ANÁLISIS, DIAGNOSTICO, DOCUMENTACIÓN Y FORMULACIÓN DE UNA PROPUESTA DE MEJORA AL PLAN DE GESTIÓN DE LA RED DE DATOS DE LA UIS

SERGIO ANDRÉS CONTRERAS BASTOS
EDGAR MACIAS ACERO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICO – MECANICAS
ESCUELA DE INGENIERIA ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
BUCARAMANGA
2006

ANÁLISIS, DIAGNÓSTICO, DOCUMENTACIÓN Y FORMULACIÓN DE UNA PROPUESTA DE MEJORA AL PLAN DE GESTIÓN DE LA RED DE DATOS DE LA UIS

SERGIO ANDRÉS CONTRERAS BASTOS
EDGAR MACIAS ACERO

Trabajo de grado presentado como requisito para optar al título de
Ingeniero Electrónico

Director
Ph.D. OSCAR GUALDRÓN GONZÁLEZ
Codirectores
Ing. BENJAMÍN PICO MERCHÁN
Ing. MARIA FERNANDA REYES SARMIENTO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICO – MECANICAS
ESCUELA DE INGENIERIA ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
BUCARAMANGA
2006

AGRADECIMIENTOS

A todas las personas que apoyaron y aportaron en la realización del trabajo de grado. En especial a nuestro director por sus acertados consejos, a los codirectores por sus sugerencias y disposición para colaborarnos.

Agradecemos también a los jefes y personal que labora en el campo de Administración de Red en la División de Servicios de Información, en la Universidad Autónoma de Bucaramanga, Universidad Santo Tomas y la Universidad de Pamplona por su disposición y colaboración con el suministro de información para el desarrollo del proyecto.

Agradezco a mis padres Rodolfo e Ilba por su apoyo continuo e incondicional, por ser mi fuente de inspiración y la razón de mi vida. A ellos Dedico mi esfuerzo y trabajo. A pesar de la distancia siempre permanecen y permanecerán en mi mente y en mi corazón…

A mis hermanos Fabián y Juan Carlos quienes son mi guía y ejemplo. Gran parte de mis logros derivan de la admiración que tengo hacia ellos. Gracias

Sergio Andrés Contreras Bastos

La vida de un hombre debe dirigirse a un solo objetivo
"La búsqueda de la inmortalidad"

Los profundos valores heredados de mis padres hacen que agradezca primero a Dios antes que a mi Familia, aunque en mi corazón los dos tienen igual valor, pues han sido mi refugio, motivación y apoyo incondicional. Gracias mamá – Edelmira, Gracias papá – Luis Francisco (que estas en el cielo), Gracias hermanos – Flor Alba y Cecilia (por recibirme en su casa), Consuelo y Nohora (por ser mi apoyo desde la distancia), Fernando (que estas en el cielo), Jhon Jairo, Héctor, Gerardo y Mauricio. Gracias a todos por su amor.
Padrino Alfredo Florez y Arnulfo Afanador (cuñado), Gracias por depositar su confianza en mí y por brindarme su ayuda en el momento en que más los necesitaba. Sin ustedes la aventura de convertirme en profesional no hubiera iniciado y por tanto en este momento no se hubiera materializado. Gracias Ramón, por abrirme las puertas de su casa. Gracias Diana por brindarme su amor. A todas las personas que me acompañaron durante estos cinco años y que por espacio no puedo nombrar, gracias.
Dedico este logro a los pequeños de la próxima generación de la familia Macias Acero (Laura Ximena, Paula Sofía, Jhon Fernando, Harold Steven, Shery Dahianna, Natalia Andrea, Fredy Alexander, Saira Liseth, Robinson Andrés y todos los que faltan por nacer).

Edgar Macias Acero

TABLA DE CONTENIDO

Pág.

LISTA DE FIGURAS

LISTA DE CUADROS

LISTA DE TABLAS

TITULO: ANÁLISIS, DIAGNÓSTICO, DOCUMENTACIÓN Y FORMULACIÓN DE UNA PROPUESTA DE MEJORA AL PLAN DE GESTIÓN DE LA RED DE DATOS DE LA UIS[*]

AUTORES: CONTRERAS BASTOS, SERGIO ANDRÉS
MACIAS ACERO, EDGAR [**]

PALABRAS CLAVE: Gestión de red, SNMP, dispositivos administrables, administración de procesos, benchmarking, Solarwinds, ITIL.

DESCRIPCION

El presente documento contiene la formulación de una propuesta de mejora al plan de gestión de red de la Universidad Industrial de Santander (UIS). La propuesta consta de la descripción de los subprocesos de instalación, monitorización y mantenimiento correctivo presentes en la gestión de red. Se realizaron guías de procedimientos para cada subproceso y se propuso la utilización del software "Solarwinds" como herramienta de gestión. La definición de los subprocesos y la descripción de sus diagramas de actividades se hizo en plantillas estándar propias de la UIS.

En el subproceso de instalación se realizó una guía básica de configuración para dispositivos activos (switches marca Avaya) y se formularon listas de chequeo para la revisión de normatividad, pruebas de conectividad y para la solución de inconvenientes en la puesta en marcha de los dispositivos. En el subproceso de monitorización se realizó la guía de configuración del software de gestión para la monitorización de los dispositivos activos administrables y de los servidores más importantes para la institución. En el subproceso de mantenimiento correctivo se realizaron listas de chequeo para la solución de problemas de configuración y conectividad en forma remota o con desplazamiento a sitio. Se realizó un formato para la documentación de los problemas reportados con sus soluciones. Se propone la creación de una base de conocimiento con la información recopilada en los subprocesos de monitorización y mantenimiento correctivo. Se propone también la creación de un centro de atención al usuario de la red.

La formulación de la propuesta de mejora se sustentó en la recopilación de las mejores prácticas en el campo de la gestión de red realizadas por personal interno de la UIS y otras instituciones educativas. Se utilizó también como referente la experiencia de un ingeniero de una empresa dedicada del sector y referentes teóricos.

---

[*] Trabajo de grado.

[**] Facultad de Ingenierías Fisicomecánicas
Ingeniería Electrónica
Director: Gualdrón González, Oscar.

TITLE: ANALISYS, DIAGNOSTIC, DOCUMENTATION AND IMPROVEMENT PROPOSAL FORMULATION FOR THE DATA NETWORK MANAGEMENT PLAN AT UNIVERSIDAD INDUSTRIAL DE SANTANDER[*].

AUTHORS: CONTRERAS BASTOS, SERGIO ANDRÉS
MACIAS ACERO, EDGAR [**]

KEYWORDS: Network Management, SNMP, Manageable Devices, Processes Administration, Benchmarking, Solarwinds, ITIL.

DESCRIPTION

The present manuscript contents the formulation of a proposal to improve the network management plan at Universidad Industrial de Santander. The proposal consists in the description of the subprocesses of the installation, the monitorization and the corrective maintenance which are included in the network management. Procedure guides for each process were prepared and also the utilization of the software "Solarwinds" as a management tool is proposed. The subprocesses definition and its diagram description activities were made on standard UIS' models.

In the installation subprocess, a basic configuration guide was prepared for the actives devices (Avaya switches) and checklists for the normativity revision, the connectivity probes and the problems solution on starting up the devices, were formulated. In the monitorization subprocess, the management software configuration guide to monitor manageable active devices and the most important servers for the university was made. In the corrective maintenance subprocess, checklists in order to sort out configuration and connectivity problems in remote way or with displacement to place were prepared.

On the other hand, a format to document reported problems with its corresponding solutions was prepared. In addition it was taken into account the information gathered in the supprocess of the monitorization and the corrective maintenance a knowledge base is proposed. As a complement of network user attention center building is recommended.

The improvement proposal formulation is supported on the best practices compilation carried in the network management area of internal UIS' personnel and other superior educative institutions. Also, as a referral was used the engineer's experience who at the present time works for an enterprise dedicated to communication sector. Besides theoretical references were consulting in the preparations of this manuscript.

---

[*] Trabajo de grado.
[**] Facultad de Ingenierías Fisicomecánicas
Ingeniería Electrónica
Director: Gualdrón González, Oscar.

INTRODUCCIÓN

Al considerar que la información es tal vez el recurso más valioso que tienen las organizaciones y que buena parte de la infraestructura tecnológica instalada está destinada a permitir su flujo, es importante que las organizaciones cuenten con planes de gestión de red estructurados a la medida de sus necesidades.

En la actualidad, cuando se habla de gestión de red no se hace referencia solo a la parte operativa (técnica y tecnológica), es decir, no implica solamente asegurar mayor disponibilidad, seguridad, rendimiento y aprovechamiento de los recursos de la red de datos. Ahora se considera a la gestión de red como un área funcional que hace parte e interactúa con las demás áreas dentro de la organización.

Por esta razón se hace necesario conocer, estudiar e implantar recomendaciones, modelos y estándares de gestión que permitan incluir todas las áreas tanto para la parte operativa como para las demás áreas de interés dentro de la gestión de red y dentro de la organización, tales como área financiera, comercial, administrativa, etc. que le permitan asegurar el uso eficiente de los recursos, estandarizar las operaciones, facilitar la realización de los trabajos, dar uniformidad a las actividades realizadas y ofrecer una calidad de servicio adecuada.

Con el propósito de cumplir estos objetivos se crearon modelos como eTOM[1] para la gestión de negocios, que incluye todas las áreas de la organización y describe la interacción entre ellas. Asimismo los lineamientos de ITIL[2] que abarca siete áreas de interés como: Servicio de Soporte, Entrega de Servicios, Administración de Seguridad, Administración de la Infraestructura de Tecnologías de la

[1] Enhancement Telecomunication Operation Management
[2] IT Infrastructure Library – Mejores prácticas para la gestión de servicios de Tecnologías de la Información - TI

Información y Comunicaciones – TIC entre otras. Estos lineamientos están incluidos dentro de la norma de gestión de calidad ISO 20000, el cual es el primer estándar internacional de referencia para la implantación de sistemas de gestión de calidad en empresas que prestan servicios de Tecnologías de la Información – TI.
Estos modelos y recomendaciones proponen implementar un marco de procesos "framework" que permita abarcar las áreas dentro la organización, describir la interacción entre ellas y cumplir con los objetivos de cada una, incluidas las actividades propias de la gestión de red operativa.

Cualquier organización independiente de su tamaño y del sector al que pertenezca (público o privado) puede implementar estos frameworks, particularizar sus necesidades y trabajar bajo procesos probados que le garanticen el uso óptimo de la Tecnología de Información.
Por ello para implantar un sistema de gestión de red, el primer paso a realizar es enmarcarlo a nivel organizacional, identificar y documentar los procesos propios de la gestión operativa y los procesos relacionados que en su conjunto interactúan para ofrecer un servicio de TI.

Particularmente, en la UIS, la administración y mantenimiento de la red de datos institucional es una tarea que exige gran atención. Mantener en funcionamiento constante servicios de información académica, acceso a Internet, información bibliográfica, financiera, de contabilidad, entre otros, a la comunidad universitaria y teniendo en cuenta que una falla que afecte estos servicios ocasiona *inconvenientes de impacto institucional*, hacen evidente la necesidad de contar con un plan estructurado de gestión para realizar esta labor. Por esta razón la Universidad cuenta con la División de Servicios de Información – DSI, dependencia dedicada a realizar las labores de administración, mantenimiento y desarrollo de la red de datos y de las tecnologías de la información en general, misión que permite identificar a la DSI como una organización que presta servicios de TI dentro de la Institución.

Por lo anterior, el presente proyecto de grado se desarrolla en el campo de la Gestión de Red. Se formula una propuesta de mejora al plan de gestión de la red de datos institucional. Se aborda desde la descripción de tres de sus subprocesos: Instalación, Monitorización y Mantenimiento Correctivo. Se elaboran guías de procedimientos para dichos subprocesos y se propone la integración del software SolarWinds como herramienta de gestión. Esta forma de abordar la propuesta, desde la descripción de subprocesos, tiene como fin aportar los primeros elementos para la implantación de un sistema de gestión de calidad dentro de la DSI.

La propuesta se sustenta en la recopilación de información proveniente de la experiencia de las personas que actualmente administran la red de datos institucional y en la indagación de las buenas prácticas que se realizan en instituciones con infraestructuras de red similares a la UIS. Se utiliza el concepto de Benchmarking como metodología para el levantamiento y análisis de la información interna y de las instituciones escogidas como socios de benchmarking: Universidad Autónoma de Bucaramanga – UNAB, Universidad de Pamplona – UP y Universidad Santo Tomás seccional Bucaramanga. Además se utiliza información externa de esquemas de procesos utilizados actualmente en el sector de proveedores de servicios.

La presentación del proyecto inicia con el marco teórico donde se abordan los conceptos básicos de Gestión de red, administración de procesos, concepto de Benchmarking y la descripción del software de gestión de red SolarWinds. En el capítulo II, se muestra la recopilación y análisis de la información producto de la aplicación de la metodología de benchmarking en la UIS y en las instituciones mencionadas. Además se incluye la información relevante suministrada a título personal por el ingeniero Juan Carlos Contreras Bastos quien labora en la empresa Emtelco S.A. Se concluye con la extracción de las ideas sobre las que se sustenta la formulación de la propuesta de mejora al plan de gestión red de la

UIS que se presenta en el capítulo III. La formulación comprende la definición y descripción de los subprocesos de Instalación, Monitorización y Mantenimiento Correctivo, la presentación de sus diagramas de actividades y la elaboración de las guías de procedimientos que incluyen la elaboración y descripción de listas de chequeo y los instructivos para cada subproceso. En el capítulo IV se muestran los resultados de la aplicación de la herramienta de gestión SolarWinds en la monitorización del switch central y algunos servidores. Se finaliza con las Conclusiones y Recomendaciones y con los Anexos que complementan los capítulos II y III.

1. MARCO TEÓRICO

Los temas tratados en este marco conceptual son de vital importancia para la comprensión y el desarrollo del presente proyecto. Se abordan conceptos básicos sobre gestión de red, descripción del software de gestión SolarWinds, administración de procesos y la metodología de Benchmarking. Los últimos tres temas son los elementos que se utilizan para desarrollar el proyecto, el cual se enfoca en la gestión de red.

1.1 GESTIÓN DE RED – CONCEPTOS[4][6][9][11]

Introducción

En la década de los 80's el mundo de las redes experimentó una rápida expansión que causó un crecimiento incontrolable y desordenado de las tecnologías e infraestructuras de red, donde predominaron los diseños y sistemas propietarios. Este hecho obligó a planear y desarrollar estrategias en busca del diseño de redes flexibles y robustas. De estas estrategias surgió la visión de automatizar la administración de las redes.

En la actualidad la gestión de red dejó de ser una visión para convertirse en una realidad y ha pasado de ser un complemento para convertirse en parte primordial y esencial tanto para fabricantes de dispositivos, quienes ofrecen equipos y herramientas estándar que permiten expansiones, actualizaciones y evoluciones transparentes de infraestructuras de red con opciones avanzadas de administración, como para las organizaciones que utilizan las redes como soporte para el intercambio de información en su interior y con el mundo exterior, con la

urgencia cada vez más marcada de poseer supervisión y control sobre sus dispositivos y sistemas de red.

La gestión de red permite superar las barreras de entornos heterogéneos en el tipo de información manejada (datos, voz, video) y el tipo de organización (entornos jerárquicos y distribuidos). Por medio de ella las organizaciones pueden poseer y manejar una gran variedad de dispositivos en ocasiones de diferente tecnología y fabricante, con el fin de mantener un servicio aceptable para sus usuarios y garantizar su permanencia y evolución.

Las inversiones realizadas por las empresas en la implementación de estrategias de gestión en sus redes, implica una inversión proporcional al grado de monitorización y control que se desee sobre cada una de ellas. Sin embargo, como ya se mencionó, la gestión es una urgencia y justifica su inversión con mejoras y beneficios para las organizaciones. Ofrece control sobre sus recursos estratégicos sin importar la complejidad sobre la cual estén implementados, reduce los tiempo de no funcionamiento de sus redes, mejora el servicio prestado y evita pérdidas.

1.1.1 Generalidades

La gestión de red es un servicio que comprende tanto la gestión operativa (técnica y tecnológica) como la gestión de los servicios que soporta la red. En este sentido es necesario identificar la gestión de red como un área funcional que hace parte e interactúa con las demás áreas funcionales de la organización donde la gestión operativa es un elemento dentro de un concepto más amplio de la gestión de red. Dentro de este concepto existen áreas que permiten la interacción de la infraestructura tecnológica, el personal dedicado a garantizar el servicio y el cliente. Las áreas a las que se hace referencia son: gestión de desempeño, configuración, fallas, seguridad, entre otras, que enmarcadas dentro de un

esquema de procesos se encarga de garantizar la prestación de un servicio a la medida de las necesidades de la organización y de los clientes.

1.1.2 Funciones de la gestión

Las funciones de la gestión operativa se pueden agrupar en dos grandes categorías:

Monitorización: corresponde a procesos "lectura". Permite observar y analizar el estado y comportamiento de la configuración de red y sus componentes.
Cumple 3 objetivos fundamentales:

* Identificar y clasificar la información a monitorizar.
* Diseñar mecanismos de monitorización.
* Utilizar la información

En general tiene como función principal, recolectar información referente al estado y funcionamiento de los elementos de la red, obtiene características de configuración (información estática) y de los eventos presentados (información dinámica) con la cual se constituye la información estadística.

Control: corresponde a procesos "escritura". La parte de control permite al administrador realizar modificaciones remotas en puntos específicos dentro de la red para realizar ajustes.
Todas las áreas de gestión abarcan monitorización y control.

1.1.3 Elementos de un Sistema de Gestión de Red

Un sistema de gestión es aquel que nos permite desarrollar la planificación, organización, supervisión y control de los elementos constitutivos de la red. Utiliza herramientas, aplicaciones y dispositivos con el propósito de mejorar la disponibilidad, el rendimiento e incrementar la efectividad de la red. Su objetivo es

garantizar un nivel de servicio aceptable acorde a las necesidades de los usuarios y a los costos establecidos por la organización.

Las arquitecturas de gestión se basan en el modelo Gestor-Agente que opera de dos maneras: *forma directa* (gestión centralizada) y *forma distribuida* (gestión distribuida). En la primera un solo elemento (gestor) dentro de la red interroga a los dispositivos administrables para obtener la información de gestión. En el esquema distribuido los agentes instalados en cada dispositivo pueden actuar tambien como gestores y recopilar información de los equipos que pertenecen al mismo nodo y hacer un único reporte al gestor principal. Todo modelo de gestión esta constituido por un conjunto mínimo de elementos software y hardware que interactúan entre sí de manera que permitan cumplir las necesidades de monitorización y control.

En este proceso intervienen elementos fundamentales como son:

- El Gestor (Proceso Gestor).
- El Agente (Proceso Agente).
- El Protocolo de Gestión.
- La Base de Información de Gestión (MIB[3]).

En la Figura 1 se esquematiza la forma como interactúan estos elementos.

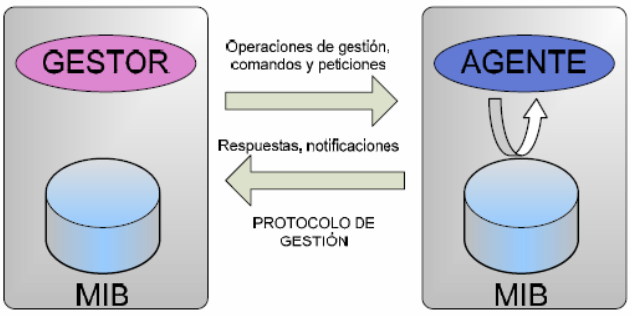


Figura 1. Esquema de interacción Modelo Gestor - Agente

[3] MIB: Management Information Base. En español significa Base de Información de Gestión.

Fuente: GUZMAN CASTILLO PAOLA F. "Análisis de la gestión de dispositivos administrables en la red de datos institucional" Trabajo de investigación, Universidad Industrial de Santander 2005. Pág. 12.

El Gestor, es la parte de la aplicación que se comunica con los diversos agentes de la red. Envía comandos a los agentes para que realicen acciones y recibe su respuesta. Se implementa en una estación de gestión y debe disponer de la MIB de cada dispositivo y de una interfaz de usuario.

El Agente, es un programa que reside en cada elemento u objeto gestionado de la red (se ubica de manera directa en cada nodo o en otro nodo externo "Proxy-Agent"). Se encarga de gestionar los recursos dentro de dicho componente y notificar el estado del objeto periódicamente o a petición del gestor.

El Protocolo de gestión, conjunto de especificaciones y convenciones que definen cómo el gestor se comunica con los agentes. En ocasiones se denomina protocolo gestor – agente Algunos ejemplos de protocolos de gestión son SNMP (Simple Network Management Protocol) para redes TCP/IP (Transmission Control Protocol/Internet Protocol) que hace parte del modelo de gestión de Internet y el protocolo CMIP (Common Management Information Protocol) para entornos OSI[4].

La Base de Información de Gestión (MIB), es una base de datos que contiene la información del estado, desempeño y configuración de cada dispositivo de red y posee el estado de sus recursos representados mediante objetos dentro de la estructura de la MIB. Todas las operaciones de monitorización consultan (leen) el valor de los objetos y las operaciones de control modifican (escriben) el valor de los objetos.

1.1.4 Modelos de Gestión

[4] OSI: Open System Interconection. En español significa Interconexión de Sistemas Abiertos

La gestión de red también ha incurrido en soluciones propietarias, limitando sus campos de acción y truncado su visión de integración, principalmente por las variedad de fabricantes en el mercado. Por esta razón surge la necesidad de poseer sistemas de gestión estandarizados que soporten las infraestructuras de red heterogéneas y permitan hacer protocolos compatibles para el intercambio transparente y unificado de la información de gestión.
De esta forma en la década de los 90`s se desarrollaron iniciativas con miras a resolver estos inconvenientes y aparecieron protocolos de gestión como SNMP y CMIP, utilizados en modelos de gestión que buscan la estandarización.

Sin embargo, las distintas soluciones que buscan la gestión integrada, siguen sin solucionar en su totalidad la barrera de una gestión totalmente integrada, ya que cada uno de estos modelos utiliza su propio protocolo, su propia estructura de información y definen sus propias variables de información.
A continuación se mencionan los tres modelos de gestión más importantes. Se profundiza en el modelo de gestión SNMP por ser el más utilizado en redes basadas en TCP/IP.

- Modelo TMN (Gestión de Sistemas de Telecomunicaciones)
- Modelo de gestión OSI
- Modelo de Gestión en Internet (SNMP)

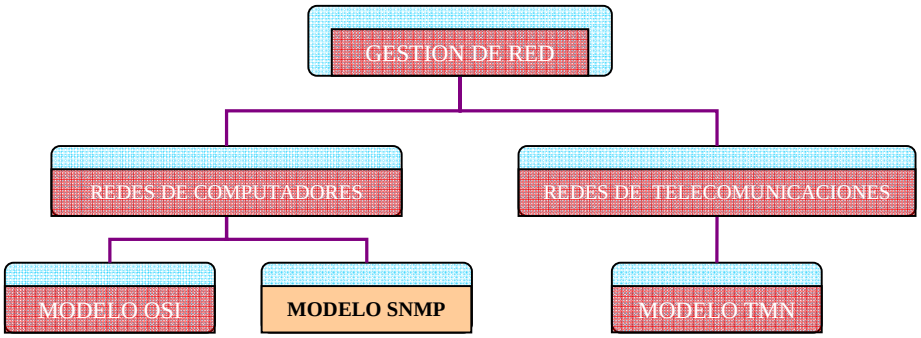


Figura 2. Esquematización de los Modelos de Gestión de Red

- *Modelo de Gestión en Internet (SNMP)*

Definido por el IAB (Internet Activities Board) para gestión de redes TCP/IP. En la actualidad las últimas versiones son compatibles con redes TCP/IP y redes basadas en OSI. Es un modelo Gestor/Agente orientado a la gestión centralizada, utiliza el protocolo SNMP que permite realizar observaciones y controles sobre los dispositivos de la red.

El modelo SNMP se ha convertido en una arquitectura de gestión ampliamente utilizada y preferida tanto por fabricantes como por administradores, por esta razón la gran mayoría de los dispositivos y equipos de redes incorporan un conjunto de estándares denominado SNMP, que incluye un protocolo, una estructura de base de datos y un conjunto de definiciones de objetos de datos, que les permite ser gestionados vía SNMP.

El modelo SNMP, también posee los elementos requeridos para la gestión de una red de datos, los componentes del esquema de gestión basada en SNMP son fundamentales para completar el proceso de gestión requerida, estos son:

Estación de Gestión: computadora de propósito general que ejecuta un software de administración especial para realizar las tareas de gestión. Permite la interacción de administrador con los dispositivos a gestionar, contiene el gestor SNMP que ejecuta los procesos para comunicarse con los agentes a través de la red, emite comandos y recibe respuestas utilizando SNMP y una MIB central.

Agente de Gestión: representa el software que reside en los dispositivos administrables y permite el acceso a los datos de gestión del dispositivo mediante peticiones por parte de gestor o notificaciones propias. Cada agente mantiene una base de datos local de variables que describe el estado y las características de cada dispositivo.

Base de Información de Gestión (MIB): permite llevar a cabo los procesos de monitorización y control. El gestor realiza la monitorización accediendo y leyendo el valor de cada objeto de la MIB y realiza el control modificando determinadas variables SNMP.

La MIB es una colección de información organizada jerárquicamente que se accede mediante la utilización de protocolos de gestión como SNMP y que contiene toda la información relacionada con el estado y configuración de los elementos de la red. La MIB contiene 126 áreas de información sobre el estado del dispositivo, el desempeño, sus conexiones y su configuración. A través de la MIB se tiene acceso a la información de gestión contenida en la memoria interna de cada dispositivo administrable. Cada una de las variables que conforman la MIB se identifica con el OID (Object Identifier) dentro del árbol de OIDs establecidos por la ASN.1 (Abstract Syntax Notation One). Los OIDs corresponden a una secuencia de enteros separados por puntos decimales que establecen niveles numéricos que permiten establecer el camino hacia cualquier objeto dentro del árbol partiendo de la raíz. Todos los objetos de interés para SNMP derivan del nodo Internet y por tanto tiene el prefijo 1.3.6.1 en sus identificadores de objeto.

Protocolo de Gestión: El Gestor y los agentes SNMP realizan las comunicaciones entre ellos utilizando el protocolo de gestión SNMP, que les permite realizar las tareas de recolección y notificación de valores determinados mediante el uso de las primitivas definidas en el protocolo.

1.1.5 Protocolo SNMP (Simple Network Management Protocol)

En los años 80 surgen tres propuestas de estándar de protocolo de gestión para TCP/IP: HEMS (High-level Entity Management System), SNMP (Simple Network Management Protocol) una versión mejorada de SGMP (Simple Gateway-Monitoring Protocol) y CMOT (CMIP over TCP/IP) que pretendía implantar los estándares del modelo de gestión OSI.

La IAB decidió desarrollar SNMP como la solución a corto plazo y CMOT a largo plazo, especulando el dominio de las redes OSI. Sin embargo, la iniciativa CMOT no prosperó con el tiempo y el protocolo SNMP fue el elegido y se convirtió en el protocolo estándar para la gestión de redes TCP/IP, que serían las redes que finalmente se desarrollarían y tendrían la mayor acogida.
SNMP es un protocolo no orientado a conexión de la capa de aplicación que se ejecuta sobre las capas IP y TCP utilizando el protocolo UDP para el intercambio de la información. Es un protocolo asimétrico (se basa en el modelo Gestor-Agente) que sirve como herramienta de gestión de red sencilla y fácil de implementar, constituyéndose ésta en su mayor ventaja.

El protocolo SNMP funciona entre los gestores y los agentes, y es utilizado para la intercomunicación entre ellos, quienes son los encargados de mantener y mejorar el desempeño de la red, manteniendo un intercambio permanente de información.

Los cinco tipos de mensajes SNMP intercambiados entre los agentes y el gestor son:

- *Get Request:* petición del gestor al agente para que envíe los valores contenidos en el MIB, para obtener el valor de una o más variables.
- *Get Next Request*: petición del gestor al agente para que envíe la siguiente variable después de una o más variables especificadas.
- *Get Response:* respuesta del agente a la petición realizada por el gestor.
- *Set Request:* petición del gestor al agente para que cambie el valor de una o más variables referente a un determinado objeto.
- *Trap:* mensaje espontáneo del agente al gestor, al detectar una situación imprevista.

SNMPv2

En 1996 se publicó un nuevo estándar del protocolo SNMPv2 que mejoró las prestaciones de la primera versión. El cambio más importante constituye la

incorporación de mecanismos de seguridad y mejoró el mecanismo de transferencia de información, de modo que se realizan menos peticiones para obtener paquetes grandes de información.

SNMP v2 define dos MIBs:

- MIB SNMPv2: guarda información relacionada con la operación e información del protocolo, agentes y gestor.
- MIB M2M (Manager to Manager): es soporte para la arquitectura de gestión distribuida, permite describir y configurar umbrales de alarma y configurar eventos.

SNMPv3

Las especificaciones definidas en la versión SNMPv2 no disponían de mecanismos de autenticación y cifrado de mensajes, debido a esto surgió en 1998 SNMPv3 para suplir estas deficiencias.

1.2 SOFTWARE DE GESTION DE RED – SOLARWINDS[12]

SolarWinds es una herramienta de administración de red que posee múltiples aplicaciones para la administración de configuración, monitorización de desempeño, ancho de banda, así como aplicaciones para el descubrimiento, modelado, pruebas de vulnerabilidad ante fallas, seguridad de red, entre otras.
Con ella se tiene control del desempeño, disponibilidad, seguridad, comportamiento e inventario lógico de la red de datos mediante la recopilación de información vía SNMP o CMIP de dispositivos administrables como switches capa 2, switches capa 3, routers y servidores.

Entre todas las ediciones de SolarWinds, la edición para ingenieros – “Solarwinds Engineer’s Edition” contiene la totalidad de herramientas para llevar a cabo una gestión técnica completa de la red.
Las herramientas con las que cuenta son las siguientes:

- *Herramientas de Gestión del Desempeño (Network Performance Management Tools)*

Permiten la monitorización del tráfico, ancho de banda, carga de la CPU y utilización de múltiples dispositivos administrables, permite la generación de alarmas vía mail o beeper cuando algún umbral de desempeño preestablecido es superado. La información es visualizada en tiempo real y almacenada para poseer datos histórico del desempeño de los dispositivos.

Además tiene la capacidad de monitorizar y graficar las estadísticas de cualquier OID dentro del árbol de la MIB que responda al protocolo SNMP.

- *Herramientas de Monitorización (Network Monitoring Tools)*

Permiten la monitorización de cientos de dispositivos, supervisa gráficamente los tiempos de respuesta y los paquetes perdidos, notifica cuando los tiempos de respuesta de la red comienzan a degradarse o cuando algún dispositivo sale de funcionamiento

Ofrece señalizaciones gráficas y sonoras para indicar eventos anómalos relacionados con los dispositivos monitorizados.

- *Herramientas de Descubrimiento de la Red (Network Discovery Tools)*

Permiten descubrir y documentar las direcciones IP dentro de la red, tienen la capacidad de escanear un rango de direcciones IP e indica cuales se encuentran reservadas, cuales están en uso y cuales libres.

Además una de sus herramientas. “Network Sonar” permite construir una base de datos de la estructura y los dispositivos en una red TCP/IP.

- *Herramientas de Diagnóstico (Ping & Diagnostic Tools)*

Herramientas que permiten monitorizar determinado numero de dispositivos como router, switches, servidores, PC`s y mostrar los resultados en tiempo real. Además permiten el escaneo de direcciones y realizar pruebas de conectividad.

- *Herramientas de Seguridad (Security Tools)*

Se utilizan para mejorar la seguridad de la red de datos, permiten, administrar las claves de acceso así como elegir contraseñas y comunidades con un alto grado de confiabilidad para evitar el acceso de personal no autorizado. Además permite probar la seguridad de los dispositivos administrables.

- *Herramientas para la Administración de Direcciones IP (IP Address Management Tools)*

Se utilizan para facilitar la documentación del espacio de direcciones IP, permite monitorizar automáticamente las direcciones en la red y clasificar cuales se encuentran reservadas, cuales están en uso y cuales libres. Además recopila información relacionada con el mapeo de nombres de dominio a direcciones IP y viceversa y monitorizar servidores DHCP para visualizar el rango de direcciones disponibles así como el porcentaje de aprovechamiento de las mismas.

- *Herramientas Misceláneas (Miscellaneous Tools)*

Entre ellas se encuentra un servidor TFTP para cargar y descargar archivos de configuración en swiches y routers y Wan Killer, generador de trafico hacia una estación deseada, ente otras.

- *Herramientas para la Revisión de la MIB (MIB Browser Tools)*

Permiten la búsqueda, visualización y modificación de los valores de la MIB de dispositivos administrables compatibles con SNMP, visualiza los resultados en tablas para facilitar su comprensión y administración.

- *Administración de dispositivos Cisco (Cisco Tools)*

Se utilizan para la actualización de software, monitorización y administración de dispositivos CISCO. Permite visualizar variables de configuración y desempeño, así como comparar distintos archivos de configuración y realizar pruebas de conectividad.

También permite la generación de alarmas de acuerdo a umbrales de carga preestablecidos por el administrador.

1.3 ADMINISTRACIÓN DE PROCESOS[7] – [8]

1.3.1 Generalidades

En el pasado las empresas se preocupaban por corregir y mejorar solo sus procesos de producción. En la década de los 80`s surge una idea que propone considerar a la empresa como una operación compleja con muchos procesos, que tiene la misma o más importancia que los procesos de producción. Ejemplos de ello son la atención al cliente, publicidad, desarrollo de comunicaciones avanzadas, desarrollo de la información, elección de proveedores, etc. los cuales emplean materiales, equipos y personas para ofrecer diferentes tipos de salidas y servicios. A estos procesos se le denominan *procesos de la empresa*.

1.3.2 Definiciones

"Un ***proceso*** es la forma en que el trabajo crea valor para los clientes. Es también un conjunto de actividades mutuamente relacionadas o que interactúan entre sí, y las cuales transforman elementos de entrada en resultados"[5].

> La ***administración de procesos*** es un enfoque administrativo que busca la identificación y la gestión sistemática de las actividades desarrolladas en la organización y en particular las interacciones entre estas. Consiste en la planeación y administración de las actividades necesarias para lograr un elevado nivel de desempeño en un proceso y en la identificación de

[5] Norma Técnica Colombiana NTC-ISO 9000 versión 2000

oportunidades de mejorar la calidad, el desempeño operacional y finalmente, la satisfacción del cliente.

Para que la administración de procesos sea exitosa en cualquier empresa, requiere de un esfuerzo organizacional muy grande en el que todos los trabajadores de la organización deben participar[6].

1.3.3 Características

Todos lo procesos bien definidos y bien administrados tienen características que los distinguen[7]:

- Tienen a alguien a quien se considera responsable de aquella forma en la cual se cumplen los procesos.
- Tienen límites bien definidos.
- Tienen interacciones y responsabilidades internas bien definidas.
- Tienen procedimientos documentados, obligaciones de trabajo y requisitos de entrenamiento, entre otros.

Centrarse en los procesos de la empresa es de utilidad para la organización de varias formas[8]:

- Permite a la compañía predecir y controlar cambios.
- Ofrece una visión sistemática de las actividades.
- Previene posibles errores.
- Da una visión sobre la forma en que ocurren los errores y la manera de corregirlos, entre otras.

1.3.4 Clasificación de los procesos dentro de una organización

[6] LINDSAY, William y EVANS, James. La Administración y el Control de la Calidad. Internacional Thomson editores, Cuarta edición. México, 2000.
[7] HARRINGTON, H. James. Mejoramiento de los Procesos de la Empresa. Santafé de Bogotá: Mc GrawHill, 1992. p. 17.
[8] Obid. p.17,18

Según la Norma Técnica Colombiana NTC-ISO 9000 versión 2000, los procesos se clasifican en:

- *Procesos de Planeación*

  Estos procesos son los que se encargan de organizar las actividades llevadas en cada proceso, para que los procedimientos allí llevados se hagan de una manera eficiente, buscando mejorar cada vez más de una forma productiva.

- *Procesos de Producción o de generación del servicio*

  Aquí se busca analizar profundamente la realización del servicio como tal, se detallan todos los procedimientos que propiamente pueden afectar la prestación de este, y se busca manejar todas las variables que pueden llegar a influir en la calidad del servicio.

- *Procesos de Apoyo*

  Estos procesos soportan los demás, son los encargados de manejar los recursos necesarios para que los procesos anteriormente nombrados, funcionen de la mejor manera posible.

- *Procesos de Medición, Análisis y Mejora*

  Son los procesos que controlan a los demás, midiéndolos, analizándolos y siempre buscando la mejora continua de la organización.

1.4 EL CONCEPTO DE BENCHMARKING[13]

El Benchmarking se desarrolla como un proceso de aprendizaje valioso por medio del cual, se analizan las actividades de los mejores procedimientos a nivel de productos, procesos u operaciones que realizan las entidades reconocidas en ese campo.

Este análisis determina cuales de los conocimientos que pueden brindar estas entidades consiguen ser transformados en acciones reestructuradas que se aplican en la organización para generar cambios con resultados óptimos, logrando así, un aprendizaje continuo de las prácticas exitosas reconocidas y de la estructura productiva de la entidad.

Las razones principales por las cuales las organizaciones tienen en cuenta el Benchmarking en su administración son:

- Es un medio para la solución de problemas introduciendo mejoras eficientes que ya han sido probadas.
- Las mejoras pueden ser introducidas en tiempos reducidos por medio de los procesos ya estudiados.
- Es un mecanismo que mantiene actualizada a la empresa en cuanto a las mejores prácticas.
- Es una herramienta para la consecución de nuevas ideas de negocios.
- Es un proceso de Planificación Estratégica debido a la recopilación de información que se puede hacer.
- Identifica tendencias y aspectos claves para realizar pronósticos.
- Permite posicionar a la empresa dentro del mercado logrando un aumento en las utilidades generadas.

1.4.1 TIPOS DE BENCHMARKING

Dependiendo de los objetivos que se pretendan alcanzar y de la forma en que se desee aplicar el Benchmarking, existe la posibilidad de trabajar de diferentes modos, aunque en esencia todos se desarrollan con los mismos fundamentos.

- *Benchmarking Interno*

Consiste en centrarse en los análisis de los mejores productos, procesos u operaciones desarrollados al interior de la organización. De esta forma se busca conocer profundamente los estándares internos manejados en la empresa para llevarlos a nivel de toda la organización, permitiendo así la generación de argumentos que permitan reconocer las prácticas exitosas desarrolladas en otras organizaciones.

- *Benchmarking Competitivo*

Consiste en centrarse en los análisis de los mejores productos, procesos u operaciones desarrollados al interior de las empresas que son competencia directa para la organización. Por tanto, es la forma de Benchmarking más difícil que existe, donde la recolección de datos se dificulta debido a la barrera impuesta por los competidores.

- *Benchmarking Funcional*

Consiste en centrarse en el análisis de los mejores productos, procesos u operaciones desarrollados al interior de las organizaciones que se destacan por su excelencia en el tipo de procedimientos que se pretenden estudiar. Este tipo de benchmarking se centra el análisis en una sola área funcional, lo que facilita su elaboración.

1.4.2 EL PROCESO DE BENCHMARKING

Las etapas que se describen a continuación son genéricas, es decir, permiten desarrollarse para cualquier tipo de Benchmarking a trabajar, además de ser adaptables según la organización que desee manejarlas.

Determinar a que se le va a hacer Benchmarking:

En este primer paso se definen claramente los procesos y las personas que requieren la información generada por el Benchmarking además de las

necesidades de las mismas, logrando así, establecer los aspectos específicos que serán estudiados.

Formar un equipo de Benchmarking:

En esta etapa se seleccionan las personas que van a conformar el equipo según los criterios de habilidad y motivación que se requieran en el proyecto, procurando obtener un talento humano brillante, con credibilidad en su medio laboral y con el enfoque suficiente para aprovechar al máximo el potencial del proceso de Benchmarking. Para que esto se dé la organización debe asignar los recursos que sean necesarios para el desarrollo del proceso, teniendo en cuenta la capacitación y reconocimiento que el equipo debe obtener para que sea apoyado en su labor.

Identificar los socios de Benchmarking:

En esta etapa se investiga de manera exhaustiva cuales son las empresas con las mejores prácticas por medio de servicios de investigación interna y externa. Esta investigación requiere que se identifique fuentes de información específica disponibles para todos los involucrados en el proceso, además, de no limitar las herramientas o la información para la investigación que tradicionalmente se emplean.

Recopilar y analizar la información de Benchmarking:

Para el desarrollo de esta etapa se requiere identificar las metodologías de recopilación de información, primero en las fuentes internas y después en las externas, implementando informes y resúmenes que mantengan la organización y el equipo preparado para el proceso de implementación, habiendo eliminado con anterioridad las posibles fuentes erróneas de información, las omisiones o repeticiones de la misma.

Teniendo toda la información disponible se deben medir las prácticas avanzadas en términos que permitan cuantificar las cualidades de las mismas para comprender como se consiguen tales resultados.

Al tener todo cuantificado se prosigue a comparar las prácticas avanzadas con las de la empresa, estableciendo las diferencias que llevarán al desarrollo de los planes de mejoramiento, con los que se pretende igualar y superar las prácticas más avanzadas. Para esto debe tener en cuenta si el plan que se pretende implementar va en el mismo sentido de la visión, misión y objetivos que enmarcan la organización.

Actuar:

Para esta etapa ya se tiene estructurado un informe coherente con el análisis de la investigación de Benchmarking, las posibles mejoras específicas de los productos o procesos, las oportunidades de aprender y la formación de las redes funcionales o de apoyo. El compromiso de la organización con el proceso es un lazo fuerte que permite llevar a cabo los planes de mejoramiento y la supervisión de sus resultados. Con la retroalimentación del proceso estudiado y de las mejoras implementadas, se le da continuidad a la herramienta de Benchmarking.

2. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LOS PLANES DE GESTIÓN DE RED A NIVEL INTERNO Y EN INSTITUCIONES SIMILARES A LA UIS APLICANDO LA METODOLOGÍA DE BENCHMARKING

En el presente capítulo se consigna la información e ideas que sustentan la formulación de la propuesta de mejora al plan de gestión de red de la UIS. Inicia con el marco de referencia donde se sitúa el proyecto dentro del contexto institucional en el que se desarrolla. Se hace una descripción del diagrama organizacional de la UIS, se ubica a la DSI dentro de este y se profundiza hasta situar el proyecto dentro del esquema de procesos de la DSI. Se continúa con la presentación de los resultados de la metodología de benchmarking. Se presenta la información recopilada en la UIS (benchmarking interno) y la información recopilada en otras instituciones educativas – UNAB, UP, Santo Tomas (benchmarking funcional). Se hace el análisis de la información mediante tablas comparativas y se muestran las mejores prácticas identificadas en las distintas instituciones. Al final se presentan las ideas relevantes de la entrevista con el ingeniero Juan Carlos Contreras Bastos de la empresa EMTELCO S.A. y con esto se colocan las bases para la formulación de la propuesta de mejora al plan de gestión de red de la UIS.

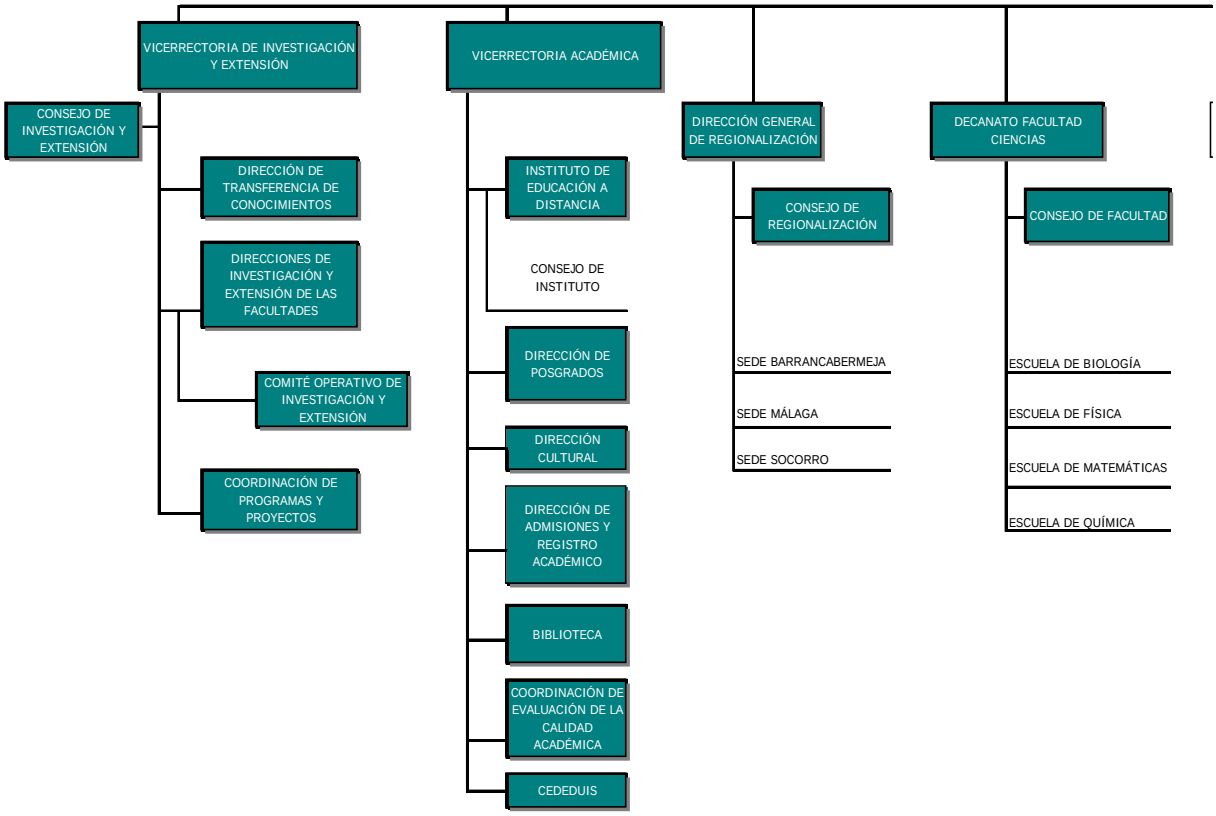
2.1 MARCO DE REFERENCIA

La UIS mediante acuerdo 073 de 2005 del Consejo Superior, estructuró su organización en 3 vicerrectorias (Investigación y Extensión, Académica y Administrativa), 5 decanaturas y la Dirección General de Regionalización. Adscrita a la Vicerrectoría Administrativa se encuentra la DSI, que se encarga de la

"administración y el desarrollo de la tecnología de la información en los ámbitos académico y administrativo"[9]. Ver Figura 3. Pág. 2

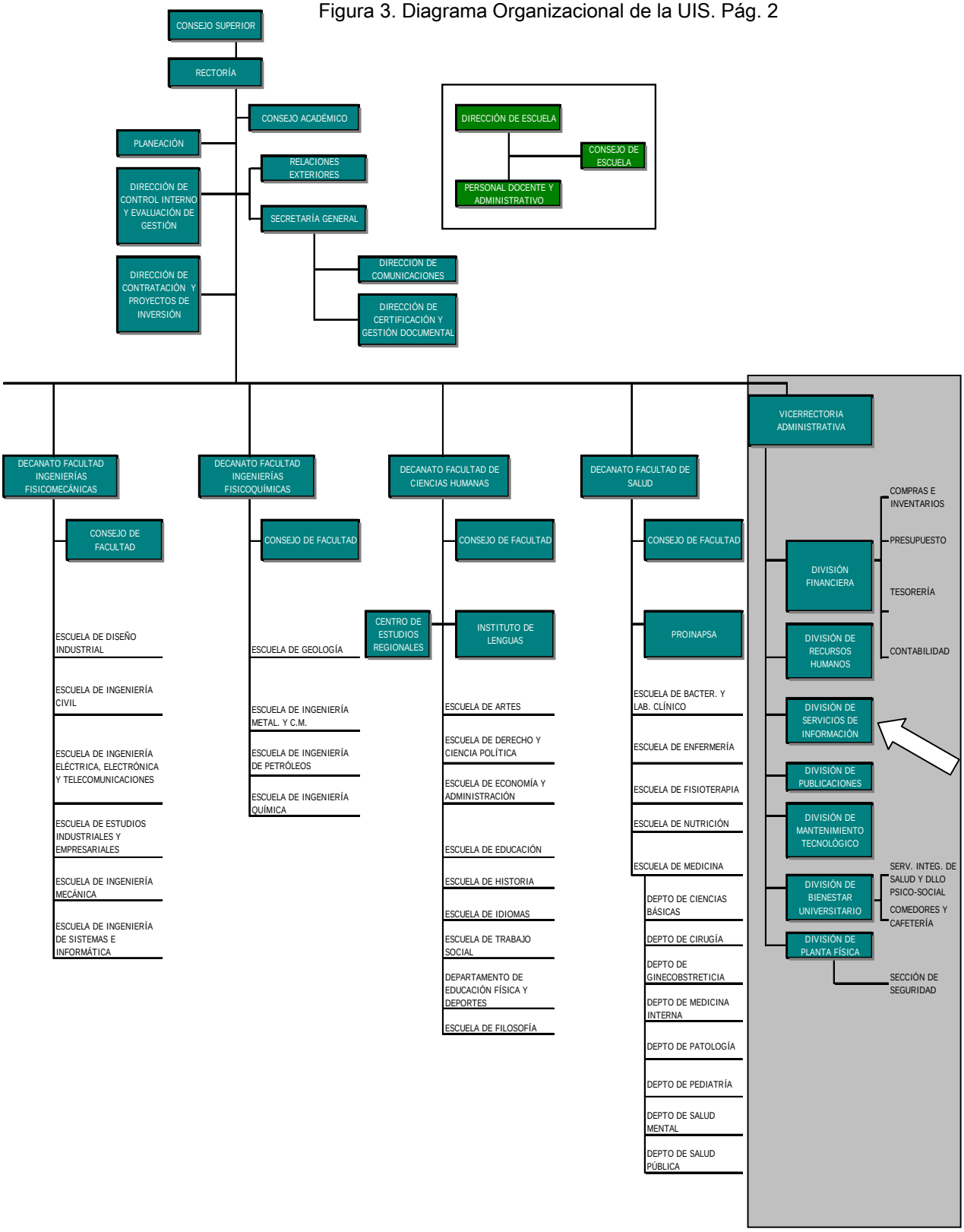
Figura 3 Diagrama organizacional de la UIS. Pág. 1

ACUERDO No. 057 DE 1994 DEL CONSEJO SUPERIOR
ACUERDO No. 041 DE 1997 DEL CONSEJO SUPERIOR
ACUERDO No. 070 DE 1998 DEL CONSEJO SUPERIOR
ACUERDO No. 029 DE 2000 DEL CONSEJO SUPERIOR
ACUERDO No. 073 DE 2001 DEL CONSEJO SUPERIOR
ACUERDO No. 009 DE 2002 DEL CONSEJO SUPERIOR
ACUERDO No. 063 DE 2003 DEL CONSEJO SUPERIOR
ACUERDO No. 073 DE 2003 DEL CONSEJO SUPERIOR
ACUERDO No. 046 DE 2004 DEL CONSEJO SUPERIOR
ACUERDO No. 060 DE 2005 DEL CONSEJO SUPERIOR
ACUERDO No. 070 DE 2005 DEL CONSEJO SUPERIOR
ACUERDO No. 071 DE 2005 DEL CONSEJO SUPERIOR
ACUERDO No. 072 DE 2005 DEL CONSEJO SUPERIOR
ACUERDO No. 073 DE 2005 DEL CONSEJO SUPERIOR



[9] División de Servicios de Información, Universidad Industrial de Santander. Disponible en Internet: https://www.uis.edu.co/portal/administracion/dsi/dsi.html

Figura 3. Diagrama Organizacional de la UIS. Pág. 2



Organizacionalmente la DSI, se divide en dos secciones: El Laboratorio Luis Eduardo Arias y la sección de Tecnología Informática y Comunicaciones que a su vez contiene las áreas de Desarrollo de Software y Soporte de Infraestructura. A está última se encuentra adscrita el área encargada de la "Administración de la red de datos". Ver figura 4.

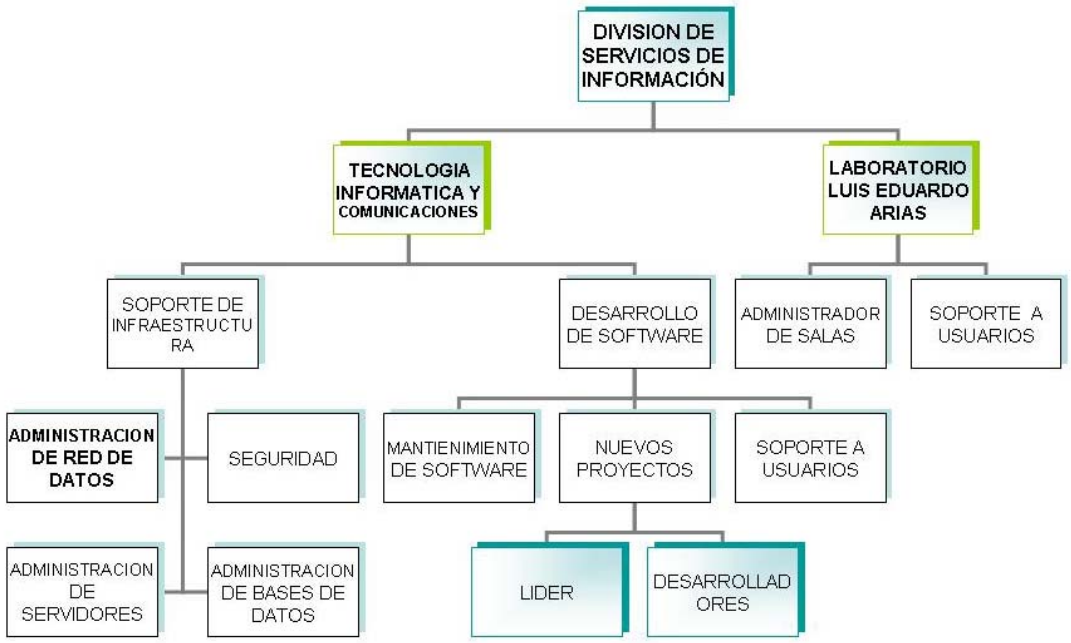


Figura 4. Esquema organizacional de la División de Servicios de Información.

Fuente: Diseño de los autores, con base en información suministrada por la DSI

Tomando como referencia el documento más reciente relativo al esquema de procesos de la DSI[10], esta organización realiza los siguientes procesos:

- Desarrollar, implantar, mantener y administrar sistemas de información.
- Impulsar la Innovación tecnológica.
- Escuchar la voz del cliente interno y externo.

[10] MESA E, ROSAS L y TOBON D. Análisis estratégico para la División de Servicios de Información – DSI de la Universidad Industrial de Santander. Trabajo de grado. Universidad Industrial de Santander 2003.

- Asesorar a las dependencias de la universidad en la adquisición de hardware y software.
- Servicios complementarios, soporte y mantenimiento de microcomputadores y equipos periféricos de la universidad.
- Servicio de correo electrónico.
- *Administrar y mantener la red de datos de la universidad*.

El presente proyecto se concentra en el último proceso "Administrar y mantener la red de datos de la universidad". Particularmente se formula la propuesta de mejora al plan de gestión de red con la definición y descripción de los subprocesos de instalación, monitorización y mantenimiento correctivo, se incluye la elaboración de guías de procedimientos y se propone la utilización del software Solarwinds como herramienta de gestión. Se utiliza la metodología de benchmarking para la indagación y recopilación de las buenas prácticas en el campo de la gestión de red en la UIS y en otras instituciones educativas.

En adelante se mostraran los resultados de la aplicación de dicha metodología.

2.2 APLICACIÓN DE LA METODOLOGÍA DE BECHMARKING

Para formular la propuesta de mejora al plan de gestión de red que se tiene actualmente en la DSI, se aplicó la metodología de Benchmarking. Su aplicación tiene como propósito elaborar una propuesta sólida sustentada en experiencias reales de acuerdo a las prácticas exitosas desarrolladas en cada una de las instituciones seleccionadas y obtener resultados concluyentes que puedan ser reestructurados y aplicados directamente en la DSI. De esta forma se formula una propuesta valedera que genere confianza en la obtención de los mejores resultados y se evitan subjetividades por parte de los autores del proyecto y/o formulaciones inexpertas.

Como primera medida se realizó un benchmarking interno para conocer los actuales estándares y políticas de trabajo dentro del área funcional encargada de la administración de la red de datos en la DSI.

Una vez consolidada la información interna se procedió a realizar un benchmarking funcional en el campo de la gestión de red aplicado a las universidades UNAB, UP y Santo Tomas, las cuales se presumía contaban con redes de datos similares a la UIS. Su propósito era recopilar suficiente información para respaldar y complementar los actuales procesos relacionados con la administración de la red de datos institucional, haciendo énfasis en los subprocesos de instalación, monitorización y mantenimiento correctivo.

El desarrollo de la metodología se describe al momento de presentar los resultados de cada tipo de benchmarking, pues existen algunas variantes entre la aplicación del benchmarking interno y el funcional. A continuación se presenta con detalle cada una de las etapas de la metodología aplicada.

2.2.1 Benchamrking Interno

Se indagaron en primera instancia aspectos generales de la DSI, tales como: esquema organizacional, esquema de procesos, personal implicado en la administración de la red y características generales de la red de datos institucional. En lo relativo a los subprocesos se indagaron aspectos específicos así:

Subproceso de instalación: Se indagó acerca de políticas y procedimientos. En el primer aspecto se preguntó por preferencias hacia algún fabricante de dispositivos e intervención de la administración de la red en la adquisición e instalación de nuevos equipos y servicios de red. En el segundo aspecto se preguntó por la existencia de documentación de soporte, tales como guías de procedimientos, manuales de equipos, existencia de metodologías para las pruebas de

funcionamiento de los dispositivos instalados y en general sobre la forma de ejecución del subproceso de instalación.

Subproceso de monitorización: Se preguntó principalmente por la existencia de una herramienta unificada para la monitorización de la red institucional o en su defecto por las herramientas con las cuales se cuenta actualmente. Se preguntó tambien por los dispositivos y variables que actualmente se monitorizan y por la existencia de acciones de mantenimiento preventivo derivadas de la monitorización.

Subproceso de mantenimiento correctivo: Se indagó en general acerca de la forma como se solucionan los problemas detectados y reportados en la red. Se preguntó por la existencia de un centro de atención al usuario, la existencia de guías de procedimientos y documentos de soporte para el subproceso, la documentación de los incidentes que se presentan con sus soluciones y por la existencia de una metodología para la solución de incidentes.

La ejecución de la metodología de benchmarking a nivel interno se realizó a través de entrevistas, observación de trabajos y recopilación de documentos. Se realizó la entrevista dirigida y personalizada a cada uno de los actores que intervienen directamente en el desarrollo de los subprocesos de instalación, monitorización y mantenimiento correctivo. Se hizo observación directa a los trabajos operativos y se recopiló la documentación interna existente (documentos propios de la DSI e investigaciones y trabajos de grado previos realizados en la DSI) relacionados con la administración de la organización y la gestión de red.

En adelante se presenta los resultados de la metodología aplicada.

2.2.1.1 Áreas funcionales, personal y características de la red.

En la DSI se identificaron dos áreas que están directamente implicadas en la realización de los subprocesos en torno a los cuales gira el presente trabajo de grado: La *Administración y mantenimiento de la red de datos de la universidad* y el *Laboratorio Luis Eduardo Arias – LEA*. Ver figura 4. Cada una cuenta con personal propio, cumplen con funciones específicas diferenciadas y en algunas tareas se complementan. Así, el área de administración de red de datos ejecuta trabajos de diseño, implementación y soporte de los servicios de conectividad mientras que el LEA brinda soporte técnico de escritorio a usuarios. Soluciona problemas de software, hardware y servicios de red en estaciones de trabajo. Los usuarios de acuerdo el tipo de incidente que se les presente acuden a una u otra área. Si acuden al LEA, el personal se desplaza a sitio, diagnóstica el problema y tiene competencia para resolver hasta problemas relacionados con la configuración de red y problemas físicos en la conexión desde el punto de acceso a la terminal. Si el incidente está relacionado con niveles mayores de red (acceso a los cuartos de cableado, configuración de dispositivos, etc.) lo remite al area de administración y mantenimiento de la red. En este sentido estas dos áreas complementan sus trabajos. Además el LEA se encarga de administrar las salas y laboratorios de informática adscritos a la DSI.

El área de *Administración y mantenimiento de la red* está a cargo de un profesional "*administrador de red"* y dos *técnicos de servicios de información.* El LEA está a cargo de un *coordinador* y cuenta con dos *técnicos de servicios de información* para brindar soporte a usuarios. Las denominaciones de los cargos mencionados son propias de la DSI. Las funciones específicas de las áreas funcionales junto con las funciones del personal en los cargos mencionados se detallan en el anexo A.

Así mismo, en la tabla que se muestra a continuación se resumen las características relevantes de la red WAN de la UIS.

Tabla 1. Características generales de la red WAN de la UIS

Topología : Estrella extendida			
Puntos de red habilitados	>2600	Puntos de red en uso	≈2500
Numero de centros de cableado	37	Numero de subredes	71
Numero de equipos activos de red	48Sws 30Hub	Numero de servidores	60

Fuente: Diseño de los autores.

2.2.1.2 Descripción de Subprocesos

A continuación se muestran los aspectos más relevantes de cada subproceso obtenidos con la aplicación de la metodología planteada.

Subproceso de instalación

- Actualmente la DSI no cuenta con herramientas ni políticas de trabajo que permitan llevar a cabo un diagnostico de los equipos de red y faciliten la identificación de fallas o patrones de fallas de hardware o software en los dispositivos activos.

- Por cuestiones de carácter económico no se tiene en cuenta el tiempo de vida útil especificado para los dispositivos activos, excepto para el switch central. Este equipo es de vital importancia para la UIS, por ser el centro de la estrella extendida de la WAN institucional. Por ello demanda mayor cuidado y soporte y en lo posible se respeta su ciclo de vida útil especificado. Además se le realiza mantenimiento periódico. De este modo los equipos activos son reemplazados únicamente por daño o fallas severas que ameriten el cambio del dispositivo.

- Cuando se desea ampliar la infraestructura de la red de datos y esta ampliación amerita la instalación de nuevos dispositivos, el primer paso a realizar por la dependencia o sección interesada, es presentar un proyecto a Planeación donde se justifique dicha necesidad. Para ello, todos los proyectos relacionados con tecnología deben llevar concepto técnico de la DSI. Una vez conseguido el recurso económico y aprobado el proyecto, la dependencia encargada acude a la DSI para recibir asesoría tecnológica. Después de adquiridos los equipos, la dependencia interesada puede contratar los servicios de la DSI para ejecutar todo el proceso de adecuación e instalación del nuevo segmento de red o puede contratarlo con personal externo. En el primer caso la DSI se encarga de dar todo el soporte necesario para llevar a cabo la nueva instalación y puesta en marcha del servicio. En el segundo caso la DSI se limita a realizar la interventoría.

- La adquisición masiva de estaciones de trabajo la realiza directamente la Universidad por medio de subastas públicas aproximadamente cada tres meses. En este proceso no interviene la DSI.

- Actualmente la DSI no permite la instalación de nuevos hubs. En su lugar recomienda instalar solamente switches. Este un requisito que debe cumplirse para dar visto bueno a cualquier proyecto de ampliación de la red.

- Los procedimientos relacionados con el proceso de instalación de dispositivos no se encuentran documentos y se cuenta con muy pocos documentos de soporte.

Subproceso de Monitorización

- Actualmente la DSI realiza una monitorización esporádica de los dispositivos administrables (switches departamentales[11] y switch central) por medio del software propietario de los dispositivos Avaya. Esta herramienta permite la visualización de algunas variables tales como estado de puertos, velocidad, tipo de comunicación full-duplex o semi-duplex, número de la VLAN configurada, entre otros.

- Se realiza monitorización del estado y configuración de los dispositivos activos mediante el acceso remoto por medio del protocolo *telnet*.

- La actuales herramientas de monitorización no permite ejecutar un proceso de mantenimiento preventivo y todos los soportes de mantenimiento se realizan de forma reactiva en respuesta a quejas en la disponibilidad o rendimiento reportadas por los usuarios.

Subproceso de Mantenimiento Correctivo

- El usuario no identifica un único punto en la DSI para reportar quejas relacionas con incidentes en los servicios que soporta la red. En su lugar solicita soporte técnico a la sección encargada de la administración de la red o al LEA dependiendo del tipo de problema. Es decir, el usuario escoge a quien solicitar soporte técnico de acuerdo a su propio juicio valorativo sobre la clasificación y causa del problema.

- Los problemas en estaciones de trabajo relacionados con conectividad, daño, desconfiguración o efecto de virus informático los solucionan los técnicos adscritos al LEA y los problemas de red los solucionan los técnicos adscritos a

[11] Denominación dada a los switches que tienen conexión física directa con el Switch Central y que se ubican en los diferentes edificios del campus universitario. Tambien se les denomina *switches o dispositivos de borde*. Las dos denominaciones se utilizan a lo largo del documento.

la administración de de red. Además tienen la capacidad solucionar problemas de conectividad en estaciones de trabajo.

- Los procesos, procedimientos y actividades relacionados con el mantenimiento preventivo y correctivo no se encuentran documentados y la documentación generada y de soporte es escasa.

- Por medio de fichas los usuarios validan las soluciones de los técnicos adscritos al LEA. Sin embargo las soluciones de los técnicos de la administración de red relacionadas con conectividad no son validadas por el usuario.

- No se lleva registro de las soluciones encontradas ni de los problemas más relevantes relacionados con conectividad.

2.2.2 Benchmarking Funcional

Para la recopilación de información al exterior de la UIS se eligió el benchmarking funcional. Este tipo de estudio permite centrarse en el análisis de los mejores productos, procesos u operaciones desarrolladas en un área funcional específica al interior de otras organizaciones.
Los aspectos que se describen a continuación permitieron aplicar la metodología empleada en el estudio de la situación actual de universidades en lo referente a la Gestión de Red.

- *Procesos Analizados:*

Los subprocesos analizados en cada una de las instituciones fueron instalación, monitorización y mantenimiento correctivo. Estos procesos pertenecen y cumplen un papel importante y primordial dentro de los planes de gestión de red.

Adicionalmente se recopiló información relacionada con los procesos de mantenimiento preventivo, seguridad, atención a usuarios, entre otros que pertenecen a la gestión de red, los cuales permitieron dar una visión más amplia de lo que seria un plan de de gestión de red definido.

- *Universidades Seleccionadas:*

Las Universidades seleccionadas como socios de benchmarking fueron:

- Universidad Autónoma de Bucaramanga – UNAB
- Universidad de Pamplona – U.P
- Universidad Santo Tomas seccional Bucaramanga

Estas Instituciones fueron escogidas teniendo en cuenta el tamaño de su actual infraestructura de red, la evolución que han tenido durante los últimos años, así como por la similitud con la UIS en los servicios que prestan y soportan cada una de sus redes de datos, lo que las convierte en instituciones que deberían poseer planes de gestión de red.

- *Fuentes de información:*

Para la recopilación de información en las instituciones seleccionadas como socios de benchmarking se utilizaron principalmente dos medios.

El primero fue la elaboración de *cuestionarios* con preguntas específicas sobre aspectos como: Ubicación de la sección encargada de la administración de la red de datos dentro del esquema organizativo de la institución, funciones y número de personas a cargo, características generales de la red (número de nodos, características de los dispositivos de backbone y periféricos, fabricantes, servicios que prestan, etc.), existencia de un esquema de procesos, entre otros, que corroboraran la similitud con la red de datos de la UIS y permitieran justificar la existencia de un esquema de gestión de red. Además se plantearon preguntas relacionadas con documentación y la forma como en dichas instituciones se llevan a cabo los subprocesos de instalación, monitorización y mantenimiento correctivo.

El segundo medio utilizado fue el de *entrevistas* con el personal encargado de la administración de la red de datos. Se utilizó con el fin de socializar, corroborar y ampliar la información obtenida a través de los cuestionarios.

- *Información Organizacional:*

En primer lugar se recopiló información acerca de los elementos organizacionales en cada una de las universidades estudiadas que permitiera identificar la dependencia encargada de la administración de la red de datos e indagar acerca de los objetivos y estándares utilizados para llevar a cabo la gestión de red.

En el cuadro 1 se presenta la información más relevante relacionada con aspectos organizacionales y funciones de cada una de las dependencias encargadas de administrar las redes de datos en cada una de las universidades. En los anexos B y C, se encuentra con mayor detalle y en forma ampliada la información recopilada en las Universidades UNAB y U.P.

Cuadro 1. Información organizacional de las Universidades

	UNIVERSIDAD AUTONOMA DE BUCARAMANGA – UNAB	UNIVERSIDAD DE PAMPLONA – UP	UNIVERSIDAD SANTO TOMAS
AREA FUNCIONAL ENCARGADA DE LA ADMINISTRACIÓN DE LA RED	Administración de redes y telecomunicaciones	• Infraestructura • Conectividad	No existe dependencia, solo existe el cargo de administrador de la red de datos.
OBJETIVOS	• Administrar y operar los servidores de aplicativos que operan bajo la Intranet e Internet. • Manejar las políticas de seguridad de la red de datos. • Diseñar, mantener y	• Infraestructura es el Área encargada del despliegue en producción de los desarrollos y administración de la plataforma de hardware, software y la conectividad requerida. • Conectividad es el Área	

	administrar la red de telecomunicaciones. • Cooperar en el diseño de un plan estratégico de desarrollo tecnológico en el área de telecomunicaciones para la UNAB. • Supervisar y mantener la red de voz, datos y vídeo de la UNAB. • Definir estándares para la implantación de redes, cableados e infraestructura de telecomunicaciones.	encargada de desarrollar trabajos de diseño, implementación y mantenimiento de redes de datos.	
DESCRIPCIÓN DEL AREA FUNCIONAL	La Administración de redes y telecomunicaciones es un área de la Coordinación de Infraestructura Tecnológica. Cuenta con tres profesionales (Administrador de red, administrador de servidores y Coordinador) y un estudiante de práctica. Trabajan en conjunto con Helpdesk, sección encargada de recepcionar todas las quejas de los usuarios relacionadas con los servicios de la red, clasificarlas y delegar la solución a quien corresponda.	Las secciones encargadas de administrar la red de datos pertenecen a la dependencia Plataforma Universitaria, que tiene bajo su cargo procesos relacionados con sistemas de información y telecomunicaciones. Infraestructura y conectividad están encargadas de administrar y ejecutar el proceso "diagnóstico, análisis e implementación de servicios de conectividad". Cuentan con 6 profesionales, ingenieros de sistemas y electrónicos. El grupo de trabajo está dividido en dos equipos: Tres personas dedicadas a la monitorización de servidores, asignación de direcciones IP, monitorización de equipos activos de red, Seguridad y	Un profesional, con el cargo de administrador de red se encarga de la gestión de la red institucional. Se encuentra adscrito al Departamento de Sistemas. Administra cuentas de correo, establece políticas de uso, realiza mantenimiento, gestiona seguridad y administra algunos servidores. Los servidores de algunos aplicativos específicos son administrados por otro profesional.

		autenticación, adscritos al área de Infraestructura. Los otros tres profesionales desarrollan trabajos de diseño, implementación y mantenimiento de redes de datos y están adscritos al área de Conectividad.	
DESCRIPCION DEL ESQUEMA DE GESTION DE RED	• *Esquema de gestión de calidad ISO 9001:2000:* Tienen documentados la mayoría de los procesos, procedimientos, instructivos, matriz de clientes, formatos, caracterizaciones y demás. • *Cadena de valor:* Definieron una secuencia global que comprende las etapas de requerimiento, factibilidad, planeación, ejecución, implantación y continuidad del servicio. (Ver. Anexo B). • *Herramientas unificadas para la gestión de red:* No cuentan con una herramienta software unificada para la gestión de red.	• Toda la dependencia Plataforma Universitaria trabaja bajo un esquema de gestión de calidad Institucional. Todos los procesos bajo su cargo se encuentran enmarcados dentro de un mapa de procesos. (Ver Anexo C). • Además la dependencia Plataforma Universitaria maneja un esquema de documentos maestros, para cada sección encargada de los procesos bajo su cargo, en este esquema se definen procesos, procedimientos, políticas y tareas.	No existe un esquema de gestión de red definido. Los procesos y procedimientos de gestión los conoce solamente el administrador de la red y no existe documentación de soporte de los mismos.

- *Información de las características de las redes de datos:*

En el cuadro 2, se muestran las características relevantes de la redes de la universidades estudiadas.

Cuadro 2. Información de las características de las redes de datos de las universidades.

	UNIVERSIDAD AUTONOMA DE BUCARAMANGA – UNAB	UNIVERSIDAD DE PAMPLONA – UP	UNIVERSIDAD SANTO TOMAS
Topología	Estrella extendida	Estrella extendida	Estrella extendida
Puntos de red habilitados	2.552	2500	600
Puntos de red en uso	1500	2500	500
Numero de centros de cableado	49	17	- -
Numero de equipos activos de red	130	120 Sw/Hub	- -
Numero de subredes	22 (lógicas)	6 (Físicas)	20 (lógicas)
Numero de servidores	>15	29	- -

- *Información de los procesos:*

Cuadro 3. Información de los procesos estudiados en las universidades.

	UNIVERSIDAD AUTONOMA DE BUCARAMANGA – UNAB	UNIVERSIDAD DE PAMPLONA – UP	UNIVERSIDAD SANTO TOMAS
Instalación	• Está enmarcado dentro de la cadena de valor definida en el esquema de gestión de calidad de la UNAB. • Solo utilizan dispositivos marca 3com. • Todas las solicitudes de nuevos equipos en la UNAB son canalizadas a través de la sección encargada de la administración de la red, quien se encarga de tramitar la adquisición y realizar la instalación. Una vez instalados se adhieren al inventario de la sección administradora de la red.	• Todos los trabajos de instalación al interior de la universidad los realiza la dependencia de Infraestructura, quienes realizan las pruebas de factibilidad, cotizaciones y la instalación. • Toda solicitud de mantenimiento y nueva instalación de cualquier tipo (conectividad, eléctrica, obra civil, etc.) debe dirigirse a la dependencia Recursos Físicos y Apoyo Logístico. En el caso de conectividad Recursos Físicos y Apoyo Logístico remite la solicitud del usuario a Infraestructura y/o conectividad • Se tiene como política la	• Solo utilizan dispositivos marca Avaya. • El administrador de la red solo emite concepto técnico para la adquisición de nuevos equipos, pero no hace gestión al respecto. • La puesta en marcha y administración de nuevos dispositivos de red los realiza personal interno del departamento de sistemas.

		instalación de solo switches. • Se ofrecen soluciones de conectividad a organizaciones y entidades externas. • Existe documentación de soporte para la realización del subproceso.	
Monitorización	No cuentan con una herramienta software unificada para la gestión de red. Utilizan aplicaciones como: MRTG: Software para monitorizar los enlaces de Internet. Nagios: Software que permite ver el estado de los dispositivos activos de red. Permite generar alarmas vía mail cuando un dispositivo sale de operación. Software propietario de los switches 3com, permite monitorizar el estado y trafico de los puertos de los switches. Software propietario (UNAB) para la monitorización de servidores, permite visualizar el estado de variables como: carga CPU, Nº usuarios, swap. Genera alarmas vía Mail/beeper cuando algún servidor presenta alguna anomalía. Llevan histórico de las variables monitorizadas en los servidores.	• No cuentan con una herramienta software unificada para la gestión de red. Utilizan el software propietario de los dispositivos activos y un software para la monitorización de las antenas. • No se realiza monitorización continua del desempeño y rendimiento de la red. Solo es posible visualizar variables de estado y configuración. • Bajo estas condiciones no es imposible anticiparse a posibles fallas en los dispositivos o enlaces. Se profundiza en un mantenimiento correctivo. • Se realiza mantenimiento preventivo. Cada 6 meses para los equipos activos, así como para las conexiones físicas e inalámbricas. • La documentación generada es escasa, no se tiene un histórico ni clasificación de eventos, tampoco un procedimiento a seguir para el mantenimiento preventivo remoto.	• No cuentan con una herramienta software unificada para la gestión de red. Utilizan el software propietario de los dispositivos Avaya como herramienta de monitorización. No cuentan con ningún otro software para tal fin.
Mantenimiento Correctivo	• *Helpdesk:* Esta sección se encarga de recepcionar todas las solicitudes de los usuarios y delegar la solución a quien	• La Dependencia Recursos Físicos y Apoyo Logístico también se encarga de canalizar las solicitudes de los usuarios referentes a cualquier	• *Atención a usuarios*: La realiza el departamento de sistemas. Se encarga de atender y resolver los problemas de red y

	corresponda, siendo Helpdesk el encargado de solucionar los problemas de estaciones finales e Infraestructura tecnológica la encargada de solucionar los problemas de red. • *Software de registro:* Usan el software libre - EXO PHP- para registrar las actividades de mantenimiento correctivo. Se registran todos los pasos y personas que intervienen desde el momento de la solicitud del usuario hasta la solución final. Se registra el tipo de problema, el encargado de solucionarlo y los comentarios de quienes participaron en la solución.	tipo de problema, incluyendo solicitudes con respecto a inconvenientes en el servicio de red. • Se abre un caso con la solicitud y se remite a la dependencia o personal encargado de solucionar este tipo de inconvenientes. • Finalizado el trabajo el usuario valida la solución y se diligencia una ficha de trabajo, se consigna la fecha de solicitud, de culminación, responsable de la solución, solicitante y se califica el trabajo realizado. • Los trabajos son realizados con base en la experiencia de los Ingenieros y no cuentan con guías de procedimientos. La documentación generada es escasa. Sin embargo existen documentos de soportes de ciertos procedimientos relacionados con el soporte a usuarios. • No se lleva registro de las soluciones encontradas en los problemas más relevantes relacionados con conectividad.	equipos terminales. • No existe un procedimiento definido para la atención a problemas en los servicios de la red. Cada problema se afronta utilizando la experiencia y presaberes de la persona encargada de su solución. • Por experiencia se tienen identificados los principales problemas en los servicios de la red de datos, pero no se genera documentación al respecto.

ANÁLISIS COMPARATIVO DE LOS ESQUEMAS DE GESTIÓN DE RED EN LAS DIFERENTES UNIVERSIDADES

Cuadro 4. Análisis comparativo de los esquemas de gestión de red en las diferentes Universidades.

	UNIVERSIDSAD INDUSTRIAL DE SANTANDER - UIS	UNIVERSIDAD AUTONOMA DE BUCARAMANGA – UNAB	UNIVERSIDAD DE PAMPLONA – UP	UNIVERSIDAD SANTO TOMAS
¿Existe una área encargada de la administración de la red de datos?	Administración red de datos.	Administración de redes y telecomunicaciones.	• Infraestructura. • Conectividad.	NO
Número de personas dedicadas a la administración de la red.	1 profesional y 5 técnicos	3 Profesionales y 1 estudiante de práctica.	6 ingenieros de sistemas y electrónicos.	1 Profesional
Se rigen por un esquema de gestión específico.	NO	Gestión de Calidad ISO 9001:2000	Esquema de gestión de calidad Institucional.	NO
Existe una dependencia que centralice las solicitudes de los usuarios?	NO Existen dos: LEA, Administración red de datos.	SI Helpdesk	SI Recursos Físicos y Apoyo Logístico	SI El departamento de Sistemas.
Cuentan con guías de procedimientos	NO	SI Para algunos procedimientos	No Los trabajos se realizan con base en la experiencia de los Ingenieros	NO
Están definidos los procesos de instalación, monitorización y mantenimiento correctivo.	NO	SI – Instalación NO – Monitorización y mantenimiento correctivo. No se encontró evidencia de la definición de estos procesos.	Si y No La instalación se encuentra definida dentro del listado maestro de documentos que contiene los procedimientos, guías, instructivos,	NO

			protocolos a seguir. El proceso de mantenimiento correctivo cuenta con escasa documentación. El proceso de monitorización no cuenta con documentación de soporte.	
Generan documentación sobre los problemas que se presentan en la red y sus soluciones.	NO Solo se validan las soluciones de los técnicos adscritos al LEA mediante fichas de trabajo.	SI Utilizan un software con acceso vía Web para el registro de los eventos.	No Solo se validan las soluciones mediante fichas de trabajo.	NO
Se lleva un registro histórico del desempeño de la red LAN.	NO	SI Registran datos históricos de la monitorización de enlaces a Internet y servidores.	NO Solo es posible visualizar variables de estado y configuración.	NO
Existe una base de conocimiento documentada sobre los problemas que se presentan en la red?	NO	SI – Pero no hacen análisis de la información recopilada.	NO	NO
Existe una herramienta de gestión unificada	NO Herramientas software propietarias.	NO Cuentan con diversas herramientas de monitorización.	NO Herramientas software propietarias.	NO
La instalación de nuevos dispositivos o puntos de red los	NO El usuario puede o no solicitar de los servicios de	SI	SI Toda instalación la administra y realiza el personal	NO

canaliza y controla la dependencia administradora de la red?	nuevas Instalación a la DSI. Es posible solicitar asesoría externa.		de Infraestructura.	
Cuentan con un sistema de información donde se recopile el inventario físico y lógico de la red, datos históricos de monitorización y demás información que genere la administración de la red.	NO No existe un sistema de información completo. Poseen un sistema de información para el inventario lógico y físico.	NO No existe un sistema de información completo. Solamente guardan datos de monitorización. No se encontró evidencia de un sistema de información para el inventario físico y lógico.	NO Sistemas de información no centralizados.	NO
¿Se tiene preferencia por algún fabricante de dispositivos – marca?	SI Avaya	SI 3Com	SI 3com	SI Avaya

2.3 ANÁLISIS COMPARATIVO DE LA INFORMACIÓN RECOPILADA

Dado que la información de las instituciones similares a la UIS se recopiló utilizando la metodología de Benchmarking, las ideas que se consignan en adelante corresponden a las *mejores prácticas* identificadas. La exposición se hará basada en los puntos tratados en el cuadro comparativo anterior.

- Se reconoce la administración de las redes de datos como un elemento importante para el cumplimiento de las metas institucionales, prueba de ello es que en tres de las cuatro universidades indagadas, existen áreas funcionales específicas, con personal calificado dedicadas a esta labor.

- El tamaño de la infraestructura de las redes de datos de las universidades indagadas es comparable con el tamaño de la red de datos de la UIS, con excepción de la red de la Universidad Santo Tomas, la cual es aproximadamente cinco veces menor.
- Se encontró que el tamaño de las redes de datos está directamente relacionado con la adopción e implementación de planes de gestión de red. En este sentido las universidades UNAB y de Pamplona tienen implementados sus planes de gestión de red basados en el sistema de gestión de la calidad ISO 9001:2000 y en un sistema institucional respectivamente. En la UIS y la Universidad Santo Tomás no se encontró evidencia de planes de gestión con estructuras similares.
- Se identificó que la documentación de soporte para los procesos y procedimientos relacionados con la administración de la red de datos existe solamente en las universidades que han acogido algún sistema de gestión de la calidad (UNAB y Universidad de Pamplona). En las dos se encontró evidencia de documentación para el proceso de instalación. De igual forma solo en estas universidades se genera algún tipo de documentación durante y después de la atención a solicitudes de los usuarios. En la UNAB se tiene un software para el registro de incidentes y en la universidad de Pamplona se registran las soluciones de forma manual en formatos preestablecidos.
- Se evidenció la importancia de contar con dispositivos activos de una sola marca. En todas las instituciones indagadas se tiene esta política, entre otros, porque facilita la administración de la red, se unifica la configuración de dispositivos y se solicita soporte a un solo fabricante. No obstante, la aplicación de dicha política es más efectiva en la UNAB, Universidad de Pamplona y Santo Tomás ya que en estas instituciones las solicitudes de nuevos dispositivos se canaliza en su totalidad a través del área encargada de la administración de la red. Caso distinto ocurre en la UIS donde existe mayor autonomía para las distintas dependencias universitarias para hacer sus adquisiciones, remitiéndose a la administración de la red solamente para solicitar concepto técnico.

- Se identificó la existencia de un único centro de atención al usuario que recepciona todas las quejas relacionas con incidentes y problemas en los servicios que presta la red de datos. Este centro de atención clasifica los problemas reportados y delega la solución a quien corresponda. De esta forma se evita que el usuario tenga que recurrir a diferentes dependencias a buscar la persona idónea para resolver su problema. Esto se evidenció en la UNAB y la Universidad de Pamplona.
- En todas las instituciones indagadas, se evidenció la ausencia de una herramienta unificada para la gestión de dispositivos. Cada una cuenta con tres o más herramientas diferentes para la monitorización y administración de enlaces y dispositivos.

2.4 LA GESTIÓN DE RED EN EL ENTORNO EMPRESARIAL DE LAS TI

Además de la información que se recopiló por medio del benchmarking funcional en instituciones similares a la UIS se realizó una entrevista al ingeniero Juan Carlos Contreras quien labora en la empresa EMTELCO S.A. especializada en ofrecer servicios de telecomunicaciones. La información suministrada por el ingeniero, la proporcionó a titulo personal y producto de su experiencia laboral en dicha compañía.

Esta entrevista permitió tener una visión más amplia de lo que significa un esquema de gestión de red estructurado y totalmente implementado por una empresa dedicada.

Las conclusiones de la entrevista fueron:

- Las empresas que prestan servicios de telecomunicaciones deben implantar modelos de gestión.

- La gestión no solo se enfoca a la parte operativa, cada área que pertenezca y cumpla un objetivo dentro de la organización (área financiera, área comercial, área administrativa, etc.) debe desempeñar un papel interactivo dentro de un modelo global, denominado modelo de gestión de negocio.

- Existen modelos de gestión de negocio ampliamente implementados en la industria de las TI (Tecnologías de la información). Uno de ellos es eTOM (Enhancement Telecomunication Operation Management). Estos modelos incluyen todas las áreas de la organización y describen la interacción entre ellas.

- Existen recomendaciones encargadas de manejar la parte operativa y de prestación de servicios como ITIL (Technology Infrastructure Library). Este indica que: "La correcta Gestión de Servicios de TI se basa en la coordinación eficiente de las tres "P": personas, procesos y producto - ITIL". El modelo ITIL corresponde a las *Mejores Prácticas para la Gestión de Servicios de TI.* Actualmente este modelo se incluye dentro de la norma ISO 20000.

- ITIL y eTOM son complementarios, uno cubre la parte operativa y servicios y el otro la parte de negocio. En el modelo eTOM se visualiza la interacción de cada una de los áreas y los objetivos de cada una de ellas, entre estas se incluyen las áreas operativa y de servicios definidas por ITIL.

- Según eTOM e ITIL, las empresas deberían implementar un esquema general de los procesos que llevan a cabo (framework[12]).

- La DSI puede ser vista como una empresa que presta un servicio de telecomunicaciones que depende de las TI para cumplir sus objetivos. De esta

[12] Framework: Palabra del idioma Inglés que traducido al español significa marco de procesos

forma estos modelos de gestión aplican y pueden ser directamente implantados en una organización de este tipo.

- Otro aspecto de vital importancia para la empresas que prestan servicios de telecomunicaciones es definir y tener un punto único de atención al usuario (Call Center, Contact Center o CSC – Centro de servicio al cliente). Este se encarga de recibir las quejas y solicitudes de los usuarios, hacer el escalamiento de un problema, falla o deficiencia en el servicio, e intentar una solución remota después de priorizar cada una de las solicitudes (se definen matrices de priorización), de acuerdo al tipo de problema.

- En la atención de solicitudes remotas y en sitio, se ejecutan listas de chequeo que ayudan en la búsqueda de la solución de inconvenientes reportados o identificados en el servicio. Estas permiten agilizar los tiempos de respuesta del personal y con ellas se documentan los incidentes, problemas y soluciones encontradas.

- Es necesario implementar y alimentar una base de conocimiento concebida producto de la experiencia donde se consignen los problemas reportados y detectados con sus soluciones. El análisis estadístico de la información de la base de conocimiento permitirá conocer el comportamiento de la red administrada, establecer condiciones para priorizar la atención de solicitudes, retroalimentar las listas de chequeo, tomar decisiones proactivas, adquirir una experiencia tangible, entre otras.

- Es importante contar con un sistema de información centralizado y sistematizado donde se documente y administre cada uno de los procesos definidos. En principio este sistema se puede implementar con formatos, documentos, plantillas, fichas etc. que se llenen en forma manual. Una vez se tengan todos los procesos definidos se puede pasar a la etapa de

sistematización de la información. La base de conocimiento hace parte del sistema de información.

Con las conclusiones obtenidas de la entrevista con el ingeniero de Emtelco S.A junto con las mejores prácticas identificadas en las distintas universidades, producto de la aplicación de la metodología de benchmarking, se procede a formular la propuesta de mejora al plan de gestión de red de la UIS en el siguiente capítulo.

3. FORMULACIÓN DE LA PROPUESTA DE MEJORA AL PLAN DE GESTIÓN DE RED INSTITUCIONAL

El desarrollo de la metodología de Benchmarking aportó ideas significativas para la formulación de la propuesta de mejora al plan de gestión de red institucional. La identificación de las mejores prácticas que actualmente arrojan buenos resultados en instituciones similares a la UIS y en empresas dedicadas del sector, es la base del planteamiento que se va a presentar.

Los subprocesos en torno a los cuales gira el presente trabajo se enmarcan dentro de las áreas de gestión de desempeño y configuración, además de abarcar la gestión de los servicios. Sin embargo es importante destacar que para garantizar un servicio adecuado se debe identificar y documentar todos los subprocesos involucrados en el área funcional de gestión de red. Entre ellos la gestión de seguridad es de gran importancia.

En el presente capítulo, se muestra en primera instancia los aspectos en los que impacta la implantación estructurada de un plan de gestión de red institucional. Se continúa con la presentación de las pautas a seguir a nivel organizacional, técnico y tecnológico para la formulación de la propuesta de mejora al plan de gestión y al final se describe de forma detallada la formulación de cada uno de los subprocesos.

3.1 IMPACTO DE LA IMPLANTACIÓN DE UN PLAN DE GESTIÓN DE RED

Con base en la experiencia transmitida por las instituciones y personas que aportaron en la realización de este proyecto se puede concluir que un plan de

gestión de red impacta positivamente a una institución como la UIS, entre otros, en los siguientes aspectos:

- *Rápida y oportuna toma de decisiones*: Contar con un plan de gestión de red estructurado, implica contar con información organizada, estructurada, centralizada y articulada. Documentar los procesos que realiza una organización da uniformidad a la forma de ejecución independientemente de las personas involucradas. Documentar los incidentes reportados en el servicio, permite identificar grupos de problemas con patrones similares de solución. Documentar los aciertos y errores en la solución de los problemas, permite aprender de las experiencias pasadas y se pasa de tener un conocimiento que solo está en la mente de quien realiza los procedimientos a una expresión tangible de la forma como se hacen las cosas. Este tipo de documentación coherente y razonable ayudará a facilitar la toma de decisiones. Una decisión puede ser algo tan simple como determinar la necesidad de realizar un mantenimiento preventivo o algo más trascendental como determinar si se debe migrar a otra tecnología, expandir la red, cambiar de fabricante, el tipo de equipos, etc. Además, un plan de gestión permite hacer proyecciones y determinar los aspectos en los que se puede mejorar. Permite tener certeza sobre las capacidades de la red. Por ejemplo si se va ofrecer un nuevo servicio (p.e. matriculas vía Web) se puede determinar si se es capaz de proveer en las actuales condiciones o se puede llegar a saber qué problemas se presentarán al ofrecerlo. Con ello se puede recomendar postergar el lanzamiento del servicio, implementar un plan de acción que corrija los problemas identificados o en su defecto un plan de contingencia para atender las eventualidades.

- *Disminución de los tiempos de respuesta en la solución de problemas*: La implantación de un plan de gestión de red, hace que los mantenimientos preventivos y correctivos se lleguen a realizar con rapidez. Las herramientas de monitorización permiten aislar e identificar más fácilmente un problema, tal que cuando se envía una persona a sitio, ya se sabe exactamente o con muy poca

incertidumbre cual es la falla y dónde se debe resolver. Además permite en muchos casos, encontrar una solución remota desde la estación gestora. Esto hace que la organización preste un mejor servicio y se haga más eficiente en la solución de problemas. También permite enfocarse hacia la ejecución de acciones proactivas en remplaza de las acciones reactivas.

- *Impacto a nivel económico*: Al analizar más a fondo el impacto de la implantación de un plan de gestión de red, se evidencian beneficios a nivel económico. Optimizar tiempo está directamente relacionado con ahorro de dinero. Escoger los mejores equipos, en contraste con unos que pueden deteriorarse rápidamente implica evitar sobrecostos. Optimizar la red de modo que se puedan ofrecer mayores servicios en línea, reduce los costos operativos de una organización, porque se evitan gastos en papelería, pago de salarios y todo los gastos que implica contratar personal, entre otros. Para la UIS por ejemplo, llegar a prestar un servicio de videoconferencia en todas las sedes a la vez, donde se ofrezca una clase desde el campus central sería un ahorro considerable, si se tiene en cuenta que se evitan desplazamientos y la contratación de más personal.

  A los beneficios citados anteriormente se pueden agregar el control que se tiene sobre los recursos y servicios de la red y la forma de aprovecharlos, además de mejorar el rendimiento, disponibilidad y seguridad de la red de datos.

3.2 PAUTAS PARA LA FORMULACIÓN DE LA PROPUESTA DE MEJORA

Las ideas sobre las que se basa la propuesta de mejora al plan de gestión de red institucional se muestran a continuación. Estas se dividen en dos grupos diferenciados: Uno organizacional y otro tecnológico. En el primero se indican los componentes que incluyen la definición de los subprocesos de instalación, monitorización y mantenimiento correctivo y la forma estos se enmarcan dentro de

la DSI. En el segundo se indican las pautas a nivel técnico y tecnológico, a partir de las cuales se van a definir dichos subprocesos.

Componente Organizacional

- Se asume la administración de la red de datos institucional como un ***proceso*** que realiza la DSI y se identifica la *instalación, monitorización y mantenimiento correctivo* como ***subprocesos*** incluidos dentro de la administración de red. Esto implica, definir y documentar los subprocesos en formatos estándar donde se muestren sus objetivos, características inherentes, diagrama de actividades que los componen con su respectiva descripción, guía de procedimientos, etc. Por esta razón se plantea la utilización de plantillas para su definición y descripción.
- La definición y descripción de dichos procesos y subprocesos apunta hacia la futura elaboración de un *manual operativo* para la DSI, donde se estructuren todos los procesos y subprocesos que realiza. Este manual servirá de soporte para la estandarización de las operaciones, facilitara la realización de cada uno de los procesos y dará uniformidad a las actividades que realiza la organización. Con esto se aportan los primeros pasos para la implantación de un sistema de gestión de calidad dentro de la DSI.
- El diagrama de actividades de cada subproceso planteado esta acompañado por su respectivo documento de soporte. En este se describe la forma de realizar cada una de las actividades, constituyéndose en las guías de procedimientos para el personal que ejecuta cada uno de los procesos.

Componente técnico y tecnológico:

- Se plantea la definición y elaboración de listas de chequeo que se incluyen dentro de las guías de procedimientos de los subprocesos de instalación y mantenimiento correctivo. Las listas de chequeo tienen como objetivo verificar y proporcionar información para crear y alimentar una base de conocimiento

tangible, que permita agilizar los tiempos de respuesta del personal, documentar los incidentes, problemas y soluciones encontradas, elaborar y retroalimentar matrices de priorización para la atención de solicitudes, tomar decisiones proactivas y adquirir una experiencia tangible, entre otras.

- El *subproceso de instalación* apunta hacia la instalación de dispositivos activos de red administrables. Se describe desde el momento de la configuración de los equipos, para ello se plantea una guía básica de configuración que permita agilizar lo mayor posible la instalación de nuevos dispositivos y pueda ser realizado por cualquier persona que labore en la administración de la red. Además se plantean actividades de revisión de normatividad y pruebas de conectividad y configuración.
- En el *subproceso de monitorización* se plantea la utilización de una herramienta software de gestión unificada que permita realizar una administración centralizada de los recursos de la red. Esta herramienta permite, entre otras cosas, controlar el inventario de dispositivos, administrar direcciones IP, monitorizar del estado y utilización de los enlaces, monitorizar el nivel de procesamiento de la CPU de los dispositivos, monitorizar servidores, monitorizar cualquier variable de la MIB de los dispositivos, etc.
- El *subproceso de mantenimiento correctivo* se centra en tres aspectos: recepción de solicitudes, solución a los incidentes/problemas reportados y documentación antes y postsolución de problemas en la red. Para la recepción de solicitudes se plantea la existencia de un único centro de atención al usuario que identifique a la DSI. Este lugar será el único reconocido por la comunidad universitaria para remitir allí sus quejas relacionadas con los servicios que soporta la red de datos. Una vez recibida una queja, la persona que atiende la llamada, intenta en primer lugar, encontrar una solución en forma remota por medio de la ejecución de una lista de chequeo. Si esta lista de chequeo no termina con una solución, al menos debe terminar con la identificación del problema y el lugar donde ocurre con la menor incertidumbre posible, con el fin de que cuando se envíe una persona a campo acuda al lugar correcto y solucione el problema lo más rápido posible. El centro de atención al usuario se

encarga de clasificar el problema y remitir la solución a quien corresponda. Además emite una orden de trabajo e inicia la documentación del reporte de dicho problema para lo cual se utiliza el *formato de mantenimiento correctivo* (Ver anexo G). Durante la solución y una vez solucionado el problema se debe documentar lo que se hizo paso a paso, las personas que intervinieron, el tiempo de ejecución, el tipo de problema, el lugar donde ocurrió, etc. con el fin de crear y alimentar una base de conocimiento que permita a mediano plazo identificar grupos de problemas con sus soluciones, dimensionar las capacidades de la red con base en datos reales y contribuir a la rápida toma de decisiones. El planteamiento del subproceso de mantenimiento correctivo busca que se reporten cada vez menos problemas y que se solucionen de forma cada vez más rápida.

Bajo estas consideraciones, en adelante se presenta la propuesta para cada subproceso que contiene la descripción general del subproceso, formulación de objetivos, el diagrama de interacción de sus actividades y la guía de procedimientos.

3.3 SUBPROCESO DE INSTALACIÓN

La propuesta se enfoca principalmente a dispositivos activos de red de segundo nivel (switches departamentales), particularmente la familia de switches Avaya P33x, con los que actualmente cuenta la UIS, por ser estos los equipos activos predominantes. Además estos dispositivos son administrables y son primordiales para la interconexión de los diferentes edificios de la Institución por lo que ameritan mayor administración y cuidado.

Salvedades

Los dispositivos de red pasivos (hubs), no se consideran directamente dentro del subproceso de instalación de equipos de red, debido a que son simples

concentradores de conexiones y no necesitan de ningún tipo de configuración. Sin embargo dentro del esquema general del subproceso planteado (Ver figura 5.) es posible incluir la instalación de estos dispositivos omitiendo los pasos particulares de dispositivos activos, con lo que se ejecutaría el estudio de normatividad, la instalación en sitio del equipo y la actualización del sistema de información.

Los switches de tercer nivel tampoco son considerados directamente dentro del proceso de instalación de equipos de red ya que su configuración es simple y sencilla de realizar, sin embargo el subproceso general se adapta a las particularidades de estos dispositivos sin importar su marca y configuración. Además no todos estos dispositivos están bajo la administración de la DSI.

Los routers no son considerados dentro del proceso de instalación de equipos de red, debido a que en la UIS, aunque se cuenta con dos dispositivos, estos son propiedad de los proveedores con los que se tiene contratado el servicio de Internet y la administración de estos equipos esta bajo la responsabilidad de cada uno de los proveedores.

Descripción de la propuesta

El proceso de instalación se describe desde el momento de la configuración de los dispositivos, pasando por un análisis básico de la normatividad de los cuartos de cableado, hasta la realización de pruebas y puesta en marcha del dispositivo.

Como primera recomendación, se plantea la utilización de un archivo básico de configuración que permita agilizar y facilitar la configuración de los switches, este se encuentra debidamente documentado y contiene los parámetros básicos de configuración actual de los switches departamentales para permitir la comunicación al interior y exterior de la Universidad, además se configuran elementos de administración que permitirán llevar a cabo el proceso de

monitorización desde la estación gestora para tener control y supervisión sobre estos dispositivos y el rendimiento de la red.

Una vez las tareas de configuración son realizadas, se procede a realizar el análisis de la normatividad del cuarto de cableado donde se va a ubicar el dispositivo. Este análisis corresponde a una revisión general de la norma para las distancias de los patch cord, ubicación y estado del cuarto de cableado. En esta parte se busca que se respeten las recomendaciones internacionales y más que cumplir con todas y cada una de las normas se busca no degradarlas, por esta razón se realiza una revisión básica.

Terminada la tarea de analizar la normatividad en el cuarto de cableado se procede a la instalación del dispositivo, las tareas a ejecutar en esta instancia del proceso corresponden a realizar las conexiones correspondientes y realizar las pruebas de conectividad y funcionamiento del dispositivo, para ello se plantea una primera lista de chequeo que permita verificar rápidamente el correcto funcionamiento del dispositivo.
En caso de tener problemas de conectividad se plantea una segunda lista de chequeo, que corresponde a pruebas generales de conectividad y revisión de la configuración actual del equipo.
Estas listas de chequeo siguen un orden específico, producto de recomendaciones extraídas de las experiencias estudiadas mediante la metodología de benchmarking y de recomendaciones de empresas dedicadas como Cisco. Ver anexo H

Por último se plantea realizar las tareas de documentación del trabajo ejecutado, alimentar el sistema de información con los datos correspondientes al inventario lógico y físico de la nueva instalación y realizar una copia de seguridad (backup) de la configuración actual para los switches departamentales, con el fin de poseer un respaldo que permita restaurar el servicio de forma rápida cuando se presente alguna eventualidad con alguno de estos dispositivos.

La plantilla general para la descripción del subproceso de instalación de dispositivos de red y el esquema general de actividades para su ejecución se muestra se muestra en las figuras 5 y 6 respectivamente. El esquema de la lista de chequeo para el análisis de normatividad, análisis de conectividad y para la revisión de conexiones y configuración se muestra en la Figura 7.

Además las guías de procedimientos donde se describe la ejecución de cada una de las actividades planteadas para el subproceso de instalación de equipos de red se encuentran en el anexo E. Allí se incluye el instructivo de la lista de chequeo.

Figura 5. Plantilla principal del subproceso de Instalación.

UNIVERSIDAD INDUSTRIAL DE SANTANDER	PRESENTACIÓN DEL SUBPROCESO	
	Administración y mantenimiento de la Red de Datos Institucional	
MANUAL OPERATIVO DIVISIÓN DE SERVICIOS DE INFORMACIÓN	INSTALACIÓN DE DISPOSITIVOS RED	Código : SIA.01.01

Elaboró:	Revisó:	Aprobó:	Fecha de creación :	Última Modificación:
Sergio Contreras-Edgar Macias	Ing. Maria F. Reyes S.	Ing. Benjamín Pico M.	Marzo 1 de 2006	

OBJETIVO DEL SUBPROCESO

Configurar los dispositivos de red y ponerlos en funcionamiento para ofrecer los servicios soportados por la red de datos institucional.

CARACTERÍSTICAS DEL SUBPROCESO

Aplicabilidad: Unidades académico – administrativas de la UIS
Periodicidad: Esporádico
Dependencia Tecnológica: Semiautomatizado.

PROVEEDORES	INSUMOS	RESULTADO
Jefe de la DSI Administrador de la red de datos (DSI). Técnicos de servicios de información DSI.	Herramientas de software (software de gestión, software de emulación de terminal) Herramientas de Hardware. (PC, Laptop, Patch Cords, cable de consola) Manuales propios de los equipos de red. Documentación existente (inventario lógico y físico de la red)	Puesta en funcionamiento de los dispositivos de red. Actualización del inventario físico y lógico de la red

CLIENTES		SUBPROCESOS RELACIONADOS
INTERNOS	EXTERNOS	
Personal encargado de la administración de la red.	Unidades académico – administrativas	

Figura 6. Plantilla principal del subproceso de Instalación – Diagrama de actividades

UNIVERSIDAD INDUSTRIAL DE SANTANDER	Administración y mantenimiento de la Red de Datos Institucional	MANUAL OPERATIVO DIVISIÓN DE SERVICIOS DE INFORMACIÓN	
	INSTALACIÓN DE DISPOSITIVOS DE RED	Código: SIA.01.01	Hoja 1 de 1
Elaboró : Sergio Contreras-Edgar Macias		Fecha de creación :	Marzo 1 de 2006
Revisó : Ing. Maria F. Reyes. S		Última Modificación :	
Aprobó : Ing. Benjamín Pico M.			

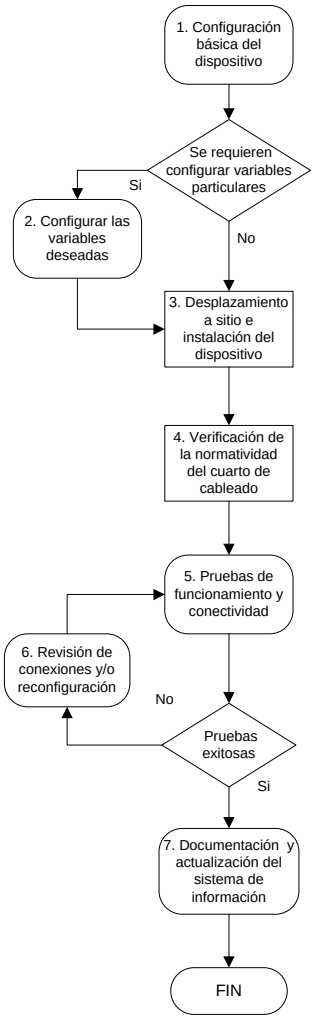
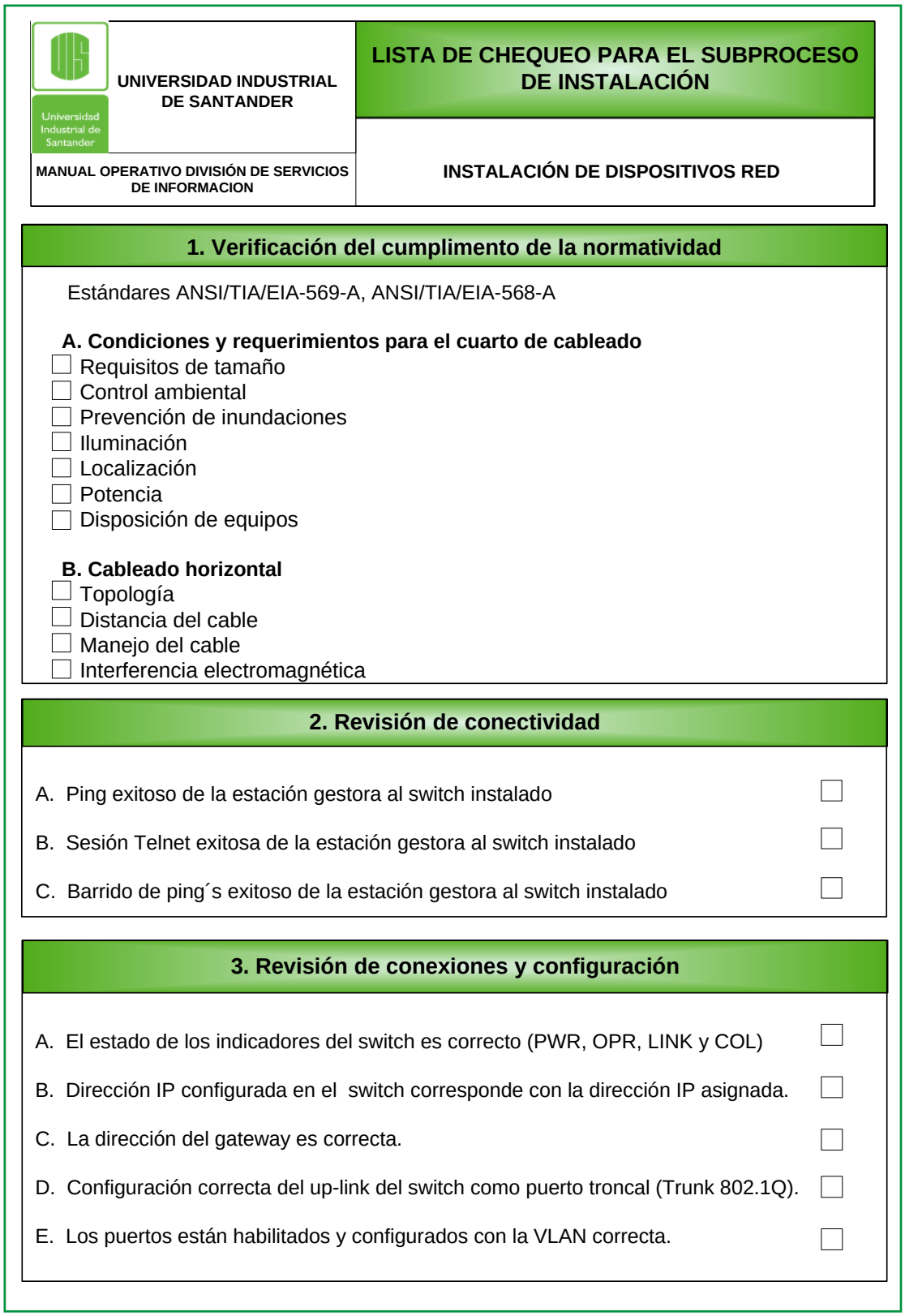
DIAGRAMA	DESCRIPCIÓN	RESPONSABLE	NORMATIVIDAD
	1. Se carga el archivo de configuración básico con los parámetros específicos del nuevo dispositivo (dirección IP, VLAN`s, Ubicación, etc) 2. Si es necesario configurar parámetros que no se encuentran en el archivo de configuración básico, consultar el manual de configuración y realizar los ajustes necesarios. 3. Con el dispositivo ya configurado desplazarse al cuarto de cableado respectivo e instalar el dispositivo en el rack correspondiente y realizar las conexiones necesarias para la puesta en marcha del dispositivo. 4. Se verifican el cumplimiento de las normas básicas del cuarto de cableado según la norma ANSI/TIA/EIA-569-A, ANSI/ TIA/EIA-568-A. 5. Se realizan las respectivas pruebas de conectividad desde y hacia el nuevo dispositivos de red, así como con los equipos directamente conectados. 6. Si la conectividad es nula se realiza una revisión de conexiones y de la configuración actual. Si es necesario se debe reconfigurar el dispositivo. 7. Se documenta la nueva instalación y si es necesario se actualiza el inventario lógico de la red de datos, para ello se introducen los nuevos datos en el sistema de información.	Administrador de red Administrador de red Equipo de técnicos de información Equipo de técnicos de información, Administrador de red Equipo de técnicos de información y/o Administrador de red Equipo de técnicos de información Equipo de técnicos de información	Norma ANSI/TIA/ EIA-569-A, ANSI/ TIA/EIA-568-A.

Figura 7. Plantilla para la lista de chequeo del subproceso de instalación.



UNIVERSIDAD INDUSTRIAL DE SANTANDER	LISTA DE CHEQUEO PARA EL SUBPROCESO DE INSTALACIÓN
MANUAL OPERATIVO DIVISIÓN DE SERVICIOS DE INFORMACION	INSTALACIÓN DE DISPOSITIVOS RED

1. Verificación del cumplimento de la normatividad

Estándares ANSI/TIA/EIA-569-A, ANSI/TIA/EIA-568-A

A. Condiciones y requerimientos para el cuarto de cableado

- ☐ Requisitos de tamaño
- ☐ Control ambiental
- ☐ Prevención de inundaciones
- ☐ Iluminación
- ☐ Localización
- ☐ Potencia
- ☐ Disposición de equipos

B. Cableado horizontal

- ☐ Topología
- ☐ Distancia del cable
- ☐ Manejo del cable
- ☐ Interferencia electromagnética

2. Revisión de conectividad

A. Ping exitoso de la estación gestora al switch instalado ☐

B. Sesión Telnet exitosa de la estación gestora al switch instalado ☐

C. Barrido de ping´s exitoso de la estación gestora al switch instalado ☐

3. Revisión de conexiones y configuración

A. El estado de los indicadores del switch es correcto (PWR, OPR, LINK y COL) ☐

B. Dirección IP configurada en el switch corresponde con la dirección IP asignada. ☐

C. La dirección del gateway es correcta. ☐

D. Configuración correcta del up-link del switch como puerto troncal (Trunk 802.1Q). ☐

E. Los puertos están habilitados y configurados con la VLAN correcta. ☐

3.4 SUBPROCESO DE MONITORIZACIÓN

Como continuación al trabajo de investigación de “GUZMAN CASTILLO PAOLA F”[5] se propone la utilización de la herramienta de gestión de red SolarWinds para realizar las actividades de control y supervisión del desempeño de la red de datos institucional. En dicho trabajo se realizó una evaluación entre las principales herramientas de gestión de red disponibles en el mercado y se determinó que la que más se adaptaba a las condiciones y necesidades de la red de datos de la UIS era la edición para ingenieros de Solarwinds.

En principio se plantea la monitorización de unas variables y dispositivos preliminares que fueron escogida(o)s producto de la experiencia del personal encargado de la administración de la red de datos de la UIS, de instituciones similares, trabajados de grado anteriores[1][2][5]. y de los eventos observados durante el transcurso del presente proyecto.

Los dispositivos a monitorizar son: los servidores de impacto institucional (servidor de Correo/DNS/Exchanger, servidor Web, servidor de la Biblioteca) y el Switch-Core. Este último es el dispositivo de mayor cuidado y dedicación por ser el núcleo de la estrella extendida de la red WAN institucional por ello se propone la monitorización continua de cada una de sus interfaces mediante la utilización de herramientas especificas de SolarWinds.

Algunas de las variables a monitorizar en el Switch Central son: Estado de las interfaces, porcentaje de utilización de los enlaces, errores transmitidos y recibidos, temperatura interna, estado de las VLANs y en los servidores son estado de la interfaz, nivel de procesamiento, porcentaje de utilización del enlace. Las variables escogidas, permitirán observar la configuración, disponibilidad, latencia y tráfico de la red de datos.

Es importante mencionar que los dispositivos y variables a monitorizar planteados corresponden solo a la primera propuesta. Una vez se decida por parte de la DSI, adoptar el software SolarWinds como herramienta de gestión y se tome la decisión de monitorizar continuamente la red de datos institucional, el administrador, de acuerdo al comportamiento observado, es quien determinará en definitiva las variables y dispositivos que necesita monitorizar. En este sentido la formulación del subproceso de monitorización es flexible a estos cambios y se destaca la importancia que tiene la experiencia del personal que lo lleve a cabo y la realimentación del subproceso con base en los datos recopilados.

La implantación de una estación gestora dedicada permitirá contar con información cuantitativa y organizada, recopilar estadísticas de las variables monitorizadas, detectar oportunamente eventos anómalos y lo más importante, permitirá obtener un indicativo del comportamiento de la red con base en información real y producto del análisis de los datos recopilados.

Este análisis de la información cuantitativa junto con el análisis de los incidentes encontrados y solucionados en el subproceso de mantenimiento correctivo hará parte de una base de conocimiento donde se registraran los incidentes más relevantes relacionados con la configuración, comportamiento, desempeño y problemas de la red de datos. Esto permitirá programar mantenimientos preventivos y atender rápidamente los mantenimientos correctivos. Por ello la propuesta del subproceso de monitorización incluye la creación de dicha base de conocimiento.

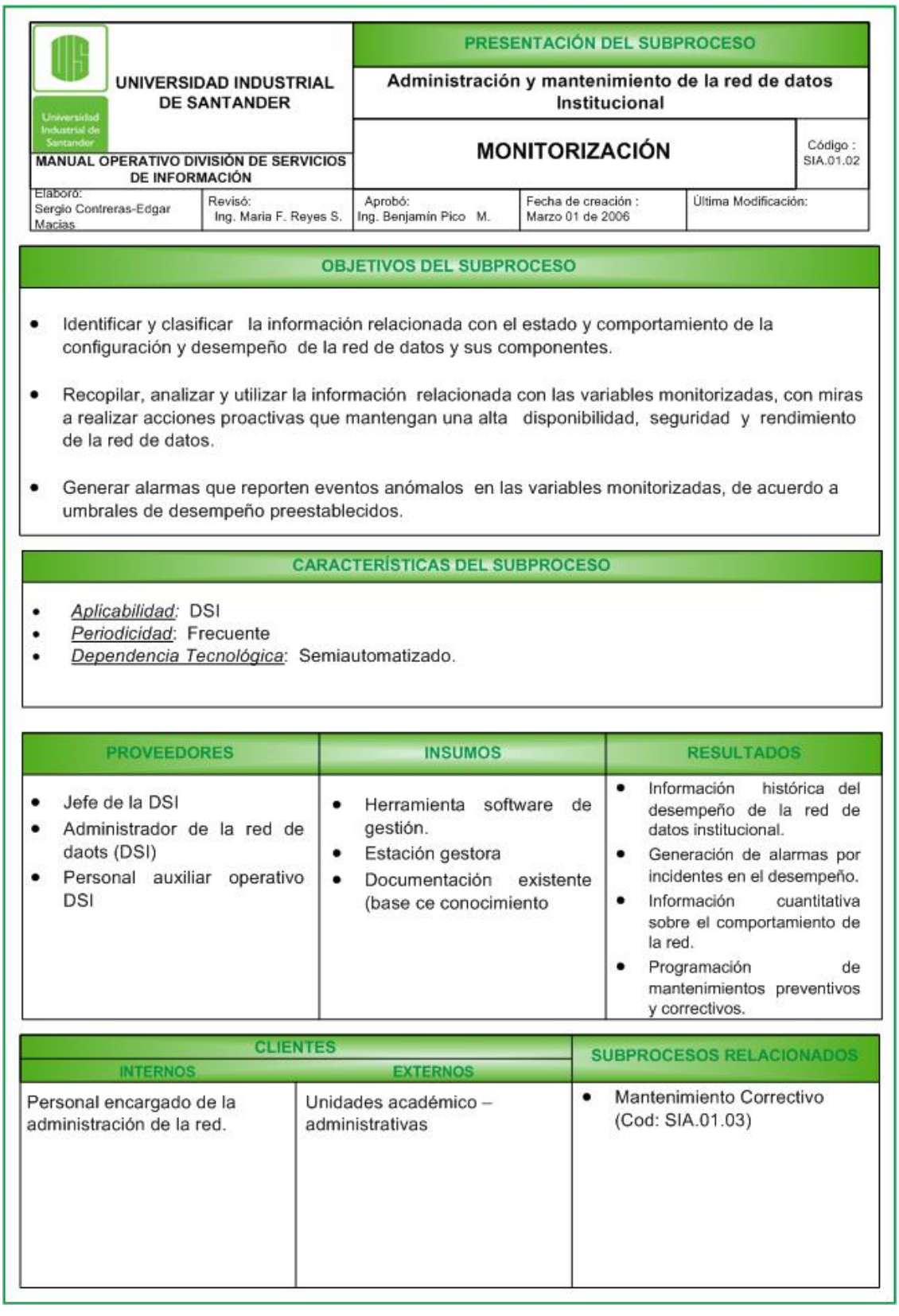
Por último la propuesta incluye un instructivo de la herramienta SolarWinds Ver anexo F donde se describen los usos, potencialidades y configuraciones que permitirán realizar una monitorización continua y documentada de la red. Este

instructivo esta orientado a estudiar las utilidades relacionadas con la monitorización[13].

En las figuras 8 y 9 se muestran las plantillas para el subproceso de monitorización.

[13] Para conocer una descripción básica de la todas la utilidades de la herramienta SolarWinds remítase a la tesis de maestría de GUZMAN CASTILLO PAOLA F. "Análisis de la gestión de dispositivos administrables en la red de datos institucional". Trabajo de investigación, Universidad Industrial de Santander 2005.

Figura 8. Plantilla principal del subproceso de monitorización.



UNIVERSIDAD INDUSTRIAL DE SANTANDER	PRESENTACIÓN DEL SUBPROCESO	
MANUAL OPERATIVO DIVISIÓN DE SERVICIOS DE INFORMACIÓN	Administración y mantenimiento de la red de datos Institucional	
	MONITORIZACIÓN	Código : SIA.01.02

Elaboró:	Revisó:	Aprobó:	Fecha de creación :	Última Modificación:
Sergio Contreras-Edgar Macías	Ing. María F. Reyes S.	Ing. Benjamín Pico M.	Marzo 01 de 2006	

OBJETIVOS DEL SUBPROCESO

- Identificar y clasificar la información relacionada con el estado y comportamiento de la configuración y desempeño de la red de datos y sus componentes.
- Recopilar, analizar y utilizar la información relacionada con las variables monitorizadas, con miras a realizar acciones proactivas que mantengan una alta disponibilidad, seguridad y rendimiento de la red de datos.
- Generar alarmas que reporten eventos anómalos en las variables monitorizadas, de acuerdo a umbrales de desempeño preestablecidos.

CARACTERÍSTICAS DEL SUBPROCESO

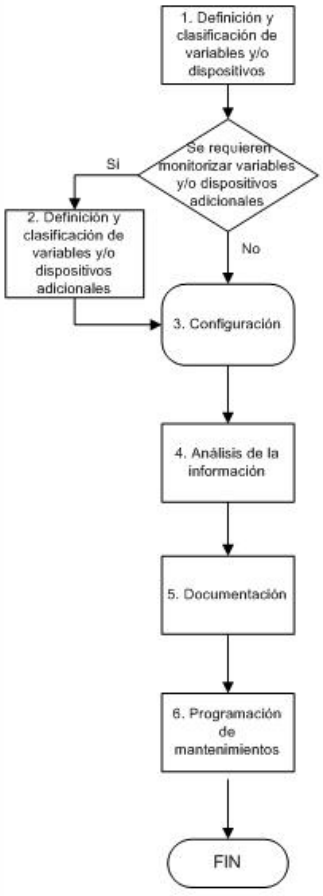
- *Aplicabilidad*: DSI
- *Periodicidad*: Frecuente
- *Dependencia Tecnológica*: Semiautomatizado.

PROVEEDORES	INSUMOS	RESULTADOS
• Jefe de la DSI • Administrador de la red de daots (DSI) • Personal auxiliar operativo DSI	• Herramienta software de gestión. • Estación gestora • Documentación existente (base ce conocimiento	• Información histórica del desempeño de la red de datos institucional. • Generación de alarmas por incidentes en el desempeño. • Información cuantitativa sobre el comportamiento de la red. • Programación de mantenimientos preventivos y correctivos.

CLIENTES		SUBPROCESOS RELACIONADOS
INTERNOS	EXTERNOS	
Personal encargado de la administración de la red.	Unidades académico – administrativas	• Mantenimiento Correctivo (Cod: SIA.01.03)

Figura 9. Plantilla principal del subproceso de monitorización – Diagrama de actividades

UNIVERSIDAD INDUSTRIAL DE SANTANDER	Administración y mantenimiento de la red de datos Institucional	MANUAL OPERATIVO DIVISIÓN DE SERVICIOS DE INFORMACIÓN	
	MONITORIZACIÓN	Código: SIA.01.02	Hoja 1 de 1
Elaboró : Sergio Contreras-Edgar Macias		Fecha de creación :	Marzo 01 de 2006
Revisó : Ing. Maria F. Reyes S.		Última Modificación :	
Aprobó : Ing. Benjamín Pico M.			

DIAGRAMA	DESCRIPCIÓN	RESPONSABLE	NORMATIVIDAD
	1. Se definen y clasifican las variables y/o dispositivos a monitorizar. Se especifican umbrales de desempeño para la generación de alarmas. Las variables a monitorizar se clasifican en información estática, dinámica.	Administrador de red	
	2. Las actividades del proceso se deben hacer en forma periódica. Si se requiere se realimenta el subproceso para redefinir las variables y umbrales de modo que se ajusten a las necesidades de la red de datos. Se seleccionan variables y/o dispositivos adicionales que requieran ser monitorizados de acuerdo al comportamiento de la red.	Administrador de red	
	3. Se configura el software de gestión de acuerdo a las variables y dispositivos seleccionados. Incluye la configuración de alarmas y la configuración para guardar los datos históricos recopilados.	Administrador de red	
	4. Con base en la información histórica recopilada y de las alarmas generadas, se procede a hacer un análisis estadístico que determine el comportamiento de la red. En este análisis se debe incluir la información registrada en el proceso de mantenimiento correctivo.	Equipo de técnicos de información, Administrador de red	
	5. Se documentan los resultados provenientes del análisis. Se almacena la información de acuerdo a los dispositivos y variables elegidas y se clasifica en información estática y estadística. La información se registra en el sistema de información, esta incluye la base de conocimiento que contribuirá para la toma de decisiones.	Equipo de técnicos de información y/o Administrador de red	
	6. Con base en las conclusiones obtenidas en el análisis de la información si es necesario se programan mantenimientos preventivos y/o correctivo en procura de un mejor desempeño de la red.	Equipo de técnicos de información y/o Administrador de red	

3.5 SUBPROCESO DE MANTENIMIENTO CORRECTIVO

La propuesta gira en torno a dos aspectos: Intentar solucionar los incidentes/problemas en forma remota o evitar al máximo el número de desplazamientos y crear y alimentar una base de conocimiento sobre los problemas de red de la red de datos institucional.

Las actividades del subproceso inician con el reporte de un incidente en los servicios que soporta la red. (Ver figura 10) Los incidentes pueden ser reportados por un usuario o pueden ser detectados por personal interno, producto de la monitorización u otro proceso. Para la recepción de solicitudes se propone la implementación de un único centro de atención al usuario a donde se solicite soporte técnico cada vez que ocurra un incidente en alguno de los servicios que soporta la DSI a través de la red de datos.

El subproceso continúa con la ejecución de las listas de chequeo, de acuerdo al tipo de incidente reportado. El objetivo de tales listas es intentar encontrar soluciones en forma remota de modo que se evite al máximo los desplazamientos. Si la lista de chequeo no finaliza con una solución remota, al menos debe finalizar con la identificación y clasificación del incidente y con la ubicación del lugar (estación de usuario o cuarto de cableado) a donde se debe desplazar el personal para su solución.

El planteamiento de las listas de chequeo para la solución de problemas de red, se hizo por una parte con base en la experiencia recopilada de las personas que a diario laboran en la UIS y en las otras instituciones visitadas y por otra parte con base en las recomendaciones que organizaciones como CISCO emiten al respecto. En este sentido CISCO recomienda[14] que las pruebas básicas de

[14] CISCO SYSTEMS. Guía del primer año CCNA 1 y 2. Pearson Educación S.A, Tercera edición 2005. Cap 18

conectividad en una red deben desarrollarse en secuencia comenzando desde una capa del modelo de referencia OSI a la siguiente. Se recomienda comenzar con la Capa 1 y continuar hasta llegar a la Capa 7, si es necesario. Ver anexo H para mayor información.

La implantación de un plan de gestión de red y en particular la ejecución de las listas de chequeo requiere contar con un inventario actualizado de la disposición física y lógica de la red. En este sentido la DSI cuenta con un sistema de información donde se registra la disposición física y configuración de red de nuevas estaciones terminales, entre otros datos. En este aspecto solo falta incrementar los esfuerzos para lograr mantener actualizado dicho sistema de información.

Durante el proceso de solución del incidente y una vez solucionado se deben *documentar* los pasos que se siguieron, los aciertos y errores, las personas que intervinieron, entre otros datos que se encuentran en el formato de mantenimiento correctivo (ver anexo G). El propósito de la documentación es crear y realimentar una base de conocimiento donde se registren los incidentes y problemas que se presentan en los servicios que soporta la red de datos.

En la propuesta se presentan guías de procedimientos para la atención a incidentes relacionados con configuración de red en terminales, configuración de dispositivos activos y para solucionar problemas de conectividad. No obstante, el planteamiento del subproceso es flexible y permite la inclusión de incidentes relacionados con cualquier servicio que soporta la DSI a través de la red datos, solamente se necesita que cada unidad de la DSI realice sus guías de procedimientos particulares. (Ver plantilla. Figura 10)

La plantilla general para la descripción del subproceso de mantenimiento correctivo junto con el esquema general de actividades se muestran a continuación (Figuras 10 y 11). Las guías de procedimientos donde se describe la

realización de cada una de las actividades planteadas para el subproceso de mantenimiento correctivo se encuentra en el anexo G. Allí se incluye también el instructivo de las listas de chequeo que se muestran en la Figura 12

Figura 10. Plantilla principal del subproceso de Mantenimiento Correctivo.

UNIVERSIDAD INDUSTRIAL DE SANTANDER	PRESENTACIÓN DEL SUBPROCESO	
MANUAL OPERATIVO DIVISIÓN DE SERVICIOS DE INFORMACIÓN	Administración y mantenimiento de la Red de Datos Institucional	
	MANTENIMIENTO CORRECTIVO	Código : SIA.01.03

Elaboró:	Revisó:	Aprobó:	Fecha de creación :	Última Modificación:
Sergio Contreras-Edgar Macías	Ing. Maria F Reyes S.	Ing. Benjamín Pico M.	Marzo 1 de 2006	

OBJETIVOS DEL SUBPROCESO

- Diseñar estrategias que permitan solucionar los problemas o fallas reportados por los usuarios de la red (Unidades Académico - administrativas) de forma efectiva.
- Solucionar las fallas reportadas por los usuarios relacionadas con los servicios que soporta la red de datos, de acuerdo a las estrategias diseñadas.
- Crear y realimentar una base de conocimiento sobre los problemas presentados en los servicios que soporta la red de datos institucional, con el fin de identificar patrones de problemas con sus soluciones, realizar inferencias estadísticas sobre los mismos y a largo plazo establecer planes de mantenimiento preventivo.

CARACTERÍSTICAS DEL SUBPROCESO

- *Aplicabilidad*: Unidades académico – administrativas de la UIS
- *Periodicidad*: Esporádico
- *Dependencia Tecnológica*: Semiautomatizado.

PROVEEDORES	INSUMOS	RESULTADOS
• Usuarios de la red de datos institucional. • Administrador de la red de datos (DSI). • Personal auxiliar operativo DSI	• Computador Personal • Herramienta software de gestión de red adoptada por al DSI. • Manuales propios de los equipos de red. • Listas de chequeo correspondiente.(Desplazamiento a campo, tiempos de respuesta largos, fallas en servicios de red • Documentación existente (base de conocimiento) • Equipos de comunicación (radio-comunicadores)	• Reestablecimiento de los servicios soportados por la red de datos Institucional. • Documentación de las características de cada problema y los aciertos y errores en la(s) solución(es) encontrada(s).

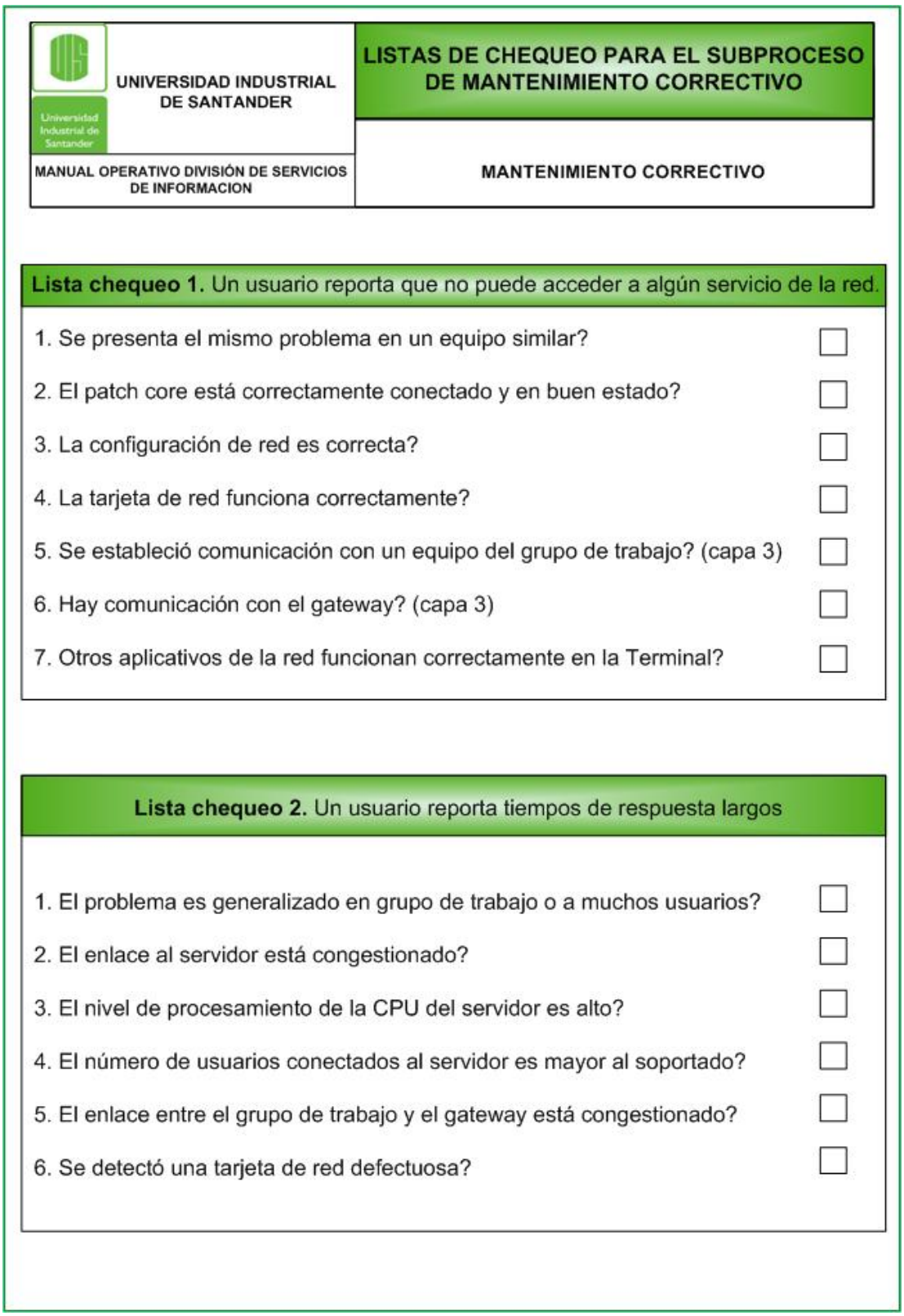
CLIENTES		SUBPROCESOS RELACIONADOS
INTERNOS	EXTERNOS	
Personal encargado de la administración de la red.	Unidades Académico - Administrativas	• Monitorización (Cod: SIA.01.02)

Figura 11. Plantilla principal del subproceso de Mantenimiento Correctivo – Diagrama de actividades

UNIVERSIDAD INDUSTRIAL DE SANTANDER	Administración y mantenimiento de la Red de Datos Institucional	MANUAL OPERATIVO DIVISIÓN DE SERVICIOS DE INFORMACIÓN
	MANTENIMIENTO CORRECTIVO	Código: SIA.01.03 / Hoja 1 de 1
Elaboró : Sergio Contreras-Edgar Macias		Fecha de creación : Marzo 1 de 2006
Revisó : Ing. Maria F. Reyes S.		Última Modificación :
Aprobó : Ing. Benjamín Pico Merchán		

DIAGRAMA	DESCRIPCIÓN	RESPONSABLE	NORMATIVIDAD
	1. Un usuario de la red de datos institucional o Personal Interno de la DSI identifica y reporta una falla en algún servicio soportado por la red. Si el reporte lo hace personal Interno de la DSI, producto de la monitorización u otro proceso se asume que el problema ya ha sido identificado.	Personal Centro Atención Usuario	
	2. Si el problema es reportado por un usuario se procede a diligenciar la lista de chequeo correspondiente y ejecutar las acciones determinadas que permita identificar el incidente o problema, clasificarlo, determinar el lugar donde ocurrió y el sitio a donde se debe acudir o encontrar una solución en remota desde el Centro de Atención al Usuario.	Personal Centro Atención Usuario	
	3. Si no se logra solucionar en forma remota, se genera una Orden de Trabajo (diligenciar el Formato de mantenimiento Correctivo) a la persona que le corresponda la solución dependiendo del tipo de problema (Relacionado con conectividad, con aplicativos o soporte de escritorio).	Personal Centro Atención Usuario	
	4. Se hace el desplazamiento al lugar mas probable donde se podría dar solución al problema y se procede a ejecutar esta.	Técnicos de información	
	5. Una vez solucionada la falla se procede a documentar los pasos y personas que intervinieron en la solución, el tipo de problema y el lugar donde ocurrió, el tiempo que demoró la solución y demás indicadores. Diligencias formato de mantenimiento Correctivo.	Personal Centro Atención Usuario Técnicos de información	
	6. Si existen problemas en espera o si se presenta uno nuevo se inicia otra vez el Subproceso.	Personal Centro Atención Usuario	

Figura 12. Plantilla para las listas de chequeo del subproceso de Mantenimiento Correctivo.



UNIVERSIDAD INDUSTRIAL DE SANTANDER	LISTAS DE CHEQUEO PARA EL SUBPROCESO DE MANTENIMIENTO CORRECTIVO
MANUAL OPERATIVO DIVISIÓN DE SERVICIOS DE INFORMACION	MANTENIMIENTO CORRECTIVO

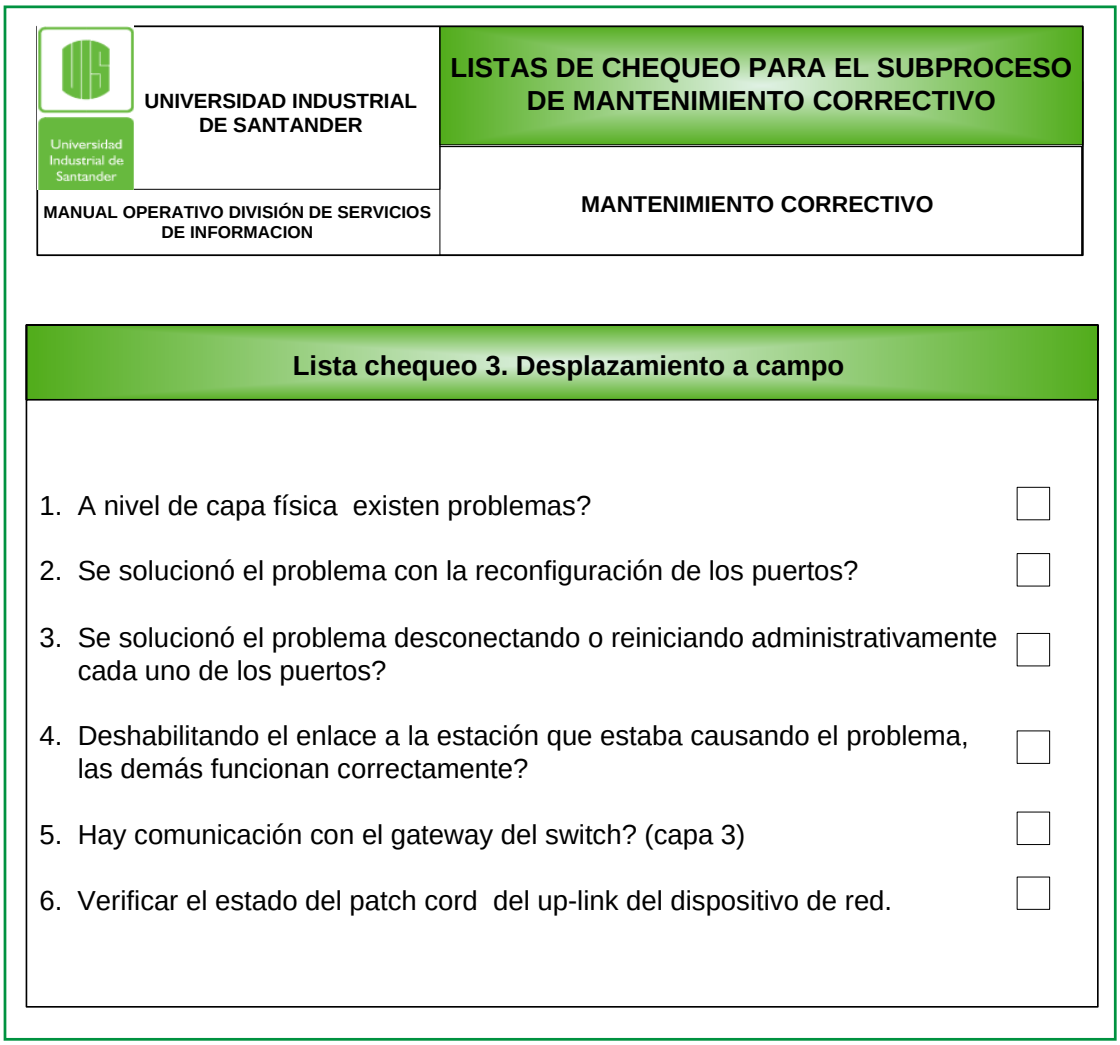
Lista chequeo 1. Un usuario reporta que no puede acceder a algún servicio de la red.

1. Se presenta el mismo problema en un equipo similar? ☐
2. El patch core está correctamente conectado y en buen estado? ☐
3. La configuración de red es correcta? ☐
4. La tarjeta de red funciona correctamente? ☐
5. Se estableció comunicación con un equipo del grupo de trabajo? (capa 3) ☐
6. Hay comunicación con el gateway? (capa 3) ☐
7. Otros aplicativos de la red funcionan correctamente en la Terminal? ☐

Lista chequeo 2. Un usuario reporta tiempos de respuesta largos

1. El problema es generalizado en grupo de trabajo o a muchos usuarios? ☐
2. El enlace al servidor está congestionado? ☐
3. El nivel de procesamiento de la CPU del servidor es alto? ☐
4. El número de usuarios conectados al servidor es mayor al soportado? ☐
5. El enlace entre el grupo de trabajo y el gateway está congestionado? ☐
6. Se detectó una tarjeta de red defectuosa? ☐

Figura 12. Plantilla para las listas de chequeo del subproceso de Mantenimiento Correctivo (Pág. 2)



UNIVERSIDAD INDUSTRIAL DE SANTANDER	LISTAS DE CHEQUEO PARA EL SUBPROCESO DE MANTENIMIENTO CORRECTIVO
MANUAL OPERATIVO DIVISIÓN DE SERVICIOS DE INFORMACION	MANTENIMIENTO CORRECTIVO

Lista chequeo 3. Desplazamiento a campo

1. A nivel de capa física existen problemas? ☐
2. Se solucionó el problema con la reconfiguración de los puertos? ☐
3. Se solucionó el problema desconectando o reiniciando administrativamente cada uno de los puertos? ☐
4. Deshabilitando el enlace a la estación que estaba causando el problema, las demás funcionan correctamente? ☐
5. Hay comunicación con el gateway del switch? (capa 3) ☐
6. Verificar el estado del patch cord del up-link del dispositivo de red. ☐

Es importante destacar que los principios sobre los que se basa la propuesta de mejora al plan de gestión de red presentado y en particular las ideas para la definición y descripción de cada subproceso corresponden en su mayoría a las mejores prácticas identificadas con la aplicación de la metodología de benchmarking en las diferentes universidades junto con las valiosas ideas aportadas por el ingeniero Juan Carlos Contreras. La investigación de las mejores prácticas y destacar la existencia de modelos de referencia para la implantación de sistemas de gestión operativa y de negocio (ITIL – ISO 2000 y eTOM) en organizaciones que prestan servicios de TI es un valioso aporte del presente trabajo. Vale la pena destacar en su orden los principios de la

propuesta de mejora: Enfocarse en procesos, definir y documentar los procesos, elaborar guías de procedimientos de soporte, calidad de servicio, base de conocimiento, herramienta de gestión unificada, monitorizar continuamente dispositivos y variables de la red, generar documentación, realimentar la base de conocimiento, enfocarse en acciones proactivas en reemplazo de las reactivas, centro de atención al usuario, evitar desplazamientos, ahorrar recursos y tiempo e incrementar la satisfacción del cliente (usuario de red). Estos términos están contenidos a lo largo de la propuesta.

También es importan resaltar que los detalles de las guías de procedimientos y de las listas de chequeo fueron corroborados y validados por el administrador de la red de datos institucional quien a su vez es codirector del presente proyecto. Esto indica que en principio la propuesta de mejora al plan de gestión de red es aplicable al entorno de la red de datos de la UIS y que solo con base en la experiencia acumulada y en el análisis de los resultados obtenidos posteriores a la implantación de la propuesta, el planteamiento presentado es susceptible de ser reajustado a las condiciones cambiantes de la red de datos institucional. Por ello, es decisión de la DSI acoger e implantar la presente propuesta y probar si los buenos resultados obtenidos en otras instituciones y organizaciones pueden ser obtenidos también al interior de la Universidad Industrial de Santander.

Para finalizar, se presenta en el siguiente capítulo los resultados de la monitorización del switch central y de algunos servidores de la red institucional que muestran las potencialidades del software de gestión SolarWinds.

4. PRUEBAS DE MONITORIZACIÓN CON EL SOFTWARE SOLARWINDS

En el presente capítulo se muestran algunas de las potencialidades y usos del software de gestión SolarWinds para la monitorización de dispositivos activos de red y servidores.

Se seleccionaron algunas de las variables y dispositivos propuestos en el subproceso de monitorización: Los dispositivos escogidos fueron el switch central, el servidor de la biblioteca y el servidor de ingeniería industrial. Se seleccionaron las herramientas “Network Performance Monitor” y “SNMP Graph” de SolarWInds para monitorizar variables de estado y desempeño de los dispositivos y sus enlaces asociados.

En adelante se mostrará en primera instancia las variables y dispositivos seleccionados para la monitorización, se continúa con las indicaciones generales para la configuración de las herramientas de SolarWinds mencionadas, indicaciones que se encuentran con mayor detalle en el anexo F. Se sigue con la muestra de resultados, empezando con los resultados de la monitorización de los servidores pelícano y carpintero respectivamente, se sigue con la exposición de los resultados obtenidos en la monitorización del switch central núcleo de la estrella extendida de la red WAN institucional y se finaliza con el análisis de los resultados de la monitorización del tráfico generado por la estación gestora.

4.1 VARIABLES Y DISPOSITIVOS SELECCIONADOS

Tabla 2. Listado de variables a Monitorizar

Variable	Nombre	Tipo	OID
Status – Estado de la interfaz	IfOperStatus	Integer	1.3.6.1.2.1.2.2.1.8
Admin Status - Estado administrativo de la interfaz (Up/ShutDown)	ifAdminStatus	Integer	1.3.6.1.2.1.2.2.1.7
Bytes received _ Bytes recibidos	ifInOctects	Counter32	1.3.6.1.2.1.2.2.1.10
Bytes transmitted _ Bytes transmitidos	ifOutOctects	Counter32	1.3.6.1.2.1.2.2.1.16
Receive Errors – Errores recibidos (pps)	ifInErrors	Counter32	1.3.6.1.2.1.2.2.1.14
Transmit Errors – Errores recibidos (pps)	ifIOutErrors	Counter32	1.3.6.1.2.1.2.2.1.20
Current Temperature - temperatura interna actual del dispositivo en grados Celsius)*	extremeCurrentTemperature	Integer	1.3.6.1.4.1.1916.1.1.1.8

* OID propietaria de Extreme Networks, solo disponible para el switch central.

FUENTE: Diseño de los autores.

Además se monitorizaron variables relacionadas con el hardware de los dispositivos, tales como el porcentaje de utilización de la memoria y la CPU. y variables relacionadas con la disponibilidad y tiempos de respuesta.

Tabla 3. Lista de dispositivos monitorizados

Dispositivo	Nombre de Dominio	Dirección IP
Servidor de la Biblioteca	pelicano.uis.edu.co	192.168.19.6
Servidor Ingeniería Industrial	carpintero.uis.edu.co	192.168.19.
Switch-Core	---	192.168.19.1

FUENTE: Diseño de los autores.

4.2 CONFIGURACIÓN DE LAS HERRAMIENTAS SELECCIONADAS PARA LA MONITORIZACIÓN

Las herramientas de SolarWinds seleccionadas fueron:

- Network Performance Monitor.
- SNMP Graph.

Para iniciar la monitorización con la herramienta solo se requiere conocer la dirección IP del dispositivo que se desea monitorizar y la comunidad SNMP de lectura si solo se desea visualización de las variables y la comunidad SNMP de lectura/escritura si se desea además de visualizar realizar cambios remotos en el estado de las variables estáticas supervisadas. Si el dispositivo tiene configurada más de una dirección IP (por ejemplo un router o un Switch capa 3) es posible acceder al dispositivo para su monitorización con cualquiera de estas direcciones.
En el anexo F se encuentra una guía detallada para la configuración y manipulación de las herramientas seleccionadas.

4.3 Muestra de resultados

El periodo de tiempo de la prueba que se consigna a continuación corresponde a un día laboral bajo condiciones normales dentro de la Universidad. El análisis que se realiza es general y no busca estudiar ni concluir condiciones de tráfico particulares, el objetivo es mostrar las potencialidades y usos de la herramienta así como su fácil configuración y utilización.

- *Monitorización de servidores:*

Para la monitorización de servidores se utilizó la herramienta Network Performance Monitor.

Servidor Pelicano

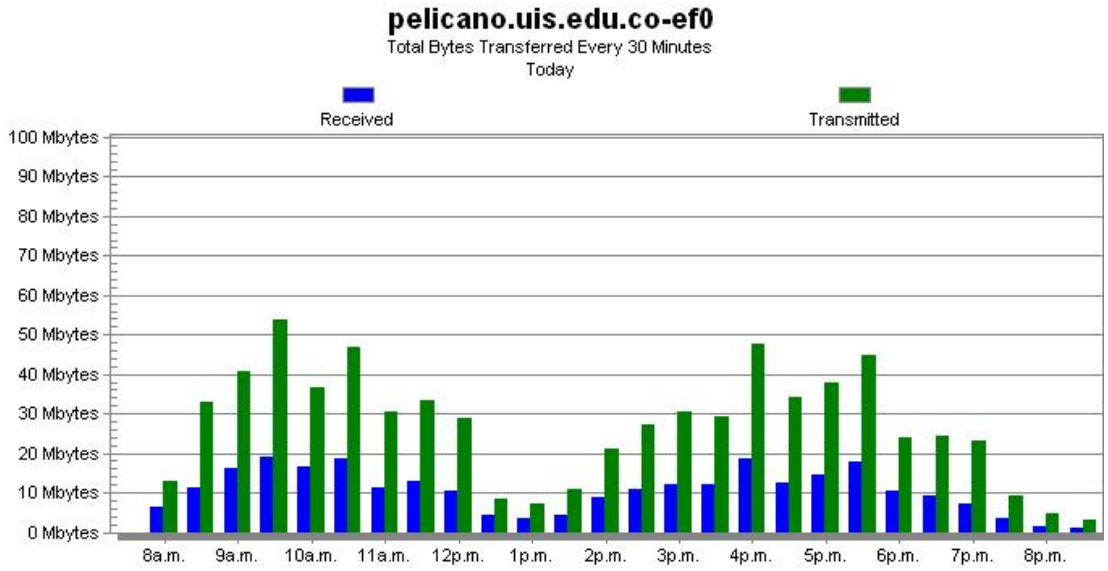


Figura 13. Bytes Totales Enviados y Recibidos cada 30min en la interfaz Fastethernet del servidor pelicano

La figura 13 muestra el tráfico de entrada y salida al servidor en (Mbps) las estadísticas son recopiladas y visualizadas para un periodo de 30 minutos. Este tipo de graficas permite mostrar la actividad continua de un servidor o cualquier otro dispositivo administrable durante todo un día y si es necesario durante periodos semanales, mensuales, anuales, etc. de tiempo. El periodo de visualización de la grafica puede ser modificado hasta 5min para obtener mayor precisión en la visualización de determinado evento relacionado con el dispositivo.

La figura 14 muestra el porcentaje de utilización del enlace asociado al dispositivo de acuerdo al tráfico entrante y saliente. En este caso particular se utiliza tecnología FastEthernet para la conexión del servidor, por lo cual se tiene un ancho de banda nominal de 100Mbps full duplex. En la grafica se observa que el porcentaje de utilización de los 100Mbps disponibles corresponde solo a una fracción entre en 0.01% y el 0.27% tanto en transmisión como en recepción, lo que indica una baja utilización del enlace durante este periodo de estudio.

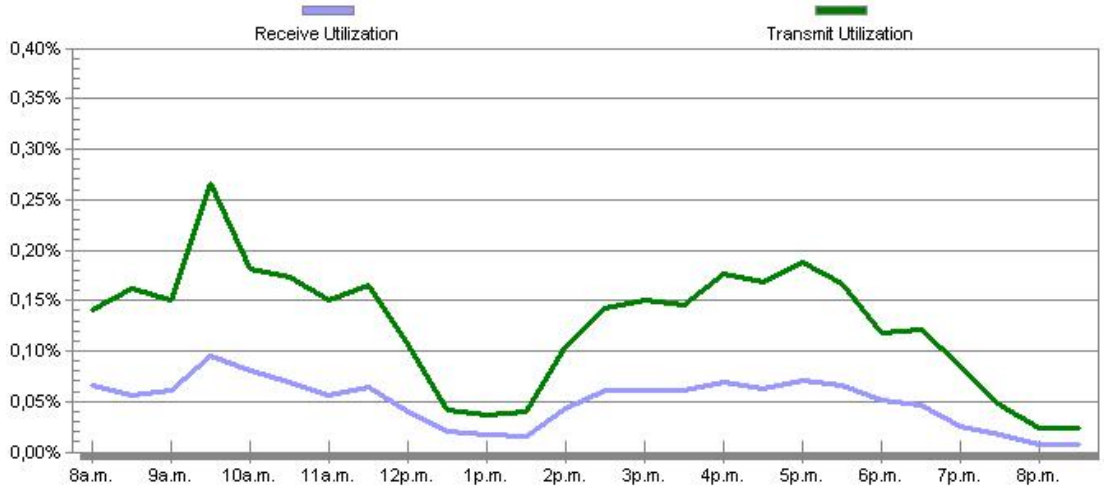


Figura 14. Porcentaje de utilización de la interfaz Fastethernet del servidor pelicano

Este tipo de gráficas (Figura 13 y Figura 14) son de gran utilidad para la supervisión de servidores que reciben constantes peticiones, soportan un gran número de usuarios y servicios. Por ejemplo sería útil para la monitorización del servidor de Correo/DNS/Exchanger, el servidor de la biblioteca entre otros.

Servidor Carpintero

La figura 15 muestra el porcentaje de utilización de la CPU del servidor de Ingeniería Industrial, en este caso el porcentaje de utilización es bajo. Sin embargo en servidores de acceso general dentro de la universidad el porcentaje de utilización de la CPU en determinados días o periodos de tiempo puede ser alto. Supervisar este tipo de utilización permite identificar degradaciones en el servicio debido a saturación en el nivel de procesamiento de la maquina, lo que permitiría dimensionar las características del dispositivos y tomar acciones preventivas que permitan mantener una calidad de servicio adecuada.

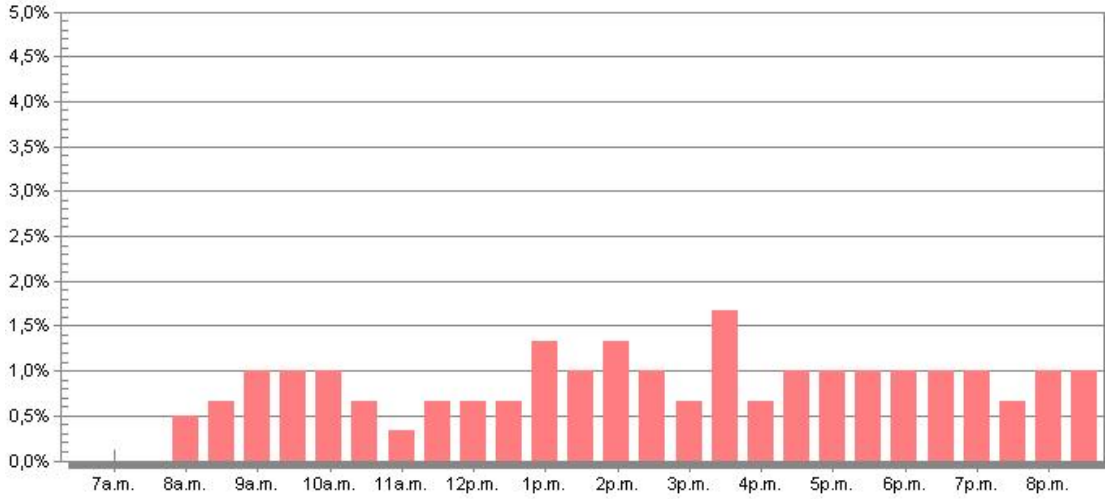


Figura 15. Porcentaje de utilización de la CPU del servidor carpintero

La figura 16 muestra el tiempo de respuesta y el porcentaje de utilización del servidor carpintero durante el periodo de estudio. Este tipo de supervisión nos permite conocer la disponibilidad del dispositivo monitorizado, además permite visualizar tiempos de respuesta largos y perdida considerable de paquetes, eventos que pueden ser asociados a inconvenientes y/o problemas con el servicio y el dispositivo.

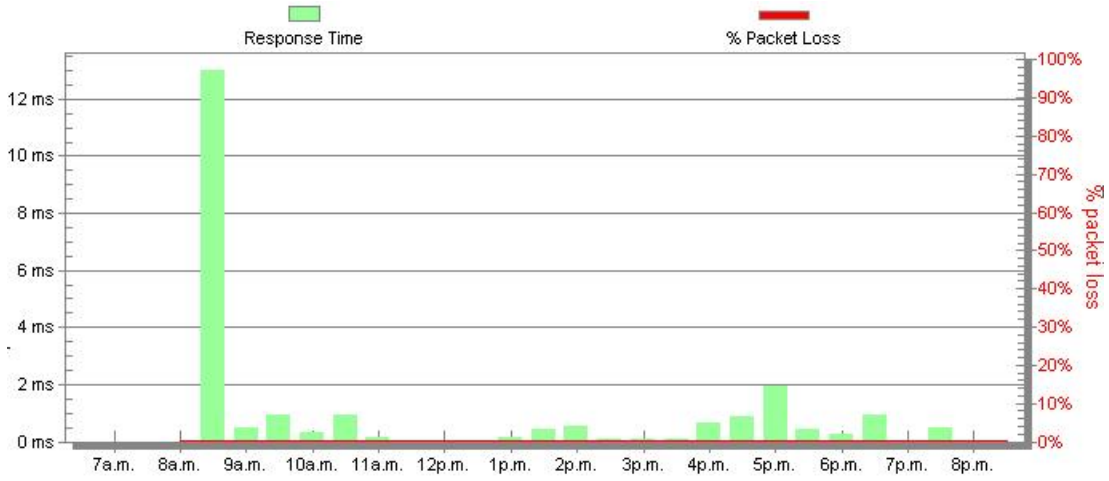


Figura 16. Tiempo de respuesta y porcentaje de paquetes perdidos del servidor carpintero.

Además de las variables visualizadas, se monitorizó el porcentaje de utilización de la memoria el cual se mantuvo en un promedio del 25% y la disponibilidad del dispositivo, que durante el periodo de estudio no presentó inconvenientes.
Para el caso de servidores se recomienda la configuración de alarmas que reporten el momento en que los tiempos de repuesta comienzan a crecer demasiado o cuando el dispositivo no responde. Para configurar esta alarma se debe seleccionar la opción Status en las variables asociadas a los nodos (Node status). Se selecciona luego la condición de alarma de acuerdo a las necesidades. Se puede seleccionar la opción extrema que corresponde a la no respuesta del dispositivo (Down) o la opción de notificación de tiempo de repuestas largos (Warning). En el anexo F se encuentra un instructivo más completo para la configuración de alarmas.

La monitorización continua, la información recopilada en la base de conocimiento y las estadísticas almacenadas para cada dispositivo son útiles al momento de establecer relaciones entre los eventos detectados en servidores y una falla en el desempeño de la red.

- *Monitorización del Switch Central*

El dispositivo de mayor atención es el switch central BlackDiamond 6808 de Extreme Networks, núcleo de la estrella extendida de la WAN de la UIS. La monitorización de este dispositivo brinda información de todo el tráfico que se maneja dentro de la red de datos de la universidad entre VLANs. Permite identificar el momento en que un switch departamental presenta problemas o sale de servicio y permite conocer y supervisar el estado y el tráfico hacia el exterior. Para lograr este tipo de supervisión es necesario monitorizar continuamente cada una de sus interfaces.

Es posible conocer el tráfico interno de cada VLAN monitorizando todas las interfaces del Switch(es) departamental(es) asociados a la VLAN en estudio.

Se realizaron las pruebas de monitorización de todas las interfaces del switch central así como la supervisión continua de su temperatura interna. Para la monitorización de las interfaces se utilizó la herramienta de Solarwinds “Network Performance Monitor” y para la monitorización de su temperatura se utilizó la herramienta SNMP Graph.

La figura 17 muestra la temperatura interna del switch central, este variable permite supervisar el estado del sistema de ventilación del dispositivo y permite tomar acciones inmediatas frente a cualquier eventualidad que se presente. Con esto es posible tomar acciones preventivas para preservar la integridad y desempeño del dispositivo.

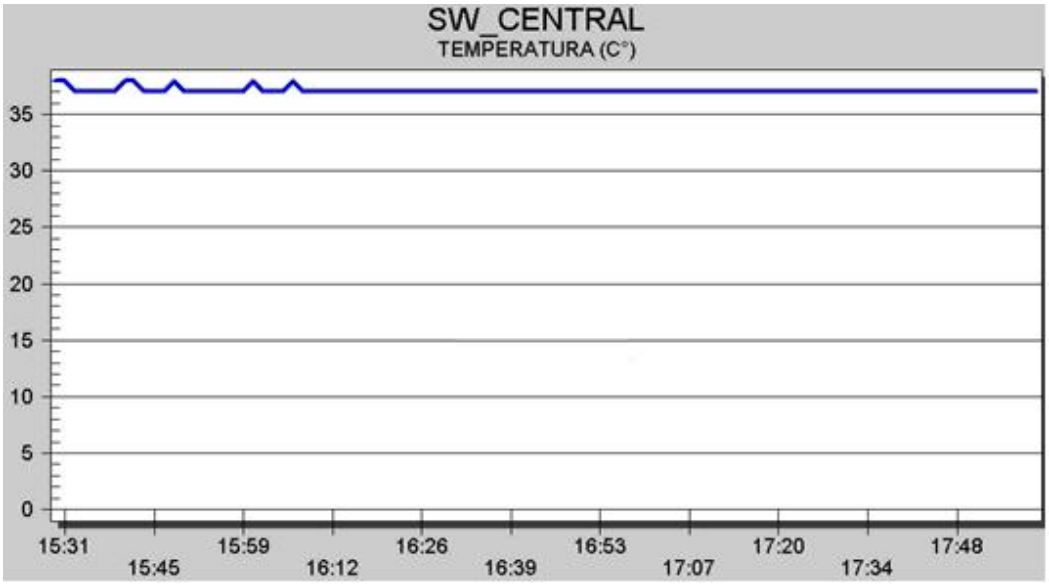


Figura 17. Temperatura interna del switch central

Las figuras 18 y 19 muestran los resultados de la monitorización de la interfaz 4:16 del switch central que corresponde al enlace de Internet. Se muestra la información de esta interfaz por ser la de más tráfico y utilización. En la grafica se visualiza la utilización prácticamente continua del enlace de 12 Mbps

correspondiente a los 6Mbps contratados con ETB y los otros 6Mbps del enlace con Telecom. Sin embargo, es posible monitorizar los enlaces por separado accediendo a las interfaces FastEthernet o seriales de los respectivos routers. Para ello, solo se necesitan conocer la dirección IP de cualquiera de las interfaces y la comunidad SNMP de lectura o de lectura/escritura.

La propuesta de monitorización plantea la supervisión continua de todas las interfaces durante un periodo indefinido de tiempo. La herramienta Network Performance Monitor permite llevar un histórico de las variables, nodos e interfaces monitorizadas. De esta forma es posible visualizar el comportamiento de cualquier variable monitorizada en periodos desde minutos a periodos de tiempo de semanas y meses. Con ello se supervisa el comportamiento de toda la red y con base en datos reales se pueden tomar decisiones proactivas, planear mantenimientos preventivos y tomar decisiones rápidas y concretas en beneficio del servicio prestado.

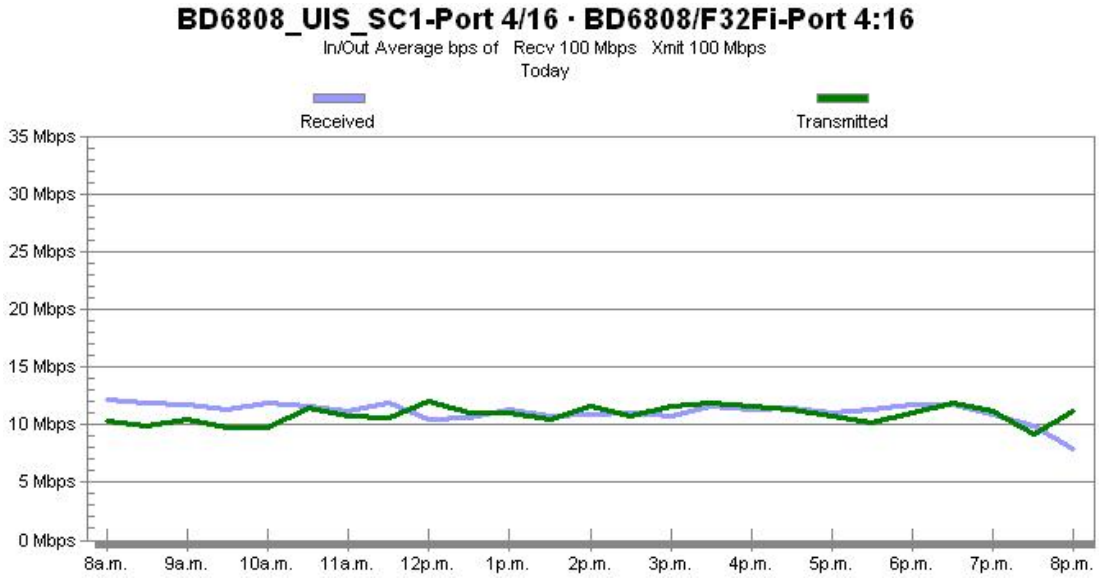


Figura 18. Utilización del enlace (Mbps). Puerto 4:16 del switch central

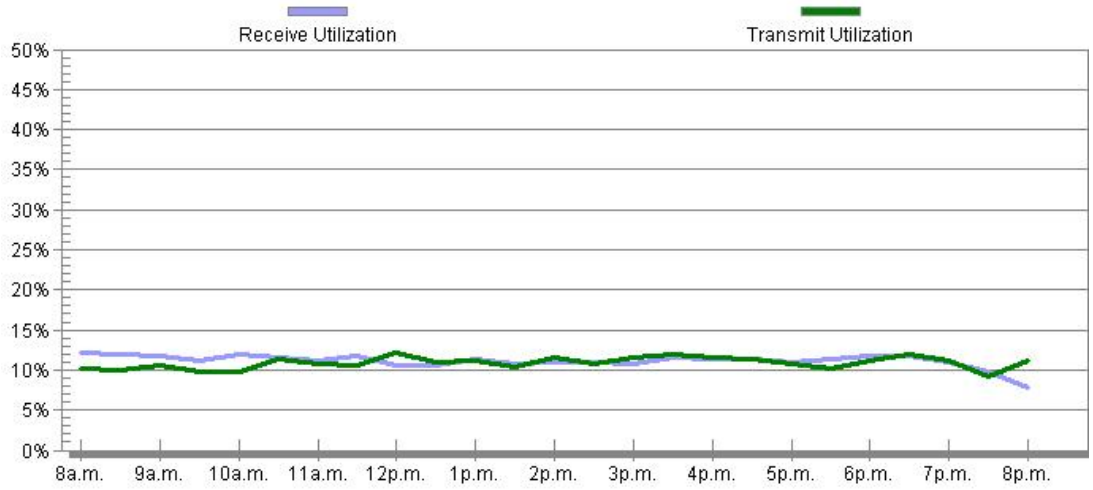


Figura 19. Porcentaje de utilización de enlace (Mbps). Puerto 4:16 del switch central

Los resultados de la monitorización de la demás interfaces del switch central mostraron una muy baja utilización de los enlaces, no se presentaron perdidas de paquetes, errores ni problemas en la disponibilidad de cada una de ellas.

La figura 20 muestra los puertos de mayor actividad aparte del 4:16 (enlace a Internet)

Puerto 4:1 – Diseño Industrial (100Mbps)
Puerto 4:2 – Facultad de salud (100Mbps)
Puerto 5:5 – Laboratorio de pasados (1Gbps)
Puerto 5:7 – Edifício Jorge Bautista (1Gbps)

Se recomienda la configuración de alarmas para supervisar la disponibilidad de todas las interfaces, además de condiciones que indiquen que el porcentaje de utilización de los enlaces de Internet presentan problemas, ya que por experiencia este porcentaje de utilización en condiciones normales no debe descender considerablemente.

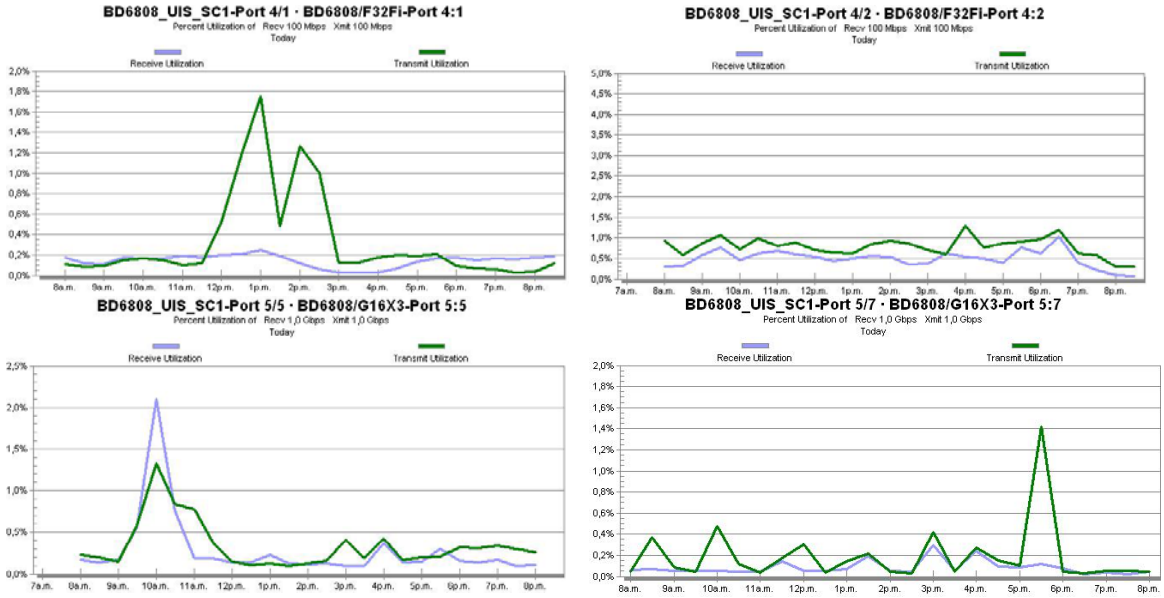


Figura 20. Porcentaje de utilización de los puertos 4:1, 4:2, 5:5 y 5:7

Con la experiencia, la base de conocimiento y los datos históricos es posible particularizar alarmas que indiquen degradaciones en el servicio y problemas con la conectividad y disponibilidad de los enlaces.

- *Tráfico generado por el gestor*

Por ultimo se realizó una prueba para visualizar el tráfico generado por la estación gestora. En esta prueba se muestra el tráfico entrante y saliente generado por el gestor al monitorizar todas las interfaces del switch central, dos servidores y un switch departamental con la herramienta Network Performance Monitor configurada con un intervalo de sondeo (polling) de 120 segundos. A esto se le suma la monitorización del puerto al cual estaba conectado el gestor con la herramienta SNMP Graph configurada con un intervalo de sondeo de 10 segundos. Para realizar esta prueba se monitorizaron los dispositivos desde una estación gestora directamente conectada a un puerto de un switch departamental. De esta forma fue posible capturar solo el tráfico de ese puerto en particular correspondiente al generado por el gestor.

Es evidente que el tráfico generado por la estación gestora no es significativo y de ninguna forma saturaría los enlaces disponibles de 100Mbps y 1Gbps. Sin embargo se recomienda conectar la estación gestora directamente a uno de los puertos del switch central para evitar que su trabajo sea interrumpido por fallas en dispositivos o enlaces intermedios.

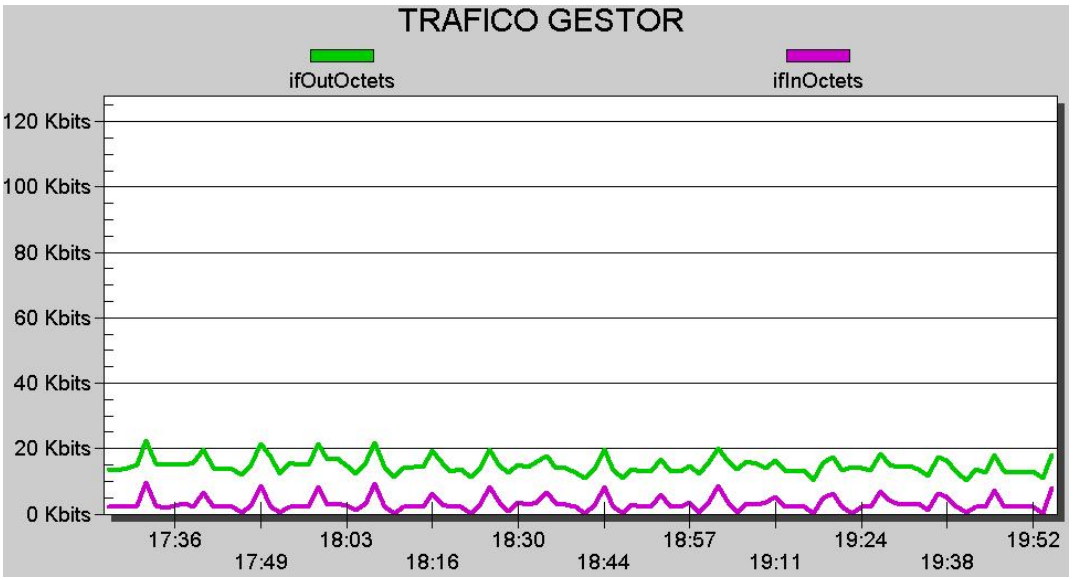


Figura 21. Tráfico generado por la estación gestora

Los resultados mostrados, indican que con solo dos herramientas de solarWinds – Network Performance Monitor y SNMP Graph es posible monitorizar una buena cantidad de variables que muestran el estado, desempeño y comportamiento de la red de datos institucional. Al uso de estas herramientas se le puede agregar el grupo de herramientas para el descubrimiento de red – Network Discovery, útil para el control de inventario de la red y la herramienta gráfica para la monitorización del estado de los nodos – Watch it. El grupo herramientas de Seguridad - Security son de gran importancia por que con ellas se puede determinar el grado de inmunidad o vulnerabilidad de la red ante usuarios no deseados y ataques externos. En fin, el software de gestión SolarWinds contiene grandes potencialidades en su variedad de herramientas que merecen ser exploradas, sin embargo, el administrador de la red es quien en últimas determina

los dispositivos y variables y consecuentemente los grupos de herramientas que necesita utilizar para determinar el comportamiento de la red y los más importante, para ofrecer un servicio con calidad aceptable a los usuarios de la red: “la comunidad universitaria y sociedad en general”

5. CONCLUSIONES Y RECOMENDACIONES

- Se definieron y documentaron los subprocesos de instalación, monitorización y mantenimiento correctivo en plantillas estándar propias de la UIS. Se elaboraron sus guías de procedimientos y se mostraron las potencialidades del software de gestión de red SolarWinds aplicado al entorno de la red de datos de la UIS. Con estos tres productos se cumplen satisfactoriamente los objetivos propuestos del presente trabajo de grado y se deja como agregado el conocimiento de las buenas prácticas en el campo de la gestión de red que están dando resultados positivos en otras instituciones educativas y a nivel empresarial.

- Las grandes virtudes de la propuesta presentada es que por un lado contiene referentes científicos combinados con referentes pragmáticos y por el otro contiene la integración de los aspectos técnicos y tecnológicos de la gestión de red con los aspectos administrativos y organizacionales del entorno donde se desempeña. Para el desarrollo de la propuesta se tuvo en cuenta y se dio continuidad a los trabajos anteriores realizados por integrantes del grupo CPS[15] en conjunto con la DSI en el campo de las redes de computadores y en particular de la gestión de red, lo que constituye el referente científico. El componente pragmático lo constituyen los resultados de la aplicación de la metodología de benchmarking en instituciones educativas con redes de datos similares a la UIS en donde se rescataron las mejores prácticas que actualmente están dando resultados positivos en la administración de sus redes de computadores. También lo constituyen las recomendaciones

[15] Grupo de Investigación en Conectividad y Procesado de Señal

provenientes de entornos empresariales[16] para la elaboración de las guías de procedimientos. Estos elementos hacen que la propuesta cuente con una base que la sustenta y que genere confianza en la obtención de buenos resultados, una vez se tome la decisión de implantarla en la DSI.

- Los detalles de las guías de procedimientos y de las listas de chequeo propuestas fueron corroborados y validados por el administrador de la red de datos institucional quien a su vez es codirector del presente proyecto. Esto indica que en principio la propuesta de mejora al plan de gestión de red es aplicable al entorno de la red de datos de la UIS y que solo con base en la experiencia acumulada y en el análisis de los resultados obtenidos posteriores a la implantación de la propuesta, el planteamiento presentado es susceptible de ser reajustado a las condiciones cambiantes de la red de datos institucional.

- Se dio a conocer la existencia de modelos de referencia para la implantación de sistemas de gestión operativa y de servicios en organizaciones que ofrecen servicios de TI. En particular las recomendaciones del modelo ITIL permiten implantar planes de gestión de red bajo principios de calidad en organizaciones públicas o privadas que ofrezcan servicios de telecomunicaciones. El modelo ITIL está incluido dentro de la norma de gestión de calidad ISO 20000.

- Con base en trabajos anteriores, se asumió a la *administración y mantenimiento de la red de datos* como un proceso que realiza la DSI y se definió la instalación, monitorización y mantenimiento correctivo como subprocesos de este proceso. Con esto se dio un primer paso para la

[16] Hace referencia a las recomendaciones básicas para pruebas de conectividad emitidas por la empresa CISCO (ver anexo H) y las recomendaciones que a título personal proporcionó el ingeniero de Emtelco S.A (ver numeral 2.4 p. 60)

estructuración del marco de procesos de la DSI de acuerdo con los principios básicos del modelo ITIL y de las normas ISO versión 2000.

- En organizaciones que ofrecen servicios de TI, los planes de gestión de red no se centran solamente en la parte operativa (técnica y tecnológica) sino que se integran y se relacionan directamente en un marco de procesos, con las demás áreas que componen la organización y que en conjunto permiten ofrecer un servicio de telecomunicaciones.

- Se recomienda la implantación de un centro de atención al usuario que identifique a la DSI y que se constituya en el único lugar reconocido por la comunidad universitaria para el reporte de quejas, solicitudes de soporte técnico y recomendaciones relativas a los servicios que ofrece y soporta la DSI a través de la red de datos institucional.

- Se recomienda la implementación de una base de conocimiento donde se registren los incidentes y problemas detectados en la red de datos institucional con sus respectivas soluciones.

- Se recomienda dar continuidad al presente trabajo y abordar la gestión de seguridad ya que durante la realización del proyecto no se encontró evidencia de la existencia de un plan definido en este sentido.

6. BIBLIOGRAFÍA

[1] AMAYA L, Ortiz E, Silva, M, “Gestión de la red de datos institucional: documentación de la infraestructura de la red de datos correspondiente al edificio de administración” Trabajo de grado, Universidad Industrial de Santander 2003.

[2] CHAVEZ, C, CONTRERAS, J, Y RUEDA, D, Evaluación del desempeño de la red de datos institucional en los edificios de Ingeniería Eléctrica, laboratorio de alta tensión. Trabajo de grado, Universidad Industrial de Santander 2002.

[3] CISCO SYSTEMS. Guía del primer año CCNA 1 y 2. Pearson Educación S.A, Tercera edición 2005

[4] CISCO SYSTEMS. Internetworking technology handbook. Cap. 6, 7, 55. Disponible en Internet: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc. Acceso Agosto de 2005.

[5] GUZMAN CASTILLO PAOLA F. Análisis de la gestión de dispositivos administrables en la red de datos institucional. Trabajo de Investigación, Universidad Industrial de Santander 2005.

[6] GUZMAN, Paola, BARCO, Leydi, Gestión en redes de computadores, Grupo de Investigación de conectividad y procesado de señal CPS, Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones, Universidad Industrial de Santander.

[7] HARRINGTON, H. James. Mejoramiento de los Procesos de la Empresa. Santafé de Bogotá. Editorial McGraw-Hill Interamericana S.A., 1992.

[8] LINDSAY, William y EVANS, James. La Administración y el Control de la Calidad. Internacional Thomson editores, Cuarta edición. México, 2000.

[9] LOZANO, J, HITA, C, Nueva visión en la gestión de redes y servicios. Disponible en Internet: http://www.tid.es/presencia/publicaciones/comsid/esp/articulos/vol18/texto14.htm. Acceso Septiembre de 2005.

[10] MESA E, ROSAS L y TOBON D. Análisis estratégico para la División de Servicios de Información – DSI de la Universidad Industrial de Santander. Trabajo de grado. Universidad Industrial de Santander 2003.

[11] MUÑOZ, J, redes comunicaciones e Internet, CAP Planificación de Redes y gestión de redes. Disponible en Internet: www.fombella.org/astic2005/Volumen%20IV%20PDF/106.pdf. Acceso Agosto de 2005

[12]SOLARWINDS. Solarwinds.net Network Management Tools. Disponible en Internet: http://www2.solarwinds.net/support/docs/toolset.zip Acceso noviembre de 2005.

[13] SPENDOLINI, Michael. Benchmarking. Editorial Norma. Bogotá, 1995.

[14] SUN Microsystems. ITIL - IT Infrastructure Library. Las Mejores Prácticas para la Gestión de Servicios de TI en su Organización. Disponible en Internet. http://es.sun.com/services/itil/itil-diptico.pdf. Acceso Marzo de 2006.

[15] Support Portal. The ITIL and ISO 2000. Disponible en Internet: http://www.15000.net/. Acceso Marzo de 2006.

ANEXOS

ANEXO A. Descripción de la División de Servicios de Información

Misión

La División de Servicios de Información de la Universidad Industrial de Santander tiene como fin la administración y el desarrollo de la tecnología de la información en los ámbitos académico y administrativo, definiendo las políticas necesarias para la gestión del patrimonio documental y de la infraestructura de servicios informáticos institucionales, garantizando el adecuado uso de los recursos e impulsando la Innovación tecnológica de la Universidad.

Visión

La División de Servicios de Información de la Universidad Industrial de Santander se proyecta como una organización orientada a utilizar la tecnología de la información como vehículo para el hacer y el saber institucional promoviendo la participación de la comunidad universitaria en la generación y uso de soluciones informáticas de la más alta calidad técnica que faciliten el proceso de modernización institucional.

Funciones

- Administrar los recursos informáticos y computacionales.
- Dirigir y coordinar los sistemas de información para soportar los procesos académicos y administrativos.
- Asesorar y proporcionar servicios informáticos dentro del proceso de modernización institucional.
- Dirigir y coordinar la administración de documentos de la Universidad, conservando y custodiando el patrimonio documental.

Descripción Organizacional

Organizacionalmente la DSI, se divide en las siguientes áreas funcionales: Administración de Documentos, Laboratorio Luís Eduardo Arias y la sección de Tecnología Informática y Comunicaciones que a su vez contiene las áreas de Desarrollo de Software y Soporte de Infraestructura (Ver figura 4). A está última se encuentran adscritas las secciones de administración de la red de datos, seguridad, administración de servidores y administración de bases de datos encargadas de llevar a cabo todos los procesos de gestión de red.

El área de administración de red de datos y el Laboratorio Luis Eduardo Arias – LEA ejecutan y administran los subprocesos de instalación de equipos de red, monitorización y mantenimiento correctivo.

El personal encargado de realizar estos tres procesos se compone de un administrador de red y un grupo de técnicos de soporte.

El Administrador de red cumple las siguientes funciones específicas:

- Planear, activar, administrar y operar la red de datos de la Universidad Industrial de Santander y garantizar su correcto funcionamiento, en todos sus campus y sedes.

- Realizar y/o supervisar el mantenimiento preventivo y correctivo de la infraestructura de la red de datos.

- Asistir a los usuarios en la solución de los problemas que presente la red.

- Realizar el mantenimiento y actualización del inventario de usuarios con acceso permitido a la red institucional

- Mantener y custodiar la información en la red, y administrar las autorizaciones y denegaciones del acceso de cada uno de los usuarios a la red.

- Responder por el funcionamiento de las unidades de control conectadas a la red, de los servidores y sus opciones.

- Informar de los incidentes relativos a la seguridad de control de accesos, según los procedimientos establecidos para tal fin.

- Realizar labores de monitorización continua sobre los equipos y el software operativo de la red de datos institucional.

Los técnicos de servicios de información, cumple las siguientes funciones específicas:

Administrar y operar los servidores centrales de la Universidad Industrial de Santander y controlar el normal desarrollo de los procesos puestos bajo su cuidado.

- Atender a los usuarios en el proceso de impresión de la información de los sistemas institucionales.

- Dar soporte a las actividades de mantenimiento, actualización y documentación de las redes de datos de la Universidad.

- Coordinar las salas y laboratorios de informática adscritos a la División de Servicios de Información y garantizar el correcto funcionamiento de los servicios que desde allí se prestan a toda la Comunidad Universitaria.

- Solucionar problemas que se presenten por daño, desconfiguración o efecto de virus informático, instalando y configurando las opciones de software y

hardware de los equipos del área asignada, de acuerdo con los procedimientos establecidos.

- Atender y dar soporte directamente o vía telefónica, si es posible, a los problemas presentados en los equipos y redes de cómputo de la Comunidad Universitaria como bloqueos, virus, configuraciones de red, Internet, correo electrónico, impresoras, instalación de software, etc.

- Llevar a cabo el mantenimiento preventivo y correctivo, limpieza y reparación de los equipos del área asignada para evitar fallas de software y hardware y garantizar su buen funcionamiento.

- Brindar capacitación técnica al personal administrativo, profesores, empleados y alumnos de la Universidad, en el marco de los diferentes programas de capacitación coordinados con las diferentes dependencias.

- Controlar los turnos de trabajo asignados a los usuarios de las salas de informática y el consumo general de materiales utilizados en el proceso. Acuerdo Superior 067 de 1993

- Responder por la integridad de la información, los documentos, los sistemas que le sean asignados y cumplir con los procedimientos de seguridad. Acuerdo Superior 067 de 1993

- Controlar el almacenamiento y préstamo de las publicaciones, documentos y elementos propios del área de trabajo, de acuerdo con los procedimientos establecidos. Acuerdo Superior 067 de 1993.

- Garantizar que las condiciones ambientales de operación sean óptimas para los procesos. Acuerdo Superior 067 de 1993

Características de la red

La red WAN de la UIS ofrece conexión a todos los edificios de sus 4 campus metropolitanos (Central, Facultad de Salud, Bucarica y Guatiguará) y de sus sedes regionales (Barrancabermeja, Socorro, Málaga y Barbosa). Todos los edificios de los campus del área metropolitana se encuentran interconectados mediante enlaces de fibra óptica FastEthernet y GigaEthernet, mientras que las sedes regionales se conectan a la red LAN universitaria mediante enlaces de datos dedicados de 256Kbps para las sedes Málaga y Barbosa y de 512 Kbps para las sedes de Socorro y Barrancabermeja, contratados con la empresa Colombia Telecomunicaciones TELECOM.

Para la conexión a Internet la UIS cuenta con dos enlaces independientes tipo Clear Channel. Un enlace de 6 Mbps contratado con la empresa Colombia Telecomunicaciones - TELECOM el cual utiliza fibra óptica monomodo como último kilómetro y un enlace de 6 Mbps contratado con la Empresa de Telecomunicaciones de Bogotá ETB que utiliza un canal inalámbrico de microondas como último kilómetro. Estos enlaces operan con un protocolo de balanceo de carga para disponer de un ancho de banda agregado de 12 Mbps.

El enrutamiento hacia y desde la Internet lo realizan 2 routers marca CISCO, modelo 3640 y 3620, los cuales reciben y gestionan el canal de cada uno de los proveedores de acceso a Internet.

Para la protección de la red contra ataques externos, la red cuenta con un firewall marca CISCO, modelo PIX 515 situado entre la red LAN de campus central de la universidad y la red de los proveedores de acceso a Internet.

La optimización del uso de los canales de acceso a Internet se realiza mediante un equipo marca CISCO, modelo Cache Engine 505 que opera como proxy

transparente por hardware para la red, y configurado con un disco duro de 10GB para cache de páginas web y un puerto FastEthernet de conexión a la red.

Para administrar, controlar, monitorizar y filtrar según políticas institucionales el tráfico y navegación Web, la red dispone de un servidor WebSense Enterprise operando sobre un equipo con sistema operativo Microsoft Windows 2000.

El core de la red WAN de la UIS lo constituye un switch central multiprotocolo y multicapa, Extreme Networks de la seria BlackDiamond 6800, con una capacidad de conmutación total de 384 Gbps, enrutamiento/filtro/reenvío de 96 millones de paquetes por segundo (pps). Dispone de una capacidad máxima de 8 puertos 10-Gigabit, 128 puertos Gigabit 1000BASE-X, 168 puertos 10/100/1000BASE-T Gigabit y 256 puertos 100BASE-FX Fastethernet. Posee amplias capacidades de administración por CLI, SNMP, RMON y HTTP locales y remotos (Telnet).

Todos los edificios del campus principal y las sedes disponen de su propio centro de cableado para la interconexión con el centro de cableado principal y para la administración del segmento de red respectivo. Cada uno de estos centros de cableado cuenta con un switch de borde marca AVAYA modelo P333T/P334T, configurado con un puerto uplink de fibra óptica FastEthernet o Gigabit Ethernet y 24/48 puertos 10/100BaseTX autosensing para la conexión de concentradores de red (hub's), equipos servidores o estaciones de trabajo instalados en el edificio respectivo.

En cada uno de los edificios y sedes, la red está implementada utilizando la tecnología de cableado estructurado según la norma ANSI/EIA/TIA 568 A, categoría 5 y 5E, lo que permite que las estaciones en los puestos de trabajo operen hasta 100 Mbps.

La red de datos soporta el portal institucional además de portales Web de cada una de las escuelas dentro de la universidad, grupos de investigación, etc. Ofrece

también servicios de correo electrónico y provee servicios de red como DNS, Proxy´s.

Los principales servidores son:

El servidor que Soporta las aplicaciones informáticas de gestión de misión crítica de la universidad (Silicon Graphics modelo Origin2000)

El servidor de correo electrónico institucional (Silicon Graphics modelo Origin200.)

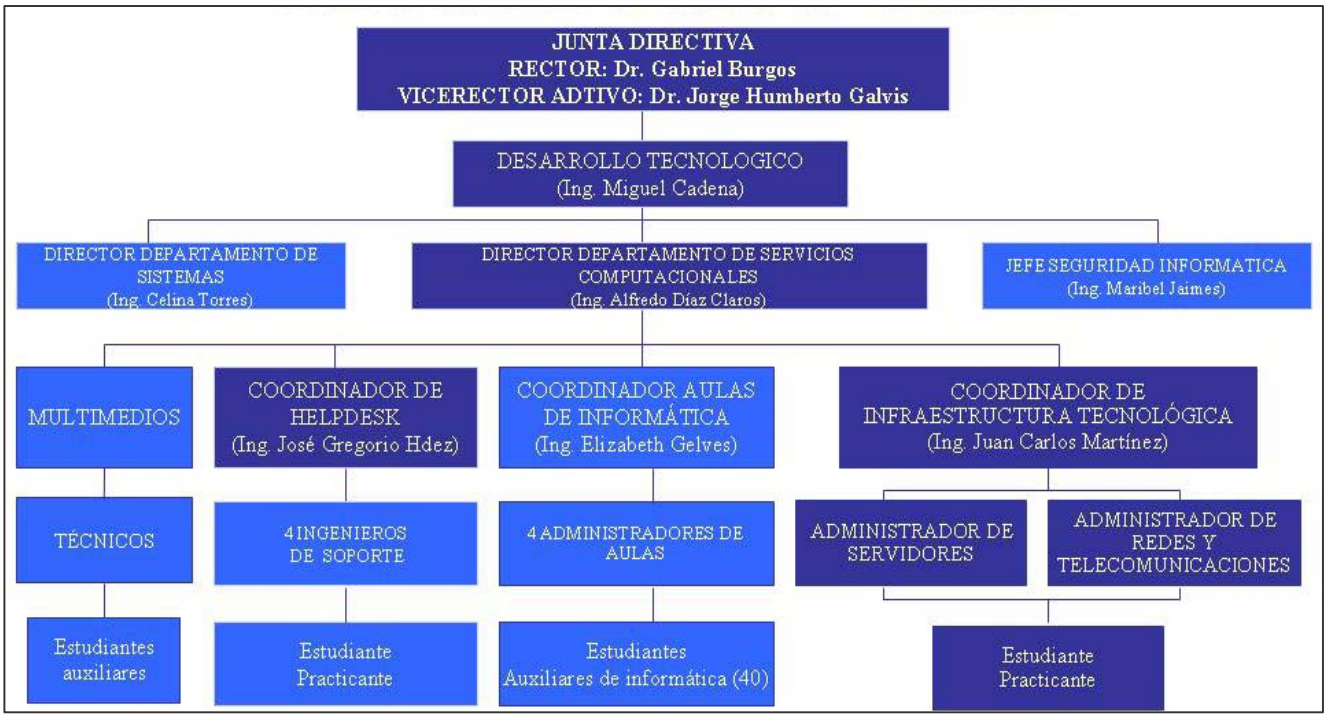
El servidor Web institucional (SUN Microsystems modelo ENTERPRISE 250 SERVER)

El servidor DNS primario de la red (Silicon Graphics modelo O2)

El servidor que soporta el sistema de intranet institucional (Silicon Graphics modelo 1450)

ANEXO B. Descripción del área de infraestructura tecnológica– UNAB

En la UNAB existe la sección de DESARROLLO TECNOLÓGICO que se ramifica en el *departamento de sistemas, seguridad informática* y el *departamento de servicios computacionales.* Este último se divide en cuatro dependencias entre las que se encuentran *Helpdesk* y la *Coordinación de infraestructura tecnológica* que tiene a su cargo la *Administración de redes y telecomunicaciones.*



Estructura organizacional de la Sección de Desarrollo Tecnológico UNAB

Fuente: Coordinación de infraestructura tecnológica UNAB.

Se identificó la sección de *desarrollo tecnológico* como la dependencia análoga de la DSI y la *administración de redes y telecomunicaciones* como la encargada de la administración de red. *Helpdesk* es importante porque brinda apoyo a los procesos que realiza la administración de red, además de atender todas las solicitudes y brindar soporte a los usuarios finales. Helpdesk es la sección encargada de recepcionar todas las quejas de los usuarios relacionadas con los servicios de la red, clasificarlas y delegar la solución a quien corresponda. Si el

problema está relacionado con software o hardware en equipos terminales lo resuelve helpdesk y si el problema está relacionado con conectividad lo resuelve la administración de la red y telecomunicaciones. Es decir, todas las solicitudes se dirigen a, y se canalizan a través de, helpdesk. En este sentido la dependencia encargada de administrar la red no es conocida por la comunidad universitaria.

Características de la red:

La red WAN de la UNAB ofrece conectividad a sus cuatro sedes. Su topología es una estrella extendida. El centro de la estrella se encuentra en el Campus el Jardín desde donde se interconecta el Campus del Tejar (o Instituto Caldas), el Campus el Bosque (Facultades de Salud) y Campus Terrazas (o CSU- Campus de Servicios Universitarios), a través de enlaces propietarios de fibra óptica, utilizando tecnología Gigabit Ethernet (1000 Mbps).

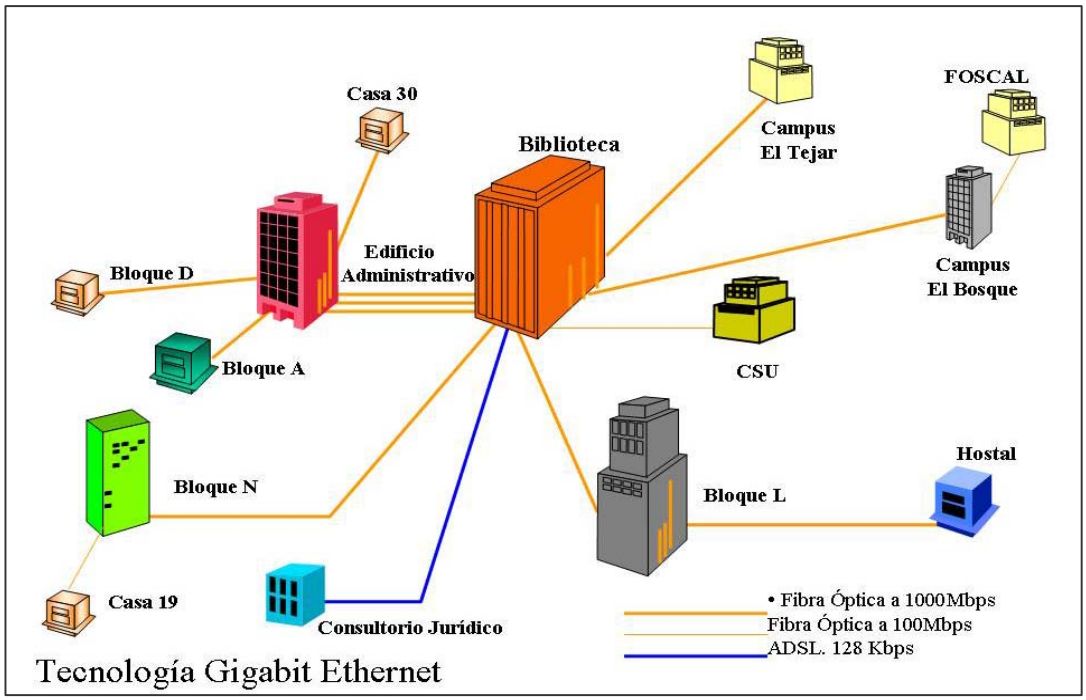
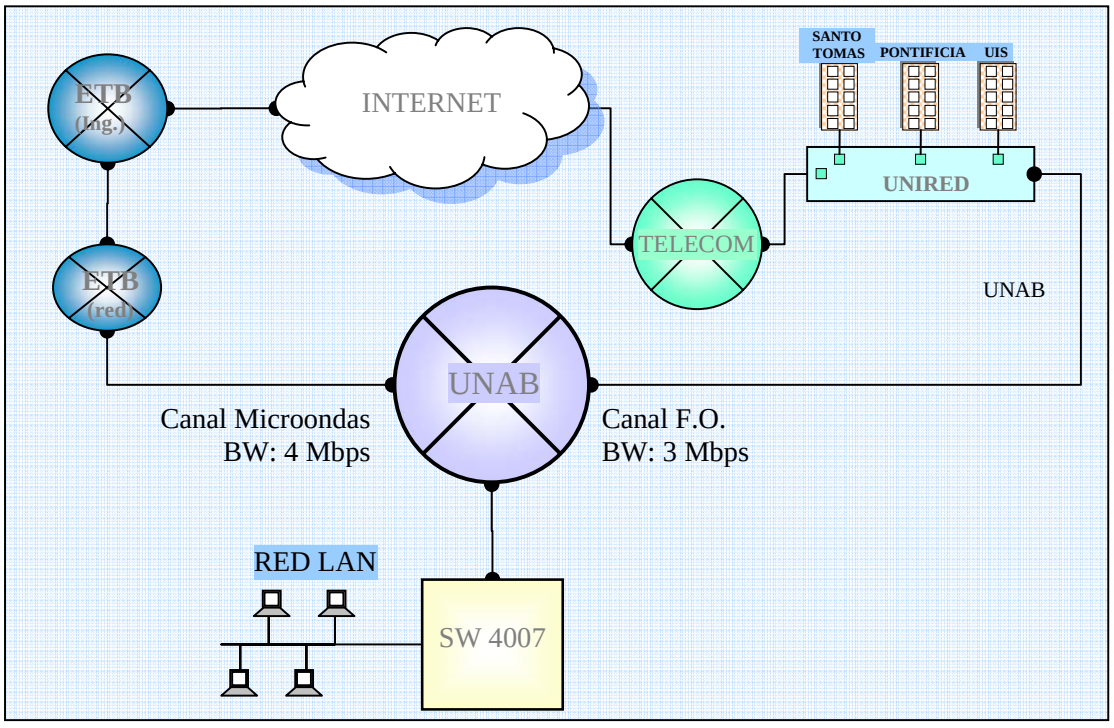


Diagrama de la red de datos institucional de la UNAB

Fuente: Coordinación de infraestructura tecnológica UNAB.

La misma tecnología se usa a nivel de backbone. La interconexión de segmentos de nivel dos se hace con fibra óptica a 100Mbps (Fast ethernet) Solamente el enlace con el consultorio jurídico lo realiza con tecnología ADSL a 128 kbps. Además cuentan con una red inalámbrica que provee conectividad dentro del campus central.

Para la conexión a Internet cuenta con dos enlaces dedicados. Un enlace de 4Mbps que utiliza un canal de microondas contratado con la Empresa de Teléfonos de Bogotá - ETB y un enlace de 3Mbps que utiliza un canal de fibra óptica que le interconecta con el núcleo de UNIRED[17] y a su vez le permite llegar a Internet a través de las redes de la empresa Colombia Telecomunicaciones – Telecom.



Esquema de conexión a Internet de la UNAB

Fuente: Coordinación de infraestructura tecnológica UNAB

El núcleo de la estrella extendida de la red lo componen un switch 3Com capa 2 acompañado de un switch capa 3 que ofrece el direccionamiento entre VLANs.

[17] Red de Universidades del Área Metropolitana de Bucaramanga

La red de datos soporta los portales institucionales (Web, WebCT, UNABTecnológica, estudiantes, cupones, Intranet, Futurosu, Uniempresarial, Sobresaltos, y Periódico 15). Ofrece también el servicio de correo electrónico con capacidad para 8000 usuarios y provee servicios de red como: LDAP, DNS, PROXY's, DHCP's y WINS. El área de infraestructura tecnológica también se encarga de la administración de servidores, donde tiene a su cargo más de 15 máquinas con plataformas SUN – SOLARIS, IBM – AIX.

Entre las políticas internas se tiene:

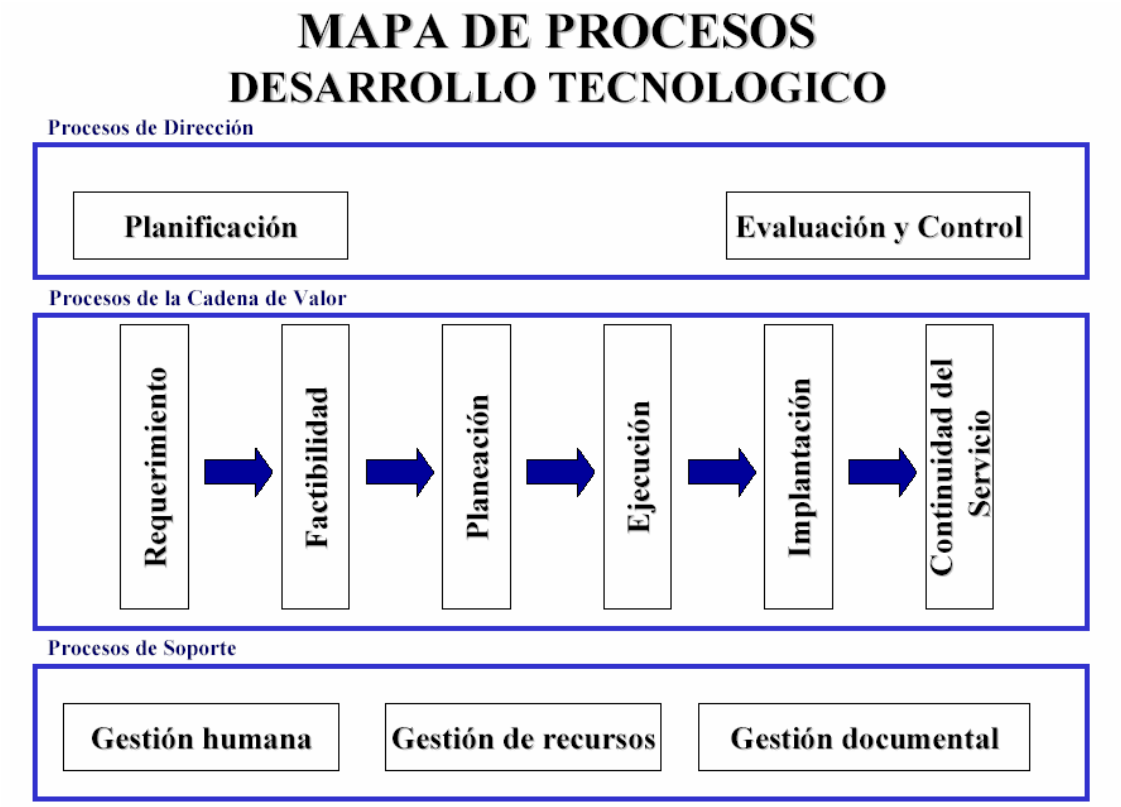
- Solo se permite el uso de protocolos FTP y HTTP.
- Hay libertad para visualizar contenido Web.
- Todos los dispositivos que ofrecen conectividad a la red LAN (Switches, routers) son de marca 3Com, para el enrutamiento hacia Internet se tiene un router CISCO 3660.
- El área de infraestructura tecnológica cuenta con tres profesionales (Administrador de red, administrador de servidores y Coordinador) y un estudiante de práctica. Para la comunicación entre el administrador y el personal en campo cuentan con radios intercomunicadores de corta alcance.

Toda la organización "Desarrollo Tecnológico", trabaja bajo el esquema de gestión de calidad ISO 9001:000, para lo cual tienen documentados los procesos, procedimientos, instructivos, matriz de clientes, formatos, caracterizaciones y demás.

En adelante se mostrarán los aspectos relevantes relacionados con los subprocesos de instalación, monitorización y mantenimiento preventivo.

Instalación

- En conectividad LAN, sólo utilizan dispositivos marca 3Com.
- Todas las solicitudes de nuevos equipos para cualquier sección dentro de la UNAB se realizan a través del área de *Infraestructura tecnológica*.
- Una vez adquiridos e instalados los nuevos dispositivos se asignan al inventario de infraestructura tecnológica, quien a su vez se encarga de su administración.
- Infraestructura tecnológica maneja la administración lógica de la red.



Mapa de procesos de la sección de Desarrollo Tecnológico UNAB

Fuente: Coordinación de infraestructura tecnológica UNAB

- El subproceso de instalación esta enmarcado dentro de una secuencia global (Cadena De valor) que soporta todos los procesos dentro de la organización de

Desarrollo Tecnológico, la cual comprende las etapas de requerimiento, factibilidad, planeación, ejecución, implantación y continuidad del servicio.

- La mayoría de los procesos, procedimientos y actividades están documentados y definidos.

Monitorización

- No cuentan con una herramienta unificada para la monitorización de dispositivos de red. En contraste cuentan con diversas aplicaciones de software para la monitorización:
  - Software propietario de los Switches 3com: Permite ver estado de los puertos y trafico en cada uno de ellos.
  - Nagios (FREE): Software que permite ver el estado de los dispositivos activos. Permite generar alarmas vía e-mail al personal encargado de la administración de red cuando un dispositivo sale de operación.
  - MRTG: Monitoriza los enlaces de Internet. Muestra gráficas de utilización vs. tiempo y el tráfico de entrada y salida.
  - Software propietario (UNAB) desarrollado por el administrador de servidores: Permite la monitorización de servidores y visualiza el estado de variables como: Carga de la CPU, número de usuarios swap, entre otros. Muestra el estado de todos los servidores en una pantalla y permite la generación de alarmas vía e-mail o beeper, cuando alguno presenta alguna anomalía. Tiene definidos los niveles de alarmas para cada variable y se interpretan en lenguaje de colores. También ofrece la posibilidad de llevar históricos de las variables monitorizadas.

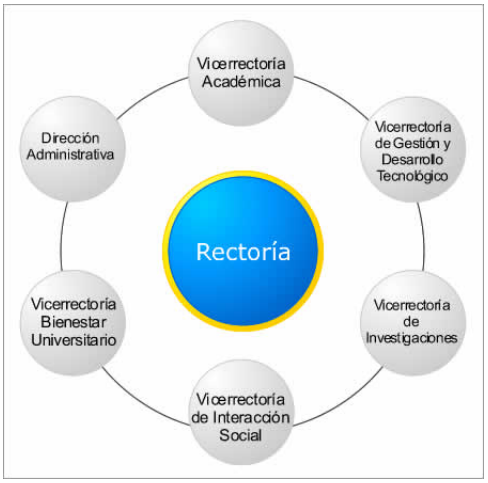
Mantenimiento Correctivo

- Todas las solicitudes se canalizan a través de HelpDesk. La sección que administra la red es transparente a los usuarios.

- Los problemas de estaciones finales los soluciona la dependencia “HelpDesk“ y los problemas de red los soluciona “Infraestructura tecnológica”.
- HelpDesk recibe la solicitud y la remite a quien le corresponda solucionarla. Si por alguna razón las solicitudes llegan directamente a la dependencia “Infraestructura tecnológica” ellos la reciben y la remiten al encargado de la solución. Con ello se evita que el usuario sea quien tenga que indagar entre dependencias en busca de la persona idónea para solucionar sus problemas.
- Poseen un software libre - EXO PHP- configurado a la medida de las necesidades de la UNAB con el que lleva control de las actividades de mantenimiento correctivo. Se registran todos los pasos y personas que intervienen desde el momento de la solicitud del usuario hasta la solución final. Se registra el tipo de problema, el encargado de solucionarlo y los comentarios de quienes participaron en la solución. Al final el usuario valida la solución. Esta herramienta está disponible en la Web.

ANEXO C. Descripción las área de Infraestructura y de Conectividad – UP

La Universidad de Pamplona – U.P cuenta con seis Vicerrectorías, dentro de la Vicerrectoria de Gestión y Desarrollo Tecnológico se encuentra la dependencia Plataforma Universitaria, encargada de llevar a cabo la administración de la red de datos entre otras funciones. Análoga a la DSI en la UIS.



Plataforma Universitaria trabaja bajo un esquema de gestión de calidad Institucional y tiene bajo su cargo los siguientes procesos que se encuentran enmarcados dentro de un mapa de procesos específicos que esquematiza la interacción y la clasificación de los mismos.

- Comercialización, diagnóstico y diseño de propuestas para la elaboración de aplicativos informáticos, implementación de redes de datos y elaboración de contenidos virtuales.
- Concepción, elaboración, construcción y transición de soluciones de aplicativos empresariales y de misión critica especifica.
- Diseño y elaboración de escenarios, objetos y contenidos multimediales basados en red.
- **Diagnóstico, análisis e implementación de servicios de conectividad.**
- Capacitación y apoyo post venta.
- Gestión de recursos de plataforma Universidad de Pamplona.

Plataforma Universitaria cuenta con el área denominada Infraestructura y un grupo vinculado a esta denominado Conectividad, como los encargados de administrar y ejecutar el proceso "**Diagnóstico, Análisis e Implementación de Servicios de Conectividad**" proceso que incluye la administración de la red de datos institucional.

Infraestructura es el Área encargada del despliegue en producción de los desarrollos y administración de la plataforma de hardware, software y la conectividad requerida.

Para llevar a cabo este proceso se cuenta con una serie de fases que se deben cumplir para realizar las actividades pertinentes y prestar el servicio solicitado dentro o fuera de la Universidad, estas fases incluyen los subprocesos de instalación, monitorización y mantenimiento correctivo.

Fases

- Diagnóstico
- Análisis y Diseño
- Elaboración de Planos
- Montaje e Implementación
- Certificación y Entrega
- Medición Análisis y Mejora
- Seguimiento

El personal a cargo de este proceso esta compuesto por un equipo de ingenieros de sistemas y electrónicos quienes están organizados para desarrollar los diferentes proyectos relacionados con infraestructura de red y conectividad, existe un líder Funcional y los demás son analistas de infraestructura.
Actualmente el grupo de trabajo está dividido en dos equipos:

Tres personas dedicadas a la monitorización de servidores, asignación de direcciones IP, Monitorización de equipos activos de red, Seguridad y autenticación, adscritos al área de Infraestructura.
Los otros tres profesionales desarrollan trabajos de diseño, implementación y mantenimiento de redes de datos y están adscritos al grupo de Conectividad.
Sin embargo todos los integrantes están capacitados y autorizados para realizar cualquiera de los trabajos relacionados con el proceso de **Diagnóstico, Análisis e Implementación de Servicios de Conectividad**".

Todas áreas dentro de Plataforma Universitaria cuentan con un listado maestro de documentos que contiene los procedimientos, guías, instructivos, protocolos a seguir de acuerdo al tipo de servicio requerido. Esto incluye a las secciones de conectividad y de infraestructura.

Características de la red:

- La intranet trabaja a una velocidad de 10/100Mbps según los estándares internacionales.
- Los centros de comunicación (IDFs) en cada edificio del campus central, se conectan utilizando fibra óptica.
- La red WAN de la U.P ofrece conectividad a sus 7 sedes (Campus central, Casa Aguda Gallardo, la Casona, Casa Domus, Cúcuta, Bucaramanga y Bogotá.
- Los edificios de la sede central en el Campus Km 1 vía Bucaramanga se conectan con fibra óptica.
- La Casa Águeda Gallardo se conecta por medio de enlace inalámbrico con tecnología 802.11b.
- La Casona y la Casa Domus se conectan por medio de enlace inalámbrico con tecnología 802.11g.
- Las sedes de Cúcuta y Bogotá se conectan usando la tecnología Frame Relay aprovechando la infraestructura del proveedor ETB.

- Las sedes de Villa del Rosario y Bucaramanga son independientes, se aprovisionan de Internet ADSL con TELECOM y TELEBUCARAMANGA respectivamente. Para Villa del Rosario se tienen dos enlaces de 1024Kbps y para Bucaramanga un enlace de 512Kbps.
- Existen 29 servidores marca SunMicrosystems, Cisco, IBM y HP.
  18 servidores gama alta:
  7 servidores para base de datos.
  7 servidores de aplicaciones.
  2 servidores para seguridad.
  1 servidor para almacenamiento.
  1 servidores Proxy.
  11 servidores gama baja:
  Prestan Servicio de correo institucional.

- La seguridad la realiza un Firewall Cisco PIX 515 y Firewall Sunblade 100.
  En los servidores se implementa la seguridad del Sistema Operativo, usando GnuPG y Certificados SSL y comunicaciones seguras protocolo SSH.

- Proveedor de equipos y materiales de red a cargo de la empresa Unión Eléctrica que es proveedora de equipos 3com.

Subproceso de instalación

- Cuando se desea realizar una nueva instalación de infraestructura de red, se debe seguir un orden para desarrollar el proyecto, antes de realizar la instalación se necesita realizar un estudio de factibilidad y llevar a cabo un proceso de adquisición de los equipos necesarios.

- La dependencia o persona que requiera la instalación de un nuevo punto(s) de red debe dirigirse a la dependencia Recursos Físicos y Apoyo Logístico, encargada de recibir y tramitar todos los mantenimientos (de conectividad,

eléctricos, obras civiles, etc.) de la universidad así como de canalizar las solicitudes de usuarios para la instalación de infraestructura de cualquier tipo. Para nuevas instalaciones se recibe la solicitud del usuario, asigna la dependencia responsable de ejecutar dicho trabajo.

- En el caso de conectividad Recursos Físicos y Apoyo Logístico establece el contacto con Infraestructura y/o conectividad a quienes se remite la solicitud del usuario con el fin de realizar las pruebas de factibilidad en el sitio de la nueva instalación, posteriormente el personal de Infraestructura pasa un reporte con los requerimientos necesarios a Recursos Físicos, incluyendo si se necesitan realizar trabajos adicionales independientes de conectividad (instalaciones eléctricas, adecuación de plan física, ente otros), en dado caso Infraestructura pasa su propia solicitud a Recursos Físicos para que se asigne un responsable de realizar estos trabajo.

- Infraestructura realiza las cotizaciones relacionadas con los dispositivos y herramientas de conectividad. El rector es el encargado de dar el visto bueno a la nueva instalación con todos los materiales necesarios para su ejecución.

- Todos los materiales llegan y salen siempre de la sección denominada Adquisiciones y Almacén encargada de realizar la disponibilidad presupuestal y continuar con el proceso de adquisición hasta recibir, entregar e inventariar los materiales a la dependencia que los va a utilizar.

- Todos los trabajos de instalación los realiza el personal adscrito a la dependencia de Infraestructura, cuentan con los instrumentos y la capacitación necesaria para ejecutar dicho trabajo, de esta forma ninguna instalación de conectividad al interior de la universidad es contratada con personal externo.

- Actualmente la dependencia Infraestructura tiene como política la instalación de solo switches como equipos de red.

- Adicionalmente la Universidad de Pamplona ofrece soluciones de conectividad a organizaciones y entidades externas por medio de la dependencia de Infraestructura, en este caso se firma un contrato con el interesado y se le da soporte durante todo el proceso de instalación y se ofrecen servicios de soporte de acuerdo a las necesidades del interesado. La ejecución de los trabajos operativos externos se rigen bajo las mismas políticas de calidad de los trabajos al interior de la Universidad.

- Existe documentación de soporte para la realización del subproceso de instalación esta se encuentra dentro del listado maestro de documentos.

Subproceso de monitorización

- Actualmente la U.P cuenta con herramientas básicas de monitorización de equipos de red, específicamente utiliza el software propietario de los dispositivos activos 3com (Network Supervisor 3com) y el software para la monitorización de las antenas que ofrecen conectividad de las distintas sedes en el área municipal, esto dificulta llevar registro y control del estado, configuración y comportamiento de la red de datos.

- Las herramientas utilizadas impiden llevar una monitorización continua del desempeño y rendimiento de la red y solo permiten la visualización de variables de estado y configuración. Permiten la visualización gráfica de la topología de red ubicando cada dispositivo de acuerdo a su dirección en la red e identifica las direcciones de los equipos asociados a cada puerto de los dispositivos activos, esto permite generar un mapa general de conexiones gracias a la unificación en marca de los dispositivos.

- Mediante el proceso de monitorización es imposible anticiparse a posibles fallas en los dispositivos o enlaces, por esta razón se profundiza en un mantenimiento correctivo.

- El mantenimiento preventivo se realiza por medio de supervisiones programadas, que buscan principalmente identificar puntos dentro de la red susceptible de mantenimiento o reemplazo, básicamente se buscan los segmento de red más antiguos.

- Adicionalmente todos los equipos de red están asegurados y cualquier inconveniente de hardware es remitido directamente a 3com.

- La documentación generada en este subproceso es escasa, no se tiene un histórico ni clasificación de eventos, tampoco un procedimiento a seguir para el mantenimiento preventivo remoto, en parte debido a las limitantes con las hermanitas de monitorización.

Subproceso de Mantenimiento Correctivo

- La Dependencia Recursos Físicos y Apoyo Logístico también se encarga de canalizar las solicitudes de los usuarios referentes a cualquier tipo de problema, incluyendo solicitudes con respecto a inconvenientes en el servicio de red.

- El usuario se comunica vía telefónica con dicha dependencia y reporta su queja, en este momento se abre un caso con la solicitud y se remite a la dependencia o personal encargado de solucionar este tipo de inconvenientes.

- En el caso de problemas de conectividad se remiten las solicitudes a Infraestructura quienes acuden al lugar a prestar soporte en el área de conectividad. Si la solución involucra soluciones fuera del área de conectividad

Infraestructura redirige el caso de nuevo a Recursos Físicos para que se asigne otro responsable. Básicamente el personal de Infraestructura realiza pruebas de conectividad en la estación afectada y en los dispositivos activos relacionados con el área afectada.

- Una vez finalizado el trabajo el usuario valida la solución y se diligencia una ficha de trabajo en la cual se consigna la fecha de solicitud, de culminación, el nombre del responsable de la solución, el nombre del solicitante y se califica el trabajo realizado.

- Los trabajos son realizados con base en la experiencia de los Ingenieros y no cuentan con guías de procedimientos. La documentación generada con respecto a los subprocesos de mantenimiento preventivo y correctivo es escasa. Sin embargo existen documentos de soportes de ciertos procedimientos relacionados con el soporte a usuarios dentro del listado maestro de documentos.

- No se lleva registro de las soluciones encontradas en los problemas más relevantes relacionados con conectividad.

ANEXO D. Descripción de las plantillas de presentación de los subprocesos

Plantilla de Presentación

Es la introducción de cada subproceso, la cual contiene su objetivo, características, proveedores e insumos, el resultado que se obtiene del mismo, los clientes internos y externos, y los subprocesos relacionados (Véase Figura 1).

En esta plantilla se encuentran los siguientes ítems:

1. **Nombre del proceso:** Este campo contiene el nombre del proceso al cual pertenece el subproceso.

2. **Título del Manual:** Contiene el tipo de manual y el área de aplicación del mismo.

3. **Nombre del Subproceso:** Contiene el nombre del subproceso.

4. **Código:** Muestra el código asignado a cada subproceso de acuerdo con la codificación previamente establecida.

5. **Elaboró:** Nombra a los encargados del levantamiento, el análisis y la documentación del subproceso.

6. **Revisó:** Nombra la(s) persona(s) encargadas de verificar el correcto levantamiento del subproceso.

7. **Aprobó:** Hace referencia a la(s) persona(s) con el grado de autoridad y conocimiento necesarios para aprobar el subproceso documentado.

8. **Fecha de Creación:** Muestra la fecha en la cual se documenta por primera vez el subproceso.

9. **Última Modificación:** Muestra la fecha en la cual se modifica por última vez el subproceso.

10. **Objetivo del subproceso:** Explica el propósito que se pretende cumplir con el subproceso.

11. **Características del subproceso:** Contiene los siguientes detalles:

- Aplicabilidad: Hace referencia al tipo de usuario al cual va dirigido el subproceso.

- Periodicidad: Se refiere a la frecuencia con la que se realiza el subproceso.
  - Frecuente: Cuando el subproceso se presenta a diario.
  - Esporádico: Cuando el subproceso se presenta eventualmente.
  - Periódico: Cuando el subproceso se presenta en periodos determinados.

- Dependencia Tecnológica: Indica los requerimientos de tecnología para desarrollar el subproceso.
  - Manual: Todo el desarrollo operativo del subproceso se realiza directamente por parte del funcionario correspondiente, sin participación directa de los Sistemas de Información.
  - Semiautomatizado: En el desarrollo operativo del subproceso participan directamente tanto el funcionario correspondiente como los Sistemas de Información.
  - Automatizado: Todo el desarrollo operativo del subproceso se realiza directamente por parte de los Sistemas de Información

12. **Proveedores:** Son las personas y entidades que entregan los recursos necesarios para desarrollar el subproceso.

13. **Insumos:** Son los recursos (información o elementos físicos) requeridos para el inicio y desarrollo del subproceso.

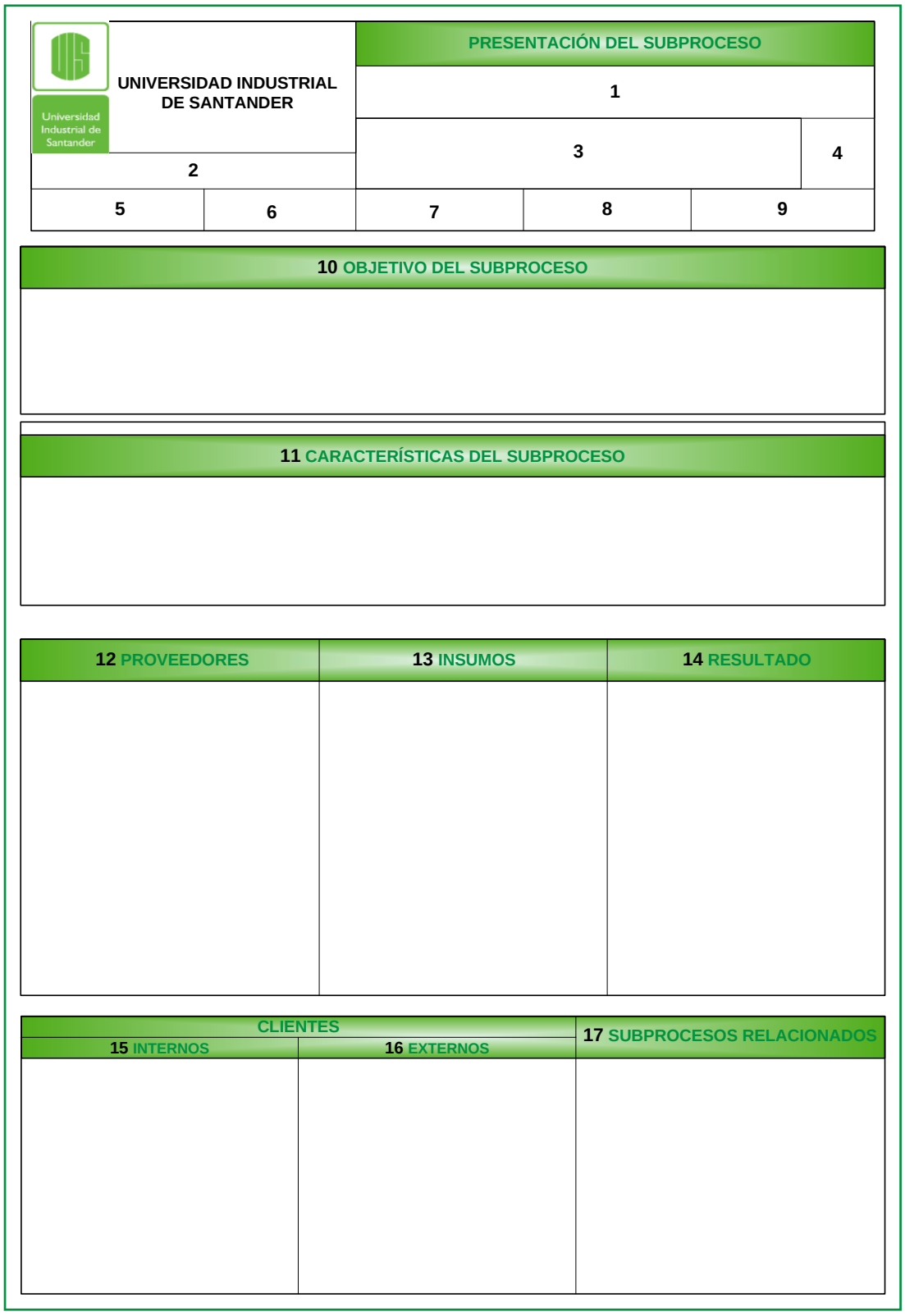
14. **Resultado:** Corresponde a los resultados que se obtienen al finalizar el subproceso, ya sean tangibles o intangibles.

15. **Clientes Internos:** Son las entidades que al interior de la División de Servicios de Información requieren de los resultados arrojados por el subproceso.

16. **Clientes Externos:** Son las entidades externas a la División de Servicios de Información que requieren de los resultados arrojados por el subproceso.

17. **Subproceso Relacionados:** Contiene los subprocesos que suministran o a los que se les suministran insumos, bien sea internos o externos a la División de Servicios de Información.

Figura 1. Plantilla de Presentación



Plantilla del Subproceso

Esta plantilla contiene el diagrama de flujo del subproceso, el cual se lee de arriba hacia abajo, siguiendo la secuencia de actividades.

La descripción es el soporte textual de las actividades que se presentan en el diagrama de flujo del subproceso. Adicionalmente, cada una de estas actividades menciona el responsable y el respaldo normativo (Véase Figura 2).

La plantilla del subproceso se encuentra distribuida de la siguiente manera:

1. **Elaboró:** Nombra a los encargados del levantamiento, el análisis y la documentación del subproceso.

2. **Revisó:** Nombra la(s) persona(s) encargadas de verificar el correcto levantamiento del subproceso.

3. **Aprobó:** Hace referencia a la(s) persona(s) con el grado de autoridad y conocimiento necesarios para aprobar el subproceso documentado.

4. **Nombre del proceso:** Este campo contiene el nombre del proceso al cual pertenece el subproceso.

5. **Nombre del Subproceso:** Contiene el nombre del subproceso.

6. **Título del Manual:** Contiene el tipo de manual y el área de aplicación del mismo.

7. **Código:** Muestra el código asignado a cada subproceso de acuerdo con la codificación previamente establecida.

8. **Página:** Muestra el número de páginas de esta plantilla.

9. **Fecha de Creación:** Muestra la fecha en la cual se documenta por primera vez el subproceso.

10. **Última Modificación:** Muestra la fecha en la cual se modifica por última vez el subproceso.

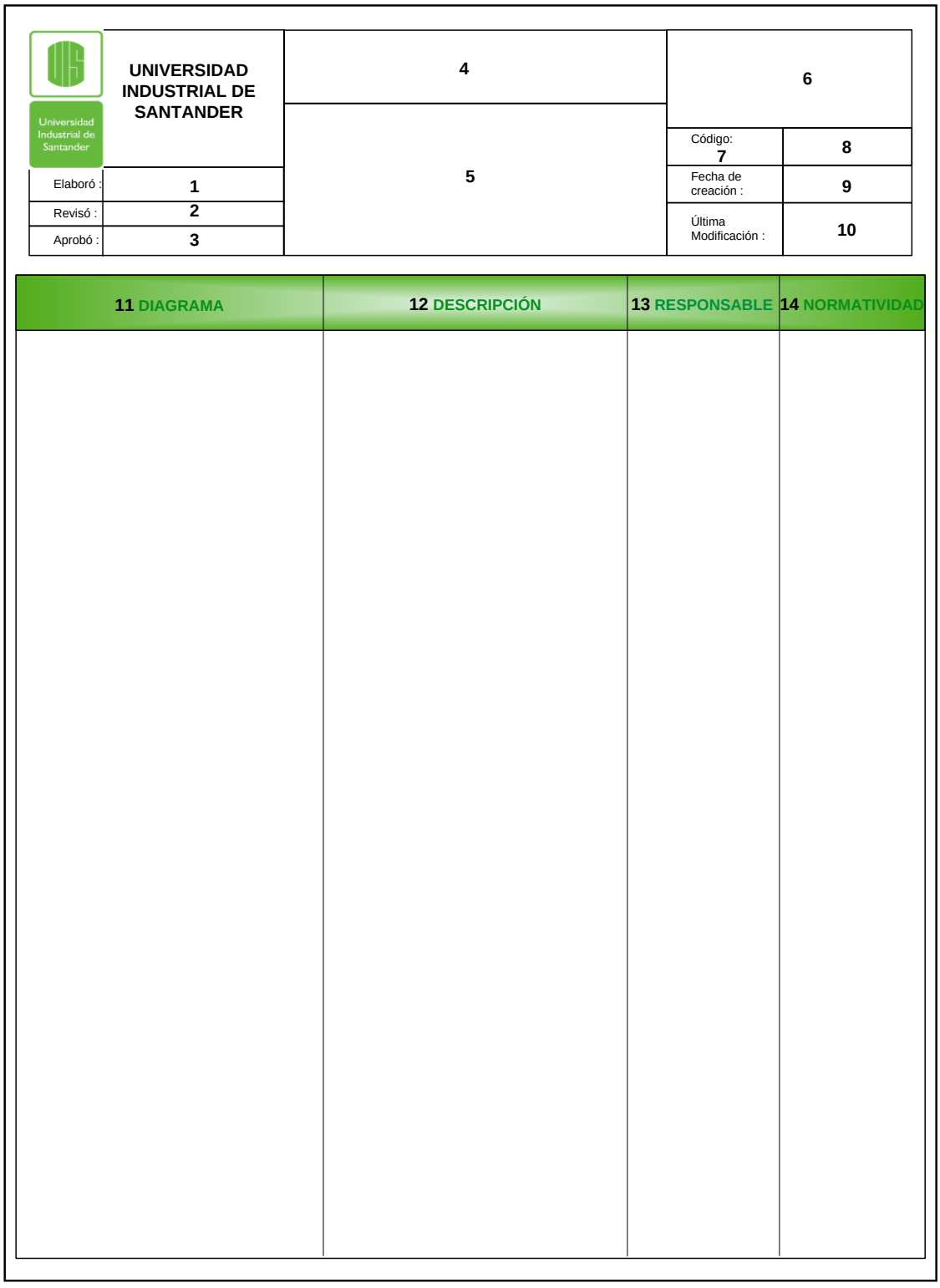
11. **Diagrama:** Contiene la representación gráfica de la sucesión en que se realizan las operaciones del subproceso.

12. **Descripción:** Contiene la descripción textual de las actividades involucradas en el diagrama de flujo del subproceso.

13. **Responsable:** Son las personas encargadas de la ejecución de cada una de las actividades del subproceso.

14. **Normatividad:** Relaciona la normatividad que soporta las actividades del subproceso.

Figura 2. Plantilla del subproceso - Diagrama de actividades

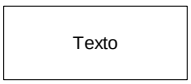
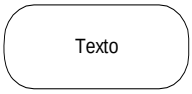
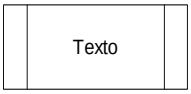
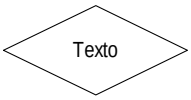


Universidad Industrial de Santander	UNIVERSIDAD INDUSTRIAL DE SANTANDER	4	6	
		5	Código: 7	8
Elaboró :	1		Fecha de creación :	9
Revisó :	2		Última Modificación :	10
Aprobó :	3			

11 DIAGRAMA	12 DESCRIPCIÓN	13 RESPONSABLE	14 NORMATIVIDAD

Simbología Utilizada en las Plantillas de Subprocesos

En el presente Manual Operativo se utilizan las siguientes convenciones:

SÍMBOLO	NOMBRE	SIGNIFICADO
	RECTÁNGULO	Indica actividades manuales.
	RECTÁNGULO CON BORDES REDONDEADOS	Indica actividades realizadas con el apoyo del Sistema de Información.
	RECTÁNGULO CON BARRAS	Indica que el subproceso se relaciona con otros subproceso documentados.
	DIAMANTE	Indica toma de decisión. Tiene dos salidas: SI ó NO.
	ÓVALO	Indica el final del subproceso respectivo.
	CÍRCULO	Indica la salida de una operación y sirve como conector a la entrada de la operación secuencial.
	FLECHA	Indica la dirección y el orden que corresponde a los pasos del subproceso.
	PENTÁGONO	Conector que indica cambio de página.

Sistema de Codificación

La codificación es un sistema que permite identificar de manera ágil el tipo de subproceso y el proceso al cual pertenece, facilitando de esta manera un control adecuado y practico del Manual Operativo.
La codificación utilizada para cada uno de los procedimientos del Manual Operativo es la siguiente:

XY . # P. # s

Donde:

X: Identifica el Área Administrativa y consta de dos letras. El Área Administrativa se identifica con las letras SI, refiriéndose a la División de Servicios de Información.

Y: Identifica la Sección dentro de la División de Servicios de Información a la cual pertenece el subproceso. La letra A hace referencia a la Sección de Administración red de datos.

P: Número de clasificación general por tipo de Proceso según el Mapa de Procesos identificado para la Sección. Este número consta de dos dígitos.

s: Número del subproceso dentro de cada Proceso, el cual consta de dos dígitos.

Esta codificación mantiene los parámetros establecidos por la Universidad.

ANEXO E. Guía de Procedimientos y descripción de la Lista de Chequeo del Subproproceso de Instalación

I. INFORMACIÓN SWITCH AVAYA P33X

Configuración Switch Avaya P33x

1. *Medios de Administración y configuración*

- **Consola**

Configuración parámetros conexión Hyperterminal:

Elegir puerto de comunicaciones serial (COM1, COM2)

Bits por segundo: 9600

Bits de datos: 8

Paridad: NO

Bit de Parada: 1

Control de Flujo NO

- **Telnet**

Acceso mediante protocolo Telnet. El dispositivo debe estar configurado con una dirección IP valida dentro de la red para acceder remotamente.

- **Web**

Acceso en línea utilizando un navegador Web, se accede mediante la dirección IP del Switch. Además es necesario tener instalado el plug-in requerido en la estación de administración.

2. *Parámetros por defecto del Switch*

Dirección IP: 149.49.32.134

BootP Mode: Never

Gateway por defecto: 0.0.0.0

Management PC SLIP IP address: 192.168.10.2

ID VLAN de administración: 1

Spanning Tree: Enable

Modo TFTP: Limited
Servidor TFTP: 0.0.0.0
Nombre del archivo (TFTP): viisa
Comunidades SNMP: Read-only → public
Read-write → public
Trap SNMP → public
Nombre de Usuario (Username): root
Contraseña (password): root

3. Características de la CLI (Command Line Interface)

Al acceder por consola o vía Telnet al switch se tienen 4 modos diferentes de operación en la CLI que permiten y restringen ciertas operaciones de configuración del switch.

- El modo de usuario sin privilegios solo permite visualizar variables y parámetros de configuración básicas del dispositivo (read-only)

  P33X-N>
  X depende del modelo del Switch
  N numero de Switches en la pila (Stack).

- El modo de usuario con privilegios permite visualizar toda la configuración y modificar los parámetros de operación del dispositivo. (read-write).

  P33X-N#

- El modo de administrador se utiliza para crear y administrar cuentas, contraseñas y niveles de acceso para los usuarios.
  En este modo también es posible acceder a los comandos de configuración para autenticación RADIUS (Remote Authentication Dial-In User Service).

P330-N(super)#

- El modo de configuración permite ejecutar comandos específicos que permiten modificar parámetros del dispositivo para operar en la capa 3 (Capa de red).

P330-N(super)#configure
P33X-N(configure)#

4. Guia de comandos

Convenciones para al uso de la guía de comandos

• Sintaxis del comando se visualiza en *cursiva.*

• Variables a ingresar se visualizan entre **<>**.

• Variables alternativas pero obligatorias están separadas por una barra vertical |.

• Caracteres alfanuméricos de dos o más palabras deben estar entre comillas invertidas “”.

Comando	Descripción
Configuración básica del Switch	
set welcome message <mensaje deseado>	Configurar el mensaje de bienvenida
hostname <texto deseado>	Cambiar nombre actual del prompt en el CLI. e.j: P330-N# **hostname “UIS Bucaramanga”** UIS Bucaramanga -N#
no hostname	Retornar los valores por defecto del prompt
Username <nombre del usuario> *password* <contraseña deseada> *access-type* <read-only | read-write | admin>	Configurar una cuenta de usuario con nombre, contraseña y nivel de acceso al dispositivo.
no username <nombre_usuario>	Remover una cuenta de usuario previamente creada
show username	Visualizar las cuentas de usuarios existentes
Otros comandos básicos	
clear screen	Limpiar la pantalla actual
configure	acceder al modo de configuración capa 3
ping <ip host remoto>	Enviar peticiones ICMP a cualquier otro nodo

Configuración de Parámetros del dispositivo	
set system name <nombre deseado>	Configurar un nombre para el dispositivo
set system contact <nombre del contacto>	Configurar una persona responsable (contacto) del dispositivo
set system location <ubicación>	Configurar la ubicación geográfica de dispositivo
Configuración de Parámetros de operación	
set device-mode <modo>	Configurar el modo básico de operación de un modulo Capa 2/ capa 3 (solo si el dispositivo soporta ambos modos) - Modos: Router – Switch opera con características de capa 2. Layer2 - Switch opera con características de capa 2 y 3.
show device-mode	Visualizar el modo de operación actual.
show system	Visualizar los parámetros del sistema.
show module	Visualizar la información del modulo.
Configuración de parámetros Ethernet Operación del Switch con características de la capa 2	
Show interface	Visualizar la configuración actual de dispositivo.
set interface <inband> <vlan> <dir_ip> <mascara>	Configurar la dirección IP del Switch. Inband: Nombre de la interfaz vlan: numero de la VLAN. La VLAN 1 es la VLAN de administración por defecto. dir_ip: Dirección IP del switch. mascara: Mascara de subred para la dirección IP del switch.
set ip route <red destino> <gateway>	Configurar una ruta estática. Red destino: Dirección IP de la red destino, si utiliza la dirección 0.0.0.0 indica cualquier destino (ruta por defecto). Gateway: Dirección IP de la puerta de enlace que le permitirá enrutamiento de paquetes fuera de a subred.

Configuración de puertos	
set port negotiation <Nºmodulo>/<Nºpuerto> *{enable|disable}*	Configuración de la velocidad de negociación, Auto-negociación (permite censar la velocidad de los dos dispositivos interconectados y ajustarse a la mejor velocidad soportada.
set port enable <Nºmod>/<Nºpuerto>	Habilitar um puerto (administrativamente).
set port disable <Nºmod>/<Nºpuerto>	Deshabilitar un puerto (administrativamente)
set port speed <10MB|100MB|1GB>	Ajustar la velocidad del puerto (10/100/1000Mbps).
set port duplex <Nºmod>/<Nºpuerto> {full|half}	Configurar en modo Full/half duplex un puerto 10-100BASE-T.
set port name <Nºmod>/<Nºpuerto> <nombre del puerto>	Configurar un nombre específico para un puerto.
set port flowcontrol {receive | send | all} <Nºmod>/<Nºpuerto> {off | on | proprietary}	Ajustar el modo de envío/recepción para el control de flujo de frames de un puerto Full duplex.
set port auto-negotiation-flowcontrol-advertisement <Nºmod>/<Nºpuerto> {no-flowcontrol|asym-tx-only|sym-only|sym-and-asym-rx}	Ajustar las notificación de control de flujo para un puerto Gigabit cuando esta configurado con la opción de autonegotiation.
set port level <Nºmod>/<Nºpuerto> <nivel>	Ajustar el nivel de prioridad de un puerto nivel: Nivel de prioridad de 0 a 7
show port <Nºmod>/<Nºpuerto>	Visualizar las características y estado de determinado(s) puerto(s).
show port flowcontrol	Visualizar información del estado de cada puerto relacionada con el control de flujo
Show port auto-negotiation-flowcontrol-advertisement	Visualizar las notificaciones del control de flujo para un puerto Gigabit usado con Autonegotiation
show cam <macaddr>/<Nºmod>/<Nºpuerto>]	Visualizar las entradas de la tabla CAM de un puerto específico.
clear cam	Limpiar (borrar) todas las entradas de la CAM
show autopartition <Nºmod>	Visualizar las características de autopartición
Configuración de VLAN`s	
show vlan	Visualizar las VLAN configuradas en el Switch
set vlan <ID vlan> *name* <nombre_vlan>	Crear una VLAN

clear vlan <ID vlan> *name* <nombre_vlan>	Borra las entradas de una VLAN. id_van: Numero ID de la VLAN nombre_vlan: Nombre asignado a la VLAN
set port vlan <Nº vlan > Nºmod>/<Nºpuerto>	Asignar una ID de VLAN a un puerto
set port static-vlan [Nºmod>/<Nºpuerto>] [Nº vlan]	Definir una VLAN estática a un puerto
clear port static-vlan [Nºmod>/<Nºpuerto>] [Nº vlan]	Borrar una VLAN estática configurada en un puerto
show port vlan-binding-mode	Visualizar las características del modo combinación de VLAN del puerto
set port vlan-binding-mode <port_list> <value>	Definir el método de encuadernación (binding) del puerto - port list: NºModulo/Nºpuerto value: • static – El Puerto soporta solamente las VLAN configuradas en ese puerto (VLAN estáticas) • bind-to-configured – El puerto soporta las VLANs configuradas en el dispositivo. • bind-to-all – El puerto soporta todo el rango de VLANs en el dispositivo.
set trunk <module/port> {off|dot1q}	Configurar un puerto como troncal (trunk), off : Configura el puerto como No-tagging dot1q: Especifica un Puerto Gigabit Ethernet IEEE 803.1Q. Puerto troncal
show port vlan-binding-mode	Visualizar las características del modo combinación de VLAN del puerto
show trunk	Visualizar información del modo troncal, modo de encuadernación (binding) y el identificador de VLAN de los puertos. Además y las VLANs permitidas en los puerto.
Comandos para almacenar, resetear y administrar la configuración del Switch.	
copy stack-config tftp <nombre archivo> <ip_tftp>	Almacenar la configuración actual del grupo de switches de la pila en un servidor TFTP remoto.

copy module-config tftp <nombre archivo> <ip_tftp> <module>	Almacenar la configuración de un switch especifico en un servidor TFTP
copy tftp stack-config <nombre archivo> <ip_tftp>	Descargar la configuración almacenada en el servidor TFTP a la pilas de switches
copy tftp module-config <nombre archivo> <ip_tftp>	Descargar la configuración almacenada en el servidor TFTP a un switch.
dir	Visualizar los archivos que han sido descargados al dispositivo.
nvram initialize {switch | all}	Resetear la memoria NVRAM, impone al switch los parámetros por defecto. switch: resetear solo los parámetros de la capa 2 all: resetear todos los parámetros de switch, incluida la configuración de capa 3.
show tftp upload status	Visualizar el estado y los detalles de la descarga/carga del archivo de configuración.
Comandos SNMP	
set snmp community <read-only|read-write|trap> <comunidad deseada>	Modificar las comunidades snmp del switch.
set snmp retries <numero intentos>	Ajustar el número de intentos para peticiones snmp.
set snmp timeout <number>	Ajustar el tiempo de espera para cerrar sesión snmp inactiva.

II. DESCRIPCIÓN SUBPROCESO DE INSTALACIÓN

1. Configuración básica del dispositivo.

Cargar el archivo básico de configuración desde el software de emulación de terminal (Hyper Terminal).

Archivo para la configuración básica de un switch departamental

set welcome message "Mensaje inicial"
set system name "Nombre de identificación de Switch"
set system contact "Responsable del Switch"

set system location "Ubicación del Switch"

Username <root> *password* <contraseña deseada> *access-type* <read-write | admin>

! Configuración de parámetros característicos del switch y su respectiva contraseña de !acceso para la administración por consola, telnet y vía Web.

set interface inband 1 <direccion IP del switch> <mascara de subred>

!Configuración de la dirección Ip del Switch.

set vlan <numero de la VLAN> *name* <nombre de la VLAN >

! Se repite el paso anterior para configuran las VLAN`s que se requieran en el switch

R*eset*

! Se reinicia el switch para que tome los cambios de la dirección IP configurada.

set ip route <ruta por defecto 0.0.0.0> <dir IP interfaz del core>

set trunk 1/51 *dot1q*

! Se configura el up-link del switch como puerto troncal (trunk IEEE 803.1Q)

set port enable <Nºmod>/<Nºpuerto o rango de puertos>

! Se habilitan los puertos que se van a utilizar

set port static-vlan [<Nºmod>/<Nºpuerto>] [<Nº vlan>]

! Se asignan las VLANs estáticas a los puertos correspondientes.

set snmp community <read-only> <comunidad de lectura>

set snmp community <read-write> <comunidad de lectura y escritura>

set snmp community <trap> <comunidad para habilitar los traps>

! Configuración de las características SNMP

2. Configurar las variables deseadas

Si es necesario configurar parámetros que no se encuentran en el archivo de configuración básico, consultar la guía de comandos y/o el manual del Switch y realizar los ajustes necesarios.

3. Desplazamiento al sitio e instalación del dispositivo

Con el dispositivo configurado desplazarse al cuarto de cableado respectivo e instalar el dispositivo en el rack correspondiente y realizar las conexiones necesarias para la puesta en marcha del dispositivo.

4. Verificación de la normatividad del cuarto de cableado
5. Pruebas de funcionamiento y conectividad
6. Revisión de conexiones y/o reconfiguración

Para realizar estos tres pasos, ejecutar la lista de chequeo del subproceso de instalación.

Lista de Chequeo para el Subproceso de Instalación

1. Verificación del cumplimento de la normatividad

Estándar ANSI/TIA/EIA-569-A de Rutas y Espacios de Telecomunicaciones para Edificios Comerciales - “Comercial Building Standard for Telecommunications Pathways and Spaces”.
Esta normativa contempla todo lo referente a la arquitectura y diseño de los cuartos de telecomunicaciones con el fin de que sean adaptables a los cambios con facilidad, contempla aspectos como espacios en los cuales deben ser situados los cuartos de telecomunicaciones, distancias y recorridos dentro y entre edificios, recorridos horizontales, recorridos para backbone, estaciones de trabajo, facilidades de acceso, sala de equipos entre otros.

Estándar ANSI/TIA/EIA-568-A de Cableado Estándar de Telecomunicaciones para Edificios Comerciales - “Comercial Building Telecommunications Cabling Standard”.
Esta normativa dicta las especificaciones a tener en cuenta para realizar el sistema de cableado estructurado en un edificio y/o campus, se describen aspectos como el cableado horizontal y del backbone, interconexión de dispositivos entre otros.

A. Condiciones y requerimientos para el cuarto de cableado[18]

El diseño del cuarto de cableado debe considerar aspectos como el tamaño del edificio, espacio del piso a servir, necesidades de los usuarios y servicios de

[18] CHAVEZ, C, CONTRERAS, J, Y RUEDA, D, “Evaluación del desempeño de la red de datos institucional en los edificios de Ingeniería Eléctrica, laboratorio de alta tensión” Pág. 47.

telecomunicaciones a utilizar. Algunos aspectos importantes considerados en la norma son:

- *Requisitos de tamaño.* En la siguiente tabla se muestran las dimensiones de un cuarto de cableado según el área del edificio.

Dimensiones recomendadas para el cuarto de cableado

Área a Servir Edifício Normal	Dimensiones Mínimas del Cuarto de Cableado
500 m^2 o menos	3,0m x 2,2m
mayor a 500m^2, menor a 800m^2	3,0m x 2,8m
mayor a 800m^2, menor a 1000m^2	3,0m x 3,4m
Área a Servir Edificio Pequeño	**Utilizar para el Cuarto de Cableado**
100 m^2 o menos	Montante de pared o gabinete encerrado
mayor a 500m^2, menor a 800m^2	Cuarto de 1,3m x 1,3m o Closet angosto de 0,6m x 2,6m
Altura mínima : 2,6m	

- *Control ambiental.* En cuartos de cableado que tienen equipo electrónico, la temperatura debe mantenerse continuamente entre 18 a 24 grados centígrados.

- *Prevención de inundaciones.* No debe haber tubería de agua pasando sobre o alrededor del cuarto de cableado. De haber riesgo de ingreso de agua se debe proporcionar drenaje de piso.

- *Iluminación.* La iluminación debe estar a un mínimo de 2,6m del piso. Las paredes deben estar pintadas en un color claro para mejorar la luminosidad dentro del cuarto de cableado.

- *Localización.* Para mantener la distancia horizontal de cable promedio en 46m o menos (máximo 90m), se recomienda localizar el cuarto de cableado lo más cerca posible al centro de área de trabajo a servir.

- *Potencia.* Debe haber un mínimo de dos tomacorrientes de 110V C.A. La alimentación específica de los dispositivos electrónicos se podrá hacer con UPS y regletas montadas en los racks. El cuarto de cableado debe contar con una barra de puesta a tierra[19].

- *Disposición de equipos.* Los racks[20] deben contar con al menos 82cm de espacio de trabajo libre alrededor de los equipos y paneles de telecomunicaciones. La distancia se debe medir a partir de la superficie más externa del rack.

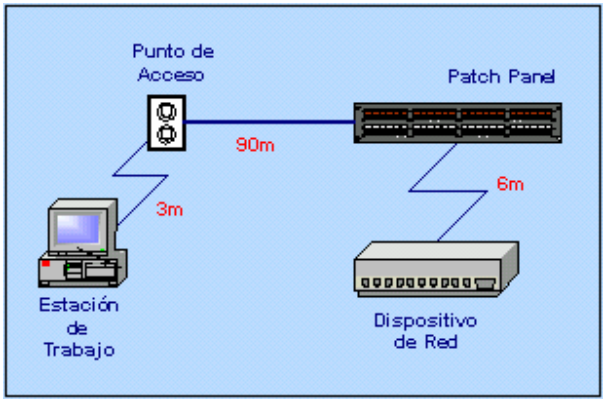
B. Cableado horizontal

El cableado horizontal incluye: las salidas de telecomunicaciones en el área de trabajo, terminales mecánicas, *patch panels* y *patch cords* utilizados en el área de trabajo y en el cuarto de cableado. Algunos aspectos importantes considerados en la norma son:

- *Topología.* El cableado horizontal se debe implementar en una topología de estrella.

- *Distancia del cable.* La distancia horizontal máxima desde el área de trabajo hasta el cuarto de cableado es de 90m independientemente del cable utilizado, se tienen 9m adicionales para la distancia de los *patch cords*: área de trabajo tres metros y en los *cross-connect* seis metros.

[19] Especificada en la norma ANSI/TIA/EIA 607.
[20] Especificados en la norma ANSI/TIA/EIA 810.



Cableado horizontal

Fuente: CHAVEZ, C, CONTRERAS, J, Y RUEDA, D, "Evaluación del desempeño de la red de datos institucional en los edificios de Ingeniería Eléctrica, laboratorio de alta tensión" tesis de grado, Universidad Industrial de Santander 2002. Pág. 49.

- *Manejo del cable.* El destrenzado de pares individuales en los conectores y *patch panels* debe ser menor a 1.25cm para cable UTP categoría 5. El radio mínimo de doblado es 2.5cm.

- *Interferencia electromagnética.* Se debe evitar el paso del cable por los siguientes dispositivos: transformadores (mínimo 1.2m), cables de corriente alterna (distancia mínima entre 13 a 91cm, dependiendo de la potencia del cable), luces fluorescentes (mínimo 12cm), intercomunicadores (mínimo 12cm), aires acondicionados (mínimo 1.2m), etc.

2. Lista de chequeo de conectividad

A. Ping exitoso del switch central al switch instalado.

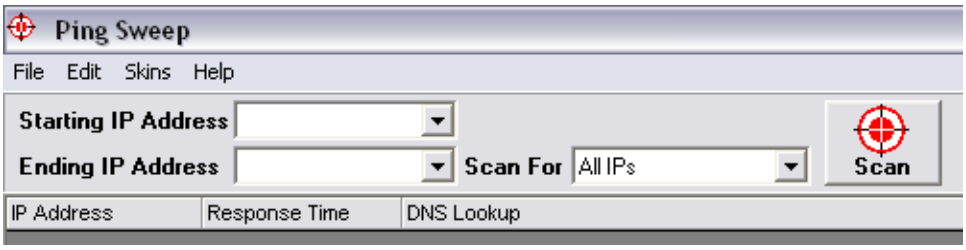
Realizar un ping a la dirección de la interfaz del switch instalado desde la estación gestora para verificar la conectividad de capa 3.
La sintaxis del comando es*: ping* [dirección IP del switch instalado]

B. Sesión Telnet exitosa de la estación gestora al switch instalado.

Abrir una sesión Telnet desde la estación gestora al switch instalado para verificar la conectividad hasta la capa de aplicación.
La sintaxis del comando es*: telnet* [dirección IP del Switch instalado]

C. Barrido de pings exitoso de la estación gestora al switch instalado.

Mediante el software de gestión SolarWinds ejecutar la herramienta de Ping Sweep que se encuentra en el conjunto de herramientas Ping & Diagnostic. Se debe introducir el rango de direcciones IP de los equipos de trabajo conectados al nuevo switch. Es necesario encender todas las maquinas directamente conectadas al switch para conectividad.



Además de la prueba con la herramienta Ping Sweep es posible verificar el correcto estado de los puertos del switch, con la ayuda de un computador personal. En este caso se verifica conectividad puerto por puerto.

3. Lista de chequeo de revisión de conexiones y configuración

A. El estado de los indicadores del Switch es correcto (PWR, OPR, LINK y COL)

Indicadores LED's de los Switches P33x

Nombre del LED	Descripción	Estado
PWR	Estado de alimentación	*Apagado*- Dispositivo apagado *Encendido* – Dispositivo encendido

<table>
<tr><td></td><td></td><td>Intermitente – Uso solamente de BUSP</td></tr>
<tr><td>OPR</td><td>Operación de la CPU</td><td>Apagado - El modulo esta Iniciando
Encendido – Operación Normal</td></tr>
<tr><td>SYS</td><td>Estado del sistema (muestra si ese Modulo es el agente maestro del stack)</td><td>Apagado – El modulo es un esclavo en una pila (stack)
Encendido – El modulo es el maestro de la pila y el cable Octaplane y redundante esta correctamente conectado.
Este LED también puede iluminar en el modo Standalone.
Intermitente – la caja (box) es una pila maestra y la pila esta en modo redundante.</td></tr>
<tr><td>LNK</td><td>Estado de puertos y el enlace</td><td>Apagado – Puerto deshabilitado
Encendido – Puerto habilitado y enlace OK
Intermitente – Puerto habilitado y enlace abajo</td></tr>
<tr><td>COL</td><td>Colisión (indica cuando hay colisiones en un puerto en Modo HDX)</td><td>Apagado - Sin Colisiones o puerto FDX

Encendido – Ocurrió una colisión</td></tr>
<tr><td>TX</td><td>Transmisión (Indica actividad de trafico de paquetes transmitidos)</td><td>Apagado – No esta trasmitiendo

Encendido – Modulo trasmitiendo datos</td></tr>
<tr><td>RX</td><td>Recepción (Indica actividad de trafico de paquetes recibidos)</td><td>Apagado – No se están recibiendo datos
Encendido – Datos recibidos de la línea dentro del modulo.</td></tr>
<tr><td>FDX</td><td>Indica el modo de operación Half/full Duplex</td><td>Apagado – Modo Half Duplex

Encendido – Modo Full Duplex</td></tr>
<tr><td>FC</td><td>Control de flujo</td><td>Apagado – Sin control de flujo
Encendido – Control de flujo Simétrico/Asimétrico el modo esta habilitado y el puerto esta en modo full duplex (FDX On)</td></tr>
<tr><td>Hspd</td><td>Muestra la velocidad del puerto</td><td><table><tr><td></td><td>10/100</td><td>1000</td></tr><tr><td>Apagado</td><td>10</td><td>--</td></tr><tr><td>Encendido</td><td>100</td><td>1000</td></tr></table></td></tr>
<tr><td>LAG</td><td>Trunking</td><td>Apagado - LAG no configurado para este puerto
Encendido – Los puertos pertenecen a un LAG</td></tr>
</table>

ROUT	Modo de operación (Indica el modo de operación actual de switch)	*Apagado* – El switch esta operando en la capa 2 *Encendido* – El switch esta operando en la capa 3

B. Dirección IP del switch corresponde con la dirección IP asignada.

Verificar si la dirección asignada por el administrador corresponde a la dirección IP configurada en el switch instalado.

Para verificar la dirección actual del switch ejecute desde la consola el comando: *Show interface*

```
P330-N>show interface
 Interface Name       Status       VLAN    IP address         Netmask
----------------  --------------  ----  ---------------  ---------------
inband            disabled        1     135.64.200.105   255.255.255.0
ppp               disabled        N/A   0.0.0.0          0.0.0.0
```

Interface Name	Nombre asignado a la interfaces configuradas.
Status	Estado actual de la interfaces. Indica si la interfaz se encuentra habilitada o deshabilitada.
VLAN	Indica a que VLAN se encuentra asignada la interfaz, Por defecto la VLAN 1 es de administración y la interfaz debe estar asignada a esta VLAN.
IP address	Muestra la dirección IP configurada a la interfaz. Cuando se configura la dirección IP de una interfaz se debe reiniciar el switch para que los cambios se actualicen.
Netmask	Muestra la mascara de Subred de las interfaces configuradas.

C. La dirección del gateway del switch es correcta.

Verificar si la dirección del gateway configurada en el switch corresponde con la dirección IP del switch central.

Para verificar las rutas estáticas configuradas en el switch ejecute el comando: *Show ip route*

```
P330-N>show ip route
Destination         Gateway
-------------       -------------
0.0.0.0             149.49.54.1
0.0.0.0             0.0.0.0
0.0.0.0             0.0.0.0
0.0.0.0             0.0.0.0
0.0.0.0             0.0.0.0
0.0.0.0             0.0.0.0
0.0.0.0             0.0.0.0
0.0.0.0             0.0.0.0
0.0.0.0             0.0.0.0
0.0.0.0             0.0.0.0
0.0.0.0             0.0.0.0
```

Destination — Dirección IP de la red destino. La red 0.0.0.0 indica que se la red destino corresponde a todas las redes.

Gateway — Dirección IP de la puerta de enlace. Indica a que dirección deben enviarse los paquetes dirigidos a una dirección destino desconocida. La ruta 0.0.0.0 149.49.54.1 de la figura corresponde a una ruta por defecto e indica que los paquetes dirigidos a cualquier red desconocida deben enviarse al la dirección 149.49.54.1.

D. Configuración correcta del up-link del switch como puerto troncal (Trunk 802.1Q).

Verificar la correcta configuración de modo trunk (dot1q) en el puerto 51 del switch.

Ejecute el comando: *show trunk*

```
P330-N>show trunk 4/1
Port   Mode   Binding mode                Native vlan
-----  -----  --------------------        -----------
41/1   off    statically bound                 1
41/2   dot1q  statically bound                 2
```

Port	Número del modulo/Número o rango de puertos
Mode	Estado de etiqueta del Puerto (dot1q – modo de etiquetado dot1Q, off – Modo limpio).
Binding mode	modo Binding del puerto.
Native VLAN	Numero de ID de la Vlan del Puerto

E. Los puertos están habilitados y configurados con la VLAN correcta.

Verificar la correcta configuración de los puertos del switch, comprobar si están habilitados y si las VLAN asignadas a cada puerto corresponden con las deseadas.

Para verificar la configuración actual de los puertos del switch ejecute desde la consola el comando: *show port*

```
P330-N>show port 3/4
Port   Name            Status    Vlan Level  Neg     Dup. Spd. Type
------ --------------- --------- ---- ------ ------- ---- ---- -----------------
 3/4   Gregory         no link   1     0     enable  half 10M  10/100BaseTx Port
```

Port	Nº modulo/Nº puerto
Name	Nombre asignado al puerto
Status	Estado del puerto: Conectado (connected) No conectado (no link) Deshabilitado (disabled)
Vlan	Numero de ID de la VLAN del puerto
Level	Nivel de prioridad del puerto (0-7)

Neg	Estado de la auto-negociación del puerto Habilitada (enabled) Deshabilitada (disabled)
Dup	Estado del modo de comunicación del Puerto (Duplex) Half Duplex o Full Duplex
Speed	velocidad de comunicación del puerto (10Mbps, 100Mbps o 1000Mbps)
Type	Tipo de Puerto, por ejemplo: 10/100Base-Tx. 1000Base-SX. Link Aggregation Group of 10/100Base-T ports, etc.

7. Documentación y actualización del sistema de información

Se documenta la nueva instalación y si es necesario se actualiza el inventario lógico de la red de datos, para ello se introducen los nuevos datos en el sistema de información.

Además se realiza el backup del archivo de configuración de switch instalado.

Creación del Backup

En el grupo de herramientas misceláneas del Software SolarWinds se encuentra un servidor TFTP.

Ejecutar el servidor TFTP.

En el modo de usuario con privilegios ejecutar el siguiente comando:

copy stack-config tftp <nombre del archivo> <dirección IP servidor TFTP>

ANEXO F. Guías de Procedimientos del Subproceso de Monitorización

Herramientas de SolarWinds Propuestas para la Monitorización

Network Performance Monitoring – Monitorización del Desempeño de la Red

Network Performance Monitor – Monitoriza el trafico y utilización de cientos de nodos y/o interfaces. Permite generar alarmas en tiempo real vía e – mail o beeper cuando una condición de alerta previamente configurada es detectada. Permite monitorizar variables como latencia, disponibilidad, paquetes perdidos, tráfico, ancho de banda utilizado, porcentaje de utilización de la CPU, la memoria del dispositivo, entre otras y recolectar estadísticas relacionadas con estas variables.

Real-time Interface Monitor – Visualiza información organizada en tablas relacionada con variables estáticas y dinámicas de las interfaces monitorizadas mediante Network Performance Monitoring. Es posible graficar cada una de las variables dinámicas pertenecientes a MIB mediante SNMP Graph.

SNMP Graph – Monitoriza y grafica las estadísticas de cualquier objeto de la MIB que responda al protocolo SNMP. Variables como tráfico, carga, procesamiento de la CPU, nivel de voltaje, temperatura, tráfico VoIP son posibles de graficar siempre y cuando el dispositivo las soporte.

Network Monitor Tools – Herramientas de monitorización de red

Whatch It! – Monitoriza servidores, switches, routers, sitios Web, etc. y notifica cuando los tiempos de respuesta de la red comienzan a

degradarse o cuando algún dispositivo sale de funcionamiento. Posee señalizaciones gráficas y sonoras para indicar eventos anómalos relacionados con los dispositivos monitorizados. Es de fácil configuración y utilización, es recomendable para la monitorización simultánea de servidores.

1. Definición y clasificación de variables y/o dispositivos

En principio se definen variables relacionadas con la configuración, disponibilidad, latencia y errores para los nodos monitorizados además de variables relacionadas con el tráfico entrante y saliente a cada una de las interfaces asociadas a los nodos estudiados.

Estáticas:

Variable	Nombre	Tipo	OID
Interface – Descripción de la interfaz.	IfDescr	DisplayString	1.3.6.1.2.1.2.2.1.2
MAC Address – Dirección Física.	ifPhysAddress	PhysAddress	1.3.6.1.2.1.2.2.1.6
Type – Tipo de Interfaz (ej: Ethernet, fastethernet, serial , Frame Relay, etc)	ifType	IANAIfType	1.3.6.1.2.1.2.2.1.3
Speed – Velocidad del puerto.	ifSpeed	Gauge32	1.3.6.1.2.1.2.2.1.5
Hardware Type - Tipo de hardware.	locIfHardType	DisplayString	1.3.6.1.4.1.9.2.2.1.1.1

Dinámicas:

Variable	Nombre	Tipo	OID
Status – Estado de la interfaz	IfOperStatus	Integer	1.3.6.1.2.1.2.2.1.8
Admisn Status- Estado administrativo de la interfaz (Up/ShutDown)	ifAdminStatus	Integer	1.3.6.1.2.1.2.2.1.7

Bytes received _ Bytes recibidos	ifInOctects	Counter32	1.3.6.1.2.1.2.2.1.10
Bytes transmitted _ Bytes transmitidos	ifOutOctects	Counter32	1.3.6.1.2.1.2.2.1.16
Receive Errors – Errores recibidos (pps)	ifINErrors	Counter32	1.3.6.1.2.1.2.2.1.14
Transmit Errors – Errores recibidos (pps)	ifIOutErrors	Counter32	1.3.6.1.2.1.2.2.1.20
Current Temperature - temperatura interna actual del dispositivo en grados Celsius*	extremeCurrentTemperature	integer	1.3.6.1.4.1.1916.1.1.1.8
Vlan Description – VLANs configuradas*	extremeVlanIfdescr	DispalyString	1.3.6.1.4.1.1916.1.1.2.1.2
Vlan Status - Estado de las VLANS activas*	extremeVlanIfStatus	RowStatus	1.3.6.1.4.1.1916.1.1.2.1.6

Dispositivos a monitorizar:

Dispositivo	Nombre de Dominio	Dirección IP
Servidor de Correo/DNS/Exchanger	condor.uis.edu.co	192.168.19.2
Servidor Web	dodo.uis.edu.co	192.168.19.15
Servidor de la Biblioteca	Pelicano.uis.edu.co	192.168.19.6
Switch-Core	---	192.168.19.1

2. Definición y clasificación de variables y/o dispositivos adicionales:

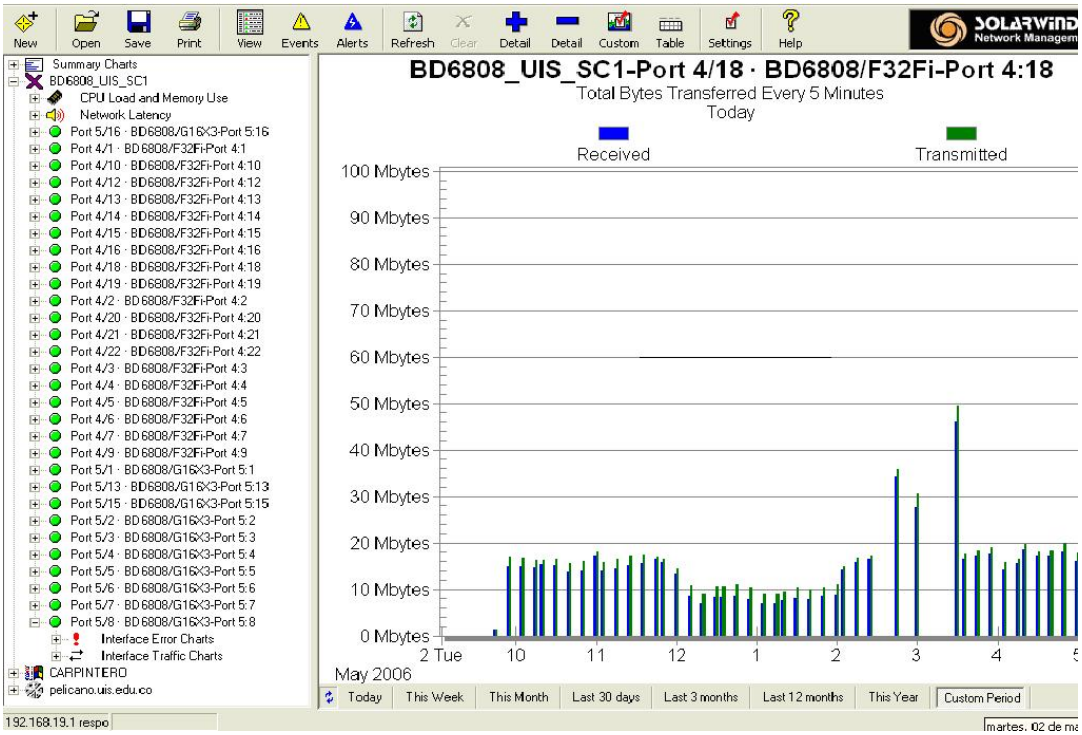
Variable	Nombre	Tipo	OID
MTU – Unidadn maxima de transmisión	IfMtu	Integer	1.3.6.1.2.1.2.2.1.4
Last Change – Timepo desde el ultimo reinicio del dispositivo	ifLastChange	Time Ticks	1.3.6.1.2.1.2.2.1.9
Power Status - estado de la fuente de alimentación.*	extremePowerStatus	integer	1.3.6.1.4.1.1916.1.1.1.21

• notPresent, • presentOK, • PresentnotOK)			

3. Descripción y Configuración de la Herramienta SolarWinds para la Monitorización

➢ NETWORK PERFORMANCE MONITOR

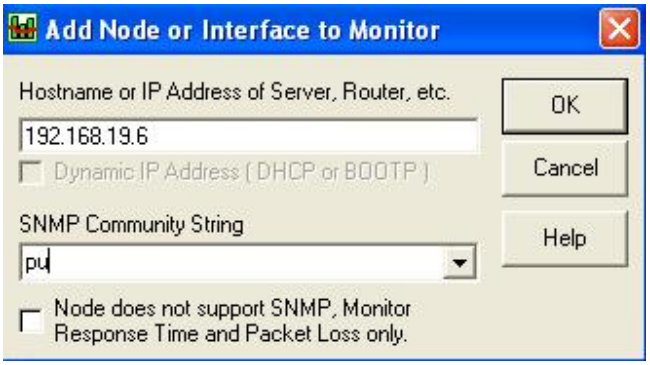
Se encuentra dentro del grupo de herramientas de Network Performance Monitoring. Se visualiza una interfaz grafica como la que se muestra en la siguiente figura.



A. Barra de herramientas

- **New:** Agregar un nuevo nodo o interfaz. Es necesario ingresar la dirección IP y la comunidad SNMP. Para realizar modificaciones remotas sobre las variables es necesario utilizar la comunidad SNMP de lectura/escritura, si se ingresa la comunidad SNMP de lectura solo se

permite la visualización de las variables. Si el nodo o interfaz no soporta el protocolo SNMP solo es posible visualizar información relacionada con disponibilidad, tiempo de respuesta y paquetes perdido.



Una vez se adicione el nodo, el software identifica las interfaces asociadas a ese nodo (por ejemplo los puerto de un router o switch), se seleccionan las interfaces y variables deseadas, además de opciones particulares de acuerdo al dispositivo relacionadas con monitorización de la CPU y memoria.

- **Open/Save/Print:** Opciones generales para almacenar, abrir o imprimir un proyecto de Network Performance Monitor. Solo es posible realizar estas acciones con la versión licenciada del software.

- **View:** Visualizar en tablas cualquier variable disponible en el menú de nodos e interfaces. Se visualizan todos los nodos junto con sus interfaces asociadas.

- **Events:** Visualizar el histórico de todos los eventos presentados relacionados con el estado de las interfaces, alarmas, cambios en la configuración de los nodos, eventos de usuario, etc.

- **Alerts:** Visualiza el histórico de las alarmas generadas. Permite la configuración de nuevas alarmas y editar las predeterminadas.

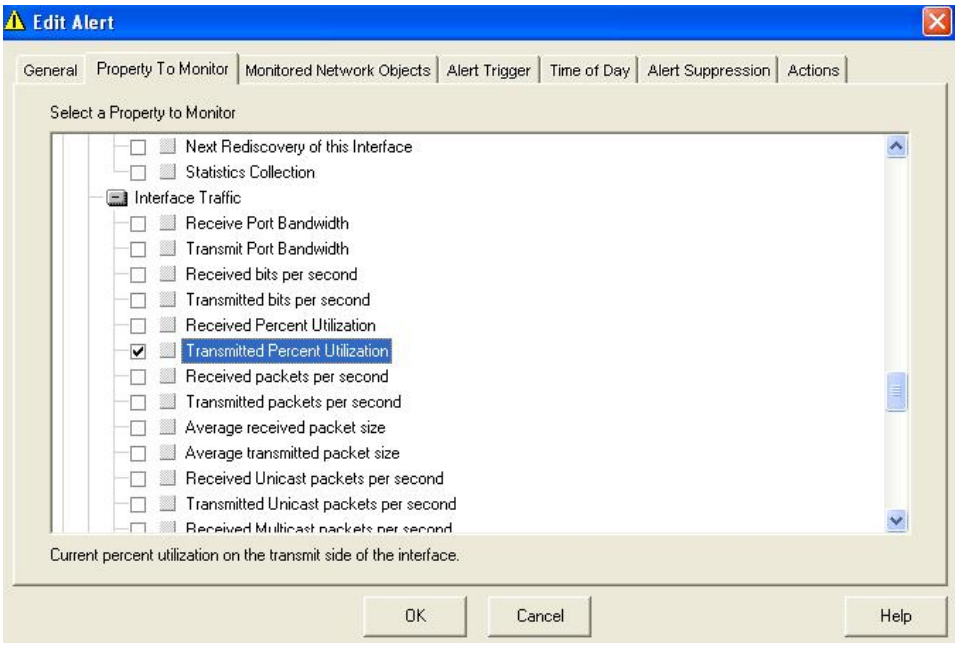
o Configuración de alarmas:

Para configurar o editar alarmas elija la opción “Configure Alerts”. Es posible editar una de las alarmas predeterminadas o crear una particular asociada con más de

150 eventos. Las Variables de interés para la monitorización del estado y desempeño de la red de datos son:

Nodos	Interfaces
Estado (Down/Up)	Estado (Down/Up)
% Paquetes Perdidos	% Utilización en Transmisión
% Utilización de la CPU	% Utilización en Recepción
% Utilización de la Memoria	Errores recibidos (x hora/día)
Tiempo de repuesta	Errores transmitidos (x hora/día)

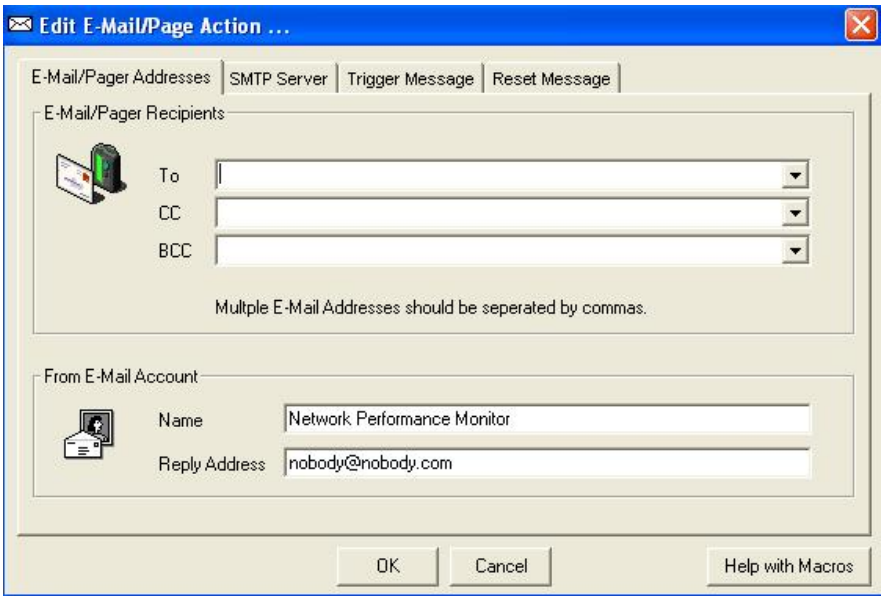
La figura muestra la ventana para la creación de una nueva alarma. Se debe seguir un orden para la configuración.



1. En el menú General, configurar un nombre para la nueva alarma. Es necesario habilitar la casilla Eneable para activar la alarma.
2. En el menú Property to monitor, seleccionar la variable que se desea monitorizar y controlar dentro de un umbral preestablecido. (por ejemplo Porcentaje de utilización en trasmisión de determinado enlace – Transmitted Percent Utilization).

3. En el menú Monitored Network Objects, seleccionar los nodos o enlaces a los que se le desea aplicar la nueva alarma, de acuerdo al tipo de variable seleccionada. Aparecen todos los nodos o enlaces que se monitorizan con la herramienta Network Performance Monitoring.
4. En el menú Alert Trigger, se establecen los umbrales superior e inferior dentro de los cuales se desea controlar la variable previamente seleccionada.
5. En el menú Time Delay, se establece el momento del día en el cual se desea que el gestor notifique al administrador las alarmas registradas. Es posible seleccionar cualquier instante del día, para que se notifique las anomalías de inmediato.
6. En el menú Alert Supresión, permite configurar una variable que estará asociada a la previamente configurada (Opcional), con el fin de crear una alarma compuesta. Esta última variable también será monitorizada y deberá estar dentro de un rango preestablecido para que las anomalías en la variable principal sean notificadas. Esta nueva variable puede estar asociada a otro dispositivo o enlace.
7. En el menú Actions, se configura el tipo de alarma que se generara cuando se presente un evento. Es posible configurar eventos como sonidos, ejecutar programas, enviar traps, enviar e-mail, entre otros.

   Para la configurar el envió de e-mail se debe seleccionar la opción Add Alert Action seguido de la opción Send E-mail/Page. Aparecerá la ventana que se muestra a continuación.



Se configura la(s) dirección(es) de correo que se desean reciban las notificaciones, también se debe configurar el servidor SMTP para que sea posible el envió de e-mail. Se ingresa el nombre de dominio o dirección del servidor (servidor SMTP de la UIS - condor.uis.edu.co). Por último se configurar los mensajes de alerta para los umbrales superior e inferior preestablecidos para la variable particular. Si se deja en blanco el espacio de determinada umbral (superior o inferior) no se enviaran cuenta las notificaciones.

Ejemplo de mensaje de alerta:

> Se ha superado el Umbral predeterminado para el % de Utilización en Transmisión de las interfaces asociadas a un dispositivo.
>
> Alerta: la Interfaz ${InterfaceName} del dispositivo ${NodeName}, presenta anomalías. Su estado actual es '${Status}'.
> El % de Utilización en Transmisión de la interfaz ${InterfaceName} es ${OutPercentUtil}.
> El tráfico actual en la interfaz es:
> Rx : ${InBps}

Tx : ${OutBps}

Este problema ocurrió a las ${DateTime}

- **Refresh/Clear/Details:** Opciones de actualización y visualización de la graficas. Es posible cambiar el intervalo de visualización de tiempo de días a solo minutos de acuerdo a las necesidades y al intervalo de sondeo y de almacenamiento de estadísticas.

- **Custom/Table:** Permiten particularizar las opciones de visualización de las gráficas, opciones relacionadas con estilo de la gráfica, colores, estilo, etc.

- **Settings:** Permite configurar opciones relacionadas con la base de datos, opciones de sondeo, estadísticas, presentación de datos e iconos y opciones ICMP y SNMP.

En la base de datos se configura el intervalo de tiempo que se desee para resumir los datos en estadísticas periódicas (por ejemplo estadísticas por día, semana, etc.) y el momento en que se debe realizar este resumen.

Las opciones de sondeo permiten ajustar el intervalo de tiempo entre cada encuesta que realiza el gestor a los nodos monitorizados (agentes), este intervalo debe ser lo suficientemente corto como para registrar los eventos presentados en la red sin llegar a generar demasiado tráfico. El valor por defecto es de 120 segundos, este es un tiempo prudente para realizar las encuestas a los agentes.

B. Menú de nodos e interfaces monitorizadas.

Se visualizan todos los nodos adicionados con sus respectivas interfaces y un resumen estadístico de las variables relacionadas con disponibilidad, tiempo de respuesta, tráfico y utilización de la CPU y memoria para cada una de las interfaces monitorizadas.

La gráfica se despliega en la parte derecha de la pantalla de acuerdo a la interfaz o nodo seleccionado y a la variable seleccionada.

Las variables de importancia y posibles de visualizar son:

- **CPU Load and Memory Use**: Porcentaje de utilización de la CPU y la memoria (Solo si el dispositivo soporta esta variable). Indicada para la monitorización de servidores y routers.

- **Network latency:**
  - o Disponibilidad de la interfaz, indica cuando un nodo sale de funcionamiento.
  - o Tiempo de respuesta y paquetes perdidos, indican cuando los tiempo de respuesta de un nodo comienzan a incrementar debido a una posible anomalía.
  - o Porcentaje de paquetes perdidos.

Tráfico y estado de las Interfaces

- **Interface Error Charts**: Número de errores en la transmisión y recepción y paquetes entrantes y salientes descartados.

- **Interface Traffic Charts:**
  - o Total Bytes Transferred: Numero de bytes transmitidos y recibidos en determinado periodo de tiempo.
  - o Porcentaje de utilización del enlace en la recepción y transmisión.
  - o Total Packets Trasmitted/Received: Numero de paquetes transmitidos y recibidos en determinado periodo de tiempo.
  - o Multicast Traffic – Tráfico de peticiones Multicast en paquetes por segundo (pps).

Además se permita la visualización de los mínimos, máximos y promedios en la transmisión entrante y/o saliente en pps o bps.

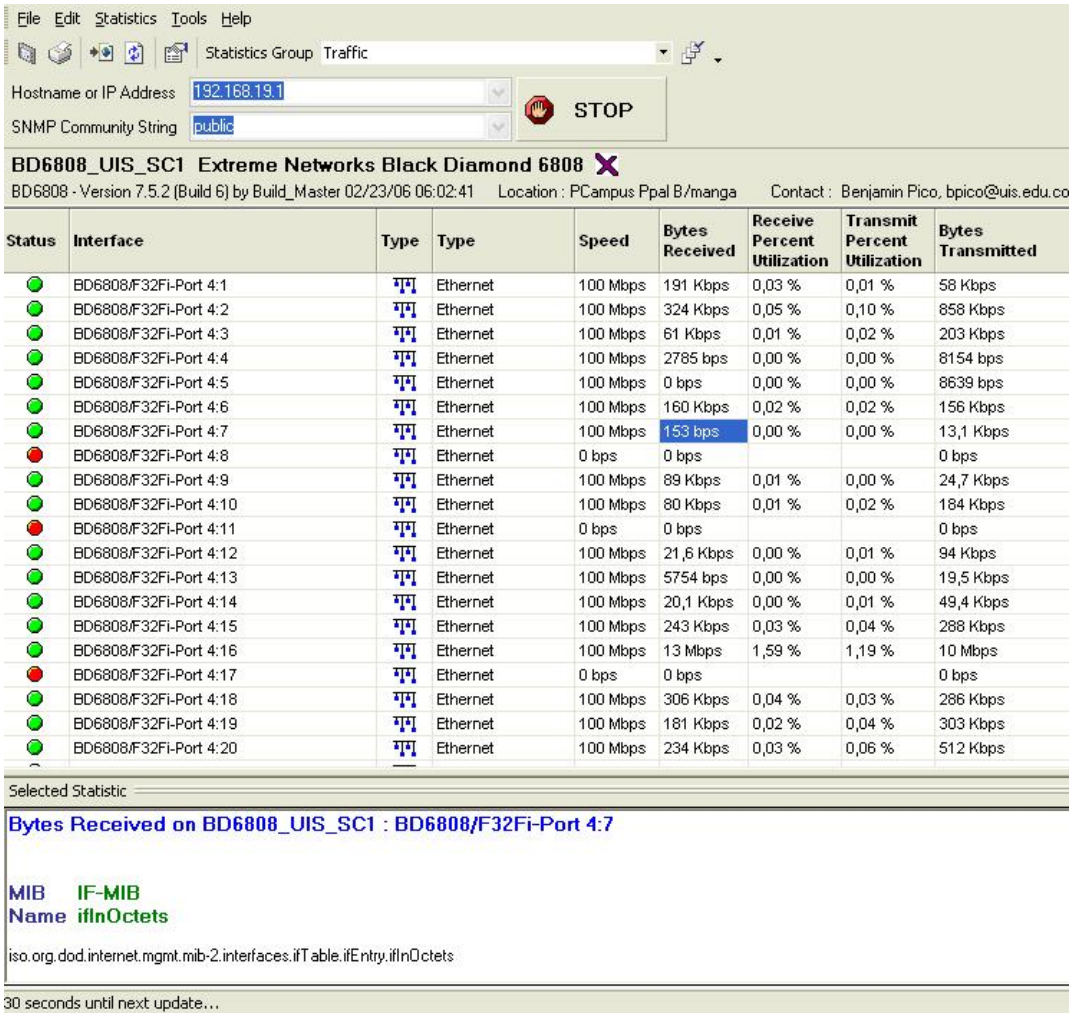
C. Gráfica.

Este campo contiene las graficas de acuerdo a los nodos y/o interfaces seleccionadas. Es posible alejar o acercar las graficas con la simple manipulación del mouse sobre la misma. Las opciones de visualización se ajustan en el campo Custom en la barra de herramientas.

Por otra parte es posible acceder desde esta aplicación a otras herramientas de interés para la monitorización. Desde cualquier interfaz habilitada se puede acceder a las herramientas Real-time Interface Monitor y Real-time Gauge. Haciendo click derecho sobre cualquier interfaz se encuentran estas opciones.

- **REAL-TIME INTERFACE MONITOR**

Se encuentra dentro del grupo de herramientas de Network Performance Monitoring. Se visualiza una interfaz gráfica como la que se muestra en la siguiente figura



A. Barra de herramientas superior

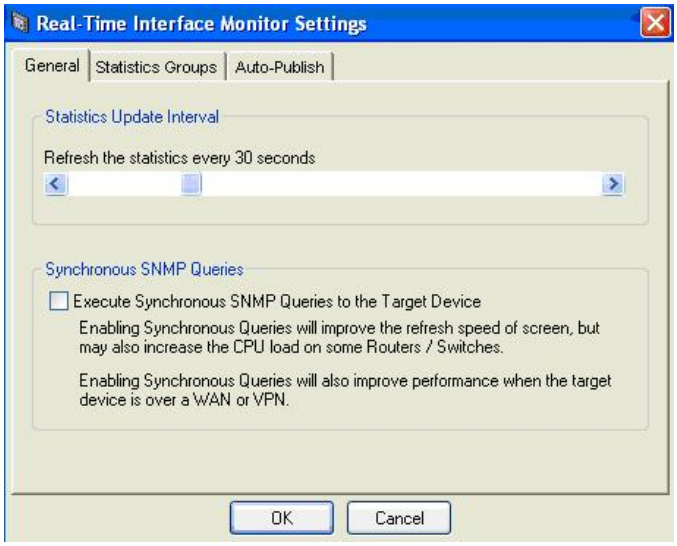
- **Statistics Group:** Permite elegir el grupo de variables a monitorizar. Se encuentran grupos de variables como: tráfico, estado, errores, configuración entre otros además de grupos de variables relacionadas con tecnologías especificas (Ehernet, Token Ring, frame Relay, ATM, 802.11, etc.)

- **Settings:**

o Configurar el intervalo de actualización de las variables, es posible obtener actualizaciones cada segundo (1segundo) hasta cada 120 segundos de acuerdo a las necesidades inmediatas.

o Configurar los grupos de variables. Es posible editar los grupos existentes, agregarle o quitarle variables, crear un nuevo grupo o simplemente renombrar uno ya existente.

o Configurar opciones de publicación de información vía Web. Real-time Interface Monitor permite publicar y actualizar una página Web automáticamente con la información recopilada (solo es posible en la versión licenciada)



- **New/Print/publish/refresh:** Opciones relacionadas con nuevos proyectos de Real-time Interface Monitor, opciones de impresión de la información, publicación vía Web de la información y actualización inmediata de los datos visualizados en la tabla de variables actual.

- **Hostname or IP Address/ SNMP Community String:** Campos para ingresar al dirección IP y la comunidad SNMP del Nodo a monitorizar. Cuando se Ingresa

desde Network Performance Monitor, no es necesaria esta información el software automáticamente actualiza la tablas con las variables monitorizadas y continua el proceso continuamente.

B. Cuadro de interfaces y variables

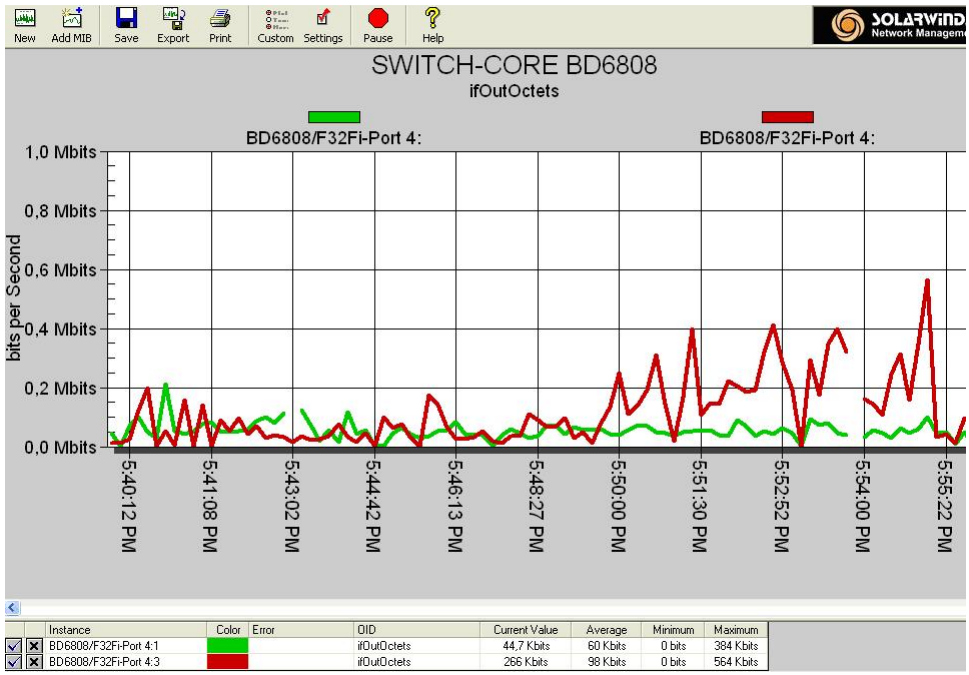
Se visualiza las características del nodo monitorizado y el estado de cada una de las variables estáticas y dinámicas configuradas. La información es desplegada en forma de tablas para facilitar su visualización y entendimiento. Al seleccionar cualquiera de las variables pertenecientes a la MIB, es posible visualizar características especificas de la misma en el cuadro inferior, además es posible graficar las variables dinámicas mediante la herramienta SNMP Graph, solo se necesita seccionar la variable a graficar, hacer click derecho y seleccionar la opción *Graph Select Statistic* o seleccionar la variable y en el menú principal buscar la opción *Graph Select Statistic* en el menú edit.

C. Frame Inferior – Información de la MIB

Para visualizar la información específica de las variables es necesario habilitar la opción *Display Statistics Details* en el menú statistics de menú principal. De esta forma es posible visualizar información de la variable seleccionada, datos relacionados con la MIB y una descripción.

- SNMP GRAPH

Se encuentra dentro del grupo de herramientas de Network Performance Monitoring. Se visualiza una interfaz gráfica como la que se muestra en la siguiente figura.



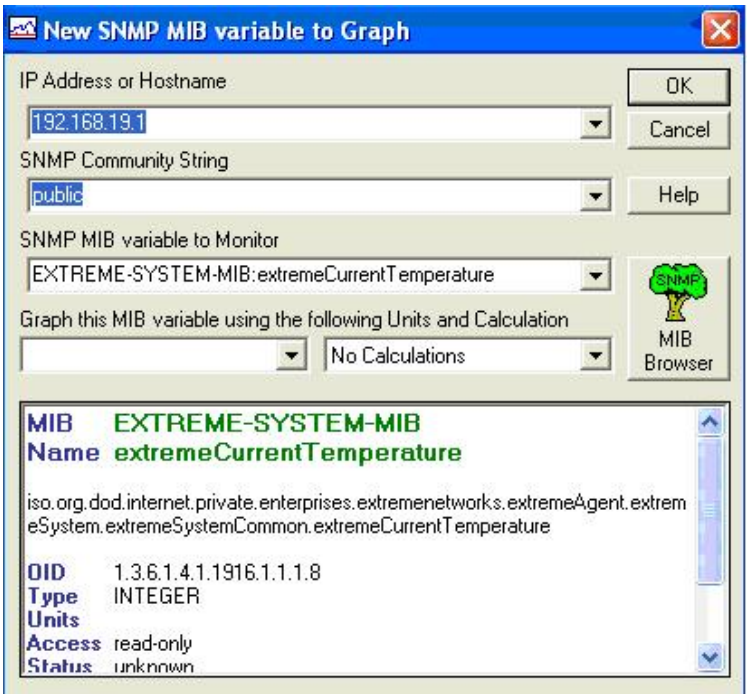
A. Barra de herramientas

- **New:** Abrir una nueva ventana independiente para graficar una variable.

- **Add MIB:** Primero que todo se debe introducir la dirección IP del dispositivo o interfaz a monitorizar junto con la comunidad SNMP.

Para seleccionar una MIB específica se bebe introducir el nombre y su ubicación o utilizar el MIB Browser para relacionar una del árbol MIB disponible incluido en el software SolarWinds.

Es posible Graficar múltiples variables en el mismo grafico.



- **Save/Export/Print:** Opciones generales para almacenar, exportar o imprimir un proyecto de SNMP Graph. Solo es posible realizar estas acciones con la versión licenciada del software.

- **Custom:** Permita configurar opciones de visualización de la grafica como: titulo, estilo, color, etc. y opciones para publicar vía Web los datos. Además permite configurar el intervalo recolección de datos del gestor hacia el agente, intervalo de tiempo entre cada actualización de la grafica. Es posible ajustar este intervalo entre 1 segundo y 600segundos. Se debe considerar un tiempo prudente para no generar demasiado tráfico y no perder información valiosa durante peticiones. El intervalo de 120 segundos utilizado en el sondeo con Network Performance Monitor es un tiempo aceptable para realizar una monitorización continua.

- **Settings:** Configurar opciones relacionadas con el intervalo de sondeo y características SNMP, además opciones de visualización de lista de OID en la parte inferior r de la pantalla, información complementaria de la grafica

- **Pause/Monitor:** Inicial o interrumpir la recopilación de la información.

B. Grafica y tabla inferior

Campo para la visualización de la grafica de acuerdo a los objetos de la MIB seleccionados. Es posible alejar o acercar las graficas con la simple manipulación del mouse sobre la misma. Las opciones de visualización de la grafica se ajustan en el campo Custom en la barra de herramientas.

La tabla en la parte inferior muestra información relacionada con los datos registrados en la grafica como: promedio, valor actual, valor mínimo/máximo, características de la variable monitorizada, etc.

Todos los resultados obtenidos mediante estas tres herramientas descritas pueden ser almacenados de forma grafica y/o mediante tablas, para ello es necesario contar con la versión licenciada. Los formatos de almacenamiento entre otros pueden ser: Cualquier formato de imagen (.gif, .bpm, .jpg, entre otros) o archivos de Excel o Word. Además se permite guardar el proyecto para la posterior visualización mediante la herramienta específica (.swc, .SNMP-Graph).

- **WHATCH IT !**

Se encuentra dentro del grupo de herramientas de Network Monitoring. Se visualiza una interfaz gráfica como la que se muestra en la figura

Se ejecuta en la parte superior derecha de a pantalla. Para adicionar un nuevo nodo es necesario introducir la dirección IP del mismo.

Es una herramienta práctica para monitorizar simultáneamente la disponibilidad y los tiempos de respuesta de interfaces y dispositivos como servidores. Es simple de ejecutar e interpretar, utiliza tres indicativos de colores y alarmas sonoras para indicar el estado de los dispositivos. El color verde indica un funcionamiento

correcto, el amarillo indica que el tiempo de repuesta ha incrementado es señal de una posible falla o problema con la disponibilidad del dispositivo y el rojo indica que el dispositivo no responde y es necesario ejecutar una acción correctiva.

4. Análisis de la información

Con base en la información histórica recopilada y de las alarmas generadas, se procede a hacer un análisis estadístico que determine el comportamiento de la red. En este análisis se debe incluir la información registrada en el proceso de mantenimiento correctivo.

5. Documentación

Se documentan los resultados provenientes del análisis. Se almacena la información de acuerdo a los dispositivos y variables elegidas y se clasifica en información estática y estadística. La información se registra en el sistema de información, esta incluye la base de conocimiento que contribuirá para la toma de decisiones.

6. Programación de mantenimientos

Con base en las conclusiones obtenidas en el análisis de la información si es necesario se programan mantenimientos preventivos y/o correctivo en procura de un mejor desempeño de la red.

ANEXO G. Guía de Procedimientos y descripción de las Listas de Chequeo del Subproproceso de Mantenimiento Correctivo

1. **Reporte del problema - ¿Quién lo reporta?** : Un usuario de la red de datos institucional o Personal Interno de la DSI identifica y reporta un incidente o

problema en algún servicio de los que soporta la red. Si el reporte lo hace personal Interno de la DSI, producto de la monitorización u otro proceso se asume que el problema ya ha sido identificado. En este caso se intenta buscar una solución remota. Si el incidente lo reporta el usuario es necesario seguir con las listas de chequeo.

2. **Lista de chequeo (Identificación y clasificación):** Si el problema es reportado por un usuario se procede a ejecutar una lista de chequeo que permita identificar y clasificar el problema, identificar el lugar donde ocurrió, el sitio más probable a donde se debe acudir en primera instancia (cuarto de cableado, estación de trabajo) o una posible solución en forma remota. Dichas lista se muestran a continuación:

Lista de chequeo 1. Un usuario reporta que no puede acceder a algún servicio de la red.

1. Se presenta el mismo problema en un equipo similar? 2. El patch cord está correctamente conectado y en buen estado? 3. La configuración de red es correcta? 4. La tarjeta de red funciona correctamente? 5. Se estableció comunicación con un equipo del grupo de trabajo? (capa 3) 6. Hay comunicación con el gateway? (capa 3) 7. Otros aplicativos de la red funcionan correctamente en la Terminal?	

Descripción y acciones a seguir en cada caso

1. Se presenta el mismo problema en un equipo similar? : Esta pregunta es muy importante porque determina si el problema es general en un grupo de trabajo o si es totalmente local en una terminal. Si la respuesta a esta pregunta es negativa se continúa con la lista de chequeo 1. Si la respuesta es afirmativa y

las estaciones están conectadas a un switch administrable y además se puede acceder a este dispositivo con el gestor se procede a mostrar el estado de los puertos y a hacer un reinicio lógico del dispositivo o de los puertos que se encuentren deshabilitados. Si el dispositivo no es administrable o no se puede acceder remotamente se debe desplazar a campo y ejecutar la lista de chequeo 3.

El acceso remoto al dispositivo se puede hacer utilizando la herramienta “Network Performance Monitor” que pertenece al grupo de herramientas “Network Monitor” de Solarwinds. Para usar dicha herramienta se da clic en la opción “New”. Allí se abre una ventana como se muestra en la figura 1 donde se agrega la dirección IP del dispositivo y la comunidad SNMP. Si se proporciona la información correcta, inmediatamente la herramienta inicia el descubrimiento de las interfaces del dispositivo y muestra el estado de las mismas. Después se selecciona la interfaz o interfaces a monitorizar y aparecen las variables posibles a monitorizar dependiendo del tipo de dispositivo. Oprimiendo el clic derecho del mouse sobre cualquiera de las interfaces o sobre la dirección IP del dispositivo se habilita un menú de opciones. Entre estas opciones se encuentre el reinicio lógico del dispositivo o de la interfaz seleccionada. En el menú de opciones principal se encuentra tambien la opción “telnet” con la que se puede iniciar una sesión fácilmente. Estas aplicaciones solo se pueden ejecutar si se proporciona una comunidad SNMP de lectura/escritura - R/W.

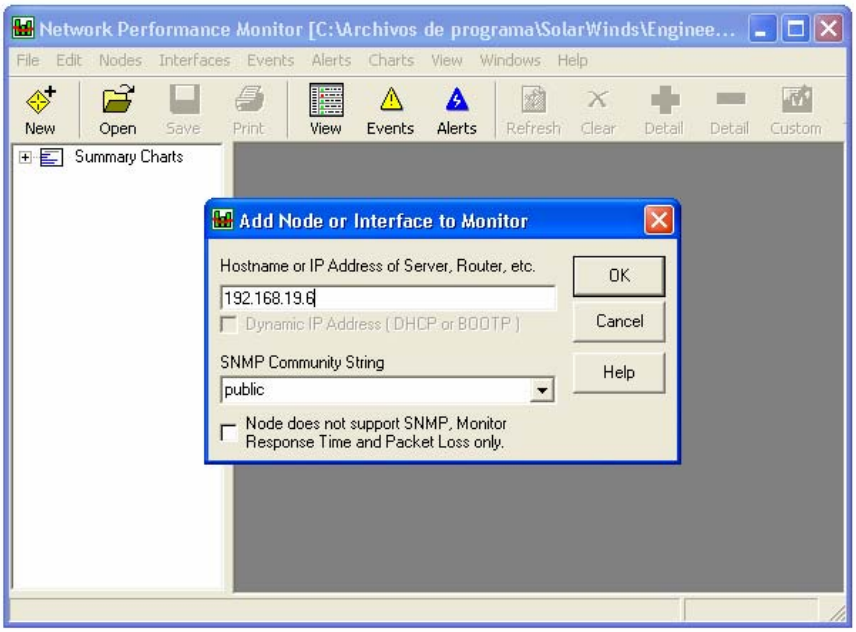


Figura 1. Interfaz de inicio para agregar un nuevo nodo.

2. El patch cord está correctamente conectado y en buen estado? (Capa 1) : Para verificar esto se observa que las luces de link de la tarjeta de red estén encendidas. Se puede comprobar que el patch cord se encuentra en buen estado intercambiándolo con el de una estación que no tenga problemas en los servicios de red. Si funciona bien en otra máquina se determina que el problema no es de capa 1 y será necesario comprobar el estado del puerto. Si no funciona el patch cord se determina que el problema está allí y se requiere desplazamiento para su solución.

3. La configuración de red es correcta? : preguntar por la configuración de red de la máquina y contrastarla con la que debería tener. Si no coincide, tal vez este es el causante del problema. Para obtener información acerca de la configuración de red, el usuario debe abrir el *símbolo del sistema* y ejecutar el comando *ipconfig* (Usuarios con Sistema Operativo Windows 98 o superior.) (Ver Instructivo para los usuarios de la red, Pág. 185). Para contrastar la configuración de red proporcionada por el usuario y contrastarla con la que debería tener se requiere contar con un sistema de información actualizado donde se encuentre el inventario físico y lógico de la red. Para solucionar el

problema en forma remota y dado que en la red de datos institucional no se cuenta con el servicio DHCP, el administrador debe determinar si es recomendable o no indicar al usuario la forma como se modifica la configuración de red en su estación de trabajo. Si esto es posible, se dicta la configuración que debe tener y se comprueba que el problema se solucione. Si esto no es posible el problema se debe solucionar desplazando un técnico para que brinde soporte al usuario. Si no se encuentra solución en este paso se continúa con el punto 4.

4. ¿La tarjeta de red funciona correctamente? : Se le pide al usuario que ejecute el comando *ping* hacia la dirección de red 127.0.0.1. Si **NO** hay respuesta, el problema está en la tarjeta de red y se requiere desplazamiento para su solución. Si la tarjeta funciona correctamente se pasa al punto 5.

5. Se estableció comunicación con un equipo del grupo de trabajo? (capa 3) : Para comprobar este punto se utiliza el comando *ping* dirigido a la dirección IP de una máquina vecina que pertenezca a la misma VLAN. Si hay respuesta, indica que la tarjeta de red, la configuración de red y el cableado (diagnóstico de capa 1 y capa 3) funcionan correctamente. Si no hay respuesta y se esta seguro que los pasos anteriores fueron correctamente ejecutados, el problema lo puede estar causando el dispositivo concentrador. Esto se esclarece ejecutando el paso 6.

6. Hay comunicación con el gateway? (capa 3): Se ejecuta el comando *ping* hacia la dirección IP del gateway. Si hay respuesta y la respuesta al punto 5 fue positiva seguramente se determinará en el siguiente paso que el problema es de ***aplicativo.*** Si la respuesta al punto 5 fue negativa, se espera que la respuesta al punto 6 también lo sea. En este caso, se accede al switch concentrador vía Web o Telnet en forma remota y se realiza un reinicio lógico del puerto al que está conectada la estación de trabajo. Si con esto NO se

soluciona el problema es necesario realizar un desplazamiento para determinar exactamente la causa del problema.

7. Otros aplicativos de la red funcionan correctamente en la terminal? : Si se ha llegado a esta instancia es porque la respuesta al paso 5 y 6 fueron positivas, entonces se esperaría que otras aplicaciones funcionaran o que por lo menos se lograra establecer una sesión Telnet con el gateway. Si esto se logra el problema es de aplicativo y se soluciona con un desplazamiento llevando el software adecuado. Si otras aplicaciones no funcionan y tampoco se logró establecer una sesión Telnet, el problema resulta complejo y es indispensable un desplazamiento. El único inconveniente aquí es que la lista de chequeo no da buenos indicios sobre el tipo de problema ni del lugar más recomendado para acudir a la solución. En este caso ya depende de la experiencia del personal que acude a campo para llevar este problema a buen término. No olvidar que es necesario documentar (utilizar formato de mantenimiento correctivo ver figura 4 pág. 186) para alimentar la base de conocimiento

Lista de chequeo 2 – Un usuario reporta tiempos de respuesta largos.

1. El problema es generalizado a un grupo de trabajo o a muchos usuarios? 2. El enlace al servidor está congestionado? 3. El nivel de procesamiento de la CPU del servidor es alto? 4. El número de usuarios conectados al servidor es mayor al soportado por este? 5. El enlace entre el grupo de trabajo y el gateway está congestionado? 6. Se detectó una tarjeta de red defectuosa?	

Descripción y acciones a seguir en cada caso

Los tiempos de respuesta largos pueden ser ocasionados por un problema local en el grupo de trabajo o por un problema en el dispositivo proveedor del servicio.

1. El problema es generalizado a un grupo de trabajo o a muchos usuarios?

Si la respuesta a esta pregunta es negativa, no se debe continuar con la lista de chequeo 2 y es necesario ofrecer atención particularizada al usuario para determinar la causa del problema. Las causas pueden ser a nivel del aplicativo instalado en el equipo, capacidad de procesamiento de la máquina, capacidad de memoria, tarjeta defectuosa, etc. En este caso solo se puede asegurar que el problema es local a un usuario.

2. El enlace al servidor está congestionado?
3. El nivel de procesamiento de la CPU del servidor es alto?
4. El número de usuarios conectados al servidor es mayor al soportado por este?

Estas preguntas están dirigidas a detectar el problema en el proveedor del servicio. Si cualquiera de las tres o las tres son positivas indica que el servidor no está en capacidad de proveer dicho servicio y es necesario migrar a una máquina de mayor capacidad. Si el nivel de procesamiento es aceptable y el enlace se encuentra congestionado, entonces la solución al problema es aumentar la capacidad del enlace. También es importante ver si este problema se presenta cuando se sobrepasa algún número determinado de usuarios. Si es así, el problema está relacionado con la capacidad del servidor. En cualquiera de estos casos la solución puede ser tardía porque implica la disposición de suficientes recursos para hacer los cambios necesarios. Otro indicativo de que el problema está del lado del servidor es que muchos usuarios reporten el mismo problema.

Para determinar si el enlace al servidor está congestionado se dirige al grupo de herramientas “Network Monitoring” de solarwinds y da clic en la herramienta “Watch it”. Aparece una ventana como la de la figura 2 y en ella digita la dirección

IP del servidor, oprime “Add Node” y luego “OK”. Luego se abre una ventana que contiene la dirección IP del dispositivo y un indicador de color. Los colores con su significado son:

Inactive	Indica que el servidor no está respondiendo. El enlace está congestionado
Warning	Indica que el servidor está descartando paquetes. Inicia congestión
Active	Indica que el servidor está respondiendo a tiempo.

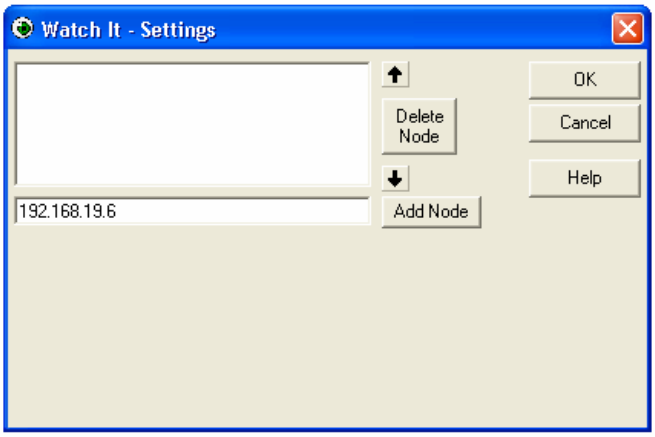


Figura 2. Interfaz de la herramienta Watch It

Las tres preguntas se pueden responder utilizando la herramienta “Network Performance Monitor” que pertenece al grupo de herramientas “Network Monitoring” de Solarwinds. En la figura 3, se muestra la ventana de monitorización para el servidor carpintero.uis.edu.co Allí se puede ver el estado de la interfaz, el nivel de procesamiento de la CPU, la cantidad de memoria usada, se despliegan las secciones actuales activas en el dispositivo, el porcentaje de utilización de la interfaz, etc. Es necesario destacar que la cantidad de variables que se pueden monitorizar con esta herramienta dependen del tipo de dispositivo. Las mejores prestaciones se obtienen para servidores Windows y dispositivos Cisco.

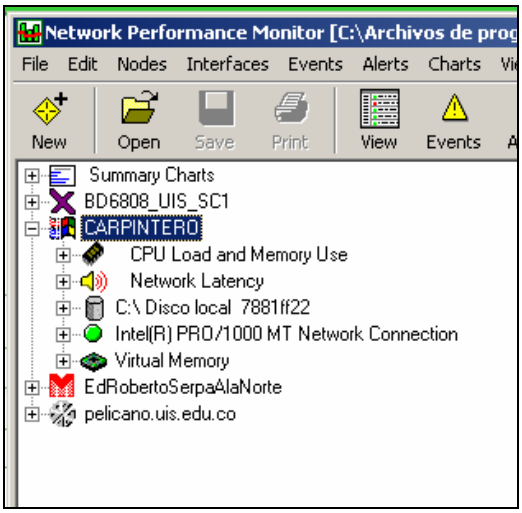


Figura 3. Interfaz de monitorización para el servidor carpintero

5. El enlace entre el grupo de trabajo y el gateway está congestionado?
6. Se detectó una tarjeta de red defectuosa?

Si la respuesta a las preguntas 2, 3 y 4 es negativa, es necesario buscar el problema en el lado del usuario. Las posibles causas pueden ser un cuello de botella en un tramo del recorrido o una tarjeta defectuosa que esta creando una tormenta de broadcast en el dominio de broadcast del grupo.

La primera causa se comprueba monitorizando el enlace desde el concentrador del grupo de trabajo al dispositivo que le sigue en jerarquía hasta llegar al core central. Si la respuesta es negativa, entonces es necesario desplazarse y buscar el problema dentro del grupo de trabajo. (Pregunta 6) Para buscar la tarjeta de red causante del problema es necesario deshabilitar uno a uno los puertos del concentrador hasta que se solucione la falla. Para resolver la pregunta 5 se ejecuta la herramienta Network Performance Monitor, igual que en el caso anterior, pero incluyendo la dirección IP y la comunidad SNMP del dispositivo de red adecuado.

3. **Orden de trabajo**: Se genera cuando no es posible solucionar el incidente o problema en forma remota. La documentación de los resultados de las listas de chequeo, la orden de trabajo y los pasos posteriores se llenan en el formato de *mantenimiento correctivo*. Ver figura 4

4. **Desplazamiento a campo:** Si se ha llegado a este punto es porque ya se identificó y clasificó el problema y se determinó que su solución debía buscarse en campo. Además se ha determinado el sitio más probable a donde se debe acudir en primera instancia (cuartos de cableado, estación de trabajo) a buscar una solución.

Lista de chequeo 3 – Desplazamiento a campo

1. A nivel de capa física existen problemas? 2. Se solucionó el problema con el reinicio lógico de cada uno de los puertos? 3. Se solucionó el problema desconectando cada uno de los puertos? 4. Deshabilitando el enlace a la estación que estaba causando el problema, las demás funcionan correctamente? 5. Hay comunicación con el gateway del switch? (capa 3) 6. Verificar el estado del patch cord del up-link del dispositivo de red.	

Descripción y acciones a seguir en cada caso

1. A nivel de capa física existen problemas? : Se deben verificar las luces de link de las tarjetas de red en las terminales y en el dispositivo concentrador y asegurarse que muestren los indicadores correctos. Asimismo es necesario verificar que todos los path cord estén bien conectados y que los dispositivos estén encendidos. Si la respuesta es afirmativa se pasa al punto 2. Si es negativa, seguramente este era el problema.

2. Se solucionó el problema con la reconfiguración de los puertos?: Si el dispositivo requiere algún tipo de configuración, se observa el estado de los puertos y se procede a reconfigurarlos. Se realiza una habilitación lógica y una reasignación de puertos a las VLANs correspondientes. (Ver Lista de Chequeo Subproceso de Instalación. Revisión de conexiones y reconfiguración)

3. Se solucionó el problema desconectando o habilitando administrativamente cada uno de los puertos? : Si el dispositivo es un hub se procede a desconectar cada uno de los patch cord de los puertos hasta que se solucione el problema.
   Si el dispositivo es un switch se deshabilitan administrativamente los puertos hasta que se solucione el problema.

4. Deshabilitando el enlace a la estación que estaba causando el problema, las demás funcionan correctamente? : Si en el paso 2 o 3 se encontró el problema se espera que deshabilitando el enlace a la estación que estaba causando el problema en las demás funcionen los servicios de red. Si esto no ocurre es necesario continuar con el procedimiento hasta encontrar los puertos a los que están conectadas las estaciones que están causando el problema.

5. Hay comunicación con el gateway del swich? (capa 3) : Si en los pasos anteriores no se encontró solución, con todos los puertos del dispositivo concentrador deshabilitados, se debe realizar una petición mediante el comando ping al Gateway del switch. Si hay respuesta, definitivamente el problema está en el dispositivo concentrador. Si no hay respuesta es posible que la configuración de la dirección del gateway del switch sea incorrecta o que existan problemas a nivel de puertos en el dispositivo de siguiente nivel.
   Si el problema se relaciona con la configuración del gateway se debe acceder por consola al switch y verificar la configuración.
   Si el problema se relaciona con los puertos de dispositivo de siguiente nivel es necesario acceder a este dispositivo (vía consola o telnet) y revisar la configuración (Ver paso 2).

6. Verificar el estado del patch cord del up-link del dispositivo de red.

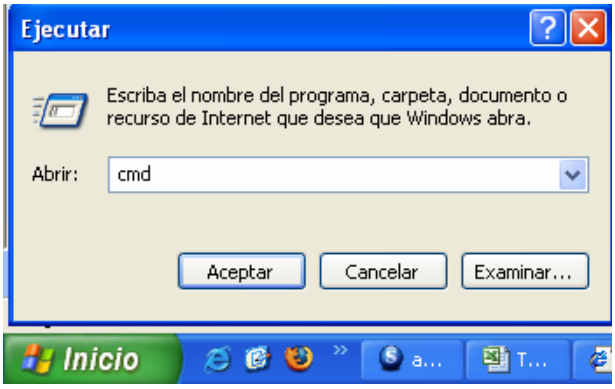
Se deben realizar pruebas de conexiones y estado de los patch cords que interconectan los dispositivos de red involucrados en el problema. (verificación Capa 1).

5. **Documentación:** Se llena el formato de ***Mantenimiento correctivo.*** Ver figura 4. página 186.

6. **¿Se presentó un nuevo problema?:** Si la respuesta es afirmativa se repiten los pasos del subproceso. Si la respuesta es negativa se finaliza el subproceso hasta que haya un nuevo reporte.

I. INSTRUCTIVO PARA LOS USUARIOS DE LA RED

Cuando se ejecuta la lista de chequeo 1 es posible que se le pida al usuario que ejecute el comando "ping" para verificar conectividad en la capa de red. Para ello necesita abrir una sesión en el intérprete de comandos de Windows. Esto se hace en 3 pasos:



1. Abrir la ventana "Ejecutar"
2. Escribir el comando "cmd" y entrar.
3. Escribir el comando ping con la siguiente sintaxis: *ping <dirección IP>*

A los usuarios se les puede enviar una ficha para dar a conocer la forma de ejecutar este comando. Se propone el siguiente diseño:

Prueba de conectividad y/o dirección de red

A. Para probar si su computador puede conectarse con otros computadores haga lo siguiente:

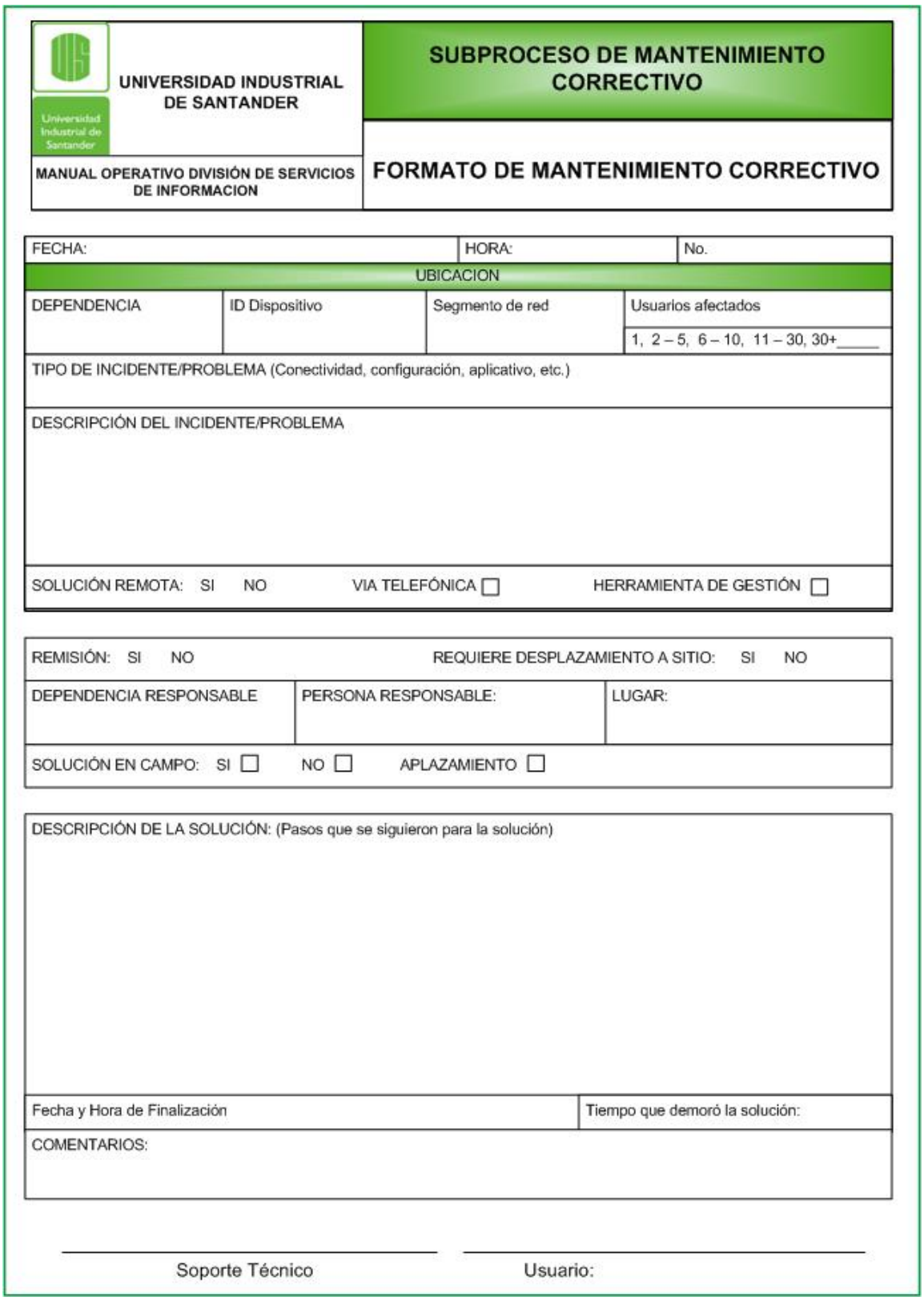
Vaya a:

1. INICIO/Ejecutar
2. Escriba **cmd** y oprima Enter
3. Escriba **ping 192.168.XXX.YYY**

Complete las XXX.YYY con la dirección IP completa del otro computador.

B. Para mirar su dirección de red ejecute los pasos 1 y 2, luego Escriba **ipconfig** y oprima Enter

Figura 4. Formato de Mantenimiento Correctivo



UNIVERSIDAD INDUSTRIAL DE SANTANDER	SUBPROCESO DE MANTENIMIENTO CORRECTIVO
MANUAL OPERATIVO DIVISIÓN DE SERVICIOS DE INFORMACION	FORMATO DE MANTENIMIENTO CORRECTIVO

FECHA:	HORA:	No.

UBICACION			
DEPENDENCIA	ID Dispositivo	Segmento de red	Usuarios afectados 1, 2 – 5, 6 – 10, 11 – 30, 30+____

TIPO DE INCIDENTE/PROBLEMA (Conectividad, configuración, aplicativo, etc.)

DESCRIPCIÓN DEL INCIDENTE/PROBLEMA

SOLUCIÓN REMOTA: SI NO VIA TELEFÓNICA ☐ HERRAMIENTA DE GESTIÓN ☐

REMISIÓN: SI NO REQUIERE DESPLAZAMIENTO A SITIO: SI NO

DEPENDENCIA RESPONSABLE	PERSONA RESPONSABLE:	LUGAR:

SOLUCIÓN EN CAMPO: SI ☐ NO ☐ APLAZAMIENTO ☐

DESCRIPCIÓN DE LA SOLUCIÓN: (Pasos que se siguieron para la solución)

Fecha y Hora de Finalización	Tiempo que demoró la solución:

COMENTARIOS:

Soporte Técnico Usuario:

Descripción del Formato de Mantenimiento Correctivo

Fecha: Se registra la fecha del reporte.
Hora: Se registra la hora a la que se hace el reporte.
Dependencia: Dependencia que reporta el incidente/problema.
ID del dispositivo: Se registra el número de inventario del dispositivo que origina el problema.
Segmento de red. Se registra el identificador del segmento de red (VLAN)
No. Usuarios afectados: Se selecciona el rango de usuarios afectados.
Tipo de incidente/problema: Se clasifica el problema en (escritorio – software, conectividad, configuración de red, degradación del servicio, etc.).
Descripción incidente/problema: Se hace una descripción que complemente el campo anterior.

Solución remota SI/NO, Vía telefónica/Herramienta Gestión Red: Se escoge la(s) que opción(es) corresponda(n).

Remisión: SI/NO. Se llena cuando la persona que atiende la llamada no logra solucionar el problema con la ejecución de la lista de chequeo.
Desplazamiento SI/NO. Se escoge la opción dependiendo de si requiere desplazamiento o no para llegar a la solución del problema.
Dependencia Responsable: Se registra el nombre de la dependencia a quien se le remite la solución del problema (LEA, Mantenimiento tecnológico, DSI, etc.).
Persona Responsable: Nombre de la persona responsable de hacer el soporte técnico.
Lugar: (Cuarto de cableado, estación de trabajo). Es lugar más probable a donde se debe acudir a solucionar el problema. Se determina con la ejecución de la lista de chequeo.
Solución en campo SI/NO/Aplazamiento: Se selecciona la opción que corresponda.

Descripción de la solución: Se describe con el mayor detalle posible los pasos que se siguieron para llegar a la solución.

Fecha y hora de finalización: Una vez encontrada y probada la solución se registra la fecha y hora.

Tiempo que demoró la solución: Corresponde a la diferencia en horas y minutos desde la hora del reporte hasta la hora en que se encontró la solución.

FIRMAS: Al final firman el responsable del soporte técnico y el usuario en conformidad con la solución.

ANEXO H. Recomendaciones para Realizar Pruebas de Conectividad

Adaptado de las recomendaciones emitidas por Cisco[21]

CISCO recomienda que las pruebas básicas de conectividad en una red deben desarrollarse en secuencia comenzando desde una capa del modelo de referencia OSI a la siguiente. Se recomienda comenzar con la Capa 1 y continuar hasta llegar a la Capa 7, si es necesario.

Al Comenzar con la Capa 1, se buscan problemas simples tales como cables de suministro conectados a la pared. Los problemas más frecuentes que se producen en las redes IP son causados por errores en el esquema de direccionamiento. Es importante verificar la configuración de direcciones antes de continuar con los siguientes pasos de configuración. Debe existir un proceso ordenado para diagnosticar fallas, con base en los estándares de networking establecidos por un administrador de red. La documentación es una parte muy importante del proceso

[21] CISCO SYSTEMS. Guía del primer año CCNA 1 y 2. Pearson Educación S.A, Tercera edición 2005. Cap 18

de diagnóstico de fallas, por que aún cuando se resuelva el problema en un entorno no estructurado, probablemente resulte imposible repetir la solución en problemas similares en el futuro.

Según CISCO, en su orden los problemas más frecuentes que se presentan capa por capa son:

Capa 1

- Cables defectuosos.
- Cables desconectados.
- Cables conectados a los puertos incorrectos.
- Conexión de cable intermitente.
- Cables inadecuados para la tarea (se deben usar los cables de conexión cruzada (roll over) y de conexión directa (straight-through) correctamente).
- Dispositivos apagados

Capa 2

- Interfaces Ethernet incorrectamente configuradas.
- Problemas en la tarjeta de interfaz de red (NIC).

Capa 3

- Direcciones IP incorrectas.
- Máscaras de subredes incorrectas.

En tres capas del modelo OSI se puede realizar un diagnóstico completo para detectar fallas.

Capa 1

Verificar las luces indicadoras: La mayoría de las interfaces o NICs cuentan con luces indicadoras que muestran si la conexión es válida y en algunos casos indican si se transmite (Tx) o se recibe (Rx). A menudo, esta luz recibe el nombre "link". Un cable no apropiado o defectuoso puede hacer que la luz de enlace indique una mala conexión o la ausencia de enlace. Por ello es necesario verificar que todos los cables se conecten a los puertos correctos, asegurarse de que todas las conexiones cruzadas realicen una adecuada conexión con la ubicación correcta utilizando el cable y método apropiados, verificar que todos los puertos del hub o switch se encuentren en la VLAN o en el dominio de colisión correctos y asegurarse siempre de que el dispositivo se encuentre encendido.

Es importante efectuar siempre los pasos más simples antes de efectuar el diagnóstico o de intentar un diagnóstico de fallas complejo.

Capa 3

El comando **ping** se utiliza en esta capa para probar la conectividad. Este comando envía un paquete al host destino y luego espera un paquete de respuesta de ese host. Los resultados de este protocolo de eco pueden ayudar a evaluar la confiabilidad de ruta hacia el host, las demoras en la ruta y si se puede acceder al host o si este funciona. El resultado del comando **ping** muestra los tiempos mínimo, promedio y máximo que tarda un paquete ping en encontrar un sistema especificado y regresar. El comando **ping** utiliza el Protocolo de Mensajes de Control en Internet (ICMP) para verificar la conexión de hardware y la dirección lógica de la capa de red. Este es un mecanismo de prueba sumamente básico para la conectividad de la red.

Capa 7

En esta capa es posible utilizar el comando **telnet** para verificar el software de capa de aplicación entre las estaciones origen y destino. Es el mecanismo de prueba más completo disponible. La aplicación de telnet se utiliza generalmente para conectar dispositivos remotos, recopilar información y ejecutar programas.
La aplicación Telnet proporciona una terminal virtual para conectarse a routers y switches que ejecutan TCP/IP. A los fines del diagnóstico de fallas, resulta de utilidad verificar que se pueda realizar la conexión utilizando Telnet. Esto prueba que, al menos, una aplicación TCP/IP es capaz de conectarse de extremo a extremo. Una conexión exitosa de Telnet indica que la aplicación de capa superior y los servicios de las capas inferiores funcionan correctamente.