Maestría en Informática Aplicada

Sistema de detección y aislamiento de fallas en la red del campus de la universidad Agostinho Neto

Trabajo final presentado en opción al título de

Máster en Informática Aplicada

Autor: Joaquim Lauriano da silva

Tutores: Dr. Orestes Febles Días

Msc. Mónica Peña Casanova

Ciudad de La Habana, diciembre de 2015

Agradecimientos

Dedicatoria

Resumen

La sociedad actual está caracterizada por un creciente uso de los medios tecnológicos, los cuales están directamente ligados a todos los sectores como es el caso de la medicina, la educación, la economía, el ejército. De igual forma que existe un avance tecnológico en el mundo, n la UAN constituye un objetivo la alineación de las TI con los objetivos de negocio, o cual ha implicado un incremento de servicios y aplicaciones en red. La adopción de la tecnología resulta en la necesidad de la gestión de la misma, actualmente existen varios estándares y guías de buenas prácticas para la gestión de medios tecnológicos y servicios, como son los casos del estándar ITIL, COBIT y la norma ISO/IEC 20000.

Por las insuficiencias observadas en el proceso de gestión de red en el campus de la universidad Agostinho Neto según lo que plantean los estándares de gestión en cuanto la detección, localización y resolución de problemas en medios tecnológicos y servicios, la presente investigación se centra en desarrollo de un sistema de detección y aislamiento de fallas en la red del campus de la universidad Agostinho Neto, lo cual tiene como valor agregado un ambiente de gestión que integre las funcionalidades de una base de datos de gestión de configuraciones para el control de los activos de la red, algoritmos proactivos en la detección y aislamiento de fallas en la red, y la automatización de medidas de control teniendo en cuenta los resultados proveídos por estos algoritmos. Los tres grupos de funcionalidades corresponden a los distintos módulos que componen el sistema y que se comunican para detectar y aislar posibles fallas en la red.

Para el desarrollo de la solución propuesta se realizó un estudio sobre la concepción de una base de datos de gestión de configuraciones según el estándar ITIL, la cual permite mantener el control de los activos de la infraestructura tecnológica, la gestión de fallas en la red para la detección, localización y resolución de problemas en la misma, y la gestión de redes basada en políticas para la automatización de medidas de control. Se prueba el sistema en un entorno de red simulado para evaluar su comportamiento en un entorno dinámico como el que podría ser en un entorno de red real.

Palabras claves: Base de datos de gestión de configuraciones, gestión de fallas en la red, gestión de redes basada en políticas, ITIL.

Índice

Introducción

La universidad Agostinho Neto (UAN) es la mayor institución de enseñanza superior y primera universidad pública de Angola. Está compuesta por una entidad central, respectivamente el rectorado, 7 facultades, 1 instituto superior y 10 centros de investigación. En 2012, se inaugura el campus universitario de la UAN, una estructura con varios edificios que permitió tener en una misma ubicación el rectorado y las facultades de ciencia e ingeniería.

En la medida que las organizaciones automatizan sus procesos, se van volviendo más dependientes de la tecnología para generar nuevas formas de negocio, reducir sus costos y generar productos y servicios innovadores a la vez que son más susceptibles del impacto de los riesgos asociados a las mismas en sus procesos. Para lograr este impacto, es necesario alinear las TI a los procesos de las organizaciones [1].

De igual forma que hay un avance tecnológico en el mundo, la tendencia en la UAN es de alinear la tecnología con sus procesos de negocio, de esto modo se verifica el incremento de servicios y aplicaciones en red.

El campus de la UAN cuenta con una red de área local (LAN, por sus siglas en ingles), que permite ofrecer los servicios del sistema integrado de gestión de examen de acceso (SIGEA), el sistema integrado de gestión académica (SIGA) y el así como el acceso a los servicios básicos de Internet. Una red de área local es una red privada contenida en un único edificio o Campus universitario con hasta algunos kilómetros de extensión [2].

Desde la concepción de la red LAN del campus de la UAN, estaba previsto su crecimiento en cuanto a su alcance geográfico y a los servicios que soportaría. El crecimiento de la red ha implicado el despliegue de servicios en servidores distribuidos en diferentes edificios del Campus para la alta disponibilidad de los mismos.

En la medida que se automatizan los procesos de negocio, aumenta la necesidad de gestionar las infraestructuras y servicios de las tecnologías de la información que los soportan debido a que las fallas de los mismos tienen un mayor impacto sobre el negocio

Actualmente existen varios estándares y guías de buenas prácticas para la gestión de medios tecnológicos y servicios, como son los casos del estándar ITIL [3], COBIT [4] y la norma ISO/IEC 20000 [5].

El estándar ITIL, que surge en mediados de los años 80 como un marco de referencia de mejores prácticas para gestionar operaciones y servicios de tecnología de

información (IT, por siglas en ingles), apunta la gestión de red como una de las funciones técnicas para la operación y entrega de servicios de calidad [3].

Para una correcta gestión de la red, el modelo OSI de gestión de red, describe cinco funciones de gestión que son [6]:

- Gestión de configuraciones cubre las funciones de hardware y software necesarias para el transporte eficiente y efectivo de los datos.
- Gestión de fallas incluye un conjunto de funciones necesarias para la detección, aislamiento y corrección de problemas.
- Gestión de rendimiento se encarga del monitoreo de los parámetros de rendimiento de la red para comprobar se estos están dentro de los límites establecidos.
- Gestión de contabilidad se encarga del registro del consumo de los recursos de la red por parte de los usuarios.
- Gestión de seguridad es responsable por la generación, distribución y mantenimiento de claves para encriptación, proveer mecanismos de control de acceso a los recursos de la red y análisis de trazas.

Para ITIL el núcleo de la gestión de operaciones y servicios de IT es la gestión de configuraciones [7], la cual hace el uso de la base de datos de gestión de configuraciones (CMDB, por sus siglas en inglés).

La CMDB es una base de datos lógica que guarda información sobre las configuraciones. Registra los atributos de cada elemento de configuración (CI, por su sigla en inglés) durante su ciclo de vida, sus relaciones con otros y los registros vinculados a cada uno, por ejemplo, registros de incidentes, problemas o cambios. Un CI, representa un activo o componente que está o deber ser controlado mediante la gestión de configuraciones. Los CI pueden variar ampliamente en complejidad, tamaño, estado y tipo, van desde un servicio completo hasta un módulo o componente de hardware de una sola aplicación, un CI puede contener otros CI [7]

Siendo la gestión de red una de las funciones técnicas para la operación y entrega de servicios de calidad en entornos IT, se torna indispensable la utilización de una CMDB para el monitoreo y control de inventario (hardware y software), localización de equipos y servicios y distribución de softwares en una LAN. De la CMDB se conocen los equipos que deben ser monitoreados para evaluar la calidad de servicio (QoS, por sus siglas en inglés) de la red.

La QoS [8], es la totalidad de las características de un servicio de telecomunicaciones que determinan su capacidad para satisfacer las necesidades explícitas e implícitas del usuario del servicio. Los parámetros de QoS son:

- Latencia que es a la suma de retardos temporales dentro de una red. Un retardo es producido por la demora en la propagación, transmisión y procesamiento de paquetes dentro de la red [9];
- El caudal o uso del ancho de banda disponible, se define como el tráfico total de datos que es recibido con éxito por el nodo destino en un tiempo determinado [10];
- La pérdida de paquetes es el parámetro que indica el número de paquetes que se pierden durante la transmisión [10];
- La disponibilidad indica la utilización de los diferentes recursos y se especifica en porciento [10]

El monitoreo de estos parámetros en los equipos permite la detección de fallas en la red. Una falla representa una propiedad inaceptable del sistema o de algún componente del sistema [11].

Hay algunas variaciones en la definición de fallas en una LAN, pero hay un concepto más genérico, que la caracteriza como una condición en la red, en la cual “el servicio ofrecido se desvía de lo especificado” [12].

Existen dos formas de actuación asociadas a la gestión de redes: el monitoreo y el control. El monitoreo es donde se engloban todas las operaciones de obtención de datos acerca del estado y comportamiento de los recursos de una red y en el control teniendo en cuenta el procesamiento de los datos obtenidos en la monitorización se realiza una configuración a la red gestionada [13].

La detección de los síntomas que preceden a la ocurrencia de fallas en la red permite a los administradores de red la aplicación de medidas de control que se anticipen a la ocurrencia de las fallas, estas medidas son aplicadas a los equipos que componen a la red, y cuanto mayor es la red más compleja se torna esta tarea, la arquitectura de gestión de red basada en políticas (PBNM, por sus siglas en inglés) propuesta por el *Internet Engineering Task Force* (IETF) ayuda a solucionar esta situación.

La tarea de monitoreo de la red es ejecutada por medio de sistemas de gestión de gestión de red. Un sistema es un conjunto de elementos, que relacionadas entre sí contribuyen para alcanzar un fin. Para la gestión de red, un sistema debe permitir la realización de una o más funciones de gestión de red.

Actualmente existe una gran variedad de sistemas que auxilian en el proceso de monitoreo de la red, como son los casos del PRTG [14], el Nagios [15], el Zenoss [16], el Cacti [17] entre otros. Normalmente estos sistemas hacen el monitoreo de servidores y servicios, de los parámetros de QoS y de rendimiento físico de los equipos, en algunos casos es necesario la aplicación de otros enfoques para la detección de los síntomas que preceden a las fallas.

En los estudios realizados por [18], [19] [20], [21] se utiliza el protocolo simples de gestión de red (SNMP, por sus siglas en inglés) para obtener los datos de las variables en la base de información de gestión (MIB, por sus siglas en inglés) de los equipos y observar los síntomas asociados a la ocurrencia de una falla mediante el análisis de estas variables, estos síntomas son llamados de anomalías. Para el autor de esta investigación este enfoque puede ser utilizado como una solución complementaria a los sistemas tradicionales para el monitoreo de la red por lo que su efectividad consiste en la anticipación de las fallas que causan la degradación o interrupción de los servicios telemáticos brindados por la red.

Por lo planteado, se verifica que cuando una institución recorre al uso de la tecnología para auxiliar en su proceso de negocio, ella debe satisfacer las necesidades de los usuarios, para lo cual es necesario un proceso de gestión que permita detectar cuando existan desviaciones con respecto al comportamiento esperado en este entorno y así aplicar medidas de control.

Una encuesta aplicada a cuatro técnicos responsables por la gestión de redes del campus de la UAN, los cuales dos son ingenieros informáticos y suman un total tres años de experiencia con la red desde la apertura del campus en 2012, arrojo que se utiliza la herramienta Nagios para el monitoreo de servidores y servicios de red y la herramienta Cacti para medir el tráfico en los switches.

Estas dos herramientas son de gran utilidad para la gestión de la red una vez que el Nagios permite saber cuándo los servidores y servicios están funcionando correctamente o no, el Cacti presenta los gráficos que ayudan en el análisis de tendencia en la red, sin embargo se verifica el siguiente escenario en la gestión de la red del campus de la UAN:

- Control de inventario de los activos de la red (*hardware y software*) deficiente no permitiendo mantener un registro automatizado de los mismos, la información acerca de la relación existentes entre ellos y sus localizaciones físicas, lo cual provoca retrasos a la atención a las fallas.

- Con las herramientas Nagios y Cacti las fallas son detectadas después que se cause la degradación de los servicios telemáticos, resultando en usuarios insatisfechos e imposibilitados de realizar las tareas que conforman los procesos de negocio de la Universidad.
- Insuficiencias en la detección de síntomas asociados a fallas de la red ya que la evaluación de parámetros de QoS y de rendimiento físico de los equipos solo permiten realizar una gestión de fallas reactiva y no proactiva y retrasa la localización de la raíz e imposibilita la automatización de las tareas de control asociadas a la solución de fallas.
- Trazabilidad de los síntomas asociados a las fallas en la red compleja lo que imposibilita evaluar de antemano los daños colaterales asociados a la ocurrencia de fallas.
- Estos problemas están asociados a que en el proceso de gestión de redes en el campus de la universidad Agostinho Neto no existe una solución complementaria a las herramientas existentes que previne efectivamente la degradación de los servicios telemáticos brindados a los usuarios de la red.
-

De acuerdo con el escenario presentado se planteó el siguiente **problema de investigación**: ¿Cómo prevenir efectivamente la degradación de los servicios telemáticos brindados a los usuarios de la red del campus de la universidad Agostinho Neto?

Para el presente trabajo, se consideró como **objeto de estudio** el proceso de gestión de redes. EL **objetivo general** del presente trabajo es desarrollar un sistema de detección y aislamiento de fallas en la red del campus universitario de la universidad Agostinho Neto.

La investigación tendrá como **campo de acción** la detección y aislamiento de fallas en una red. Se plantea como **hipótesis** que el desarrollo de un sistema de detención y aislamiento de fallas en la red que incluya una base de datos de gestión de configuraciones para el control de los activos de la red, algoritmos proactivos en la detección y aislamiento de fallas en la red, y la automatización de medidas de control teniendo en cuenta los resultados proveídos por estos algoritmos permitirá prevenir efectivamente la degradación de los servicios telemáticos brindados a los usuarios de la red del campus de la universidad Agostinho Neto.

Teniendo como marco el cumplimiento del objetivo general se plantean los siguientes los **Objetivos específicos:**

- Elaborar el marco teórico referencial que incluya las teorías concernientes a la gestión de red y temas relacionados, para la obtención de los elementos claves en la detección y aislamiento de fallas en la red.
- Implementar algoritmos proactivos para la detección de fallas y para el análisis de su propagación sobre la red.
- Desarrollar el sistema de detención y aislamiento de fallas en la red.
- Realizar pruebas que permitan verificar la efectividad del sistema propuesto.

Para el presente trabajo los métodos de investigación empleados son el método **analítico-sintético** para el análisis de las teorías relacionas con la gestión de red y de allí extraer los elementos esenciales, el método **inductivo-deductivo** para la generalización de experimentos hechos sobre casos particulares o inferir de conocimientos generales para casos particulares y el **hipotético-deductivo** en la previsión del impacto que cada uno de los componentes del sistema tendrá en la realidad actual.

La tesis está compuesta por un resumen, una introducción, tres capítulos, cuenta también con conclusiones y recomendaciones, referencias bibliográficas, y anexos.

En el capítulo 1, **la gestión de redes y temas relacionados**, se elabora el marco teórico referencial sobre la gestión de redes y temas relacionados para la detección y aislamiento de fallas en la red.

En el capítulo 2, **sistema de detección y aislamiento de fallas en la red del campus de la universidad Agostinho Neto**, se presenta diagnóstico actual de la gestión de redes en campus de la universidad Agostinho Neto y el modelado de la arquitectura del sistema de detección y aislamiento de fallas en la red, en que se describen cada componente y su implementación.

En el capítulo 3, **validación y pruebas de efectividad del sistema de detección y aislamiento de fallas en la red**, se hace un resumen de las pruebas realizadas para validar las funcionalidades del sistema durante la fase de implementación y su prueba en un entorno de red simulado.

Capítulo 1 – La gestión de redes y temas relacionados

La gestión de red es un proceso que incluye la inicialización, el monitoreo y el control de una red de comunicaciones para que ella cumpla con el objetivo de su construcción, en el que varios métodos y algoritmos son implementados para lograr el correcto funcionamiento de una red. La gestión de la red camina hacia la automatización en el cual la gestión de redes basada en políticas se ve como una solución prominente.

Este proceso constituye una de las funciones prácticas para la operación y entrega de servicios de calidad en entornos IT, los cuales son próvidos de un conjunto de estándares y guías de buenas prácticas para gestionar de los mismos, como son los casos del COBIT, CMMI-DEV, ISO/IEC 2000 y ITIL que es uno de los más aceptados por la comunidad.

1.1 Estándar Itil

El estándar ITIL, que surge en mediados de los años 80 como un marco de referencia de mejores prácticas para gestionar operaciones y servicios de tecnología de información (IT, por siglas en ingles), apunta la gestión de red como una de las funciones técnicas para la operación y entrega de servicios de calidad [3].

Además de ITIL, existen otros estándares y guías de buenas prácticas para la gestión de IT, como son los casos de COBIT [4], CMMI-DEV [22] y ISO/IEC 2000 [5] los cuales presenta las siguientes características:

- La primera publicación de COBIT surge en 1996, por la ITGI como un marco de trabajo y un conjunto de herramientas de gobierno de tecnología de información, que permite la mayor compatibilidad entre los requerimientos de control, aspectos técnicos y riesgos de negocios, permitiendo con eso el desarrollo de políticas claras y buenas prácticas para la gestión de tecnología de información a lo largo de las organizaciones.
- El CMMI-DEV es un modelo que se enfoca en las actividades para desarrollar productos y servicios de calidad. Contiene prácticas que cubren los procesos de administración de proyectos, administración de procesos, establecimiento de servicios, entrega de servicios, así como otros procesos de soporte.
- ISO/IEC 2000 es un estándar internacional e independiente para la calidad en la gestión de servicios de IT, posibilita que las organizaciones puedan demostrar la calidad de los servicios IT que ofrecen a sus clientes, así como construir y mantener un sistema de gestión de servicios que tenga calidad. ITIL es

totalmente compatible con el estándar ISO/IEC 20000 y las organizaciones que implementan ITIL fácilmente obtienen una certificación ISO/IEC2000 [23].

Estos estándares son de grande aceptación a nivel mundial, su empleo dependerá en gran medida del entorno en cuestión, el CMMI-DEV se centrar principalmente en el desarrollo de los servicios, el ISO/IEC 20000 está más virado en la conformidad de los requerimientos para una gestión de servicios de calidad, el COBIT que puede ser utilizado en complemento con ITIL, está enfocado en la verificación de la conformidad en cuanto a disponibilidad, rendimiento y riesgos asociados a servicios.

De acuerdo con esto, el estándar ITIL mejor se adecua a las necesidades presentadas, además de que es el más aceptado y usado por la comunidad, describe mejor los aspectos relativos a la construcción de una base de datos de gestión de configuraciones.

Para ITIL la gestión de servicios es basado en un ciclo de vida del servicio, lo cual está dividido en 5 fases que son [3] :

- Estrategia del servicio, proporciona a las organizaciones las habilidades para diseñar, desarrollar e implementar a la gestión de servicios como un activo, así como para pensar y actuar de una manera estratégica, es relativo a los procesos para la estrategia, gestión de portafolio, gestión de la demanda y gestión financiera del servicio.

- Diseño del servicio, es responsable por el diseño de un servicio nuevo o modificado para su introducción en el ambiente de producción, aquí tenemos procesos como gestión de niveles de servicio, de catálogo de servicios, de configuraciones, de disponibilidad, de seguridad de la información, de proveedores, de capacidad y continuidad de servicio

- Transición del servicio, establece las expectativas del cliente acerca de cómo se puede utilizar el servicio para habilitar procesos de negocio, aquí los proceso a realizar son planeación y soporte en la transición, gestión de cambios, gestión de activos de servicio y de configuraciones, gestión de liberaciones e implementación, validación y pruebas del servicio, evaluación y gestión del conocimiento.

- Operación del servicio, es responsable por la gestión continua de la tecnología que se emplea para entregar y soportar el servicio, sus procesos vitales son la gestión de eventos, de incidentes, soluciones de servicio, problemas y acceso.

- Mejora continua del servicio, alinear continuamente los servicios de tecnología de información con los requerimientos del negocio al identificar implementar oportunidades de mejora para soportar el proceso de negocio, de modos que se aumente la eficiencia y reducción de costos.

En cada fase del ciclo de vida del servicio, hay un conjunto de procesos asociados al mismo, siendo respectivamente los procesos de gestión de [3]:

- Incidentes, tiene como objetivo resolver cualquier incidente que cause una interrupción en el servicio de la manera más rápida y eficaz posible;
- Problemas, responsable por investigar las causas subyacentes a toda alteración, real o potencial, del servicio TI, determinar posibles soluciones a las mismas, proponer las peticiones de cambio (RFC**,** por sus siglas en inglés) necesarias para restablecer la calidad del servicio, realizar revisiones de pos implementación (RPI, por sus siglas en inglés) para asegurar que los cambios han surtido los efectos buscados sin crear problemas de carácter secundario;
- Cambios, aquí se hace la evaluación y planificación del proceso de cambio para asegurar que, si éste se lleva a cabo, se haga de la forma más eficiente, siguiendo los procedimientos establecidos y asegurando en todo momento la calidad y continuidad del servicio TI;
- Versiones, es el proceso encargado de la implementación y control de calidad de todo el software y hardware instalado en el entorno de producción;
- Capacidad, es responsable por garantizar que todos los servicios TI se vean respaldados por una capacidad de proceso y almacenamiento suficiente y correctamente dimensionada;
- Disponibilidad, es responsable de optimizar y monitorizar los servicios TI para que estos funcionen ininterrumpidamente y de manera fiable, cumpliendo los niveles de servicios acuerdados (SLAs, por sus siglas en ingles) y todo ello a un coste razonable. La satisfacción del cliente y la rentabilidad de los servicios TI dependen en gran medida de su éxito
- Continuidad del servicio, se preocupa de impedir que una imprevista y grave interrupción de los servicios TI, debido a desastres naturales u otras fuerzas de causa mayor, tenga consecuencias catastróficas para el negocio;
- Niveles de servicio, su objetivo es de poner la tecnología al servicio del cliente;
- Financiera, es el de evaluar y controlar los costes asociados a los servicios TI de forma que se ofrezca un servicio de calidad a los clientes con un uso eficiente de los recursos TI necesarios

- De configuraciones, su encargo es mantener el registro actualizado de la estructura de IT, para esto hacen el uso de una base de datos de gestión de la configuración (CMDB, siglas en inglés);

Se observa la gestión de configuraciones como uno de los procesos a ser realizado en que la fase de diseño de servicio, según Klosterboer [7], este proceso es el núcleo de ITIL y de ello dependen todos los demás.

La gestión de configuraciones hace el uso de la CMDB, que es una base de datos lógica que guarda información sobre las configuraciones. Registra los atributos de cada elemento de configuración (CI, por su sigla en inglés) durante su ciclo de vida, sus relaciones con otros y los registros vinculados a cada uno, por ejemplo, registros de incidentes, problemas o cambios. Un CI, representa un activo o componente que está o deber ser controlado mediante la gestión de configuraciones. Los CI pueden variar ampliamente en complejidad, tamaño, estado y tipo, van desde un servicio completo hasta un módulo o componente de hardware de una sola aplicación, un CI puede contener otros CI [7].

La sección que sigue es relativa a la concepción de una CMDB de acuerdo con ITIL.

1.1.1 Base de datos de configuraciones

La CMDB es la base para el proceso de gestión de configuraciones y debe servir de soporte para los procesos de gestión de incidentes, de problemas, de cambios, de versiones, de capacidad, de disponibilidad, de continuidad del servicio, de niveles de servicios y financiera.

Un incidente es cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad del mismo [24], por lo tanto la gestión de incidentes trata de detectar cualquiera alteración en los servicios TI, registra y clasifica estas alteraciones, asigna el personal encargado de restaurar el servicio según se define en el SLA correspondiente. Hay una base de conocimientos asociada los incidentes, permitiendo consultar el proceso de resolución para incidentes similares que han ocurrido y facilita en la resolución. Para cada incidente se asocia los CI envueltos en el mismo, y una vez que se haya resuelto, sus datos son persistidos en la CMDB.

Pueden ocurrir situaciones en las que el incidente es recurrente y no se encuentra una solución definitiva al mismo, en este caso se convierte en un problema. Por lo tanto, entra la gestión de problemas para el estudio detallado de las causas subyacentes y

encontrar posibles soluciones. Cuando ya se conocen las causas para determinado problema, él pasa a ser un error conocido y se proponen soluciones para el mismo, enviadas a la gestión de cambios mediantes RFCs. Para cada problema, debe haber un registro en la CMDB conteniendo los CIs implicados, causas, síntomas asociados, soluciones temporales, servicios involucrados, niveles de prioridad, urgencia e impacto y estado.

En presencia de un RFC, la gestión de cambio es responsable por el registro del mismo en la CMDB, evaluar la propuesta de cambio a ver si acepta o rechaza la implementación. Los RFCs pueden provenir de la gestión de problemas, de la necesidad de implementación de nuevos servicios, de la necesidad de actualización de software de terceros o derivados de aspectos legales. Independientemente de su origen, se debe mantener una descripción del cambio propuesto (motivación, propósito, los CI involucrados), su estatus, esta información es actualizada durante todo el proceso relacionado al mismo.

Los cambios que si quieren implementar pasan por un proceso de diseño, prueba e instalación en el entorno de producción, de esto se encarga la gestión de versiones, ella en colaboración con la gestión de cambios y de configuraciones deben asegurar que los cambios se ven igualmente reflejados en la CMDB. Cada versión es referente a un grupo de CIs de nueva creación o modificados que han sido validados para su instalación en el entorno de producción.

Los RFCs, están asociados a cambios en la infraestructura y están relacionados a la corrección de problemas para mejora de servicios o la implementación de nuevos servicios involucrando CIs. Esto requiere la estimación de la capacidad necesaria de los CI, en términos de memoria y rendimiento para que soporten el servicio especificado, de esto se encarga la gestión de capacidad. Esto quiere decir que es responsabilidad de la gestión de capacidad asegurar el cumplimiento las necesidades de capacidad tanto presentes como futuras, controlar el rendimiento de la infraestructura, desarrollar planes de capacidad asociados a los SLA, gestionar y racionalizar la demanda de servicios. Todo este proceso produce datos que son almacenados a una base de datos de gestión de capacidad (CDB, por sus siglas en inglés) para su posterior uso, esta puede hacer parte de la CMDB o no, pero siempre debe existir una forma de relaciónalas de modos a que sea posible tener una visión general de los CIs e información relativa a su capacidad.

Se verifica una estrecha relación entre los procesos descritos, hay una necesidad de si solucionar los incidentes antes que se conviertan en problemas, transformar los

problemas en errores conocidos para rápida resolución, estudiar los cambios evitando que resulten en problemas, estimar la capacidad necesaria para la operación de los servicios y monitorear el rendimiento. Esto se hace con el fin de que los servicios estén disponibles para el usuario y que funcionen correctamente, que es el objetivo de la gestión de disponibilidad. El proceso es soportado por los indicadores de disponibilidad (porcentaje de tiempo sobre el total acordado en que los servicios TI han sido accesibles al usuario y han funcionado correctamente, la fiabilidad (medida del tiempo durante el cual los servicios han funcionado correctamente de forma ininterrumpida), la mantenibilidad (capacidad de mantener el servicio operativo y recuperarlo en caso de interrupción) y la capacidad de Servicio.

El conocimiento sobre la profundidad de la infraestructura IT y de los CIs involucrados a cada servicio, especialmente los críticos y estratégicos, ayuda a la gestión de continuidad del servicio a estimar el coste de la consecuencia de la indisponibilidad de los mismos en presencia de desastres naturales, o mismo de desastre puramente informáticos. Es también del encargo de la gestión de la continuidad de servicio analizar las posibles amenazas y estimar sus probabilidades, detectar los puntos más vulnerables y crear mediadas de prevención y recuperación basadas en ellos. Normalmente estas medidas resultan en la necesidad de inversiones financieras con la adquisición de nuevos productos.

Aunque parezcan solamente gastos, estas inversiones deben ser debidamente evaluadas para que se cumplan los niveles de servicios acuerdados. Este proceso es llevado a cabo en conjunto con la gestión de niveles de servicio y la gestión financiera. Para que se cumplan los niveles de servicios acuerdados, la gestión de niveles de servicios define los requisitos tecnológicos para la prestación de los servicios, la gestión financiera es responsable por evaluar el coste real a la prestación de servicio, proporcionar toda la información financiera precisa para la toma de decisiones y fijación de precios.

Por lo tanto, se verifica que todos estos proceso están relacionados con la CMDB quiere sea explícita o implícitamente, el nivel de detalle y alcance de la misma depende de la organización en cuestión, sus objetivos y necesidades. Estos son aspecto que se deben tener en cuenta a la hora de elegir la implementación de una Base de datos de gestión de configuraciones. Por otro lado, para el estándar ITIL una de las funciones técnicas para la operación y entrega de servicios de calidad es la gestión de redes, lo cual es fundamentalmente un proceso de monitoreo y control de una red de comunicaciones.

1.2 La gestión de redes de computadoras

La red es uno de los recursos más importantes de un sistema informático y por ello requiere un sistema de gestión y control para obtener un buen rendimiento y un alto nivel de seguridad [25]. Podemos definir la gestión de red como un proceso que incluye la inicialización, el monitoreo y el control de una red de comunicaciones para que ella cumpla con el objetivo de su construcción [6]. Muchos fueron los estudios realizados sobre la gestión de red, consecuentemente surge la arquitectura de gestión en entornos TCP/IP denominada SNMP, la arquitectura sistema de administración de información común / protocolo de administración de información común (CMIS/CMIP, por sus siglas en inglés) que inicialmente se han diseñado para operar con protocolos OSI y la arquitectura de redes abiertas (ONA, por sus siglas en inglés) que opera en redes SNA [25].

La arquitectura de gestión SNMP, es un conjunto de aplicaciones de gestión de red que utiliza los servicios ofrecidos por TCP/IP, que permite el control de la red. La misma es caracterizada por uno o más gestores SNMP y un conjunto de agentes SNMP, que hacen el uso de la información contenida en una base de datos de información de gestión (MIB, por sus siglas en inglés).

El modelo de gestión en OSI se encuentra estandarizado en ISO/IEC 10040 [26] y contempla la estructura de gestión, las funciones de gestión, y el flujo de control entre proceso. Las funciones descriptas por el modelo OSI de gestión de red son [6]:

- Gestión de configuraciones cubre las funciones de hardware y software necesarias para el transporte eficiente y efectivo de los datos;
- Gestión de fallas incluye un conjunto de funciones necesarias para la detección, aislamiento y corrección de problemas;
- Gestión de rendimiento se encarga del monitoreo de los parámetros de rendimiento de la red para comprobar se estos están dentro de los límites establecidos;
- Gestión de contabilidad se encarga del registro del consumo de los recursos de la red por parte de los usuarios;
- Gestión de seguridad es responsable por la generación, distribución y mantenimiento de claves para encriptación, proveer mecanismos de control de acceso a los recursos de la red y análisis de trazas;

Cada una de estas funciones se encargan de aspectos específicos, pero existe una estrecha relación entre ellas.

Por la complejidad y el gran tamaño de los entornos de red actuales, la gestión de redes camina hacia la automatización, siendo la gestión basada en políticas una de las técnicas empleadas en este contexto. El *Internet Engineering Task Force* (IETF) propuso una arquitectura de gestión de red basada en políticas (PBNM, por sus siglas en inglés) que permite a la automatización de la aplicación de medidas de control sobre la red en función de las condiciones dinámicas de la propia red.

Los entornos de red de área local actuales son caracterizados por el uso de la arquitectura TCP/IP, por tanto esta investigación se centra en la gestión mediante la arquitectura SNMP, las funciones gestión definidas en el modelo OSI, la de configuración para el control de activos de la red, la de rendimiento en la evaluación de las prestaciones de servicio de la red y la de fallas para detectar y aislar posibles fallas en la red y la gestión de redes basada en políticas para la automatización de la aplicación de medidas de control sobre la red en función de las condiciones dinámicas de la propia red, una vez estos temas están relacionados a la problemática.

1.2.1 Gestión de redes según la arquitectura SNMP

El proceso de gestión según la arquitectura SNMP, está enfocado a variables de gestión, es caracterizada por uno o más gestores, un conjunto de agentes que permiten obtener la información de gestión de los componentes de la red.

La arquitectura está basa en el protocolo simple de gestión de redes (SNMP, por sus siglas en inglés), lo cual fue originalmente desarrollado para la gestión de redes TCP/IP y Ethernet [6].

El protocolo SNMP es un protocolo de la capa de aplicación, actualmente se encuentra en la tercera versión. Su primera versión fue publicada en 1988, la cual presencio una gran expansión un su uso, y en el año 1993, fue publicado el SNMPv2. Con la agregación de mecanismos de seguridad como autenticación y control de acceso, durante el año 2000 fue publicado el SNMPv3.

Existen tres componentes para el protocolo SNMP, respectivamente el proprio protocolo, la MIB y la estructura de la información de gestión (SMI, por sus siglas en ingles) [27]. La SMI es un conjunto de reglas que definen los objetos dentro de la MIB, incluyendo tipos genéricos usados para describir la información de gestión.

El protocolo funciona basado en los siguientes elementos, el software gestor, el software agente y la MIB. El software gestor curre en una estación de gestión de red, es responsable por solicitar informaciones a los agentes por medio de comandos SNMP. El software agente representa un programa que curre dentro del dispositivo a ser

gestionado, tales como estaciones, un enrutadores, bridges o un Gateway[1]. Cada agente gestionado almacena los datos y probé estos datos al software gestor cuando este solicita. El tercer elemento es la MIB, esta es una base de datos que probé una representación estandarizada de los datos recogidos, está estructurada en forma de árbol e incluye grupos de objetos que pueden ser gestionados [6], como es ilustrado por la Figura 1.1.

El software gestor (*management console*) puede enviar uno de los comandos SNMP, para solicitar alguna información de los dispositivos gestionados (*HP3000, cisco router*), el software agente (*agent*), consulta la MIB y responde con la información relativa a la solicitación.

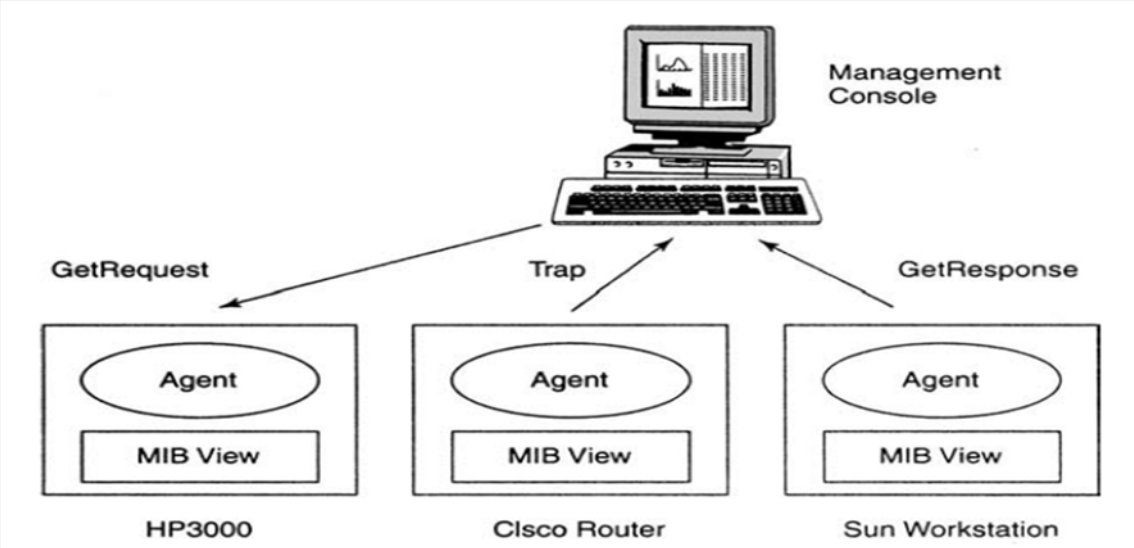

Figura 1.1 - Arquitectura de funcionamiento del protocolo SNMP. (Freman 2005)

Los comandos SNMP que permiten la comunicación entre el software agente y el softwares gestor son [27]:

- *GET-REQUEST:* Operación ejecutada por el software gestor para obtener el valor de una o varias variables de la MIB de un dispositivo.
- *GET-NEXT-REQUEST*: Operación ejecutada por el software gestor para obtener el valor de una o varias variables de la MIB de un dispositivo. La diferencia con la operación anterior radica en que esta devuelve la próxima variable del árbol de la MIB.

[1] *Una pasarela, puerta de enlace o gateway es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del*
protocolo utilizado en una red al protocolo usado en la red de destino

- *GET-BULK-REQUEST*: Operación ejecutada por el software gestor para obtener el valor de una o varias variables de la MIB de un dispositivo de forma eficiente. Es muy usada para obtener los valores de tablas de gran tamaño.
- *SET-REQUEST:* Operación realizada por el software gestor para establecer un valor sobre una o varias variables de la MIB en un dispositivo administrado.
- *RESPONSE:* Operación ejecutada por el agente SNMP en respuestas a las operaciones *GET-REQUEST*, *GET-NEXT-REQUEST* o *SET-REQUEST* para enviar los datos solicitados.

Las variables en una MIB está organizadas en una estructura en forma de árbol, compuesta por los siguientes grupos [28]:

- *System*, probé una lista de objetos relacionados a la operación del sistema, como o tempo de funcionamiento, contacto y nombre del sistema;
- *Interfaces (if)*, rastrea el status de cada interface en una entidad gestionada, hace el monitoreo de las interfaces en funcionamiento o inactivas y rastrea aspectos, como octetos enviados y recibidos, errores y eliminados;
- *Address translation (at*), es fornecido solamente para para mantener la compatibilidad con versiones anteriores;
- *Internet protocol (ip),* rastrea os diversos aspectos de la capa de red;
- *Internet control message protocol (icmp)*, rastrea aspectos como errores del ICMP;
- *Transmission control protocol (tcp)*, rastrea, entre otros aspectos, el estado de las conexiones TCP;
- *User datagram protocol (udp)*, rastrea dados estadísticos del UDP
- *Exterior Gateway protocol (egp)*, rastrea diversos dados estadísticos sobre o EGP
- *Simple network management protocol (snmp)*, evalúa el tráfico SNMP

Cada grupo de variables describe la funcionalidad de un protocolo específico en el equipo de red, por tanto dependiendo del tipo de información que se quiere o del tipo de equipo a monitorear, se debe elegir un grupo de variables apropiado.

El protocolo puede ser utilizado para obtener o establecer un valor de o sobre una o varias variables de la MIB de los equipos controlados por la gestión de configuraciones, proceso que se describe en la sección que se sigue.

1.2.2 Gestión de configuraciones

Una red de área local normalmente es un ambiente complejo y en constantes cambios, se torna evidente que se debe tener un profundo conocimiento de la misma y los cambios asociados para una correcta gestión, de esto se encarga la gestión de configuraciones.

La gestión de configuraciones cubre las funciones de hardware y software necesarias para el transporte eficiente y efectivo de los dato. Por lo tanto, la gestión de configuraciones consiste en tener bajo control los dispositivos de hardware, incluyendo cables, computadoras y adaptadores de red, como también la configuración lógica de la red por medio de la instalación de un sistema operativo de red, la selección de los protocolos de red y la forma como los utilizadores pueden acceder a los recursos de la red [6].

Mantener una visión general de todos los componentes de la red, soportar la configuración de los dispositivos de red y mantener un registro de los cambios en la red es la responsabilidad de la gestión de configuraciones [29]. Por lo tanto, en el centro de las operaciones realizadas por la gestión de configuraciones se encuentra la base de datos de gestión de configuraciones, que permite mantener el registro de la estructura y componentes de la red.

Es un proceso que incluye varias tareas, como tal tenemos la planificación, clasificación y registro, monitorización, Control y auditorias, que son descriptas a continuación [3]:

- En la planificación se designa un responsable, por lo que una descentralización excesiva puede generar descoordinación y llevar al traste todo el proceso, se elige alguna herramienta de software adecuada a las actividades requeridas, una organización manual es impracticable, se realiza un cuidadoso análisis de los recursos ya existentes, se establece el alcance y objetivos, el nivel de detalle y el proceso de implementación.
- En la clasificación y registro, son caracterizados el alcance, el nivel de detalle y profundidad de la base de datos de gestión de configuraciones. El alcance es relativo a los sistemas de hardware y software implicados en los servicios críticos, los componentes que se deben incluir dependiendo de su ciclo de vida. Determinar los atributos de los componentes de red, las relaciones lógicas y físicas entre eles los diferentes componentes son aspectos relativos al nivel de detalle y profundidad.

- La monitorización permite conocer el estado de cada componente durante todo su ciclo de vida, permite conocer los componentes responsables por una degradación en la calidad de servicio de la red.
- Mantener actualizada la base de datos de gestión de configuraciones, relativamente a los cambios observados en la red, es correspondiente a la tarea de control. Aquí se debe asegurar que todos los componentes estén registrados en la base de datos de gestión de configuraciones, monitorizar el estado de los componentes, actualizar las relaciones entre ellos e informar sobre el estado de las licencias.
- Como se ha visto la estructura de la red es dinámica, la auditoria debe verificar la conformidad entre el ambiente real de la red con la información almacenada en la base de datos de gestión de configuraciones.

Tener en cuenta los aspectos referenciados, es el primer paso para un proceso de gestión eficiente, pues una correcta gestión de configuraciones permite la resolución más rápida de los problemas, que redunda en una mayor calidad de servicio, es imprescindible conocer la estructura antes de efectuar un cambio, ayuda en la reducción de costes por duplicidad, se pueden identificar tanto copias ilegales de software que pueden suponer incumplimientos de los requisitos legales que pueden repercutir negativamente en la organización, incrementa los niveles de seguridad y una mayor rapidez en la restauración del servicio.

De la gestión la de configuraciones resulta el control de activos, conocimiento de la topología de la red y se fornece a la gestión de rendimiento información sobre que equipos se debe evaluar las prestaciones de servicio.

1.2.3 Gestión de rendimiento

La gestión de rendimiento es referente a aquellas actividades necesarias para asegurar que la red funcione de un modo regulado, sin retardos irrazonables en los servicios [6]. Por lo tanto, la satisfacción de los usuarios de una red, es cuestión dependiente de la calidad de servicio ofrecida por la misma.

La calidad de servicio (QoS, por sus siglas en inglés) [8] es la totalidad de las características de un servicio de telecomunicaciones que determinan su capacidad para satisfacer las necesidades explícitas e implícitas del usuario del servicio.

En una red de área local, los parámetros de QoS más significativos son [30]:

- Latencia que es a la suma de retardos temporales dentro de una red. Un retardo es producido por la demora en la propagación, transmisión y procesamiento de paquetes dentro de la red [10];
- El caudal o uso del ancho de banda disponible, se define como el tráfico total de datos que es recibido con éxito por el nodo destino en un tiempo determinado [10];
- La Pérdida de paquetes es el parámetro que indica el número de paquetes que se pierden durante la transmisión [10];
- La disponibilidad indica la utilización de los diferentes recursos y se especifica en porciento [10];

La gestión de rendimiento evalúa el rendimiento de la red, incluyendo la latencia, la pérdida de paquetes, el caudal y el *jitter* (variaciones en el retardo) [29]. Esto quiere decir que, se torna responsabilidad de la gestión de rendimiento, el monitoreo de estos parámetros para verificar se estos están dentro de los límites especificados. El monitoreo incluye tanto la circulación de datos entre estaciones, como también entre estaciones y servidores, el uso de enrutadores, puentes, Gateway y la utilización de cada segmento de red de acuerdo con su capacidad máxima.

Como resultado del monitoreo, se obtiene las informaciones que permiten ajustar el uso de los componentes de hardware y software de la red, como también considerar la reconfiguración de la misma para mejor proveer de servicio, permitiendo a la gestión de fallas evitar los problemas antes que estos ocurran.

1.2.4 Gestión de fallas

Independientemente de su entorno, todos los sistemas son susceptibles a tener momentos no deseables, por lo tanto las redes de área local también presentan escenarios no satisfactorios en los cuales un componente falla y otros problemas puedan ocurrir. Una falla representa una propiedad inaceptable del sistema o de algún componente del sistema [11], y la gestión de fallas incluye un conjunto de funciones necesarias para la detección, aislamiento y corrección de problemas en la red [6].

Se tratando de una red de área local, se torna difícil la caracterización de lo que es una falla, podemos estar hablando de un corte de corriente, de cables cortados, de un enrutador o switch quebrado, del uso inapropiado de la red, de la congestión temporaria causando retardos en la red, de una estación con placa de red quebrada, o errores en los protocolos. Para un administrador de red el sobrepaso de umbrales establecidos para los parámetros de Qos puede ser un síntoma indicador de una falla y si se trata de

la perspectiva del usuario, demoras demasiado altas en las respuestas a las requisiciones pueden significar una falla.

Hay algunas variaciones en la definición de fallas en redes de área local, pero hay un concepto más genérico, que la caracteriza como una condición en la red, en la cual “el servicio ofrecido se desvía de lo especificado” [12].

Muchos autores [18] definen dos tipos de fallas en una red de área local, que son duras y blandas. Una falla dura es caracterizada por la incapacidad de entrega de paquetes, mientras que una falla blanda es caracterizada por una pierda parcial del ancho de banda disponible.

Conocer los síntomas de una falla es el primer paso para la detección e identificación de la misma, una falla dura es fácilmente notada, una vez que la red se queda inhabilita para ofrecer servicios. Una falla blanda puede ocurrir y no siempre los usuarios se dan cuenta hasta que tenga un efecto más severo en la red.

Por tanto, las fallas blandas y duras pueden ser asociadas al protocolo básico de las métricas de rendimiento, tales como la latencia y el caudal. Para identificar que parámetros son afectados por una falla y como son afectados envolví la recoja empírica de datos en presencia de la falla, y la ocurrencia de la degradación del rendimiento es determinada usando la detección de anomalías [18]. Las anomalías en la red, normalmente son referentes a situaciones en las que la operación de la red se desvía del comportamiento normal [20].

Fenómenos como falla en el servidor de ficheros, paginación de la red, tormenta de *broadcast* y congestión de la red, son algunas de las anomalías que representan fallas blandas, o sea con implicación en el rendimiento de la red [20]. Una falla en el servidor de ficheros se puede dar debido al incremento en el número de requisiciones *ftp* al mismo, una paginación de la red ocurre cuando en una estación corre un proceso que requiere una capacidad mayor de memoria física de la que esta posee, resultando en un elevado intercambio de paquetes con el servidor, se esto perdura durante un largo periodo de tiempo puede resultar en una caída en el ancho de banda disponible. Una tormenta de *broadcast* se refiere a una situación en la que paquetes de *broadcast* son largamente enviados hasta el punto de deshabilitar la red. Pueden ocurrir situaciones en que una estación empieza a enviar pequeños paquetes en un ciclo infinito para checar alguna información.

Tottan y Ji [20] plantean que el tipo de falla que puede ser detectado depende de la fuente de los datos que se consulte. Se pueden obtener los datos por pruebas a la red,

usando herramientas como *ping* y *tracerout,* filtrado de paquetes para la estadística basada en el flujo, en que se hacen captura de la cabecera de un conjunto de paquetes que circulan en distinto puntos de la red, datos provenientes de los protocolos de enrutamiento y datos provenientes de los protocolos de gestión (ICMP y SNMP).

La detección de los síntomas o anomalías que preceden a la ocurrencia de fallas en la red permite a los administradores de red la aplicación de medidas de control antes mismo que la falla ocurra, estas medidas son aplicadas a los equipos que componen a la red, y cuanto mayor es la red más compleja se torna esta tarea.

Por la complejidad y el gran tamaño de los entornos de red actuales la aplicación de medidas de control se torna un proceso requiere de mucho esfuerzo por parte de los administradores, por eso la gestión de redes camina hacia la automatización, siendo la gestión basada en políticas una de las técnicas empleadas en este contexto.

1.3 Gestión de redes basada en políticas

En la gestión tradicional de redes uno o más operadores, normalmente miembros de un grupo IT o una organización similar dentro de una empresa, configuran manualmente cada recurso (servidores, enrutadores, switches u hosts) de la red para la implementación de las políticas de la empresa sobre el uso de la red [31]. Una política es un conjunto de directivas o reglas especificadas por el operador para gestionar ciertos aspectos, que permiten obtener los resultados deseados en el comportamiento de la red entre usuarios y aplicaciones [32].

Por otro lado, la gestión tradicional de redes es un proceso exhaustivo, y típicamente lento en dar respuesta al cambio de las condiciones de la red [31]. La gestión de redes basada en políticas (PBNM, por sus siglas en inglés) supone un cambio importante en la gestión tradicional de redes, en lugar de la configuración exhaustiva para cada recurso de la red permite controlar y coordinar de manera dinámica los elementos de red, tomando decisiones de forma automática a través de reglas, solicitudes del personal que administra la red y/o los servicios.

La arquitectura PBNM [33] propuesta por el *Internet Engineering Task Force* (IETF) recomienda una serie de elementos, protocolos y lenguajes de especificación de políticas como ilustra la Figura 1.2. Esta arquitectura permite centralizar la gestión de las políticas e integrar diferentes modelos de gestión para regular las comunicaciones entre los elementos de red que participan en la gestión distribuida.

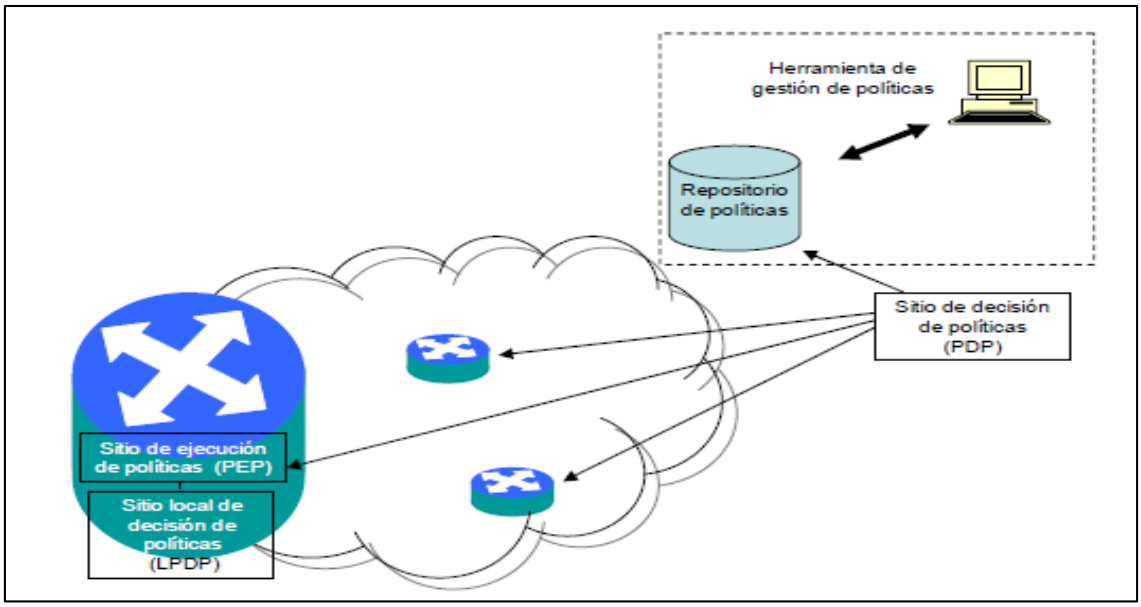

Figura 1.2 - Arquitectura PBNM

Un sistema de gestión desarrollado según esta arquitectura incluye los siguientes elementos:

- Herramienta de creación de políticas, ayuda a los administradores a crear políticas.
- Repositorio de Políticas: se almacenan las políticas que se generan.
- Punto de ejecución de políticas (PEP, por sus siglas en ingles), es una entidad donde las políticas son aplicadas.
- Punto de decisión de políticas (PDP, por sus siglas en ingles), es el responsable de obtener las políticas de las bases de datos de políticas y generar las decisiones acordes con las peticiones de los PEP.
- Punto local de decisión de políticas (LPDP, por sus siglas en inglés): es opcional y está localizado en el PEP. En caso de que se emplee, debe mantener la operación si la conexión con el PDP se interrumpe.

En la implementación de la PBNM son necesarios algunos estándares entre los cuales están:

- El SNMP, está enfocado a variables de gestión, es caracterizada por uno o más gestores, un conjunto de agentes que permiten obtener la información de gestión de los componentes de la red.
- El *Policy Core Information Model* (PCIM), es un estándar desarrollado por la IETF (RFC 3060) que recoge la terminología asociada al empleo de políticas así como la forma en que las políticas son modeladas, creadas y aplicadas.

- El *Common Object Policy Service protocol* (COPS) [34], fue definido en el grupo de trabajo IETF *Resource Allocation Protocol* (RAP) para apoyar el uso de políticas en redes IP con QoS, empleando COPS los servidores de políticas administran la red, comunicando la política decidida a los clientes (los elementos de la red), dónde las decisiones son implementadas.

La inclusión de las políticas dentro de la gestión de red tradicional persigue el añadir más flexibilidad a las operaciones de gestión con vistas a ser capaces de traducir los requisitos del negocio en políticas concretas que enlacen las necesidades del negocio con el comportamiento deseado de la red.

La aplicación conjunta de algoritmos para el diagnóstico de fallas en la red y la PBNM permite la elaboración de políticas teniendo en cuenta los síntomas asociados a las fallas, añadiendo al proceso de gestión de red tradicional la capacidad de toma de decisiones correctas de configuración de los elementos de red basándose en dichas políticas, y permitiendo finalmente su ejecución dentro de los dispositivos de red.

1.4 Algoritmos para el diagnóstico de fallas en la red

En los últimos años muchas soluciones han sido desarrolladas para el diagnóstico de fallas en la red, empleándose máquinas de estado finito [35] [36] [37], métodos estadísticos [19] [20] [38], aproximaciones basadas en reglas, ajustes de patrones, redes neuronales, lógica de fuzzy y teoría de grafos.

Estas soluciones están divididas en algoritmos para la detección de fallas y algoritmos para la localización [21]. La detección de fallas puede ser entendida como una indicación en línea de que algún componente de la red está funcionando mal, normalmente los componentes de red proveen indicadores, en forma de alarmas, cuando notan un mal funcionamiento [39]. Estos componentes sólo tienen una vista local de la falla, y por lo tanto no pueden describir la falla, apenas sus consecuencias visibles [40].

Los algoritmos para la localización de la falla son responsables por el análisis de las alarmas generadas por los componentes de la red proponiendo posibles hipótesis sobre la causa de la falla [39].

Para la elaboración de soluciones que visen a la detección y aislamiento de fallas en la red son empleados varias técnicas tales como máquinas de estado finito [41] [42], métodos estadísticos, aproximaciones basadas en reglas [43], ajustes de patrones, redes neuronales [44] [45] [46] [47] [48], lógica de fuzzy y teoría de grafos [42]. Estas

técnicas son utilizadas por algoritmos para la detección y localización de fallas en la red, los cuales son descriptos en las secciones que se siguen.

1.4.1 Algoritmos para la detección de fallas en la red

Los algoritmos para la detección de fallas están divididos en dos categorías que son los basados en la signatura de la anomalía y los basados en el comportamiento normal de la red [21].

Para los algoritmos basados en la signatura de la anomalía se conocen las características de los síntomas relativos a las fallas y se crean perfiles de estos, los datos reales obtenidos de la red son comparados a estos perfiles a ver se corresponden, de entre ellos podemos mencionar los siguientes abordajes:

- En [18], se presentó un algoritmo de detección de fallas basado en la signatura de la anomalía, donde se crea el llamado arreglo de falla que presenta las anomalías relativas a cada falla, las fallas eran identificadas por correspondencia de los datos obtenidos de la red con las características contenidas en el arreglo, generando así una alarma.
- En los trabajos [35] [37] se usaran máquinas de estado finito [41] para la detección de fallas en la red, las máquinas de estado finito fueran diseñadas para cada falla específica, de la cual se tiene un completo conocimiento previo mediante los datos históricos. Los objetivos perseguidos con su implementación son muy amplios, ya que no solo se persigue la detección del comportamiento anómalo, sino la identificación y diagnóstico del problema que origina la falla, además de que reducen el número de falos alarmas.

La mayor dificultad para la implementación de algoritmos de detección basados en la signatura de anomalía es que se debe tener un conocimiento previo sobre las fallas para posterior modelación, lo que no siempre es posible debido a la propia complexidad de los entornos de red, además de que nuevas fallas pueden pasar sin ser detectada.

En los algoritmos basados en el comportamiento normal de la red, el perfil que se crea no es el de la falla, pero si el del comportamiento que se admite normal para la red y los desvíos de este perfil representan las anomalías, o sea los síntomas asociados a la ocurrencia de una falla de entre ellos podemos mencionar los siguientes abordajes:

- La signatura digital del segmento de red (DSNS, por sus siglas en ingles), desarrollado por [49], se crea el perfil normal de operación de la red por medio de la llamada signatura digital del segmento de red para un grupo de variables

MIB, el trafico real de la red es comparado al perfil creado y son considerados síntomas o anomalías asociadas a fallas los desvíos de este perfil.

- Para Tottan y Ji [19] [20] en el **algoritmo de detección de cambio**, la elaboración del perfil de comportamiento normal de la red puede ser hecha mediante métodos estadísticos [50] [51], en el que una anomalía es la observación de cambios bruscos en los valores las variables MIB a lo largo del tiempo, para tal las series temporales de estas variables son modeladas a través de un proceso auto regresivo (AR, por sus siglas en inglés) y se aplica un teste de hipótesis basado en la razón verosimilitud generalizada (*GLR,* por sus siglas en inglés) entre ventanas de tiempo adyacentes para verificar se hay cambios bruscos entre las dos series.

Como una única falla en la red puede generar un conjunto de alarmas en cadena, de forma a localizar la raíz se utilizan algoritmos para localizar el elemento inicial en la cadena de alarmas.

1.4.2 Algoritmos para localización de fallas en la red

Los algoritmos de detección normalmente analizan los componentes de la red de forma individual y generan alarmas. En una red de computadoras gran, una única falla puede generar varias alarmas, lo que frecuentemente dificulta el aislamiento de causa primaria de la falla [39]. Esto se debe al hecho de que hay una relación entre los componentes de la red y los síntomas o anomalías inherentes a una falla en uno de ellos se pueden propagar a los demás componentes generando varias alarmas.

Una vez que se hayan detectado las anomalías en los componentes, más dos fase precisan ser concluidas para la localización de la falla, respectivamente la fase de elaboración panorámica del problema donde se hace la correlación de las alarmas generadas y la fase de teste donde hay la confirmación de la origen del problema como resultado de la verificación de los datos obtenidos de la elaboración panorámica [52].

De este modo, se debe elegir una técnica que permita la localización o aislamiento de la causa raíz de la falla, por ejemplo:

- Los sistemas basados en reglas [43], pueden ser utilizados para el proceso de localización de fallas, en estos se hace la modelación de un conjunto de reglas relacionadas as fallas y que son almacenadas en una base de datos, estas reglas representan el conocimiento de un sistema experto que simula el comportamiento humano.

- Otros algoritmos son desarrollados considerando la estructura de la red, en que la correlación de alarmas es hecha en función de las relaciones entre los componentes de la red, aquí se pueden usar grafos [42] para modelar la relación entre ello.
- La teoría de los grafos es muy útil en el análisis de propagación de anomalías inherentes a fallas, se pueden utilizar grafos para modelar la propagación y gramáticas libres de contextos, técnicas de *codebook* y algoritmos divide y vencerás para analizar estos modelos.

En el **modelo de detección de anomalías en redes de computadoras** propuesto por Zarpelão [21], la estructura de la red es representada por medio de un grafo $G = (V, E)$, donde cada vértice V representa uno de los dispositivos en la red y los bordes E representan los enlaces entre estos dispositivos. Posteriormente se hace la correlación de las alarmas para permitir la visualización de la propagación de los síntomas sobre la red. En este modelo no está prevista la fuente de datos sobre la topología de la red, el autor de esta investigación plantea que si se concibe una CMDB como fuente de datos sobre la topología de la red, además de la obtención del dispositivo raíz de los síntomas que se propagan sobre la red, es posible el conocimiento de las características del mismo y su localización física.

Los sistemas basados en reglas presentan la desventaja en la adaptación a nuevos problemas que no hacen parte de la base de datos, lo que requiere el incremento constante de reglas lo que dificulta en la manutención. Los grafos que representan las relaciones de dependencia entre los componentes de la red y que permiten la modelación de la propagación, pueden ser adicionados en la base de conocimiento para mejorar la capacidad en el diagnóstico y conferir la capacidad de adaptación a nuevos problemas. Otra situación difícil es que la definición de un modelo propagación de anomalías no es sencilla y se pueden ignorar anomalías no previstas en el momento de la modelaje.

El conjunto de técnicas presentadas contribuyen a la detección y localización de fallas en la red, algunos de los sistemas tradicionales para la gestión de redes emplean estas técnicas o similares para lograr el mismo objetivo.

1.5 Soluciones existentes para la gestión de redes

Por la complejidad que son los entornos IT y las necesidades específicas de cada organización en la gestión de red para la operación y entrega de servicios de calidad, hasta el momento han sido desarrollados una gran variedad de sistemas de gestión de red, que brindan las funcionalidades de una CMDB dedicada, que facilitan en el

monitoreo de servidores y servicios, de los parámetros de QoS y de rendimiento físico de los equipos, permitiendo la detección y aislamiento de fallas en la red.

Dedicadas al soporte de la gestión de configuraciones de los activos de IT de una organización, son descriptas las CMDB que se siguen:

- HP universal CMDB es una base de datos de gestión de configuraciones de distribución comercial, desarrollada por la empresa Hewlett-Packard (HP, siglas en inglés), que almacena, controla y gestiona los componentes de software e infraestructuras, así como sus relaciones y dependencias asociadas. Proporciona una visibilidad de las infraestructuras que muestra cómo los componentes están relacionados para una prestación de servicios de negocio y de TI constante y de confianza. La visibilidad mejora y simplifica el control de cambios para evitar interrupciones del servicio y facilita el seguimiento, la gestión y el control de las infraestructuras de TI. HP UCMDB reduce el tiempo de las reparaciones de forma eficiente [53].
- ITOP es una CMDB de código abierto que permite la gestión del inventario, gestión de incidencias, gestión del cambio en el entorno IT, gestión del servicio [54].
- La CMDB de ServiceDesk Plus desarrollado por el grupo ManageEngine Lleve un registro y administre sus CI con un solo repositorio centralizado. Está diseñado para obtener más visibilidad de sus activos mediante el conocimiento de las interrelaciones y dependencia de cada CI [55].

En función de los objetivos que se persiguen se pude elegir de entre las CMDB presentadas o pensarse en el desarrollo de una de raíz. Estas sirven como la base para el proceso de gestión de configuraciones, pero los entornos IT como las redes de computadoras son dinámicos, donde hay un gran flujo de datos y requieren de otras soluciones que hacen el constante monitoreo del ambiente, tarea esta que es desempeñada por herramientas como:

- El Zenoss core [16] es la versión de código abierto y de distribución libre de Zenoss, por medio de una consola basada en web permite la gestión de la infraestructura IT, hace el monitoreo la red, servidores, y hasta aplicaciones. El sistema posee una CMDB para el registro de los recursos que se quiere gestionar, los datos de monitoreo son recogidos por SNMP, SSH o *Windows managment instrumentation* (WMI) permitiendo medir la disponibilidad, perdidas de paquetes y tiempo de respuestas. Los síntomas asociados a fallas son

detectadas con la emisión de alarmas que representan el sobrepaso de umbrales establecidos para los parámetros de QoS y de rendimiento físico de los equipos en la red por mensajes de registro de sistema (*syslog*) y capturas SNMP (*SNMP traps*), resultando en el envío de notificaciones a los administradores sobre un nuevo evento activo [16].

- El PRTG [14] es una herramienta para el monitoreo de la red desarrollada por la Paessler, la cual recomienda que para su correcto funcionamiento debe ser instalado en un ambiente con sistema operativo Windows. Se puede usar para el monitoreo de servidores y servicios de red (HTTP, SMTP, POP3 y FTP), el ancho de banda en cada puerto de un enrutador o switches, disponibilidad de la red, uso de CPU y carga de memoria en los equipos. Para la recogida de estos datos, el PRTG está soportado por los protocolos SNMP, WMI, *packet sniffer*, *Netflow*, *sFlow* y *jFlow*. Para cada parámetro que se quiere monitorear el PRTG tiene un sensor asociado, por defecto el sistema define umbrales para algunos de estos parámetros, representando estado del sensor el correcto funcionamiento o la presencia de anomalías dentro de la red, lo cual depende del valor del parámetro. En el caso de una anomalía es disparada una alarma en el sensor, la cual pose características que permiten saber si se trata de una falla blanda o dura. Además, el PRTG hace un análisis estadístico de los datos de monitoreo basados en la hora del día y día de la semana, generando alarmas cuando hay comportamientos anormales en los datos actuales.

- El Nagios core es la versión de código abierto y de libre distribución de Nagios [56], está escrito en C, lo que garantiza una rápida ejecución, permite la adición de plugins escritos en diferentes lenguajes, esos plugins son los sensores de Nagios que generan datos interpretados por él para visualización y elaboración de notificaciones [15]. Nagios core es apropiada para la monitorización de servicios de red y recursos de un host (carga del procesador, uso de los discos y trazas del sistema) en varios sistemas operativos, haciendo el recurso del plugin NRPE_NT o el protocolo SNMP para ambientes Windows, se pode hacer el monitoreo remoto por SSL o SSH, reportes y estadísticas del estado de disponibilidad de servicios y host [56]. El sistema puede ser configurado a fin de establecer umbrales que permiten determinar cuando el valor resultante de un chequeo corresponde a una anomalía generando alarmas en el caso que sea positivo, se crea un evento y notificaciones pueden ser enviadas a los administradores informando dichos cambios [15].

- El WhatsUp Gold es una herramienta para el monitoreo de red y aplicaciones, fue desarrollada pela compañía IP SWITCH. El sistema posee un proceso de descubierta basado en roles que busca por los dispositivos en la red, determina sus tipos de acuerdo con los atributos. Después de esto el dispositivo puede ser almacenado en la base de datos, siendo presentado en la lista de dispositivos o en mapas gráficos. Él es instalado con cinco monitores de rendimiento que monitorean tipos de datos específicos de los dispositivos de la red: utilización de CPU, utilización de Disco, utilización de ancho de Banda, utilización de Memoria, latencia y disponibilidad vía Ping [57]. El sistema realiza el monitoreo activo para saber del status de los dispositivos, con lo cual se puede checar los servicios en el dispositivo y una escucha pasiva para mensajes de registro del sistema y capturas SNMP. Cuando el contenido resultante tanto del monitoreo corresponde a una situación anormal, el sistema puede generar alertas notificando los cambios observados. Basado en la dependencia existente entre los dispositivos, el sistema hace la de alertas, evitando la sobrecarga del sistema por redundancia de chequeos.
- El OpManager es una herramienta multiplataforma que sirve para el monitoreo de red, probé a los administradores de red una plataforma integrada para gestionar enrutadores, cortafuego, servidores, switches e impresoras. Hace el monitoreo de servidores y servicios de red, tales como HTTP, FTP, SMTP, DNS, LDAP, mide la disponibilidad de aplicaciones como Oracle, MySql y otras. Además mide el rendimiento del hardware y software de la red, tales como el ancho de banda, la utilización de la memoria, disco y CPU, los tiempos de repuesta por la recoja periódica de datos [58]. El OpManager probé mecanismos para la gestión de fallas basados en el establecimiento de umbrales para los parámetros monitoreados. Los datos son recogidos mediante ICMP, capturas SNMP y mensajes de registro del sistema, son procesados, en los casos que se verifica algún desvío del comportamiento esperado se crea un evento y como consecuencia son generadas alarmas [58]. Otra característica importante en el OpManager es el tratamiento para la de-duplicación, la correlación de eventos y la automatización.
- Cacti es una herramienta publicada bajo la licencia GPL4 (GNU Public License). Pone a disposición un soporte gratuito mantenido por la comunidad mediante una lista de correos y un foro. La recolección de datos se realiza mediante el protocolo SNMP y se almacenan los resultados en una base de datos [17]. Los parámetros el caudal y la pérdida de paquetes son obtenidos mediante el protocolo SNMP, y la disponibilidad a través de requisiciones ICMP. Muestra

gráficamente el estado de cada uno de los equipos, mediante el uso avanzado de gráficas [17].

Los sistemas presentados están próvidas de funcionalidades indispensables para la gestión de redes y de fallas en particular, por otro lado los administradores de red necesitan de soluciones complementarias o alternativas por lo siguiente:

- Sistemas como la HP universal CMDB, la CMDB de ServiceDesk, el PRTG, el WhatsUp Gold, OpManager son de distribución comercial, lo que requiere de constantes actualizaciones de licencias, además no permiten a los administradores la implementación de nuevas funcionalidades.
- El Nagios, el PRTG, el OpManager y el Zenoss permiten el monitoreo de servidores y servicios de red, emitiendo alarmas cuando hay alguna falla, en algunos casos las fallas en lo servidores y servicios son consecuencia de otras condiciones en la red como lo es el uso indebido de la red por parte de los usuarios.
- El Cacti, el PRTG, el OpManager, el Zenoss y el WhatsUp Gold hacen con que sea posible el monitoreo de los parámetros de QoS y de rendimiento físico de los equipos para la emisión de alarmas cuando hay el sobrepaso de los umbrales definidos, sin embargo en algunos casos se torna necesario la aplicación la aplicación de otros enfoques para la detección de los síntomas que preceden a las fallas.

Es responsabilidad de los administradores de red elegir los sistemas teniendo en cuenta el tipo de licencia y los recursos financieros disponibles y la flexibilidad en cuanto a su extensibilidad, considerar la aplicación de soluciones complementarias como los abordajes utilizados por Tottan [20], Zarpelão [21], y Feather [18] en la detección y localización de anomalías relacionadas a posibles fallas, una vez que los sistemas presentados y sus similares normalmente hacen el monitoreo de servidores y servicios, de los parámetros de QoS y de rendimiento físico de los equipos, no permitiendo la detección anticipada de fallas con síntomas fuera de este contexto.

Conclusiones del capítulo

El estándar ITIL plantea la gestión de configuraciones como el proceso nuclear para la gestión de tecnología de información. Este proceso es soportado por una base de datos de gestión de configuración, la cual es un depósito de información en el que no sólo se almacenan datos sobre los activos de una infraestructura de tecnología de información sino que, además, se definen y establecen las relaciones entre ellos.

La gestión de redes es una de las funciones técnicas para la operación y entrega de servicios de calidad en entornos de tecnología de información, por eso se torna imprescindible tener una base de datos de gestión de configuraciones que soporte la función de gestión de configuraciones en la red que permita el conocimiento de la infraestructura. De este modo, las otras funciones de gestión de redes descriptas por el modelo OSI de gestión de redes pueden ser realizadas teniendo en cuenta la información brindada por la base de datos de gestión de configuración.

La gestión de configuración provee a la gestión de rendimiento y de fallas informaciones relevantes asociadas a los equipos que se deben monitorear. Dichas funciones son realizadas por herramientas que hacen el monitoreo de servidores y servicios de red, de los parámetros de QoS y rendimiento físico para detectar posible fallas. Otros abordajes, implementan algoritmos que consideran el análisis de las variables MIB de cada equipo en la red para la detención temprana de las fallas.

Estos algoritmos permiten detectar los síntomas o anomalías relacionadas a posibles fallas antes que causen la degradación o interrupción de los servicios en la red y pueden ser aplicadas como una solución complementaria a las herramientas de gestión de redes que se utilizan en el campus de la UAN para prevenir efectivamente la degradación de los servicios telemáticos brindados a los usuarios de la red. Si se consideran las anomalías detectadas es posible la aplicación de medidas de control teniendo en cuenta a las misma, de esto se encarga la gestión de redes basada en políticas, la definición de un conjunto de directivas o reglas especificadas por el operador para gestionar ciertos aspectos, que permiten obtener los resultados deseados en el comportamiento de la red entre usuarios y aplicaciones.

Capítulo 2 – Sistema de detección y aislamiento de fallas en la red del campus de la universidad agostinho neto

Los temas relacionados a la gestión de red descriptos en el capítulo anterior sirvieron de base para la obtención del diagnóstico actual sobre la gestión de red en el campus universitario de la universidad Agostinho Neto, que tuvo implicación en la modelación de la arquitectura propuesta para el sistema de detección y aislamiento de fallas en la red, tanto el diagnóstico como la arquitectura son descriptos en la secciones que se siguen.

2.1 Diagnóstico actual en la UAN

En esta sección se presenta el resultado de un proceso analítico realizado sobre la gestión de red en el campus universitario de la universidad Agostinho Neto, que permitió saber cómo es realizado el proceso, las herramientas de gestión de red que lo auxilian y las insuficiencias existentes. Para el efecto, las herramientas utilizadas fueron la encuesta y la entrevista, que fueran aplicadas a cuatro técnicos responsables por la gestión de redes del campus de la UAN, de los cuales dos son ingenieros informáticos y suman un total tres años de experiencia con la red desde la apertura del campus en 2012.

Inicialmente, la encuesta fue utilizada para saber cómo es el proceso de según la perspectiva individual de los técnicos. La entrevista fue realizada de acuerdo a las respuestas obtenidas en la encuesta, enfocándose en las ventajas y desventajas observadas en la gestión de red en el campus de la UAN.

De la encuesta se pudo arrojar que se utiliza la herramienta Nagios para el monitoreo de servidores y servicios de red y la herramienta Cacti para medir el tráfico en los switches. Estas dos herramientas son de gran utilidad para la gestión de la red una vez que el Nagios permite saber cuándo los servidores y servicios están funcionando correctamente o no, el Cacti presenta los gráficos que ayudan en el análisis de tendencia en la red.

La utilización de las dos herramientas es de gran utilidad para la gestión de red, además de esto, es necesaria una solución que provea el control de los activos de la red, el conocimiento de la estructura de la red y los cambios efectuados sobre la misma, que sea proactiva en la detección y aislamiento de fallas en la red, la cual permita visualizar la propagación de anomalías en la red y en base a esto la aplicación de medidas de control ante mismo que el Nagios emita alarmas para fallas en los servidores o servicios.

La utilización de una base de datos de gestión de configuraciones hace que sea posible mantener el control de los activos de la red, conocer la estructura de la red. Un análisis estadístico sobre las variables MIB que están asociadas al transporte de datos en la red permite detectar anomalías que tienen implicación en el rendimiento de la red y que puedan afectar el comportamiento de servidores y servicios. Si se considera la PBNM es posible crear políticas para evitar que las anomalías causen la interrupción de los servicios de la red.

Por lo planteado se propone una solución que integre las funcionalidades de una base de datos de gestión de configuraciones, algoritmos para la detección de anomalías y la visualización de su propagación sobre la red y las funcionalidades relativas a la gestión de red basada en políticas. Una solución con dichas característica previne efectivamente la degradación de los servicios telemáticos brindados a los usuarios de la red del campus de la UAN, la cual es descripta en la sección que sigue.

2.2 Arquitectura del sistema de detección y aislamiento de fallas en la red

Un sistema es un conjunto de elementos, relacionados entre sí que contribuyen para alcanzar un fin. El sistema de detección y aislamiento de fallas en la red debe permitir mantener el control de los activos de la red y conocimiento de la estructura de la red, la detección de anomalías que tienen implicación en el rendimiento de la red y su propagación sobre la misma red, y la creación de políticas para evitar que las anomalías causen la interrupción de los servicios de la red.

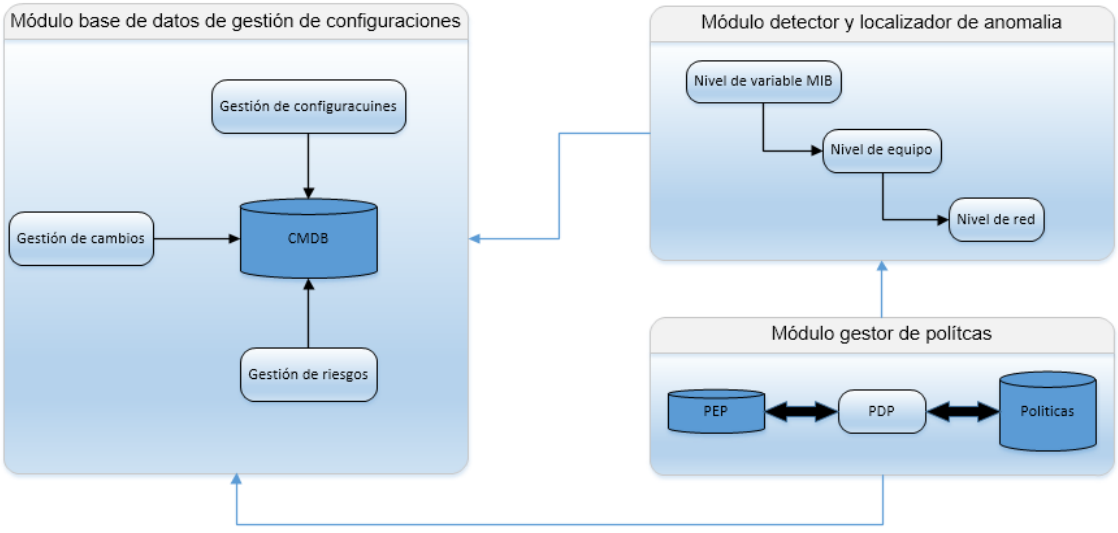

Figura 2.1 - Arquitectura del sistema

Para lograr su objetivo, conforme ilustra la Figura 2.1, el sistema tiene como elementos los módulos:

- Base de datos de gestión de configuraciones, encargada de mantener el control de los activos de la red, conocer la estructura de la red.
- Detector y localizador de anomalías, responsable por la detección de anomalías que tienen implicación en el rendimiento de la red, localizar la raíz y permitir visualizar su propagación sobre la red.
- Gestor de políticas, responsable de permitir la creación de políticas para evitar que las anomalías causen la interrupción de los servicios de la red.

Estos módulos están organizados de tal forma que la comunicación entre ellos permita la detección y aislamiento de posibles fallas en la red.

2.2.1 Módulo base de datos de gestión de configuraciones

El módulo base de datos de gestión de configuraciones es el elemento base del sistema, sobre su estructura operan los demás módulos. La inclusión del módulo CMDB en el sistema tiene como finalidad resolver el aspecto relacionado a la inexistencia de un control de inventario (hardware y software), facilitando la localización física de equipos y servicios como parte del proceso de gestión de red en el campus universitario de la UAN.

No siendo suficiente tener una lista de los activos de la red, el control inventario se extiende hasta el mantenimiento del registro actualizado de todos los activos y sus características, las interrelaciones entre ellos, los riesgos asociados a cada uno de ellos, los cambios efectuados en la red y la representación de la topología.

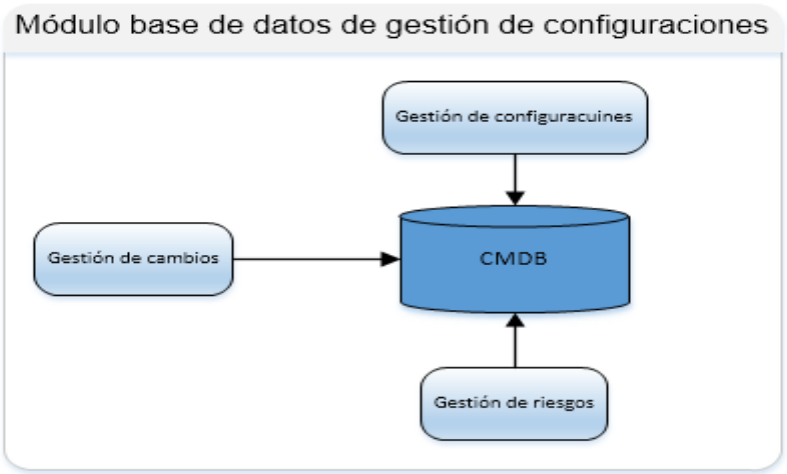

Figura 2.2 – Grupos de funcionalidades del módulo base de datos de gestión de la configuración

A tal efecto, el módulo CMDB provee funcionalidades de los procesos gestión de configuraciones, de cambios y de riesgos para la gestión de la configuración en IT descritos en la sección 1.1 del Capítulo 1 conforme ilustra la Figura 2.2. Cumpliendo estas funcionalidades, el módulo CMDB debe permitir verificar el cumplimiento de las políticas para llevar a cabo los controles de activos de la red en el campus universitario de la UAN. Sobre los activos controlados por este módulo operan los módulos detector y localizador de anomalías y el gestor de políticas.

2.2.2 Módulo detector y localizador de anomalías

El módulo detector y localizador de anomalías es responsable de detectar los síntomas asociados a la ocurrencia de posibles fallas en la red. Es incluido en el sistema para proveer un enfoque de análisis distinto de la evaluación de los parámetros de QoS y rendimiento físico de los equipos en la detección de los síntomas, además de esto permitir visualizar la propagación de los síntomas sobre la red lo que implica la detección temprana de la falla y localización de la raíz.

Para cumplir con su propósito, en el módulo detector y localizador de anomalías se hace un análisis en tres niveles, respectivamente a nivel de variable MIB, a nivel de equipo y a nivel de la topología de red.

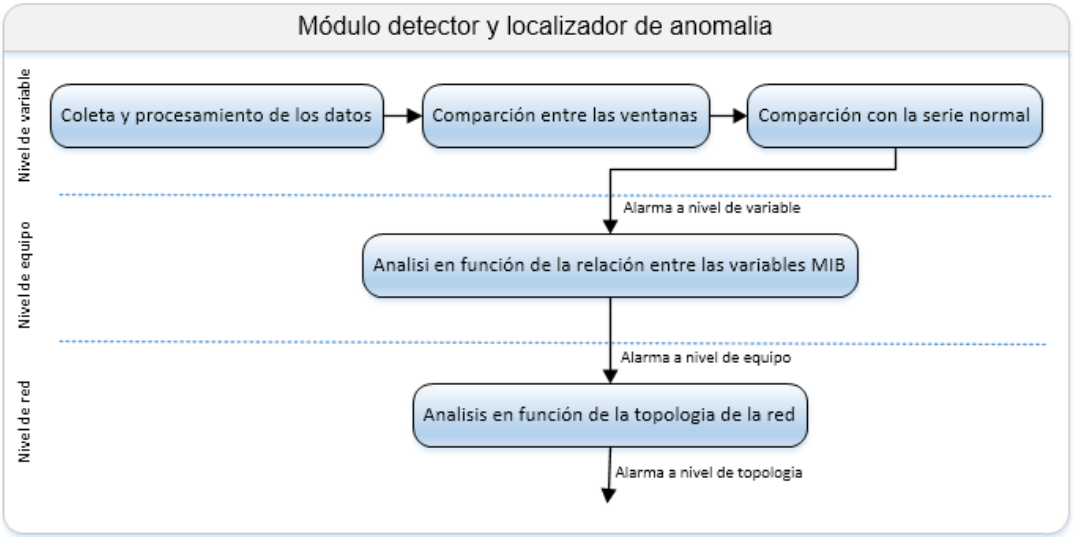

Figura 2.3 – Niveles de análisis y flujo de información en el Módulo detector y localizador de anomalías

Se verifica en la Figura 2.2, los diferentes niveles de análisis para este módulo y las tares en cada uno de ellos, el análisis a nivel de variable MIB es realizado mediante la implementación del **algoritmo de detección de cambios** propuesto por Tottan y en los

restantes niveles de análisis es implementado el **modelo de detección de anomalías en redes de computadoras** desarrollado por Zarpelão.

A. Análisis a nivel de variable MIB

El análisis a nivel de variable MIB es realizada en dos etapas, en la primera etapa se hace la recopilación y procesamiento de los datos y en la segunda etapa se verifica si existen o no anomalías. La primera etapa consiste en la observación periódica de 15 segundos de los valores de las variables MIB. Estos valores son cambiantes en el tiempo y forman series temporales no estacionarias. Estas series temporales son divididas en segmentos estacionarios, estos seguimientos estacionarios son modelados utilizando un proceso auto regresivo (AR, por sus siglas en ingles).

En una observación temporal para una variable MIB, se consideran dos ventanas de tiempo adyacentes $R(t)$ y S(t) de tamaños $N_R = N_s = 10$ según la Figura 2.3. Consideremos:

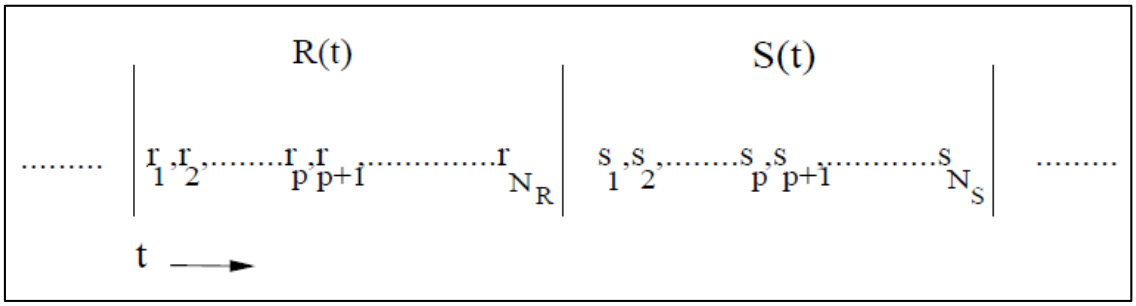

Figura 2.4 - Ventanas de tiempo adyacentes

$$R(t) = \{r_1(t), r_2(t), \dots, r_N(t)\} \quad (1)$$

Se expresa $r_i(t)$ como $\tilde{r}_i(t)$, donde $\tilde{r}_i(t) = r_i(t) - \mu$ y μ es la media del seguimiento $R(t)$. Ahora $\tilde{r}_i(t)$ es modelado como un proceso AR de orden p $(p = 1)$ con error residual $\in_i$.

$$\in_i (t) = \sum_{k=0}^{p} \propto_k \tilde{r}_i(t-k) \quad (2)$$

Donde $\propto_R = \{\propto_1, \propto_2, \dots, \propto_p\}$ son los parámetros $\in_i (t)$ es el ruido blanco. De la ecuación (2), y asumiendo que cada muestra del error residual $\in_i (t)$ as igual para una distribución $N(0, \sigma_R^2)$, la probabilidad conjunta del residuo de la serie temporal es:

$$p\left(\in_{p+1}, \dots, \in_{N_R} \mid \propto_1, \dots, \propto_p\right) = (1/\sqrt{2\pi}\sigma_R^2)^{N_R} \exp\left(-N'_R\, \sigma_R^2/2\hat{\sigma}_R^2\right), \quad (3)$$

Donde σ_R^2 es la varianza del residuo en el segmento $R(t)$, y $N'_R = N_R - p$ y $\hat{\sigma}_R^2$ es la covarianza estimada para σ_R^2. Aplicando los mismos procedimientos en el segmento

$S(t)$ obtenemos una expresión similar. Por lo tanto la probabilidad conjunta l para el error residual en los segmentos $R(t)$ y $S(t)$ es dado por:

$$l = (1/\sqrt{2\pi}\sigma_R^2)^{N_R}(1/\sqrt{2\pi}\sigma_S^2)^{N_S} \exp(-N'_R\,\sigma_R^2/2\hat{\sigma}_R^2)\ \exp(-N'_S\,\sigma_S^2/2\hat{\sigma}_S^2), \quad (4)$$

Donde σ_S^2 es la varianza del residuo en el segmento $S(t)$, y $N'_S = N_S - p$ y $\hat{\sigma}_S^2$ es la covarianza estimada para σ_S^2. Una vez obtenida la expresión de l que es estadísticamente suficiente, se pasa a la segunda etapa de análisis.

En la segunda etapa de análisis se verifica si hay cambios en el comportamiento de la serie temporal de la variable MIB, para tal se utiliza la expresión l que es estadísticamente suficiente, aplicándole un test de hipótesis binaria.

Las hipótesis son H_0 implicando que no hubo cambios entre los dos seguimientos en H_1 significa la ocurrencia de cambios. Sobre la hipótesis H_0 se tiene:

$$\propto_R = \propto_S \quad (5)$$

$$\sigma_R^2 = \sigma_S^2 = \sigma_P^2. \quad (6)$$

Sobre la hipótesis H_1 se tiene:

$$\propto_R \neq \propto_S \quad (7)$$

$$\sigma_R^2 \neq \sigma_S^2. \quad (8)$$

De las condiciones en las ecuaciones (6) y (8) se tiene razón de verosimilitud como:

$$\lambda = {\sigma_P}^{-(N'_R+N'_S)}{\sigma_R}^{N'_R}{\sigma_S}^{N'_S} \exp\left(-\frac{\hat{\sigma}_p^2(N'_R+N'_S)}{2\sigma_S^2} + \frac{1}{2}\left[\frac{N'_R\hat{\sigma}_R^2}{\sigma_R^2} + \frac{N'_S\hat{\sigma}_S^2}{\sigma_S^2}\right]\right) \quad (9)$$

Con la utilización del estimador de máxima verosimilitud con respecto a las varianzas, se tiene el logaritmo de la razón de verosimilitud como:

$$-\ln\lambda = N'_R\left(\ln\hat{\sigma}_p^2 - \ln\hat{\sigma}_R^2\right) + N'_S(\ln\hat{\sigma}_p^2 - \ln\hat{\sigma}_S^2) \quad (10)$$

El log de la razón de verosimilitud $\ln\lambda$ es comparado a un parámetro h elegido por optimización, este parámetro es el que permite determinar el punto de cambio, siendo así se tiene:

$$-\ln\lambda > h \rightarrow H_1 \quad (11)$$

$$-\ln\lambda \leq h \rightarrow H_0 \quad (12)$$

En el caso de que se verifica el cambio, se emplea una nuevo test de hipótesis para determinar si el cambio corresponde a una situación anormal. En este segundo test de

hipótesis la media μ_p y la varianza σ_P del seguimiento combinado ($R(t)$ y S(t)) es comparado con la media μ_0 y la varianza σ_0 normal usando el test de razón de verosimilitud y un nuevo parámetro η. La media μ_0 y la varianza σ_0 pertenecen a una seria temporal que corresponde a un periodo de observación de la variable MIB en cuestión que se tiene como normal para el funcionamiento de la red.

Las hipótesis consideradas H_0 con una distribución $N(\mu_0, \sigma_0)$ implicando un cambio normal y H_1 con una distribución $N(\mu_p, \sigma_p)$ implicando que ha ocurrido un cambio anormal, y en este caso es generada una alarma a nivel de variable MIB. Los parámetros h y η definen el nivel de sensibilidad para la generación de alarma. La alarma generada es relativa a una sola variable, lo que corresponde a apenas una de las capas del modelo OSI, se torna necesario verificar las otras capas

B. Análisis a nivel de equipo

Realizada el análisis en el nivel de variable se hace el análisis a nivel de dispositivo. El objetivo de este tipo de análisis es determinar si las alarmas generadas a nivel de variable MIB corresponden a una anomalía o no, para tal fin, las alarmas son correlacionas en función de la relación entre las variables MIB en el transporte de datos.

Para la obtención de la relación entre las variables MIB se utilizó la herramienta diagrama case, la cual presenta el posicionamiento de las variables en el flujo de datos entre las diferentes capas del modelo OSI.

Se obtuvieron dos conjuntos que representan la relación entre las variables MIB asociadas al transporte de datos en los niveles de enlace, red y transporte, respectivamente los grupos *interface, ip, tcp* y *udp* de una MIB.

Forman parte del primer conjunto, el conjunto de entrada de datos en el dispositivo las variables:

- *IfInOctets,*
- *IpInReceiveds,*
- *tcpInSegs,*

Del segundo conjunto que representa la salida de datos del dispositivo forman parte las variables:

- *IfOutOctets,*
- *IpOutRequest,*
- *TcpOut*,

Se utiliza un grafo direccionado $G = (V, E)$ para representar la relación entre las variables MIB en cada uno de los conjuntos, donde cada vértice V representa la variable MIB analizada y los bordes E representan la relación entre las mismas. Cada borde en este grafo es representado por el par ordenado (x, y). El sentido de los bordes representa el sentido en que una anomalía se puede propagar dentro de cada conjunto, y de acuerdo al tipo de equipo para cada conjunto de variable existe un conjunto de variables definidas como iniciales y otras como finales.

Teniendo en cuenta el sentido de propagación de una anomalía en cada uno de los conjuntos, la correlación entre las alarmas a nivel de variable MIB es realizada de la siguiente forma:

- Cuando es generada una alarma para una de las variables del conjunto, se busca verificar si existen alarmas para las demás variables del conjunto;
- Si se comprueba la existencia de alarmas para todas las variables del mismo conjunto, significa que hay una anomalía que se propaga sobre este conjunto;
- En el caso de que se haya identificado la ocurrencia de la anomalía para determinado conjunto, es generada una alarma a nivel de dispositivo para el respectivo conjunto;

```
    Programa principal
1.  Inicio
2.      Para cada v ∈ (V_i ∩ V_a) haga
3.          BusquedaProfundidad(v)
4.  Fin Programa
    Procedimiento BusquedaProfundidad(v)
5.  Inicio
6.      Marcar v como visitado
7.      Empilar v en P
8.      Si (v ∈ V_f) entonces
9.          Anomalía detectada;
10.     Para cada (v' ∈ C(v)) haga
11.         Si v' no esta marcado entonces
12.             BusquedaProfundidad(v')
13.     Fin para
14.     Desenfilar P
15. Fin procedimiento
```

Figura 2.5 - Correlación de alarmas a nivel de variable MIB

El proceso de correlación es descripto por el algoritmo de búsqueda en profundidad de la Figura 2.5 en que se tiene como entradas las alarmas de nivel de variable MIB y como salida las alarmas a nivel de equipo. Donde V_i es el conjunto de variables definidas como iniciales, V_f es el conjunto de variables MIB definidas como finales, V_a conjunto de

variables con alarmas, P es la pila utilizada en la búsqueda en profundidad, $C(\mathrm{v})$ es la función que retorna todas las variables que son adyacentes v y que presentan alarmas. La presencia de alarmas en nivel de dispositivo, da lugar al análisis a nivel de topología de la red.

C. Análisis a nivel de topología de la red

El análisis a nivel de topología de la red, tiene como objetivo presentar el escenario de propagación de las anomalías sobre la red, para lo cual se considera el siguiente:

- De la CMDB se extrae la topología de la red, y se utilizan grafos para representar la misma.
- Cada dispositivo en la red es representado por un vértice del grafo y los enlaces entre ellos son los bordes.
- Partiendo del principio de que una anomalía puede tener inicio en uno de los dispositivos, o este dispositivo ser el destino, o el mismo ser apenas el punto de encaminamiento, mediante la estructura del grafo que representa la topología de la red es posible obtener una visualización de la propagación de una anomalía sobre vértices adyacentes.
- Se hace una correlación temporal de las alarmas de nivel de dispositivo, y de acuerdo a la topología de la red y se obtiene una representación de la propagación de la anomalía sobre la red.

Por lo planteado anteriormente, es posible identificar los síntomas o anomalías asociados a posibles fallas en la red mediante el análisis estadístico de las variables MIB y observar su propagación sobre la red.

Por el escenario de propagación de anomalías sobre la red, es posible que el administrador de red visualice sobre qué servicios impactarán esas anomalías y por su propia experiencia aplicar medidas de control. El módulo gestor de políticas permite a la automatización de estas medidas de control.

2.2.3 Módulo gestor de políticas

El módulo gestor de políticas se encarga de la automatización de las tareas de control, permite las definiciones de políticas teniendo en cuenta las alarmas a nivel de dispositivo y su propagación sobre los principales servicios de la red. La Figura 2.4 es referente al funcionamiento de este módulo.

Se comunica con el módulo de gestión de configuraciones solicitando información de los dispositivos que componen a la red, los cuales corresponden a los puntos de

ejecución de políticas. La aplicación de políticas sobre los PEP depende de las alarmas a nivel de topología de la red que provee el módulo detector y localizador de anomalías, las cuales reflejan el estado de los PEP.

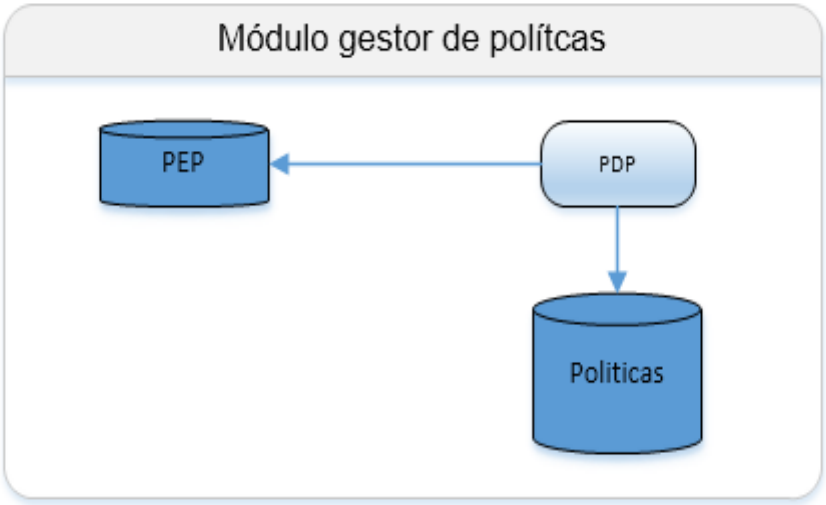

Figura 2.6 – Modulo Gestor de Políticas

2.3 Diseño e implementación del sistema de detección y aislamiento de fallas en la red

El desarrollo del sistema de detección y aislamiento de fallas en la red tuvo como guía la metodología de programación extrema, que consiste en las fases de:

- **exploración**, se describen las historias de usuarios (HU), en correspondencia con cada uno de los requisitos funcionales identificados.
- **planificación** se realiza la estimación del esfuerzo por cada HU, el plan de iteraciones y el plan de duración de cada iteración. Además, se identifican los patrones de diseño y de arquitectura a utilizar en la implementación del sistema, así como los estándares de codificación.

El primer paso consistió en la identificación de los actores del sistema y los requisitos funcionales para la especificación de las historias de usuario. En la Tabla 2-1 se describe los roles para los actores del sistema.

Posteriormente a la identificación de los actores para el sistema, se identificaran los requisitos funcionales y no funcionales para cada módulo del sistema (ver **Tabla de requisito** en los **Anexos**), en los que cada requisito funcional corresponde a una historia de usuario.

Tabla 2-1 Descripción de roles

Actores	Descripción de rol
Supervisor de la configuración	Encargado de proyectar, dirigir y controlar todo el proceso de gestión de la configuración.
Especialista de la configuración	Responsable de recopilar y analizar la información referente a los elementos de la configuración.
Administrador del sistema	Responsable de dar mantenimiento a la información requerida manejada por el sistema
Supervisor de la configuración	Encargado de proyectar, dirigir y controlar todo el proceso de gestión de la configuración.
Técnico de red	Encargado del monitoreo y control de los servicio telemáticos brindados por la red

Se adoptó la CMDB ITOP para realizar las funcionalidades referentes al módulo base de datos de gestión, debido a que la misma cumple con casi todos los requisitos funcionales para este módulo y, es de distribución libre y de código abierto, lo que permite su extensibilidad. Para su inclusión en el sistema se le agregaron las funcionalidades para mantener la información relacionada a la localización de los equipos en los diferentes edificios conforme al diseño de base de datos gestión de configuraciones elaborado.

En la fase de planificación se realizó la estimación del esfuerzo por cada HU, el plan de iteraciones y el plan de duración de cada iteración, y el patrón arquitectónico, lo cual expresa el esquema organizativo estructural para el sistema. En el sistema propuesto se hizo uso del patrón modelo vista controlador (MVC) que permitió realizar la programación multicapa, separando en tres componentes distintos los datos de la aplicación, la interfaz del usuario y la lógica de control.

Definidos los aspectos referidos anteriormente, se diseñó el modelo datos para los módulos detector y localizador de anomalías, y gestor de políticas conforme la Figura 1.1. Para la persistencia de estos datos se eligió el gestor de base de datos MySql, por el hecho de que en los requerimientos para los módulos detectores y localizador de anomalía y gestor de políticas implican que estos deben funcionar como servicios que

siguen ejecutándose, se eligió e el lenguaje de programación java para su implementación.

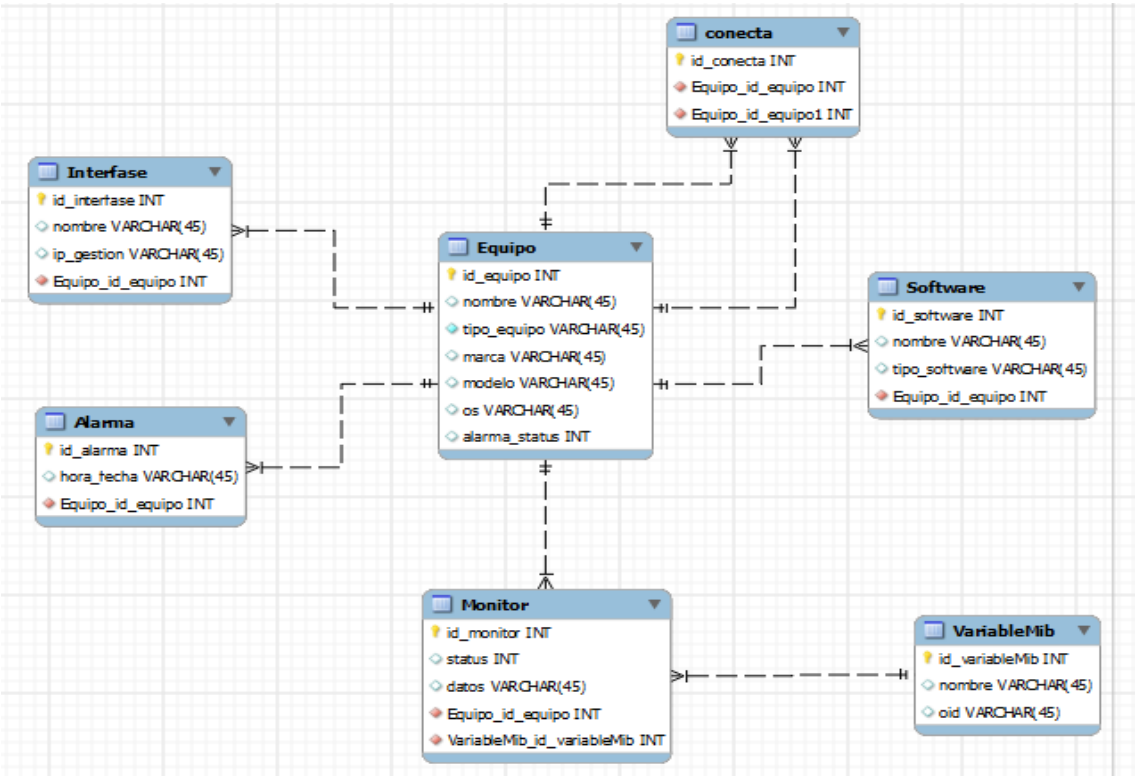

Figura 2.7 - Modelo de datos del módulo detector y localizador de anomalías y gestor de políticas

Conclusiones del capítulo

La encuesta aplicada a los técnicos de red de la UAN permitió arrojar informaciones sobre el proceso de gestión de red en el campus de la universidad Agostinho Neto. Teniendo en cuenta a la información obtenida se modeló la arquitectura del sistema para detección y aislamiento de fallas en la red compuesta por los módulos base de datos de gestión de configuraciones, detector y localizador de anomalías, y gestor de políticas para resolver las insuficiencias relacionadas a los estándares de gestión IT y proveer un mecanismo complementario para la detección proactiva de fallas en la red. Se definió la metodología XP para el desarrollo del sistema y el patrón arquitectónico MVC.

Capítulo 3 – Validación y pruebas de efectividad al sistema de detección y aislamiento de fallas en la red

El análisis de software desde el punto de vista de calidad, permite evaluar cómo se le da cumplimiento a los requisitos del sistema y verificar si fueron implementadas de forma correcta las HU definidas. A tal efecto, se ha realizado un conjunto de pruebas para validar la solución desarrollada. Luego se procede la prueba del sistema en un escenario de red simulado.

3.1 Pruebas unitarias y de aceptación

Finalizando la etapa de desarrollo del sistema quedan definidas el conjunto de pruebas a realizar en la fase final de validación de los resultados obtenidos durante el proceso de implementación del componente.

Uno de los pilares de la Programación Extrema (XP) es el proceso de pruebas. XP divide las pruebas del componente desarrollado en dos grupos: pruebas unitarias, encargadas de verificar el código y es diseñada por los programadores, y pruebas de aceptación o pruebas funcionales, destinadas a evaluar si al final de una iteración se consiguió la funcionalidad requerida diseñada por el cliente [59] .

La producción de código está dirigida por las pruebas unitarias. Las pruebas unitarias son establecidas antes de escribir el código y ejecutadas constantemente ante cada modificación del sistema. Los clientes escriben las pruebas funcionales para cada historia de usuario que deba validarse [59].

En el transcurso de implementación de cada historia de usuario perteneciente a una determinada iteración se realizaron, al código generado, una serie de pruebas para determinar su correcto funcionamiento. El método del camino básico permite obtener una medida de la complejidad de un diseño procedimental, y utilizar esta medida como guía para la definición de una serie de caminos básicos de ejecución, diseñando casos de prueba que garanticen que cada camino se ejecuta al menos una vez.

Para realizar estas pruebas se utiliza la complejidad ciclomática de McCabe [60], que consiste en la ejecución de un conjunto de caminos independientes proporcionando una medición cuantitativa de la complejidad lógica de un programa, así como determinar el número de casos de prueba que se deben realizar para asegurar que se ejecuta cada sentencia al menos una vez. La complejidad ciclomática consta de tres formas para calcularse:

$$V(G) = R \quad (1)$$

$$V(G) = A - N + 2 \quad (2)$$

$$V(G) = P + 1 \quad (3)$$

Donde R es número de regiones en del grafo, A es el número de arcos del grafo, N es el número de nodos y P es el número de nodos predicado. La Figura 3.1 es un ejemplo de la aplicación de la aplicación de la complejidad ciclomática de McCabe al método gentmonitores () de la clase EquipoControlo para determinar la cantidad de pruebas que deben ser hechas.

```
    private List<Monitor> getmonitores() {

        //  lista de monitores
        List<Monitor> listaMonitores, listaMonitoAuxiliar;

        listaMonitores = new ArrayList<>();

        EntityManagerFactory emf = Persistence.createEntityManagerFactory("DetectorAnomaliaPU");

        MonitorJpaController monitorJpaController = new MonitorJpaController(emf);

        listaMonitoAuxiliar = monitorJpaController.findMonitorEntities();

        if (listaMonitoAuxiliar != null) {

            for (Monitor listaMonitoAuxilia : listaMonitoAuxiliar) {

                if (listaMonitoAuxilia.getEquipoidequipo().equals(equipo)) {
                    listaMonitores.add(listaMonitoAuxilia);
                }

            }
            return listaMonitores;
        }

        return null;

    }

}
```

Figura 3.1 - Método generaAlarmaEquipo()

A continuación se muestran los pasos requeridos para realizar la prueba de camino básico al código anterior:

Paso 1: *Generar el grafo correspondiente al código del método (*Figura 3.2*).*

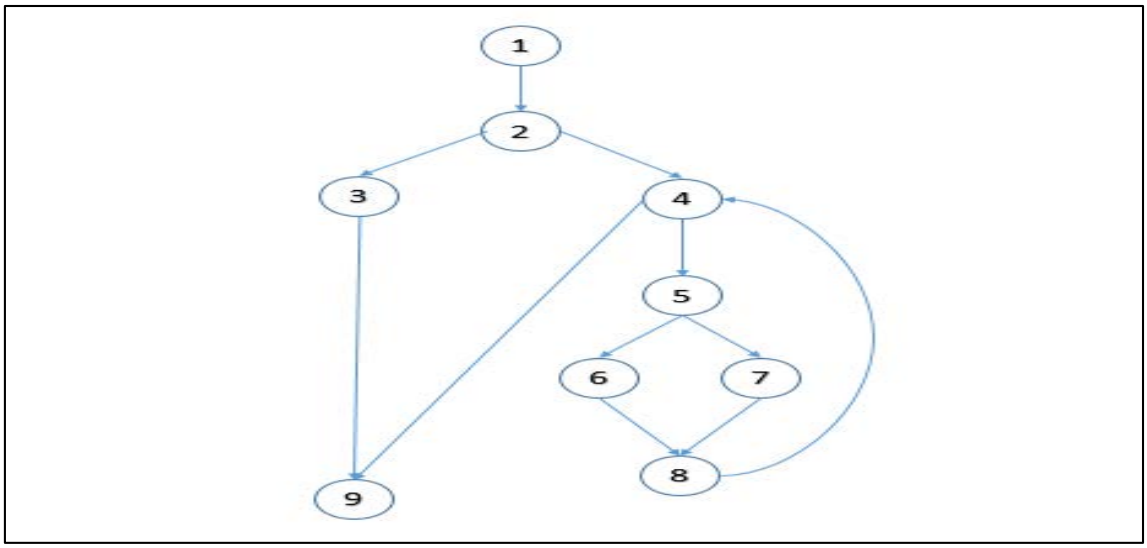

Figura 3.2 - Grafo del método generaAlarmaEquipo()

***Paso 2**: Se definen las áreas o regiones en que se divide el grafo generado (*Figura 3.3*).*

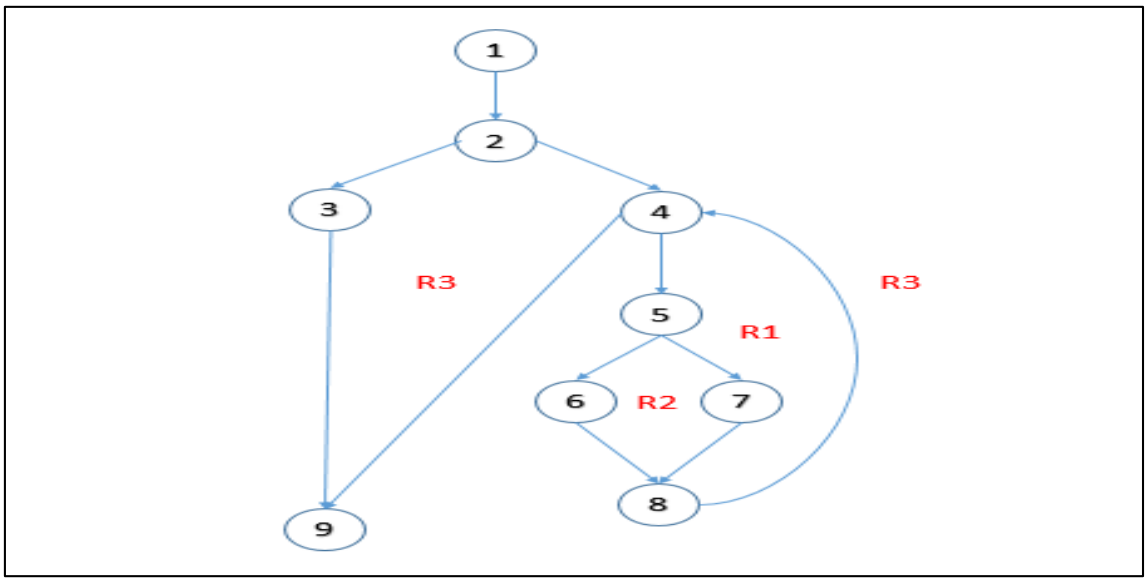

Figura 3.3 - Áreas divididas en el grafo

Paso 3: Se procede a calcular la complejidad ciclomática del método.

V (G) = 4

V (G) = 11 - 9 + 2 = 4

V (G) = 3 + 1 = 4

Una vez calculada la complejidad ciclomática del fragmento de código, se puede determinar el riesgo que supone utilizando la Tabla 2-1 [60].

Tabla 3-1 - Complejidad ciclomática evaluación del riesgo

Rango	*Descripción*
1 - 10	Programa simple, sin mucho riesgo.
11 - 20	Más complejo, riesgo moderado
21 - 50	Complejo, programa de alto riesgo
51 o mas	Programa no comprobable, muy alto riesgo

Utilizando la Tabla 3-1 se determina que existen 4 caminos linealmente independientes, lo cual determina que es un método simple y sin mucho riesgo. La complejidad ciclomática indica el número exacto de casos de prueba necesarios para probar cada punto de decisión en un programa. Por tanto, este método requiere de al menos 4 casos de prueba para probar correctamente su validez. Posteriormente se realizan las pruebas de aceptación.

Las pruebas de aceptación son pruebas de caja negra que se realizan a partir de las HU. Durante una iteración la HU seleccionada se convertirá en una prueba de aceptación [61]. Una HU puede tener todas las pruebas de aceptación que desee para asegurar su funcionamiento. El objetivo específico de esta prueba es garantizar que los requerimientos han sido cumplidos y que el sistema ha sido aceptable [62]. Como resultado de las pruebas de aceptación se obtendrán artefactos descritos en tablas llamadas caso de prueba de aceptación, la Tabla 3-1 es el ejemplo de un artefacto para prueba de aceptación.

Cada prueba de aceptación debe ser evaluada de acorde al resultado de la misma, esta evaluación tendrá uno de los tres resultados que a continuación se describen:

- **Bien,** cuando el resultado de la prueba es exactamente el esperado por el usuario.
- **Parcialmente bien,** cuando el resultado no es completamente el esperado por el cliente o usuario de la aplicación y muestra resultados erróneos o fuera de contexto.
- **Mal:** cuando el resultado de la prueba realizada genera un error de codificación en la aplicación o muestra como resultado elementos no deseados o fuera de contexto, trayendo como consecuencia que la funcionalidad requerida por el cliente no tenga resultado, lo que invalida también la HU.

Tabla 3-2 – Caso de prueba de aceptación para la HU número 62

Historia de usuario	
Código: HU62_62	**HU:** 62
Nombre: Visualizar las alarmas a nivel de equipo	
Usuario: Administrador de red, Técnico de red	
Condiciones de ejecución: para la visualización de alarmas a nivel de equipo es necesario que los monitores de todas las variables MIB de uno conjunto de los grupos reporten alarmas a nivel de variable	
Entrada/ pasos de ejecución : Cuando se verifica una alarma a nivel de variable MIB, se identifica el conjunto al cual pertenece esta variable, posteriormente se hace una correlación para verificar si las demás variables del conjunto también generaran alarmas, en el caso positivo se genera una alarma a nivel de equipo	
Resultado esperado: La confirmación de que existe o no una alarma a nivel de equipo	
Descripción: El sistema debe la visualización de las alarmas a nivel de equipo.	
Evaluación de la prueba: Bien	

Cada caso de prueba insatisfactorio genera una no conformidad, las cuales deben ser autos explicables y relacionados con el punto del sistema y deben ser tan concisas como sea posible. Las no conformidades fueron clasificadas según su complejidad de tres formas:

- Alta
- Media
- Baja

Las principales no conformidades encontradas estaban asociadas a la generación de alarmas a nivel de equipo y de topología de red, sobretodo en la sincronización y partilla de recursos por parte de los hilos responsables por generar las alarmas en cada nivel, además de esto se verificó también mensajes de errores asociadas a excepciones desconocidas. Con la corrección de los errores detectados en las pruebas, se pudo evidenciar que las mismas fueron satisfactorias. Se comprobó el cumplimento de las funcionalidades descritas en las HU, conforme ilustra la Figura 3.4 con las no conformidades encontradas en cada iteración de pruebas, clasificadas por los tipos definidos.

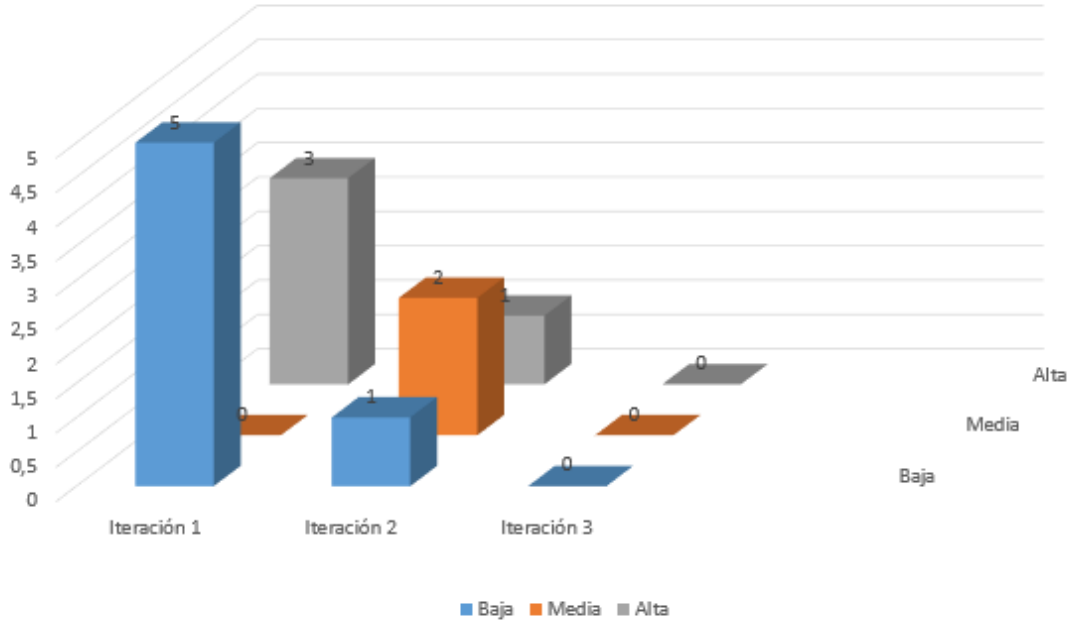

Figura 3.4 - No conformidades por iteración

Las pruebas de aceptación tienen más peso que las unitarias ya que constituyen un indicador de la satisfacción del cliente con la solución, además de marcar el final de una iteración y el comienzo de la siguiente.

Al final de la tercera iteración en la que se han realizado un total de 108 pruebas funcionales para comprobar que el sistema funciona correctamente, mostrando las salidas para cada escenario, 108 han sido clasificadas exitosas constituyendo un 100% de pruebas exitosas. Posteriormente se probó el comportamiento del sistema en un escenario de red simulado.

3.2 Característica del escenario de pruebas para el sistema de detección y aislamiento de fallas en la red

El escenario de prueba consiste en la simulación de una red de área local para probar las funcionalidades del sistema de detección y aislamiento de fallas en la red. Para el efecto, se utilizó el GNS3 como la herramienta simuladora de red, la cual trabaja en conjunto con otros programas para lograr la emulación de dispositivos de redes reales, creando una plataforma que permite el fácil diseño de topologías de redes complejas.

La Figura 3.1 representa la topología creada en el GNS3 con los equipos presentes en Tabla 2-1. El Cliente es una computadora HP con el sistema operativo Windows 8, y es la encargada de generar las requisiciones hacia el Servidor, lo cual tiene instalado el sistema operativo Windows XP en una máquina virtual.

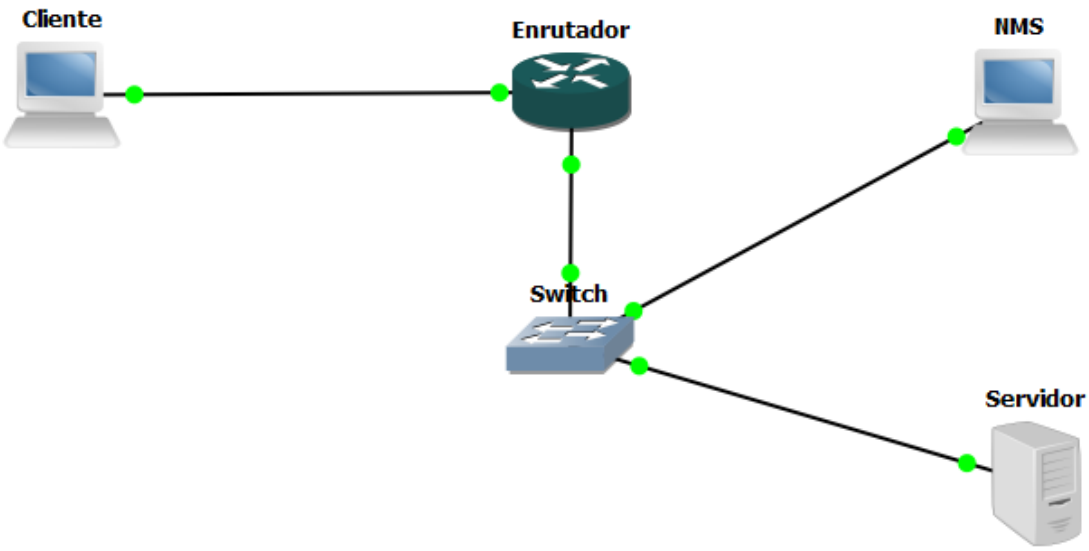

Figura 3.5 - Topología de la red creada en GNS3

La estación de gestión de red (NMS) está en la máquina en que se encuentra instalado el GNS3 sobre el sistema operativo Windows 8 y reside el sistema de detección y aislamiento de fallas en la red. Tanto en la máquina Cliente, la máquina NMS, la máquina servidor y el enrutador fueron instalados y configurados un agente SNMP.

Tabla 3-3 - Equipos de la topología en el GNS3

Nombre de equipo	Descripción
Cliente	En él se simula la generación del tráfico anómalo en la red
Servidor	Recibe el tráfico anómalo proveniente del cliente
NMS	Es la estación de gestión de la red en donde se encuentra el sistema de detección y aislamiento de fallas en la red
Enrutador	Responsable por el encaminamiento de paquetes entre el Cliente y el servidor
Switch	Switch que conecta las máquinas ServidorJper y NMS al red

La prueba consiste en la evaluación del comportamiento del sistema bajo las siguientes condiciones:

- **Funcionamiento normal de la red (FNR)**, en el que la red opera sin grandes cantidades de tráfico.

- **Funcionamiento anormal de la red (FAR)**, en el que se genera grandes cantidades de tráfico en determinado punto de la red para simular el comportamiento anormal debido al uso indebido de la red por parte de los usuarios y que tienen implicación en el rendimiento de la red.

De igual forma que se procedió en la evaluación de las pruebas de aceptación fue necesario clasificar el resultado de cada test realizado. Cada test realizado tiene una de las siguientes clasificaciones:

- **Positivo:** cuando el resultado del test es exactamente el esperado en función del tipo de condición.
- **Negativo:** cuando el resultado del test realizado no es el esperado para el tipo de condición definida.

Para la generación del tráfico que simule el comportamiento anormal debido al uso indebido de la red por parte de los usuarios se utilizó la herramienta Ostinato [63] que es una herramienta que permite la generación de un gran volumen de datos utilizando varios protocolos, tales como TCP, UDP e ICMP.

Con el Ostinato es posible simular tráfico anómalo, para el efecto el comportamiento anormal fue creado con la configuración del Ostinato en la máquina Cliente para generar un volumen de tráfico ICMP de 10.000 paquetes por segundo hacia la máquina Servidor, en una transmisión de duración igual a 10 minutos. La serie temporal que corresponde el perfil normal de operación de la red fue constituida durante una hora de observación de cada variable MIB sin el tráfico generado por la herramienta ostinato.

En la Tabla 3-1 se presenta el resultado de los testes realizados, en el test número 1 ninguna alarma fue generada que es el resultado que se esperaba por el tipo de condición definida para el test, sin embargo fue obtenido el mismo resultado para el test número 2 en el que su tipo de condición representa el comportamiento anormal debido al uso indebido de la red por parte de los usuarios y que tienen implicación en el rendimiento de la red, esto se dio por el nivel bajo de sensibilidad definido en el sistema para la generación de alarma, resultando que para el sistema en los dos testes se trataba de una condición normal.

Tabla 3-4 – Testes realizados

Número del test	Tipo de Condición	Alarmas Generadas	Clasificación
1	FNR	0	Positivo

2	FAR	0	Negativo
3	FNR	2	Negativo
4	FNR	0	Positivo
5	FAR	2	Positivo
6	FNR	0	Positivo
7	FAR	2	Positivo

Con la redefinición del nivel de sensibilidad para la generación de alarmas relativamente alto en comparación a lo de los testes anteriores, en el test número 3 correspondiente a una condición normal se han generados 2 alarmas a nivel de equipo, fue necesario bajar este nivel para que en el test siguiente no fuera generada ninguna alarma.

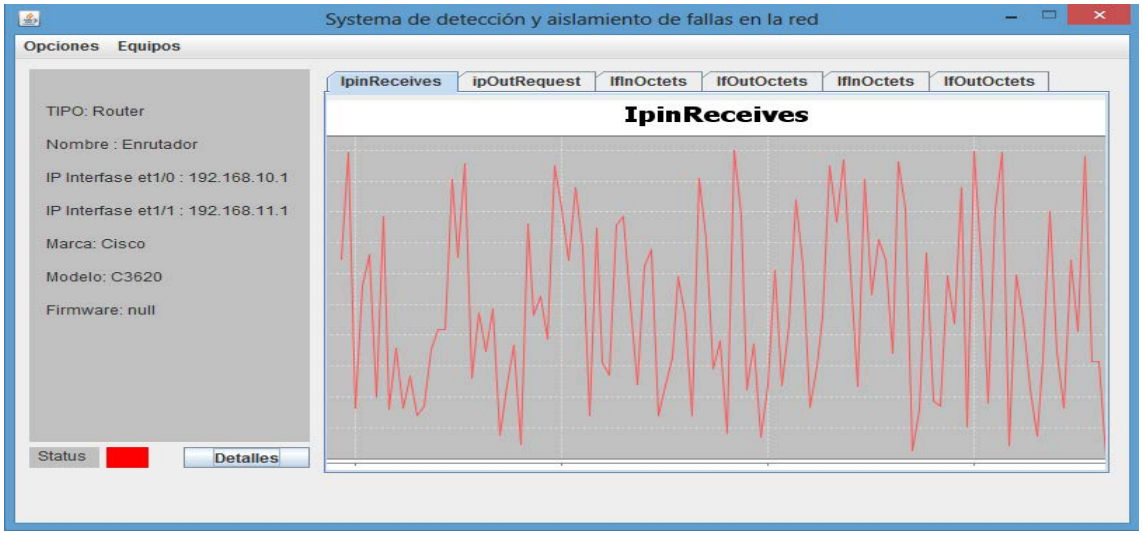

Figura 3.6 - Alarma a nivel de equipo

Manteniéndose el mismo valor para el nivel de sensibilidad se procedió a la realización del test número 5 que se trataba de la simulación del funcionamiento anormal de la red en que fueran generadas alarmas a nivel de equipo conforme ilustra la Figura 3.6. Los testes 6 y 7 fueron realizados con las mismas condiciones establecidas para los testes 4 y 5 con el fin de verificar si el sistema se comportaría de la misma forma.

La Figura 3.7 presenta la forma como las alarmas a nivel de equipo son vistos desde la perspectiva de la topología de la red, en que se tiene la información en cuanto el equipo, que genera el tráfico anómalo, el equipo de destino y la hora.

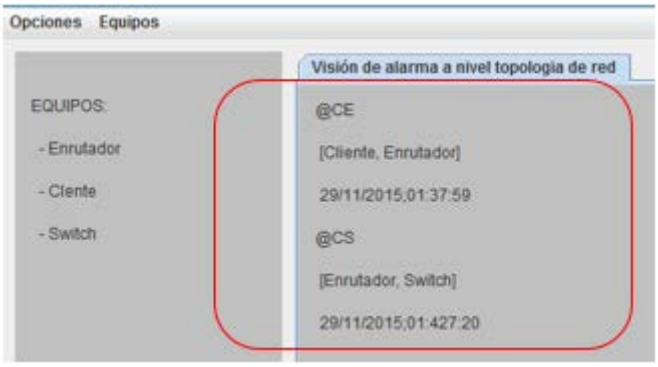

Figura 3.7 - A alarma a nivel de topología

3.3Evaluación de los resultados de la prueba

En los testes en que se han generado alarmas a nivel de equipo, los mismos correspondieron a los dos conjuntos de alarmas. Si nos enfocamos en las alarmas generadas en el test 3 se observa que fueron generadas alarmas de entrada y de salida en el enrutador. Para la alarmas de entrada corresponde al tráfico anómalo que es generado en la sub 192.168.11.0/24 por la máquina Cliente con el enderezo 192.168.11.2 para el puerto del enrutador en esta subred con el enderezo IP 192.168.11.1. Esta alarma corresponde a la correlación de las alarmas a nivel de variable MIB para las variables *InfInOctets* e *IpInReceives* conforme indica el área seleccionada en la Figura 3.8.

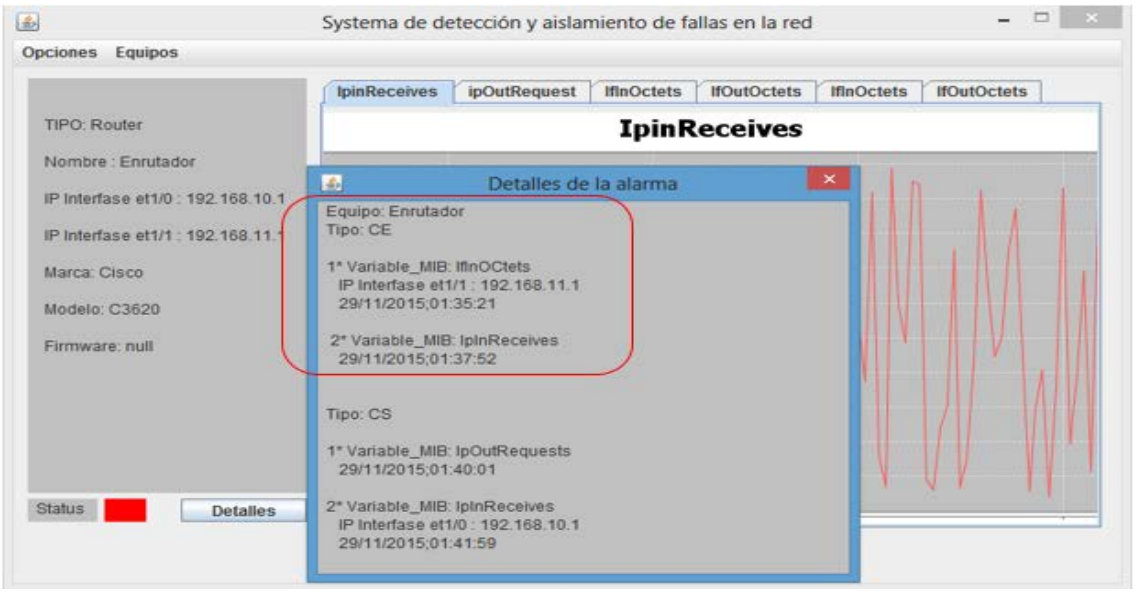

Figura 3.8 - Detalles de la alarma a nivel de equipo

En la Figura 3.9 el área seleccionada representan las alarmas a nivel de variable MIB que constituyeron a la alarma a nivel de equipo para el conjunto de salida (CS en la figura), lo cual representa el tráfico anómalo que se propaga de la variable

IpOutRequest para la variable IfOutOctets. La alarma de salida corresponde al tráfico anómalo que sale del puerto del enrutador con el enderezo IP 192.168.10.1 para la subred 192.168.10.0/24 donde se encuentra la máquina Servidor con el enderezo IP 192.168.11.2.

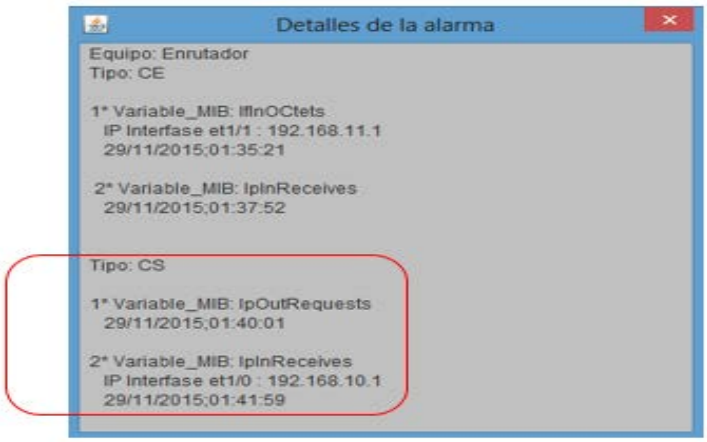

Figura 3.9 - Detalles de la alarma a nivel de equipo para el conjunto de salida

Al final de los 7 testes realizados 2 de ellos fueron clasificados como negativo debido a la configuración del nivel de sensibilidad definida y 5 fueron clasificados como positivo conforme la Figura 3.10, correspondiendo a un total de 29 % de testes no exitosos y 71 % de testes exitosos.

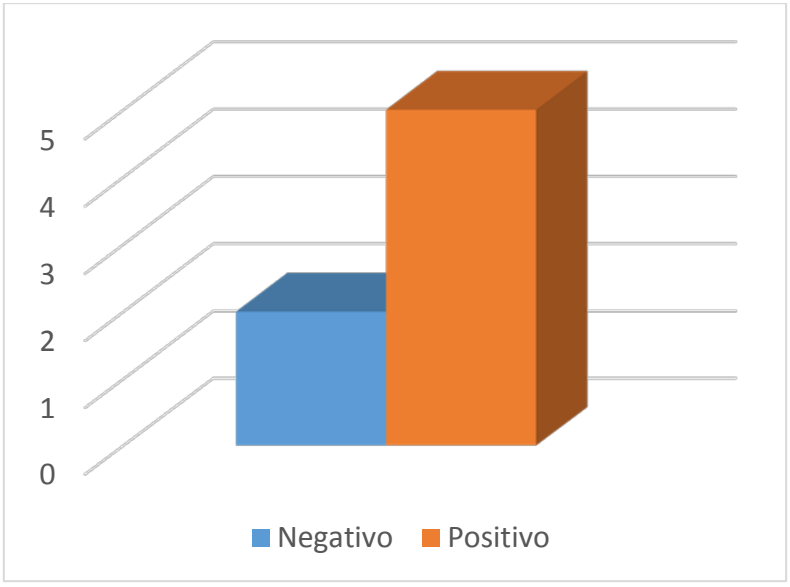

Figura 3.10 - Evaluación de los testes realizados

Conclusiones del capítulo

Las pruebas unitarias y de aceptación realizadas durante la fase de implementación permitieron el desarrollo controlado del sistema, la corrección de no conformidades en cada iteración teniendo como resultado el cumplimento de los requisitos funcionales.

Con la aplicación del sistema en el escenario de red simulado en la plataforma GNS3 para evaluar su comportamiento en un entorno dinámico se arrojó que la detección de anomalías no solamente depende del tipo de tráfico en la red sino que también depende del nivel de sensibilidad definido para la generación de la alarma.

Por tanto en función de su experiencia con la red que administra y los eventos pasados detectados por otras fuentes, el administrador de red debe definir el nivel de sensibilidad para la generación de alarmas y utilizar el sistema de detección y aislamiento de falla como una solución complementaria. La anticipación de las fallas por detección de los síntomas permite la aplicación de medidas de control y previne efectivamente la degradación de los servicios telemáticos brindados a los usuarios de la red.

Conclusiones generales

- La elaboración del marco teórico referencial hizo posible la identificación de los elementos claves para la gestión de redes que permitan la detección y aislamiento de fallas en la red, y con la confrontación de estos con los resultados arrojados por la encuesta aplicada a los técnicos de red en el campus de la UAN fueron identificadas deficiencias en el proceso de gestión de redes en la Universidad.
- Basándose en este resultado se condujo la modelación de la arquitectura para el sistema de detección y aislamiento de fallas en la red de forma a solucionar estas deficiencias.
- Con el conjunto de pruebas realizadas al sistema en el escenario de red simulado en la plataforma GNS3 se verificó que los algoritmos proactivos implementados previenen efectivamente la degradación de los servicios telemáticos con la anticipación de las fallas.

Recomendaciones

- Seguir con la investigación con el propósito de dotar el sistema de detección y aislamiento de fallas en la red con la capacidad para la clasificación de fallas en función de los síntomas detectados.
- Crear una versión Web para el módulo detector y localizador de anomalías para que este sea accedido vía navegador desde cualquier punto de la red.
- La aplicación del sistema como parte del proceso de gestión de redes en el campus de la universidad Agostinho Neto para evaluar su comportamiento en un ambiente en producción.

Referencias bibliográficas

[1] D. Tilson, K. Lytinen y C. Sorensen, «Research commentary: digital infrastructures – the missing IS research agenda,» *Information Systems Research,* vol. 21, 2010.

[2] A. Tanenbaum, Computer network forth edition, Prentice-Hall, 2003.

[3] A. Cartlidge, A. Hanna, C. Rudd, I. Macfarlane, J. Windebank y S. Rance, The It Infraestrucure Library: An Overviw of ITIL V3, UK: ItSMF Ltd, 2007.

[4] ISACA, COBIT 5: A business Framework for the Governance and Managment of Interprise IT, Isaca ISBN 978-1-60420-237-3, 2012.

[5] M. ROVERS, ISO/IEC 20000-1:2011: A pocket guide., Van Haren Publishing, ISBN 978-90-8753-68- 4, 2012.

[6] G. Hed, Ethernet network, forth edition, The Atrium, Southern Gate, Chichester,England: John Willey and Son Ltd, 2003.

[7] L. Klosterboer, Implementing ITIL configuration managemente, Indianopolis: IBM Press, 2008.

[8] ITU, «E.800 : Definitions of terms related to quality of service,» 09 2008. [En línea]. Available: https://www.itu.int/rec/T-REC-E.800-200809-I/en.

[9] I. G. D. Andrade y m. s. Sebastiá, «Evaluación de las prestaciones de una red epon mediante el programa opnet,» [En línea]. Available: http://w3.iec.csic.es/ursi/articulos_gandia_2005/articulos/te1/6006.pdf.

[10] u.-t. Y.1540, «Aspectos del protocolo internet – calidad de servicio y características de red.,» In,, 2005.

[11] M. Witczack, Soft Computing in fault detectión and insolation, 2005.

[12] J.-c. Laprie, «Dependable computing and fault tolerance: concept san terminology.,» de *In the twelfth confereence on fault tolerant computing system*, 1985.

[13] B. A. Forouzan, Data Communications and Networking, McGraw-Hill, 2013.

[14] Paessler, Prtg network monitor user manual., Ciudad de nuremberg: paessler ag,, 2014.

[15] T. Ryder, Nagios Core administration Coock book, Birmingham: Packt Publishing Ltd, 2013.

[16] Zenoss, Zenoss core administration., Austin, texas: zenoss inc, 2014 .

[17] S. Ali, Practical Linux Infrastructure, Apress, 2014.

[18] F. Feather. , D. Siewiork y R. Maxion, «Fault detección in an ethernet network using signature maching,» de *Sigcomp*, 1993.

[19] M. Thottan y C. Ji, «proactive Anomaly Detection Using Distributed Intelligent Agents,» *Network, IEEE ,* vol. 12, pp. 21 - 27, 1998.

[20] M. Tottan y c. Ji, «Anomaly detection in ip networks.,» *Ieee transactions on signal processing, vol. 51, no. 8,* august 2003.

[21] . B. B. Zarpelão , *Detecção de anomalias em redes de computadores. Tesis de Doctorado,* Brasil, São Paulo, 2010.

[22] SEI, CMMI para desarrollo CMMI-DEV, version 1.3, 5 Eglin Street: Carnegie Mellon University, 2010.

[23] Y. S. G. Gallardo, *Sistema de Gestión de Servicios de Soporte,* La Habana: UCI, 2012.

[24] CCTA , Service Support, London: Stationary office, 2004.

[25] J. G. Tomas y E. A. Lancharro, Introduccíon a la teleinformática, Ciudad Ferlindez : Mc Graw Hill, 1993.

[26] ITU, «X.701 : Information technology - Open Systems Interconnection - Systems management overview,» 08 1997. [En línea]. Available: http://www.itu.int/rec/T-REC-X.701-199708-I.

[27] R. L. Freman, Fundamental of telecommunication Second edition, Hoboken, New Jersey: John Wiley & Sons, Inc., 2005.

[28] M. Rose, The simple book: An introduction to internet management, Second edition, Englewood Cliffs, NJ: Prentice-Hall, 1996.

[29] V. Faltinsen y G.-A. Vindheim, Framework condition and requeriments for network monitoring in a campus network: best pratice Document, Noroega: Terena, 2011.

[30] M. D. R. Cruz, R. Martínez , I. G. Viciedo y Y. Garcia, «Modelo analítico del protocolo 802.3 para la evaluación de la qos,» de *Memorias del vi simposio internacional de telecomunicaciones en la xv convención y feria internacional, informática* , 2013 .

[31] D. M. Putzolu, F. Grove y US, «Policy-based network management system using dinamic policy generation». USA Patente US 6,578,076B1, 2003.

[32] C. M. Keliiaa, L. F. Tolendino, M. . J. Ernest, M. . A. Rios, J. . L. Taylor, T. . L. MacAlpine, E. . J. Klaus y C. . A. Morgan, «Policy Based Network Management: State of the Industry and Desired Functionality for the Enterprise Network and Security Policy / Testing Technology Evaluation,» Sandia National Laboratories, Albuquerque, New Mexico 87185 and Livermore, California 94550, 2005.

[33] R. Rajan, «A Policy Framework for Integrated and Differentiated Services in the Internet,» *IEEE Network,,* Vols. %1 de %2Vol. 13 No. 5,, September/October 1999.

[34] D. Durham, «The COPS (Common Open Policy Service) Protocol,» January 2000.

[35] I. . Katzela y M. Schwarz, «Schemes for fault identification in communication networks,» *IEEE/ACM Trans. Networking, vol. 3, pp. 753–764,,* 1995.

[36] I. Rouvellou y G. Hart, «Automatic alarm correlation for fault identification,» *in Proc. IEEE INFOCOM, Boston, MA,* 1995.

[37] A. Bouloutas, G. Hart y M. Schwartz, «On the design of observers for failure detection of discrete event systems and Control,» de *Network Management*, New York, 1990.

[38] H. Hajji, «Statistical Analysis of Network Traffic for Adaptive Faults Detection,» *IEEE Transactions on neural networks TRANSACTIONS ON NEURAL NETWORKS, VOL. 16, NO. 5, SEPTEMBER ,* 2005.

[39] A. T. Boulotas, S. Calo y A. Finkel, «Alarm Correlation and fault identification in Communication Network,» *IEEE transaction on communication vol 42, No 2/3/4,* pp. 523-533, 1994.

[40] J.-H. Bellec y T. Kechadi, «Fuzzy correlation algorithm in wide telecommunication networks,» *Internacional Journal of multimedia and ubiquitous. Vol 3, No 2 ,* April 2008.

[41] S. Lipschutz y M. L. Lipson, Teoria e problemas de matemática discreta, segunda edição, São Paulo, Brasil: BookMaan, 2008.

[42] R. H. Kenneth, Discrete Mathematics and Its Aplications, Seventh edition, New York: Mc Graw Hill, 2012.

[43] T. Jones, AI application programming, Higham, Massachusetts: Charles River Media, 2003.

[44] W. S. Mcculloch y Pitts, «Bulletin of mathematical biosphysics,» de *Pitts. A logical calculus of ideas in nervos activity.*, 1943, pp. 115-153.

[45] D. O. Hebb, The organization of behavior:a neuropsycological theory, New york: wiley, 1949.

[46] J. A. Freeman y D. M. Skapura, Redes neuronales: algoritmos, aplicaciones y técnicas de propagación., México: addison-wesley, 1993.

[47] B. Krose y P. V. D. Smagt, An introdution to neural networks eighth edition., The universit of amsterdam, 1996.

[48] B. M. Del Brio y A. S. Molina, Redes neuronales y sistemas difusos: 2 edición, Zaragoza: AlfaOmega Ra-Ma, 2001.

[49] M. L. Proença Junior, *Baseline Aplicado a Gerência de Redes. Tesis de doctorado,* Campinas, São Paulo: Faculdade de Engenharia Elétrica e de Computação, Universidade federal de Campinas, 2005.

[50] G. C. Canavos, Probabilidad y estadítica: Aplicaciones y métodos, Mexico: Mc Graw-Hill/ Interaméricana, 1988.

[51] G. Maibaum, Teoria de probabilidad y estadística matemática, Editorial Pueblo y educación, 1988.

[52] M. Steinder y A. A. Sethi, «A survey of fault localization techniques in computer networks,» *Science of computer programming n 53,* pp. 165-194, 2004.

[53] Hewlett-Packard Development Company, L.P., HP Universal CMDB Software Version: 10.20: Administration Guide, 2015.

[54] Combodo, «Itop documentation: Configuration Management (CMDB) Module,» 12 /11/ 2014. [En línea]. Available: https://wiki.openitop.org/doku.php?id=2_1_0:datamodel:itop-config-mgmt.

[55] ManageEngine, «ServiceDesk Plus,» 2014. [En línea]. Available: https://www.manageengine.com/es/service-desk/.

[56] Nagios enterprise, « Nagios core overiew,» [En línea]. Available: web: http://www.nagios.org . [Último acceso: 29 septiembre 2014].

[57] Ipswitch, «Whats up gold: monitoreamento de redes para profissionais,» [En línea]. Available: http://www.whatsupgold.com. [Último acceso: 29 septiembre 2014].

[58] Zoho Corporation, OpManager User Guide, 2013.

[59] J. J. Gutiérrez, M. J. Escalona y M. Mejías, «Pruebas de aceptación en programación extrema,» 2010.

[60] T. J. McCabe, «Complexity measure,» *IEEE Transactions on software,* 1976.

[61] R. Allende, Desarrollo de portales y extranet con plone, 2006.

[62] Beck, Planeando en programación extrema, 2000.

[63] Ostinato, «Packet traffic generator,» 2015. [En línea]. Available: http://code.google.com/p/ostinato. [Último acceso: 13 11 2015].

[64] A. Konar, Artificial intelligence and soft computing: Behavioral and cognitive modeling of human brain, New York: CRC Press, 2000.

Anexos

Anexo A Tabla de requisitos funcionales

Requisitos funcionales para el Módulo Gestión de configuraciones		
	Requisitos	Actor
1	Insertar un elemento de la configuración teniendo en cuenta el nombre, la descripción, el costo y la fecha de fabricación	Administrador de la CMDB, Especialista de la configuración
2	Modificar el nombre, la descripción, el costo y la fecha de 1 fabricación de un elemento de la configuración.	Administrador de la CMDB, Especialista de la configuración
3	Eliminar un elemento de la configuración.	Administrador de la CMDB, Especialista de la configuración
4	Insertar usuario, teniendo en cuenta su nombre, contraseña, si está activo o no en el sistema y el cliente al que pertenece.	Administrador de la CMDB, Especialista de la configuración
5	Modificar el nombre, la contraseña, la propiedad de activar en el sistema y/o el cliente del usuario.	Administrador de la CMDB, Especialista de la configuración
6	Eliminar un usuario.	Administrador de la CMDB, Especialista de la configuración
7	Insertar rol con su nombre y descripción.	Administrador de la CMDB, Especialista de la configuración
8	Modificar el nombre y/o la descripción del rol.	Administrador de la CMDB,
9	Eliminar un rol.	Administrador de la CMDB,
10	Asignar un rol a un usuario.	Administrador de la CMDB,
11	Modificar la asignación de un rol a un usuario determinado.	Administrador de la CMDB,
12	Eliminar la asignación de un rol a un usuario determinado.	Administrador de la CMDB,

13	Insertar un riesgo con su nombre y descripción.	Administrador de la CMDB,
14	Modificar el nombre y/o la descripción del riesgo.	Administrador de la CMDB
15	Eliminar riesgo.	Administrador de la CMDB
16	Insertar las localizaciones disponibles para los elementos de la configuración, teniendo en cuenta su dirección.	Administrador de la CMDB
17	Modificar la dirección de las localizaciones disponibles para los elementos de la configuración.	Administrador de la CMDB,
18	Eliminar las localizaciones que no se encuentren disponibles para los elementos de la configuración.	Administrador de la CMDB
19	Crear el historial de localizaciones por las que transcurre cada elemento de la configuración, teniendo en cuenta la fecha en la que un elemento de la configuración se sitúa en una localización.	Administrador de la CMDB
20	Modificar la fecha, la localización y/o el elemento de la configuración del historial de localizaciones por los que transcurre cada elemento de la configuración.	Administrador de la CMDB, Especialista de la configuración
21	Eliminar el historial de localizaciones por las que transcurre cada elemento de la configuración.	Administrador de la CMDB, Especialista de la configuración
22	Insertar los estados de los elementos de la configuración, teniendo en cuenta su nombre y descripción.	Administrador de la CMDB, Especialista de la configuración
23	Modificar el nombre y/o la descripción de los estados de los elementos de la configuración.	Administrador de la CMDB, Especialista de la configuración
24	Eliminar los estados de los elementos de la configuración.	Administrador de la CMDB, Especialista de la configuración
25	Crear el historial de estados por los que transcurre cada elemento de la configuración, teniendo en cuenta la fecha en la que un elemento de la configuración arriba a un estado.	Administrador de la CMDB, Especialista de la configuración
26	Modificar la fecha, el estado y/o el elemento de la configuración del historial de estados por los que transcurre cada elemento de la configuración.	Administrador de la CMDB, Especialista de la configuración

27	Eliminar el historial de estados por los que transcurre cada elemento de la configuración.	Administrador de la CMDB, Especialista de la configuración
28	Insertar los proveedores a cada elemento de la configuración, teniendo en cuenta su carnet de identidad, nombre, apellidos y descripción.	Administrador de la CMDB, Especialista de la configuración
29	Modificar el carnet de identidad, el nombre, los apellidos y/o la descripción de los proveedores de elementos de la configuración.	Administrador de la CMDB, Especialista de la configuración
30	Eliminar los proveedores de elementos de la configuración.	Administrador de la CMDB, Especialista de la configuración
31	Insertar el fabricante cada elemento de la configuración, teniendo en cuenta su carnet de identidad, nombre, apellidos, descripción y dirección.	Especialista de la configuración
32	Modificar el carnet de identidad, el nombre, los apellidos, la descripción y/o la dirección del fabricante de elemento de la configuración	Especialista de la configuración
33	Eliminar un fabricante de elemento de la configuración.	Especialista de la configuración
34	Insertar los tipos de relación que pueden existir entre los elementos de la configuración, teniendo en cuenta su nombre y descripción.	Especialista de la configuración
35	Modificar el nombre y/o la descripción de los tipos de relación que pueden existir entre los elementos de la configuración.	Especialista de la configuración
36	Eliminar un tipo de relación entre elementos de la configuración.	Especialista de la configuración
37	Insertar la relación existente entre un elemento de la configuración con otro.	Especialista de la configuración
38	Modificar el tipo de relación y/o los elementos de la configuración en cuestión, de una relación existente entre dos elementos de la configuración.	Especialista de la configuración
39	Eliminar la relación existente entre dos elementos de la configuración.	Especialista de la configuración
40	Insertar los clientes de los elementos de la configuración, teniendo en cuenta su carnet de identidad, nombre, apellidos y descripción.	Especialista de la configuración

41	Modificar el carnet de identidad, el nombre, los apellidos y/o la descripción de los clientes de los elementos de la configuración.	Especialista de la configuración
42	Eliminar un cliente de elemento de la configuración.	Especialista de la configuración
43	Insertar los trabajadores, teniendo en cuenta su carnet de identidad, nombre, apellidos y correo electrónico.	Administrador de la CMDB, Especialista de la configuración
44	Modificar el carnet de identidad, el nombre, los apellidos y/o el correo electrónico de los trabajadores.	Administrador de la CMDB, Especialista de la configuración
45	Eliminar un trabajador	Administrador de la CMDB, Especialista de la configuración
46	Insertar relación de los elementos de la configuración con las incidencias existentes.	Administrador de la CMDB, Especialista de la configuración
47	Modificar el elemento de la configuración y/o la incidencia de la relación existente entre estos.	Administrador de la CMDB, Especialista de la configuración
48	Eliminar la relación existente entre los elementos de la configuración y las incidencias.	Administrador de la CMDB, Especialista de la configuración
49	Insertar relación de los elementos de la configuración con los problemas existentes.	Administrador de la CMDB, Especialista de la configuración
50	Modificar el elemento de la configuración y/o el problema de la relación existente entre estos.	Administrador de la CMDB, Especialista de la configuración
51	Eliminar la relación existente entre los elementos de la configuración y los problemas.	Administrador de la CMDB, Especialista de la configuración
52	Insertar relación de los elementos de la configuración con los cambios existentes.	Administrador de la CMDB, Especialista de la configuración
53	Modificar el elemento de la configuración y/o el cambio de la relación existente entre estos.	Administrador de la CMDB, Especialista de la configuración

54	Eliminar la relación existente entre los elementos de la configuración y los cambios.	Administrador de la CMDB, Especialista de la configuración
55	Insertar relación de los elementos de la configuración con los eventos existentes.	Administrador de la CMDB, Especialista de la configuración
56	Modificar el elemento de la configuración y/o el evento de la relación existente entre estos.	Administrador de la CMDB, Especialista de la configuración
57	Eliminar la relación existente entre los elementos de la configuración y los eventos.	Administrador de la CMDB, Especialista de la configuración
58	Generar Reportes de los elementos de la configuración	Administrador de la CMDB, Especialista de la configuración

Requisitos funcionales para los módulos detector y localizador de anomalías y gestor de políticas		
	Requisitos	Actor
59	Importar información sobre topología de red	Administrador de red, Técnico de red
60	Insertar el nivel de sensibilidad para las alarmas en función del tipo de equipo	Administrador de red, Técnico de red
61	Visualizar las gráficas de monitoreo	Administrador de red, Técnico de red
62	Visualizar las alarmas a nivel de equipo	Administrador de red, Técnico de red
63	Insertar una nueva política con su nombre y descripción	Administrador de red, Técnico de red
64	Modificar nombre y/o descripción de política	
68	Eliminar política	
69	Relacionar política con los equipos	Técnico de red

Requisitos no funcionales del Sistema

	Requisitos
70	**Seguridad:** Sólo el personal autorizado deberá hacer uso del sistema, entiéndase personal autorizado los usuarios registrados en el sistema
71	**Confiabilidad:** El sistema debe estar disponible a tiempo completo para los usuarios autorizados.
72	**Restricciones en el diseño y la implementación:** Se utilizará como sistema gestor de base de datos MySql, como servidor web Apache y como lenguaje de programación PhP y Java.
74	**Software:** El sistema debe ser multiplataforma, debe poder ejecutarse tanto en las versiones de GNU/Linux como de Windows.
75	**Rendimiento:** Los tiempos de respuesta del sistema deben ser como máximo de 1 segundo, así como la velocidad de procesamiento de la información.
76	**Seguridad:** Sólo el personal autorizado deberá hacer uso del sistema, entiéndase personal autorizado los especialistas del Centro de Soporte UCI.
77	**Confiabilidad:** El sistema debe estar disponible a tiempo completo para los usuarios autorizados.

Anexo B Historias de usuarios

Historia de usuario	
Número: 1	**Nombre:** Insertar un elemento de la configuración teniendo en cuenta el nombre, la descripción, el costo y la fecha de fabricación
Usuario: Administrador de la CMDB, Especialista de la configuración	
Modificación de historia numero	**Iteración Asignada:** 1
Prioridad en Negocio: Alta	
Riesgo en Desarrollo: Alto	
Descripción: El sistema debe permitir insertar un elemento de la configuración tantas veces como sea necesario especificando en cada una de ellos el nombre, la descripción, el costo y la fecha de fabricación. Para guardar los cambios realizados, se debe presionar la opción guardar, en caso contrario cancelar	
Observaciones: El nombre para un elemento de configuración debe ser único en el sistema. Para una correcta inserción del elemento de la configuración se debe establecer el nombre, la descripción, el costo y la fecha de fabricación como parámetros obligatorios.	

Historia de usuario	
Número: 37	**Nombre:** Insertar la relación existente entre un elemento de la configuración con otro.

Usuario: Administrador de la CMDB, Especialista de la configuración
Modificación de historia numero | **Iteración Asignada:** 1
Prioridad en Negocio: Alta
Riesgo en Desarrollo: Alto
Descripción: El sistema debe permitir Insertar la relación existente entre un elemento de la configuración con otro.
Observaciones: La relación entre los elementos de configuraciones debe representar los enlaces físicos en la red y los softwares instalados en servidores

Historia de usuario	
Número: 62	**Nombre:** Visualizar las alarmas a nivel de equipo
Usuario: Administrador de red, Técnico de red	
Modificación de historia numero	**Iteración Asignada:** 1
Prioridad en Negocio: Alta	
Riesgo en Desarrollo: Alto	
Descripción: El sistema debe la visualización de las alarmas a nivel de equipo.	
Observaciones: Las alarmas a nivel de equipo son generados de acuerdo al tipo equipo	

Anexo C Encuesta sobre la gestión de red en el campus de la UAN

Técnico	Grado Académico	Años de experiencia con la red	Cargo
A	Ingeniero Informático	3	Administrador
B	Ingeniero Informático	3	Administrador
C	Estudiante de ciencias de la computación (3 año)	1	Técnico de operaciones
D	Estudiante de ciencias de la computación (3 año)	1	Técnico de operaciones

Según el proceso de gestión actual es posible:	Cantidad		
	Si	No	No sabe
a) ¿Obtener una lista de los activos de la red?	4		
b) ¿El control automatizado de inventario de los activos de la red?	1		3
c) ¿Mantener el registro de la relación existente entre los diferentes activos de la red?		1	3
d) ¿Mantener el histórico de los cambios efectuados en la infraestructura?		3	1
e) ¿Obtener información relacionada a los fabricantes y proveedores de cada tipo de activo?	1		3
f) ¿La topología de la red según el diseño elaborado para la misma?	1	2	3
Sobre el rendimiento y fallas en la red			
a) ¿Se mantiene el control sobre la calidad de servicio y rendimiento físico de los equipos?	4		
b) ¿Es posible detectar los síntomas de posibles fallas?	3		1
c) ¿Es posible observar la propagación de estos síntomas sobre la red?			4
d) ¿Se hace de forma sencilla la localización física de un equipo en falla?	2	1	1
Sobre las herramientas de gestión	**Herramienta**		
a) ¿Qué herramientas son utilizadas para la realización de las tareas de gestión de la red?	Nagios (4), Cati(4)		