DISEÑO E IMPLEMENTACION DE POLITICAS EN GESTION DE REDES PARA LA UNIVERSIDAD TECNOLOGICA DE BOLIVAR

LAURA VICTORIA YEPEZ RODRIGUEZ

JAVIER EDUARDO DIAZ MACHUCA

UNIVERSIDAD TECNOLOGICA DE BOLIVAR

FACULTAD DE INGENIERIAS

PROGRAMA DE INGENIERIA DE SISTEMAS

CARTAGENA DE INDIAS, D. T. Y C.

2011

DISEÑO E IMPLEMENTACION DE POLITICAS EN GESTION DE REDES PARA LA UNIVERSIDAD TECNOLOGICA DE BOLIVAR

LAURA VICTORIA YEPEZ RODRIGUEZ

JAVIER EDUARDO DIAZ MACHUCA

PROYECTO DE GRADO PARA OPTAR AL TITULO DE

INGENIERO DE SISTEMAS

JAIRO ALBERTO GUTIERREZ DIAGO

Ingeniero de Sistemas y Computación

M.Sc. Computer Science

Ph.D. Information Systems

DIRECTOR

UNIVERSIDAD TECNOLOGICA DE BOLIVAR

FACULTAD DE INGENIERIAS

PROGRAMA DE INGENIERIA DE SISTEMAS

CARTAGENA DE INDIAS, D. T. Y C.

2011

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma Comité de Investigación

_____
Firma del Evaluador

_____
Firma del Evaluador

Cartagena de Indias, D.T. y C., Bolívar, Colombia

A los ____ días de _____ de _____.

AUTORIZACION

Yo, LAURA VICTORIA YEPEZ RODRIGUEZ, manifiesto en este documento mi voluntad de ceder a la Universidad Tecnológica de Bolívar los derechos patrimoniales, consagrados en el artículo 72 de la Ley 23 de 1982 sobre Derechos de Autor, del trabajo final denominado DISEÑO E IMPLEMENTACION DE POLITICAS EN GESTION DE REDES PARA LA UNIVERSIDAD TECNOLOGICA DE BOLIVAR producto de mi actividad académica para optar al título de INGENIERO DE SISTEMAS de la Universidad Tecnológica de Bolívar.

La Universidad Tecnológica de Bolívar, entidad académica sin ánimo de lucro, queda por lo tanto facultada para ejercer plenamente los derechos anteriormente cedidos en su actividad ordinaria de investigación, docencia y extensión. La cesión otorgada se ajusta a lo que establece la Ley 23 de 1982. Con todo, en mi condición de autor me reservo los derechos morales de la obra antes citada con arreglo al artículo 30 de la Ley 23 de 1982. En concordancia suscribo este documento que hace parte integral del trabajo antes mencionado y entrego al Sistema de Bibliotecas de la Universidad Tecnológica de Bolívar.

_____

LAURA VICTORIA YEPEZ RODRIGUEZ

AUTORIZACION

Yo, JAVIER EDUARDO DIAZ MACHUCA, manifiesto en este documento mi voluntad de ceder a la Universidad Tecnológica de Bolívar los derechos patrimoniales, consagrados en el artículo 72 de la Ley 23 de 1982 sobre Derechos de Autor, del trabajo final denominado DISEÑO E IMPLEMENTACION DE POLITICAS EN GESTION DE REDES PARA LA UNIVERSIDAD TECNOLOGICA DE BOLIVAR producto de mi actividad académica para optar al título de INGENIERO DE SISTEMAS de la Universidad Tecnológica de Bolívar.

La Universidad Tecnológica de Bolívar, entidad académica sin ánimo de lucro, queda por lo tanto facultada para ejercer plenamente los derechos anteriormente cedidos en su actividad ordinaria de investigación, docencia y extensión. La cesión otorgada se ajusta a lo que establece la Ley 23 de 1982. Con todo, en mi condición de autor me reservo los derechos morales de la obra antes citada con arreglo al artículo 30 de la Ley 23 de 1982. En concordancia suscribo este documento que hace parte integral del trabajo antes mencionado y entrego al Sistema de Bibliotecas de la Universidad Tecnológica de Bolívar.

_____

JAVIER EDUARDO DIAZ MACHUCA

DEDICATORIA

Al gran Arquitecto del Universo por permitirnos hacer uso de la inteligencia como su principal herencia.

A la Universidad Tecnológica de Bolívar, por brindarnos la oportunidad de afianzar nuestros conocimientos, por permitirnos estar en contacto con sus tutores de los que tomamos lo mejor de sus saberes.

A los Compañeros de grupo que se convirtieron en puntos de referencia para buscar lo mejor de cada uno.

A Nuestros familiares que son en la mayoría de los casos el impulso al crecimiento.

LOS AUTORES.

AGRADECIMIENTOS

Al Gran creador, por enviarnos a esta dimensión a su imagen y semejanza, como únicas criaturas capaces de crecer a través de la reflexión, y proyectados como seres dinamizadores de cambio y transformación humana y espiritual.

A los maestros tutores, por sus espíritus de cooperación en el más alto grado de altruismo, y el interés mostrado para que cada uno de los miembros de este grupo fortaleciera sus conocimientos y saberes.

A Jairo Alberto Gutiérrez Diago, por regalarnos su tiempo y asumir el papel de Maestro y Asesor.

A Nuestros familiares por aceptar que robáramos tiempo a su compañía para poder cumplir con el compromiso que asumimos como estudiantes.

A La Universidad Tecnológica de Bolívar, por habernos albergado en su seno en estos productivos semestres de pregrado.

Cartagena de Indias, D.T. y C., 5 de Diciembre de 2011

Señores:

COMITÉ DE INVESTIGACIONES
Universidad Tecnológica de Bolívar
Facultad de Ingenierías
Programa de Ingeniería de Sistemas
Ciudad

Cordial saludo.

Adjunto a la presente hacemos entrega del proyecto de grado titulado **DISEÑO E IMPLEMENTACION DE POLITICAS EN GESTION DE REDES PARA LA UNIVERSIDAD TECNOLOGICA DE BOLIVAR** como requisito para optar al título profesional en Ingeniería de Sistemas.

Esperamos de su parte una respuesta satisfactoria y agradecemos su amable atención.

Lo anterior fue aprobado y revisado por el director de proyecto.

Atentamente,

LAURA V. YEPEZ RODRIGUEZ
C.C. No. 1.143.343.224

JAVIER E. DIAZ MACHUCA
C.C. No. 1.143.335.630

Cartagena de Indias, D.T. y C., 5 de Diciembre de 2011

Señores:

COMITÉ DE INVESTIGACIONES
Universidad Tecnológica de Bolívar
Facultad de Ingenierías
Programa de Ingeniería de Sistemas
Ciudad

Cordial saludo.

En calidad de director del proyecto de grado titulado **DISEÑO E IMPLEMENTACION DE POLITICAS EN GESTION DE REDES PARA LA UNIVERSIDAD TECNOLOGICA DE BOLIVAR** elaborado por los señores Laura Victoria Yepez Rodríguez y Javier Eduardo Díaz Machuca, manifiesto que he participado en la orientación del desarrollo del mismo en todas sus etapas y por consiguiente estoy satisfecho con los resultados obtenidos.

Atentamente,

_____

JAIRO A. GUTIERREZ DIAGO, PhD

CONTENIDO

1. INTRODUCCIÓN

Hoy en día las redes de telecomunicaciones se basan en diferentes tecnologías para transmitir datos, telefonía, videoconferencias y otros servicios. Estas redes suelen tener sistemas complejos de gestión extremadamente costosos y es la razón por la que los nuevos modelos de sistemas de gestión de redes heterogéneas se estudian. Esto incluye la capacidad de control de sus infraestructuras, garantizar el acuerdo de nivel de servicio (SLA) [1] contratado por el usuario, etc.

Como podemos observar, estas redes pueden llegar a ser muy complejas y por tanto requerir esquemas de gestión poderosos que optimicen la ejecución de los elementos que conforman la red. Los nuevos modelos de gestión de red ven la conjunción de redes heterogéneas interconectadas como un sistema integral en el que es posible resolver aspectos que van desde la planeación de tareas a largo plazo hasta la provisión de los recursos del día a día.

A lo largo de la historia podemos encontrar diferentes propuestas para simplificar todas las tareas de gestión de redes. Como ejemplos, podemos mencionar los sistemas de gestión de red mediante el Simple Network Management Protocol (SNMP) [2]: en 1989 se acogió como estándar para las redes TCP/IP y se hizo muy popular, luego adoptó una actualización conocida como SNMPv2c que incluía mejoras en la estructura de información de administración (SMI), y el SNMPv3 que surgió después para brindar acceso seguro a las MIB mediante la autenticación y

el cifrado de paquetes que viajan por la red, más tarde se da un gran paso hacia la administración de redes interconectadas gracias a RMON [3], el cual provee información vital sobre la red al administrador de redes. También vemos los sistemas de gestión donde los usuarios y la gestión de grupos de dispositivos de red de área local a través del Servicio de Información de la Red (NIS) [35], la conversión de nombres a direcciones IP en las redes utilizando Nombres de Dominio (DNS) [4], la tecnología adecuada para la gestión de red integrada como la arquitectura WBEM [5] o CORBA [6] que proporcionaron un acceso uniforme de gestión de información y la implementación de Java [7] como software de solución en gestión de red más barato en comparación con otros software (tales como las aplicaciones basadas en CORBA).

Todos estos recursos nos muestran sólo una solución parcial a varios problemas. Sin embargo, la gestión de la red como una unidad del sistema integral es una tarea muy compleja que debe resolver diferentes aspectos tales como la programación a largo plazo y la disposición del día a día de los recursos. Uno de los mayores retos de hoy en día es el de mejorar las tareas de gestión automatizada y ampliar su área de aplicación teniendo en cuenta siempre la integridad, seguridad y confiabilidad en el sistema.

Con la gestión de red basada en políticas (PBNM) [8] se presenta una posible solución a este problema. Ofrece un control dinámico y coordinado de los elementos de la red ya que las decisiones se toman de manera automática basándose en reglas, peticiones de usuarios o de servicios. Esta gestión dinámica

de los elementos de la red representa un cambio cualitativo, desde el punto de vista empresarial, ya que permite la gestión de los recursos de la red y de los servicios de manera más eficiente.

Consideramos que la Universidad Tecnológica de Bolívar (UTB) cree en el desarrollo de reglas que puedan ser entendidas presentando una descripción de estas, para conllevar a hacer de la red un ambiente seguro en los estudiantes, profesores y administrativos de la institución.

1.1. FORMULACIÓN DEL PROBLEMA

En términos generales, la Gestión de Redes Basada en Políticas (Policy Based Network Management, PBNM) es aquella que dirige y restringe, de forma autónoma, el comportamiento de un sistema según reglas de alto nivel que expresan la “política” del administrador del sistema.

Estamos estudiando la Gestión de Redes Basada en Políticas porque es un paradigma que permite reducir la complejidad de gestionar y controlar redes de telecomunicaciones y facilitar la adaptación de la red ante cambios en el ambiente gestionado para la Universidad Tecnológica de Bolívar dándole flexibilidad y escalabilidad de la cual carece el sistema tradicional.

Creemos que la implementación de las recomendaciones de esta investigación traerá mejoras en la gestión de la red Universitaria, porque la utilización de las políticas permiten realizar muchas de las tareas o actividades de gestión, desde las más simples hasta las más complejas de forma más ágil, sencilla y con cierto grado de autonomía brindando una gestión mucha más proactiva.

Así pues, ¿qué conceptos se deben conocer para diseñar e implementar políticas en gestión de red, mediante un caso de estudio para la Universidad Tecnológica de Bolívar y sirva como complemento de enseñanza en la Administración y Seguridad de la red Universitaria?

1.2. JUSTIFICACIÓN

En la actualidad se están realizando diversos esfuerzos para realizar la visión futurista de las redes de telecomunicación auto gestionadas. La gestión de red basada en políticas ha sido reconocida como una herramienta potencial para habilitar esta visión. Mayoritariamente, ésta técnica ha sido reconocida como proveedora de flexibilidad, adaptabilidad y soporte para asignar recursos, controlar Calidad de Servicio y Seguridad, de una manera automática y de acuerdo a reglas administrativas [9]. Adicionalmente, se ha considerado que la gestión basada en políticas proveería tal flexibilidad en tiempo de ejecución y como resultado de cambios en la red, interacciones entre usuarios, aplicaciones y disponibilidad de recursos.

En un sentido más amplio, una política [10] es una especificación de los objetivos o de un conjunto de acciones a desempeñar en el futuro como resultado de una actividad regular.

Las políticas representan objetivos o metas de negocios, así que una transformación se debe realizar para pasar los objetivos o metas de negocios a las metas de la red. Un ejemplo de esto puede ser los Acuerdos sobre niveles de servicios (SLA), los cuales son usados para proveer un servicio de red específico a los clientes [11].

A continuación se muestra el esquema para el uso de PNMB:

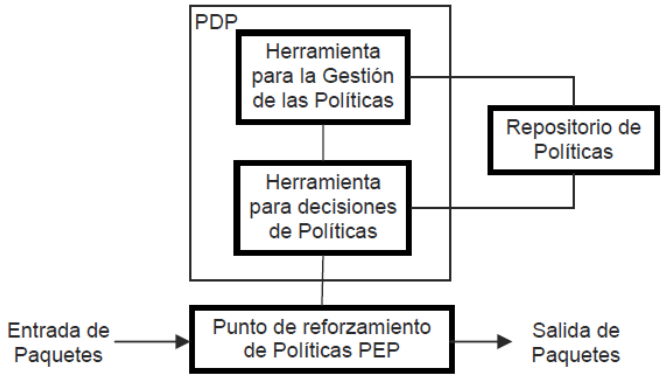

Fig. 1. Gestión de Redes Basado en Políticas. [31]

Como se puede observar en la figura anterior un esquema de Gestión de Redes Basado en Políticas está compuesto de 3 partes principales [12]:

Punto de Decisión de Políticas (Policy Decision Point, PDP): Este punto cuenta con una interfaz para la captura de las políticas, un módulo en donde se toman las decisiones necesarias dependiendo de las políticas y realizara la traducción de esta política a código entendible por el elemento de red.

Punto de Refuerzo de Políticas (Policy Enforcement Point, PEP): En este lugar es donde las políticas son aplicadas, previa pregunta al PDP sobre qué política tiene que aplicar.

Repositorio de Políticas: En este lugar donde se guardan las políticas.

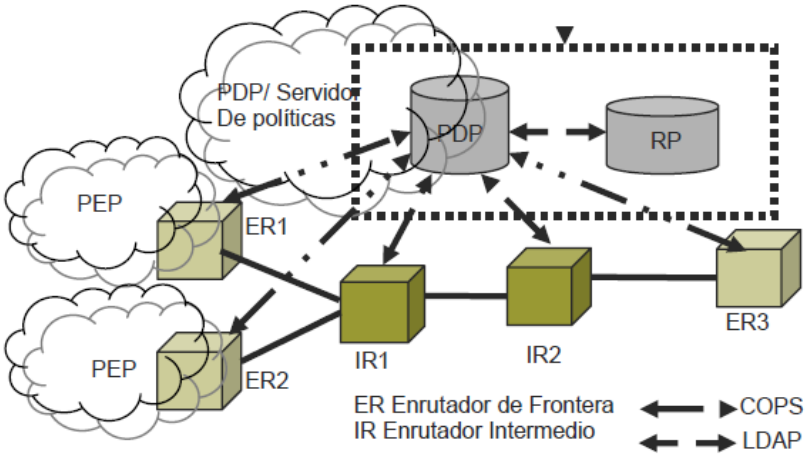

Fig. 2. Esquema de red para la aplicación de PBNM. [31]

En un esquema de red, las políticas se aplican en los enrutadores de frontera y esto se hace mediante un protocolo llamado Servicio Común de Políticas Abiertas (COPS) [13], este protocolo funciona en un esquema cliente-servidor bajo el protocolo TCP. La información que se intercambia entre el PDP y el Repositorio de Políticas se hace utilizando el Protocolo de Acceso Directo Liviano (LDAP) el cual encripta la información que envía sobre el Protocolo TCP.

A pesar de los enormes avances realizados en la industria y la penetración que ha tenido este sistema de gestión con lenguajes de especificación de políticas, arquitecturas de gestión en diversos dominios y estandarización, la gestión de red basada en políticas en la Universidad Tecnológica de Bolívar aún no es una realidad.

Esta Tesis aborda el problema de políticas de gestión de la red de la Universidad Tecnológica de Bolívar. Damos una visión de lo que hay en la red y lo que proponemos para mejorar tal situación.

Las políticas tienen como objeto definir un conjunto de directivas o normativas especificadas por el administrador para gestionar ciertos aspectos de la Universidad Tecnológica de Bolívar (UTB) que garanticen la integridad y confidencialidad de la información fundamentada en la Gestión de red basada en Políticas (PBNM).

Inicialmente se estudiará la red de la Universidad en sus dos campus para proponer nuevas políticas basadas en PBNM (Policy Based Network Management), desde el estudio y análisis formal hasta la creación de las políticas o reglas en su utilización.

Utilizamos una metodología de caso de estudio para aplicar los conceptos introducidos en el marco de trabajo desarrollado en esta Tesis en sistemas de Gestión de Red Basada en Políticas.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Analizar cómo se está llevando a cabo la gestión de red de la Universidad Tecnológica de Bolívar y aplicar los conceptos de políticas en gestión de red para implementar estas mediante un caso de estudio específico hacia la red de campus universitario.

1.3.2. OBJETIVOS ESPECIFICOS

1. Identificar cuáles son las políticas institucionales que se pueden implementar con las técnicas de Gestión de Red basada en Políticas (PBNM).
2. Establecer las directrices necesarias para el correcto funcionamiento de la red Universitaria de la Tecnológica de Bolívar, mediante las normativas y políticas de Gestión de red.
3. Transformar políticas de administración gerencial de alto o mediano nivel a políticas de bajo nivel para PBNM.
4. Conocer como se está llevando a cabo la gestión de red de la Universidad y presentar un levantamiento de información para determinar las políticas necesarias en la red universitaria.
5. Otorgar un conjunto de políticas creadas y editadas por un lenguaje de implementación y guardarlas en un repositorio siguiendo el modelo esencial de Gestión de redes basada en Políticas.

1.4. ADMINISTRACION DEL PROYECTO

Las relaciones de las personas a participar, especificando su calificación profesional y su función de investigación para la realización del proyecto: “Diseño e Implementación de Políticas en Gestión de Redes para la Universidad Tecnológica de Bolívar”, al igual que el cronograma de trabajo, están referenciados en el anexo [A1].

2. MARCO TEÓRICO

2.1. INTRODUCCIÓN A LA GESTIÓN DE REDES

Al principio las primeras redes de ordenadores eran relativamente pequeñas y no era tan necesaria una administración compleja. Los años fueron pasando y las necesidades de las redes aumentando. A medida en que la red aumentaba y evolucionaba, esta se convertía en un recurso crítico para la organización.

Entonces con esta necesidad nace una administración definida como la suma total de todas las políticas que intervienen en la planeación, configuración, control de monitoreo de los elementos que conforman a una red, con el fin de asegurar el eficiente y efectivo empleo de sus recursos lo cual se verá reflejado en la calidad de los servicios ofrecidos.

2.2. SNMP

Es el protocolo más amplio para la gestión de redes. Este protocolo trabaja en la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

La versión original de SNMP conocido como SNMPv1 se convirtió rápidamente en el proveedor independiente más utilizado en gestión de red. Sin embargo, sus deficiencias se hicieron evidentes. Estos incluyen la falta de comunicación administrador a usuario, la incapacidad de hacer la transferencia de datos y la falta de seguridad. Todas estas deficiencias se abordaron en SNMPv2, publicado como un conjunto de estándares de Internet propuesto en 1993.

El modelo de gestión de red que se utiliza para SNMP incluye los siguientes elementos clave:

- Administración de la estación
- Agente de administración
- Gestión de base de información
- Network Management Protocol

Una estación de administración suele ser un dispositivo independiente, pero puede ser una capacidad de aplicación en un sistema compartido. En cualquier caso, la estación de administración sirve como interfaz para el administrador de la red en el sistema de gestión de red. La estación de administración tendrá, como mínimo:

- Un conjunto de aplicaciones de gestión para el análisis de datos, recuperación de fallos, y así sucesivamente.
- Una interfaz que permite al administrador de red poder monitorear y controlar la red. Es decir, la interfaz entre el usuario y las aplicaciones de gestión de red permite al usuario solicitar acciones seguimiento y control

que se llevan a cabo por la estación de administración mediante la comunicación con los elementos gestionados de la red.

- Un protocolo por cada estación de administración y control de cambios controlados y entidades de gestión de información.
- Una base de datos de información de gestión de todas las entidades gestionadas en la red. Es decir, la estación de administración mantiene al menos un resumen de la gestión de la información mantenida en cada uno de los elementos gestionados en la red.

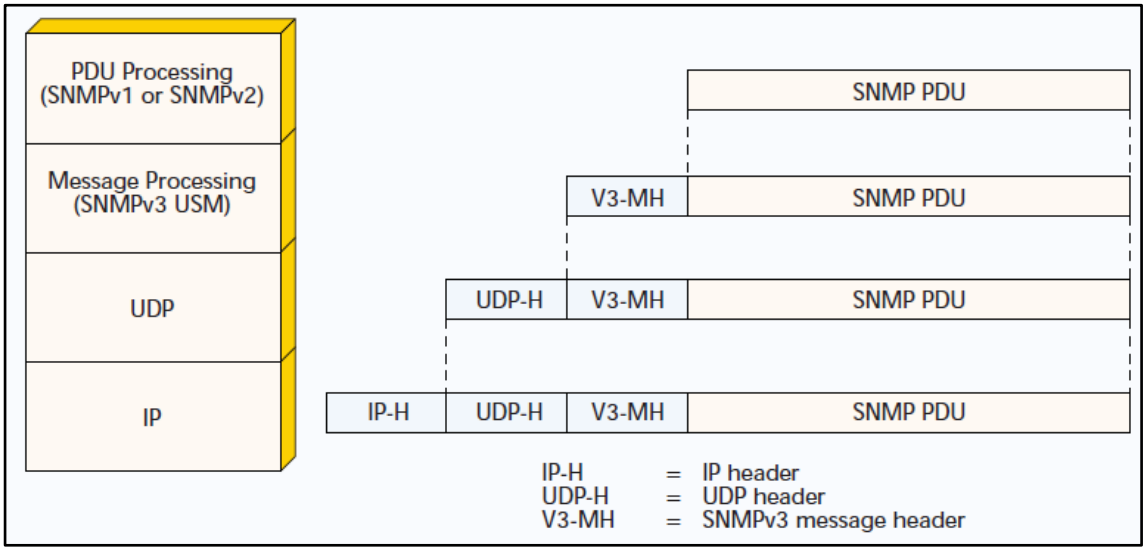

Fig. 3 SNMP protocol architecture [33]

2.3. Common Object Request Broker Architecture (CORBA)

CORBA [6] es una arquitectura de software por el Object Management Group (OMG) para el desarrollo de aplicaciones distribuidas basadas en el paradigma orientado a objetos. El Object Request Broker (ORB) proporciona los mecanismos por los que los objetos de forma transparente envian solicitudes y reciben respuestas, que proporciona interoperabilidad entre aplicaciones en diferentes máquinas en entornos de sistemas distribuidos y perfectamente interconectados con los sistemas de varios objetos.

Los componentes de una aplicación basada en CORBA son objetos cuyas interfaces se definen con un lenguaje de definición de interfaces (IDL) e implementados en algún lenguaje de programación (C, C + +, Smalltalk, Java, etc.) Por lo tanto, una aplicación CORBA consiste en un conjunto de objetos que interactúan a través de los mecanismos de comunicación con el apoyo de la ORB. En cada interacción entre dos objetos, uno juega el papel de cliente (que tiene acceso a una referencia de objeto e invoca alguna de las operaciones definidas en la interfaz del objeto) y el otro juega el papel de servidor (la implementación del objeto es de recibir la operación con sus parámetros, ejecutarla y dar vuelta el resultado para el cliente). Todos los traslados entre el cliente y el servidor son compatibles con la plataforma CORBA y ocultos para el cliente y el servidor. Localización de objetos, implementación del objeto y el estado del objeto de ejecución (el ORB se encarga también de la partida y la activación de un objeto

antes de entregar una solicitud a la misma) son una de las principales ventajas que proporciona CORBA.

Además, CORBA especifica un conjunto de protocolos inter-ORB que permiten la interacción transparente entre los objetos que residen en ORBs de diferentes proveedores, y facilitan la integración con los protocolos y aplicaciones existentes en otros entornos como Open Software Foundation (OSF), DCE y COM de Microsoft. Estas características permiten la integración de sistemas heredados a través de plataformas heterogéneas [6].

2.4. Web-Based Enterprise Management (WBEM)

Es un conjunto de tecnologías de gestión y de Internet. Es un estándar desarrollado para unificar la gestión de entornos de computación distribuida. WBEM proporciona la capacidad de ofrecer un conjunto bien integrado de herramientas de gestión basadas en estándares, facilitando el intercambio de datos a través de tecnologías [5].

Como una tecnología, WBEM proporciona una forma para que las aplicaciones de gestión compartan datos independientemente del vendedor, protocolo, sistema operativo o estándar de gestión.

El DMTF ha desarrollado un conjunto núcleo de estándares que componen a WBEM, el cual incluye un modelo de datos, el estándar CIM; una especificación de

codificación, xmlCIM; y un mecanismo de transporte, Operaciones CIM sobre HTTP.

2.4.1. ARQUITECTURA WBEM

WBEM [5] está basado en un programa que corre sobre el sistema gestionado, llamado CIMOM (CIM Object Manager). El CIMOM es accedido por una aplicación cliente que monitorea y controla el dispositivo gestionado. Para atender los requerimientos de la aplicación cliente, el CIMOM usa proveedores, quienes son los que realmente realizan las tareas de gestión ya que ellos acceden los diferentes recursos.

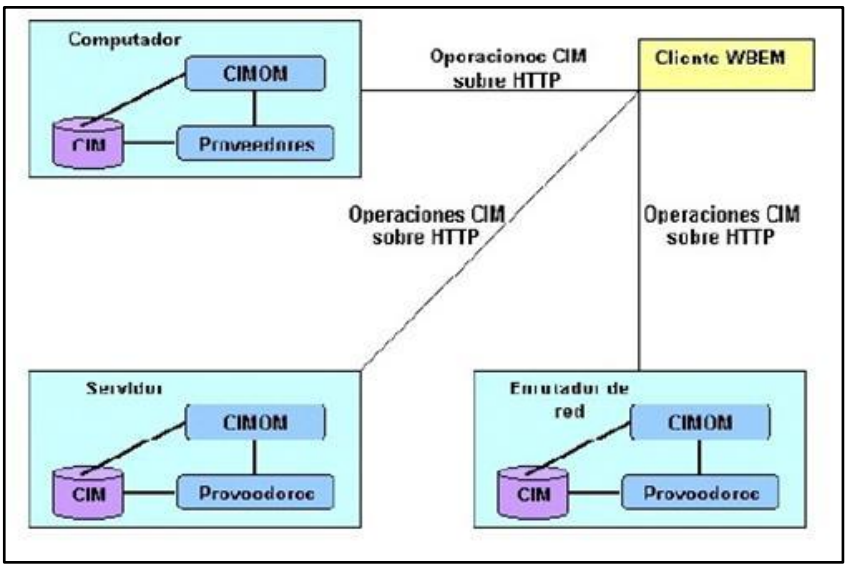

Fig. 4 Arquitectura WBEM [5]

2.5. JAVA-BASED NETWORK MANAGEMENT

Java, al ser un lenguaje de programación portátil y orientado a objetos, es la instrumentación de una amplia variedad de paradigmas de gestión de red, que van desde la computación distribuida, de gestión basada en web, o para agentes inteligentes. Debido a este amplio campo de aplicación, muchas gestiones basadas en Java han sido propuestas diseñadas para el apoyo a las aplicaciones de gestión de red [7].

Lo que hace una buena tecnología Java para la red gestión en general es en primer lugar, el despliegue de soluciones basadas en Java en un software relativamente barato en comparación con otras soluciones de gestión de software, tales como Aplicaciones basadas en CORBA. La máquina virtual Java (JVM) es en tiempo de ejecución solo el apoyo que necesita un software basado en Java, y también es fácil de implementar y requiere de muy poco mantenimiento. En segundo lugar, a medida que más y más este habilitada la JVM [7], los dispositivos de la red estarán más tiempo disponibles y también lo hace la disponibilidad del soporte para Java.

Además, Java podrá entrar a trabajar con los navegadores web, que son buenos candidatos para las consolas de administración. En tercer lugar, es dinámico y la descarga de código permite la distribución dinámica de los objetos Java. Esto no sólo abre la oportunidad para las extensiones de servicio en tiempo de ejecución, sino que también abre la oportunidad a las delegaciones de gestión. En cuarto

lugar, Java es la plataforma independiente, portátil, en cualquier plataforma de gestión existente que apoya la JVM. Por último, el software de Java es fácil de desarrollar, ya que existen muchos apoyos para el desarrollo del entorno y de sus herramientas.

2.6. AGENTES INTELIGENTES

Los agentes inteligentes [32] tienen las siguientes características: Autonomía, habilidad social, reactividad, pro actividad, movilidad, aprendizaje y convicción. Los agentes inteligentes son entidades independientes capaces de realizar actividades complejas y resolver problemas para su administración. A diferencia de la movilidad de código, los agentes inteligentes no necesitan recibir instrucciones de trabajo para su funcionamiento, solo necesitan los objetivos de alto nivel. El uso de los agentes inteligentes niega completamente la necesidad de agentes dedicados, pues ellos realizan las tareas de gestión de la red de forma distribuida y coordinada a través de comunicaciones entre las gerencias [32].

Muchos investigadores creen que los agentes inteligentes son el futuro de la gestión de redes, ya que el uso de estos agentes inteligentes es muy ventajoso. En primer lugar, los agentes inteligentes proporcionan soluciones totalmente escalables para la mayoría de las áreas en la gestión de redes. Cada jerarquía de los agentes inteligentes podría realizar tareas fáciles dentro de su entorno local y luego unirse de manera global para realizar un mismo objetivo, para el

mantenimiento del uso de las redes generales cerca de los máximos. En segundo lugar, el procesamiento de datos y la toma de decisiones son de forma distribuida, que alivia los cuellos de botellas que se ven en la gestión centralizada de las soluciones de gestión de redes. Además, el sistema de gestión de red resultante es mucho más robusto y tolerante a fallos, pues el mal funcionamiento de algunos agentes no tiene impacto significativo en la gestión de red global. En tercer lugar, el sistema de gestión de redes es la red autónoma, sólo los administradores tendrían que proporcionar las directivas de nivel de servicio al sistema.

Por último, los agentes inteligentes son de auto-configuración, auto- gestión y auto-motivación. Al final, es posible construir un sistema de gestión de redes que es completamente autónomo y se auto-mantiene. Tal sistema en gran medida alivia la carga de la red rutinas de manejo que un administrador de red tiene que en la actualidad.

2.7. Policy Based Network Management (PBNM)

La gestión basada en políticas hace referencia a la agrupación de recursos (personas y equipo) basada en las políticas (reglas) que determinan cómo interactuarán entre sí [16] [17].

La gestión basada en políticas permite asegurar calidad de servicio de extremo a extremo mediante una serie de reglas del tipo de los sistemas expertos o automatizados para proporcionar calidad o clases de servicio basadas en

prioridades ya sea de usuario, de servicio o de red. El código de instrucción (acción) puede residir en cualquier combinación de sistemas de gestión de redes, routers, conmutadores, servidores, bases de datos, aplicaciones y sistemas de almacenamiento. Aunque actualmente las políticas suelen implementarse en routers y conmutadores, es posible hacer que las políticas residan en módulos de software cargables en los nodos de hardware, en programas dependientes de las plataformas de gestión de red o en servidores dedicados específicamente a esta tarea [16] [17].

Estos elementos se encargan de recibir las peticiones de tráfico solicitadas por los conmutadores u otros nodos, recabar información de políticas de bases de datos y directorios, y, en consecuencia, configurar los dispositivos de red de acuerdo con las peticiones recibidas y los derechos establecidos en la especificación de nivel de servicio acordada entre el usuario y el proveedor de servicio Internet.

2.7.1. Lenguajes De Libre Distribución De Políticas

Los lenguajes de libre distribución para políticas definen y aplican las políticas en la red, para ello utilizan un gestor que controla los recursos de la red mediante un conjunto de políticas predefinidas. Los lenguajes de políticas especifican reglas que son independientes de las entidades que implementan las políticas. Estos lenguajes se definen en términos de métricas de ejecución como ancho de banda,

retraso y pérdida de paquetes y permiten la definición de eventos y condiciones de red.

La mayoría de los lenguajes de políticas siguen el modelo de políticas, es decir, tienen como componentes elementales un PDP, uno o varios PEPs, un servidor de políticas y un repositorio LDAP para las políticas. Existen diversos lenguajes de libre distribución para la gestión basada en políticas, algunos de ellos dan mayor énfasis a la seguridad, otros a la gestión de recursos.

- Ponder del Imperial College of Science en Inglaterra.
- Policy Description Language (PDL) de la Universidad de Munich
- Security Policy Language (SPL) del Institute Mageland en Portugal

2.7.1.1. Ponder

Ponder es uno de los lenguajes de políticas de libre distribución más antiguos y avanzados [34]. Es un lenguaje declarativo orientado a objetos para especificar políticas de gestión y de seguridad para sistemas de objetos distribuidos. El lenguaje permite cubrir el amplio rango de los requerimientos actuales que presentan los paradigmas de los sistemas distribuidos.

Ponder utiliza dominios para facilitar la especificación de políticas relacionadas a sistemas grandes, con millones de objetos; las políticas se especifican para

colecciones de objetos almacenados en dominios en lugar de objetos individuales, lo cual proporciona escalabilidad y flexibilidad.

Las políticas que Ponder soporta incluyen: Políticas básicas, compuestas y meta - políticas. Las políticas básicas pueden ser:

1. Políticas de autorización. Definen control de acceso y uso de privilegios sobre los objetos destino.

2. Políticas de obligación. Especifican políticas que deben ser ejecutadas sobre determinados objetos cuando ocurren eventos específicos.

3. Políticas por delegación. Especifican acciones que un usuario puede delegar a otros.

Las políticas compuestas constan de:

1. Grupos: Son políticas y restricciones que tienen relaciones semántica similares y deben utilizarse conjuntamente.
2. Roles: Especifican derechos y obligaciones para posiciones organizacionales.
3. Relaciones: Entre políticas que definen roles.
4. Tipo de especialización: Permiten la extensión a nuevas definiciones de políticas utilizando la herencia.

Hemos elegido Ponder porque es el único lenguaje en la actualidad de código abierto y de gran éxito usado por la industria, la academia, y además es de libre

distribución. Es un lenguaje que se puede utilizar para especificar políticas de seguridad y de gestión de redes. Se puede determinar políticas de autorización para diversos mecanismos de control como Firewall, Sistemas Operativos, Bases de datos y Java, también políticas de Obligación que desencadena un Evento-Condición-Acción (ECA) como normativa para gestionar la red. Posee conceptos claves como los dominios para agrupar los objetos a los cuales se les aplicaran las políticas, Las reglas de las políticas, y las funciones que tendrán dentro de un dominio específico.

3. ESTADO DEL ARTE

Anterior a la década de los 80 existía algo que se llamaba Policy Based Management (PBM) [14], el cual es un modelo de gestión que separa las normas que rigen el comportamiento de un sistema. Las políticas de autorización deben especificar lo que las actividades de un gerente, las que son permitidas o prohibidas hacer a un conjunto de objetos de destino y son similares a las políticas de seguridad de control de acceso.

En esta época se observaron diferentes modelos de seguridad basados en políticas como lo son el de Access-control matrices (1966,1969); En este modelo, la característica esencial de un dominio es que tiene potencial derechos de acceso diferentes a otros dominios. Los objetos se reparten entre los dominios y son las cosas del sistema que requieren protección. Objetos típicos incluyen procesos, archivos, segmentos de memoria, terminales, y dominios. El acceso de control se asegura mediante un control de acceso de la matriz. Cada uno (dominio, objeto) como entrada en la matriz contiene una lista de accesos a los atributos que definen los derechos de acceso de ese dominio a los objetos. Los atributos pueden ser de diferentes formas, tales como leer, escribir, propietario de llamadas, control, etc. [14].

Otro de los modelos más destacados de la época es el Modelo de Bell-LaPadula (1973) [15] que también es considerado como el primer modelo formal de confidencialidad de los datos a través de políticas. Una política de confidencialidad

impide la divulgación no autorizada de información, por tal, el modelo se basa en una máquina de estados.

En la década de los 80 el área de implantación de sistemas y las redes de telecomunicaciones se expanden. Así es como las empresas empiezan a sentir la necesidad de una nueva administración de la gestión de red. Cuando las empresas empezaron a expandir sus redes, con más ordenadores y mayor variedad de tipos de dispositivos (servidores, routers, firewall), esta tendencia de crecimiento trajo con ello un gran problema el costo de las redes y una mayor administración, se necesitaba personal ampliamente capacitado para la administración de dicha red y sobre todas las cosas una gestión de red eficiente para asegurar con ello la disponibilidad, supervisión y resolución de problemas, etc. Estas herramientas son las que se denominan sistemas de gestión de red.

Alrededor de hace una década, empezaron las actividades acerca de Policy Based Network Management (PBNM) [16] [17]. Aunque la idea de políticas viene de años anteriores esto nace con el aumento de tamaño y complejidad de la gestión y los requerimientos de los servicios que demandan las redes de hoy, por el contrario, los modelos de gestión planteados con anterioridad no cubrían la necesidad y esta debió ser reemplazada con una gestión de red distribuida.

Los primeros pasos de la gestión de red distribuida se basaron en Simple Network Management Protocol (SNMP) [17]: Este fue diseñado para proporcionar una fácil administración de la capa de aplicación basada en los índices más altos de redes

múltiples. La versión original de SNMP se apodero rápidamente del mercado como el protocolo más usado, pero al poco tiempo se empezó a notar sus deficiencias tales como la falta de comunicación administrador a administrador, la incapacidad para la transferencia de datos a gran volumen y la falta de seguridad.

Por estas deficiencias fue que se pensó en una nueva versión de Simple Network Management Protocol (SNMPv2) que fue publicado como un grupo de estándares de internet propuesto en 1993, el cual brinda soporte a las estrategias administrativas distribuidas y centralizadas e incluía las mejoras en la estructura de la información de administración (SMI) [18], las operaciones de protocolos, la arquitectura administrativa y la seguridad [19]. Fue diseñado para trabajar en ambos modelos como el OSI [18] y TCP/IP [19].

Las mejoras más notables fueron la introducción del tipo de mensajes GetBulkRequest, que era un método ineficiente para recolectar la información. En el SNMPv1 solo se podía solicitar una variable a la vez. El tipo de mensaje GetBulkRequest soluciona esta debilidad ya que solicita más información con tan solo una petición. En segundo lugar, los contadores de 64 bits resolvieron el problema del rápido reinicio de los contadores, especialmente con los enlaces de mayor velocidad Gigabit Ethernet [20].

A pesar que el SNMP versión 2 fue muy aceptado se pensó en una nueva versión de Simple Network Management Protocol (SNMPv3). Para resolver las limitaciones del SNMP versión uno y dos, el SNMPv3 brinda un acceso seguro

para las MIB mediante autenticación y el cifrado de los paquetes que viajan por la red. Es importante resaltar que SNMPv3 no es un estándar que va a reemplazar las versiones anteriores, este define la seguridad en conjunto con cualquiera de las versiones anteriores preferiblemente la versión dos.

De los 90 surgieron los denominados modelos de gestión de red integrada, que definían un protocolo y unos modelos de información de gestión estándares con el objetivo de que fuesen adoptados por distintos fabricantes, permitiendo en teoría la interoperabilidad entre gestores y elementos gestionados de múltiples fabricantes. Algunos modelos más relevantes son:

ENTORNO	PROTOCOLO	LENGUAJE	MODELOS DE INFORMACION
TMN/OSI	CMIP	GDMO	X.721, M.3100
Internet	SNMP	SMI	MIB II, Otros
Desktops	DMI	MIF	Master MIF
Procesos Distribuidos	CORBA/IIOP	IDL	X.780, M.3120
Web Based Management	HTTP/XML	MOF/CIM	CIM Schemas

Tabla 1. Modelos de Gestión de Red Integrada. [9]

Estos modelos de gestión permiten emprender la gestión de recursos heterogéneos utilizando un mismo mecanismo de comunicaciones y acceso a la

información de gestión, oponiéndose a los mecanismos de gestión propietarios de los fabricantes.

Cada una de las propuestas ha especializado en ámbitos diferentes: mientras que la gestión OSI se utiliza sobre todo para la gestión de equipos y servicios de redes de telecomunicación a través de la arquitectura TMN (Red de Gestión de Telecomunicaciones) [21], SNMP se utiliza ampliamente en Internet y está más orientado a la gestión de equipos y servicios de redes de datos, DMI se utiliza para la gestión de equipos de mesa como computadores portátiles, y la aplicación de la tecnología CORBA [22] de procesamiento distribuido permite acceder directamente a los parámetros gestionables de aplicaciones que proporcionan un servicio.

Todo esto supone un nuevo obstáculo para alcanzar una verdadera gestión de red integrada. En este escenario de utilización de múltiples modelos de gestión de red integrada surge la misma problemática que se intentó solucionar con dichos modelos (recursos heterogéneos), ya que un mismo gestor tendrá que interactuar con recursos de distintos entornos utilizando distintos mecanismos. El problema de esta falta de interoperabilidad radica en que cada modelo de gestión utiliza su propio protocolo, su propia definición de gestión y su propia estructura de información, como puede verse en la Tabla 1.

Una vez que un conjunto de políticas se generaba después de un proceso de refinamiento, ya sea manual o automático, no era suficiente comprobar la sintaxis

de las nuevas políticas antes de que se hayan desarrollado dentro del sistema. El despliegue de políticas contradictorias en un sistema causaba comportamientos anormales que eran generalmente difíciles de diagnosticar y medir [23]. Existen tres tipos de conflictos: (i) Obligation Conflicts, (ii) Unauthorized Obligation conflicts y (iii) Authorization conflicts. La resolución de conflictos entre las reglas de política ha sido estudiada desde hace tiempo en muchas áreas, tales como la inteligencia artificial y las bases de datos.

En los últimos años se han puesto en acción muchas gestiones de redes basadas en políticas: En el 2005 se obtuvo un gran avance en Administración Basada en políticas de los sistemas de computación en red (PMAC), que es una plataforma política de middleware (es un software de conectividad que ofrece un conjunto de servicios que hacen posible el funcionamiento de aplicaciones distribuidas sobre plataformas heterogéneas) genérica que se puede utilizar para administrar varios aspectos de una escala de sistemas distribuidos de gran tamaño, como la calidad de servicio (QoS), la configuración y auditoría. Otro objetivo igualmente importante de la plataforma PMAC es proporcionar los componentes de software que puede ser embebido en aplicaciones de software para reducir el costo de la escritura de aplicaciones capaces de tomar la entrada de una gestión basada en políticas del sistema [24].

Son muchos los beneficios de la gestión basada en políticas, como son las alternativas inteligentes para la asignación de los recursos a cada uno de los

usuarios de la red, una mejor calidad de servicio, seguridad, disponibilidad, mejorar la forma de configuración de los equipos.

Las políticas también tienen sus propios lenguajes de especificación que son la forma adecuada de representación. Clark's Policy Term (1989) [25] constituye una de las primeras especificaciones de las políticas para redes. Clark propone una plantilla para presentar las políticas llamada Policy Term. La escalabilidad se logra mediante el uso de Regiones Administrativas (ARs), que permiten incluir redes, enlaces, routers y Gateway. La notación utilizada por Clark era un buen punto de partida para la representación abstracta de políticas de red, sin embargo carece de la capacidad de representar rutas de acceso explicitas por una secuencia de ARS como parte de los términos [26].

Traffic flow policy languages (1998-2001) son relativamente lenguajes de políticas de bajo nivel que hacen uso de patrones en la selección de la red al tráfico en que una política puede ser aplicada. Su eficiencia en la gestión basada en políticas es limitado, ya que no proporciona una visión general de como la política del sistema administra la red de trabajo. Una política es simplemente un dispositivo abstracto de representación de la funcionalidad de un nodo. PAX-PDL [27], SRL [24] y PPL [26] son unos ejemplos de esas lenguajes.

En los últimos años ha habido una tendencia en generar un modelo de gestión de red basado en políticas; Una política es definida como un conjunto de directivas especificadas por el administrador para gestionar ciertos aspectos de los

resultados deseados de las interacciones entre usuarios, entre aplicaciones, y entre usuarios y aplicaciones. Las políticas proporcionan las guías para especificar como los diferentes elementos de red, como por ejemplo routers, switches, servidores, firewalls, deberían manejar el tráfico generado por los diferentes usuarios y aplicaciones. Cada política está formada, como mínimo, de una cláusula de condición y una cláusula de acción. Si la cláusula de condición es verdadera entonces las acciones definidas en la cláusula acción son ejecutadas. Por lo tanto la política es representada como un conjunto de clases y relaciones que definen la semántica de la construcción de bloques de representación de política (Figura 3). Estos bloques están formados como mínimo de una regla de política, una condición y una acción [28].

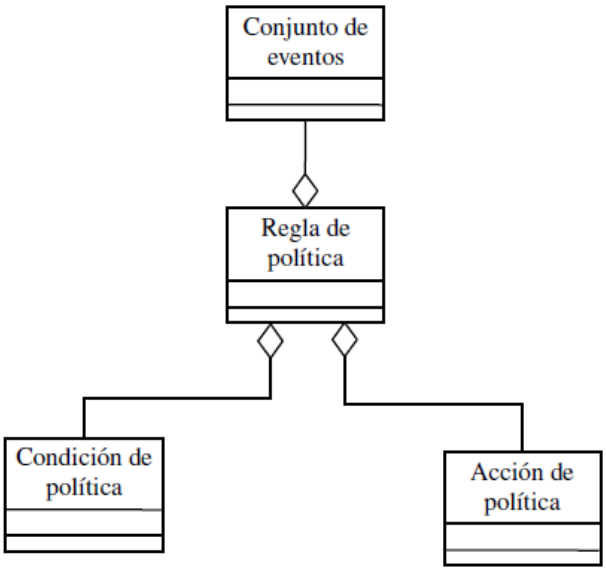

Fig. 3. Representación de los bloques que representan un modelo de Políticas simples. [31]

El término de Gestión de red basado en políticas (PBNM – Policy Based Network Management) es un método independiente para facilitarle al administrador la operación de redes basadas en IP e introducir el concepto de control dinámico. En este tipo de arquitectura el comportamiento del sistema es especificado por reglas de políticas de alto nivel y no por configuraciones explícitas de elementos del sistema individuales como en las redes tradicionales. Las políticas son los enlaces entre una especificación de servicio deseado de alto nivel y configuraciones de los elementos de red que proporcionan esos servicios. Las políticas pueden manejar configuración de red, incluyendo QoS, Service Level Agreement (SLA), Virtual Private Network (VPN), y problemas de seguridad, por mencionar algunas.

La gestión basada en políticas simplifica la gestión de red por medio de dos técnicas básicas:

- *Configuración centralizada*: La configuración de la red es especificada no solamente configurando cada dispositivo de red individualmente, sino especificando las políticas para la red completa en una localización central.
- *Abstracción simplificada*: Cuando se ofrece una abstracción de alto nivel simplificada de la configuración de los dispositivos físicos, el administrador solo debe introducir las políticas en término de las actividades del día a día.

La arquitectura de políticas definida por el IETF está formada por una serie de componentes funcionales (Figura 4). La herramienta de gestión de políticas es utilizada por el administrador para especificar las diferentes políticas que estarán

activas en la red. La herramienta recibe como entrada las políticas de alto nivel que un usuario o administrador introduce en la red y las convierte a políticas de bajo nivel que pueden ser aplicadas a los diferentes dispositivos que conforman la red. Todas las políticas generadas por la herramienta de gestión son almacenadas en un contenedor de políticas (PR – Policy Repository). El PR puede ser usado para almacenar las políticas generadas. Los dispositivos que pueden aplicar y ejecutar las diferentes políticas son conocidos como Punto de ejecución de políticas (PEP - Policy Enforcement Point). El PEP usa un elemento intermediario conocido como Punto de decisión de políticas (PDP - Policy Decision Point), el cual se comunica con el PR mediante algún protocolo de comunicación (comúnmente el PR es un servicio de directorio basado en el protocolo LDAP [29]) y es el responsable de interpretar las políticas almacenadas en el PR y proporcionar respuesta a las peticiones realizadas por él. El PDP tiene tres tareas básicas:

1. Consultar las políticas existentes en el repositorio.
2. Traducirlas al formato específico del dispositivo.
3. Distribuirlas a los PEPs.

El PDP es el elemento principal de la arquitectura definidas por IETF y es el encargado de tres tareas básicas: realizar consultas de las políticas existentes en el contenedor, llevar a cabo la traducción de cada política al formato específico por el dispositivo y distribuirlas a los PEPs de acuerdo a las peticiones realizadas [11]. El PDP puede hacer uso de mecanismos y protocolos adicionales para llevar a

cabo funcionalidades adicionales. La comunicación entre el PDP y el PEP comúnmente es llevada a cabo mediante el protocolo Common Open Policy Service (COPS).

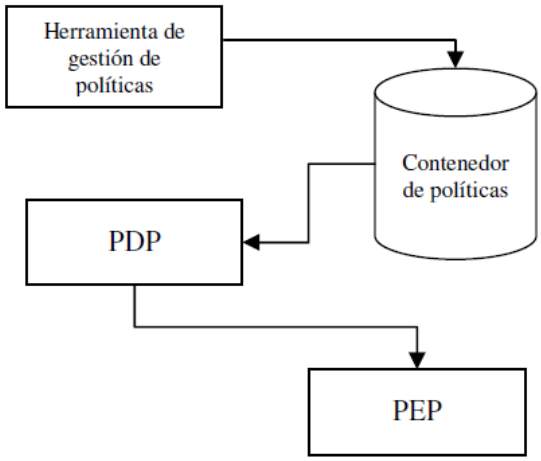

Fig. 4. Elementos principales de un modelo de gestión de redes basado en políticas. [31]

4. METODOLOGÍA DE CASO DE ESTUDIO

La metodología a utilizar en nuestra investigación es un caso de estudio, basado en las recomendaciones de Robert K. Yin [30]. Se optó por este autor debido a que describe de una manera completa los pasos y características del estudio de caso como metodología de investigación.

Este tipo de investigación permite el estudio de un objeto o caso, cuyos resultados permanecerán ciertos solo en ese caso en específico. Sin embargo, mediante este estudio de caso se podrá obtener una percepción más completa examinando las tendencias en cuanto a la Gestión de Redes Basadas En Políticas (PBNM) en la Universidad, teniendo en cuenta que es el proceso por el cual la administración es simplificada y automatizada.

A continuación se muestran los pasos a seguir, de acuerdo con la metodología [30]:

a. *Diseño del Caso de Estudio*
b. *Preparación para la colección de datos*
c. *Recolección de datos*
d. *Análisis del Caso de Estudio*
e. *Elaboración del Informe*

4.1. Diseño del Caso de Estudio

Mediante este caso de estudio queremos realizar una investigación de alta validez y fiabilidad dentro de un contexto, para poder interpretar de manera detallada y organizada el tema abordado en el área de gestión de redes.

El diseño de la investigación consiste en ligar los datos a ser recolectados con las preguntas iniciales del estudio. Los cinco componentes principales:

4.1.1. Preguntas del Estudio

Se formulan las preguntas de investigación del tipo ¿cómo?, ¿porque?, o bien, ¿cuáles?, es decir, preguntas de tipo exploratorio. Las preguntas que se buscan resolver son las siguientes:

- Qué políticas se deben implementar para ayudar a mejorar el rendimiento de la red universitaria.
- Cómo simplificar y automatizar el proceso de gestión de la red basado en políticas en la universidad.
- Cuáles son las políticas a transformar de alto nivel a políticas de bajo nivel para la gestión de PBNM.

4.1.2. Proposiciones del Estudio

Según Yin, cada proposición dirige su atención a algo que debe ser examinado dentro del alcance del estudio de caso [30]. Algunas hipótesis que podemos plantear para posteriormente ayudar a la definición de las unidades de análisis son las siguientes:

- La gestión de red basada en políticas proporciona un modo específico de asignar recursos de red, calidad de servicio y seguridad, considerando un juego de políticas antes definido. Estos sistemas proporcionan escalabilidad y facilidad para adaptarse a los cambios de las redes en tiempo real.

- La aplicación de políticas que permitan conseguir una política deseada utilizando comandos que, aplicados sobre distintos equipos de redes, permitan cambiar su configuración para conseguir Calidad de Servicios (QoS), seguridad, rendimiento, etc.

4.1.3. Unidades de Análisis

Para la realización de este proyecto promovemos un estudio de caso único, en donde se estudie el uso que se tiene de la red Universitaria y cuyo objeto de estudio sean los resultados obtenidos en los dos campus a través de entrevistas e informaciones suministradas por el personal de sistemas de la Universidad.

4.1.4. Criterios para la interpretación de resultados

Los resultados del estudio pueden ser interpretados de diferentes formas. En este caso, los resultados permiten comparar si las políticas llevan a la red universitaria a obtener éxito en sus diseños e implementación de las mismas para garantizar la seguridad, desempeño y análisis de la gestión de la red llevado a cabo antes de implementar las políticas. La comparación se realizara a través de datos cualitativos (Entrevistas, extracción de información) y no se va a hacer ninguna prueba estadística para llevar a cabo la comparación.

4.2. Preparación para la colección de datos

El protocolo es la herramienta que contiene los instrumentos, procedimientos y reglas generales para desarrollar el estudio de caso en cuestión.

Según Yin [30], el protocolo debe contener las siguientes secciones:

- Visión general del proyecto de caso de estudio
- Procedimiento de campo
- Preguntas del caso de estudio

4.2.1. Visión general del proyecto de caso de estudio

La visión general incluye información antecedente acerca del proyecto y los objetivos del mismo. Los objetivos más relevantes de esta investigación son:

- Analizar la red universitaria y mediante un levantamiento de información suministrada, implementar políticas hacia la red de campus universitario.
- Identificar las políticas institucionales que se pueden implementar con las técnicas de gestión de red basada en políticas (PBNM).
- Simplificar y Automatizar el proceso de la gestión de red basada en políticas presentando una descripción de levantamiento de la información por parte del personal del departamento de informática de la institución.

Para el cumplimiento de estos objetivos es necesario conocer cómo se está llevando a cabo la gestión de red en la universidad con el apoyo del personal que haga parte de este departamento.

4.2.2. Procedimiento de campo

Este aspecto se refiere al grado de accesibilidad al lugar del estudio y a la información necesaria para la investigación. En este caso, las entrevistas se llevaran a cabo en las horas acordadas con el personal del departamento que maneja la gestión de red universitaria y se pedirá autorización para observar las actividades que llevan a cabo en la red y cuya información sirva como

complemento para el logro de los objetivos de nuestra investigación y por ende de nuestro proyecto.

4.2.3. Preguntas del caso de estudio

Según Yin [30], estas preguntas son para el investigador y no para el entrevistado.

Las preguntas que debemos mantener siempre presente como investigadores para este caso de estudio específico son:

- Que modificaciones ha recibido la gestión de red universitaria en los últimos años.
- Como el administrador de red maneja los recursos estipulados por la universidad para que la red se mantenga confiable y saludable a todo el personal universitario.

4.3. Recolección de datos

Yin [30] menciona que la evidencia de los casos de estudio puede ser recolectada a través de documentos, archivos, entrevistas, observación directa, observación participativa (el investigador asume roles dentro de la situación) y artefactos físicos (dispositivos tecnológicos, herramientas o instrumentos).

En el caso específico del presente estudio se llevara a cabo la recopilación de datos principalmente de entrevistas realizadas a los coordinadores principales de la red en la Universidad Tecnológica de Bolívar, particularmente a Alfredo Figueroa Mercado (Administrador de la red) y a Humberto Marbello Peña (Coordinador de seguridad y Administrador de servicios informáticos), así como también se utilizaran datos secundarios, es decir, documentación brindada por el mismo departamento sobre el manejo que se está haciendo actualmente en materia de gestión de red, el cual nos permita una mejor perspectiva a evaluar en nuestro proyecto.

4.4. Análisis del Caso de Estudio

El análisis de los datos consiste en examinar, categorizar, tabular, probar o recombinar la evidencia para poder alcanzar las proposiciones e hipótesis formuladas.

En este caso, el análisis de los datos buscará evidenciar que las directivas o normativas en políticas para la gestión de la red Universitaria garantizan la integridad y confidencialidad de la misma, identificando los factores de éxito que tendrá la red llevándose a cabo la implementación de políticas y posterior a eso, validarlas mediante un software de código abierto que nos permita demostrar exitosamente nuestros objetivos.

4.5. Elaboración del Informe

El reporte se definirá y se desarrollará en la etapa del anteproyecto y durante la colección y análisis de datos. La audiencia principal de este reporte serán los administradores de la red y los beneficiados de esta investigación serán los usuarios que hacen parte de la organización, porque tendrán acople a los beneficios por contar con políticas de alto nivel y están sean convertidas a políticas de bajo nivel.

5. DISEÑO Y EDICIÓN DE POLÍTICAS

Una política es un conjunto de reglas definidas en un lenguaje de alto nivel por el administrador de red, es decir, una directiva a la red que puede contener simples mandatos como asignar mayor ancho de banda a un sector que a otro o que un nodo debe autenticarse antes de ingresar a una red. Por lo tanto, las políticas expresan como debe ser utilizada la red por parte de los usuarios, las aplicaciones, entre otros.

La información suministrada para categorizar y diseñar las políticas, fueron producto de las entrevistas realizadas a los coordinadores de la gestión de red en la Universidad. Sin ello, sería imposible y difícil poder dar a conocer la validez de nuestro proyecto y la elaboración de las políticas que no es más, una de las motivaciones para elaborar esta investigación.

5.1. Políticas actuales en la red UTB

El termino administración de red en la Universidad Tecnológica de Bolívar es definido como la suma total de todas las políticas y procedimientos que intervienen en la planeación, configuración, control y monitoreo de los elementos que conforman a la red con el fin de asegurar el eficiente empleo de los recursos, lo cual será reflejado en la calidad de sus servicios ofrecidos.

A continuación se describirán las políticas actuales en la red basado en el modelo de administración de redes OSI que distingue cinco áreas funcionales y a veces

recibe el nombre de FCAPS [36] (Fault, Configuration, Accounting, Performance, Security):

5.1.1. GESTIÓN DE FALLAS

1. Reportar a las autoridades universitarias las fallas en el desempeño de la red, vía telefónica.
2. Cuando a un auxiliar se le notifica la falla en cierto nodo, este debe ir al Firewall de la red para monitorear los tráficos, las alertas que genera o el ancho de banda para localizar la falla.
3. Al corregir una falla en cierto nodo, el auxiliar debe entregarle al usuario un reporte físico donde se describe la falla, la hora, la fecha y el departamento donde se encuentra, y solo el usuario es quien firma el recibido.
4. Cuando la falla en la red es general, se les notifica a todos los usuarios vía correo electrónico y no se hace entrega de un reporte físico.

5.1.2. GESTIÓN DE CONFIGURACIÓN

1. Se debe informar anticipadamente cuando haya un cambio en la red, vía correo electrónico, en el sector donde afecten a dichos usuarios.
2. Cuando un usuario necesite un software en su computador, debe llamar a la oficina de servicios informáticos para que envíen un auxiliar y este pueda instalar el programa necesario para el usuario.

3. Para configurar un nodo de la red, se debe dirigir la persona encargada hasta ese punto para realizar las configuraciones pertinentes.
4. El administrador decidirá, sobre el uso de los recursos del sistema, las restricciones de directorios y programas ejecutables para los usuarios.
5. El inventario de los elementos de la red solo lo puede manejar el administrador en un archivo Excel y es quien debe actualizarlo periódicamente.
6. La topología de la red solo la puede manejar el administrador en un archivo Visio.
7. Antes de realizar un cambio a un dispositivo de la red, se debe realizar un backup manual.
8. Para la realización de un mantenimiento lógico de equipos, se define la fecha de ejecución al usuario vía telefónica y se le hace un estimado sobre el tiempo de duración de cada paso de la instalación.

5.1.3. GESTIÓN DE CONTABILIDAD

1. Para registrar un nuevo componente de la red, el administrador debe ingresarlo a un archivo Excel donde tiene todo el inventario de la red.
2. La red debe estar dividida en: Estudiantes y Administrativos
3. La red Estudiantes no contiene clave de seguridad cuando la conexión es inalámbrica pero si se debe autenticar. Cuando la conexión es alámbrica, no hay necesidad de autenticarse.

4. La red Administrativo es para docentes y personal administrativo de la Universidad; El usuario debe digitar una clave de acceso cuando desee conectarse inalámbricamente.

5.1.4. GESTIÓN DE DESEMPEÑO

1. Solo el administrador es quien monitorea la red universitaria, en cualquier momento del día.
2. Cuando el administrador detecta que la conexión a internet esta lenta, este debe realizar un análisis del tráfico que está circulando en ese momento en la red. Puede ser a cualquier hora del día.
3. Para monitorear la red, detectar los tipos de tráfico más utilizados en la red o encontrar los elementos que más solicitudes hacen y atienden, se debe utilizar el firewall de la universidad.
4. Si se requiere observar que está haciendo cierto nodo en la red, se digita la IP en el firewall para ver que está haciendo o que paginas está visitando.

5.1.5. GESTIÓN DE SEGURIDAD

1. Cualquier usuario puede ingresar a la red universitaria y en cualquier VLAN, sea colocando un cable utp en el conector RJ-45 o ingresando inalámbricamente por la red Estudiantes o Administrativos.
2. Si un usuario desea ingresar desde una VPN, ya sea que quiera ingresar a la red desde su casa, este debe solicitarlo en un formato dado en la oficina de servicios informáticos

3. No se permite rechazar el acceso a un usuario que esté haciendo mal uso a la red universitaria. Ej.: Visitando páginas pornográficas, un administrativo en chat, etc.
4. Para realizar un backup a un equipo, el usuario de dicho equipo debe acercarse al departamento de informática para solicitar este servicio llenando un formulario.
5. Se consideran usuarios especiales a ciertos administrativos importantes de la universidad, y que se le deben realizar backups diarios sin ellos tener el conocimiento de ello, Ej. La rectora
6. Para controlar la ejecución de comandos en gestión de red, el administrador posee todos los privilegios. Le siguen los coordinadores con algunas restricciones y los auxiliares de sistema con pocos privilegios.
7. Los puertos SNMP siempre deben permanecer bloqueados.

5.2. Conversión

Según la Gestión de Redes basada en Políticas, un modelo que debe llevar una política simple se compone de la regla, la(s) condición(es) y la(s) acción(es). A continuación, presentaremos las políticas actuales llevadas a cabo en la universidad según el modelo propuesto por PBNM, de acuerdo al modelo FCAPS:

5.2.1. Fallas

1.

evento: *Falla en una maquina*

condición: No carga una página web a un usuario **OR** No carga una aplicación **OR** El usuario se da cuenta que el icono de conexión a internet se encuentra en estado no conectado **OR** El equipo no enciende **OR** Falla en el arranque del disco duro **OR** Pantallazo Azul debido a un error en el sistema **OR** La pantalla no enciende **OR** El tiempo de respuesta del dispositivo es lento **OR** Error en el arranque del Sistema Operativo **OR** Al encender el pc se desconfigura el BIOS **OR** Falla en el POST del Sistema **OR** Cierto tipo de Hardware no responde (Teclado, Mouse, Unidad de CD-ROM, WebCam) **OR** El sistema notifica una duplicación de IP **OR** Problemas de DNS **OR** No se puede detectar la tarjeta de red del equipo

acción: El auxiliar disponible debe ir al firewall de la red para monitorear los tráficos, las alertas que genera o el ancho de banda para localizar la falla **AND** Dirigirse hacia la oficina del usuario que notificó la falla para que firme un reporte físico que describe la falla, hora, fecha y oficina donde se encuentra.

2.

evento: *Falla en otros dispositivos finales (Impresoras, Faxes, Escáneres, Copiadoras, Teléfonos IP)*

condición: No cargan los servicios un servidor **OR** No hay conexión al Servidor (Correo Electrónico o Aplicación ERP **OR** Problemas de Impresión **OR** Problemas de Escáner **OR** Problemas de Fax **OR** Problemas en Copiadoras

acción: El auxiliar disponible debe ir al firewall de la red para monitorear los tráficos, las alertas que genera o el ancho de banda para localizar la falla **OR** Dirigirse hacia la oficina del usuario que notificó la falla para que firme un reporte físico que describe la falla, hora, fecha y oficina donde se encuentra.

3.

evento: *Falla un dispositivo de red*

condición: No enciende un switch **OR** No enciende un enrutador **OR** No enciende un Hub **OR** No enciende un Access Point **OR** No carga el sistema operativo de un switch **OR** No carga el sistema operativo de un enrutador **OR** No carga el sistema operativo de un Hub **OR** No carga la configuración de un Access Point **OR** No carga la configuración de un switch **OR** No carga la configuración de un hub **OR** No carga la configuración de un enrutador **OR** Cliente

inalámbrico sin conexión **OR** Cable dañado (Rendimiento a la red pobre)

acción: El auxiliar disponible debe ir al firewall de la red para monitorear los tráficos, las alertas que genera o el ancho de banda para localizar la falla **OR** Dirigirse hacia el sitio donde se notificó la falla y el auxiliar debe realizar el respectivo reporte físico de la fecha, hora y ubicación del dispositivo analizado.

4.
evento: *Conexión en la red lenta*
condición: - Un nodo está generando mucho tráfico en la red
- El administrador de la red detecta que la conexión está lenta.
- Los coordinadores o auxiliares de la red le notifican al administrador que la red está lenta.
acción: - El administrador analiza el tráfico de la red para tomar acciones pertinentes. Esto lo puede realizar a cualquier hora del día y por medio del Firewall.
- Digitar la IP del nodo que está generando mucho tráfico para observar que tareas está realizando.

5.
evento: *Falla en el desempeño general de la red*
condición: No hay acceso a internet en todos los nodos que hacen parte de la red
acción: Posterior a la corrección de la falla, notificarle a los usuarios vía correo electrónico la falla que hubo

5.2.2. CONFIGURACION

1.
evento: *Solicitar una instalación de un programa en un nodo de la red.*
condición: Requerimiento de Instalación de un programa en un computador
acción: Verificar con los auxiliares del departamento de informática si dicho programa puede ser instalado en la máquina **OR** Un auxiliar se debe dirigir hacia la oficina del usuario que solicitó el servicio.

2.
evento: *Cambio en un dispositivo en la red*
condición: Se requiere actualizar un dispositivo **OR** Reemplazar un dispositivo viejo por uno nuevo

acción: Informar anticipadamente vía correo electrónico cuando haya un cambio en la red, en el sector donde afecten a dichos usuarios **AND** Antes de realizar cualquier cambio, realizar un backup manual del dispositivo.

3.

evento: *Solicitar una configuración para una estación de trabajo*

condición: Se requiere configurar los controladores y los programas para un nuevo computador en algún sector de la red

acción: Agregar un usuario a un dominio existente **OR** Definir un dominio nuevo y agregar un usuario a ese dominio **OR** El administrador decidirá los privilegios que puede tener el computador y los programas que se podrán instalar en la maquina

4.

evento: *Solicitar una configuración para un dispositivo de red*

condición: Se requiere agregar un dispositivo en cierto punto de la red **OR** configurar los controladores para el uso del dispositivo

acción: El administrador decidirá los privilegios que puede tener el computador y los programas que se podrán instalar en la maquina

5.

evento: *Programación de mantenimiento lógico a una estación de trabajo*

condición: Fecha exacta para la realización del mantenimiento **OR** El usuario debe confirmar su disponibilidad en la fecha y hora a realizar el mantenimiento

acción: Un auxiliar se acercará a la oficina del usuario para realizar el respectivo mantenimiento. Durante el tiempo de esta ejecución, el usuario no podrá utilizar el equipo. **OR** Al finalizar la tarea, el usuario debe firmar un reporte del mantenimiento realizado.

6.

evento: *Ingresar/Quitar un componente de la red o periférico de un computador*

condición: Incorporación de un periférico **OR** Reparación de un periférico.

acción: El administrador debe registrar el nuevo componente o periférico de computador en su archivo Excel donde maneja el inventario de los equipos en la red.

5.2.3. CONTABILIDAD

1.
evento: *Medir el uso de los recursos utilizados por los usuarios de la red*
condición: Se requiere recolectar información acerca de los recursos utilizados por los elementos de la red desde equipos de interconexión **OR** recolectar información acerca de los recursos utilizados por los elementos de la red desde los usuarios finales
acción: Mantener un registro de uso del ancho de banda **OR** Mantener un registro de uso del almacenamiento del correo electrónico **OR** Mantener un registro de uso de los backups **OR** Mantener un registro de uso del Backbone interno

5.2.4. DESEMPENO

1.
evento: *Monitoreo en la Red UTB*
condición: Caracterización de Tráfico Interno **OR** Caracterización de Tráfico Externo **OR** Caracterización de utilización de segmentos
acción: Recolectar datos de rendimiento **OR** Realizar medidas de tráfico en el backbone **OR** Realizar medidas de tráfico en la conexión al ISP **OR** Realizar medidas de tráfico en segmentos congestionados

5.2.5. SEGURIDAD

1.
evento: *Ingreso a la red para los Estudiantes*
condición: Cualquier usuario puede ingresar a la red **OR** Un nodo solicita conectarse a la red por medio de un cable UTP **OR** Un nodo solicita conectarse a la red vía inalámbrica
acción: Por medio del cable, el usuario debe enchufar su cable UTP con el conector para tener acceso a la red **OR** Vía inalámbrica, El nodo debe autenticarse antes de ingresar a la red

2.
evento: *Ingreso a la red para los Empleados*
condición: Los Profesores y Administrativos de la Institución solo están autorizados para ingresar a esta red **OR** Un nodo solicita conectarse a la red vía inalámbrica
acción: El nodo debe ingresar una clave tipo WPA2 antes de ingresar a la red.

3.

evento: *Solicitud de ingreso a la red por medio de un VPN.*
condición: El usuario debe solicitar formalmente este servicio
acción: Permitir el control remoto al usuario durante el tiempo necesario que hizo la solicitud del servicio **OR** Autorizar al usuario para utilizar este servicio

4.

evento: *Un nodo está haciendo mal uso de la red*
condición: El usuario está visitando paginas indebidas (Pornográficas, MediaFire) y los administradores de la red los detectan revisando logs.
acción: El servidor verifica si la IP a la que quiere acceder puede ser peligrosa, y en algunos casos no permite ingresar a esa página **OR** Si el usuario violo las restricciones de acceso, no se puede rechazar su acceso

5.

evento: *Un usuario solicita realizar un backup a su equipo*
condición: El usuario requiere realizar un cambio de máquina **OR** El usuario solicitó previamente que su máquina realizara copias de seguridad en ciertos días de la semana **OR** El usuario es de tipo especial (Ej. La rectora, La vicerrectora, entre otros)
acción: Un auxiliar se debe dirigir hacia la oficina del usuario para realizar la respectiva copia de seguridad, y guardarla en el disco duro del servidor.

Las preguntas realizadas en la entrevista otorgada por los coordinadores de la red universitaria, las podemos ver en el anexo [A2]. También podemos conocer las políticas anteriormente comprendidas, totalmente codificadas y posibles para ser guardadas en un repositorio, se debe dirigir al anexo [A3].

6. RESULTADOS

Este proyecto denominado “Diseño e Implementación de Políticas en Gestión de Redes para la Universidad Tecnológica de Bolívar”, contiene las normativas actuales llevadas a cabo desde el departamento de servicios informativos hacia la red universitaria en sus diversos campus.

Estimamos la oportunidad de entrevistar a los coordinadores principales que llevan a cabo la gestión de la red en la universidad, concediéndoles una serie de preguntas repartidas gracias por el modelo FCAPS para determinar específicamente las políticas implementadas que llevan a cabo saludable la red.

Luego de analizar y estudiar las respuestas dadas por los coordinadores, hemos encontrado que los errores y fallas que se presenten en la red se deben verificar y localizar de forma manual, los reportes hechos por las mismas no se están guardando en registros de fecha y hora de forma automatizada, no se tiene una clasificación de severidad de fallas a partir de los errores comunes presentados en la red, la falta de documentación de cambios en la red para una futura evidencia, no existe un software que permita automatizar una incorporación o salida de un dispositivo a la red en un registro, no existe un software que ayude a modelar el futuro de la red o por lo menos, durante un tiempo se lleve a cabo la planificación - rediseño de la misma, y toda persona externa a la universidad que posea un computador personal, puede ingresar a la red sin mucho inconveniente. Estos son

los resultados que previamente habíamos intuido que estarían pasando en la red de la universidad, y que hemos comprobado.

Se pudo detectar que aun cuando la universidad no posea un manual que exprese en escrito un conjunto de políticas en la red, la institución universitaria en cabeza de sus coordinadores de red y sus administrativos, las aplica para garantizar el desempeño y seguridad hacia sus usuarios.

Relevamos que no existe uniformidad de criterio entre sus usuarios para el uso de los recursos por computador, y además, no tienen claro que pueden tener y que no pueden tener, así mismo, que pueden instalar y que no pueden instalar. Siempre deben llamar a algún representante del departamento de servicios informáticos para salir de dudas.

La UTB como institución de educación superior, debe dar a conocer a sus usuarios las políticas de uso en la red, y estas deben ir acompañadas de una serie de acciones administrativas y capacitaciones a los usuarios, de manera que tengan clara la importancia y la forma de uso de los recursos en la red, puesto que constituye uno de los elementos más valiosos que dispone ella.

7. CONCLUSIONES

La implementación de políticas en la gestión de redes de la Universidad Tecnológica de Bolívar, no pretende suplantar a los coordinadores o auxiliares de la red, lo que intenta es automatizar procesos manuales para minimizar errores humanos que impidan el máximo desempeño de la red.

Se deben dar a conocer las políticas para el uso de la red mediante una documentación o manual, y los nuevos usuarios deben enterarse de ellas para que hagan buen uso de ella. Deben tener claro que pueden hacer y que no pueden hacer, y si hay una violación de cualquier política, los coordinadores de la red deben notar la anomalía inmediatamente, antes de que el problema se salga de las manos.

Un desarrollo futuro sobre el proyecto es la utilización de los componentes restantes que hacen funcionar de manera eficiente la gestión de redes basada en políticas. Implementar para la ejecución de las políticas en gestión de redes, el PDP (Policy Decision Point), quien decide las acciones pertinentes acordes a los eventos y el PEP (Policy Enforcement Point), que es el punto donde y como actuará la política. Estos desarrollos no se incluyeron en el alcance del proyecto por factores de tiempo y recursos.

Se recomienda optimizar las políticas en gestión de red, a partir de Policy – Based Network Management (PBNM) haciendo las subdivisiones del modelo FCAPS para un mayor entendimiento:

FALLAS

1. Un software del equipo cliente debe informar a un software del servidor sobre una falla en un nodo o dispositivo de la red, para ser detectada y reportada de manera inmediata.
2. Una falla puede ser notificada por un sistema de alarmas incluso antes de que el usuario se halla percibido (proceso automatizado), o por un cliente que reporta la falla (proceso manual).
3. Un reporte es creado después de haber recibido una notificación sobre la existencia de un problema en la red, ya sea por una alarma, una llamada telefónica de un usuario, por correo electrónico o cualquier otro medio. La idea es que un software cree un registro de falla como evidencia.
4. Registrar y dar seguimiento a todos los reportes generados por los usuarios o por el mismo administrador de la red.
5. A partir de los reportes generados por fallas, clasificar las alarmas por:

   De comunicaciones: Asociadas con el transporte de información, como las pérdidas de señal.

   De procesos: Asociadas con el software o los procesos, como cuando un procesador excede su porcentaje normal.

   De equipos: Asociadas con los equipos, una falla en la fuente de poder, memoria RAM, etc.

   Ambientales: Asociadas con las condiciones ambientales en las que un equipo opera, por ejemplo una alta temperatura en un computador.

De servicios: Degradación de un servicio en cuanto a límites predeterminados, como excesos en la utilización del ancho de banda o abundancia de peticiones icmp.

6. A partir de los reportes generados por fallas, clasificar la severidad de las fallas por:

   Critica: Evento severo o de atención inmediata. Se relaciona con fallas que afectan el funcionamiento global de la red.

   Mayor: Un servicio ha sido afectado y se requiere su inmediato restablecimiento. Puede ser cuando el correo institucional deja de operar eficientemente.

   Menor: Condición que no afecta al servicio pero que deben ser tomadas las acciones pertinentes para prevenir una situación mayor. Puede ser cuando se alcanza cierto límite en la utilización del enlace, esto no indica que el servicio está afectado pero lo será si se permite que siga avanzando.

   Indefinida: El nivel de severidad no ha sido determinado por alguna razón.

CONFIGURACION

1. Documentar los cambios en la red para futuras evidencias.
2. El administrador debe poseer un respaldo frecuente de las configuraciones de los equipos de la red, porque son un elemento importante que requieren especial cuidado.

CONTABILIDAD

1. Automatizar el registro de los nuevos componentes que se incorporan a la red, movimientos o cambios que se lleven a cabo.

DESEMPEÑO

1. El tráfico en la red debe ser monitoreado y administrado continuamente por un personal de telecomunicaciones con la finalidad de optimizar el ancho de banda como parte de la operación rutinaria de la red para diagnóstico, mantenimiento o para resolver problemas, ya sea en forma general o para un dispositivo de red especifico.
2. El monitoreo del tráfico en la red de la UTB debe involucrar solamente información de los encabezados en los paquetes más no los datos de los mismos, a menos que se requiera para verificar la existencia de virus o para detección de intrusos.

SEGURIDAD

1. Los usuarios (Estudiante/Administrativo/Docente) deben identificarse en la red para comprobar que son quien dicen ser.
2. Un estudiante debe ingresar por la red “Estudiantes” digitando su código estudiantil en el campo username y un password que sea proporcionado por el

departamento de telecomunicaciones por un algoritmo de encriptamiento a la hora de autenticarse a la red. Esto corresponde a la política de Listas de acceso y detección de intrusos.

3. Un docente/Administrativo debe ingresar por la red “Administrativos” digitando su código en el campo username y un password que sea proporcionado por el departamento de telecomunicaciones por un algoritmo de encriptamiento a la hora de autenticarse a la red. Esto corresponde a la política de Listas de acceso y detección de intrusos.
4. Restringir el acceso a internet en los departamentos que no posean servidores en horas no laborales. Ej. De 6pm a 5am del día siguiente, Bienestar Universitario no tendrá acceso a internet.
5. Cuando se necesite brindar acceso en la red a terceros, el administrador deberá habilitar una conexión sin autenticación en el intervalo de tiempo que lo necesiten, Ej. Entre las 7:00am y 12m, los usuarios que están en un seminario realizado en el auditorio de la universidad, podrán tener acceso a internet por medio de la red inalámbrica temporal “Auditorio”.
6. Los comandos de SNMP o cualquier otro protocolo similar de administración de redes, deben ser utilizados por personas de gestión que estén debidamente autenticadas.

8. REFERENCIAS

[1] J. Evans and C. Filsfils, “Deploying DiffServ at the Network Edge for Tight SLAs, Part 2,” *IEEE Internet Computing*, pp. 2–10, Mar./Apr. 2004.

[2] William Stallings, SNMP y SNMP v2: The Infrastructure Management. Mar, 1998.

[3] William Stallings, SNMP, SNMP v2 y RMON: Practical Network Management. Pag. 264. 1996. [4] D. Pecos Martínez, Domain Name Server , Castellón, 1 de Diciembre 2003

[5] J. Patrick Thompson, Web – Based Enterprise Management Architecture, IEEE Communications Magazine, March 1998.

[6] J. Pavón and J. Tomás, CORBA for Network and Service Management in the TINA Framework, IEEE Communications Magazine, March 1998.

[7] R. Boutaba and J. Xiao, Network Management, Java - Based Network Management, ACM Digital Library, 2002.

[8] Introduction to Policy-Based Networking and Quality of Service, IPHighway, White Paper, Jan. 2000.

[9] J. Strassner. Policy Based Network Management - Solutions for the Next Generation. Morgan Kaufman, 2003.

[10] Morris Sloman, Policy Driven Management for Distributed Systems, Journal of Network and Systems Management, Plenum Press. Vol.2 No.4, http://dpnm.postech.ac.kr/policy/presen/policy-driven.ppt, 1994.

[11] Yu Kang, Song Ouyang, a Multilevel Policy-Based Network Management System for Differentiated Services Network, 2009.

[12] Dinesh C. Verma, Simplifying Network Administration Using Policy - Based Management, Agu. 2002.

[13] D. Durham et al., “The COPS (Common Open Policy Service) Protocol”, RFC 2748, IETF, Jan. 2000.

[14] Raouf Boutaba and Issam Aib David R. Cheriton School of Computer Science, Policy-Based Management: A Historical perspective, University of Waterloo, Canada. December 2007.

[15] D. Elliott Bell and Leonard J. LaPadula. Secure computer systems: Mathematical foundations. Technical report esd-tr-278, MITRE Corporation, Bedford, MA, 1973.

[16] Koch T., Kramer B., Rohde G., On a Rule Based Management Architecture, The 2nd International Workshop on Services in Distributed and Networked Environments, IEEE Computer Society, Whistler, Canada, 1995.

[17] Moffett J., Sloman M., Policy Hierarchies for Distributed Systems Management, IEEE Journal on Selected Areas in Communication, Vol. 11, No. 9, Dec. 1993.

[18] S. Karris, Network: Design and Management. Pag 8-9. 2009.

[19] C. Hunt, TCP/IP Network Administration. Pag 1. 2002.

[20] C. Hunt, TCP/IP Network Administration. Pag 31-34. 2002.

[21] International Telecommunications Union – Telecommunications Standardization Sector (ITU-T), Resumen de TMN Recommendations, Recomendacion M.3000, febrero de 2000.

[22] Chappel, David (May 1998). "Trouble with CORBA". www.davidchappel.com. Retrieved 15 March 2010.

[23] Emil C. Lupu and Morris Sloman. Conflicts in policy-based distributed systems management. IEEE Transactions on Software Engineering, Special issue on inconsistencies management, pp 852-869, 1999.

[24] Nevil Brownlee. SRL: A language for describing traffic flows and specifying actions for flow groups. IETF Internet draft, Expird February 2000, Aug 1999.

[25] David D. Clark. Policy routing in internet protocols. IETF Network Working Group, RFC 1102, May 1989.

[26] Gary N. Stone, Bert Lundy, and Geoffrey G. Xie. Network policy languages: a survey and a new approach. IEEE Network, 15(1):10–21, January/February 2001.

[27] M. Nossik, F. Welfeld, and M. Richardson. PAX PDL: A Non-Procedural Packet Description Language. Technical report, Sept. 30 1998.

[28] Dinesh C. Verma, “Policy-Based Networking: Architecture and Algorithms”, 1st Ed., Indianapolis: New Riders, 2001.

[29] Chappel, David (May 1998). "Trouble with CORBA". www.davidchappel.com. Retrieved 15 March 2010.

[30] Yin, Robert. Case study research: design and methods – Cap.1 Thousand Oaks, CA: Sage Publications, 2003.

[31] J.A. Guerrero Ibañez y A. Barba Marti. Arquitectura de Gestión de red basada en políticas para un Ambiente Integrado 3G – WLAN. Junio de 2008.

[32] Cheikhrouhou M. M., Conti P., Labetoulle J., Intelligent Agents in Network Management: A State-of-the-art, 1998

[33] William Stallings, Snmpv3: A Security Enhancement For SNMP. 1998.

[34] Proyecto Ponder2, http://www.ponder2.net/#Ponder2

[35] Kristy Westphal, NFS and NIS Security, http://www.symantec.com/connect/articles/nfs-and-nis-security, Jan 22, 2001

[36] Brijendra Singh, Network Security and Management 2nd Edition, Goal of Network Management, Pag. 173. 2009.

ANEXOS

[A1] ADMINISTRACIÓN DEL PROYECTO

Recursos Humanos

INVESTIGADORES	
Laura Victoria Yépez Rodríguez Autor del Proyecto	Estudiante de Ingeniería de Sistemas UTB
Javier Eduardo Díaz Machuca Autor del Proyecto	Estudiante de Ingeniería de Sistemas UTB
Jairo Alberto Gutiérrez Diago Asesor del Proyecto	Director de Investigación e Innovación de la UTB Ingeniero de Sistemas y Computación M.Sc. Computer Science Ph.D. Information Systems
FACILITADORES DE LA INVESTIGACION	
Alfredo Figueroa Mercado Encargado de la red UTB	Jefe de Hardware y Tecnología de Servicios Informáticos UTB
Humberto Marbello Peña Encargado de la red UTB	Coordinador de Seguridad y Administrador de Servicios Informáticos UTB

Recursos Disponibles

DISEÑO E IMPLEMENTACION DE POLITICAS EN GESTION DE RED PARA LA UNIVERSIDAD TECNOLOGICA DE BOLIVAR	
FINANCIACION PROPIA **(Conceptos)**	**Gastos**
Internet e impresiones	**$ 402.500**
Transporte e insumos alimenticios	**$ 62.300**
Fotocopias de documentos y carpetas	**$ 182.500**
Llamadas Telefónicas	**$ 50.000**
Otros gastos	**$ 51.200**
Costo total del proyecto	**$ 748.500**

Cronograma

FASE I

TIEMPO	MARZO				ABRIL				MAYO				JUNIO				JULIO			
ACTIVIDADES	1-4	7-11	14-18	21-25	4-8	11-15	18-22	25-29	2-6	9-13	16-20	23-27	6-10	13-17	20-24	27-30	4-8	11-15	18-22	25-29
Bibliografía																				
Temas propuestos por el Asesor																				
Propuesta Inicial del Trabajo																				
Anteproyecto																				

FASE II

TIEMPO	JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE			
ACTIVIDADES	4-8	11-15	18-22	25-29	1-5	8-12	15-19	22-26	1-9	12-16	19-23	26-30	3 -7	10-14	17-21	
Correcciones																
Proyecto Final																
Entrevista con el personal de Gestión de la red																
Identificación de políticas institucionales																
Diseño de políticas																
Validación de las políticas																
Entrega del Proyecto Final																

[A2] ENTREVISTA A LOS RESPONSABLES DEL FUNCIONAMIENTO DE LA RED DE ACUERDO AL MODELO FCAPS EN LA UNIVERSIDAD TECNOLOGICA DE BOLIVAR

ENTREVISTADO(S): Alfredo Figueroa (*Jefe de Hardware y Tecnología*) y Humberto Marbello (*Coordinador principal de la Red*)

CATEGORIA: Gestión de Redes

Fecha: 8 de Agosto de 2011

FALLAS

1. Quien se da cuenta de una falla en la red?
2. Como se localiza una falla en la red?
3. Que pruebas de diagnóstico se realizan para predecir una falla (Física, Lógica)
4. Cuál es el procedimiento de reparación de una falla
5. Como administran el reporte a una falla (Registro, Manejo de la falla, Quien lo hace)
6. Clasifique la severidad de las fallas en la red por: Critica, Mayor, Menor o Indefinida

CONFIGURACION

1. Cada cuanto tiempo se lleva a cabo el proceso de planificación y rediseño de la red
2. Cuáles son las necesidades específicas y de índole tecnológico que urge en la red.
3. Como se notifica cuando se agrega o se sustituye un dispositivo de red o hardware a un equipo?
4. Como se notifica a los usuarios sobre un cambio en la red?
5. Se documenta el cambio para futuras evidencias? Quien lo hace?
6. Qué control se lleva sobre los programas instalados de los pc? Lo realiza un operador en la propia maquina o remotamente?
7. Se puede configurar remotamente un dispositivo o pc?
8. Como planifican los requerimientos óptimos que debe tener en hardware y software un pc o dispositivo.
9. Se tiene una gestión de inventario? (Base de datos de los elementos de la red, Historia de cambios y problemas, etc.)
10. Se tiene algún respaldo frecuente de las configuraciones de los equipos? Como se cargan estas configuraciones

11. Topología de la red Física y Lógica de los recursos (cables, componentes de red, nodos, software): Como estos recursos están interconectados y la información sobre sus relaciones lógicas.

CONTABILIDAD

1. Como se contabiliza la utilización de la red y los servicios que provee? Como está organizado? (Ancho de banda, procesamiento, etc.)
2. Como manejan el registro de los nuevos componentes que se incorporan a la red, los movimientos que se hacen y los cambios que se llevan a cabo

DESEMPEÑO

1. Como se recolecta y se analiza el tráfico que circula por la red en:
   a. Un momento particular (Tiempo real)
   b. Intervalo de Tiempo

Se realiza por variables? Cuáles son?

2. Que software o proceso se lleva a cabo para mantener monitoreada las operaciones diarias de la red?
3. Como distribuyen el tráfico en la red
4. Como se detectan los tipos de tráfico que son más utilizados en la red (Páginas web frecuentes, ftp, etc.)
5. Como encuentran los elementos de la red que más solicitudes hacen y atienden? Cuales son por frecuencia (Depto.? Estación en particular?)
6. Como previenen los problemas a futuro? Algún software? (Si es así, que hace este software)
7. Se puede observar que está haciendo cierto nodo en la red?

SEGURIDAD

1. Quienes pueden ingresar a la red? Como lo hacen?
2. Que estrategias de prevención y detección de ataques utiliza la red
3. Que herramientas de seguridad se emplean en la red (Control de acceso, Firewall, TACACS+, IPSec, MD5, etc.)
4. Como llevan a cabo el manejo de los servicios de seguridad: Confidencialidad, Autenticación, Integridad, Control de acceso
5. Se puede rechazar el acceso a un usuario que está haciendo mal uso de la red? (Pornografía, chat)
6. Cada cuanto se realiza un backup? Donde se realizan? En qué hora? Donde se guardan?

7. Como se controla la ejecución de comandos de gestión de red (Network Management). Que usuarios están autorizados a ejecutar esos comandos?

[A3] POLÍTICAS EDITADAS

FALLAS

```
//Falla en una maquina
//Crear una política para detectar una falla en una maquina
	policy := root/factory/ecapolicy create.
	policy event: root/event/fallamaquina;
	policy event: root/event/monitoreo;
	policy condition: [ :TiempoRespuestaPagina :Aplicacion : NODO :SendBytes
	:ReceivedBytes :Encendido :DiscoDuro :ErrorSistema :UsoCPU :DuplicacionIP
		: TiempoRespuestaPagina > 30 //No carga una página web (Tiempo en segundos)
	|	: Aplicacion == 0		//No carga una aplicacion
	|	: NODO == (SendBytes == 0) && (ReceivedBytes == 0)	//Icono conexion
	a  internet no conectado
	|	: Encendido == 0		//El equipo no enciende o Falla Codigo POST
	|	: DiscoDuro == 0		//Falla en el arranque del disco duro
	|	: ErrorSistema == 1		//Error del Sistema Operativo
	|	: UsoCPU > 90			//Tiempo de Respuesta PC (Tiempo en
	Porcentaje)
	|	: DuplicacionIP == 1		//Duplicación de Dirección IP
	];
	policy action: [
		domain red/ execute monitoreo  //"Monitorear la red desde el Firewall para
		localizar la falla"
	&	root print: "Entregar reporte físico al usuario que notifico la falla"
	]

//Falla en otros dispositivos finales (Impresoras, Faxes, Escaneres, Copiadoras,
Telefonos IP)
//Crear una política para detectar una falla en el resto de dispositivos finales del
usuario
	policy := root/factory/ecapolicy create.
	policy event: root/event/falladispfinales;
	policy event: root/event/monitoreo;
	policy condition: [ :ServiciosServidor :ConexionServidor :ProblemaImpresion
	:ProblemaFax :ProblemaCopiadora |
		: ServiciosServidor = 0		//No cargan los servicios del servidor
	|	: ConexionServidor == 0		//Valores en bytes
	|	: ProblemaImpresion == 1	//Hay problema con la impresora
	|	: ProblemaFax == 1		//Hay problema con el fax
	|	: ProblemaCopiadora == 1	//Hay problema con la copiadora
	];
	policy action: [
		domain red/ execute monitoreo  //"Monitorear la red desde el Firewall para
		localizar la falla"
	&	root print: "Entregar reporte físico al usuario que notifico la falla"
	]
```

```
//Falla un dispositivo de red (Hub, Switch, Router, AccessPoint)
//Crear una política para detectar una falla en un dispositivo de red
       policy := root/factory/ecapolicy create.
       policy event: root/event/falladispred;
       policy event: root/event/monitoreo;
       policy condition: [ :EncendidoSwitch :EncendidoEnrutador :EncendidoHub
       :EncendidoAP :ErrorSistemaEnrutador :ErrorSistemaHub :ErrorSistemaAP
       :ErrorSistemaSwitch :ErrorConfiguracionSwitch :ErrorConfiguracionHub
       :ErrorConfiguracionEnrutador :Senal_AP                                  |
              : EncendidoSwitch = 0              //No enciende un switch
       |      : EncendidoEnrutador == 0          //No enciende un enrutador
       |      : EncendidoHub == 0                //No enciende un hub
       |      : EncendidoAP == 0                 //No enciende un AccessPoint
       |      : ErrorSistemaEnrutador == 1       //No carga el sistema operativo del
       Enrutador
       |      : ErrorSistemaHub == 1             //No carga el sistema operativo del Hub
       |      : ErrorSistemaAP == 1              //No carga el sistema operativo del
AccessPoint
       |      : ErrorSistemaSwitch == 1          //No carga el sistema operativo del
Switch
       |      : ErrorConfiguracionSwitch == 1    //No carga la configuración del Switch
       |      : ErrorConfiguracionHub == 1       //No carga la configuración del Hub
       |      : ErrorConfiguracionEnrutador == 1  //No carga la configuración del
Enrutador
       |      : Senal_AP <= 18                   //Velocidad en Mbps
       ];
       policy action: [
              domain red/ execute monitoreo  //"Monitorear la red desde el Firewall para
              localizar la falla"
       &      root print: "Entregar reporte físico al usuario que notifico la falla"
       ]

//Conexión en la red lenta
//Crear una política para detectar una falla cuando la conexión en la red es lenta

       policy := root/factory/ecapolicy create.
       policy event: root/event/conexionlenta;
       policy event: root/event/monitoreo;
       policy event: root/event/digitarip;
       policy condition: [ :trafico |
              : trafico > 70                    //Mucho tráfico en la red (%)
              ];
       policy action: [
              domain red/ execute monitoreo  //"Monitorear la red desde el Firewall para
              localizar la falla"
       |      domain red/ execute ip;      // Digitar IP desde el firewall hacia el nodo
       que está generando mucho tráfico
       ]

//Falla en el desempeño general de la red
//Crear una política para detectar la falla en el desempeño general de la red

       policy := root/factory/ecapolicy create.
       policy event: root/event/fallageneral;
       policy event: root/event/correomasivo;
       policy condition: [ :RED :SendBytes :ReceivedBytes |
              : RED == (SendBytes == 0) && (ReceivedBytes == 0) //No hay acceso a la red
              en todos los nodos
              ];
```

```
policy action: [
        domain red/ execute correomasivo  //"Notificar la descripción de la falla
        vía correo electrónico a todos los usuarios"
        ]
```

CONFIGURACIÓN

```
//Solicitud de instalación de un programa en un nodo de la red
//Crear una política para solicitar la instalación de un programa en un computador
        policy := root/factory/ecapolicy create.
        policy event: root/event/instalacionprograma;
        policy condition: [ :nodo_mac |
                root print: "Requerimiento de instalacion de programa en " + nodo_mac
        ];

        policy action: [      :instalacion          //0= no se puede ; 1= se puede
                              :nodo_mac |
                        IF (instalacion == 0)
                        root print: "Programa  no permitido a instalar"
                        IF (instalacion == 1)
                        root print: "Programa  a instalar en la maquina" + nodo_mac
                        ]

//Cambio en un dispositivo de red
//Crear una política para requerir actualizar un dispositivo o reemplazar uno viejo por
uno nuevo
        policy := root/factory/ecapolicy create.
        policy event: root/event/cambiodispositivo;
        policy event: root/event/correomasivo;
        policy condition: [ :nodo_mac |
                root print: "Actualizar dispositivo " + nodo_mac
        |       root print: "Reemplazar dispositivo" + nodo_mac
        ];

        policy action: [      :nodo_mac
                domain red/ execute correomasivo  //Enviar emails a usuarios afectados por
                cambios
        &       root print: "Realizar backup al equipo" + nodo_mac
        ]

//Solicitar una configuración para una estación de trabajo
//Crear una política cuando se solicite realizar una configuración a una estación de
trabajo
        policy := root/factory/ecapolicy create.
        policy event: root/event/configuracion_estacion;
        policy condition: [ :nodo_mac |
                root print: "Configurar controladores y programa al nodo " + nodo_mac
        ];
        policy action: [      :nodo_mac :dominio
                root print: "Agregar" + nodo_mac + "al dominio" + dominio
        |       root print: "Definir nuevo dominio" & root print: "Agregar" + nodo_mac +
                "al dominio" + dominio
        |       root print: "Decidir privilegios para el pc" + nodo_mac
        ]

//Solicitar una configuración para un dispositivo de red
//Crear una política cuando se solicite realizar una configuración a un dispositivo de
red
        policy := root/factory/ecapolicy create.
```

```
        policy event: root/event/configuracion_disp_red;
        policy condition: [ :nodo_mac :vlan        |
                root print: "Agregar " + nodo_mac + "en la VLAN" + vlan
        ];
        policy action: [      :nodo_mac
        |       root print: "Definir privilegios para el dispositivo" + nodo_mac
        ]

//Programación de mantenimiento lógico a una estación de trabajo
//Crear una politica para realizar el mantenimiento logico a una estacion en cierto
tiempo

        policy := root/factory/ecapolicy create.
        policy event: root/event/prog_mantenimiento;
        policy condition: [ :mantenimiento :nodo_mac      |
                mantenimiento == 1          //Se debe realizar el mantenimiento
        &       disposibilidad == 1         //Confirmacion de disponibilidad por parte del
usuario
                root print: "Realizar mantenimiento al dispositivo" + nodo_mac
        ];

        policy action: [      :nodo_mac
                root print: "Realizar mantenimiento al dispositivo" + nodo_mac
        ]

//Ingresar/Quitar un componente de la red o periférico de un computador
//Crear una política cuando haya que ingresar o quitar un componente de la red o
//un periférico de un pc

        policy := root/factory/ecapolicy create.
        policy event: root/event/ingresar_quitar;
        policy event: root/event/registro;
        policy condition: [ :incorporar_periferico :reparar_periferico   |
        [       incorporar_periferico == 1          //Ingresar un nuevo periférico
        &       reparar_periferico == 1             //Reparar un periférico
        ]
        |
        [       ingresar_componente == 1     //Ingresar un nuevo componente de la red
        &       reparar_componente == 1      //Reparar un componente de la red
        ]
        ];
        policy action: [
                domain red/ execute registro  //Registrar nuevo componente
        ]
```

CONTABILIDAD

```
//Medir el uso de los recursos utilizados por los usuarios de la red
//Crear una política para medir el uso de los recursos utilizados por los usuarios de la
red
        policy := root/factory/ecapolicy create.
        policy event: root/event/medir_recursos;
        policy event: root/event/monitoreo;
        policy event: root/event/registro_ancho_banda;
        policy event: root/event/registro_email;
        policy event: root/event/registo_backups;
        policy event: root/event/registo_backbone;
        policy condition: [ :recolectar_elementos_red :recolectar_usuarios_finales     |
                recolectar_elementos_red == 1       //Equipos de interconexion
```

```
        |       recolectar_usuarios_finales == 1    //Equipos de usuario final
        ];
        policy action: [
                domain red/ execute registo_ancho_banda //Mantener registro de uso del
                ancho de banda otorgado por el ISP
        |       domain red/ execute registo_email //Mantener registro de uso de
                almacenamiento del correo
        |       domain red/ execute registo_backups //Mantener registro de uso de backups
        |       domain red/ execute registo_backbone //Mantener registro de uso del ancho
                de banda en el backbone interno
        ]
```

DESEMPEÑO

```
//Monitoreo en la Red UTB
//Crear una política para caracterizar los tráficos internos y externos de la red
        policy := root/factory/ecapolicy create.
        policy event: root/event/medir_recursos;
        policy event: root/event/monitoreo;
        policy condition: [ :recolectar_elementos_red :recolectar_usuarios_finales     |
                root print: "Monitorear trafico interno"   //Equipos de interconexion
        |       root print: "Monitorear trafico externo"   //Equipos de usuario final
        |       root print: "Monitorear segmentos de la red"
        ];
        policy action: [
                domain red/ execute monitoreo
        &
                domain red/ execute registo_ancho_banda //Mantener registro de uso del
                ancho de banda otorgado por el ISP
        |       domain red/ execute registo_email //Mantener registro de uso de
                almacenamiento del correo
        |       domain red/ execute registo_backups //Mantener registro de uso de backups
        |       domain red/ execute registo_backbone //Mantener registro de uso del ancho
                de banda en el backbone interno
        ]
```

SEGURIDAD

```
//Ingreso a la red para los estudiantes
//Crear una política para el ingreso de los estudiantes a la red UTB
        policy := root/factory/ecapolicy create.
        policy event: root/event/ingreso_estudiantes;
        policy condition: [ :recolectar_elementos_red :recolectar_usuarios_finales     |
                solicitud_cable == 1
        |       solicitud_nodo_inalambrico == 1
        ];
        policy action: [      :nodo_mac      :ip
                root print: "Conexion establecida al nodo" + nodo_mac
                ip:= nodo
        |       root print: "Nodo autenticado"
                root print: "Conexion establecida al nodo" + nodo_mac
                ip:= nodo
        ]

//Ingreso a la red para los empleados
//Crear una política para el ingreso de los docentes o administrativos a la red UTB
        policy := root/factory/ecapolicy create.
        policy event: root/event/ingreso_empleados;
        policy condition: [ :recolectar_elementos_red :recolectar_usuarios_finales     |
                solicitud_cable == 1
```

```
        |             solicitud_nodo_inalambrico == 1
        ];
        policy action: [      :nodo_mac      :ip
                root print: "Nodo autenticado"
                root print: "Conexion establecida al nodo" + nodo_mac
                ip:= nodo
        ]

//Solicitud de ingreso a la red por medio de un VPN
//Crear una política para el ingreso de los docentes o administrativos a la red UTB
        policy := root/factory/ecapolicy create.
        policy event: root/event/ingreso_empleados;
        policy condition: [ :recolectar_elementos_red :recolectar_usuarios_finales     |
                solicitud_cable == 1
        |       solicitud_nodo_inalambrico == 1
        ];
        policy action: [      :nodo_mac      :ip
                root print: "Nodo autenticado"
                root print: "Conexion establecida al nodo" + nodo_mac
                ip:= nodo
        ]

//Un nodo está haciendo mal uso de la red
//Crear una política para detectar cuando un nodo está haciendo mal uso de la red
        policy := root/factory/ecapolicy create.
        policy event: root/event/nodo_mal_uso;
        policy condition: [ :nodo_mac :pagina_sospechosa :log_prohibido  |
                pagina_sospechosa == 1
        &               log_prohibido == 1
                root print: "El nodo" + nodo_mac + "está haciendo mal uso de la red"
                set alarm true
        ];
        policy action: [      :nodo_mac :ip :restriccion
        [
                IF (ip == restriccion)
                nodo_mac print:"No se puede acceder a la página"
        ]
        ]

//Un usuario solicita realizar un backup a su equipo
        policy := root/factory/ecapolicy create.
        policy event: root/event/solicitud_backup;
        policy condition: [ :nodo_mac :pagina_sospechosa :log_prohibido  |
                cambio_maquina == 1
        |       solicitud == 1
        |       usuario_tipo_especial == 1
                set alarm true
        ];
        policy action: [      :nodo_mac :ip :restriccion
                root print "Auxiliar dirigirse hacia el nodo" + nodo_mac
        ]
```