades del Sistema Operativo:

Nombre del Sistema Operativo	Microsoft Windows XP Professional
Nombre de código del Sistema Operativo	Whistler
Idioma del Sistema Operativo	Español (alfabetización internacional)
Tipo de núcleo del Sistema Operativo	Uniprocessor Free
Versión del Sistema Operativo	5.1.2600 (WinXP Retail)
Service Pack del Sistema Operativo	Service Pack 2
Fecha de instalación del Sistema Operativo	27/10/2008
Carpeta Raíz del Sistema Operativo	C:\WINDOWS

Información sobre la licencia:

Propietario registrado	WinuE
Organización registrada	Windows uE

Procesadores cubiertos por la licencia	2
Identificación del producto	55274-640-4350801-23782
Clave del producto	B3P7V-Q2WTH-CRK4R- YHJRF-39H4M

Programas instalados

Programa	Versión	Tamaño
Adobe Flash Player 9 ActiveX	9	Desconocido
Adobe Reader 7.0.8 - Español [español - española (alfabetización tradicional)]	7.0.8	Desconocido
Adobe Shockwave Player	10.1.4.20	Desconocido
AIDA32 v3.93		Desconocido
AVG Free 8.0		Desconocido
Borland C++ 5.01		Desconocido
Compresor WinRAR		Desconocido
Corman Lisp 2.51	2.51.0000	Desconocido
DAMN NFO Viewer Setup	2.10	Desconocido
Dev-C++ 5 beta 9 release		Desconocido

(4.9.9.2)

Hotfix for Windows XP (KB915865)	10	Desconocido
Hotfix for Windows XP (KB926239)	2	Desconocido
Image Resizer Powertoy for Windows XP	1.00.0001	Desconocido
Java(TM) SE Runtime Environment 6	1.6.0.0	Desconocido
K-Lite Codec Pack 2.81 Full	2.81	Desconocido
Microsoft .NET Framework 1.1 [español (alfabetización internacional)]	1.1.4322	Desconocido
Microsoft .NET Framework 1.1 Hotfix (KB886903)		Desconocido
Microsoft .NET Framework 1.1		Desconocido
Microsoft .NET Framework 2.0 with Security Updates		Desconocido
Microsoft .NET Framework 2.0 with Security Updates	2.0.50727	Desconocido
Microsoft Compression	1	Desconocido

Client Pack 1.0 for Windows XP			
Microsoft Internationalized Domain Names Mitigation APIs			Desconocido
Microsoft National Language Support Downlevel APIs			Desconocido
Microsoft Office Professional Edition 2003 [español (alfabetización internacional)]	11.0.7969.0		Desconocido
Microsoft SQL Server 7.0			Desconocido
Microsoft User-Mode Driver Framework Feature Pack 1.0			Desconocido
Microsoft Visual C++ 2005 Redistributable	8.0.56336		Desconocido
Nero 7.5.9.0			Desconocido
QuickTime Alternative 1.76	1.76		Desconocido
Real Alternative 1.51 Lite	1.51		Desconocido
Reproductor de Windows Media 11			Desconocido

Security Update para Microsoft .NET Framework 2.0 (KB917283)	1	Desconocido
Security Update para Microsoft .NET Framework 2.0 (KB922770)	1	Desconocido
Spybot - Search & Destroy 1.4	1.4	Desconocido
TaskSwitchXP	2.0.11	Desconocido
TuneUp Utilities 2006	5.3.2343	Desconocido
Unlocker 1.8.5	1.8.5	Desconocido
Winamp AudioPlayer	5.32.1003	Desconocido
Windows Genuine Advantage Validation Tool (KB892130)	1.5.0530.0	Desconocido
Windows Internet Explorer 7	20061107.210142	Desconocido
Windows Media Format 11 runtime		Desconocido
Windows Media Format 11 runtime		Desconocido
Windows Media Player 11		Desconocido
XPize 4.6 Lite BETA 1	4.6 Lite BETA 1	Desconocido

Licencias

Programas	Clave del producto
Microsoft Internet Explorer	B3P7V-Q2WTH-CRK4R- YHJRF-39H4M
Microsoft Office Professional Edition 2003	GWH28-DGCMP-P6RC4- 6J4MT-3HFDY
Microsoft Windows	B3P7V-Q2WTH-CRK4R- YHJRF-39H4M

INFO 39

Ordenador:

Sistema operativo	Microsoft Windows XP Professional
Service Pack del Sistema Operativo	Service Pack 2
Internet Explorer	7.0.5730.11
Nombre del sistema	INFO-39 (Info-39)
Nombre de usuario	Estudiantes

Nombre de dominio de INFO-39

Placa base:

Tipo de procesador de Intel Pentium 4, 1800 MHz

Nombre de la Placa Base de la VIARAMA U8668 (Pro) (3 PCI, 1 AGP, 1 CNR, 2 SDR DIMM, 2 DDR DIMM, Audio, Video, LAN)

Chipset de la Placa Base de la VIA VT8751 Apollo P4M266

Memoria del Sistema de 224 MB

Tipo de BIOS de Award (08/04/03)

Puerto de comunicación de Puerto de comunicaciones (COM1)

Puerto de comunicación de Puerto de impresora (LPT1)

Monitor:

Tarjeta gráfica de S3 Graphics ProSavageDDR (Microsoft Corporation) (32 MB)

Acelerador 3D de S3 SuperSavageDDR

Monitor de Samsung SyncMaster 501s/551s/551v/MagicSyncMaster CM151A (HCGW655637)

Multimedia:

Tarjeta de sonido de VIA AC'97 Enhanced Audio Controller

Almacenamiento:

Disquetera de 3 1/2 Unidad de disquete

Disco duro SAMSUNG SV0411N (40 GB, 5400 RPM, Ultra-ATA/133)

Lector óptico ATAPI-CD ROM-DRIVE-56MAX (56x CD-ROM)

Particiones:

C: (NTFS) 29996 MB (26157 MB libre)

Dispositivos de entrada:

Teclado Teclado estándar de 101/102 teclas o Microsoft Natural PS/2 Keyboard

Ratón Mouse compatible PS/2

Red:

Dirección IP principal 192.168.3.231

Dirección MAC 00-E0-4C-A1-AA-A7

principal

Tarjeta de Red Adaptador Fast Ethernet compatible VIA
(192.168.3.231)

Propiedades de la BIOS:

Vendedor	Phoenix Technologies, LTD
Versión	6.00 PG
Fecha de salida	08/04/2003
Tamaño	256 KB
Dispositivos de arranque	Floppy Disk, Hard Disk, CD-ROM, ATAPI ZIP, LS-120
Funciones disponibles	Flash BIOS, Shadow BIOS, Selectable Boot, EDD
Standards soportados	DMI, APM, ACPI, ESCD, PnP
Posibilidades de expansión	PCI, AGP, USB

Sistema operativo

Propiedades del Sistema Operativo:

Nombre del Sistema Operativo	Microsoft Windows XP Professional
Nombre de código del Sistema Operativo	Whistler
Idioma del Sistema Operativo	Español (alfabetización internacional)
Tipo de núcleo del Sistema Operativo	Uniprocessor Free
Versión del Sistema Operativo	5.1.2600 (WinXP Retail)
Service Pack del Sistema Operativo	Service Pack 2
Fecha de instalación del Sistema Operativo	27/10/2008
Carpeta Raíz del Sistema Operativo	C:\WINDOWS

Información sobre la licencia:

Propietario registrado	WinuE
Organización registrada	Windows uE
Procesadores cubiertos por la licencia	2
Identificación del producto	55274-640-4350801-23820
Clave del producto	B3P7V-Q2WTH-CRK4R-YHJRF-39H4M

Sesión actual:

Nombre del sistema	INFO-39
Nombre de usuario	Estudiantes
Nombre de dominio	INFO-39
Tiempo transcurrido desde que inició el ordenador	3334 seg (0 días, 0 horas, 55 min, 34 seg)

Versión de los componentes:

Common Controls	6.00
Internet Explorer	7.0.5730.11
Outlook Express	6.00.2900.2180 (xpsp_sp2_rtm.040803-2158)
Windows Media Player	11.0.5721.5145 (WMP_11.061018-2006)
Internet Information Services	Ninguno
Novell Client	Ninguno
DirectX	4.09.00.0904 (DirectX 9.0)
OpenGL	5.1.2600.2180 (xpsp_sp2_rtm.040803-2158)
ASPI	Ninguno

Database Drivers:

MDAC	2.81.1117.0 (xpsp_sp2_rtm.040803-2158)
ODBC	3.525.1117.0

(xpsp_sp2_rtm.040803-2158)

MySQL Connector/ODBC	Ninguno
Oracle Client	Ninguno
PsqlODBC	Ninguno
Sybase ASE ODBC	Ninguno
Borland Database Engine	3.00

Programas instalados

Programa	Versión	Tamaño
Adobe Flash Player 9 ActiveX	9	Desconocido
Adobe Reader 7.0.8 - Español [español - españa	7.0.8	Desconocido

(alfabetización tradicional)]

Adobe Shockwave Player	10.1.4.20	Desconocido
AIDA32 v3.93		Desconocido
AVG Free 8.0		Desconocido
Borland C++ 5.01		Desconocido
Compresor WinRAR		Desconocido
Corman Lisp 2.51	2.51.0000	Desconocido
DAMN NFO Viewer Setup	2.10	Desconocido
Dev-C++ 5 beta 9 release (4.9.9.2)		Desconocido
Hotfix for Windows XP (KB915865)	10	Desconocido
Hotfix for Windows XP (KB926239)	2	Desconocido
Image Resizer Powertoy for Windows XP	1.00.0001	Desconocido
Java(TM) SE Runtime Environment 6	1.6.0.0	Desconocido
K-Lite Codec Pack 2.81 Full	2.81	Desconocido
Microsoft .NET Framework 1.1 [español (alfabetización internacional)]	1.1.4322	Desconocido
Microsoft .NET		Desconocido

Framework 1.1 Hotfix (KB886903)			
Microsoft .NET Framework 1.1			Desconocido
Microsoft .NET Framework 2.0 with Security Updates			Desconocido
Microsoft .NET Framework 2.0 with Security Updates		2.0.50727	Desconocido
Microsoft Compression Client Pack 1.0 for Windows XP		1	Desconocido
Microsoft Internationalized Domain Names Mitigation APIs			Desconocido
Microsoft National Language Support Downlevel APIs			Desconocido
Microsoft Office Professional Edition 2003 [español (alfabetización internacional)]		11.0.7969.0	Desconocido
Microsoft SQL Server 7.0			Desconocido
Microsoft User-Mode Driver Framework Feature Pack			Desconocido

1.0			
	Microsoft Visual C++ 2005 Redistributable	8.0.56336	Desconocido
	Nero 7.5.9.0		Desconocido
	NOD32 antivirus system		Desconocido
	NOD32 FiX v2.1		Desconocido
1.76	QuickTime Alternative	1.76	Desconocido
	Real Alternative 1.51 Lite	1.51	Desconocido
	Reproductor de Windows Media 11		Desconocido
	Security Update para Microsoft .NET Framework 2.0 (KB917283)	1	Desconocido
	Security Update para Microsoft .NET Framework 2.0 (KB922770)	1	Desconocido
	Spybot - Search & Destroy 1.4	1.4	Desconocido
	TaskSwitchXP	2.0.11	Desconocido
	TuneUp Utilities 2006	5.3.2343	Desconocido
	Unlocker 1.8.5	1.8.5	Desconocido
	Winamp AudioPlayer	5.32.1003	Desconocido
	Windows Genuine Advantage Validation Tool	1.5.0530.0	Desconocido

(KB892130)

Windows Internet Explorer 7	20061107.210142	Desconocido
Windows Media Format 11 runtime		Desconocido
Windows Media Format 11 runtime		Desconocido
Windows Media Player 11		Desconocido
XPize 4.6 Lite BETA 1	4.6 Lite BETA 1	Desconocido

Licencias

Programas	Clave del producto
Microsoft Internet Explorer	B3P7V-Q2WTH-CRK4R-YHJRF-39H4M
Microsoft Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY
Microsoft Windows	B3P7V-Q2WTH-CRK4R-YHJRF-39H4M

Antivirus

Descripción de	Versión de	Fecha de la	Virus
----------------	------------	-------------	-------

la aplicación	la aplicación	Base de datos de los virus	conocidos
NOD32	3642 (20081126)	2008-11-26	?

HOJA DE METADATOS

Título	DESARROLLO DE UN PLAN DE GESTION PARA LA RED DEL PROGRAMA DE LA LICENCIATURA EN INFORMATICA DE LA UNIVERSIDAD DE ORIENTE NUCLEO DE SUCRE
Subtítulo	

Autor(es)

Apellidos y Nombres	Código CVLAC / e-mail	
GONZALEZ M., MALVINA	CVLAC	V- 12665756
	e-mail	
	e-mail	

Palabras o frases claves:

Gestión de redes
Administración de redes
Plan de gestión

Líneas y sublíneas de investigación:

Área	Subárea
Ciencia	Informática

Resumen (abstract):

Dado el continuo crecimiento de las redes y el auge tecnológico en las últimas décadas, ha surgido la necesidad de buscar herramientas que apoyen la gestión de redes de forma integrada y automática. En el presente trabajo se desarrolló un plan de gestión para los servicios teleinformáticos de la red del Programa de la Licenciatura en Informática del núcleo de Sucre de la Universidad de Oriente, el cual permite a los administradores de red realizar labores de gestión a la red local. Para la elaboración del plan de gestión se implementó la metodología Métrica[1], la cual permitió determinar las necesidades de planificación e identificar los requisitos, para ello fue necesario realizar entrevista que proporcionaron la información sobre los procesos que se ejecutaban en la red, lo que ayudó a conocer las actividades de administración y a determinar los requisitos necesarios tomándose en cuenta las áreas funcionales para la gestión de redes (configuración, avería, desempeño y seguridad). Esto permitió diseñar un plan de gestión para la red del Programa de la Licenciatura de Informática, que permitiera mejorar los procesos de administración, se propusieron procesos como monitoreo, documentación automatizada, políticas de seguridad, entre otras como actividades primordiales para gestionar la red. Para el diseño también se tomó en cuenta la administración de red que implementa el programa Networking Cisco, el cual ayudó a determinar cómo debe implementarse la documentación y proporcionar seguridad a la red en estudio. El desarrollo de este plan de gestión permitió mejorar los servicios que se ofrecen en la red y proporcionar herramientas de gestión que apoyen las funciones que cumplen los administradores y técnicos de la red, brindando a los usuarios una red eficiente, óptima y segura.

Contribuidores:

Apellidos y Nombres	ROL / Código CVLAC / e-mail	
Hugo Marcano	ROL	A C <input type="checkbox"/> AS <input checked="" type="checkbox"/> TU <input type="checkbox"/> JU <input type="checkbox"/>
	CVLAC	V-6.766.726
	e-mail	
	e-mail	
Daniel Jeremías	ROL	A C <input type="checkbox"/> AS <input type="checkbox"/> TU <input type="checkbox"/> JU <input checked="" type="checkbox"/>
	CVLAC	V-8.645.325
	e-mail	
	e-mail	
Ramón Gorrin	ROL	A C <input type="checkbox"/> AS <input type="checkbox"/> TU <input type="checkbox"/> JU <input checked="" type="checkbox"/>
	CVLAC	V-9.665.681
	e-mail	
	e-mail	

Fecha de discusión y aprobación:

Año Mes Día

2010	06	25
-------------	-----------	-----------

Lenguaje: spa

Archivo(s):

Nombre de archivo	Tipo MIME
Tesis_GonzalezM.doc	Application/Word

Alcance:

Espacial: Nacional (Opcional)

Temporal: Temporal (Opcional)

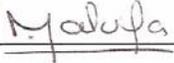
Título o Grado asociado con el trabajo: Licenciado en Informática

Nivel Asociado con el Trabajo: Licenciado

Área de Estudio: Informática

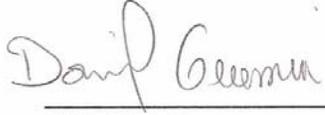
**Institución(es) que garantiza(n) el Título o grado:
Universidad de Oriente**

Yo Malvina Gonzalez Mistage autora intelectual de esta tesis le doy el derecho a la Universidad de Oriente para divulgar esta tesis siempre y cuando resguardando la patente de industria y comercio si se diera el caso.


AUTOR


ASESOR


JURADO 1


JURADO 2

POR LA COMISIÓN DE TESIS:

