Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

GUÍA PRÁCTICA PARA LA IMPLEMENTACIÓN DE UN GESTOR DE GESTORES DE FALLAS, EN REDES DE TELECOMUNICACIONES

Lilian Zyiomara Linares Rivera
Asesorado por el Ing. Gerardo de Jesús Paredes Navarrete

Guatemala, septiembre de 2012

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

GUÍA PRÁCTICA PARA LA IMPLEMENTACIÓN DE UN GESTOR DE GESTORES DE FALLAS, EN REDES DE TELECOMUNICACIONES

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

LILIAN ZYIOMARA LINARES RIVERA
ASESORADO POR EL ING. GERARDO DE JESÚS PAREDES NAVARRETE

AL CONFERÍRSELE EL TÍTULO DE

INGENIERA ELECTRICISTA

GUATEMALA, SEPTIEMBRE DE 2012

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. Juan Carlos Molina Jiménez
VOCAL V	Br. Mario Maldonado Muralles
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Herbert René Miranda Barrios
EXAMINADOR	Ing. Edwin Alberto Solares
EXAMINADOR	Ing. Edgar Neftalí Carrera
EXAMINADOR	Ing. Edgar Montufar Urizar
SECRETARIA	Inga. Gilda Marina Castellanos de Illescas

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

GUÍA PRÁCTICA PARA LA IMPLEMENTACIÓN DE UN GESTOR DE GESTORES DE FALLAS, EN REDES DE TELECOMUNICACIONES

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 10 de agosto de 2011.

Lilian Zyomara Linares Rivera

Guatemala 3 de mayo de 2012

Ing. Carlos Guzmán
Coordinador Área Electrónica
Facultad de Ingeniería
Universidad San Carlos de Guatemala

Estimado Ingeniero Guzmán:

Reciba un cordial saludo, el motivo de la presente es para manifestarle que revisé y aprobé el documento de trabajo de tesis: "GUÍA PRÁCTICA PARA LA IMPLEMENTACIÓN DE UN GESTOR DE GESTORES DE FALLAS EN REDES DE TELECOMUNICACIONES", desarrollado por la estudiante Lilian Zyiomara Linares Rivera, carné 8812409.

Sin otro particular, agradezco su amable atención.

Atentamente,

Ing. Gerardo Paredes Navarrete
COL. 1,988
Ing. Gerardo Paredes Navarrete
Colegiado No.1988

ÁD DE SAN CARLOS
E GUATEMALA

TAD DE INGENIERIA

Ref. EIME 23. 2012
Guatemala, 7 de MAYO 2012.

Señor Director
Ing. Guillermo Antonio Puente Romero
Escuela de Ingenieria Mecànica Elèctrica
Facultad de Ingenieria, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: "GUÍA PRÁCTICA PARA LA IMPLEMENTACIÓN DE UN GESTOR DE GESTORES DE FALLAS, EN REDES DE TELECOMUNICACIONES", de la estudiante, Lilian Zyiomara Linares Rivera, que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,
ID Y ENSEÑAD A TODOS

Ing. Carlos Eduardo Guzmán Salazar
Coordinador Area Electrónica

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

CEGS/sro

IDAD DE SAN CARLOS
E GUATEMALA

TAD DE INGENIERIA

REF. EIME 33. 2012.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; Lilian Zyiomara Linares Rivera titulado: "GUÍA PRÁCTICA PARA LA IMPLEMENTACIÓN DE UN GESTOR DE GESTORES DE FALLAS, EN REDES DE TELECOMUNICACIONES", procede a la autorización del mismo.

Ing. Guillermo Antonio Puente Romero

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

GUATEMALA, 12 DE JUNIO 2,012.

d de San Carlos
uatemala

de Ingeniería
ecanato

DTG. 426.2011

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al trabajo de graduación titulado: **GUÍA PRÁCTICA PARA LA IMPLEMENTACIÓN DE UN GESTOR DE GESTORES DE FALLAS, EN REDES DE TELECOMUNICACIONES,** presentado por la estudiante universitaria **Lilian Zyiomara Linares Rivera,** autoriza la impresión del mismo.

IMPRÍMASE:

Ing. Murphy Olympo Paiz Recinos
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, 7 de septiembre de 2012

/gdech

ACTO QUE DEDICO A:

Mi Dios	Porque en los momento más difíciles ruego a él y él me responde y en los momentos de paz sé que me observa y está conmigo.
Mis hijos	Isabel y Pablo Ortiz Linares porque son el motor que me impulsa cada día a ser mejor, por ser lo más importante que existe en mi vida, todo mi amor para ellos dos.
Mis padres	Amada Rivera y Edmundo Linares con cariño.
Mis hermanas	En especial a Roxana, Leticia, Patricia y Sandra Linares Rivera por todo el apoyo recibido.
Mis hermanos	Mynor y Carlos Linares Rivera con cariño.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

AA	Alarma generada dentro del módulo experto.
AB	Alarma original del sistema de gestión nativo.
AM	*Access Module.*
AO&M	Administración, Operación y Mantenimiento.
API	*Application Programming Interface* (Interfaz de programación de aplicaciones).
ASCII	*American Standard Code for Information Interchang.*
ASN. 1	*Abstract Syntax Notation One.*
ATM	*Asynchronous Transfer Mode.*
***Black* office**	Oficina parte del NOC que atiende fallas más especiales principales conexiones de la red de la red de transporte. *Front Office* Oficina parte del NOC que atiende primeramente las fallas.
Backbone	Es un software que constituye las partes más importantes del Sistema Operativo.

VER	Basic Encoding Rules.
B-ISDN	Broadband Integrated Services Digital Network.
BRMS	Sistemas de Gestión de Reglas de Negocios.
C++	Lenguaje de programación.
CMIP	Common Management Information Protocol.
CMIS	Common Management Information Service.
CORBA	Common Object Request Broker Architecture.
DSLAM	Digital Subscriber Line Access Multiplexer.
ECC	Canales anidados de datos.
eTOM	Enhanced Telecom Operations M.
FGS	Funciones de Gestión de Sistemas abiertos.
FM	Funtion Module.
GAT	Graphical ASCII Toolkit.
GDMO	Guía para la definición de objetos gestionados.
GIO	General Inter ORB.

HTML	Hyper Text Markup Lenguaje.
IDL	Interface Definition Lenguaje.
IEEE	Institute of Electrical and Electronics Engineers.
IIOP	Internet Inter-ORB Protocol.
IP	Internet Protocol.
ISDN	Integrated Services Digital Network.
ISO	International Standards Organization.
Kernel	Es un software que constituye la parte más importante del Sistema Operativo.
LAN	Local Area Network.
LAP D	Link Access Protocol for D-channel.
LLA	Arquitectura Lógica en Capas.
MAC	Control de Acceso al Medio.
MIB	Management Information Base.
MIR	Management Information Repository.

MOC	Clases de Objetos Administrables.
MPLS	MultiProtocol Label Switching.
MTTR	Tiempo medio de atención de fallas Mean Time to Repair.
NE	Elemento de red.
NGN	Elemento de red de nueva generación.
NOC	Centro de operación de la red.
OMG	Objet Management Group.
OML	Alarma de pérdida de señal de transmisión.
ORB	Objet Request Broker.
OS	Sistema Operativo.
OSF/Motif	Open Software Foundation/biblioteca para la creación de entornos gráficos bajo X Window System en sistemas Unix.
PDH	Plesiochronous Digital Hierarchy.
Picking	Área donde se preparan los pedidos con diversos productos.

PM	Presentation Module.
Proceso	Secuencia de pasos o elementos para alcanzar un fin.
Productividad	Es la realización óptima de los recursos invertidos por la empresa.
Proxi	Es un programa o dispositivo que realiza una acción en representación de otro.
PSTN	Red telefónica pública conmutada.
QoS	Quality of Service.
RCD	Red de comunicación de datos.
RDSI	Red Digital de Servicios Integrados.
RGT	Red de Gestión de Telecomunicaciones.
SDH	Synchronous Digital Hierarchy.
SGFRT	Sistema de Gestión de Fallas de Red de Telecomunicaciones.
SGN	Sistema de Gestión Nativo.
SLA	Service Level Agreement.

SNMP	Simple Network Management Protocol.
TAC	Centro de soporte del proveedor.
TCP	Transmissión Control Protocol.
TL1	Transaction Lenguaje 1.
TMF	Telemanagement Forum TMF.
Traps	Son los eventos que el agente envía hacia el gestor como alarma.
TT	Trouble Ticket o boleta de atención de falla.
UDP	User Datagram Protocol.
UIT-T	Unión Internacional de Telecomunicaciones.
VoIP	Protocolo de Voz sobre Internet.
WAN	*Wide Area Network.*

RESUMEN

Este trabajo de graduación proporciona los lineamientos para la implementación de un sistema de gestión de gestores de fallas en redes de telecomunicaciones, además proporciona ejemplos de documentos diseñados para la colección de datos, donde se establezcan claramente los requerimientos que serán importantes para la implementación de SGFRT, así como el diseño de catálogos de las alarmas que impactan el servicio y que pueden generar apertura de *ticket* para atención de fallas.

La SGFRT será una plataforma compuesta de hardware y software que forma parte de la arquitectura definida en la REC. UIT- M.3010, para la gestión de redes de Telecomunicaciones de la UIT-T, pudiendo interactuar con otros OS, equipos de mediación o los propios NE, así mismo, cumple con ISO ya que consiste en un sistema abierto, lo que significa que es posible interoperar con otros sistemas, esto es de suma importancia ya todos los sistemas de gestión nativos (sistemas de gestión de cada red) son multivendor-multitecnología-multiservicio).

Dentro del documento se hace un análisis del funcionamiento interno del SGFRT, compuesto por los diferentes módulos, esto es necesario ya que esta herramienta pasará a ser administrada también por personal del centro de gestión y es de suma importancia que conozcan cómo funciona y su alcance.

La implementación de una herramienta de este tipo, permite a través de la colección de las alarmas generadas por todas las redes de diferentes tecnologías, hacer una correlación entre ellas, para detectar la causa raíz y así generar *tickets* automáticos a través de un módulo especializado en esto. Una herramienta de esta magnitud debe generar reportes estadísticos que ayuden a un mantenimiento preventivo.

Es importante indicar que con su funcionamiento e incorporación en un centro de atención y gestión de fallas, es necesario modificar los procesos de atención de éstas, es por ello, que se plantea a través de un diagrama de flujo cómo pueden cambiar los roles del personal dedicado a su atención, esto con el fin de optimizar el potencial que este tipo de herramienta es capaz de desarrollar para que junto al recurso humano se logren los objetivos de la empresa.

OBJETIVOS

General

Proporcionar una guía práctica para la implementación de un sistema de gestión de gestores de las redes de telecomunicaciones de datos, voz y video, que sea multivendedor y multiprotocolo.

Específicos

1. Delimitar el alcance del sistema de gestión de gestores, a través de establecer las normas internacionales y de la empresa que aseguren su correcto funcionamiento.

2. Colectar el tipo de tecnología, capacidades y marcas de las redes existentes en la empresa.

3. Analizar la arquitectura y funcionamiento del sistema de gestión de gestores de fallas de redes de telecomunicaciones.

4. Proporcionar los aspectos relacionados con la implementación y definición de reglas de correlación para el correcto funcionamiento del sistema de gestión de gestores de fallas adquirido.

INTRODUCCIÓN

Empresas grandes de telecomunicaciones que prestan variedad de servicios, desde voz, datos, televisión, se enfrentan a la problemática de la coexistencia de múltiples tecnologías, multiples servicios, multiples marcas de equipos, pese a que cada red cuenta con su propio gestor nativo de fallas, debe existir un gestor de gestores que centralice todas las fallas y permita hacer una correlación de las mismas para encontrar una causa raíz.

En el presente trabajo de graduación se plantea un escenario en un centro de gestión de red de una empresa de Telecomunicaciones, que tiene que enfrentarse a la implementación de sus redes con las variedades descritas anteriormente, donde una falla grave o crítica puede afectar en cascada desde el *backbone*, red de transporte hasta accesos e impactar en la red de conmutación o datos.

Por ejemplo, si la falla es afecta a un solo tipo de equipo debe ser relativamente sencillo aislarla y darle solución, si existe una falla grave dada en el *backbone* del área de transporte por ejemplo, se verá reflejada en el acceso, surgirán alarmas en ambas redes, esto dará inicio a un cotejamiento de información entre los técnicos de turno para verificar en qué red, qué tecnología y el impacto de dicha falla, se estarán monitoreando diversos sistemas de gestión hasta aislar la falla y darle solución.

Dada la situación descrita anteriormente surge la necesidad de unificar en un solo sistema de gestión todas las alarmas provenientes de las diferentes redes y que logre hacer una correlación para encontrar la causa raíz del problema.

Este documento presenta una guía para la implementación de un gestor de gestores de fallas de redes de transporte, voz y datos para una empresa de Telecomunicaciones, en dicho documento se dan ejemplos de lo que puede ser implementado así como un análisis más afondo del funcionamiento interno que puede tener un sistema de gestión de fallas de redes de telecomunicaciones o SGFRT.

Incluye paso a paso los procesos necesarios para su implementación, desde la delimitación del alcance lo cual puede ser variado dependiendo de las políticas de la empresa, los recursos económicos, equipos en uso, etcétera, recolección de la información, es decir, software y hardware, interfaces, selección de la aplicación, hasta la implementación, cuyo objetivo principal es ayudar a estas empresas de telecomunicaciones a correlacionar las fallas entre los diferentes tecnologías y marcas para disminuir los tiempos de solución de fallas y con ello mantener la calidad en el servicio prestado para ser competitivos en el mercado de las telecomunicaciones.

1. DELIMITACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE FALLA DE REDES DE TELECOMUNICACIONES

1.1. Definición de los requerimientos de la empresa

Las empresas dedicadas a vender el servicio de voz, datos o televisión, cuentan como norma con un centro de gestión de la red, para su administración, en dicho centro se encuentran instalados los Sistemas de Gestión Nativos (SGN) que son los que colectan las fallas de cada tecnología, uno o más por cada tecnología, tipo de red y proveedores distintos, que a la vez utilizan distintos protocolos de comunicación, esto lleva consigo el desafío de correlacionar todas la fallas de dichas redes para encontrar la causa raíz, esto se hace usualmente de forma manual, es decir, dada una falla en una red los supervisores del SGN se comunican verbalmente para establecer la causa.

Un sistema de gestión de gestores de fallas en redes de telecomunicaciones (SGFRT) puede hacer dicha correlación en forma automática. Sin embargo, para su implementación el Ingeniero encargado de su adquisición e implementación, debe conocer de las opciones en el mercado así como los detalles de la puesta en funcionamiento, conocer cuales son las limitaciones y alcance que la empresa desea, es por ello, que se hace crítico contar con un documento que le indique la secuencia lógica de los requerimientos y necesidades en su planificación, adquisición e implementación.

La estructura del SGFRT debe estar fundamentada sobre bases sólidas, como son las recomendaciones internacionales de la UIT-T o ISO, sin dejar de tomar en cuenta las políticas internas de la empresa. Son tratados aspectos que deben ser de prioridad para su implementación. La gestión integrada de fallas permitirá hacer una correlación de las fallas dadas en las diferentes redes permitiendo la disminución del tiempo medio de solución MTTR y con ello lograr las metas propuestas por la empresa y los acuerdos de disponibilidad (SLA) acordados con los clientes.

A continuación serán tratados cada uno de los aspectos que el ingeniero a cargo de la implementación de la plataforma solución o SGFRT debe considerar para alcanzar la compra, instalación y puesta en funcionamiento.

- Interoperabilidad

La interoperabilidad se refiere a la capacidad de comunicarse y operar entre dos equipos de tecnologías de diferente proveedor. La RGT (Red de Gestión de Telecomunicaciones) deberá soportar dos formas de integración generales (según REC. UIT-T M.3010), el de gestión de sistemas CMIP/OSI y el marco general CORBA.

Es necesario realizar pruebas entre la plataforma solución y los sistemas de gestión a integrar para asegurar su funcionamiento. Las pruebas de interoperabilidad deben comprobar los protocolos de interfaz, la información compartida o expuesta sobre estas interfaces y la funcionalidad de la interfaz del sistema.

Para algunos casos los proveedores ya cuentan con interfaces que garantizan la interoperabilidad con otros proveedores, esto debe ser verificado durante la evaluación de los diferentes SGFRT existentes en el mercado.

- Estructura de la solución

La REC M.3010, define tres aspectos a tomar en cuenta para planificar una red de gestión de telecomunicaciones y para lograr una interconexión entre diversos tipos de sistemas de operación, estos tres aspectos serán tomados como base para la implementación de la SGFRT, a continuación son descritos:

  - Arquitectura funcional

La arquitectura funcional definida en la REC. UIT-T M. 3010, describe las distintas funciones necesarias para gestionar un sistema y las interrelaciones entre ellas y cómo estas funciones se agrupan en las denominadas áreas funcionales (de fallos, de configuración, de contabilidad, de prestaciones y de seguridad) para satisfacer los requisitos del usuario para gestión de:

    - Fallos
    - Configuración
    - Contabilidad, de prestaciones
    - Seguridad

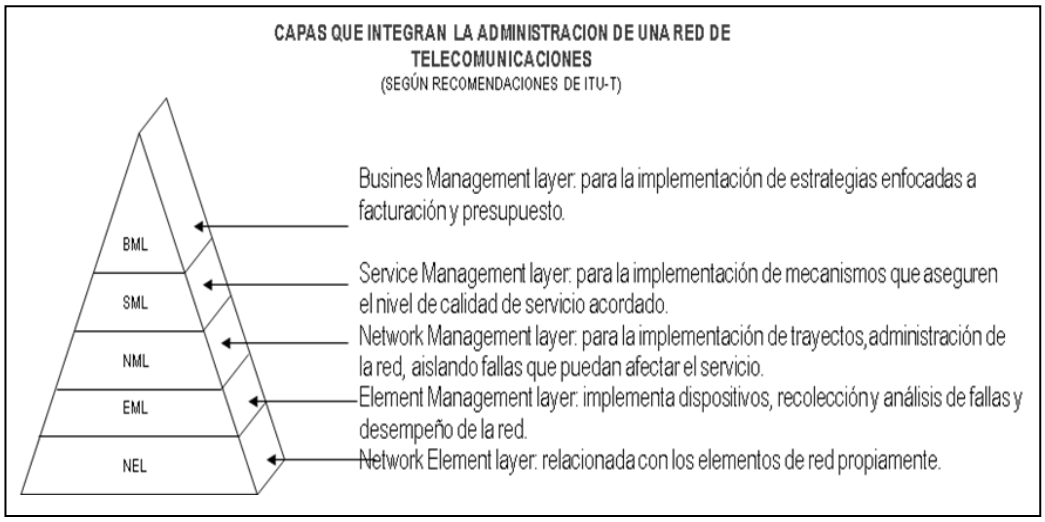
También descritas en la REC. UIT-T X.700 para Sistemas Operativos abiertos. Para mantener delimitado el campo de trabajo de la SGFRT, esta se basará solamente en la gestión de fallos, es decir, la plataforma solución permitirá hacer una recolección de fallas de las múltiples tecnologías permitiendo hacer una correlación que lleve a una solución rápida y efectiva de las fallas.

Así mismo, para facilitar la comprensión y mantener un orden que proporcione estructura a la Arquitectura funcional definida por la REC. M3010 hace una subdivisión de capas lógicas o LLA (arquitectura lógica en capas). Cada capa lógica describe aspectos relacionados con su función y agrupa información de gestión en relación con la misma, las capas son las siguientes:

- Capa empresarial
- Capa de servicios
- Capa de red
- Capa de elementos

Estas capas servirán para ubicar la solución propuesta en la capa de elementos de red y la gestión de dichos elementos, a continuación se describe la pirámide propuesta por la REC. UTT-T M. 3010, vea figura 1 en la siguiente página, en la cual se indica cómo pueden ser integradas las siguientes capas para lograr una completa gestión del negocio de las Telecomunicaciones, por el momento solamente se establecerá en la capa de gestión de elementos de red.

Figura 1. **Pirámide de administración de una red de telecomunicaciones**



Fuente: elaboración propia.

- La arquitectura de la información

El área de la arquitectura de la información, describe la abstracción en objetos de los recursos que están siendo gestionados y de los recursos necesarios para la gestión y la definición de la base de información de gestión (MIB: Management Information Base), estas MIBs deberán ser proporcionadas por los supervisores de cada SGN para ser cargadas en el SGFRT.

Si se necesita modelar la información para la pila de protocolos seleccionada en la red debe utilizarse una técnica de modelización de información normalizada. Para el paradigma de gestión de sistema CMIP/OSI este modelo de información ha de basarse en las Rec. UIT-T X.720 (5) y X.722 (21).

En el caso de CORBA, se proporciona más de un posible paradigma para el modelo, el cual ha de ser conforme con la serie de Rec. UIT-T X.780, cuando corresponda. En el modelo se ha de especificar cuál ha sido el marco escogido.

Además, se podrá hacer uso de los siguientes protocolos para integración de aquellos sistemas de gestión que no puedan ser integrados a través de OSI o CORBA.

- SNMP
- ASCII

- Arquitectura física

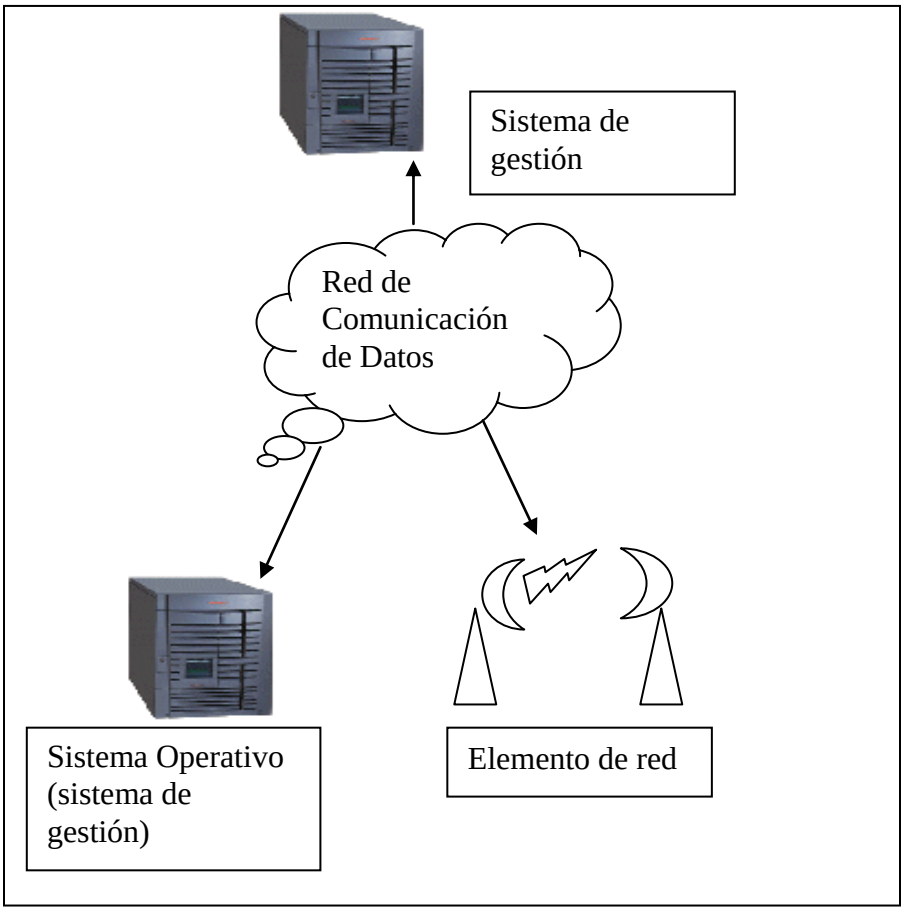
La arquitectura física define cada uno de los elementos que conforman una red de gestión de telecomunicaciones y de cómo estos interactúan entre sí para el objetivo final que es la gestión de la misma, es de hacer notar que la solución propuesta está ubicada dentro de los OS y tiene la facilidad de comunicarse a través de interfaces normalizadas y haciendo uso de la función de información de protocolos estandarizados con el fin de modelar la información proveniente de cada gestor nativo como se indicó en el párrafo anterior.

La red de comunicación de datos, servirá para transportar los datos de gestión entre los elementos de red y los gestores nativos y la plataforma solución, proporciona funcionalidad dentro del servicio de transporte de las cuatro capas inferiores del modelo de referencia OSI definido en la REC. X.200.

Su uso se encuentra definido en la REC. M3010 en la arquitectura física de una RGT.

En la figura 2 se observa un ejemplo de los elementos que interconectará la RCD, puede utilizar una red externa o una red interna en los canales anidados de datos ECC, utilizando por ejemplo el protocolo LAP D en la tecnología SDH.

Figura 2. **Red de comunicación de datos (RCD**)



Fuente: elaboración propia.

Para este caso su uso será exclusivamente externo, es decir, independiente a la red de telecomunicaciones, pudiendo constar de cierto número de subredes individuales de tipos distintos, interconectados entre sí. La RCD puede utilizar una LAN o una WAN, es técnicamente independiente, puede utilizar UIT-T X.25, TCP, UDP, etcétera.

- Campo de aplicación

El centro de gestión debe ser el ente encargado de monitoreo de las alarmas de todas la redes ya sea fija o móvil, a nivel local o internacional, según las políticas dictadas por las empresas. A continuación se describen las redes que pueden ser gestionadas:

Se indican a continuación ejemplos de redes, servicios de telecomunicación y tipos principales de equipo que pueden ser gestionados por la RGT:

Redes públicas y privadas, incluidas las RDSI de banda estrecha y de banda ancha, (incluido el ATM) redes móviles, redes telefónicas privadas, redes privadas virtuales y redes inteligentes.

La propia RGT; terminales de transmisión (multiplexores, transconectores, equipos de modulación de canal, jerarquía digital síncrona, etcétera).

Sistemas de transmisión digitales y analógicos (cable, fibra, radio, satélite, etcétera).

Computadoras principales, procesadores frontales y servidores
Centrales digitales y analógicas
Redes de área (ampliada, metropolitana o local)
Redes con conmutación de circuitos y de paquetes

- Interfaz hombre/máquina

Los servicios de presentación (interfaz hombre/máquina) pueden estar basados por ejemplo en OSF/Motif, proporcionándose una interfaz gráfica unificada para sistemas de explotación denominada LUEX-Gráfico. Dicha interfaz permite tener distintas vistas de la planta gestionada así como actuar sobre los íconos que representan a los elementos que componen dicha planta, ofreciendo para ello una representación gráfica de las alarmas presentes en dichos elementos. El LUEX-Gráfico permite, además, la construcción automática de comandos mediante formularios que muestran los valores permitidos de los parámetros de cada comando.

- Lineamientos internos a la empresa

A parte de los requerimientos establecidos bajo normas internacionales tales como las indicadas en párrafos anteriores, es decir, la UIT-T e ISO, toda empresa tiene lineamientos establecidos según sus necesidades o políticas de administración, a continuación se darán una serie de estos requerimientos planteados con base en la experiencia en el campo de adquisición e implementación de soluciones de esta índole.

- Escalabilidad

Debe estar proyectado para escalar a las siguientes capas de gestión de la arquitectura funcional de la Telecomunication Manager Network, según recomendaciones (capa gestión de red, capa gestión de servicio, capa administración comercial) ver figura 1.

- Colección de datos

Debe ser capaz de colectar todos los eventos enviados por los diferentes sistemas de gestión nativos y almacenarlos en una base cuyo límite debe ser determinado por la cantidad de elementos de red existentes y los proyectados.

Las interfaces entre los sistemas de gestión y la plataforma solución deben estar desarrolladas o por desarrollar en un tiempo no mayor de 3 meses.

- Tratamiento de los eventos reportados

La detección y consolidación de las fallas debe ser en tiempo real, es decir, debe implementarse un protocolo de sincronización en el cual converjan tanto gestores nativos como la plataforma solución, es de hacer notar que para una correcta correlación de fallas es necesario que tanto los elementos de red como su gestor estén conectados a la misma fuente de sincronía con una estampa de tiempo.

- Análisis de la alarma

Debe hacer la correlación de alarmas en los tres niveles: básico (rafaja de eventos, intermitencias), intradominio (dentro de la misma tecnología) e interdominio (diferentes tecnologías y redes), infiriendo la causa-raíz de la falla.

Los umbrales en el primer nivel de correlación pueden ser: por tiempo, frecuencia, grupo, valor o una adaptación de los requerimientos de la empresa.

Detectar la causa-raíz de las fallas, permitiendo visualizar la alarma raíz y las alarmas asociadas al seleccionar la alarma raíz.

A través de la aplicación de las reglas de almacenamiento, establecimiento de umbrales y correlación debe reducirse la cantidad de alarmas presentadas al operador, indicando en la pantalla la prioridad de la alarma de acuerdo al impacto, pudiendo utilizar un etiquetado, que indique la causa-raíz, permitiendo ver en forma inmediata todas las alarmas que generó.

Debe alertar al usuario con problemas confirmados o situaciones que potencialmente podrían generar un problema en la red.

Inferir condiciones anormales y generar alarmas de elementos que no cuenten con acceso directo a un sistema de gestión, por ejemplo, equipos que se encuentren en última milla, esto a través de creación de reglas de correlación de alarmas.

Debe ser capaz de mostrar el avance en la solución de la falla.

- Soporte a la operación

Debe permitir la automatización del tratamiento de fallas recurrentes o periódicas que requieren tomar el mismo tipo de acción.

Capacidad de insertar información al evento o falla, para dar soporte a la operación.

Priorización de las alarmas de acuerdo con políticas de la empresa.

- Estadísticas y reportes

Acceso a información retrospectiva o en tiempo real, sobre el comportamiento de dispositivos, enlaces o servicios, para la elaboración de reportes de acuerdo con las necesidades de la empresa o estandarizados.

Debe manejar variables como por ejemplo: prioridad de falla, frecuencia de falla, tiempo de solución, cantidad de fallas por tecnología, proveedor, dominios (datos, conmutación, transmisión) áreas geográficas (regiones), por estación (nodo) etcétera.

Elaboración de gráficas con tendencias del comportamiento de la red, de elementos, de servicios, para toma de acciones en la mejora de la calidad del servicio o criterios para el aprovisionamiento de equipos por tecnología y proveedores.

- Notificación

La notificación de las fallas a la parte administrativa de la empresa debe ser en forma automática, escalonada en relación al tiempo y personal involucrado de acuerdo a requerimientos de la empresa, por medio de mensajes al teléfono celular.

- Seguridad

    - Seguridad para el acceso a la información

    - Seguridad en disponibilidad de la plataforma a través de memoria no volátil.

    - Protección de servidor, proponer configuración N+1 hot stand by o en espejo.

    - Copias de respaldo en CD-R y/o cintas magnéticas

- Hadware y software

Proponer capacidad y tipo de servidor, de acuerdo con la cantidad de eventos reportado por cada SGN.

    - Sistema Operativo sobre Unix
    - Interfaz gráfica usuario puede ser Open view, Motif o mejor
    - Indicar cantidad de NE soportados o S.O.
    - Indicar cantidad de alarmas simultáneas que puede procesar

- Debe evolucionar según se requiera actualizar los reléase de NE o S.O que lo alimentan.

Capacidad para crecer con otros S.O.

- Soporte técnico

Asistencia a la operación del sistema de gestión integrada de fallas, como mínimo un año.

El soporte técnico debe tener un horario de atención de 7 x 24 horas, con disponibilidad de personal que hable español.

El plazo mínimo para mantener soporte técnico de la plataforma de software debe ser 3 años.

El proveedor de hardware debe mantener la vigencia de la plataforma de cómputo por un período mínimo de 3 años.

- Garantía

Debe establecerse un tiempo máximo para solución de reclamos. El tiempo que se exceda de este plazo no se computará como tiempo corrido para la garantía.

Tiempo mínimo de garantía 2 años.

- Capacitación

El servicio de asistencia indicado anteriormente, debe considerar la capacitación del personal.

Entrega de un juego de manuales de hardware y software en disco compacto y una copia de respaldo en idioma español.

Entrega de un juego de manuales de hardware y software impreso en idioma español.

- Tiempo de implementación

Tiempo máximo de implementación de la solución 5 meses.

- Presentación de la propuesta

    - Detalle de la propuesta
    - Interfaces que deben desarrollarse (en base al resumen de sistemas de gestión).
    - Interfaces con las que cuentan
    - Tiempo total de desarrollo
    - Soporte
    - Costos detallados
    - Costo total

1.2. Análisis de la situación previa a la implementación de la herramienta

Como se mencionó con anterioridad, una arquitectura típica de una red de telecomunicaciones estará compuesta por redes de diferentes tecnologías, por ejemplo ATM, SDH, PDH, conmutadores, redes IP, etcétera, implementadas con diferentes proveedores, prestando diferentes servicios como voz, datos o video.

Siguiendo una arquitectura de gestión de redes, según recomendaciones internacionales, estará compuesta por elementos de red (NE), así como los sistemas de gestión nativos cargados en Sistemas Operativos (OS).

Anteriormente, los SGN se encontraban en los sitios (también llamados Nodos) donde estaban los elementos de red, tal es el caso de centrales de conmutación en donde en el mismo nodo se encontraban los supervisores para dar mantenimiento desde los sistemas de gestión ubicados en el mismo sitio, sin embargo, como mejores prácticas estos sistemas de gestión fueron centralizados en un sólo sitio, donde los supervisores deben acceder remotamente a los elementos de red, por ejemplo, centrales de conmutación, radios, multiplexores, etcétera, solamente en casos en los que es necesario el cambio de hardware o descarga local de software los supervisores se trasladan directamente del nodo donde se encuentra el NE.

Siguiendo con modelos de operación establecidos por organismos internacionales, surge el NOC (Network Operation Center) sitio donde están instalados todos los sistemas de gestión y los supervisores de los mismos, desde este sitio se hacen las notificaciones, asignaciones y escalamientos de las fallas, se crea un mejor manejo de la atención de las fallas y estadísticas de comportamiento de las redes lo que facilita la operación.

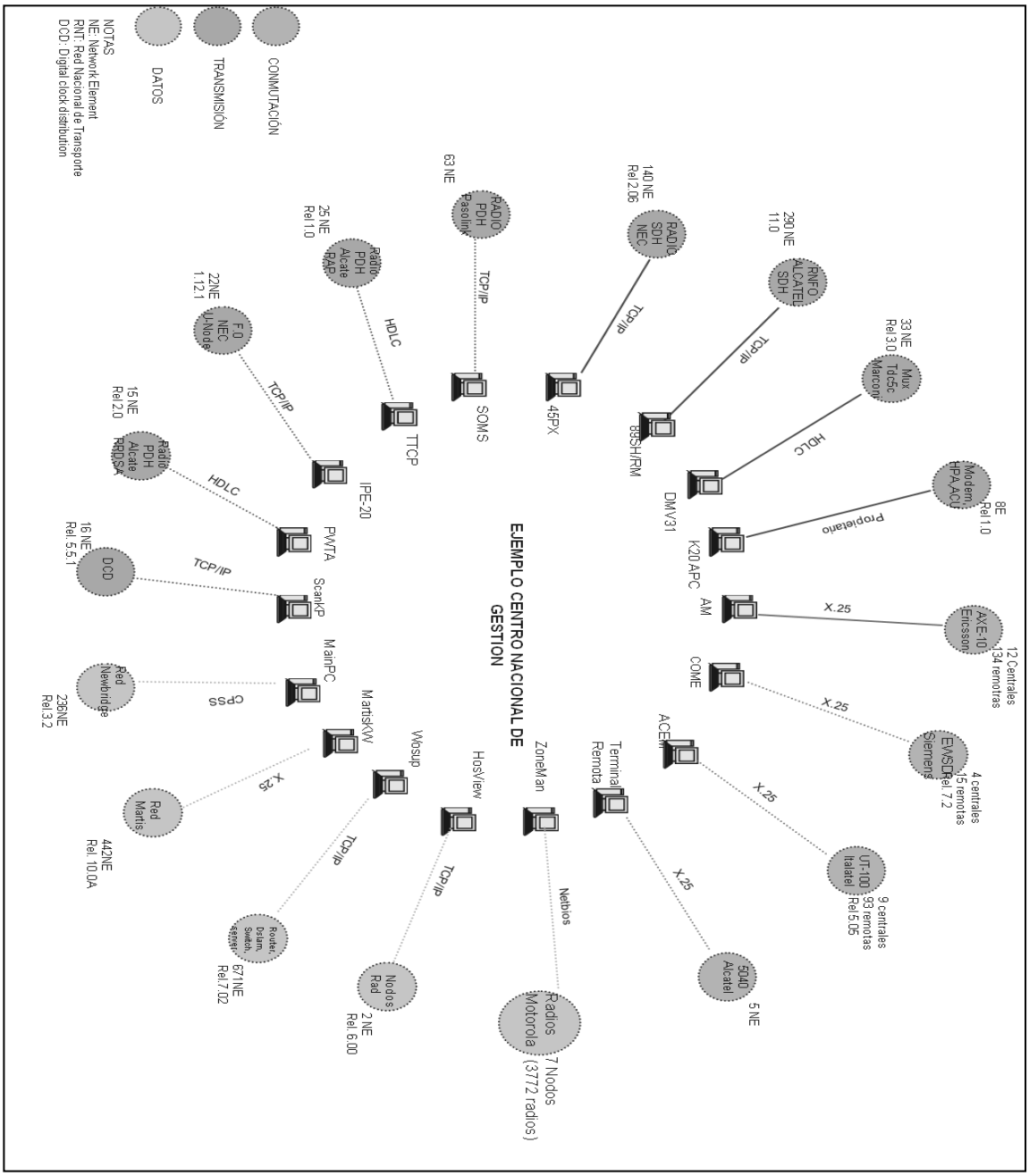
Con todo esto, las redes implementadas con múltiples tecnologías, múltiples proveedores y múltiples protocolos hacen la tarea de atención de fallas más complejo, ya que al estar completamente aisladas las redes de gestión, el tiempo de inferir el efecto de una falla en una red sobre otra, aumenta el tiempo medio de solución de la misma.

1.2.1. Arquitectura actual de la red de gestión

A continuación se describen varias redes que típicamente se presentan en empresas de telecomunicaciones. Como se observa en la figura 3, a pesar de que físicamente se encuentran en un sitio para este caso el NOC, en ningún momento se interrelacionan o convergen en un punto, ni son gestionados por un único sistema de gestión.

En la siguiente gráfica se listan las posibles redes de datos, transporte y conmutación, la cantidad de elementos, la aplicación del sistema de gestión nativo y el protocolo de red para comunicarse entre los elementos de red y sus respectivos gestores nativos.

Figura 3. **Sistemas de gestión existentes de un centro de gestión de telecomunicaciones**



Fuente: elaboración propia.

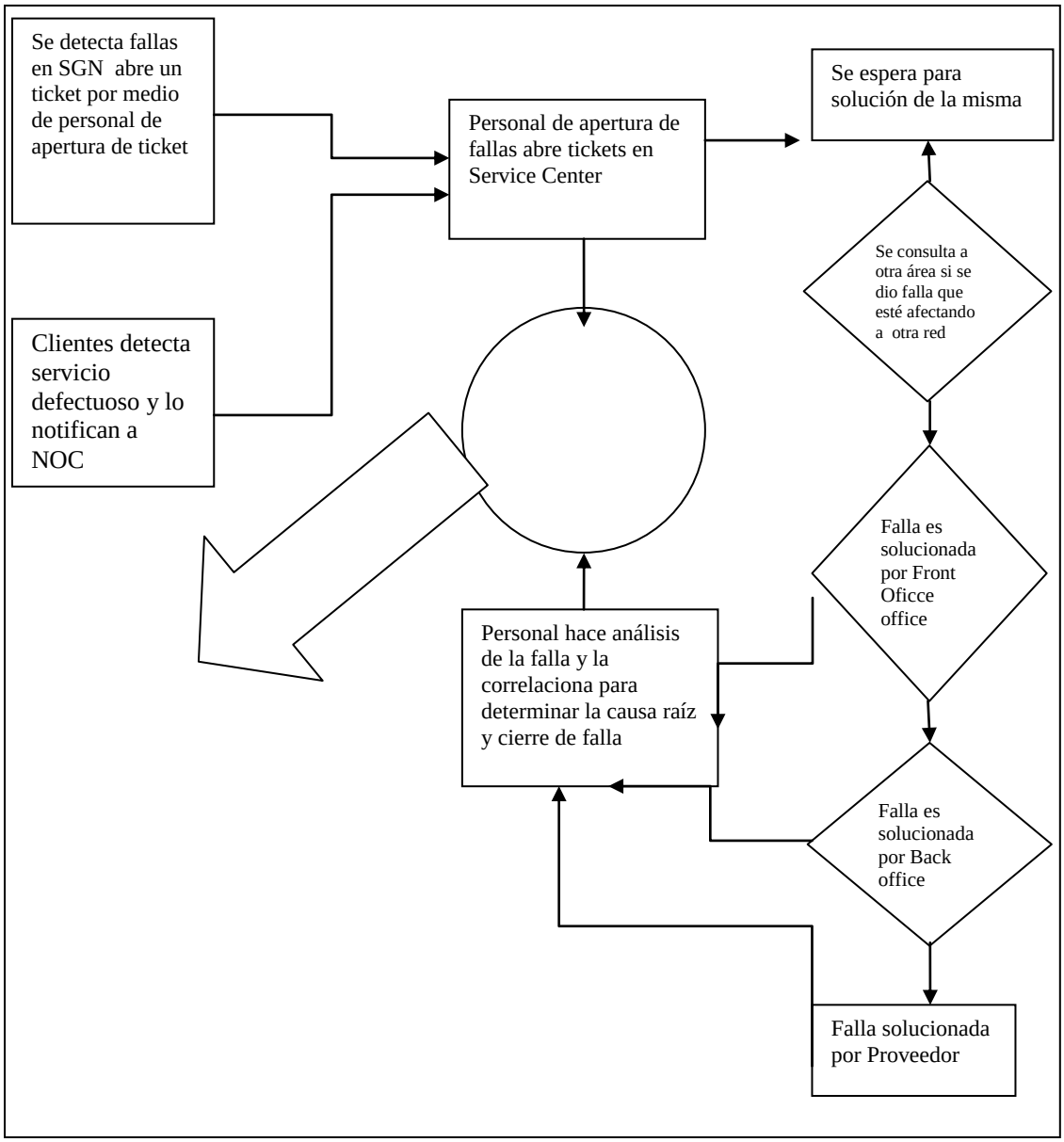
1.2.2. Procesos actuales para atención de fallas

El proceso de atención de fallas que corresponde a una arquitectura como la anterior, donde cada red de gestión es independiente, el proceso de atención sigue el diagrama de flujo de la figura 4, el registro de las fallas es alimentado por aquellas fallas detectadas desde SGN o desde una fuente externa (clientes). Dentro del proceso de registro se llena un documento que describe el tipo de falla, la gravedad, el tiempo en que se detectó, el personal encargado de su solución y finalmente un número asociado a dicha falla para su posterior control y estadísticas.

El personal que detecta la falla la soluciona a través de comandos desde el SGN, si es necesario un cambio de hardware o descarga local de software desde el nodo donde se encuentra el NE se procede a escalar la falla a personal operativo de campo, si no es posible su solución por estos dos frentes de trabajo se procede a escalarlo hacia el TAC del proveedor.

Paralelo a la solución de falla, también se realiza un seguimiento administrativo por parte del personal de Registro de Falla, realizando audio-conferencias y notificando a personal administrativo responsable de las redes afectadas. Una vez solucionada la falla se da por cerrada para posteriores estadísticas.

Figura 4. **Proceso anterior a la implementación de la herramienta para atención de fallas**



Fuente: elaboración propia.

1.2.3. Mediciones de MTT actuales

Es de suma importancia para el cumplimiento de los contratos SLA (Service Level Agreement) o Acuerdo de Nivel de Servicio, que los mismos sean de conocimiento de la parte operativa ya que de la atención y estabilidad de la red recae directamente en la atención a la operación.

Esto hace que se tomen todas las medidas necesarias para cumplir con estos contratos, ya que implican tiempo en que el servicio dejará de prestarse. Cuando la solución de las fallas se hace lenta y engorrosa incide directamente en el SLA y por lo tanto, en pérdidas no sólo de tráfico en general sino multas definidas en dichos documentos.

Para implantar con éxito un SLA han de tenerse en cuenta una serie de factores clave, de los que va a depender en gran medida la obtención de los resultados deseados como la definición de procedimientos estándares y los mecanismos de evaluación y seguimiento.

Para la implantación de un SLA se deben seguir los siguientes puntos:

- Definición de objetivos: mejora de la eficacia, reducción de costes y formalización de la relación.

- Identificar expectativas: qué es lo que espera la organización de este acuerdo.

- Adecuada planificación temporal.

- Optimización/rediseño de procesos (revisar los procesos si el SLA no asegura ningún cambio o como mínimo formalizarlos).

Errores más frecuentes en la implantación

- Definir niveles de servicio inalcanzables
- Regulación excesiva
- Error en la definición de prioridades
- Complejidad técnica
- Irrelevancia (si un SLA no tiene ningún efecto sobre el cliente, el objetivo no tiene sentido).

Un punto importante y que refleja si se está en la correcta dirección de cumplir los acuerdos de SLA es la medición de los MTTR (tiempo medio de atención de fallas):

MTTR = ∑ (tiempo total de inactividad) / ∑(número de fallas)
Tiempo medio significa, estadísticamente, el tiempo promedio.

El Tiempo Medio Para Reparar (MTTR) es el tiempo promedio que toma reparar algo después de una falla.

Es por lo tanto, el MTTR un factor que debe continuamente evaluarse para mejorar proceso o implementar otros que ayuden a mantener las expectativas con los clientes.

Para una empresa con una arquitectura como la vista anteriormente un tiempo medio de solución de fallas puede ser:

Tabla I. **Ejemplo de tiempos por línea de operación**

Tecnología	Tiempo de solución	Tiempo de solución por campo
Cx Fija	28:30	16:48
Datos	10:40	13:15
Movil	50:30	10:41
Sistemas	30:00	No dato
SVA	63:00	06:11
Transporte	43:40	13:07

Fuente: elaboración propia.

En la tabla I se da un ejemplo de los tiempos medios de solución de fallas de un centro de atención de fallas donde no hay correlación de las mismas.

2. COLECCIÓN DE DATOS

2.1. Hardware y software de los gestores nativos y elementos de red

Para el dimensionamiento de SGFRT es necesario contar con la información de cada uno de los sistemas de gestión nativos y de los elementos de red, dicha información puede dividirse en tres secciones:

- Información del sistema de gestión o aplicación
- Información de software (Sistema Operativo)
- Atribuciones de AO&M (Administración, Operación y Mantenimiento)

Información del sistema de gestión*:*

Los sistemas de gestión de los elementos de red, son los OS dentro de una Red de Gestión de Telecomunicaciones, su función es comunicarse con los NE para su administración. Es necesario hacer una recopilación y presentación de la información necesaria para el dimensionamiento de la solución, es importante hacer notar que el ingeniero implementador debe conocer los tipos de redes a ser gestionadas a través de la SGFRT, ya que será necesario el filtrado de las alarmas, para esto debe conocer qué tipos de fallas son generadas por los elementos que forman cada una de las redes.

2.1.1. Red de conmutación

Las redes de conmutación de circuitos fueron diseñadas para tráfico de voz, cuando una persona en un extremo A desea comunicarse con otra en otro punto B, se establece un enlace que reserva los recursos tanto de transporte como de las centrales de conmutación y son mantenidos para el uso exclusivo entre A y B hasta que la conversación es finalizada, a este tipo de enlace se le denomina orientado a la conexión ya que para que esto suceda es necesario previamente establecer la conexión exclusiva entre A y B, aún en los momentos en los que existen silencios el enlace se mantiene, esto hace de este tipo de comunicaciones seguras pero costosas. La transmisión es transparente y simula una conexión de punto.

Las empresas de telecomunicaciones invierten gran cantidad de dinero en la tecnología de las centrales de conmutación, el papel que desempeñan estas centrales también varían de acuerdo con la tecnología comprada y a su función dentro de la red así existen:

- Centrales locales
- Centralestránsito
- Unidad remota

En las redes de conmutación de circuitos, como es la red telefónica pública conmutada (PSTN), se transmiten varias llamadas a través del mismo medio de transmisión. Inicialmente el medio era cobre, pero debido a la creciente demanda y a la facilidad de ampliar el ancho de banda ahora se utiliza fibra óptica.

Para una mejor comprensión se puede hacer la analogía de una red PSTN que una agrupación de las redes telefónicas públicas de conmutación de circuitos del mundo y la red Internet la cual es una agrupación de las redes públicas de conmutación de paquetes basadas en IP del mundo.

VoIP el protocolo de voz sobre Internet (VoIP) es una tecnología que contiene hardware y software que permite el uso de una red basada en IP como el medio de transmisión de las llamadas telefónicas. En VoIP, los datos de voz se envían en paquetes mediante IP en lugar de las transmisiones de circuitos tradicionales o las líneas de conmutación de circuitos de la PSTN.

VoIP en una red de conmutación de paquetes. VoIP comparte el ancho de banda disponible con todas las otras aplicaciones de red y hace un uso más eficaz del mismo, lo contrario que la conmutación de circuitos que hace uso exclusivo de los medios hasta que finaliza la comunicación.

- Redes de conmutación de paquetes

La técnica de conmutación de paquetes divide un mensaje de datos en unidades más pequeñas llamadas paquetes. Estos se envían a su destino siguiendo la mejor ruta disponible y se reensamblan en el extremo de recepción.

En la conmutación de paquetes, utiliza protocolos que no garantizan la entrega del paquete, es decir, no existe una confirmación de la entrega esto debido a que utilizan el protocolo UDP el cual no contempla estos mecanismos, tampoco está orientado a la conexión ya que solamente se establece una vía de entrega o envío del paquete mientras se esté enviando los datos, no como sucede con la conmutación de circuitos en los cuales se esté enviando o no información la conexión se mantiene hasta que cualquiera de los interlocutores cuelga.

En las redes de conmutación de paquetes, como es Internet, los paquetes se direccionan a su destino por la ruta más oportuna, pero no todos los paquetes que viajan entre dos *hosts* siguen la misma ruta, ni siquiera los que pertenecen a un mismo mensaje. Esto prácticamente garantiza que los paquetes llegarán en diferentes momentos y desordenados. En una red de conmutación de paquetes, los paquetes (mensajes o fragmentos de mensajes) se enrutan individualmente entre los nodos en vínculos de datos que pueden estar compartidos por otros nodos.

En la conmutación de paquetes, a diferencia de la conmutación de circuitos, las diferentes conexiones con nodos de la red comparten el ancho de banda disponible y utilizan técnicas de control de acceso al medio. Cuando los paquetes llegan a su destino, un ensamblador de paquetes los vuelve a ordenar. El ensamblador de paquetes es necesario por las diferentes rutas que pueden seguir los paquetes.

En la conmutación de circuitos, todos los paquetes llegan al receptor en orden y por un solo camino.

En una LAN basada en Ethernet, un marco de Ethernet contiene la carga o la porción de datos del paquete y un encabezado especial que incluye la información de dirección de control de acceso de medios (MAC) del origen y el destino del paquete. Las redes de conmutación de paquetes han hecho posible que exista Internet y, al mismo tiempo, ha hecho que las redes de datos, especialmente las redes IP basadas en LAN, estén más disponibles de forma más generalizada.

Tabla II. **Equipos de gestión de centrales de conmutación, información de elementos de red, software y atribuciones AO&M**

	INFORMACIÓN DE EQUIPO DE GESTIÓN				INFORMACIÓN		ATRIBUCIONES AO&M		
No.	Nombre del sistema de gestión	Release	Fabricante	Protocolo entre gestor y elementos de red	Servidor	Sistema Operativo	Promedio de eventos recibidos en un día	Elementos de red gestionados	Reporte de eventos
1	KNOSS-1		ERICSSON	X.25		UNIX	30	CENTRALES DE CONMUTACIÓN Y REMOTA	SI
2	LASEM		ITALTEL	X.25		SUN SOLARIS	20	CENTRALES DE CONMUTACIÓN Y REMOTA	SI
3	ETMANAGE		SIEMENS	X.25		UNIX	8	CENTRALES DE CONMUTACIÓN Y REMOTA	SI

Fuente: elaboración propia.

En la tabla II se da un ejemplo de cómo se puede recopilar la información necesaria para la implementación de la herramienta de gestión de fallas integradas.

2.1.2. Redes de transporte de voz y datos

En teoría para establecer una llamada entre un punto A y un punto B solamente hace falta una central de conmutación entre ambos puntos, sin embargo, en una empresa de telecomunicaciones de gran capacidad existen varias centrales de conmutación que deben intercomunicar a miles de miles de usuarios para que dichas centrales se comuniquen entre sí, son necesarios medios de transporte que hagan uso de la tecnología capaz de lograr el transporte de gran cantidad de enlaces. Es así como surge el área de transporte como una más dentro de las Telecomunicaciones por ejemplo, SDH, PDH, ATM, etcétera.

La transmisión digital tiene más ventajas que la analógica debido a que pueden manipularse más fácilmente (ejemplo: codificación, modulación, multicanalización, compresión, etcétera), por tal motivo la tendencia de las redes de la actualidad es la digitalización gradual de sus sistemas.

- Multiplexación

La multicanalización es la técnica que se utiliza para transmitir varias fuentes de información como voz, datos y vídeo sobre un mismo canal de comunicación. El multicanalizador, frecuentemente llamado mux, es un equipo de comunicación utilizado para este propósito. La principal ventaja de la multicanalización es la de reducir los costos de la red al minimizar el número de enlaces de comunicación entre dos puntos. Los multicanalizadores de la actualidad tienen cada vez más inteligencia y la adicional inteligencia brinda más beneficios.

Una red de transmisión SONET/SDH está compuesta de varios equipos de telecomunicaciones, algunos de los más importantes se enuncian a continuación:

- Multicanalizador Terminal (TM, Terminal Multiplexer)
- Multicanalizador de inserción/remosión (ADM Add-drop Multiplexer)
- Repetidor/Regenerador
- Sistema digital de conexión cruzada (DCS, Digital Cross-Connect)
- Un equipo de la red SDH (multiplexor Add-Drop, terminal de línea óptica o radioenlace, Cross-connect, etcétera) puede visualizarse como una serie de unidades de distintas misiones y funciones.

- ISDN

La red digital de servicios integrados (ISDN, Integrated Services Digital Network) provee acceso a servicios de red de cobertura amplia (WAN, Wide Area Network) sobre redes de conmutación de circuitos basados en líneas de cobre.

- B-ISDN

La red digital de servicios integrados de banda amplia (B-ISDN, Broadband Integrated Services Digital Network) está diseñada para operar sobre una infraestructura de telecomunicaciones basada en sistema de fibra óptica.

Aunque inicialmente fue propuesta como una extensión de ISDN, finalmente la ITU-T definió una serie de estándares para la integración de servicios de voz, datos y video a altas velocidades de hasta 155 Mbps utilizando enlaces SONET/SDH y servicios de conmutación ATM (Asynchronous Transfer Mode). Aunque B-ISDN es totalmente dependiente de los enlaces de fibra óptica, esta tecnología no ha sido ampliamente implementada a la fecha.

- ATM converge a SONET/SDH

ATM es una tecnología orientada a la conexión, en la que las comunicaciones se establecen mediante circuitos virtuales que permiten mantener múltiples comunicaciones con uno o varios destinos.

El Servicio ATM proporciona una multiplexación estadística de diferentes comunicaciones establecidas en circuitos virtuales, permitiendo la compartición de una misma línea de transmisión. Los circuitos virtuales son de carácter permanente.

ATM está diseñado fundamentalmente para aplicaciones de entorno de Red de Área Local, es decir, transporte transparente de datos a alta velocidad, bajo retardo y alto caudal, transporte conjunto de diferentes tipos de tráfico y múltiples protocolos; también permite el transporte de voz y video.

Tabla III. **Equipos de gestión de las redes de transporte, información de elementos de red, software y atribuciones AO&M**

EQUIPOS DE RED DE TRANSPORTE									
	INFORMACIÓN DE EQUIPO DE GESTIÓN				INFORMACIÓN		ATRIBUCIONES AO&M		
NO.	NOMBRE DEL SISTEMA DE GESTIÓN	RELEASE	FABRICANTE	PROTOCOLO ENTRE GESTOR Y ELEMENTOS DE RED	SERVIDOR	SISTEMA OPERATIVO	PROMEDIO DE EVENTOS RECIBIDOS EN UN DÍA	ELEMENTOS DE RED GESTIONADOS	REPORTE DE EVENTOS
1	873SH		Ericsson	TCP/IP		HP-UNIX	1200	EQUIPOS SDH	SI
2	AD654RM		ITALTEL	TCP/IP		HP-UNXI	1200	EQUIPOS SDH	SI
3	SCAN		Siemens	TCP/IP		SUN	25	EQUIPOS SINCRONIA	SI
4	KVN-100			TCP/IP			15	EQUIPOS SDH	SI
5	SMX-10			TCP/IP			140	RADIOS SDH	SI
6	NlMS			TCP/IP			60	RADIOS PDH	SI

Fuente: elaboración propia.

En la tabla III se observa un ejemplo de cómo se puede recopilar la información necesaria para la implementación de la herramienta de gestión de fallas integradas.

2.1.3. Redes de datos

Las redes Ethernet y sus interfaces FE, Gb, 10Gb, etcétera, han venido a sustituir por su gran capacidad de transporte a las redes SDH o SONET, sin embargo, se hizo necesario el uso de *routing* de paquetes para garantizar ciertas entregas, para lo cual el MPLS es una solución a esto.

Con el auge de Internet el protocolo IP (Internet Protocol) se ha convertido en la base de las redes de telecomunicaciones, esto debido a su gran capacidad de transporte y económica implementación en comparación con redes como SDH o SONET. IP es un protocolo de capa de red (nivel 3 OSI) la versión más utilizada en el país es IPv4 especificada en la RFC 791, pese a que es un protocolo no orientado a la conexión y por lo tanto, no seguro para el encaminamiento de paquetes aunque es posible que se utilice junto con TCP (Transmissión Control Protocol) (nivel 4 OSI) para garantizar la entrega de los paquetes.

Conforme se expande el uso de Internet la demanda de calidad de servicio se hace más importante, es por ello, que surge ATM (Asyncronous Transfer Mode) en la capa de enlace (nivel 2 de OSI), ATM utiliza el encaminamiento inteligente de nivel 3 de los *routers* IP en la red de acceso, incrementa el ancho de banda y rendimiento con base a la alta velocidad de los *switch* de nivel 2 y los circuitos permanentes virtuales de los *switch* ATM en la red troncal.

MPLS (MultiProtocol Label Switching) surge para estandarizar el uso de la tecnología ATM e IP, el cual está definido en la RFC 3031. MPLS proporciona los beneficios de la ingeniería de tráfico del modelo de IP sobre ATM, pero además, otras ventajas; como una operación y diseño de red más sencillo y una mayor escalabilidad.

Por otro lado, a diferencia de las soluciones de conmutación de nivel 2 propietarias, está diseñado para operar sobre cualquier tecnología en el nivel de enlace, no únicamente ATM, facilitando así la migración a las redes ópticas de próxima generación, basadas en infraestructuras SDH/SONET y DWDM.

MPLS es un estándar IP de conmutación de paquetes del IETF, que trata de proporcionar algunas de las características de las redes orientadas a conexión a las redes no orientadas a conexión, se establecerá un camino a través de la red MPLS y se reservarán los recursos físicos necesarios para satisfacer los requerimientos del servicio previamente definidos para el camino de datos.

Tabla IV. **Equipos de gestión de datos, información de elementos de red, software y atribuciones AO&M**

	INFORMACIÓN DE EQUIPO DE GESTIÓN				**INFORMACIÓN**		**ATRIBUCIONES AO&M**		
NO.	NOMBRE DEL SISTEMA DE GESTIÓN	RELEASE	FABRICANTE	PROTOCOLO ENTRE GESTOR Y ELEMENTOS DE RED	SERVIDOR	SISTEMA OPERATIVO	PROMEDIO DE EVENTOS RECIBIDOS EN UN DÍA	ELEMENTOS DE RED GESTIONADOS	REPORTE DE EVENTOS
1	Alcatel, Newbridge								
2	Tellabs								
3	Rad Data Comunication								
4	4647AWS								

Fuente: elaboración propia.

En la tabla VI se da un ejemplo de cómo se puede recopilar la información necesaria para la implementación de la herramienta de gestión de fallas integradas.

2.2. Interfaces norte en los gestores nativos

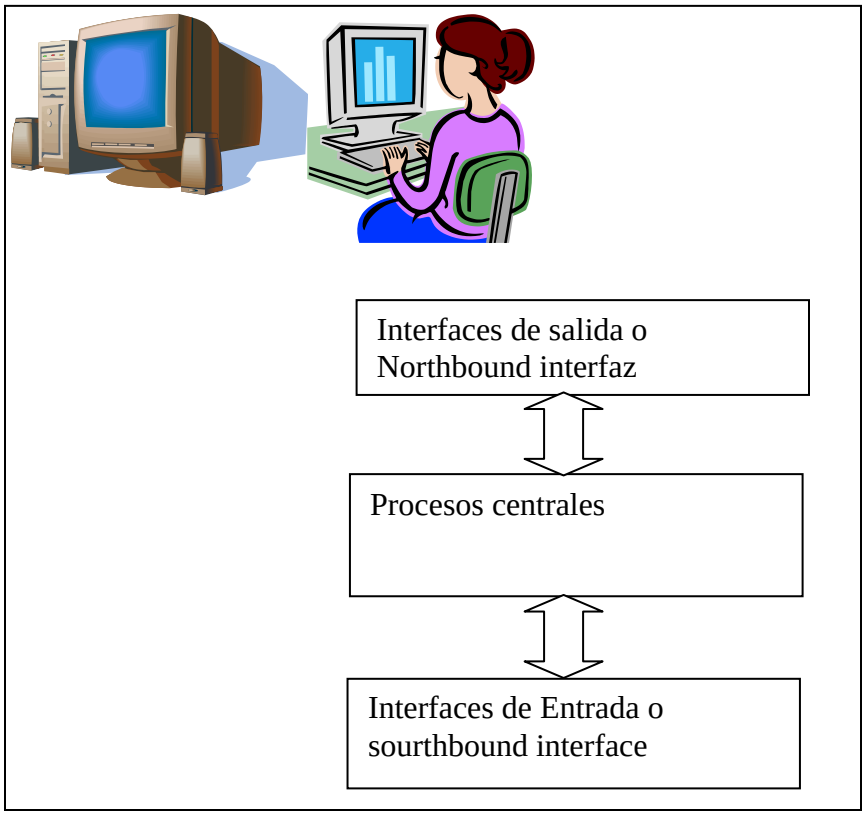
Es necesario que el ingeniero integrador verifique en cada uno de los SGN a integrar en el SGFRT, que exista la interfaz norte para comunicarse con dicha plataforma, dicha interfaz deberá cumplir con los requerimientos que tenga el módulo de accesos del lado del SGFRT. De no existir el software o hardware de la interfaz norte, debe hacerse la compra con el proveedor del equipo gestor.

2.2.1. Clasificación e integración de los gestores nativos o elementos de red a la solución de gestión integrada según interface norte, clasificación por los módulos de acceso con protocolo SNMP o CMIP así como técnicas como ASCII y CORBA

La interfaz en dirección norte o northbound interface, es el software necesario en los SGN para la exportación de las alarmas al SGFRT. Existen interfaces estándares como CORBA para integrar con terceros, estas son llamadas norte porque es el enlace entre todas las conexiones o integraciones con tercero es decir, puertos de salida.

Las interfaces norte establecen comunicación con la unidad central para ejecución de los procesos requeridos.

Figura 5. **Diagrama de relación entre las interfaces norte, centro y sur**



Fuente: elaboración propia.

En la figura 5 se observa el diagrama de flujo de la comunicación entre las distintas interfaces.

A continuación se hace una descripción de las interfaces norte que permitirán la interconexión entre los sistemas de gestión nativos y la plataforma solución que integrará a cada uno. En la tabla V se indican las interfaces norte por tecnología y proveedor que pueden ser encontradas en el mercado.

Interfaz norte CORBA: es un conjunto de especificaciones, gestionadas por OMG (Objet Management Group) cuya finalidad es facilitar la interoperabilidad entre componentes software implementados en cualquier lenguaje y se ejecutan en cualquier sistema y plataforma de hardware, consiste de IDL (Interface Definition Lenguaje), ORB (Objet Request Broker) y GIO (General Inter ORB). Para ver más detalles ver capítulo 3).

CMIP: Common Management Information Protocol, es un protocolo a nivel de capa de aplicación del modelo OSI, sirve para la comunicación entre funciones CMIS, CMIS (CMI Service) ISO -9595. Los servicios aquí definidos se realizan mediante el protocolo de comunicaciones CMIP. Permite cambios de atributos o estado de objetos y recibe reportes de Trap.

El principio de funcionamiento es Gestor-agente y una MIB para la administración de la base de datos. Los siguientes son servicios de este protocolo.

- Event-report
- Get
- Set
- Action
- Create
- Delete

- Cancel_Get

Interfaz norte SNMP: es un protocolo para gestión de elementos de red del mundo IP es el análogo al protocolo CMIP, su principio de funcionamiento es el mismo, es decir, un Gestor, un agente y una base de datos y el uso de consultas entre el gestor y el agente, está basado en el sistema de petición-respuesta.

La arquitectura SNMP consta de los siguientes componentes:

- Gestores (NMS's)
- Agentes (nodos administrados)
- MIB (base de datos con información)
- SMI (administración de la base de datos)
- Protocolos (órdenes)
- El gestor SNMP puede lanzar cualquiera de estos tres comandos sobre un agente SNMP:
  - Get. Una petición por el valor específico de un objeto en la MIB del agente. Este comando es utilizado por el gestor para monitorizar los dispositivos a gestionar.

- Get-next. Una petición por un valor en el siguiente objeto en la MIB del agente. Este comando es utilizado para obtener cada valor sucesivo en un subconjunto o rama de la MIB.

- Set. Utilizado para cambiar el valor de un objeto en la MIB de un agente, en el caso de que el objeto tenga habilitada la lectura y escritura de su valor. Debido a la limitada seguridad de SNMP, la mayoría de los objetos de la MIB sólo tienen acceso de lectura. Este comando es utilizado por el gestor para controlar los dispositivos a gestionar.

- Interfaz norte ASCII

El *toolkit* ASCII es usado para construir los AM GAT y puede administrar cualquier NE usando ASCII-based command language (Bellcore/Telcordia TR-TSY-000833), que es el protocolo para gestión ampliamente usado en telecomunicaciones, siendo un protocolo para línea de comandos, sirve para integrar información de alarmas, estados, controles, desempeño y pruebas en una red de telecomunicaciones, los mensajes son diseñados para ser leídos sin analizador de protocolo, por lo general las plataformas de gestión centralizadas pueden interpretar mensajes en TL1 lo que hace más fácil la integración.

Tabla V. **Cuadro de interfaces norte en sistemas de gestión nativos**

Sistema de Gestión	Proveedor	Red	Interfaz norte (nombre comercial)
Bsem	Italtel	Conmutación	POL
NetDomain	Siemens	Conmutación	BNM
KBoss	Ericsson	Conmutación	BNMSI
478NM	Alcatel	Transporte/SDH/fibra	IOO
467AR	Alactel	Transporte/SDH/fibra	IOO
PNMS	Nec	Transporte/PDH/Microonda	PKN
PSD-134	Nec	Transporte/SDH/fibra	PKN
Scan	Symetricon	Sincronía	IOOA

Fuente: elaboración propia.

En la tabla V se listan ejemplos de las interfaces norte que pueden existir en el mercado para las diferentes tecnologías y marcas.

2.2.2. Catálogos y filtros de fallas, necesarios en las interfaces norte a implementar y definición de severidad de alarmas según políticas de la empresa y recomendaciones internacionales

- Severidad de las fallas

Una falla en una red de telecomunicaciones es aquella que afecta a un NE y que le impide su correcto funcionamiento, el impacto que tenga sobre el servicio prestado por dicha empresa ya sea voz, datos o video es el que determina su severidad.

Dentro de la configuración de gestión de los NE ya vienen definidos los niveles de criticidad así como el texto de la falla y los capos que la describen, por el proveedor del NE los cuales deben estar fundamentados en la REC UIT-T X.733, un ejemplo es la pérdida de señal que es considerada una falla crítica porque afecta el servicio prestado, otro ejemplo sería un módulo de reloj de una central que esté desenganchado de su referencia primaria, también es considerada una falla crítica porque puede ocasionar slip en la red que degraden paulatinamente el servicio.

Estos son casos de fallas en dos diferentes redes la de transporte y la de conmutación. A pesar que los proveedores se basan en las recomendaciones internacionales para definir la severidad de una falla, también puede ser definida y configurada según políticas de la empresa que compra dicho equipo.

Para mantener los acuerdos de servicio con los clientes es importante la inmediata detección de problemas reflejados como degradación del servicio, antes de que ocurran pérdidas de servicio, es necesario tener mecanismos de umbral, como mediciones de tasa de error, esto alerta con cierto intervalo de tiempo al técnico para proceder antes de una falla completa que afecte el servicio.

Para lograr la correlación de fallas entre diferentes equipos, que prestan diferentes servicios, es necesario mantener una presentación del informe de alarmas de forma normalizada, utilizando un conjunto común de tipos de notificación, con parámetros normalizados y definiciones de parámetros, independiente del objeto gestionado, por lo cual los tipos de notificaciones deben ser aplicables a cualquier objeto gestionado.

- Normalización del formato de alarmas necesario para la correlación de las mismas

Debido a que es necesaria la recepción de las alarmas generadas por los diferentes gestores nativos en SGFRT es importante establecer formatos para la presentación y procesamiento de dicha información, por lo que dicha presentación debe fundamentarse en el conjunto de notificaciones genéricas, parámetros y semántica definidos en la REC. UIT-T X.733, notificaciones genéricas:

Para las notificaciones genéricas la REC. UIT-T X.733 define los siguientes términos:

- Tipo de evento
- Información de evento
- Respuesta a evento

Las anteriores notificaciones pueden generar entradas en ficheros de registro cronológico (archivo histórico) de gestión de sistemas. La Rec UIT-T X.721, define una clase de objeto de registro de ficheros a partir del cual se derivan todas las entradas y la información adicional se especifica por los parámetros de información de evento y respuesta a evento.

- Descripción de las notificaciones genéricas

Tipo de evento: este parámetro da una clasificación de la alarma y puede indicarse cinco categorías básicas:

- Tipo de alarma de comunicaciones: se asocia con los procedimientos o procesos para transportar información de un punto a otro, ya que como se indica está relacionado a las comunicaciones.

- Tipo de alarma de calidad de servicio: este tipo de alarma está asociado principalmente con una degradación de la calidad de servicio; obedece a umbrales establecidos según criterios de la empresa o a acuerdos de calidad con los clientes de la empresa.

- Tipo de alarma de error de procesamiento: está relacionado al mundo IT e indica fallo en procesamientos internos de algún sistema.

- Tipo de alarma de equipo: se relaciona con una avería del equipo; ejemplo falla en alguna tarjeta que forma parte del equipo.

- Tipo de alarma de entorno: se asocia con problemas del medio donde se encuentra el equipo, por ejemplo, alta temperatura.

Información de evento: para el informe de los eventos también están especificados los campos que pueden presentarse para dicho informe.

Causa probable: aquí se hace una especificación más detallada de la causa probable de las alarmas. Los valores de la causa probable para las notificaciones se indicarán en la cláusula del comportamiento de la definición de la clase de objeto. Está intrínsecamente relacionado con la clase de objetos gestionados, estos valores se encuentran en la Rec UIT-T X. 721 UIT-T/10165-2ISO. La sintaxis de causas probables normalizadas será el identificador de objetos de tipo ASN.1.

El ingeniero integrador debe ser el encargado de definir la causa probable más específica aplicable según la clase de objeto gestionado.

Problemas específicos: este parámetro identifica otros parámetros, diferentes a los indicados como probable causa y están definidos por el ingeniero integrador para especificar un conjunto de identificadores que deben usarse en clases de objetos gestionados.

Gravedad percibida: según la REC. UIT-T X.733 define seis niveles de gravedad, según sea la afectación del objeto gestionado. Los niveles definidos para utilización con este parámetro obligatorio son:

Eliminado: este parámetro indica la eliminación de una o más alarmas señaladas anteriormente. Esta alarma elimina todas las alarmas para este objeto gestionado que tienen el mismo tipo de alarma, causa probable y problemas específicos (si se dan). Pueden eliminarse múltiples notificaciones asociadas utilizando el parámetro notificaciones correlacionadas (definido más adelante).

Indeterminado: el nivel de gravedad indeterminado indica que el nivel de gravedad no puede determinarse.

Crítico: este nivel de gravedad indica que existe una falla en el elemento de red que afecta su correcto funcionamiento y por lo tanto, afecta el servicio prestado, por lo cual es necesario la intervención del mismo para su restablecimiento, de este tipo de falla es posible que se genere un *ticket* para alertar al operador para su pronta solución.

Mayor: este nivel indica que el elemento de red presenta afectación que degrada el servicio aún cuando no sea completa la pérdida del mismo, también puede ser que la afectación sólo afecte a pocos usuarios, sin embargo, también implica intervención del operador y también puede ser generador de *ticket*.

Menor: para este nivel de falla el elemento de red no ha sido afectado y no afecta corte en el servicio ni parcial ni total, no genera *ticket*, sin embargo, si es necesario tomar una medida correctiva para prevenir mayores daños.

Aviso: el nivel de gravedad aviso indica la detección de una avería posible o inminente que afecta al servicio, antes que se hayan sentido efectos importantes. Deben tomarse medidas para un diagnóstico más detallado (si es necesario) y corregir el problema con el fin de evitar que se convierta en una avería más grave que afecte al servicio.

Información de umbral: este tipo de parámetro se da cuando la alarma se presenta por superación del umbral previamente configurado en el equipo y tiene cuatro subparámetros:

- Umbral activado
- Nivel de umbral
- Valor observado

- Tiempo de reactivación

Notificaciones correlacionadas: es el grupo de las notificaciones con las que se considera que una notificación está correlacionada, es decir, dada una falla en algún elemento de red afecta de forma directa o indirecta a otro elemento de red.

Definición de cambio de estado: este parámetro indica un cambio de estado según se indica en la REC UIT-T X.731.

Atributos supervisados: este parámetro establece los cambios de atributos dados cuando ocurre la falla, es decir, sirve como un monitor que indica qué cambios ha tenido el elemento de red cuando se ha producido una falla en el mismo.

Acciones de reparación propuestas: este parámetro establece las posibles soluciones a la falla presentada y está determinado por el definidor de clase de objeto.

Texto adicional: este parámetro es una descripción adicional de la alarma presentada y es libre de su uso y contenido.

Objetos gestionados: un registro de alarma es una clase de objeto gestionado derivada de la clase de objeto, registro de fichero y registro cronológico de eventos definidos en la REC. X.721 del CCITT | ISO/CEI 10165-2. La clase de objeto registro de alarma representa información almacenada en ficheros registro cronológico como resultado de la recepción de un informe de evento cuando el tipo de evento es uno de los tipos de alarma definidos en esta recomendación Norma Internacional.

- Catálogo de fallas

Es un documento que describe por tecnología y proveedor todas aquellas alarmas que pueden darse en los NE, detalla el tipo, su severidad y describe rápidamente en qué parte del NE se está dando la falla, esto servirá para establecer cuáles de estas alarmas deben ser filtradas y cuáles no dentro de la plataforma solución o SGFRT con base en su grado de severidad y a los requerimientos de la empresa, esto permitirá hacer más fácil su correlación y generación de un TT (Troubled Ticket) o boleta de falla, en el entendido que solamente se requiere generar TT si existe afectación al servicio.

Dicho documento debe estar fundamentado en los documentos entregables de cada proveedor de los NE y sistemas de gestión que describen de forma detallada el funcionamiento de dichos NE.

Otras de las funciones de los catálogos de fallas a realizar por tecnología y por proveedor, será estandarizar la información requerida de la interfaz norte de los sistemas de gestión nativos hacia la interfaz sur del SGFRT, como ejemplos de catálogos ver tablas VI, VII, VIII, para las distintas redes.

Tabla VI. **Catálogo de red de transporte**

GESTOR	**NODO**	**TEXTO ALARMA**	**SEVERIDAD**
Bsem	Ericsson	Server Signal Failure	
Netdomain	Italtel	LossOfFrame	
Kboss	Siemens	ExcessiveBER	
478Nm	Nec	Loss Of Supervisory Channel Frame	
467Ar	Nec	AIS	
Nms	Nec		

Fuente: elaboración propia.

Tabla VII. **Catálogo de red de conmutación**

GESTOR	NODO	TEXTO ALARMA	SEVERIDAD
Mnssis	Ericsson	Central unit alarm	
Msemax	Italtel	Recovery alarm	
Netman	Siemens	Rsu isolation alarm	
		Equipment alarm	
		Switching network alarm	

Fuente: elaboración propia.

Tabla VIII. **Catálogo de red de datos**

GESTOR	NODO	TEXTO ALARMA	SEVERIDAD
Alcatel, Newbridge	Alcatel	MPLS/te	
Tellabs	Tellabs	If down	
Rad Data Comunication	Rad	ospfNbrStateChange>> IP	
893AWS	Alcatel	Pim-5-NBRCHG: neighbor down on interface	
		LDP-5-NBRCHG: LDP Neighbor is down	

Fuente: elaboración propia.

3. ARQUITECTURA DE LA SOLUCIÓN DE SGFRT

En este capítulo se describe la arquitectura y funciones que puede tener un SGFRT no necesariamente tienen que ser los únicos.

El enfoque tradicional de una estructura monolítica para administrar los ambientes convergentes (voz, datos y televisión) ha dejado de ser una solución viable para el futuro, ya que una estructura monolítica duplica en cada computadora todos los elementos que lo conforman: interfaz de usuario, lógica o reglas de negocio y acceso de datos, esto es costoso y el impacto es sobre cada computadora cuando se requiere implementar nuevas tecnologías.

La organización de sistemas, bajo este enfoque, no puede acompañar fácilmente los cambios necesarios para mantener el liderazgo en el mercado. Se torna costoso adaptarse a los cambios de requerimientos y es difícil o en algunos casos es imposible integrar con nuevas aplicaciones.

Tradicionalmente, se considera uno de los dos enfoques para construir los sistemas de soporte a la operación:

- Integraciones *ad-hoc* extremo-a-extremo que dan como resultado sistemas complejos que no pueden evolucionar y que son difíciles de mantener.

- Sistemas suministrados por un único proveedor, que no pueden incorporar funciones no suministradas por este proveedor.

Ambas son limitadas para administrar las redes de la actualidad y no serán capaces de adaptarse para administrar las tecnologías de redes en el futuro.

Las aplicaciones tradicionales de OSS han sido construidas para englobar etapas específicas de los procesos de negocios sin considerar proyectos organizativos de mayor envergadura.

Una herramienta que solucione estas limitaciones se logra atendiendo a una necesidad básica de negocio: integración de aplicaciones enfocadas en los procesos de aseguramiento de servicios (gestión de fallas, TT e inventario).

La plataforma solución o SGFRT debe estar enfocada en una arquitectura en capas o distribuida, que separa la interfaz de clientes, el servidor de aplicaciones que procesa las reglas de negocio y un servidor de datos los cuales serán responsables de la gestión de redes de Telecomunicaciones wireline, wireless, data/IP, deja de ser por lo tanto, una estructura monolítica.

Suministrará un conjunto de funciones de gestión, dando a los operadores del sistema una visualización global de su red y de todas las redes, permitiéndoles activar funciones y operaciones de gestión desde una o múltiples estaciones de trabajo, si fuera necesario crecer en los servidores de aplicación o en la base de datos puede realizarse sin afectar a los clientes, como era con el uso de la estructura monolítica.

3.1. Módulos requeridos, distribución y modularidad

La SGFRT será una solución completa de forma distribuida o en capas porque como se dijo anteriormente estará conformada por:

- Cliente
- Aplicaciones
- Base de datos

Configurada para gestión de sistemas multivendor, multiprotocolo y multiservicios.

EL SGFRT proporcionará un ambiente abierto de desarrollo, es decir, puede interoperar con otros proveedores ya que fundamentalmente los protocolos de comunicación, el modelado de objetos gestionables y las base de información (MBI) están estandarizados según recomendaciones internacionales (ISO/UIT-T), que permite su expansión ya sea con la adición de módulos del proveedor, módulos desarrollados por terceros o módulos desarrollados por el usuario.

Debe ser modular constituido por un conjunto de módulos de gestión consistentes en software dedicado a determinadas funciones, que en conjunto proporcionan capacidades de gestión de fallas necesarias.

Los siguientes son los tres módulos principales:

- Function Module (FM): que permite el procesamiento y almacenamiento de información.

- Presentation Module (PM): que representa a las interfaces con los usuarios.

- Access Module (AM): que representa a las interfaces con la red administrada.

Cada módulo funcional está relacionado y se comunica a través de API, dentro de las características generales de la plataforma solución proporciona un directo control de las redes de trabajo a través de las interfaces norte de los OS gestionados y sur (o AM) de la plataforma, pudiendo también gestionar directamente los elementos de red, por lo tanto, da la arquitectura para la red de administración a un nivel más alto que los OS que se comunican directamente con los NE que forman las redes de trabajo, proporciona en forma general las siguientes funciones:

- Administración de las funciones relacionadas con la administración de las fallas y el reporte de afectaciones o problemas.

- Administra las funciones y procesos específicos para cada módulo que lo conforma.

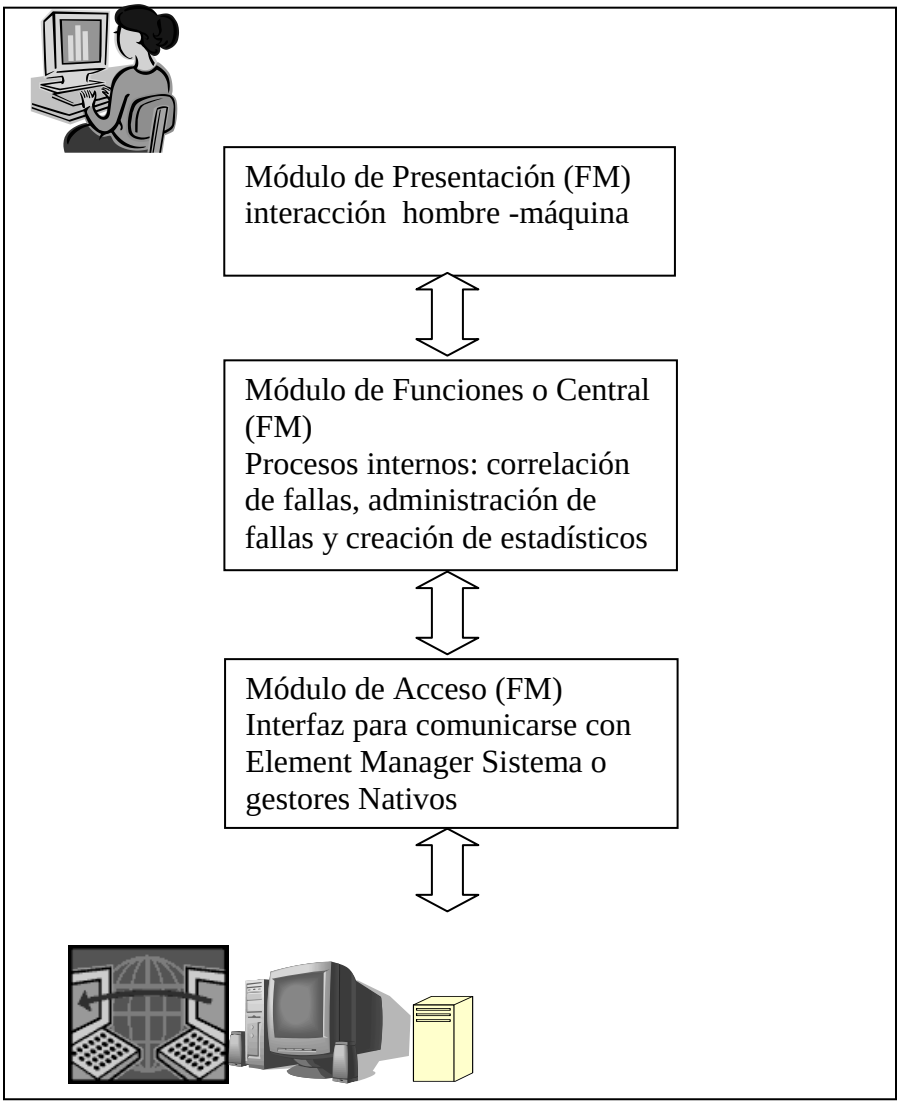
- Una interfaz gráfica para facilidad del usuario.

- Administración de elementos de red a través de sus gestores nativos o directamente a los elementos de red.

- Puede integrar nuevos módulos.

- Trabajar con otras aplicaciones de otros proveedores por utilizar sistemas abiertos.

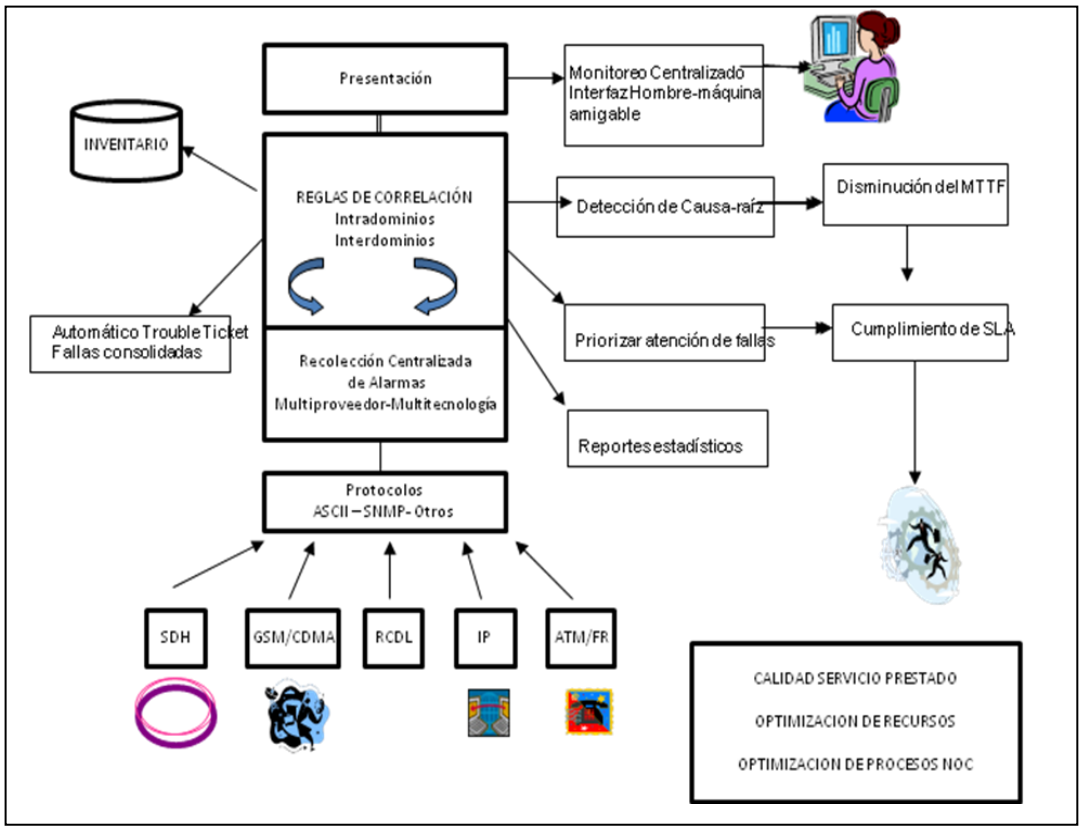
Figura 6. **Diagrama de flujo del SGFRT**



Fuente: elaboración propia.

En la figura 6 se muestra el diagrama de flujo del SGFRT

Figura 7. **Arquitectura de la SGFRT**



Fuente: elaboración propia.

En la figura 7 se muestra la arquitectura de la SGFRT, con todas las funciones requeridas.

3.1.1. Módulo de interfaces sur AM´s o submódulos de recolección de alarmas (AMs)

La frontera sur del SGFRT, abarca el conjunto de dispositivos de conexión con la red a gestionar. Estos dispositivos tienen la función principal de establecer la conexión hacia cada punto de las redes a ser monitoreado (a través de los SGN), una vez establecido, monitorear los eventos que ocurren, enviándolos a los módulos de aplicación. Estos dispositivos de comunicación soportan diferentes diálogos entre la aplicación que reside en la capa de núcleo (representa el módulo funcional) y la red.

La interfaz con la red también es llamado Módulos de Acceso (AM), esto módulos son distintos según el protocolo que se utilice y son responsables por el establecimiento y mantenimiento de la conexión con el elemento manejado y por la traducción de los mensajes recibidos en forma propietaria (si fuera el caso de un gestor nativo antiguo) a una forma patrón según REC. UIT-T X.733 (relativa al formato de las alarmas generadas por el sistema). Pueden tener funciones también de recolección de datos de desempeño o de envío de comandos, según su programación.

A continuación se listan varias aplicaciones comerciales de gestión de las áreas de datos, voz y transporte, para las cuales ya existen módulos de acceso disponibles en el mercado.

- LMEM Italtel
- Siemens Doctmanager
- Ericsson KMN-PSS
- Alcatel 8953PM
- Alcatel 4589M

- Simmetricon SKcan
- NEC PLINC-120
- NEC 589X
- NEC LOMS
- Alcatel 980
- Rad Data Radview
- Alcatel AWS892
- UT STARCOM
- Cisco

Ya que este módulo es responsable del manejo y traducción de los mensajes recibidos desde las interfaces norte de los gestores nativos, es aquí donde se hace la estandarización y modelado de las alarmas para posterior proceso interno de la herramienta, debe tomarse en cuenta que la información recibida en los AM ya se encuentra estandarizada a través de sus MIB , lo cual simplifica el manejo y modelado (entendiéndose como modelado la creación de la MIB propia de la plataforma de gestión) de esta información dentro de la herramienta para su posterior procesamiento.

El proceso de comunicación entre el SGFRT y los elementos de red se trata en un principio de la arquitectura de gestión más básica, esto es, el sistema gestor/agente, es decir, en este caso el gestor envía un mensaje al agente y este contesta.

Por lo tanto, el principio de funcionamiento para la herramienta está basado en el principio gestor/agente definido en la REC. UIT-T M3010, sin importar el tipo de protocolo de comunicación que se utilice para este fin.

- El papel de gestor corresponde a lo(s) centro(s) de control de red y el de agente a los sistemas gestionados.

- Un gestor solicita información o solicita la ejecución de comandos a los sistemas gestionados.

- El agente interacciona con el gestor y es responsable de administrar los objetos de su sistema.

Es también en este módulo donde deben intercomunicarse con los gestores nativos a través de diferentes protocolos de comunicación estandarizados, como el SNMP, CORBA, ASCCII, CMIP los cuales fueron descritos en el capítulo 2, estos son aplicables también para las interfaces norte de los gestores nativos o SGN a integrar a la plataforma, a continuación se describen las propiedades habilitadas en la plataforma solución.

A través del SGFRT pueden ser personalizadas de las herramientas para cada uno de los módulos de acceso:

- Internet SNMP *toolkit*
- Osi *toolkit* (CMIP)
- Corba *toolkit*
- Graphical Asccii *toolkit*
- C++ development *toolkit*

La parte servidora de SNMP consiste en un software SNMP gestor, responsable del sondeo de los agentes SNMP para la obtención de información específica y del envío de peticiones a dichos agentes solicitando la modificación de un determinado valor relativo a su configuración.

Es decir, son los elementos del sistema de gestión ubicados en la plataforma de gestión centralizada de red, que interaccionan con los operadores humanos y desencadenan las acciones necesarias para llevar a cabo las tareas por ellos invocadas o programadas.

La parte cliente de SNMP consiste en un software SNMP agente y una base de datos con información de gestión o MIB. Los agentes SNMP reciben peticiones y reportan información a los gestores SNMP para la comunidad a la que pertenecen; siendo una comunidad, un dominio administrativo de agentes y gestores SNMP. Es decir, son los elementos del sistema de gestión ubicados en cada uno de los dispositivos a gestionar, e invocados por el gestor de la red.

El principio de funcionamiento reside, por consiguiente, en el intercambio de información de gestión entre nodos gestores y nodos gestionados. Habitualmente, los agentes mantienen en cada dispositivo gestionado información acerca de su estado y su configuración. El gestor pide al agente, a través del protocolo SNMP, que realice determinadas operaciones con estos datos de gestión, gracias a las cuales podrá conocer el estado del recurso y podrá influir en su comportamiento.

Cuando se produce alguna situación anómala en un recurso gestionado, los agentes, sin necesidad de ser invocados por el gestor, emiten los denominados eventos o notificaciones que son enviados a un gestor para que el sistema de gestión pueda actuar en consecuencia.

El gestor SNMP puede lanzar cualquiera de estos tres comandos sobre un agente SNMP:

- Get. Una petición por el valor específico de un objeto en la MIB del agente. Este comando es utilizado por el gestor para monitorizar los dispositivos a gestionar.

- Get-next. Una petición por un valor en el siguiente objeto en la MIB del agente. Este comando es utilizado para obtener cada valor sucesivo en un subconjunto o rama de la MIB.

- Set. Utilizado para cambiar el valor de un objeto en la MIB de un agente, en el caso de que el objeto tenga habilitada la lectura y escritura de su valor.

Debido a la limitada seguridad de SNMP, la mayoría de los objetos de la MIB sólo tienen acceso de lectura. Este comando es utilizado por el gestor para controlar los dispositivos a gestionar.

Por otro lado, un agente SNMP podría también mandar un mensaje a un gestor SNMP sin el envío previo de una solicitud por parte de este. Este tipo de mensaje es conocido como trap. Los traps son generalmente enviados para reportar eventos, como por ejemplo, el fallo repentino de una tarjeta del dispositivo gestionado.

El protocolo SNMP debe tener en cuenta y ajustar posibles incompatibilidades entre los dispositivos a gestionar. Los diferentes ordenadores utilizan distintas técnicas de representación de los datos, lo cual puede comprometer la habilidad de SNMP para intercambiar información entre los dispositivos a gestionar. Para evitar este problema, SNMP utiliza un subconjunto de ASN.1 (Abstract Syntax Notation One) en la comunicación entre los diversos sistemas.

El corazón del modelo SNMP es el grupo de objetos administrados por los agentes y leídos y escritos por la estación administradora. Para hacer posible la comunicación multiproveedor, es esencial que estos objetos se definan de una manera estándar. Por esta razón, se requiere un lenguaje de definición de objetos estándar, así como reglas de codificación. El lenguaje usado por el SNMP se toma del OSI y se llama ASN.1 (Abstract Syntax Notation One), Notación de Sintaxis Abstracta uno.

Una sintaxis de transferencia ASN.1 define la manera en que los valores de los tipos ASN.1 se convierten sin ambigüedad en secuencia de *bytes* para su transmisión (y se decodifican sin ambigüedad en el otro terminal). La sintaxis de transferencia usada por el ASN.1 se llama BER (Basic Encoding Rules), Reglas Básicas de Codificación.

La principal ventaja de SNMP para los programadores de herramientas de gestión de red, es su sencillez frente a la complejidad a CMIP. De cara al usuario de dichas herramientas, CMIP resuelve la mayor parte de las muchas limitaciones de SNMP, pero por contra, consume mayores recursos (alrededor de 10 veces más que SNMP), por lo cual es poco utilizado en las redes de telecomunicaciones empresariales.

La limitación más importante de SNMP es que carece de autentificación, lo cual supone una alta vulnerabilidad a varias cuestiones de seguridad, como por ejemplo: modificación de información, alteración de la secuencia de mensajes, enmascaramiento de la entidad emisora, etcétera. En su versión original, cada gestor y agente es configurado con un nombre de comunidad, que es una cadena de texto plano.

Los nombres de comunidad, enviados junto a cada comando lanzado por el gestor, sirven como un débil mecanismo de autentificación, puesto que el mensaje no está cifrado, es muy sencillo que un intruso determine cuál es dicho nombre capturando los mensajes enviados a través de la red. Cuando un agente SNMP captura una petición SNMP, primero comprueba que la petición que le llega es para la comunidad a la cual pertenece.

Solamente en el caso de que el agente pertenezca a dicha comunidad o bien consulta en la MIB el valor del objeto solicitado y envía una respuesta al gestor SNMP con dicho valor en el caso de un comando Get o bien cambia el valor en el caso de un comando Set. CMIP, por trabajar en modo conectado, ofrece una mayor seguridad que SNMP.

SNMP sólo define el protocolo para el intercambio de información de gestión entre el gestor y el agente y el formato para representar la información de gestión o MIB. Por ello, para facilitar la gestión de red, es conveniente adquirir un gestor de red gráfico multifabricante basado en SNMP, utilizando plataformas comerciales como: OpenView de Hewlett Packard (que es el producto más representativo con más de un 40% de cuota de mercado), SunNet de Sun Microsystems, NetView de IBM, etcétera. Muchas veces, estas plataformas multifrabricante, suelen convivir con otras plataformas de gestión de red monofabricante, con el fin de aprovechar al máximo los desarrollos propios y particulares de cada proveedor.

Por medio de este módulo se integrarán todos aquellos elementos de red como *host*, gateways y *router*, para lo cual utilizarán lo siguiente:

- SNMP
- MIB II

- Los eventos son transferidos por SNMP traps para lo cual se hace uso del IST Internet SNMP toolkit, que soporta:

    - Agente proxy
    - Multiple IP addreses
    - SNMP parameters
    - IP- POLLER
    - Polls el equipo y genera alarmas cuando encuentra cambios
    - TRAP DISPATCHER

Convergencia en la Administración de Telco e IP, esto permite la gestión unificada de alarmas de estas dos redes, siempre y cuando los equipos de Telco sean gestionados a través del protocolo SNMP, lo cual está siendo más frecuente por la expansión del uso de este protocolo.

Los beneficios que se obtienen de realizar este tipo de gestión son los siguientes:

- Modelización del objeto
- SNMP trap para el traslado de alarmas hacia la plataforma solución
- Acceso directo a agente proxy
- Propagación de alarmas
- Personalización
- Estatus y correlación de alarmas
- Autodescubrimiento y autoconfiguración: inventario y topología

OSI *toolkit*

Para la gestión de sistemas, OSI establece para el intercambio de información de gestión el protocolo CMIP (Common Management Information Protocol) o Protocolo Común de Información de Gestión el cual proporciona el Servicio CMIS (Common Management Information Service), Servicio Común de Información de Gestión). Este protocolo está orientado a la conexión por lo que hace segura la información intercambiada.

Es importante anotar que CMIP puede utilizar otras pilas de protocolos como CMIP over TCP (RFC 2126).

Los grupos de servicio que integra CMIS son:

- Servicios de notificación. Únicamente hay un servicio de este tipo: M-EVENT-rEPORT, que permite a los agentes informar a los gestores de determinados sucesos especiales en los objetos gestionados que mantienen, permite una gestión orientada a objetos.

- Servicios de operación. Hay seis servicios de operación, son usados por el gestor para invocar operaciones de gestión a los agentes y para devolver los resultados de esas operaciones a los gestores. Estos servicios son: M-GET, M-SET, M-ACTION, M-CREATE, M-DELETE, M-CANCEL-GET.

Para OSI el modelo de información se basa en el concepto de objeto gestionado, lo cual es la abstracción de los recursos o elementos de red gestionados. De la misma manera se definen clases de objetos gestionados como el conjunto de objetos que tienen las mismas propiedades, esto con el fin de su procesamiento en el sistema de gestión. Para llevar a cabo la especificación de las clases de objetos gestionados OSI utiliza la sintaxis GDMO (Guidelines for the Definition of Managed Objects), Directrices para la Definición de Objetos Gestionados. GDMO se basa en la utilización de unas plantillas.

Abstract Syntax Notation (ASN.1) para la codificación y decodificación de unidades de protocolo CMIP (PDUs). Por ejemplo, existe una versión de CMIP sobre protocolos TCP/IP denominada, CMOT (CMIP over) o bien el caso de una versión de CMIP sobre protocolos IEEE de LANs denominada CMOL.

El toolkit OSI es usado para la construcción del AM que utiliza este tipo de protocolo, el cual monitorea y administra los NE usando el protocolo IS/CMIP (Standard Common Management Information).

CORBA toolkit

CORBA es una tecnología cuyas bases y administración son definidas por el OMG (Objet Management Group), satisface las necesidades de comunicación entre un cliente y el servidor para la aplicación de determinados servicios por lo que utiliza una de las tres técnicas existentes para dicho fin (mensajes, llamadas remotas y objetos distribuidos). El desarrollador no gestiona mensajes o llamadas a procedimientos individuales sino que obtiene referencias a objetos, pudiendo llamar a métodos, obtener y establecer propiedades.

Su finalidad es facilitar la interoperabilidad entre componentes de software independientemente del lenguaje de programación en que están desarrollados, la plataforma hardware y el Sistema Operativo sobre el que se ejecute.

Esta tecnología está básicamente compuesta por:

- IDL: Interface Definition Lenguaje, no es un lenguaje de programación como Java, C++, Cobol, sino un lenguaje descriptivo, como se indica sirve para describir interfaces, los parámetros necesarios y el tipo de valor que devolverán, existen compiladores propios de cada lenguaje que interpretarán el leguaje del servidor y el cliente.

- Básicamente sirve para llevar a un lenguaje descriptivo lo que se quiere trasladar del cliente al server o viceversa, es independiente del lenguaje de programación, sin embargo, utiliza compiladores IDL que realmente no son compiladores (no generan código ejecutable) sino sirven para traducir la descripción IDL a un lenguaje específico por lo que sí son propios de cada lenguaje, habiendo diversidad de ellos.

- ORB: Objet Request Broker encargado de traducir la llamada del cliente realizada en determinado lenguaje y sobre una determinada plataforma lo traduce a un formato neutro, totalmente independiente que se pueda transportar sobre cualquier medio. Sin embargo, tanto el cliente como el servidor cuentan con un ORB adaptado a sus necesidades, es decir un ORB específico al leguaje utilizado.

- IIOP: Internet Inter-ORB protocol determina cómo deben comunicarse entre dos ORB, indica qué servicios existen y cuáles son las conexiones utilizadas TCP/IP para transporte.

El CORBA toolkit es utilizado para la construcción del AM CORBA, para interactuar con CORBA objets, el toolkit incluye:

- CORBA AM MSL from IDL and delta IDL
- Librería override C++classes and funciones
- Colección de eventos soporta la colección de eventos para el mundo de CORBA.

GRAPHICAL ASCII Toolkit (GAT)

El toolkit ASCII es usado para construir los AM GAT y puede administrar cualquier NE usando ASCII-based command language (Bellcore/Telcordia TR-TSY-000833), que es el protocolo para gestión ampliamente usado en telecomunicaciones, siendo un protocolo para línea de comandos, sirve para integrar información de alarmas, estados, controles, desempeño y pruebas en una red de telecomunicaciones, los mensajes son diseñados para ser leídos sin analizador de protocolo, por lo general las plataformas de gestión centralizadas pueden interpretar mensajes en TL1 lo que hace más fácil la integración.

Soporta diferentes protocolos de transporte: X25, TCP/I¨P, RS232, Telnet, además soporta especificas funciones: Polling ( ), Keep alive ( ), Heartbeat ( ) y resincronizacion ( ).

- Licencias de Módulos de Acceso (AM)

Los módulos de acceso (AMs) proveen el mapeo de protocolos entre los Network Elements o Management Systems y el mundo estándar del SGFRT donde se encuentran los AMs.

Se pueden clasificar los módulos de acceso, en función de criterios tales que los protocolos de comunicación, la complejidad del modelo de información, el número de alarmas/eventos mapeados, etcétera.

A continuación se dan algunos ejemplos de la clasificación por los módulos de acceso con protocolo SNMP y ASCII.

Tabla IX. **Para los módulos de acceso SNMP con funcionalidad de fallas simples**

Consideraciones generales	• Una MIB específica • Número de líneas de las MIB o combinaciones de archivos de MIBS < 500. • Número de traps < 10 • Clases jerárquicas < 10 niveles (empezando del nodo enterprise 1.3.6.1.4.1). • Se asume que la MIB tiene una sintaxis correcta ASN.1
Modelado	• No se crea una clase global
Funcionalidad	• Mapeo de las alarmas de acuerdo a los campos de eventos OSI (usando los variables de los traps).
Conectividad	• Configuración de agente (proxy)
Documentación	• Instalación y configuración • Especificación funcional • SDP (Software Product Description) • Releases notes

Fuente: elaboración propia.

Tabla X. **Para los módulos de acceso ASCII con funcionalidad de fallas simples**

Consideraciones Generales	• Documentación sobre el acceso a los elementos de red o a sus gestores. • Definición clara del modelo del equipo del proveedor. • Acceso a un Log de alarmas reales • La estructura del mensaje debe ser clara
Modelado	• Limitado a un número de clases < 5 (una global y el resto subclases).
Funcionalidad	• Solamente es fallas • Número de alarmas tipo a procesar < 15 • No existe resincronización • Permite la duplicación de alarmas • No procesos de heartbeat o Keep Alive • No tiene comandos, ni para configuración
Conectividad	• Se puede usar una comunicación estándar (sólo TCP/IP) (No debe venir caracteres binarios en los mensajes, ni caracteres de control).
Documentación	• Instalación y configuración • Especificación funcional • SDP (Software Product Description) • Releases Notes

Fuente: elaboración propia.

En la tabla siguiente se describen los módulos de accesos con su clasificación en función de la información que se recolectó durante el proceso de investigación (los datos son ficticios).

Tabla XI. **Módulos de acceso**

Tipo de Red	Sistema de gestión	Interfaz	Disponibilidad	Disponibilidad plataforma	Requisito
Voz	SiemensXY1	SNMP	Si	Si	SNMP agente disponible y configurado
Transporte	Alcatel 5879UX	ASCCI	Si	No (desarrollo)	Interfaz disponible y configurada
Datos	Cisco 21K	CORBA	CORBA	Si	Instalación y configuración

Fuente: elaboración propia.

3.1.2. Módulo central

Los módulos funcionales (FM) son responsables por el procesamiento de todas las informaciones recibidas por los AM y proveen las funciones básicas para la recepción, manejo y almacenamiento de alarmas. Nuevos módulos pueden ser agregados a un sistema en producción a cualquier momento. Esta flexibilidad permite un crecimiento de la solución adecuado al crecimiento de la red.

La capa central de aplicaciones que reside en el núcleo de la arquitectura contiene los módulos que procesan la información proveniente del adaptador de interfaces en la frontera Sur de la solución y también soportan las interfaces de operación. En términos de configuración el centro puede estar equipado con los módulos para procesamiento de alarmas, creación de filtros, perfiles de usuario, entre otros.

Es el corazón del sistema y está constituido por:

- Kernel que proporciona las funciones de Sistema Operativo de la solución.

- Un conjunto de capas distribuidas de módulos de administración (Management Modules) que se comunican entre sí mediante una API.

- Una base de datos

Funciones generales del Módulo de Funciones (FM):

- Administración de fallas y problemas

- Proceso de modelado de la información

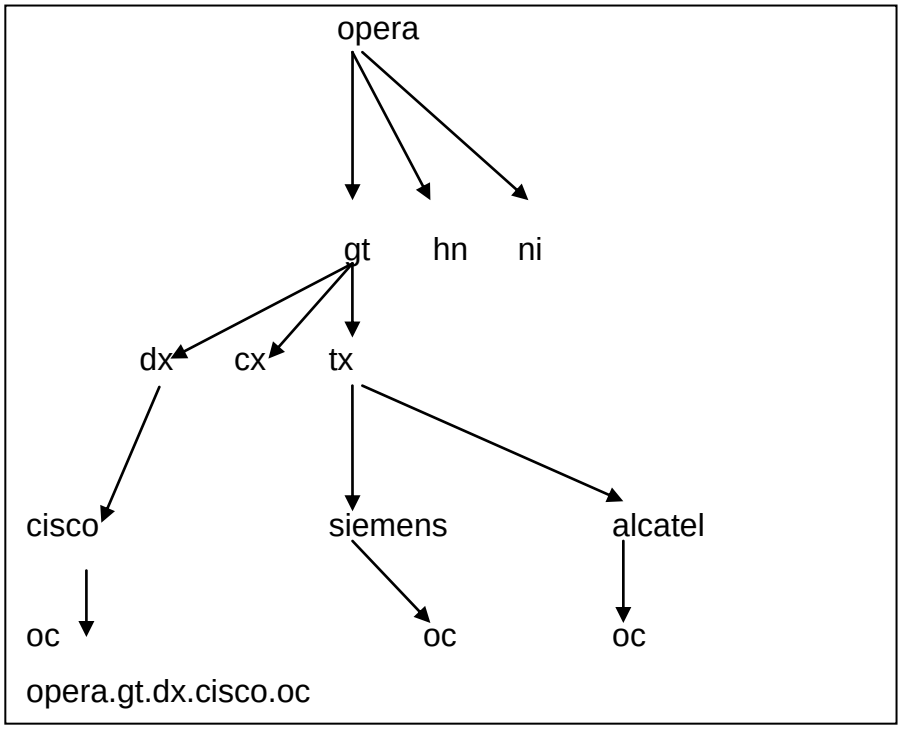
La definición de las clases de objetos gestionados se realiza utilizando el estándar GDMO (X.722), que proporciona una sintaxis con la que se especifican las MIBs de los equipos TNM.

GDMO es un metalenguaje de plantillas (templates) simple (ISO 10165-4), basado en ASN.1 (ISO 8824). Es utilizado para describir las Clases de Objetos Administrables (MOCs) en el modelo de información de la arquitectura de administración OSI. GDMO especifica el formato y los lineamientos para las definiciones de las MOC. En las definiciones de plantilla se puede hacer referencia a otras (definiciones de) plantillas.

Clases de objetos: la plantilla managed object class es el nivel más alto; otras plantillas pueden ser utilizadas para definir esta de manera más exacta utilizando una descomposición descendente (por ejemplo, la clase está compuesta por paquetes (o particiones), el paquete o partición está compuesto por atributos, notificaciones, comportamientos y parámetros).

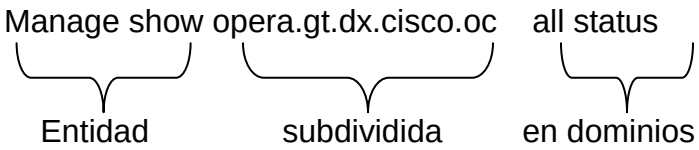
Las clases o entidades, se pueden subdividir en dominios, puede ser cualquier grupo de criterios, tipos de redes, geográficos, technical, funciones, etcétera), esto en la telecomunicaciones o administración de redes es común realizarlo para facilidad de la administración.

Figura 8. **Ejemplo de una MIB**



Fuente: elaboración propia.

Ejemplo:



La Clase de objetos gestionados viene dado por:

- Los atributos que posee
- Las operaciones que pueden ejecutar sobre él
- El comportamiento que presenta
- Las notificaciones que puede emitir

All status= operational state= disabel, enabled
All count= contadores, AO total, AO terminated, AO out stand
All Attr=all atributos
All char= all characteristics

Representación de los NE en clases de entidades

Como se ha indicado anteriormente, el SGFRT puede ser una plataforma orientada a la administración de objetos, cualquier recurso de la red, puede ser representado por una clase de entidad y es estructurado y aplica todo lo anterior, la clase de objetos gestionados viene dado por:

- Los atributos que posee
- Las operaciones que pueden ejecutar sobre él
- El comportamiento que presenta
- Las notificaciones que puede emitir

Para especificar cualquier pieza del equipo, se puede crear una instancia de entidad a esto se le llama instanciar y se refiere a definir o modelar al elemento de red que pertenece a una clase global y a una partición dentro de dicha clase global o entidad, usando la entidad clase template (platilla), lo cual puede facilitar el trabajo modelado, esto se refiere a la descripción propia de los elementos de red y a los reportes de alarmas que envían.

- Las clases de objetos deben especificarse para todo un conjunto de funciones físicas, lógicas, humanas, etcétera, en el modelo de red.

- El núcleo de las propiedades especificadas en una clase de objetos son los atributos, funciones y cápsulas.

- Las clases se organizan en una jerarquía de herencia con una generalización que se incrementa hacia arriba y una especialización que se incrementa hacia abajo.

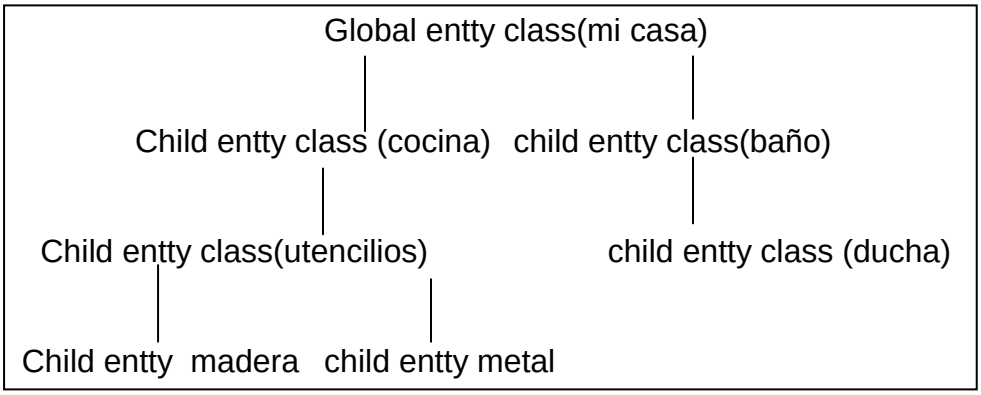
- Cuando se decide especializar una nueva clase de objetos de una clase de objetos existente, se debe seleccionar una base de especialización.

- La base de especialización actúa como un factor que permite distinguir entre subclases.

Para el desarrollo de productos o redes usando metodologías de modelado orientado a objetos, la arquitectura de la red debe organizarse usando jerarquías de herencia y agregación.

La jerarquía de herencia debe enumerar todas las versiones y diferentes configuraciones que la red o el producto puede manifestar.

Figura 9. **Ejemplo de árbol de clases globales**



Fuente: elaboración propia.

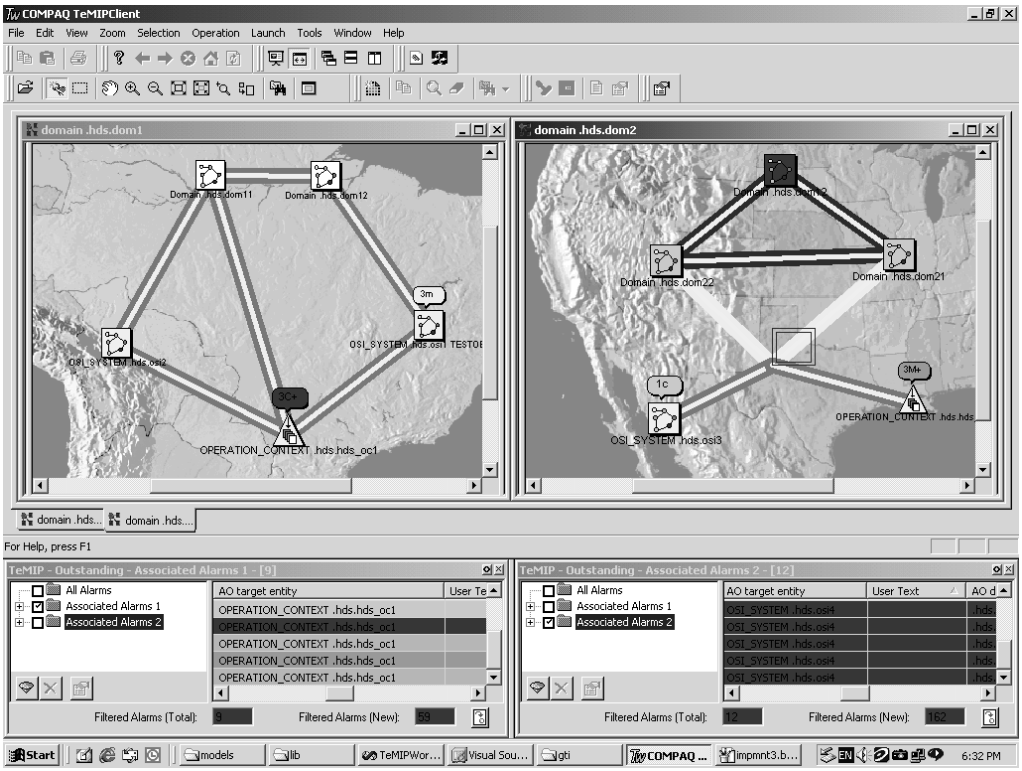
3.1.3. Módulos de interfaz norte

El módulo de presentación también conocido como PM constituye lo que se conoce como interfaz norte porque se comunica con cualquier otro sistema arriba de él, consta principales interfaces de usuarios, ejemplo de esto son las siguientes interfaces, que pueden presentarse en cualquier plataforma dentro del mercado:

El observador de mapa que está totalmente basada en una plataforma abierta. El SGFRT debe cumplir con los estándares de los organismos internacionales UIT, TMF, IETF, incluyendo la familia de Normas del ITU-T de la serie M.3010 debe proveer una visión jerarquizada de la red y de sus elementos de acuerdo con las necesidades del operador.

El reconocedor de alarmas muestra las alarmas en una tabla con todas las informaciones patrón REC. UIT-T X.733, también es organizada de acuerdo con las necesidades del operador.

Figura 10. **Vista de interfaz gráfica de un sistema de gestión**



Fuente: http://h20195.www2.hp.com/V2/GetPDF.aspx/4AA1-7653ENW.pdf. Consulta: septiembre de 2011.

Este módulo de presentación tiene las siguientes funciones:

- Transmisión de peticiones del usuario

- Entrega de información para el usuario o para otras aplicaciones de la northbound, dichas aplicaciones pueden ser un conjunto de interfaces hacia los usuarios de diferentes perfiles. La solución propuesta trabaja con dos formas de interfaces. La interfaz con los módulos funcionales que constituyen la solución (interfaces cliente basadas en Web o Windows) y la interfaz para exportar eventos a otros sistemas.

Debe tener la posibilidad de exportar eventos hacia otra plataforma gracias a que debe tener sus interfaces abiertas y publicadas y puede contener:

- Vista de topología (observador de alarmas), línea de comando (FCL o TCL).

- El escritorio contiene una serie de aplicaciones las cuales pueden ser: observador de mapa que es una presentación gráfica de la topología de la red o parte de ella, puede ser organizada en forma jerárquica.

- El mapa editor y símbolo del editor.

- El reconocedor de alarmas (hace un despliegue en tiempo real de las alarmas pendientes, proporciona varias presentaciones en tiempo real a demás de poder hacer filtros).

- Historial de alarmas (despliega las alarmas que han sido reconocidas y terminadas, en forma histórica).

- Management views.

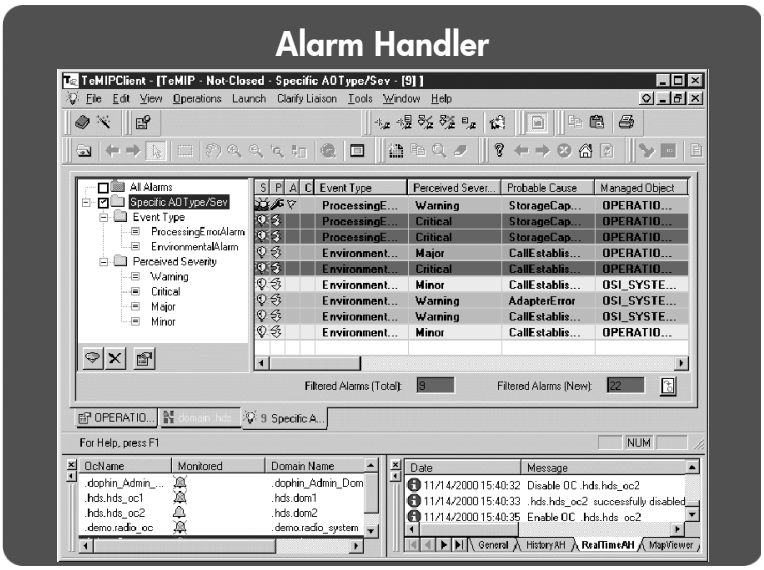
- Entity browser.

- Dictionary browser.
- Alarm forwarding.
- Resynchronization GUI.
- State viewer.
- Outage viewer.
- Web Service Northbound Interfaz: interfaz norte para comunicación hacia un sitio Web.

El cliente o usuario del SGFRT, es el que tiene instalado un agente de la aplicación del SGFRT o puede comunicarse a él por medio de la Web, de ambas formas será conectado al SGFRT por medio del PM.

Debe ser posible también que un determinado usuario abra simultáneamente varias ventanas del problema presentado, pudiendo ser personalizada cada una de ellas. Por ejemplo, puede existir una ventana que muestre solamente las alarmas críticas y otra que muestra solamente las alarmas de un determinado EMS.

Figura 11. **Vista del reconocedor de alarmas**



Fuente: http://h20195.www2.hp.com/V2/GetPDF.aspx/4AA1-7653ENW.pdf.
Consulta: septiembre de 2011.

A continuación se describe la información de la alarma que se presenta en la tabla:

- Severidad de la alarma (crítica, mayor, menor, *warning, cleared, indeterminate*).

- Fecha y hora de ocurrencia de alarma.

- Localidad en que ocurre la alarma.

- En la ventana de alarma presentes se pueden ejecutar las siguientes operaciones:

    - Visualizar los detalles de una alarma

    - Localizar el objeto correspondiente en el mapa de red

Las operaciones ejecutadas por los usuarios sobre las alarmas mostradas en el problema presentado serán almacenadas en una base de datos. Las tablas de la base de datos podrán ser consultadas para proceso de auditoría.

Windows Iconic map, los Items de los Mapas son los objetos desplegados en el mapa, creados en Windows Iconic Map. Estos items son objetos sobre todo virtuales, es decir, objetos como polígonos, círculos, líneas o rectángulos.

Ejemplo de funciones específicas que puede tener un SGFRT

- Funcionalidad administrador de eventos

Recibe la información proveniente del módulo de filtro de eventos FM y analizador de alarmas para su administración.

Es el centro de los componentes para la administración de alarmas y eventos en la estructura de la herramienta, incluye funciones de administración de alarmas de acuerdo a Normas ISO.

Soporta la Norma ISO 10164-4 o UIT-T X.730 (funciones de gestión de sistemas abiertos) de reporte de alarmas incluyendo el formato de estas (*alarm type, severity, probable cause, status*), la manera de reportarlas (*acknowledgement, clearance, closure*). Todas las operaciones realizadas con las alarmas son etiquetadas para su posterior análisis.

- El filtro de eventos FM

Esta es una función estándar, utiliza para escritura el código C++ para modificar los campos de las alarmas. Puede ser creador de perfiles para diferentes tipos de alarmas. Provee los servicios para control de los filtros de OSI eventos y alarmas entrantes al sistema.

- El analizador de eventos

Esta función se encarga de realizar cambios de *performing*, de los campos según sea requerido por el usuario, esto se logra por medio de filtros correctivos. Una vez realizado esto además del complemento de los filtros impuestos por el filtro de eventos según se requiera, la alarma es procesada hacia el administrador de eventos.

- Funcionalidad reconocedor de alarmas

Reconocedor de alarmas se refiere al manejo y administración de las alarmas y problemas, lo que provee es lo siguiente: filtros, colección, (almacenamiento) y administración de servicios en OSI, construye la correlación de alarmas.

Aquí se hacen filtros de alto nivel llamado CD, entendiéndose como los filtros visuales que puede hacer el usuario del cliente de la herramienta.

- Funcionalidad maestro experto

El SGFRT puede contar con un sistema maestro experto que trabaja con reglas, las cuales son definidas por el personal experto en la operación de la red. La intención de las reglas es emular al operador experto en la determinación de la causa raíz de los problemas. Además, de la funcionalidad de determinación de causa raíz, el sistema experto es usado como herramienta de automatización de creación de reportes de problema (Trouble *tickets*).

Por ejemplo, el personal experto en la operación de la red determina que ante la ocurrencia de cierta secuencia de alarmas es necesario crear un reporte de falla, este será creado de manera automática por una acción del sistema experto sin la intervención del operador.

Maestro experto, se basa en reglas ILOG y es un sistema que permite tomar decisiones de forma automática por medio de condiciones secuenciales. En particular se usa para reducir la cantidad de alarmas por medio de filtrado y correlación y para realizar tareas de forma automática.

Maestro experto puede realizar acciones automáticas para:

- Filtrado de alarmas

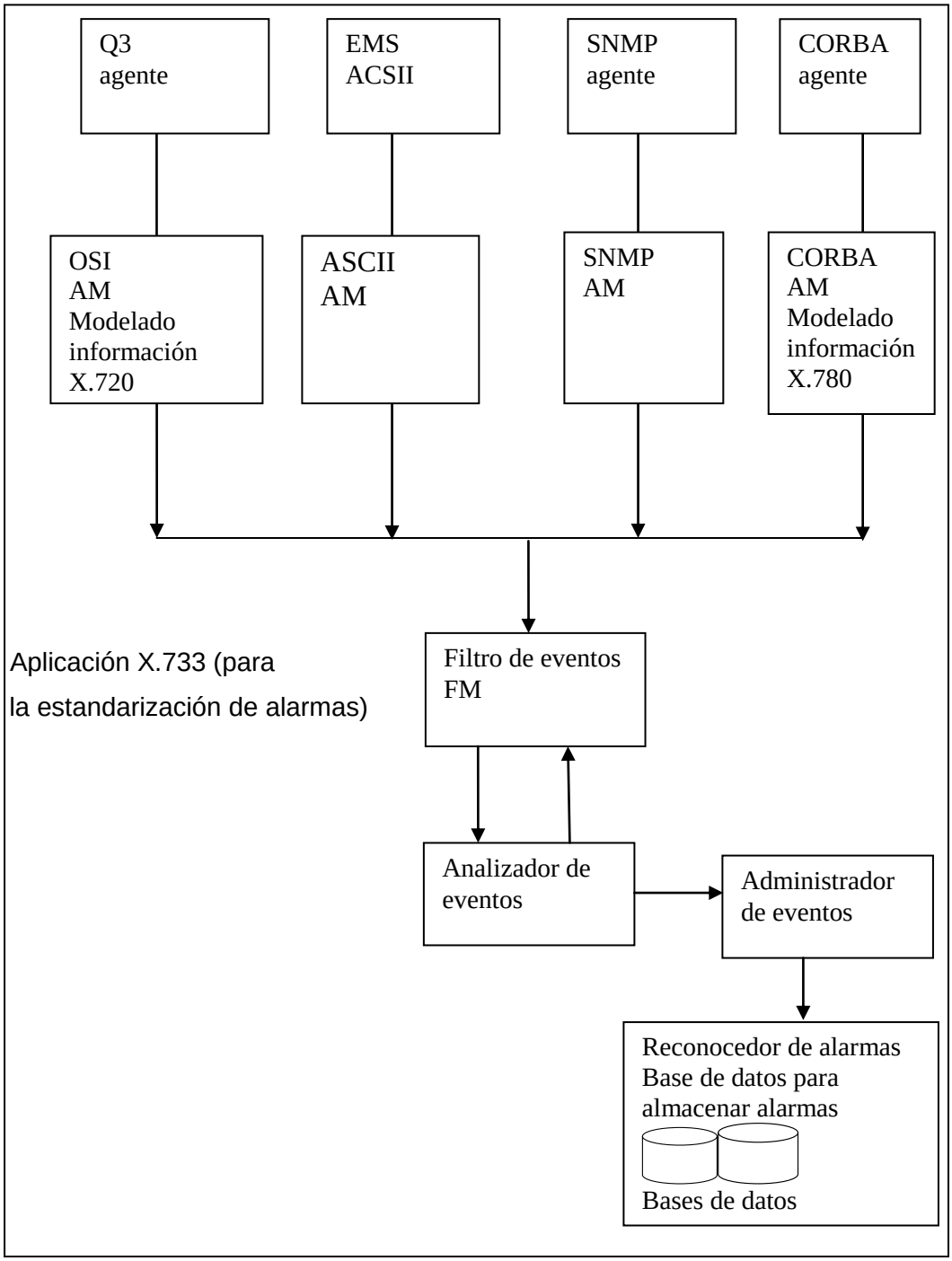
- Modificación de alarmas

- Análisis de la causa raíz
- Análisis en el impacto sobre el servicio

La funcionalidad de experto se basa en:

- Reglas ILOG, un ambiente de desarrollo para construir sistemas expertos
- El *toolkit* de la funcionalidad maestro experto provee una API para personalizar el modelado de los objetos de maestro experto.

Figura 12. **Diagrama de flujo de los módulos relacionados**



Fuente: elaboración propia.

3.1.4. Módulos estadísticos

Para mantener concordancia con la ISO standars, los reportes son modelados de dos formas:

- Configuración de eventos: creación del objeto, borrado de objetos, cambio de valores atribuidos.

- Notificación de eventos: reporte de alarmas, el comportamiento de las alarmas en *run-time* (tiempo real).

- Reporte de alarmas: equipo, comunicación, calidad de servicio.

- Reporte de alarmas de seguridad.

3.2. Software y hardware de la solución

El software de la solución debe residir en una arquitectura distribuida o en capas, es decir, se debe contar con un módulo central o kernel donde deben residir las aplicaciones del módulo de funciones y el módulo de acceso, en otro servidor estará integrado el módulo de presentación y en un tercer servidor el de la base de datos. En cada uno de los usuarios residirá el cliente de la aplicación los cuales se comunicarán con el servidor de presentación a través de CORBA conectado a la red por medio de una LAN.

El servidor central o kernel contendrá, así también, las funciones especiales de correlaciones de alarmas como la de estadísticas.

Hardware

La distribución se obtiene a través de los módulos de gestión de distribución, también conocidos como directores. Esto permite que las funciones operen de forma transparente a través de las fronteras de los servidores. Nuevos directores pueden ser añadidos a una solución que ya este en operación sin afectar los módulos existentes. Esta flexibilidad permite la adaptación de la solución de gestión como una función del crecimiento proyectado de la red de gestión.

Cada instancia de un director tiene un nombre global único. Un director distribuido permite el envío y recepción de comandos de gestión para y desde otro director distribuido para cualquier combinación de nombre, entidad y partición en la interfaz de llamadas (Call Request Interface).

3.3. Capacidades

La capacidad de hardware tiene que estar definida de acuerdo con la cantidad de eventos monitoreado, al historial almacenado, cantidad de SGN a integrar, en la siguiente tabla XII se da un ejemplo.

Tabla XII. **Ejemplo de un listado de hardware**

tem	Servidor	Sistema Operativo	Descripción	Software asociado
	RP 4440	HP UX11.11	• 4 CPUs de 1 GHz • 10GB RAM • 2x 72GB • 2 tarjetas de red 10/100 • DVD	• TeMIP Bundle • AMs • TeMIP Expert • TeMIP Map • Oracle
	RP 3440	HP UX 11.11	• 2 CPUs de 1GHz • 6GB RAM • 2x 72GB • 2 tarjetas de red 10/100 • DVD	• OV NNM • Oracle • OV Customer View (opcional)
		Windows 2k	• 1 CPU • 2 G RAM • 18 G HD • tarjeta de red 2x100Eth • DVD • en rack	• TeMIP Web Server

Fuente: elaboración propia.

3.4. Seguridad

En el área de la seguridad la p SGFRT debe soportarse sobre las recomendaciones UIT.T Q. 816 que define los servicios de seguridad genéricos tratados en el foro del grupo de gestión de Objetos OMG (Objet Management Group) para la actividad de gestión realizada a través del paradigma CORBA.

Para la seguridad cuando se utilice el protocolo CMIP deberá aplicarse las recomendaciones UIT-T X.736.

Para el área de control de acceso a la solución se debe basar en las clausulas 6.3/X.810 y REC. UIT-T X.812.

La seguridad entre los flujos de información para que solamente circulen entre los puntos extremos autorizados deberá fundamentarse sobre la REC. UIT-T X.805.

3.5. Licencias

La licencia es el contrato entre el desarrollador o la empresa proveedora del software y el cliente en este caso la empresa de telecomunicaciones, en dicha licencia se establecen los derechos del autor y el usuario y otorga el derecho de utilizar el software.

Para este caso y debido a que son varios usuarios del software la licencia deberá ser adquirida por bloque, es decir, con un número establecido de usuarios.

3.6. Diseño e implementación de DNC (Digital Network Chanel) para interconexión de la solución

Como se mencionó en el capítulo anterior, la red de comunicación de datos servirá para transportar los datos de gestión entre los elementos de red y los gestores nativos o gestores nativos y la plataforma solución, puede utilizar una red externa o una red interna como los canales anidados de datos ECC, utilizando por ejemplo, el protocolo LAP D en la tecnología SDH o puede utilizar X.25, TCP, UDP de forma externa, técnicamente es independiente de la red de telecomunicaciones aún cuando utilice dichos canales anidados de datos.

Para este caso en que la integración es de cada gestor nativo hacia la plataforma la DCN utilizarán canales de comunicación vía los protocolos TCP o vía Telnet según se requiera.

- Equipos a administrar deben estar conectados a la red (DCN) y deben contar con dirección IP asignada.

- Equipos a administrar deben tener un puerto dedicado y configurado a exportación automática (a la DCN) de alarmas, en formato ASCII o SNMP.

Cuando se utiliza el protocolo telnet para conectar un *host* remoto a un equipo que funciona como servidor, a este protocolo se le asigna el puerto 23. Se describe en el RFC 854 - Especificaciones del protocolo telnet y RFC 855 - telnet option specifications. El protocolo telnet se aplica en una conexión TCP para enviar datos en formato ASCII codificados en 8 bits, entre los cuales se encuentran secuencias de verificación telnet. Por lo tanto, brinda un sistema de comunicación orientado bidireccional (semidúplex) codificado en 8 bits y fácil de implementar.

4. IMPLEMENTACIÓN

4.1. Reglas de correlación de fallas

Las reglas de correlación consisten en relacionar las fallas dadas en las diferentes redes o en la misma, para encontrar la causa raíz y presentar al técnico que monitorea los sistemas de gestión, solamente la falla llamada causa raíz, con la posibilidad de desplegar las fallas hijas o provocadas por la falla principal.

Para realizar reglas de correlación inicialmente las alarmas deben ingresar al gestor integrador o SGFRT en formato normalizado según recomendación X.733 (tratado en capítulo 2), esto lo deben cumplir todos los desarrolladores de software para gestión de redes, ya que al gestor integrador ingresan alarmas generadas por estas diferentes redes (a través de sus respectivos gestores nativos). Pese a que cada uno de los proveedores debe cumplir con esto, el gestor integrador se asegura a través de su módulo de acceso de que esto se realice, estandarizando el formato de alarmas para asegurar su proceso ya dentro del SGFRT.

Una vez las alarmas ingresan por el respectivo módulo de acceso, estas son procesadas por el módulo de funciones FM, aquí son normalizadas según rec X. 721 en cuanto a la sintaxis y son filtradas según los parámetros seleccionados, es decir, según los dominios de la declaración de objetos gestionados y son seleccionadas según la tecnología o servicio y presentados en diferentes dominios en el PM según esta clasificación.

Dentro de esta separación o filtrado también se ejecutan otros filtros que seleccionan las alarmas según el impacto en la red, para el caso de las críticas estás son direccionadas a un sector específico llamado maestro experto o ME (visto en el capítulo 3) donde se generan alarmas artificiales, son llamadas artificiales porque son generadas por la correlación con otras alarmas, no provienen de un gestor nativo especifico, estas tienen potencial de generar *ticket*, sin embargo, esto no se da a menos que cumplan con la condición de generar pérdida de tráfico, la clasificación de la criticidad de las alarmas es especificada en el catálogo de alarmas que es elaborado por el ingeniero de desarrollo y personal experto en la tecnología tratada.

Una vez creada una alarma artificial que involucra pérdida parcial o total de servicio, el módulo experto por medio de una interfaz norte se comunicará con otro módulo (independiente del SGFRT) el cual creará un *ticket* de forma automática. Con este módulo se logra correlación de alarmas y automatización de acciones, reduce los costos de operación y mejora la calidad del servicio prestado.

A través del ME se puede hacer de forma más rápida y mejor lo siguiente:

- Crear trouble *tickets*
- Hacer el análisis de la causa raíz
- Crear, terminar alarmas objetos

Los implementadores del SGFRT pueden crear y desplegar con facilidad aplicaciones basadas en reglas que automaticen decisiones, además de reducir el tiempo, esfuerzo y coste del desarrollo de aplicaciones y del mantenimiento continuado.

Este módulo ME está basado en ILOG Rules 7 for C++ de IBM. IBM ILOG es una compañía internacional de software de propiedad de IBM. Que crea productos de software empresarial para la cadena de suministro , gestión de reglas de negocio, visualización y optimización. Es compatible con varias plataformas de software, incluyendo C++, C #, . NET, Java, Ajax y Adobe Flex / AIR. Para la implementación de esta plataforma se usa C++.

IBM es el líder mundial en soluciones para Sistemas de Gestión de Reglas de Negocios (BRMS) que permiten la automatización flexible de la toma de decisiones en sistemas que están sujetos a reglas complejas, variables y en constante evolución, herramienta específica y entornos para desarrolladores, expertos del negocio y operadores de TI, brindando una plataforma de validación y de gestión de reglas en todo su ciclo de vida.

Ejemplo de la lógica para crear una regla en el ME.

Llámese reglas a los programas creados en un lenguaje C++ que establecen un resultado si ciertas condiciones de fallas son verdaderas o falsas, la parte fundamental en dicha creación son dichas condiciones claves que relacionen sitios, equipos, trayectos o estados, es decir, que detecten la causa raíz de una serie de fallas que se relacionan por esa causa raíz.

Ejemplo de creación de reglas

Un nodo es un sitio donde existe equipo o elementos de red de diversa tecnología, puede ser de transmisión, conmutación, celdas, etcétera. Dicho nodo está interconectado con otros nodos. Para este ejemplo el nodo tendrá dos celdas de tecnología GSM, red 1900 y red 900 cada celda tendrá tres sectores radiantes, por lo tanto, se pueden generar hasta 6 alarmas bases porque son las generadas por el elemento de red fallado, estas pueden ser:

- GSM cell out of servicio (alarma base)

- OML Fault (Además de la alarma base y común para todas de transmisión fallada).

Regla 1: falla transmisión

El maestro experto generará una alarma llamada artificial si desde la herramienta llegan alarmas del tipo GSM cell ut of servicio y OML Fault, la alarma artificial será:

- Sitio fuera por transmisión (alarma artificial)

Regla 2: falla energía

El módulo experto generará una alarma artificial si desde el ME llegan alarmas del tipo:

- Main Input (alarma base)

- OML Fault (alarma base, que indica pérdida de señal de transmisión)

- Alarma artificial: sector fuera

Con una alarma artificial de Sitio fuera ya sea por transmisión o por energía después de 10 minutos enviará un mensaje para apertura automática de *ticket*.

El SGFRT también permitirá que los operadores puedan crear *tickets* llamados semiautomáticos porque requiere la intervención de ellos, estos *tickets* semiautomáticos son creados un módulo exterior al SGFRT pero a través de su interfaz norte como se mencionó anteriormente, estos *tickets* pueden ser abiertos desde la interfaz del cliente en forma gráfica que es con la que interactúan los técnicos que monitorean la red.

4.2. Mediciones de MTT, SLA

El objetivo principal de una solución de gestión de red es reducir el MTTR (Mean Time To Repair) y con ello cumplir con los acuerdos de servicio realizados con los clientes, esto se logra a través del SGFRT ya que como se ha visto puede hacer filtros que ayudan a disminuir la cantidad de alarmas vistas por el operador limitándolo a monitorear solamente aquellas que impactan el servicio, como ejemplo de la disminución o filtrado de estas alarmas puede observase el apéndice 1.

Así mismo, conforme se implementan correlaciones a través de reglas, las fallas automáticas abiertas a través del SGFRT se van incrementando respecto a aquellas abiertas manualmente, lo que automatiza todo el proceso, un ejemplo de esto se puede observar en el apéndice 2.

En la tabla XIII se muestran los tiempos medios de solución de fallas ya con la implementación del diagrama de flujo del proceso de atención de fallas indicado en la figura 13, es decir, con el SGFRT implementado en un NOC, como puede observarse el MTTR ha disminuido y la atención de fallas es más inmediata, por una parte por la generación de *ticket* automáticos generados por el SGFRT implementados a través de la correlación de fallas entre las redes y además por la modificación de procesos de atención de fallas que ahora son escalonados.

Tabla XIII. **Ejemplo de tiempos por línea de operación posterior a la implementación del SGFRT**

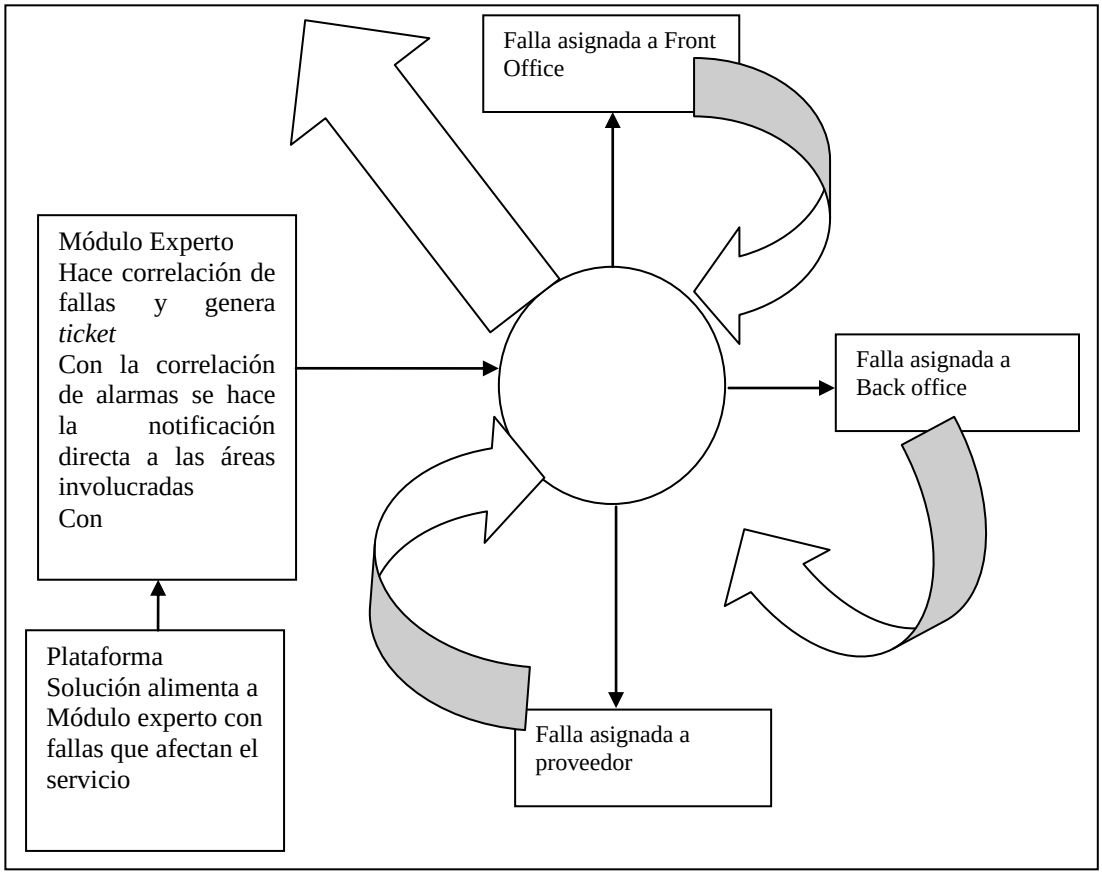
Tecnología	Tiempo de solución por Front Office	Tiempo de solución por Back Office	Tiempo de solución por campo
Cx fija	00:33	18:33	16:48
Datos	05:38	02:34	13:15
Sistemas		14:56	
SVA	09:28	23:44	06:11
Movil	04:07	30:27	10:41
Transporte	02:46	20:41	13:07

Fuente: elaboración propia.

4.3. Procesos posteriores a la implementación de la herramienta para atención de fallas, aplicación de eTOM

Una vez implementada la herramienta, todo el proceso de atención de fallas del centro de gestión deberá cambiar, ya que sin la correlación de alarmas entre las diferentes redes cada técnico solucionaba las fallas de la red monitoreada. A través de la gestión integrada de todas las fallas el mismo técnico tendrá una vista de todas las redes con la detección de la causa raíz y, podrá actuar de forma inmediata, estos técnicos son los pertenecientes al Frot office, de no poder solucionarla la deberá escalar a personal con más experiencia, personal del *Back Office*, los cuales finalmente podrán escalarla al proveedor si no les es posible darle solución ellos mismos, está estructura es la mostrada en la figura 13.

Figura 13. **Proceso de atención de fallas después de implementar el SGFRT**



Fuente: elaboración propia.

- eTOM

Desarrollado por Telemanagement Forum TMF, sirve como marco de referencia para la estandarización de todos los procesos del área de las telecomunicaciones, basado en las mejores prácticas.

4.4. Documentación

La documentación debe ser entregada por parte del proveedor en forma escrita y magnética. A continuación manuales básicos que deben entregar:

- Guía del operador de la herramienta: es un documento resumido de las facilidades de la herramienta específicamente del cliente con el cual interactúa el operador diariamente, en dicho documento se debe especificar cada campo que verá en la interfaz gráfica, cómo interactuar con la herramienta, cuáles son los filtros admitidos a este nivel, cómo crear gráficas y topologías según necesidades.

- Fundamentos del funcionamiento a nivel de software: consiste en un documento resumen del funcionamiento global del software, dirigido a los operadores encargados de dar mantenimiento e implementaciones a nivel de línea de comandos y de forma gráfica (con el cliente).

Documentación completa de todo el software y hardware en que consistirá la herramienta enfocado a los ingenieros encargados de implementar y dar soporte a la herramienta.

4.5. Soporte

El soporte puede ser contratado a requerimiento de la empresa por horas o días, por ejemplo, puede ser de 8 x 5 es decir 8 horas diarias durante 5 días a la semana y debe incluir:

- Dar soporte técnico a los usuarios de la herramienta en la operación y administración correcta del sistema, en lo que se refiere a la utilización y administración de las herramientas implementadas, según indicado anteriormente, en el cotidiano y en los procedimientos básicos de resolución de problemas.

- Personalización a través de parámetros de las aplicaciones de software de los módulos mencionados.

- Accionar el soporte de tercer nivel del proveedor de la aplicación para la corrección de errores de software.

- Instalar *patches* y *upgrades* de aplicación de software

- Escalar y abrir *ticket* hacia el TAC para solución de problemas que requieran intervención directamente del proveedor.

- Entregables que consiste en informes semanales, en forma de log, sobre las actividades desempeñadas y los eventos relevantes que ocurrieron durante ese período.

- Además del soporte en sitio, también puede contratarse el proporcionado por el TAC, el cual tiene de objetivo dar solución a aquellos problemas más específicos o que requieran personal más especializado. Este soporte puede ser de 24 x 7, es decir, las 24 horas del día durante los 7 días de la semana de forma remota.

CONCLUSIONES

1. El establecimiento del alcance del sistema de gestión de gestores de redes de telecomunicaciones a ser implementado, permite delimitar su tamaño y asegura que cumpla con recomendaciones internacionales, así como, las propias de la empresa que necesita adquirirlo.

2. La colección de datos es una de las tareas más importantes dentro del dimensionamiento y establecimiento de los límites de la herramienta ya que describe cada uno de los elementos que serán integrados, con ello, se verifica si existe disponibilidad inmediata de la integración con el SGFRT o se estima en qué tiempo podrá ser integrado.

3. La arquitectura del sistema de gestión de gestores de fallas define los módulos que lo componen y su funcionamiento, esto permite tener un conocimiento preciso de la herramienta a implementar.

4. Durante la implementación de la herramienta de gestión de gestores se definen las reglas de correlación de las alarmas, que servirán para el trouble *ticket* automático.

5. Con una herramienta de gestión integrada de fallas se disminuye el tiempo medio de solución de las mismas, a través de la automatización de la apertura de trouble *ticket*, logrando con esto cumplir con los acuerdos de SLA firmados con los clientes.

RECOMENDACIONES

1. El alcance del sistema de gestión de gestores de redes de telecomunicaciones debe fundamentarse en las recomendaciones UIT-T e ISO, así como las propias de la empresa.

2. Debe hacerse un análisis de los procesos de atención de fallas anterior a la implementación de la SGFRT y modificarlos posterior a su implementación para la obtención de óptimos resultados.

3. La recolección de datos debe hacerse siguiendo un formato previamente establecido y debe ser completado por cada supervisor de cada sistema de gestión, esta a su vez debe ser validada por el ingeniero implementador para que cumpla con lo solicitado.

4. La arquitectura del SGFRT debe ser del tipo distribuida ya que esto permitirá mantener separado al cliente y la aplicación, para lo cual será necesario el servidor central o kernel, el servidor de presentación y la base de datos, esto permitirá hacer ampliaciones sin afectar al cliente.

5. Durante la implementación del sistema de gestión de gestores de fallas de redes de telecomunicaciones deben establecerse las reglas de correlación de fallas.

BIBLIOGRAFÍA

1. CHARTE OJEDA, Francisco. *Introducción CORBA* [en línea]. <www.google.com>. [Consulta: 3 julio de 2011].

2. ILOG. *Desarrollo reglas de correlación* [en línea]. <http://www.ilog.com>. [Consulta: 12 agosto de 2011].

3. *Modelo OSI.* [en línea]. <http://www.monografías.com>. [Consulta: 11 julio de 2011].

4. Monografías. *Northbound interface* [en línea]. <http://www.monografías.com>. [Consulta: 23 septiembre de 2011].

5. *MPLS*. [en línea]. <http://www.monografías.com>. [Consulta: 5 septiembre de 2011].

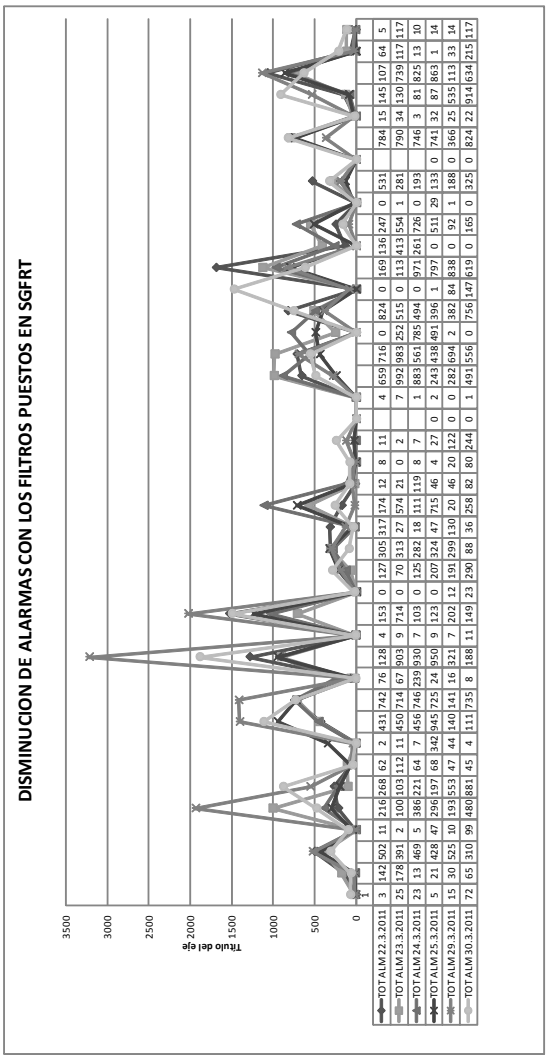
6. *Northbound interface*. [en línea]. <http://www.monografías.com>. [Consulta: 7 septiembre de 2011].

7. Unión Internacional de Telecomunicaciones. *Gestión de sistemas: función señaladora de alarmas, UIT-T X.733, ISO/CEI 10164-4*, Suiza, 1992 [en línea]. <http://www.uit.com>. [Consulta: 13 septiembre de 2011].

8. _____.*Principios para una red de gestión de las telecomunicaciones. Recomendación UIT-T M.3010.* Suiza: UIT, 2000 [en línea]. <http://www.uit.com>. [Consulta: 1 septiembre de 2011].

APÉNDICES

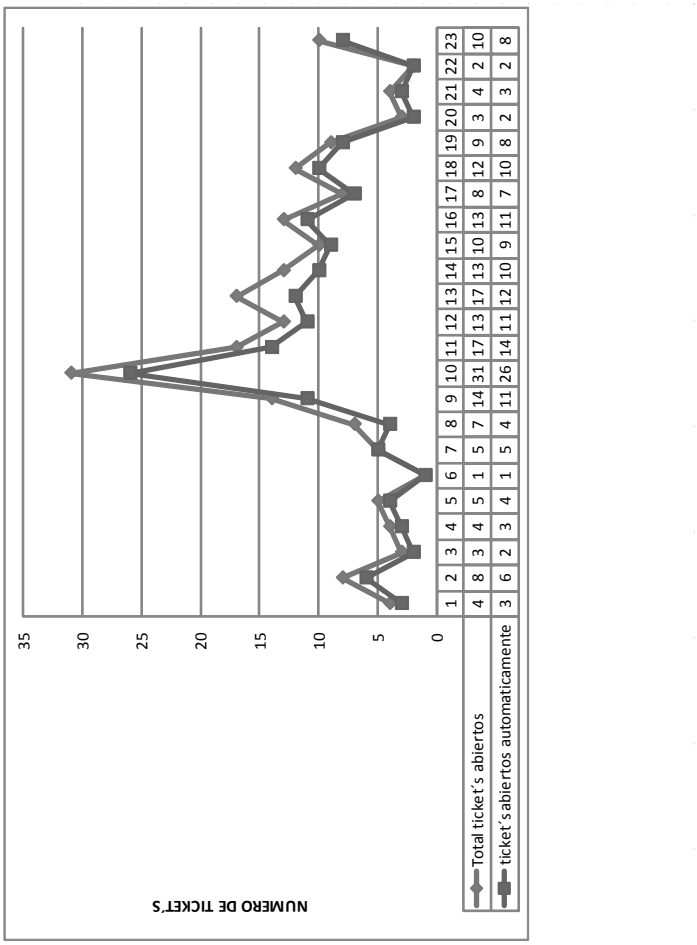
Apéndice 1. **Disminución de alarmas con los filtros puestos en SGFRT**



TOT ALM 23.3.2011	TOT ALM 1	TOT ALM 24.3.2011	TOT ALM 25.3.2011	TOT ALM 29.3.2011	TOT ALM 30.3.2011
3	25	23	5	15	72
142	178	13	21	30	65
502	391	469	428	525	310
11	2	5	47	10	99
216	1007	386	296	1937	480
268	103	221	197	553	881
62	112	64	68	47	45
2	11	7	342	44	4
431	450	456	945	1405	1117
742	714	746	725	1416	735
76	67	239	24	16	8
1284	903	930	950	3219	1887
4	9	7	9	7	11
1530	714	1038	1239	2026	1498
0	0	0	0	12	23
127	70	125	207	191	290
305	313	282	324	299	88
317	27	18	47	130	36
174	574	1116	715	20	258
12	21	119	46	46	82
8	0	8	4	20	80
11	2	7	27	122	244
			0	0	0
4	7	1	2	0	1
659	992	883	243	282	491
716	983	561	438	684	556
0	252	785	491	2	0
824	515	494	396	382	756
0	0	0	1	84	1475
1690	1130	971	797	838	619
136	413	261	0	0	0
247	554	726	511	92	165
0	1	0	29	1	0
531	281	193	133	188	325
			0	0	0
784	790	746	741	366	824
15	34	3	32	25	22
145	130	81	87	535	914
1071	739	825	863	1136	634
64	117	13	1	33	215
5	117	10	14	14	117

Fuente: elaboración propia.

Apéndice 2. **Total de *tickets* abiertos**



Total ticket´s abiertos	ticket´s abiertos automaticamente
4	3
8	6
3	2
4	3
5	4
1	1
5	5
7	4
14	11
31	26
17	14
13	11
17	12
13	10
10	9
13	11
8	7
12	10
9	8
3	2
4	3
2	2
10	8

Fuente: elaboración propia.