DISEÑO DE UN SISTEMA DE SOPORTE DE OPERACIONES (OSS) PARA GESTIÓN DE FALLAS EN REDES 3G

CLAUDIA INES ALBORNOZ VILLOTA
JUAN PABLO BUSTAMANTE BEDOYA

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Grupo de Nuevas Tecnologías en Telecomunicaciones
Popayán, diciembre de 2005

DISEÑO DE UN SISTEMA DE SOPORTE DE OPERACIONES (OSS) PARA GESTIÓN DE FALLAS EN REDES 3G

CLAUDIA INES ALBORNOZ VILLOTA
JUAN PABLO BUSTAMANTE BEDOYA

TRABAJO DE GRADO

Director: I.E. Alejandro Toledo Tobar

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Grupo de Nuevas Tecnologías en Telecomunicaciones
Popayán, diciembre de 2005

CONTENIDO

pag.

LISTA DE TABLAS

pag.

LISTA DE FIGURAS

pag.

GLOSARIO

ADAC: *Automatically Detected and Automatically Cleared,* Automáticamente detectado y automáticamente clareado.
ADMC: *Automatically Detected and Manually Cleared*, Automáticamente detectado y manualmente clareado.
AN: *Access Network*, Red de Acceso.
AO: *Associated Objects,* Objetos Asociados.
AS: *Application Server*, Servidor de aplicaciones.
ASN.1: *Abstract Syntax Notation,* Notación de sintaxis abstracta.
ATM: *Asynchronous Transfer Mode,* Modo de transferencia asíncrono.
AuC: *Authentication Centre*, Centro de Autenticación.
BG: *Border Gateway*, Pasarela de Frontera.
BSC: *Base Station Controller*, Estación base controladora.
BSS: *Business Support Systems*, Sistema de soporte de negocios.
BSS UTRAN: *Base Station System,* Sistema de estación base UTRAN.
BTS: *Base Transceiver Station,* Estación base transceptora.
C: *Condicional,* Condicional.
CAMEL: *Customised Applications for Mobile network Enhanced Logic*, Aplicaciones personalizadas para lógica mejorada de redes móviles.
CBC: *Cell Broadcast Center*, Centro de difusión celular.
CBE: *Core Business Entities,* Entidades de red central.
CBS: *Cell Broadcast Service*, Servicio de difusión celular.
CME: *Conformant Management Entities*, Entidades de gestión conformes.
CMIP: *Common Management Information Protocol*, Gestión basada en el protocolo de información de gestión común.
CMIS: *Common Management Information Service*, Servicio de información de gestión común.
CMISE: *Common Management Information Service Element,* Servicio de Información de gestión común.
CN: *Central Network*, Red central.
CS: *Circuit Switched*, Conmutación de circuitos.
CSCF: *Call Session Control Function*, Función de control de estado de Llamada.
CS-MGW: *CS - Media Gateway Function*, CS-Función de Pasarelas Multimedia.
DAF: *Directory Access Function,* Función de acceso al directorio.
DSF: *Directory System Function,* Función de sistema de directorio.
DSA: *Directory System Agent,* Agente de sistema de directorio.
DUA: *Directory User Agent,* Agente usuario de directorio.
EDGE: *Enhanced Data Rate for GSM Evolution, Tasa de datos mejorada para evolución de GSM.*

EIR: *Equipment Identity Register*, Registro de identidad de equipos.
EJB: *Enterprise Java Beans.*
EM: *Element Managers*, Gestores de elementos.
eTOM: *Enhanced Telecom Operation Map*, Mapa de operaciones de telecomunicaciones mejorado.
FM: *Fault Management*, Gestión de fallas.
FRC: Fichero Registro Cronológico.
GCR: *Group Call Register*, Registro de llamada de grupo.
GERAN: *GSM/EDGE Radio Access Network*, Red de acceso a radio GSM/ EDGE.
GDMF: *Guidelines for the Definition of TMN Management Functions*, Guía para la definición de funciones de gestión de la TMN.
GDMS: *Guidelines for the Definition of Management Services*, Guía para la definición de servicios de gestión.
GGSN: *Gateway GPRS Support Node*, Pasarela nodo soporte GPRS.
GMLC: *Gateway Mobile Location Center*, Pasarela centro de localización móvil.
GMSC: *Gateway MSC*, Pasarela MSC.
GPRS: *General Radio Packet Services,* Servicio general de radio paquetes.
GSM: *Global System for Mobile communications,* Sistema global de comunicaciones móviles.
HLR: *Home Location Register*, Registro de Posición Base.
HN: *Home Network*, Red Base.
HSS: *Home Subscriber Server*, Servidor de abonados base o domésticos.
ICF: *Information Conversion Function,* Función de conversión de información.
IMSI: *International Mobile Subscriber Identity*, Identidad de suscriptor móvil internacional.
IMS IP: *IP Multimedia Subsystem*, Subsistema de Multimedia IP.
IMT-2000: *International Mobil Telecommunications 2000,* Telecomunicaciones móviles internacionales-2000.
IOC: *Information Object Class,* Clase Objeto de Información.
IP: *Internet Protocol*, Protocolo de Internet.
IRP: *Integration Referente Point*, Punto de referencia de integración.
ISVs: *Independent Software Vendors,* Vendedores de software independiente.
IS: *Information Service*, Servicio de Información.
ISDN: *Integrated Services Digital Network,* Red digital de servicios integrados.
Itf-N: interfaz N.
IWF: *InterWorking Function*, Función de Interworking.
J2EE: *Java 2 Enterprise Edition.* Java 2 Edición empresarial.
JCP: *Java Community Process.* Proceso de la comunidad Java.
JMS: *Java Message Service.* Servicio de Mensajes Java.
JNDI: *Java Naming and Directory Interface,* Interfaz de directorio y nombrado Java.
JSR: *Java Specification Requests.* Requisitos de Especificación de Java.
JVT: *Java Value Type*, Tipo de valor Java.
LCS: *Location Services*, Servicio de localización.
LMU: *Location Measurement Unit*, Unidad de medida de localización.

M: *Mandatory,* Obligatorio.
MAF: *Management Application Function,* Función de aplicación de gestión.
MCF: *Message Communication Function,* Función de comunicación de mensajes.
ME: *Mobile Equipment*, Equipo Móvil.
MGCF: *Media Gateway Control Function*, Función de Control de Pasarelas Multimedia.
MIB: *Management Information Base*, Base de Información de Gestión.
MF: *Mediation Function,* Función de mediación.
MNP: *Mobil Number Portability*, Portabilidad de número móvil.
MNP-SRF: *Mobile Number Portability/Signalling Relay Function*, Portabilidad de número móvil / Función de relevo de señalización.
MO: *Manager Object*, Objetos gestionado.
MORT: *Managed Object Referring to Test*, Objeto gestionado referenciador de una prueba.
MRF*: Multimedia Resource Function*, Función de Recursos Multimedia.
MS: *Mobile Station,* Estación Móvil.
MSC: *Mobile-services Switching Centre*, Central de Conmutación de Móviles.
MSC-S: *MSC Server*, Servidor de MSC.
MSISDN: *Mobile Subscriber ISDN Number*, Número ISDN del suscriptor móvil.
MSRN: *Mobile Subscriber Roaming Number*, Número de roaming del suscriptor móvil.
MT: *Mobile Termination*, Terminación Móvil.
NE: *Network Element*, Elementos de red.
NEPs: *Network Equipment Providers,* Proveedores de equipo de red.
NGOSS: *Next Generation Operations Systems and Software*, Sistemas de operaciones y software de nueva generación.
NM: *Network Management*, Gestores de red.
NPDB: *Number Portability Database*, Base de datos de portabilidad de número.
NRM *Network Resource Model*, Modelo de recursos de red.
O: Optional, Opcional.
OS: *Operation System*, Sistema de operaciones.
OSA: *Open Service Architecture*, Arquitectura de servicio abierta.
OSI: *Open System Interconnection*, Interconexión de sistemas abiertos.
OSS/J: OSS a través de Java.
OSS: *Operations Support Systems*, Sistemas de soporte de operaciones.
OSF: *Operations Systems Function,* Función de sistema de operaciones.
PCO: *Point Of Control and Observation,* Punto de control y observación.
PDU: *Protocol Data Unit*, Unidad de datos de protocolo.
PLMN: *Public Land Mobile Network*, Red móvil publica terrestre.
PS: *Packet Switched*, Conmutación de paquetes.
PTO: *Public Telecommunications Operator*, Operadores públicos de telecomunicaciones.
QoS: *Quality of Service,* Calidad de Servicio.
RFRC: Registro de Fichero de Registro Cronológico
RCD: Red de Comunicación de Datos

RD&M: *Resource Development & Management,* Gestión y Desarrollo de Recursos.
RFCs: Registros de Fichero Cronológico.
RM&O: *Resource Management & Operations*, Operaciones y gestión de recursos.
RNC: *Radio Network Controller*, Red de Radio Controladora.
RNS: *Radio Network Subsystems*, Subsistemas de Red Radio.
SDH: *Synchronous Digital Hierarchy,* Jerarquía digital sincrónica.
SGSN: *Serving GPRS Support Node*, Nodo Soporte GPRS Servidor.
SGW: *Signalling Gateway Function*, Función de pasarela de señalización.
SIs: *System Integrators, Integradores de sistemas.*
SID: *Shared Information and Data,* Información y datos compartidos.
SIM: *Subscriber Identity Module*, Módulo de identidad del suscriptor.
SLA: *Service Level Agreement*, Acuerdos de Nivel de Servicio.
SMLC: *Serving Mobile Location Center*, Centro de localización móvil servidor.
SM&O: *Service Management & Operations*, Operaciones y gestión de servicios.
SMS-GMSC: *SMS Gateway MSC*, Pasarela SMS/MSC.
SN: *Serving Network,* Dominio de red servidora.
SNMP: *Simple Network Management Protocol*, Protocolo de gestión de red simple
SNMPv2: SNMP versión 2
TA: *Terminal Adapter*, Adaptador Terminal.
TAP: Trayecto de Acceso a la Prueba
TE: *Terminal Equipment*, Equipo Terminal.
TIB: *Task Information Base*, base de información de tareas
TMForum: *TeleManagement Forum*
TMN: *Telecom Management Network*, Red de gestión de telecomunicaciones
TMSI: *Temporary Mobile Subscriber Identity*, Número temporal de la estación móvil.
TN: *Transit Network*, Red de Tránsito
TO: *Test Object*, Objeto de Prueba
TOM: *Telecom Operation Map*, Mapa de operaciones de telecomunicaciones
UDP: *User Datagram Protocol*, Protocolo de datagrama de usuario
UE: *User Equipment*, Equipo de Usuario.
UISF: *User Interface Support Function,* Función de soporte de interfaz de usuario
UMTS: *Universal Mobile Telecommunications System,* Sistema de telecomunicaciones móviles universal.
USIM: *User Services Indentity Module*, Modulo de Identidad de Servicios de Usuario.
UTRA: *Universal Terrestrial Radio Access*, Acceso radio terrestre universal.
UTRAN: *UMTS Terrestrial Radio Access Network*, Red de acceso a radio terrestre UMTS.
VLR: *Visitor Location Register*, Registro de posición de visitantes.
WSF: *Workstation Function,* Función de estación de trabajo.
WSSF: *Workstation Support Function,* Función de soporte de estación de trabajo.
XML: *Extensible Markup Language,* Lenguaje de etiquetas extensible.

INTRODUCCIÓN

La gestión de redes entendida como la planificación, organización, operación, mantenimiento y control de los elementos que forman una red para garantizar un nivel de servicio de acuerdo a un costo, puede jugar un papel decisivo en cuanto a establecer diferenciación y poder competir en un mercado que evoluciona rápidamente, ya que está directamente involucrada con los procesos de negocio y estrategias generales que implementan las empresas tanto a nivel interno como en la relación externa con sus clientes y proveedores.

La continua búsqueda de la optimización de las redes por parte de los proveedores de servicio y los desarrolladores de las tecnologías de la información, ha llevado a éstos a centrarse en el aumento de los sistemas de gestión, los cuales permiten la reducción de los costos de operación, incrementan la productividad del personal y protegen las fuentes de ingresos. Dentro de estos sistemas de gestión, la gestión de fallas, llega a tener gran importancia, debido a que al aumentar la disponibilidad de la red, mediante la adecuada monitorización del rendimiento de los servicios, la rápida identificación y localización de los problemas (antes de que éstos ocurran), se logra un aumento en el grado de satisfacción de los usuarios, y se tiene también como resultado la reducción de las pérdidas de ingresos por la caída de los mismos.

El mundo de las comunicaciones evoluciona rápidamente, y los operadores y proveedores de servicio luchan por mantenerse en el mercado implementando estrategias como la inclusión de nuevos servicios y disminución de fallas dentro de su red para lograr una diferenciación en calidad y servicio con su competencia. En ese sentido las redes móviles de 3G, están incursionando a nivel global con innovadores servicios y con sistemas de gestión y soporte de operaciones que garantizan la calidad y rentabilidad a su red.

En la actualidad, es indispensable para una red de telecomunicaciones, ya sea móvil o fija, tener un sistema relacionado con las actividades que controlan, supervisan y registran la utilización de los recursos de telecomunicaciones y permiten la evaluación de la calidad de funcionamiento de estos. Muchas empresas en Colombia y en el mundo han adquirido este tipo de sistemas de gestión para soportar algunas de sus operaciones. En la mayoría de los casos se han inclinado por sistemas de soporte de operaciones (OSSs, Operation Support Systems) con módulos únicamente de gestión de servicios pero su tendencia es a adquirir OSSs mas completos que les brinden una gestión integrada que asegure la flexibilidad de la configuración y la supervisión del estado de los recursos de sus redes, para proporcionar a los usuarios servicios de telecomunicaciones con un cierto nivel de calidad.

El presente proyecto plantea el diseño de un OSS, con el cual se dará solución a factores

esenciales en la gestión de redes como son: la detección, localización, aislamiento de averías, ya que incluyen las técnicas destinadas a minimizar las pérdidas de servicio provocadas por éstas, de forma que la calidad de los servicios ofrecidos al abonado sea la mejor. La rápida evolución de las telecomunicaciones y el auge de las redes de 3G en el mundo, orientan este proyecto hacia este tipo de redes, que aunque por el momento no existen en nuestro país, muy seguramente se emergerá a ellas debido al continuo avance y crecimiento de las telecomunicaciones y la necesidad de inclusión de nuevos servicios que permitan a las empresas mantenerse y proteger sus ingresos.

El Diseño del OSS para gestión de fallos en redes de 3G se basa en los conceptos del modelo de arquitectura de gestión TMN que define los protocolos usados para la gestión que trata el proyecto, y es considerado en la actualidad el más eficaz para este tipo de desarrollos debido a las facilidades que presenta en cuanto a integración y gestión de elementos. Para el diseño a realizar, también se analizarán cuales son las herramientas que nos presenta la tecnología J2EE con la iniciativa OSS/J, de la cual hay demasiada expectativa en el campo debido a que es una tecnología de componentes reusables y la cual aún se encuentra en proceso de estandarización.

La contribución de este proyecto a la FIET, en especial al Departamento de Telecomunicaciones y al grupo de investigación GNTT es en el área de gestión de redes de Telecomunicaciones donde se dejará el Diseño de un sistema de soporte de operaciones para una red 3G basado en estándares, acompañado del análisis y aplicación de la tecnología J2EE de Java que servirá de guía para futuras implementaciones orientadas a sistemas de soporte de operaciones y a la gestión de fallas en diferentes redes de telecomunicaciones.

1. GENERALIDADES DE GESTION DE REDES Y OSS's

La gestión de redes surge a partir de la demanda creciente sobre calidad de las redes y costos operacionales en aumento (mas precisamente: por la necesidad de reducir esos costos), debido al incremento del volumen de computadoras y otros dispositivos inteligentes, que tenían que ser interconectados por diferentes herramientas de comunicación (líneas de comunicación de datos, LANs, etc.). El incremento de la complejidad de los elementos de red amplifica la importancia de tener sistemas de gestión de elementos robustos con base en una plataforma total de gestión. Si una red no opera de modo confiable, sino se pueden identificar posibles errores por métodos simples, y sino se pueden mantener bajo control determinados parámetros operacionales de la red, y eventualmente ser modificados, los usuarios no obtendrán demasiados beneficios de la red implementada con gran costo.[1]

Como resultado de la aplicación de un sistema de gestión de red se puede obtener las siguientes ventajas:

- Incremento de confiabilidad gracias a la disminución de tiempo requerido para detección de error, diagnóstico y corrección de errores,
- Incremento de la eficiencia de los procesos de corrección de errores y la posibilidad de reenrutar tráfico de red automáticamente si alguna parte de la red opera en déficit.
- Acceso a la red controlado y regulado para cada usuario y de acuerdo a autorizaciones y autenticaciones predefinidas lo que permite un incremento de seguridad en la red.
- Nuevos servicios provistos a los usuarios de red (adquisición de información de tarificación, de tráfico, etc.).
- Almacenamiento de información de tarificación, estadística, seguimiento y evaluación de carga y rendimiento de la red, así como estadísticas de errores, y soporte de estrategias de desarrollo de red, que permiten un efectivo monitoreo del sistema

Para obtener estas ventajas en la red, el sistema de gestión debe operar siguiendo una serie de pasos que comienzan en la adquisición y recolección de datos acerca de los elementos de la red, como de su operación e interrelación en la red es decir de su desempeño, condiciones operacionales, condiciones de falla, parámetros de tráfico entre otros. Posteriormente estos datos son almacenados y evaluados en un centro de procesamiento de datos para dar lugar al control operacional de la red.

Se debe tener en cuenta que si el sistema de gestión realiza operaciones de gestión de servicios o de negocios, es necesario incluir unos pasos adicionales como el registro de contratos de servicio y gestión de servicios de cliente, elaboración de planes de negocios, modelado y diseño, simulación

de procesos técnicos y/o financieros.

Pero para poder llevar a cabo estos pasos del proceso de gestión en una red es necesario contar con una arquitectura de red sofisticada, elementos de red apropiadamente elaborados, y un sistema de gestión de red apropiado.

En la actualidad, los proveedores de servicios buscan mejorar sus redes pensando en la completa satisfacción del cliente, pues no se puede olvidar que las exigencias y requerimientos acordes a las necesidades del cliente evolucionan rápidamente, además buscan la forma de aumentar el valor de sus redes y mejorar su situación financiera. Para encontrar esa mejora los proveedores adoptan nuevas tendencias, que exigen la implementación de sistemas de soporte de operaciones OSS's para incrementar la eficacia operacional y dar visibilidad a los datos de red y prontitud en el servicio a nivel de gestión de cliente. [2]

En la redes de 3G la gestión es una preocupación aún más importante, ya que los operadores buscan una mayor facilidad de acceso a la amplia gama de soluciones de servicios y funcionamiento de los mejores distribuidores del mercado. Las redes de tercera generación y los nuevos modelos comerciales continuamente aumentan la demanda de soluciones de gestión, donde las interfaces abiertas son uno de los principales impulsores.

1.1 SISTEMAS DE SOPORTE DE OPERACIONES OSS's

En el contexto de la Gestión de Redes fueron creados dos grandes grupos de sistemas para dar soporte a los procesos operacionales de una proveedora de servicios de telecomunicaciones:

- los sistemas de soporte de negocios (BSS, Business Support Systems) que involucran sistemas como facturación y CRM, y
- los sistemas de soporte de operaciones OSS.

Un OSS es una entidad lógica que representa un sistema de gestión aceptado para telecomunicaciones y redes de datos que provee grandes ventajas. Un OSS integrado es una combinación de aplicaciones que actúan con otras redes para lograr una vista consolidada de la gestión y la funcionalidad de la red entera. Una plataforma OSS planeada e integrada permite que los proveedores de servicios de telecomunicaciones operen la red de forma más eficientemente manejando bajos costos mientras generan más ingresos con el mismo inventario.

Los OSSs están compuestos por un amplio conjunto de aplicaciones usadas por los proveedores de servicios para unir su red de infraestructura a los usuarios finales. Un OSS se puede dividir en tres categorías principales:

- Cumplimiento del servicio: Aplicaciones, tales como la entrada de pedidos, el suministro y el inventario, que se usan para suministrar un servicio.
- Seguridad del servicio: Aplicaciones, tales como los acuerdos de nivel de servicio, la gestión de fraudes y la gestión de fallos, que se utilizan para garantizar un servicio.
- Tarificación y atención al cliente: Aplicaciones que se usan para recoger las ganancias de un servicio y para dar soporte a los usuarios; incluyen la recogida y transmisión de los registros de los detalles de las llamadas y los centros de llamada de los clientes.

Un OSS puede proporcionar a los proveedores de servicios importantes beneficios como los son alta productividad, menos errores, número reducido de visitas a los clientes, automatización, mejor uso de los activos, menor desorden, entre otros.

El software OSS es requerido por proveedores de servicio para gestionar y soportar operaciones diarias como la gestión de un rango de dispositivos, donde cada uno de los dispositivos puede tener un sistema de gestión de elemento correspondiente que extraiga y proporcione información para el OSS.

En la actualidad las soluciones OSS existentes no cubren el rápido incremento de escala de las redes, la diversidad de tecnologías de comunicaciones y el aumento de expectativas en cuanto a disponibilidad y confiabilidad. Con el fin de dar soporte e impulsar el desarrollo y utilización de este tipo de soluciones el TMForum (TeleManagement Forum) definió en 1998 la información necesaria para la gestión de los operadores de telecomunicaciones en el mapa de operaciones de telecomunicaciones (TOM, Telecom Operation Map), donde se identifica una serie de procesos relacionados con atención al cliente, gestión de servicio y gestión de red, y se ofrece una visión de alto nivel de estos, consolidando una visión operacional de la empresa como un todo por medio de la integración de las funciones de BSS y OSS. [3]

En el 2002 el TMForum perfecciona el modelo TOM y le da el nombre de mapa de operaciones de telecomunicaciones mejorado (eTOM, Telecom Operation Map), el cual describe todos los procesos de negocio que requiere un proveedor de servicios, sirviendo este como plano-piloto para la dirección de procesos y como punto de referencia para las necesidades de reestructuración de procesos internos, asociaciones, alianzas y acuerdos generales de funcionamiento con otras empresas para lograr la anhelada interoperabilidad de redes. El modelo eTOM estandarizado en la recomendación ITU-T M.3050 ayuda a establecer los limites en los componentes software de los sistemas de soporte de tal forma que se adecuen a las necesidades de los clientes y sirva para definir sus funciones, entradas y salidas.

El eTOM mejora el mapa de operaciones de telecomunicaciones anterior, en el sentido que mejora la visión de los procesos y los vínculos entre procesos de negocio en la gestión de la empresa utilizados por los proveedores de servicio, añadiendo el aseguramiento de la integración de los sistemas de soporte de la empresa relacionados con suministro de servicio y soporte de servicio.

Además provee una base en el análisis y concepción de procesos de negocio para la industria y también una guía para el desarrollo de OSS/BSS.

Vale mencionar que eTOM como marco de procesos de negocios forma parte de la iniciativa de los sistemas de operaciones y software de nueva generación (NGOSS,) del TMForum y sirve de vínculo con otros trabajos que se realizan en relación con los NGOSS.

El eTOM expone en detalle los elementos de proceso que conforman cada área de la actividad de la empresa que provee servicio de forma que esos elementos o componentes se colocan en un marco definiendo las relaciones organizacionales, funcionales y flujos de proceso que se intercambian en las diferentes actividades de negocio. El mayor logro obtenido con este marco por los proveedores de servicio y operadores de red radica en que los productos que han adquirido para la gestión de red y negocios y servicios logran una mejor integración y bajos costos como resultado de la automatización de estos procesos.

Si la integración se planea alrededor del eTOM, el proveedor de servicio será capaz de llevar un mejor control sobre los procesos comerciales, lo que tiene un impacto directo en los ingresos.

Las áreas principales del eTOM son:

- El área de procesos Operacionales es el corazón del eTOM, dónde se incluye todos aquellos procesos que soportan las operaciones y administraciones con los clientes.
- El área de procesos de Estrategia, infraestructura y Producto incluye todos los procesos necesarios para desarrollar estrategias, construir la infraestructura, desarrollar y administrar productos, que son llevados a cabo por la cadena de proveedores y/o socios de negocios.
- El área de procesos de la Administración Corporativa incluye los procesos básicos para operar cualquier tipo de negocio. Estos procesos están enfocados en los niveles de procesos corporativos, en las metas y objetivos. Estos procesos tienen interfaces con casi todos los procesos de la corporación, ya sean procesos operacionales, sobre productos o infraestructura.[4]

1.2 OSS's y REDES DE 3G

Cómo mantener el sistema (equipos de telecomunicaciones) en un estado en que la calidad de los servicios ofrecidos al abonado sea aceptable, es la preocupación fundamental de los operadores y se convierte entonces en la base de todo sistema de gestión, es necesario que las redes de tercera generación cuenten con un sistema de gestión de fallos que permita identificar los fallos o alarmas que se produzcan en toda la red, y que permita encaminar la información obtenida en esa gestión hacia las personas adecuadas, para que se tomen las medidas necesarias según sea el caso.

Los sistemas de gestión de fallos para 3G deben cumplir con los siguientes puntos esenciales en la gestión de redes:

- El mantenimiento preventivo con el objetivo fundamental de minimizar la aparición de averías.
- Detección, localización y aislamiento de averías, que permita restaurar los sistemas en caso de alguna avería. Es necesario igualmente crear mecanismos de aislamiento para minimizar la repercusión de dichas averías.
- Mantenimiento correctivo, el cual una vez detectado, localizado y aislado el error o fallo, debe repararse o sustituirse la unidad afectada (soporte lógico o soporte físico).

Al ser implementado un sistema gestor de fallas se obtiene grandes ventajas como lo son el incremento de la productividad, reducción en el tiempo fuera de servicio de la red, resolver problemas fácil y rápidamente y satisfacer a los clientes en la solución de problemas.

Para gestión de fallas en redes de telecomunicaciones de 3G se debe tener en cuenta la recomendación de la UIT-R M.1168 [5], para la gestión de las telecomunicaciones móviles internacionales-2000 (IMT-2000, International Mobil Telecommunications 2000) donde se hace énfasis en una arquitectura de red de gestión organizada, con el objetivo de lograr la interconexión entre los diversos tipos de sistemas de funcionamiento y equipos de telecomunicaciones de forma que pueda haber un intercambio de información de gestión utilizando una arquitectura acordada con interfaces normalizadas.

A continuación se mencionan las consideraciones y objetivos propuestos en la recomendación M.1168 [5], en lo que corresponde a gestión de fallas.

- Asegurar la integridad, la flexibilidad de la configuración y la supervisión del estado de los recursos de las IMT-2000, para proporcionar a los usuarios servicios de telecomunicaciones con un cierto nivel de calidad;
- Ofrecer una arquitectura abierta para las IMT-2000 que permita una fácil introducción de los avances tecnológicos así como distintas aplicaciones;
- Tener capacidades de gestión de complejidad variable;
- Intercambiar la información de gestión adecuada entre los distintos operadores de las IMT-2000;
- Interoperabilidad entre las IMT-2000 y la amplia gama de redes y servicios asociados actuales o futuros;
- Ofrecer una arquitectura de gestión para soportar un entorno de IMT-2000 multivendedor.
- Definir la información de gestión que va a intercambiarse entre las interfaces normalizadas en términos del modelo OSI.
- Soportar la capacidad y dispersión geográfica de las funciones de control.

- Considerar la interoperabilidad entre los operadores de las IMT-2000, tanto públicos como privados, que den servicio a zonas superpuestas o adyacentes.
- Permitir la suficiente flexibilidad en la configuración del sistema de manera que puedan satisfacerse los requisitos concretos del operador de las IMT-2000 relativos a la disponibilidad de los servicios ofrecidos por estos sistemas.
- Ofrecer la capacidad de informar sobre sucesos y reacción a los mismos de manera común, a fin de permitir el control remoto y simplificar las intervenciones de mantenimiento.
- Minimizar la complejidad de la gestión de las IMT-2000.
- Minimizar la carga provocada por el tráfico de gestión cuando se utiliza la red de telecomunicaciones para cursarle.
- Definir los métodos y el tipo de control que debe utilizarse para realizar de la manera más rápida posible el establecimiento del sistema e introducir modificaciones en el mismo.
- Permitir el soporte y el control de un número cada vez mayor de recursos, lo que permitiría iniciar el sistema con una configuración pequeña y sencilla que iría creciendo, tanto en tamaño como en complejidad, a medida que sea necesario.

1.3 TMN Y OTRAS ARQUITECTURAS DE GESTIÓN

Para saber que arquitectura es la más conveniente, en la realización del proyecto es necesario saber las incidencias que tienen estas en cuanto a determinados campos claves en el diseño del OSS para gestión de fallas en una red de 3G. Para ello se describe en esta sección las características esenciales de estas y su aplicabilidad a redes móviles de tercera generación.

1.3.1 Gestión basada en el protocolo de gestión de red simple (SNMP, Simple Network Management Protocol). SNMP en si es un grupo de estándares de protocolos que definen reglas de intercambio entre las diferentes entidades software de gestión (Agente, Gestor y Base de Información de Gestión), que debido a su gran éxito se ha convertido en un estándar de facto en gestión de redes.

La información que ofrecen los dispositivos SNMP se definen a través de una base de información de gestión (MIB, Management Information Base), que son las variables ofrecidas para realizar las consultas. La MIB está descrita en ASN.1 para facilitar su transporte transparente por la capa de red.

Cada agente SNMP ofrece información dentro de una MIB, tanto general (definida en los distintos Registros de Fichero Cronológico RFCs) como de aquellas extensiones que desee proveer cada uno de los fabricantes.

SNMP es generalmente utilizado como una aplicación cliente/servidor asincrónica, de tal forma que

tanto el agente como el gestor pueden generar un mensaje para el otro y esperar una respuesta, en caso de que haya que esperar una. SNMP utiliza UDP como un protocolo de transporte de mensajes. Los mensajes están formados por un identificador de versión, un nombre de comunidad SNMP y una unidad de datos de protocolo (PDU, Protocol Data Unit). [6]

- **Aplicabilidad en 3G.** SNMP posee una gran ventaja es que permite fácilmente tener una sencilla implementación en las redes, que le da grandes posibilidades de actualización y expansión, además que la información de gestión requerida o que se necesite intercambiar ocupa pocos recursos de la red.

  Por ser uno de los primeros protocolos, la gran mayoría de fabricantes diseñan dispositivos que soportan SNMP. Por lo cual en la actualidad es el sistema más extendido.

  El gran inconveniente de este modelo es que presenta grandes fallas de seguridad, que pueden permitir a personal no autorizado, o intrusos acceder a la información que lleva la red, e incluso pueden llegar a bloquear o deshabilitar terminales. En la segunda versión SNMPv2, se introducen mecanismos para corregir este problema como:

  - Privacidad de los datos. Los intrusos no puedan tomar información que va por la red.
  - Autentificación, para prevenir que los intrusos manden información falsa por la red.
  - Control de acceso, que restringe el acceso a ciertas variables a determinados usuarios

  El principal problema de SNMP es que la información está poco organizada. La segunda versión introduce estructuras de datos para hacer más fácil el manejo. [7]

  La falta de eficiencia y flexibilidad de este modelo respecto a otros como OSI o TMN es una razón determinante a la hora de aplicarlo a una red de 3G ya que es un protocolo básicamente basado en técnicas de sondeo, lo cual le impide ejercer un buen control sobre redes extensas, y es principalmente concebido para proveer funcionalidad de gestión a nivel de red y de elemento de red y no es regido por eventos. Además SNMP no puede ser considerado como un verdadero Sistema de Gestión de Red orientado a objetos ya que no permite la reutilización de atributos y definiciones, lo cual va en contra de la recomendación M.1168 en la cual se especifica que la información sobre gestión de las IMT-2000 debe describirse utilizando el paradigma orientado a objeto. Sumando desventajas de SNMP ante una red 3G, este es un protocolo no orientado a la conexión lo que disminuye sus posibilidades frente a otros protocolos, porque cuando se envía un mensaje nunca se puede asegurar que el mensaje llega a su destino.

1.3.2 Gestión basada en el protocolo de información de gestión común (CMIP, Common Management Information Protocol). El Protocolo Común de Gestión de Información “CMIP”, esta basado en SNMP y soluciona los problemas y errores que presentaba este, volviéndose un

arquitectura de gestión de red más detallada.

En la gestión basada en CMIP, el proceso de aplicación de usuario es provisto con el servicio común de información de gestión (CMIS, Common Management Information Service). El gestor como elemento software del sistema puede generar operaciones de gestión en forma de request CMIS a cualquier agente utilizando el protocolo CMIP y el agente retransmite los requests a los objetos gestionados (MOs, Manager Objects) que representan los recursos físicos o lógicos.

La gestión sobre el modelo de interconexión de sistemas abiertos (OSI, Open System Interconnection) se basa en el uso del protocolo de la séptima capa (Aplicación) para el intercambio de información de gestión según el paradigma gestor–agente, donde la entidad agente se encarga de aplicar operaciones sobre los objetos gestionados.[8]

- **Aplicabilidad en 3G.** OSI tiene múltiples ventajas frente a otras arquitecturas de gestión de redes, entre ellas encontramos:

  - CMIP utiliza una técnica basada en eventos. Esto permite a CMIP ser más eficiente que SNMP en el control de grandes redes.
  - CMIP a diferencia de SNMP es un protocolo orientado a conexión. Esto significa que la carga de proceso de SNMP es reducida, pero cuando se envía un mensaje no se puede asegurar que el mensaje llega a su destino. La seguridad de los datos no es prioritaria para SNMP.
  - CMIP permite la implementación de comandos condicionales sofisticados, mientras que SNMP necesita el nombre de cada objeto.
  - CMIP permite, mediante una única petición, la recogida de gran cantidad de datos de los objetos gestionables, enviando información de retorno en múltiples respuestas. Esto no está permitido en SNMP.
  - CMIP está especialmente preparado para gestionar grandes redes distribuidas, mientras que SNMP está recomendado para la gestión Internet.
  - CMIP realiza una distinción clara entre los objetos y sus atributos. SNMP no permite esto, lo cual hace imposible la reutilización de atributos y definiciones.

Todas estas ventajas sumadas a que la recomendación M.1168 impone como condición que la información de gestión que va a intercambiarse entre las interfaces normalizadas se debe definir en términos del modelo OSI, hace que este sea una buena opción a utilizar.

Mas sin embargo se requiere gran cantidad de recursos para realizar la gestión, 10 veces más que SNMP, lo cual implica realizar grandes modificaciones a la red a gestionar para que soporte este sistema.

1.3.3 Gestión de Redes de Telecomunicaciones (TMN, Telecommunications Management Network).

El término TMN fue introducido por la ITU-T, y está definido en la recomendación M.3010 [9]. TMN incorpora conceptos del modelo OSI como lo son la adopción del paradigma gestor-agente, es orientado a objetos y trabaja con dominios de gestión.

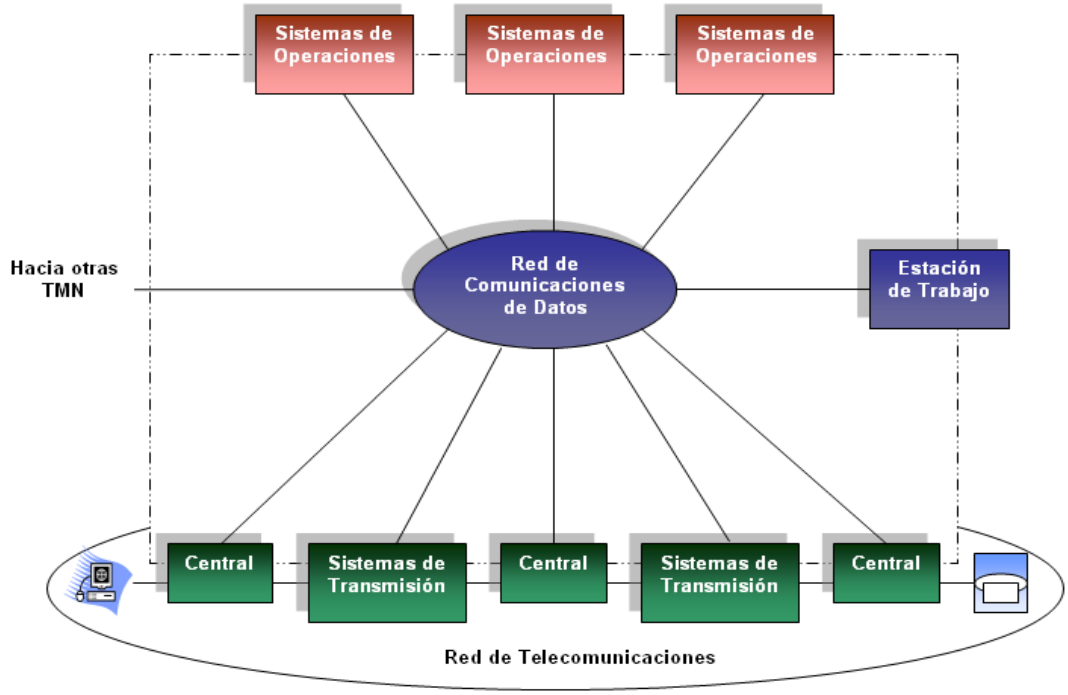
En la recomendación M.3010 de la ITU-T se define el término gestión como un conjunto de capacidades que permiten intercambio y procesamiento de la información de gestión para ayudar a los operadores públicos de Telecomunicaciones (PTO, Public Telecommunications Operator) a realizar sus actividades con eficacia; el termino red de telecomunicaciones se define como un conjunto de equipos de telecomunicaciones digitales y analógicos y equipos de soporte asociados, y finalmente el concepto de servicio se muestra como una gama de capacidades proporcionadas a los clientes.

TMN ofrece a los proveedores de servicio una arquitectura organizada, para la interconexión de los diferentes sistemas de operaciones y elementos de telecomunicaciones. En la Figura 1 se puede observar claramente la relación entre una TMN y una red de telecomunicaciones.

Los requisitos de la arquitectura TMN con el propósito de orquestar diferentes sistemas de gestión y lograr la eficiencia de la red son:

- intercambio de información de gestión entre la red gestionada y la red TMN;
- intercambio de información entre entornos TMN;
- conversión de información de gestión de un formatos a otro para un intercambio consistente de información;
- transferencia de información entre diferentes puntos de una TMN;
- análisis de la información de gestión y la capacidad de actuar en función de ella;
- manipulación de la información de gestión en un formato útil para el usuario de la misma;
- entrega y presentación apropiada de la información de gestión al usuario de esta;
- acceso seguro a la información de gestión por los usuarios autorizados.

Figura 1. Relación general entre una TMN y una red de Telecomunicaciones



- **Aplicabilidad en 3G.** Anteriormente se dijo que el modelo OSI era una buena opción; es de recordar en este momento que TMN, como sistema de gestión estandarizado, más comprensible, y basado en OSI, resulta una mejor opción como modelo de gestión para 3G que CMIP, además TMN hace referencia en que la red que transporta información de gestión este separada de la red que se gestiona, lo cual corrige el problema de OSI que requiere gran cantidad de recursos para realizar la gestión, lo que implica realizar grandes modificaciones a la red a gestionar para que soporte este sistema.

  TMN ofrece a la redes de 3G una variedad de funciones como planificación, instalación, puesta en servicio, explotación, mantenimiento, administración y servicios de abonado en un entorno multivendedor y multioperador, y de acuerdo a la recomendación M.1168 las IMT-2000 deben aplicar dicho concepto de TMN para su gestión de red.

  Adicionalmente TMN proporciona a los operadores de redes de tercera generación un conjunto de capacidades para permitir el intercambio y procesamiento de la información sobre gestión de forma que los ayuda a realizar sus actividades comerciales de manera eficaz.

  Por las ventajas que presenta TMN frente a las otras arquitecturas de gestión, es la arquitectura escogida para el diseño del OSS para gestión de fallas en redes de 3G.

2. DISEÑO DEL OSS PARA GESTIÓN DE FALLAS EN UNA RED 3G.

2.1 METODOLOGÍA APLICADA AL DISEÑO DEL OSS

Para llevar a cabo el diseño planteado en este proyecto se seguirá la metodología propuesta en la recomendación M.3020 [11] de la ITU-T con el Titulo “Metodología de Especificación de Interfaz de la Red de Gestión de las Telecomunicaciones”, donde se describe la metodología de especificación de interfaces de la TMN y los procesos utilizados para derivar especificaciones de la interfaz TMN con base en los requisitos de los usuarios de esta. Las directrices están redactadas en forma de servicios de gestión que contienen descripciones de objetivos, funciones de gestión y recursos de telecomunicaciones TMN.

Esta metodología está dividida en dos áreas de actividad principales: tareas de aplicaciones y tareas de protocolo.

Cada tarea tiene una base de información asociada.

Cada base de información de tareas (TIB, task information base) contiene el resultado de iteraciones anteriores de la metodología, y representa una manera acumulativa normalizada de efectuar determinada tarea dentro de la metodología [11].

De acuerdo a la recomendación ITU-R M.1168 [5] “Marco General para la Gestión de las Telecomunicaciones Móviles Internacionales-2000 (IMT-2000)” se recomienda solo implementar las primeras 4 tareas, las cuales serán seguidas en este proyecto para definir la arquitectura funcional, física y de la información del OSS para gestión de fallas, estas son:

- Tarea 0: Generación de directrices
  - TIB 0: Directrices
- Tarea 1: Descripción de servicios de gestión de la TMN y sus objetivos desde el punto de vista de los usuarios de la TMN
  - TIB A: Servicios y objetivos de gestión de la TMN
- Tarea 2: Descripción del contexto de gestión de la TMN
  - TIB B: Cometidos de gestión de la TMN, recursos de telecomunicaciones y funciones de gestión de la TMN (conjuntos de funciones de gestión/grupos de conjuntos de funciones)
  - TIB X: Modelos de información genéricos y específicos de la tecnología
- Tarea 3: Modelado de información
  - TIB C: Biblioteca de información de gestión
  - TIB D: Diagramas de relación entre objetos

- Tarea 4: Consolidación de la información disponible

Para el diseño del OSS para gestión de fallas en redes de 3G no se desarrolla las TIBs para evitar la redundancia en la información debido a que estas, son listados y descripciones de la información que se extraen de cada tarea.

2.2 TAREA 0. GENERACIÓN DE DIRECTRICES

La tarea 0 consta de las directrices, recomendaciones o documentos tomados como referencia para llevar a cabo el diseño de la red de gestión de fallos y una breve explicación de su utilización en esta metodología. Las principales recomendaciones utilizadas se listan a continuación:

- *ITU-R M.1168 Marco General para la Gestión de las Telecomunicaciones Móviles Internacionales-2000 (IMT-2000)* [5]. Recomendación utilizada para la extracción de los requisitos de Gestión en una red de 3G.
- *ITU-T M.3010 Principios para una red de gestión de las telecomunicaciones* [9]. Esta recomendación se utiliza como base conceptual de TMN para el desarrollo de la arquitectura funcional, física, lógica y de la información del OSS.
- *ITU-T M.3020 Metodología de Especificación de Interfaz de la Red de Gestión de las Telecomunicaciones* [11]. Recomendación en la cual se encuentra estandarizada la metodología en la que se basa el desarrollo de este proyecto.
- *ITU-T M.3200 Servicios de Gestión de Red de Gestión de las Telecomunicaciones y Sectores Gestionados de las Telecomunicaciones* [12]. En esta recomendación se encuentra la plantilla para la definición de los servicios de gestión (GDMS, *Guidelines for the Definition of Management Services*), que se utiliza para llevar a cabo la tarea 1.
- *ITU-T M.3400 Funciones de gestión de la red de gestión de las telecomunicaciones* [10]. Recomendación utilizada para la extracción de las funciones de los componentes que conforman la red de gestión de fallas y los mensajes de interacción entre ellos.
- *ITU-T M.3050 Mapa de Operaciones de Telecomunicaciones Mejorado (eTOM, Enhanced Telecom Operations Map)* [13]. Es utilizada para la definición de los cometidos de gestión que tiene el sistema de soporte de operaciones para gestión de fallos.
- *CCITT X.710 Servicio común de información de gestión* [14]. Esta Recomendación define un elemento de servicio común de información de gestión, utilizado por las interfaces que hacen parte de la arquitectura de información para intercambiar información e instrucciones a los efectos de la gestión de la red 3G
- *ITU-T X.733 Gestión de Sistemas: Función Señaladora de Alarmas* [15]. Se utiliza con el fin de obtener conceptos básicos para la gestión de alarmas en una red de Telecomunicaciones.
- *CCITT X.734 Gestión de sistemas: Función de gestión de informe de evento* [16]. Documento de donde se obtiene conceptos básicos sobre los informes de evento que se generan en la red de gestión.
- *CCITT X.735 Gestión de sistemas: Función control de ficheros registro cronológico* [17].

Recomendación usada con el fin de obtener conceptos básicos sobre los ficheros que representan los almacenes principales de información de gestión del OSS.

- *ITU-T X.737 Gestión de Sistemas: Categorías de Pruebas de Confianza y de Diagnóstico [18].* Esta recomendación es utilizada para la extracción de las categorías de prueba que se pueden desarrollar en los diferentes elementos de la red de telecomunicaciones.
- *ITU-T X.745 Gestión de sistemas: función de gestión de prueba* [19]. Se utiliza con el fin de obtener conceptos básicos para la realización y gestión de pruebas en una red de Telecomunicaciones.
- *ITU-T X.790 Función de gestión de dificultades para aplicaciones del sector de normalización de las telecomunicaciones de la unión internacional de telecomunicaciones* [20]. Documento utilizado para la extracción de conceptos referentes a la gestión de dificultades en el OSS para gestión de fallas.
- 3GPP TR 23.821 V1.0.1 *Principios Arquitecturales Versión 2000* [21]. Recomendación utilizada para la definición de los elementos a gestionar en una red móvil de 3G.
- 3GPP TS 32.101 V3.4.0 *Gestión de Telecomunicaciones 3G: Principios y requerimientos de alto nivel (Versión 1999)* [22]. Recomendación utilizada para la extracción de los requerimientos de gestión de una red UMTS.
- 3GPP TS 32.111-1 V6.0.0 *Gestión de telecomunicaciones; Gestión de fallas; Parte 1: Requerimientos de gestión de fallas en 3G* [23]. Recomendación utilizada para la obtención de los requerimientos en cuanto a gestión de fallos en una red 3G, y definición de los objetivos de Gestión del OSS.
- *3GPP TS 32.111-2 V6.4.0 Gestión de telecomunicaciones. Gestión de fallas; Parte 2: Punto de Referencia de Integración (IRP) de Alarmas: Servicio de Información (IS, Information Service)* [24]. Esta recomendación es utilizada en el diseño con el fin de obtener un modelo estandarizado que sirva de base, para el desarrollo de la arquitectura de la información del OSS.
- *3GPP TS 32.111-4 V6.4.0 Gestión de telecomunicaciones. Gestión de fallas. Parte 4: Punto de referencia de integración de alarmas (IRP, Integration Referente Point): Protocolo de gestión de información común (CMIP, Common Management Information Protocol), Set de Solución (SS, Solution Set)* [25]. Se utiliza para obtener conceptos básicos de las interfaces CMIP, y definiciones GDMO para gestión de alarmas sobre las interfaces CMIP, que sirven de soporte a la arquitectura de la información del OSS.
- *3GPP TS 32.312 V6.2.0 Gestión de telecomunicaciones. Punto de referencia de integración (IRP) de gestión genérico; Servicio de Información* [26]. Documento donde se define un servicio común soportado por todos los IRPs. Es utilizado para definición de los puntos de referencia de integración de los diferentes sistemas de gestión que componen el OSS de gestión de fallas.
- *3GPP TS 32.322 V6.1.0 Gestión de telecomunicaciones. Punto de Referencia de Integración de Pruebas. Servicio de Información (IS)* [27]. Esta recomendación es utilizada en el diseño del OSS, para la extracción de conceptos referentes a los atributos que posee una prueba.
- *3GPP TS 32.622 V6.4.0 Gestión de telecomunicaciones; Punto de referencia de integración*

(IRP) de gestión de configuración de recursos de red: Modelo de recursos de red (NRM, Network Resource Model) [28]. Esta recomendación presenta un modelo de información de gestión enfocado hacia los recursos de la red, que es utilizado para la definición de las clases de objetos de información relacionados con las entidades que son monitoreadas por el OSS para gestión de fallas.

- *3GPP TS 32.692 V6.1.0 Gestión de telecomunicaciones. Punto de referencia de integración (IRP) de gestión de inventario de recursos de red: Modelo de recursos de red (NRM)* [29]. Recomendación utilizada en el diseño con el fin de obtener un modelo estandarizado que sirva de base, para el desarrollo de la arquitectura de la información del OSS.

2.3 TAREA 1. DESCRIPCIÓN DE SERVICIOS DE GESTIÓN DEL OSS Y SUS OBJETIVOS

Siguiendo el orden de la metodología propuesta, en la tarea 1 se realiza la descripción de servicios de gestión del OSS y sus objetivos desde el punto de vista de los usuarios. Esto se realiza tomando como referencia los puntos 1 y 2 de la plantilla para la definición de los servicios de gestión (GDMS, *Guidelines for the Definition of Management Services*) presentada en el Anexo A de la recomendación ITU –T M.3020 [11].

2.3.1 Descripción del servicio de gestión. La gestión de fallos se logra por medio de varios Procesos/Subprocesos como, vigilancia de alarmas, detección de fallas, localización de esas fallas, reporte fallas, corrección de la fallas, reparación de la fallas, pruebas. Estos Procesos/Subprocesos están situados sobre diferentes capas de gestión, sin embargo, la mayoría de ellas están situadas principalmente sobre las capas de elemento de red y de gestión de elemento de red, puesto que esta infraestructura subyacente de la red tiene capacidades “autocurativas”.

Es posible, sin embargo, que algunas fallas que afectan los servicios de telecomunicación sean detectadas dentro de las capas de “gestión de la red y servicios", correlacionando las alarmas/eventos (originado por diversos elementos de red) y correlacionando datos de la red, a través de la gestión de datos de red.

Adicionalmente a estos procesos se debe hacer una correcta gestión de los problemas que el cliente reporta a la red, de tal forma que permitan vislumbrar fallas que no han sido detectadas. De forma similar si la ocurrencia de una falla afecta un servicio, se debe tomar las medidas de gestión necesarias para que el cliente final sufra el menor impacto posible en el servicio, y sea informado en caso de una interrupción.

2.3.2 Objetivos de gestión. Cualquier evaluación del estado operacional de la red móvil de 3G, así como la gestión de calidad y mantenimiento requiere una adecuada gestión de fallas, que permita detectar, aislar y corregir un funcionamiento anormal de la red de telecomunicaciones y de

su entorno sin que el cliente se percate o tenga una afectación notoria en el servicio, importante para mejorar la calidad del servicio, y para disminución de costos operacionales además de obtener la satisfacción del cliente y el cumplimiento de los SLAs (Acuerdos de Nivel de Servicio).

2.3.3 Requerimientos de Gestión de Fallas en 3G. Cualquier evaluación del estado operacional de los elementos de red (NEs, Network Elements) y la red global requiere la detección de fallas en la red, y consecuentemente, la notificación de alarmas a los OSs (Operation Systems) gestores de elementos (EM, Element Managers) y/o gestores de red (NM, Network Management).

Dependiendo de la naturaleza de las fallas, estas pueden ser combinadas con un cambio del estado operacional de los recursos físicos o lógicos afectados por las fallas. La detección y notificación de esos cambios de estado es tan esencial como lo es para las alarmas. Una lista de alarmas activas en la red y la información del estado operacional así como datos del historial de estados y alarmas son requeridos por el operador del sistema para su posterior análisis. Además, los procedimientos de prueba pueden ser usados con el fin de obtener información más detallada si es necesaria, o verificar una alarma, estado, o correcta operación de los NEs y sus recursos lógicos y físicos.

Adicionalmente es también necesaria una adecuada gestión de dificultades que permita reflejar la detección de fallas en los elementos de red, hacia los servicios que se prestan al cliente.

Las siguientes numerales explican la detección de fallas, el manejo de alarmas, cambios de estado, la ejecución de pruebas y la gestión de dificultades que conforman la funcionalidad que debe poseer un sistema de soporte de operaciones integral para gestión de fallas.

2.3.3.1 Fallas y Alarmas. Las fallas que pueden ocurrir en la red pueden ser agrupadas dentro de una de las siguientes categorías:

- Fallas de Hardware, por ejemplo el malfuncionamiento de un recurso físico dentro de un NE.
- Problemas Software por ejemplo virus, bases de datos inconsistentes.
- Fallas funcionales, por ejemplo fallas de algún recurso funcional en el NE, donde ningún componente hardware puede ser encontrado responsable del problema.
- Pérdida de alguna o todas las capacidades especificas de los NEs debido a situaciones de sobrecarga.
- Fallas en las comunicaciones entre dos NEs, o entre NE y OS, o entre dos OSs.

2.3.3.2 Detección de fallas. Cuando algún tipo de las fallas ya descritas ocurre dentro de una red de 3G, las entidades de red afectadas deben ser capaces de detectarlas inmediatamente, usando circuitos y procedimientos autónomos de comprobación propia o self-check, incluyendo en el caso de NEs, la observación de medidas, contadores y umbrales. Los umbrales de las medidas pueden ser predefinidos por el fabricante y ejecutados de forma autónoma en los NE, o pueden estar

basados en medidas de desempeño o funcionamiento administradas por el EM.

Las fallas deben tener condiciones bien definidas para la declaración de su presencia o ausencia, por ejemplo las condiciones de su ocurrencia y clareo. Las entidades de red deben ser capaces reconocer cuando una falla con características de autodetección y autoclareo (ADAC, Automatically Detected and Automatically Cleared) que ha sido detectada previamente, deja de estar presente. Para algunas las fallas, no existen condiciones de clareado ya que son automáticamente detectadas pero manualmente clareadas (ADMC Automatically Detected and Manually Cleared), entonces la red de gestión deberá informar al operador sobre la falla, para que el realice las actividades pertinentes para su adecuado clareo. En otros casos, no hay necesidad de alguna acción a corto término, ni de los operadores del sistema ni de la entidad de red en si misma, debido a que la condición de falla dura solo un corto periodo de tiempo y desaparece.[23]

Para cada falla los procesos de detección de fallas suplirán la siguiente información:

- las pequeñas unidades reemplazables dispositivos/recursos/archivos/funcionalidad.
- el tipo de la falla;
- la severidad de las fallas (indeterminada, advertencia, menor, mayor, critica);
- la probable causa de la falla;
- el tiempo en el cual la falla fue detectada en la entidad de red defectuosa;
- la naturaleza de la falla, por ejemplo ADAC o ADMC;
- alguna otra información que ayuda a entender la causa y la ubicación de la situación anormal (sistema o implementación específica).

Para algunas fallas, medios adicionales, tal como funciones de pruebas y diagnostico, pueden ser necesarias para obtener el nivel requerido de detalle.

2.3.3.3 Generación de alarmas. Cada falla detectada, se apropia de alarmas que son generadas por la entidad de red defectuosa, independiente de si esta es una falla ADAC o una ADMC. Cada alarma contendrá toda la información proveída por el proceso de detección de fallas.

Para simplificar la localización y reparación de fallas, la entidad de red defectuosa generará para cada falla, una alarma singular y múltiples eventos relacionados a esta en el caso en que una falla cause una degradación de las capacidades operacionales de uno o más recursos lógicos o físicos dentro de la entidad de red. Si una entidad de red no esta en capacidad de reconocer una falla, manifiesta esto mismo en diferentes caminos, de tal forma que la falla es detectada como múltiples fallas y origina múltiples alarmas. En este caso sin embargo, cuando la falla es reparada la entidad de red será capaz de detectar la reparación de todas las múltiples fallas y clarear las múltiples alarmas relacionadas.

Cuando una falla ocurre sobre un medio de conexión entre dos NEs o entre una NE y una OS, y

afecta las capacidades de comunicación entre cada NE/OS, cada NE/OS afectada detectara la falla como se describe en el numeral correspondiente a *Detección de fallas* y generará su propia alarma asociada de comunicación hacia el gestor OS. En este caso es la responsabilidad del OS correlacionar o asociar las alarmas recibidas de diferentes NEs/OSs y ubicar la falla en el mejor camino posible.

Todas las alarmas generadas por los NEs serán introducidas a una lista de alarmas activas, la cual estará a disposición de los OSs para soportar las diferentes actividades de gestión que requieran de esta información. [23]

2.3.3.4 Clareo de alarmas. Las alarmas originadas como consecuencia de fallas necesitan ser clareadas. Para clarear una alarma es necesario reparar la correspondiente falla. Este procedimiento de reparación de fallas es una implementación dependiente o condicional que puede llevarse a cabo por medio de las actividades que se presentan a continuación:

- Las fallas de software son reparadas por medio de la inicialización de sistemas globales o parciales, por medio de parches software o actualizaciones.
- Las fallas de comunicaciones son reparadas por el reemplazo del equipo de transmisión defectuoso o, en caso de ruido excesivo, por la remoción de la causa del ruido.
- Las fallas de QoS son reparadas por la remoción de las causas que degradan la QoS o por mejoramiento de la capacidad del sistema para reaccionar contra las causas que pueden resultar en una degradación de QoS.
- Solucionar los problemas de ambiente reparando las fallas del ambiente, por ejemplo alta temperatura, alta humedad, etc.

Es también posible que una falla ADAC sea espontáneamente reparada, sin la intervención del operador (por ejemplo una falla de cruce de umbral). En un principio, El NE usa el mismo mecanismo para detectar que una falla ha sido reparada, como para la detección de la ocurrencia de una falla. Sin embargo, para fallas ADMC, la intervención manual por el operador es siempre necesaria para clarear la falla. Prácticamente, varios métodos existen para que el sistema detecte que una falla ha sido reparada y las alarmas y las fallas que las provocan han sido clareadas. Por ejemplo:

- El operador del sistema implícitamente pide al OS clarear una falla, por ejemplo inicializar un nuevo aparato o dispositivo que remplace uno defectuoso. Una vez el nuevo dispositivo ha sido exitosamente colocado en servicio, el NE clareara la falla. Consecuentemente, el NE clareara todas las alarmas relacionadas.
- El operador del sistema explícitamente pide el clareo de una o más alarmas. Una vez la alarma/alarmas ha sido clareada, el sistema gestor de fallas debe reproducir esas alarmas (como nuevas alarmas) en caso que la situación de falla aún persista.
- El NE detecta el intercambio de un aparato defectuoso por uno nuevo y lo inicializa de forma

autónoma. Una vez el nuevo dispositivo ha sido colocado exitosamente en servicio, el NE clareara las fallas. Consecuentemente el NE clareara todas las alarmas relacionadas.

- El NE detecta que una alarma de cruce de umbral previamente reportada ya no tiene más validez. Este entonces clareara la correspondiente alarma activa y la falla asociada, sin requerir alguna intervención del operador. Los detalles de la administración de umbrales y la condición exacta para que el NE claree alarmas de cruce de umbral son implementaciones específicas.
- Las alarmas y fallas ADMC puede, por definición, no ser clareadas por un NE automáticamente. Por lo tanto, en algún caso, las funciones del operador del sistema serán capaces de pedir el clareo de alarmas y fallas ADAC en el NE creadas como consecuencia de una falla ADCM. En el caso que la alarma o falla ADCM haya sido clareada, el NE clareara la falla o alarma ADAC asociada.

Los detalles de estos mecanismos son sistemas o aplicaciones específicos.

En el momento en que una alarma es clareada el NE generará un evento apropiado de clareo de alarma. Un clareo de alarma es definido como una alarma, excepto que su severidad es iniciada en "clareada". La relación entre una clareo de alarma y activación de alarma es establecida:

- Por la reutilización de un conjunto de parámetros que identifican excepcionalmente la activación de alarma.
- Por la inclusión de una referencia a la alarma activa en la alarma clareada.

Cuando un clareo de alarma es generado, la correspondiente activación de alarma es removida de la lista de alarmas activas.

2.3.3.5 Envío y filtrado de alarmas. Tan pronto como una alarma es ingresada o removida de la lista de alarmas activas las notificaciones serán enviadas por el OS agente, en forma de notificaciones no solicitadas hacia el OS gestor.

Si el envío no es posible en ese momento, por ejemplo debido a que la comunicación esta fallando, entonces las notificaciones serán enviadas tan pronto como las capacidad de comunicación haya sido recuperada. El espacio de almacenamiento es limitado. La capacidad de almacenamiento es dependiente del operador e implementación. Si el número de notificaciones retardadas excede el espacio de almacenamiento entonces un proceso de sincronización de alarma será corrido cuando la capacidad de comunicación haya sido recuperada. El OS detectará las fallas en la comunicación que impiden la recepción de alarmas y levantan una alarma apropiada al operador.

El reporte de eventos incluirá toda la información definida para el respectivo evento, más una identificación del NE que generó el reporte. El operador del sistema será capaz de permitir o suprimir el reporte de alarma por cada NE. Como mínimo, el siguiente criterio será soportado por el filtrado de alarma:

- El NE que genero la alarma.
- Los dispositivos/recursos/funciones relacionados con la alarma.
- La severidad de la alarma.
- El tiempo en el cual las alarmas son detectadas, por ejemplo el tiempo de alarma.
- Alguna combinación de los criterios anteriores

2.3.3.6 Almacenamiento y recuperación de alarmas desde el NE. Para los propósitos de gestión de fallas (FM), se debe almacenar y recuperar la siguiente información:

- Una lista de las alarmas activas, que aún no han sido clareadas;
- La información de historial de alarma, por ejemplo notificaciones relacionadas a la ocurrencia y clareo de alarmas.

El espacio de almacenamiento del historial de alarmas en los OSs es limitado. La capacidad de almacenamiento, y la duración, por la que los datos pueden ser retenidos o guardados, es a criterio del operador e implementación independiente.

2.3.3.7 Recuperación de fallas: una vez la falla ha sido detectada y el reemplazo de las unidades defectuosas han sido identificadas, algunas funciones de gestión son necesarias con el fin de ejecutar el sistema de recuperación y restauración, automáticamente por el NE y/o el EM, o manualmente por el operador. Las funciones de recuperación de fallas son usadas en varias fases de la gestión de fallas (FM):

- Una vez la falla ha sido detectada, el NE será capaz de evaluar el efecto de la falla en los servicios de telecomunicaciones y de forma autónoma toma acciones de recuperación con el fin de minimizar la degradación o discontinuidad del servicio.
- Una vez la unidades defectuosas han sido reemplazadas o reparadas, será posible desde el EM colocar previamente la unidad defectuosa nuevamente en servicio a fin que la operación normal sea restaurada. Esta transición deberá ser hecha de forma que los servicios de telecomunicaciones proveídos actualmente no sean mínimamente interrumpidos o perturbados.
- En algún momento el NE estará habilitado para ejecutar acciones de recuperación si son requeridas por el operador. El operador pueden tener varias razones para requerir tales acciones; por ejemplo el ha deducido un condición defectuosa o fallida por el análisis y correlación de los reportes de alarma, o el desea verificar que el NE es capaz de ejecutar las acciones de recuperación (mantenimiento proactivo).

Las fallas se pueden dividir en dos categorías: fallas software o fallas hardware. En el caso de las fallas SW, dependiendo de la severidad de la falla las acciones de recuperación pueden ser inicializaciones de sistemas(a diferentes niveles), activación de la carga de un software backup (soporte), activación de la carga de un software fallback (sistema de soporte UPC en situación de

emergencia para reponer la información que se perdió), descarga de una unidad de software, etc. En caso de fallas en el hardware, las acciones de recuperación dependen en la existencia y tipo de redundancia de los recursos. La redundancia de algunos recursos puede ser proveída en el NE con el fin de lograr tolerancia a fallas y para mejorar la disponibilidad del sistema.

Si los recursos defectuosos no tienen redundancia, las acciones de recuperación serán:

a) Aislar y remover del servicio, el recurso para que no pueda perturbar la operación de otros recursos.
b) Remover del servicio los recursos funcionales y físicos que son dependientes de uno defectuoso. Esto previene la propagación de los efectos de la falla a otros recursos libres de falla.
c) Actividades relacionadas a la gestión del estado para el recurso defectuoso y otros recursos afectados /dependientes.
d) Generar y enviar las notificaciones apropiadas para informar al OS sobre todos los cambios ejecutados.

Si los recursos defectuosos son redundantes, el NE ejecuta las acciones a), c), y d) anteriores. Existen varios tipos de redundancia (por ejemplo: hot stand-by, cold stand-by, duplex, simétrica/asimétrica, Redundancia N plus one o N plus K, etc.), y para cada una, hay una secuencia especifica de acciones para ser ejecutadas en caso de falla.

En caso de una falla en un recurso proveedor de un servicio, la secuencia de recuperación comenzará inmediatamente. Antes o durante el cambio, una temporal y limitada perdida de servicio será aceptable. En caso de un comando de gestión, el NE ejecutará el cambio sin la degradación del servicio de telecomunicaciones. [23]

2.3.3.8 Configuración de alarmas. Será posible configurar las acciones de alarmas, umbrales y severidad por medio de comandos de acuerdo a los siguientes requerimientos:

- El operador será capaz de configurar algún umbral que determine la declaración o clareo de una falla. Si una serie de umbrales son definidos para generar alarmas de varias severidades, entonces para cada severidad de alarma el valor de umbral será configurable individualmente.
- Será posible modificar la severidad de las alarmas definidas en el sistema.

2.3.3.9 Gestión de estado. La gestión de estado es un servicio común definido en la gestión de configuración y usado para varias áreas de gestión, incluyendo la gestión de fallas. En esta cláusula son definidos algunos requerimientos detallados en la gestión de estado que se aplican a la gestión de fallas.

Desde el punto de vista de la gestión de fallas, son utilizados dos tipos de estados, *el estado*

administrativo y el estado operacional. Adicionalmente los recursos pueden tener algunos atributos de “status” secundarios que darán posteriormente información detallada sobre la razón del estado primario.

- Para corrección de fallas el estado Administrativo puede ser usado para aislar los recursos defectuosos;
- En caso de redundancia el estado administrativo puede ser usado para cerrar el recurso activo y dejar el recurso en stand by para ponerlo activo (mantenimiento preventivo).
- Para gestión de pruebas el estado Administrativo puede ser usado para colocar un recurso fuera de servicio para correr una prueba intrusa en este.

El estado operacional da la información sobre la capacidad real de un recurso para proveer o no proveer servicio.

- El estado operacional es “habilitado” cuando el recurso es capaz de proveer el servicio, “deshabilitado” cuando el recurso no puede proveer el servicio.
- Un recurso puede perder la capacidad de proveer servicio a causa de una falla o a causa de otros recursos de los cuales este depende están fuera de servicio. (Por ejemplo deshabilitados o cerrados).
- En caso que un recurso no pierda completamente su capacidad para proveer servicio, El estado operacional será “habilitado” y el estado de disponibilidad será “degradado”.

Cuando un cambio de estado es generado por una falla, la notificación de alarma y la notificación de cambio de estado relacionada estará correlacionada con otras por medio de la relación explicita de información.

2.3.3.10 Propagación y Cambio de Estado. Dentro de un elemento gestionado, cuando por alguna razón un recurso cambia de estado, el cambio será propagado, en un camino consistente o uniforme, para todos los otros recursos que sean funcionalmente dependientes del primero. Por consiguiente:

- En caso que una falla ocurra en un recurso, hace que el recurso quede completamente fuera de servicio, si el estado de operación actual esta (habilitado), este será cambiado a “deshabilitado” y una notificación de cambio de estado será generada. Entonces todos los recursos condicionados (siguiendo el diagrama específico de dependencia de fallas) serán chequeados y en caso que ellos sean “habilitados” ellos serán cambiado a “deshabilitados”. En este proceso, también el estado secundario será cambiado regularmente, de forma que será posible distinguir si un objeto es deshabilitado por estar fallando o porque este es funcionalmente dependiente de otros objetos los cuales están deshabilitados.
- En el caso que un recurso defectuoso es reparado, el estado operacional de ese recurso es cambiado de “deshabilitado” a “habilitado” y todos los recursos dependientes son vueltos a

"habilitados" (este es un simple caso). En un caso más complejo, algunos de los objetos pueden ser deshabilitados por diferentes causas (diferentes fallas o fallas mejor detectadas en recursos superiores), en este caso los recursos reparados pueden ser vueltos a "habilitados" solo cuando todas las causas sean cambiadas regularmente.

- En el caso que un operador frena o pone fuera de servicio un recurso, el proceso de propagación de cambio de estado es similar al primer caso (recurso defectuosos) excepto por el recurso cerrado el cual no cambia su estado operacional pero si sus estado administrativo de "abierto" a "cerrado". Los recursos dependientes son procesados como en el primer caso.
- En el caso que un operador abre (unlocked) un recurso, el proceso de propagación de cambio de estado es similar al segundo caso (reparación de fallas) excepto por el primer recurso (el abierto) el cual no cambia su estado operacional pero si el estado administrativo de "cerrado" a "abierto". Los recursos dependientes son procesados como en el primer caso.

2.3.3.11 Gestión de pruebas. Las funciones de gestión proveen capacidades que pueden ser usadas en diferentes fases de la gestión de fallas (FM). Por ejemplo:

- Cuando una falla ha sido detectada y si la información proveída a través del reporte de alarma no es suficiente para localizar el recurso defectuoso, pueden ejecutarse pruebas para mejor localización de las fallas.
- Durante la operación normal del NE, las pruebas pueden ser ejecutadas para el propósito de detección de fallas.
- Una vez un recurso defectuosos ha sido reparado o reemplazado, antes de ser restaurado para el servicio, se pueden hacer pruebas ejecutadas en este recurso para asegurar que esta libre de fallas.

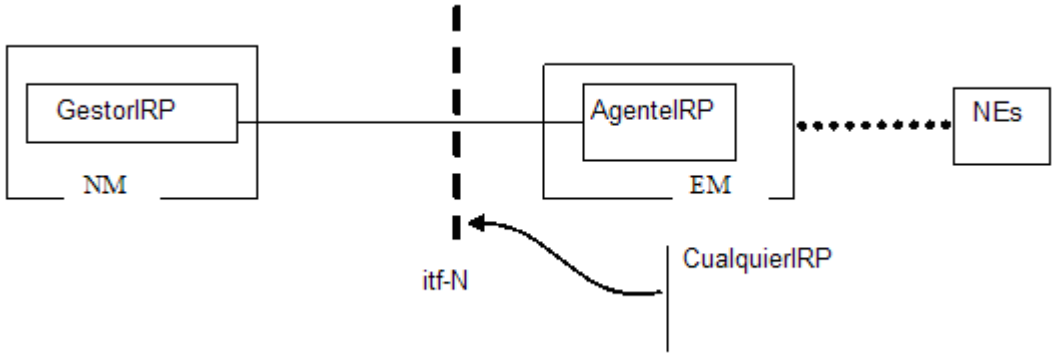
Sin embargo, a pesar del contexto donde la prueba es usada, su objetivo es siempre el mismo: verificar si los recursos físicos o funcionales de un sistema se desempeñan o ejecutan apropiadamente y, en caso que este pase a ser defectuoso, provee toda la información para ayudar al operador a localizar y corregir las fallas.

El testeo o pruebas es un actividad que involucra al operador, el sistema de gestión (el OS) y el sistema o elemento gestionado (el NE). Generalmente el operador solicita la ejecución de pruebas desde el OS, y el NE gestionado ejecuta autónomamente las pruebas sin un posterior soporte del operador. En algunos casos, el operador solicita que solo un sistema de pruebas sea establecido (por ejemplo establecer conexiones internas especiales, proveer puntos de acceso a pruebas, etc.). El operador puede entonces ejecutar la prueba real, la cual puede requerir algún soporte manual para manejo de equipo de prueba externo. Una vez la prueba concluye el OS que hizo la petición recibirá el resultado de la prueba o el informe sobre la causa de la terminación de ésta, adicionalmente el OS podrá observar o cambiar los parámetros de la prueba mientras está permanezca activa. Las notificaciones e informes generados como resultado de la prueba serán almacenados por el OS gestor para su posterior análisis.

2.3.3.12 Gestión de Fallas concepto de interfaz N. Un sistema de operaciones en el nivel de gestión de red (por ejemplo: el NM) provee servicios de gestión de fallas y funciones requeridas por el operador 3G sobre el nivel de gestión de elementos.

La interfaz N (Itf-N) puede conectar el sistema de gestión de red (NM, Network Management) a los gestores de elementos (EMs, Element Managers) o directamente a los elementos de red (NEs, Network Elements). Esto es hecho por medio de puntos de Referencia de Integración (IRPs Integration Referente Points). Posteriormente el término "entidades subordinadas" define EMs o NEs, las cuales están encargadas de soportar la interfaz N. (Ver Figura 2)

Figura 2. Diagrama Interfaz N



3rd GENERATION PARTNERSHIP PROJECT. Telecommunication management. Generic Integration Reference Point (IRP) management: Information Service (IS). 3GPP, 2005. p 8.: il.(3GPP TS 32.312)[26].

En la Figura 2 se puede identificar el concepto de itf-N en términos de implementaciones llamadas GestorIRP y AgenteIRP.

El GestorIRP representa un proceso que interactúa con el AgenteIRP con el propósito de recibir notificaciones por medio del IRP. El o los AgenteIRP envían notificaciones que transportan eventos al GestorIRP. Un GestorIRP puede ser un proceso que corre en un NM. El AgenteIRP implementa y soporta el IRP y corre dentro de un EM con uno o más NEs.

Proveer a la NM la capacidad de Gestión de Fallas de la red implica que las entidades subordinadas tienen que proveer información sobre:

- Eventos y fallas que ocurren en las entidades subordinadas.
- Eventos y fallas de las conexiones hacia las entidades subordinadas y también de las conexiones en la red 3G.
- La configuración e inventario de red (por el hecho que las alarmas e información de cambios

de estado relacionados son siempre originados por recursos de redes). Por lo tanto, para el propósito de la gestión de fallas las entidades subordinadas envían notificaciones a un NM indicando.

- Reporte de alarmas (indicando la ocurrencia o el clareo de fallas en las redes subordinadas), así que la información de las alarmas relacionadas pueda ser actualizada.
- Reporte de eventos de cambio de estado, con el fin de que el informe de estado (operacional) relacionado pueda ser actualizado.
- Configuración y reportes de pruebas.

El envió de esas notificaciones es controlado por el operador NM usando mecanismos de filtraje adecuados en las entidades subordinadas.

El Itf-N provee también medios para permitir al operador NM el almacenamiento ("logging") y después la evaluación de la información deseada en las entidades subordinadas.

Para una red de tercera generación, se pueden identificar tres IRPs fundamentales para soportar los procesos de gestión de fallos, una IRP para información correspondiente a alarmas, una IRP para información relacionada con el estado de los recursos o inventario, y una para lo que concierne a información de gestión de pruebas.

A la capacidad de recuperación de la información relacionada con alarmas le conciernen dos aspectos:

- Recuperación de información "dinámica" (por ejemplo estados, alarmas), los cuales describen la condición de alarma momentánea en las entidades subordinadas y permite al operador NM una sincronización de sus datos de visión de alarmas.
- La recuperación de la información del historial desde los logs (anotación de las actividades que se producen en un ordenador o en dos ordenadores, por ejemplo; la activación y clareo de alarmas y cambios de estado ocurridos en el pasado), los cuales permiten la evaluación de eventos que podrían haber sido perdidos, por ejemplo después de una falla en la interfaz Itf_N o un sistema de recuperación.

En cuanto al inventario y estado de los NEs se refiere la itf-N permite al NM alterar el estado administrativo y operacional de un recurso de red inventariado, así como la modificación de sus atributos. También le es permitido al NM la adición o eliminación de recursos con el fin de dar soporte a la gestión de fallas de la red de 3G. Por medio de este IRP el EM notifica al NM sobre cualquier evento ocurrido en el inventario o cualquier cambio en el estado de los recursos.

El IRP correspondiente a gestión de pruebas permite al NM enviar peticiones de pruebas hacia el EM y este a su vez responder con notificaciones que transportan el resultado de estas.

Como una consecuencia de los requerimientos descritos anteriormente, ambos el NM y la entidad subordinada serán capaces de iniciar la comunicación.

- **Mapeo de alarmas y reportes de cambios de estado y pruebas.** Las alarmas, los reportes de cambio de estado y resultados de pruebas recibidos por el NM están de acuerdo con el modelo de información de Itf-N. Este modelo de información hecho a la medida de las capacidades del multi-proveedor es diferente desde el modelo de información de la interfaz EM-NE (si un EM esta disponible) o desde el modelado de recursos interno en el NE (en caso de interfaz directa NM-NE). Por lo que un mapeo de alarmas y reportes de eventos de cambios de estado y pruebas es ejecutado por una función de mediación en la entidad subordinada. La función de mediación traduce el reporte original de evento de alarma, cambio de estado o resultados de pruebas (que puede contener parámetros propietarios o valores de parámetros) teniendo en cuenta el modelo de información de Itf-N.

- **Envió de reportes de eventos en Tiempo-Real.** Si la Itf-N esta en operación normal, los reportes son enviados en tiempo real por medio de la apropiada filtración localizada en la entidad subordinada. Esos filtros pueden ser controlados local o remotamente por la gestión NM (vía la Itf-N) y garantiza que solo los reportes de eventos que cumplen con los criterios predefinidos pueden alcanzar el NM superior.

2.3.3.13 Gestión de dificultades. A veces todos los sistemas que comprenden redes de comunicaciones tienen problemas o funcionamientos defectuosos denominados dificultades. Una dificultad en una red de comunicaciones es un problema que tiene un efecto negativo sobre la calidad de servicio percibida por los usuarios de la red y puede ser detectada como resultado de un informe de alarmas, por un informe de dificultad introducido por un usuario o por un informe hecho automáticamente por el sistema. La gestión de ese informe de dificultades es necesaria para asegurar que es atendido con miras a restablecer el servicio a su nivel de capacidad anterior.

Para llevar a cabo de forma satisfactoria la gestión de dificultades es preciso el intercambio de información sobre problemas ya detectados e información anticipada sobre inaccesibilidad del servicio. Por tanto, un proveedor de servicio puede necesitar informar a un cliente de futuras inaccesibilidades de este.

La gestión de dificultades de acuerdo a la recomendación ITU-T X.750 es el informe y el seguimiento de la dificultad entre entidades de gestión conformes (CME, *Conformant Management Entities*) que interfuncionan cooperativamente para resolver una dificultad, esto significa que la CME del gestor y la CME del agente pueden compartir la responsabilidad para resolver la dificultad.

La función de gestión de dificultades en una red de 3G puede ser utilizada por una CME que actúa con:

- un cometido de gestor para gestionar dificultad(es) y cualesquiera informes de dificultades correspondientes que han sido presentados a una CME por el cometido de agente para su resolución;
- un cometido de agente responsable de resolver una dificultad o dificultades o cualesquiera informes de dificultades correspondientes que le han sido presentados por una CME con el cometido de gestor;
- un cometido de agente y de gestor para gestionar dificultades y cualesquiera informes de dificultades correspondientes que han sido presentados internamente (es decir, a la parte que ejecuta el cometido de agente), por otra parte que ejecuta el cometido de gestor. En este caso, la propia CME es responsable de resolver la dificultad.

La gestión de dificultades es iniciada por una petición a un OS agente para crear un informe de dificultades, el cual contiene información necesaria para que un gestor gestione y siga el informe y el agente gestione y resuelva la dificultad en un entorno de cliente a proveedor de servicio. Es posible que la información contenida en un informe de dificultades y la relacionada con su gestión tenga que pasar a través de la interfaz interoperable entre dos CME. Una vez creado, el informe de dificultades pasa desde la puesta en cola hasta los estados de solución y cierre, como resultado de las acciones realizadas normalmente por la CME que actúa con el cometido de agente durante la solución de la dificultad. Las transiciones de situación y de estado pueden también producirse como resultado de la intervención de la CME con el cometido de gestor en el entorno de proveedor de servicio a proveedor de servicio.

2.4 TAREA 2. DESCRIPCIÓN DEL CONTEXTO DE GESTIÓN DEL OSS

En la tarea 2 *Descripción del contexto de gestión del OSS* se enumeran los cometidos, los recursos y las funciones de la TMN asociados con el servicio de gestión de la TMN. Esto se realiza tomando como referencia los puntos 3, 4 y 5 de la plantilla para la definición de los servicios de gestión (GDMS) presentada en el Anexo A de la recomendación M.3020 [11].

2.4.1 Descripción del contexto de gestión. Los recursos que se gestionaran en el sistema de soporte de operaciones planteado están representados por el dominio de infraestructura y entidades funcionales que conforman la arquitectura de este segmento en una red móvil de 3G. Es indispensable aclarar que no podemos hacer referencia a elementos físicos definidos, ya que no se tiene una red física base para hacerlo. En el Anexo A se muestra y se definen los componentes y la arquitectura funcional de una red UMTS Versión 2000 tomada de la recomendación 3GPP TR 23.821 V1.0.1 [21], sobre la cual se implementará el diseño del OSS para gestión de fallas.

El dominio de infraestructura consiste de los nodos físicos que realizan varias funciones requeridas

para terminar la interfaz de radio y para soportar los servicios de telecomunicaciones requeridos por los usuarios. La infraestructura es un recurso compartido que provee servicio a todos los usuarios finales autorizados dentro del área de cobertura.

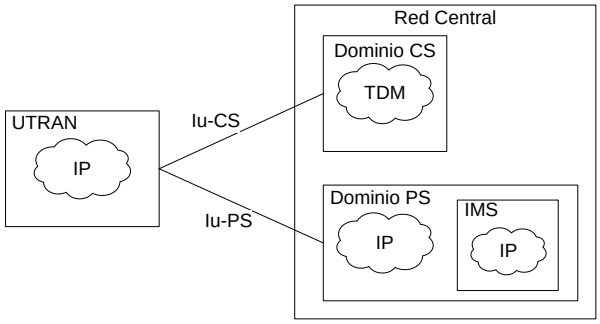
El dominio de infraestructura se divide en:

- **Red de Acceso (AN):** esta conformada por la red de acceso a radio terrestre UMTS (UTRAN, UMTS Terrestrial Radio Access Network) que consiste de entidades físicas que gestionan recursos de la red de acceso y proveen al usuario con mecanismos para acceder al dominio de red Central, y la red de acceso a radio GSM (GERAN, GSM/EDGE Radio Access Network) basada en las técnicas de transmisión de alta velocidad EDGE, combinada con mejoras sobre la interfaz del enlace de radio GPRS para dar soporte adecuado al nuevo rango de aplicaciones y clases de servicio conversacionales y de flujo continuo (streaming), incluyendo las aplicaciones de IP multimedia de UMTS.
- **La red central (CN):** esta comprendida por entidades físicas que proveen soporte para redes y servicios de telecomunicaciones, donde ese soporte incluye funcionalidades como la gestión de la información de localización de usuario, control de red y servicios, mecanismos de transferencia (conmutación y transmisión) para señalización e información generada por el usuario. El CN puede subdividirse en:

  - Dominio de Red Servidora (SN, Serving Network): es la parte de la CN conectada a la AN, y representa las funciones de la CN que son locales al punto de acceso del usuario y por tanto su ubicación cambia cuando el usuario se mueve, es responsable también del enrutamiento de llamadas y del transporte de información y datos de usuario desde la fuente hacia el destino, así como de abastecer al dominio de base de datos de usuario.
  - Dominio de Red Base (HN, Home Network): representa las funciones de la CN que son conducidas a una ubicación permanente, independiente de la posición del punto de acceso del usuario; y es responsable de la gestión de información de subscripciones y datos de usuario. El USIM está relacionado con la suscripción en la HN.
  - Dominio de Red de Tránsito (TN, Transit Network). La TN es la parte de la CN ubicada en el camino de comunicación entre la SN y la parte remota. [30]

  La CN enmarca los elementos funcionales de red que posibilitan brindar los servicios UMTS. En este sentido esta constituida por un conjunto de entidades básicas divididas en dos dominios, un dominio de conmutación de circuitos (CS) y un dominio de conmutación de paquetes (PS), los cuales difieren del camino que ellos soportan para tráfico de usuario pero tienen cosas en común como por ejemplo algunas entidades. Una Red móvil publica terrestre (PLMN, Public Land Mobile Network) puede implementar uno o ambos dominios (Ver figura 3). [31]

Figura 3. División de la red central en los dominios CS y PS



MORENO, Manuel. ÁLVAREZ, Martín Manuel. y SANZ, Joan Vinyes. Propuesta de utilización de SIP como protocolo de señalización en la red de acceso radio de sistemas UMTS. AHCIET, 2002. p 74.:il.[31]

EL dominio CS se refiere a todo el conjunto de entidades CN que ofrecen “Tipo de conexión CS” para tráfico de usuario así como todas las entidades que soportan la señalización relacionada. Un “tipo de conexión CS” es una conexión por la cual recursos de redes dedicadas son destinados o asignados al establecimiento de la conexión y liberados cuando la conexión es finalizada.

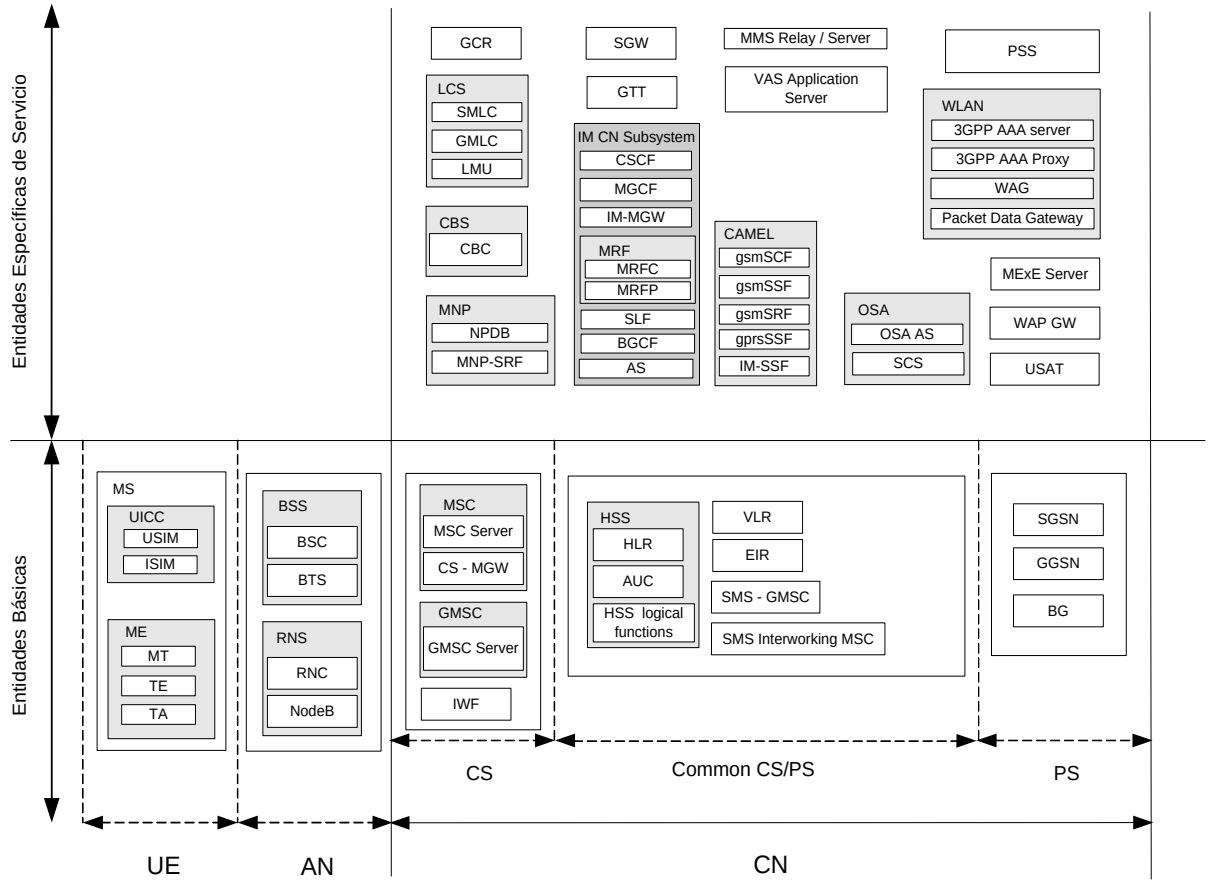
El dominio PS se refiere al conjunto de entidades CN que ofrecen “tipo de conexión PS” para tráfico de usuario así como todas las entidades que soportan la señalización relacionada. Un “tipo de conexión PS” transporta la información de usuario utilizando concatenaciones autónomas de bits llamadas paquetes: cada paquete puede ser enrutado independientemente del anterior.

Dentro del dominio PS también se encuentra el subsistema de multimedia IP (IMS, IP Multimedia Subsystem) que abarca todos los elementos de la CN para la provisión de servicios multimedia IP que comprenden audio, video, texto, chat, etc., que cumplen la función de soportar terminales con este tipo de aplicaciones.

En la red central también se encuentran otras entidades específicas de servicio dedicadas al aprovisionamiento de un determinado conjunto de servicios. Estas pueden ser o no implementadas en la PLMN, pero el impacto de su implementación deberá ser limitado para las otras entidades que conforman la red móvil.

Las entidades que conforman los dominios definidos se encuentran en la figura 4, las definiciones de estas entidades se encuentran en mayor extensión en el Anexo A de este documento.

Figura 4. Entidades que conforman los dominios de UMTS



UE: User Equipment
AN: Access Network
CN: Core Network
CS: Circuit Switched
PS: Packet Switched
MS: Mobile Station
USIM: User Services Identity Module
ME: Mobile Equipment
TE: Terminal Equipment
TA: Terminal Adaptation
BSS: Base Station System
RNS: Radio Network System
MSC: Mobile Switching Centre
GMSC: Gateway MSC

IWF: Internet Working Function
HSS: Home Subscriber Server
VLR: Visitor Location Register
EIR: Equipment Identity Register
SMS-GMSC: Gateway MSC for Short Message Service
SGSN: Serving GPRS Support Node
GGSN: Gateway GPRS Support Node
BG: Border Gateway
GCR: Group Call Register
LCS: Location Services
CBS: Cell Broadcast Services
MNP: Mobile Number Portability

SGW: Signalling Gateway
IMS: IP Multimedia Subsystem
CSCF: Call Session Control Function
MGCF: Media Gateway Control Function
MRF: Media Resource Function
MMS Relay /Server: Multi Media SMS Message Relay/Server
VAS applicable Server: Value Added Services applicable Server
CAMEL: Customised Application for Mobile Enhanced Logic
OSA: Open Service Architecture
WAP: Wireless Application Protocol

3rd GENERATION PARTNERSHIP PROJECT. Telecommunication management: Architecture. 3GPP. p 16.: il.(3GPP TS 32.102) [32]

2.4.2 Cometidos del OSS. Para lograr obtener los beneficios deseados de la gestión de redes en el OSS planteado es necesaria la aplicación del eTOM a sus cometidos para gestión de fallos, entendiéndose como cometidos las actividades que se esperan del sistema, para realizar la gestión de las telecomunicaciones. Para esto se tomo la división horizontal en bloques del nivel 0 del eTOM, que permite observar claramente la relación entre cometidos y facilita la visualización de

estos en cuanto a sus funciones. Las divisiones de nivel 0 del eTOM tomadas en cuenta son:

- Mercado, producto y cliente.
- Servicio.
- Recursos (Aplicación, informática y red).
- Proveedor/Asociado.

En la Figura 5 se puede observar la descomposición de nivel 2 del eTOM, donde se puede identificar los grupos de procesos que intervienen en la gestión de fallas. Para mayor comprensión se resaltan con rojo aquellos procesos tenidos en cuenta para el desarrollo del proyecto, los cuales tienen que ver con gestión de fallas en redes móviles de 3G, esto servirá para reconocer las asociaciones entre procesos que deben tenerse en cuenta en el sistema de soporte de operaciones.

2.4.2.1 Cometidos de Mercado, producto y cliente.

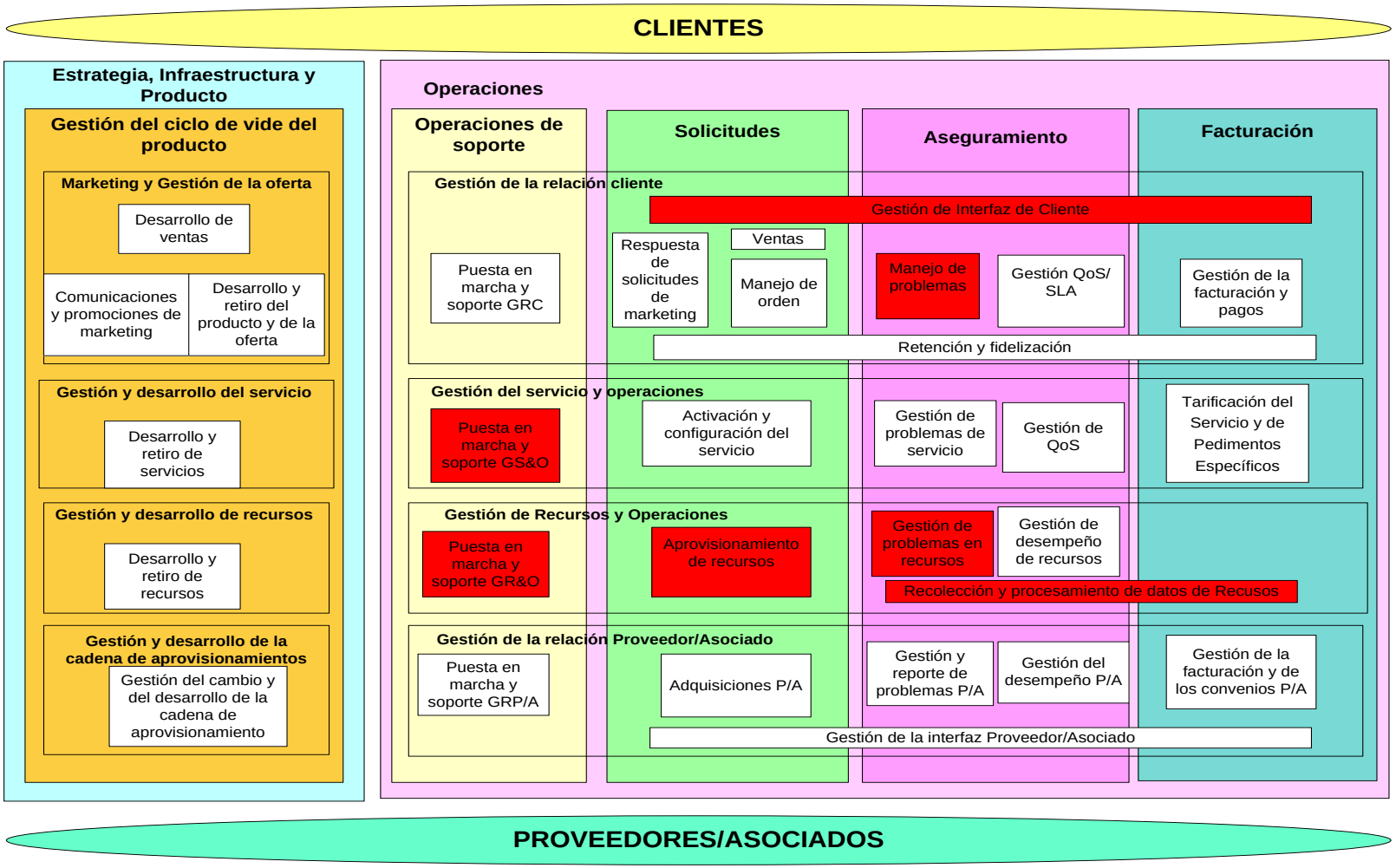
- **Manejo de Problemas.** Se encarga de recibir reportes de fallas de los clientes, resolverlos y proporcionar la reparación de estos para la restauración de la actividad al cliente. Dentro de este proceso son útiles para el diseño los siguientes subprocesos:

  - **Aislar problemas e Iniciar resolución:** se encarga de registrar y analizar reportes de problemas recibidos de clientes, aislar la fuente del problema con el fin de determinar las acciones a ser tomadas, e iniciar la solución del problema.
  - **Reportar el Problema:** el propósito de este proceso es generar y administrar todos los informes relacionados a problemas que serán publicados al cliente y/o a otros procesos.
  - **Rastreo y administración de problemas:** el propósito de este proceso es rastrear y administrar la evolución del problema durante su ciclo de vida. Para lo cual se obtiene información pro-activamente sobre el estado del problema, consiguiendo sus atributos.
  - **Cerrar Problema:** el propósito de este proceso es asegurar que un problema que afecte al cliente sea solucionado; posiblemente el cliente es contactado para preguntar por su satisfacción con la solución del problema.

- **Gestión de Interfaz de Cliente.** Dentro de este proceso son útiles para el diseño los siguientes subprocesos:

  - **Gestión de requerimientos:** el propósito de este proceso es manejar todos los requerimientos hechos por los clientes existentes o potenciales. Este recibe la demanda, habilita su ejecución automática, y activa el proceso oportuno para satisfacer el requerimiento. Puede proporcionar la información de estado en cualquier momento en el requerimiento esta activo; este cierra la demanda cuando todas las actividades relacionadas se han terminado.

Figura 5. Marco de Procesos de Negocios eTOM – Procesos de Nivel 2



Basada en INTERNATIONAL TELECOMMUNICATION UNION. Telecommunication standardization sector of ITU. Enhanced Telecom Operations Map (eTOM) .The business process framework. ITU-T, 2004. p49.:il.(ITU-T M.3050)[13]

2.4.2.2 Cometidos de Servicio.

- **Puesta en marcha y soporte.** (SM&O Service Management & Operations). Maneja clases de servicios que aseguran que la capacidad apropiada esté disponible y preparada para soportar y gestionar instancias de servicios. Dentro de este proceso son útiles para el diseño los siguientes subprocesos:
  - **Habilitación de la Activación y Configuración del servicio:** aseguran que capacidad de servicio está disponible para la asignación a un cliente. Con el propósito de mantener el funcionamiento satisfactorio del servicio o agregar capacidad servicio específica, estos procesos pueden emprender actividades de reconfiguración o pueden activar los procesos de ciclo de vida de la infraestructura con el fin de crear reglas de capacidad de servicio.
  - **Soporte de la Gestión de fallas en el servicio:** aseguran que se mantiene la disponibilidad de la clase de servicio para evitar que los clientes sean afectados por estos problemas. También realizan análisis estadísticos de los problemas, mantenimiento programado, análisis de fallas rutinario, etc., y la iniciación de acciones correctivas.

2.4.2.3 Cometidos de Recursos (Aplicación, informática y red).

- **Gestión de problemas en recursos.** Este proceso es responsable de la gestión de problemas con los recursos asignados. Dentro de este proceso son útiles para el diseño los siguientes subprocesos:
  - **Examinar y analizar Problemas de Recursos:** su objetivo es monitorear fallas de recursos en tiempo real. Las responsabilidades de este proceso incluye:
    - Analizar Eventos de Fallas de Recursos: abarca la identificación del evento. Incluye la notificación de alarmas nuevas, o los cambios de estado de alarmas previamente reportadas, así como también mensajes de cuando las alarmas han sido clareadas.
    - Correlación y Filtrado de alarmas: abarca la correlación de eventos transientes, redundantes, o implícitos con un evento específico o causa principal.
    - Detección y reporte de eventos de fallas.

    Estos procesos son también responsables de monitorear y provocar la acción apropiada cuando un problema no se resuelve dentro de un período predefinido de tiempo.
  - **Localizar Problemas de Recurso:** el objetivo de este proceso es identificar la causa principal del problema del recurso. Las responsabilidades de estos procesos incluyen: asegurarse si la configuración del recurso corresponde a las características apropiadas de servicio, realizar diagnóstico, pruebas, iniciar y parar auditorias en los recursos, programar rutinas de prueba.
  - **Corregir y Recuperar Problemas de Recursos:** el objetivo es restaurar o reemplazar recursos que han fallado y asegurar que los servicios dependientes de esos recursos sean recuperados. Estos procesos son también responsables de aislar unidades con fallas y gestionar las unidades de recursos redundantes. También reportan restauración exitosa o un intento sin éxito en la restauración, rastreo y administración de Problemas. Este proceso también se comunicará con los procesos de Soporte de Gestión de Falla de Recurso para posiblemente reparar o reemplazar el recurso o unidad defectuosa.

- **Rastrear y Gestionar Problemas de Recursos:** el objetivo es asegurar que las actividades de reparación sean asignadas y rastreadas eficazmente. Las responsabilidades de este proceso incluyen: creación de un reporte de problemas con la información apropiada, añadir información adicional para un reporte de un problema existente, modificar información de un reporte de problema existente, modificar el estado de un reporte de un problema, cancelar un reporte de un problema cuando el problema esta relacionado con una falsa alarma, reportar el cambio de estado de Problemas de Recursos. Este grupo también informará a los procesos de Cerrar Problemas de Recursos cuando el problema del recurso se ha resuelto.
- **Reporte de Problemas de Recursos:** el objetivo es reportar problemas de Recursos, por ejemplo, para los procesos de Gestión de Problemas de Servicio en caso que un informe nuevo de problema sea creado o el estado de un informe existente de problema se altere.
- **Cerrar Problemas de Recursos:** el objetivo es cerrar un reporte de problema cuando el problema del recurso se ha resuelto. También incluye interacción con los procesos de Problemas de Recursos para propósitos de reporte.

- **Recolección y Procesamiento de Datos de Recursos.** Recolecta eventos de uso de red y de tecnología de la información, e información de rendimiento para su distribución a otros procesos dentro de la empresa. Dentro de este proceso son útiles para el diseño los siguientes subprocesos:
  - **Procesar Datos de Recursos:** estos procesos son responsables de procesar la información en bruto recogida de los recursos. Esto incluye la filtración de los datos de recurso basados en criterios bien definidos, así como el suministro de los resúmenes de los datos del recurso a través de la recolección. Estos procesos son también responsables de formatear los datos del recurso antes de distribuirlos a otros procesos dentro de la empresa.
  - **Reportar Datos de Recursos:** este proceso es responsable de distribuir datos procesados del recurso a otros procesos dentro de la empresa para el análisis futuro y/o divulgación.
  - **Auditorear Datos de Uso de Recursos:** los procesos de Auditoria de Datos de Uso de Recursos son responsables de auditorear la colección de datos de recursos para identificar anomalías posibles.

- **Aprovisionamiento de Recursos.** Dentro de este proceso son útiles para el diseño los siguientes subprocesos:
  - **Configuración y Activación de Recursos:** el objetivo de este proceso es configurar y activar los recursos reservados para dar soporte a una instancia específica de servicio. Si estas actividades tienen éxito, entonces la condición de los recursos se variará entre reservada y fuera de servicio. El proceso Configurar y Activar el Recurso puede recibir peticiones múltiples para arreglar problemas de recursos y añadir capacidad de recursos para hacer frente a los problemas de rendimiento.
  - **Prueba del Recurso**: la responsabilidad del este proceso es probar recursos dando

soporte a una instancia específica de servicio. El objetivo es asegurarse si los recursos trabajan correctamente y se encuentran en los niveles apropiados de rendimiento. Si estas pruebas tienen éxito, entonces los recursos serán marcados como en servicio lo que quiere decir que los recursos están disponibles para el uso.

- **Recolectar, Actualizar y Reportar Datos de Configuración de Recursos:** el objetivo del proceso es asegurar que la Base de Datos del Inventario del Recurso refleja recursos que se están utilizando para un cliente específico.

- **Puesta en marcha y Soporte (RM&O, Resource Management & Operations).** Maneja clases de recursos, asegurando la apropiada aplicación, disponibilidad y preparación de recursos de red y computacionales para soportar y gestionar instancias de recursos. Dentro de este proceso son útiles para el diseño los siguientes subprocesos:
  - **Soporte de la gestión de fallos o problemas de los recursos**: estos procesos son responsables de asegurar que los recursos están trabajando efectiva y eficientemente. Realizan actividades de mantenimiento en recursos para identificar problemas potenciales, previendo los servicios afectados y llevan a cabo actividades de reparación. Los medios por los que los procesos de soporte de la gestión de fallas y problemas en recursos identifican fallas potenciales en los recursos incluyen el análisis de las tendencias de funcionamiento en los informes de gestión de Problema de Recurso y gestión del desempeño del Recurso y la activación de procesos de prueba y análisis de los resultados.
  - **Gestión del inventario de recursos:** Maneja los procesos de inventario de recurso que soportan todos los procesos RM&O y RD&M. Aseguran que el Banco de datos de Inventario de Recurso se sincronice con la base de recursos actual instalada por medio de las auditorias y, si soporta, mecanismos de auto descubrimiento. También abarcan la supervisión constante del nivel de disponibilidad del recurso.
  - **Gestión de Mano de Obra o Fuerza de Trabajo:** estos procesos diseñan, asignan, expiden y manejan las actividades de personal empleado que opera en la empresa. También hacen posible el monitoreo y reporte actividades asignadas.

2.4.2.4 Cometidos de Proveedor/Asociado. Para el diseño del sistema de soporte de operaciones para gestión de fallos no son implementados procesos dirigidos hacia los proveedores y asociados como tal , más sin embargo se debe tener en cuenta que estos, pueden acceder a información de gestión en cualquiera de los niveles de gestión para su posterior análisis.

2.4.3 Conjuntos de funciones de gestión de TMN y grupos de conjuntos. Ya obtenidos los cometidos del OSS para gestión de fallos es necesario saber los conjuntos de funciones que se deben implementar para cumplir satisfactoriamente esos cometidos. Estos conjuntos de funciones son obtenidos a partir del mapeo de los procesos del eTOM aplicables al diseño planteado, hacia los conjuntos de funciones de gestión que se encuentran especificados en la recomendación ITU-T M.3400 "*Funciones de gestión de la red de gestión de las telecomunicaciones"* [10].

Para definir los conjuntos de funciones que se utilizarán, se tomo como referencia las directrices

para la definición de las funciones de gestión de la RGT (GDMF, Guidelines for the Definition of TMN Management Functions) la cual contiene los siguientes ítems:

- Nombre del conjunto de funciones
- Requisitos de gestión
- Modelo funcional
- Funciones de gestión de la TMN

Para el desarrollo de esta sección de la metodología se debe tener en cuanta que tanto los requisitos de gestión, como el modelo funcional para cada conjunto de funciones, no serán especificados, pero puede ser consultado en la recomendación ITU-T M.3400 [10].

Para llevar a cabo los cometidos planteados son necesarios los siguientes conjuntos de funciones:

- **Cometidos de Recursos (Aplicación, Informática y Red):**
  - Conjunto de funciones de notificación de interrupción del servicio.
  - Conjunto de funciones de notificación de interrupción de la red.
  - Conjunto de funciones de notificación de interrupción de elementos de red.
  - Conjunto de funciones de política de alarmas.
  - Conjunto de funciones de señalamiento de alarmas.
  - Conjunto de funciones de resumen de alarmas.
  - Conjunto de funciones de criterios de eventos de alarma.
  - Conjunto de funciones de control de fichero-registro cronológico.
  - Conjunto de funciones de correlación y filtrado de alarmas.
  - Conjunto de funciones de localización de averías de la red.
  - Conjunto de funciones de localización de averías de elementos de red.
  - Conjunto de funciones de restablecimiento automático.
  - Conjunto de funciones de control y recuperación de red de acceso de prueba.
  - Conjunto de funciones de configuración de acceso de prueba.
  - Conjunto de funciones de informe de resultados y situaciones.
  - Conjunto de funciones de señalamiento de anomalías.
  - Conjunto de gestiones de indagación de información sobre anomalías.

- **Cometidos de Servicios:**
  - Conjunto de funciones de administración de fichas de anomalías.
  - Conjunto de gestiones de indagación de información sobre anomalías.
  - Conjunto de funciones de notificación de cambio de la situación del informe de anomalías.
  - Conjunto de funciones de gestión del proceso de reparación.
  - Conjunto de funciones de reparación de averías de elementos de red.

- **Cometidos de Mercado Producto y Cliente:**
  - Conjunto de funciones de acuerdo de reparación con el cliente.
  - Conjunto de gestiones de indagación de información sobre anomalías.

Dando continuidad a la metodología escogida para el desarrollo del diseño, en el siguiente capitulo se definen las funciones especificas de los conjuntos de funciones aquí establecidos que serán utilizadas para la definición de la arquitectura funcional del OSS para gestión de fallas planteado.

3. ARQUITECTURA FUNCIONAL Y FÍSICA

En este capítulo se muestra las funciones de gestión de fallas de la red de gestión, para poder definir los bloques funcionales a partir de los cuales se tiene la arquitectura funcional del OSS para gestión de fallas en redes móviles de 3G.

3.1 FUNCIONES DE GESTIÓN

Para llevar a cabo el desarrollo de la arquitectura funcional se formulan a continuación las funciones de gestión de TMN necesarias para el diseño de la red de gestión de fallas. El texto en negrilla representa el nombre de la agrupación de los conjuntos de funciones y se emplea la siguiente nomenclatura:

NX: Notificación de orden X
OX: Operación de Orden X
NAX: Notificación Adicional de orden X
OAX: Operación Adicional de Orden X

Las funciones identificadas con la nomenclatura NX y OX son funciones de gestión de TMN extraídas de la Recomendación ITU–T M.3400 [10]. Las funciones identificadas con NAX, OAX y son funciones adicionales a las encontradas en la recomendación M.3400 [10], su interacción en la red de gestión de fallas y su definición se encuentran en el Anexo B.

3.1.1 Garantía de la calidad de RAS (fiabilidad, disponibilidad y supervivencia).

- **Conjunto de funciones de notificación de interrupción del servicio:**
  - Detectar interrupción del servicio. -OA1
- **Conjunto de funciones de notificación de interrupción de la red:**
  - Detectar interrupción de la red o un segmento de red. -OA2
- **Conjunto de funciones de notificación de interrupción de elementos de red:**
  - Detección de interrupción de elemento de red. -OA3
  - Informe de interrupción del elemento de red. –NA1
  - Finalización de interrupción de elemento de red. -OA4
  - Informe de finalización de interrupción del elemento de red. –NA2
  - Adición de información relativa a interrupciones del elemento de red. –OA5

3.1.2 Vigilancia de alarmas.

- **Conjunto de funciones de política de alarmas:**
  - Establecimiento de condiciones de anulación de una señal de alarma en un cuadro. –OA6
  - Establecimiento del nivel de gravedad que se ha de asignar a unas condiciones de alarma específicas en un cuadro. –OA7
- **Conjunto de funciones de señalamiento de alarmas:**
  - Informe de alarma. –N1
  - Encaminamiento de informes de alarma. –N2
  - Petición de encaminamiento de informes de alarma. –O1
  - Asignar atributos del discriminador de remisión de los eventos especificados por el gestor. -OA8
  - Señalamiento de alarma condicional. –O2
  - Informe de asignación vigente de los atributos especificados de informe de alarmas. -NA3
  - Petición de condición de control de informe de alarma. –O3
  - Autorización/inhibición de señalamiento de alarma. –O4
  - Informe de historial de Alarmas. -NA4
  - Petición de historial de alarmas. –O5
  - Reconstrucción de historial de alarmas o de un segmento de este. -OA9
- **Conjunto de funciones de resumen de alarmas:**
  - Informe de resumen de alarmas vigentes. –N3
  - Autorización/inhibición de resumen de alarmas vigentes. –O6
  - Petición de resumen de alarmas vigentes. –O7
- **Conjunto de funciones de criterios de eventos de alarma:**
  - Acondicionamiento de criterios de eventos de alarma. -O8
- **Conjunto de funciones de control de fichero-registro cronológico:**
  - Adicionar/Eliminar informe de alarma en fichero cronológico. -OA10
  - Autorización/inhibición de inscripción en el fichero-registro cronológico. –O9
  - Inscripción condicional en el fichero-registro cronológico. –O10
  - Informe de asignación vigente de atributos especificados del fichero-registro cronológico. -NA5
  - Petición de condición de fichero-registro cronológico. –O11
- **Conjunto de funciones de correlación y filtrado de alarmas:**
  - Envío de eventos de Elementos de Red. -NA6
  - Envío de eventos adaptados o mapeados para objeto de gestión. -NA7
  - Establecer la identidad única de un evento. -OA11
  - Establecimiento de condiciones de Mapeo de Eventos. -OA12

- Adaptar un evento proveniente de un agente para el posterior manejo en el gestor. -OA13
- Filtrar eventos. -OA14
- Suprimir eventos transitorios de ocurrencia rara o intermitente. -OA15
- Suprimir eventos redundantes. -OA16
- Mantenimiento de interdependencias de evento. –O12
- Gestionar eventos de orden de llegada erróneo. -OA17
- Gestionar las condiciones del entorno. -OA18
- Activación/desactivación de acciones automáticas. –O13
- Ejecutar acción en base a la no llegada de un evento dentro de un periodo de tiempo especificado. -OA19
- Recepción de datos brutos. –O14

3.1.3 Funciones de localización de averías

- **Conjunto de funciones de localización de averías de la red:**
  - Detección de Alarma. -OA20
  - Mensaje al cliente. –N4
  - Apertura/cierre de tiques del sistema. –O15
  - Anulación/supresión de tiques de anomalía. –O16
  - Actualización de la situación de anomalía. –O17
  - Selección de una alternativa. –O18
  - Selección de un problema. –O19
  - Examen de la base de datos de anomalías. –P20
- **Conjunto de funciones de localización de averías de elementos de red:**
  - Petición de datos de diagnóstico. –O21
  - Informe de diagnóstico. –N5
  - Análisis del estado operacional en una unidad o elemento de red. -OA21
  - Informe del estado operacional de una unidad o elemento de red. -NA8
  - Cambio de Estado Operacional de una unidad o elemento de red. -OA22
  - Informe de cambio de estado operacional de una unidad o elemento de Red. -NA9
  - Planificación de pruebas de rutina. –O22
  - Comienzo/detención de pruebas de rutina. –O23
  - Informe de plan de pruebas de rutina. –N6

3.1.4 Reparación de averías

- **Conjunto de funciones de gestión del proceso de reparación:**
  - Adición de reparación. –OA23

- Reporte de finalización de reparación. –NA10
- Asignación de personal a reparación. –OA24
- Asignación de tiempo de reparación. –OA25
- Calculo de tiempo medio de reparaciones. –OA26

- **Conjunto de funciones de acuerdo de reparación con el cliente:**
  - Adicionar demanda de cliente. -OA27
  - Cerrar o finalizar demanda del cliente. -OA28
- **Conjunto de funciones de reparación de averías de elementos de red:**
  - Detección de restablecimiento automático. -OA29
  - Informe de restablecimiento automático. –N7
  - Procedimiento de auxilio inmediato. –O24
  - Procedimiento de recarga. –O25
  - Informe de recarga. –N8
- **Conjunto de funciones de restablecimiento automático:**
  - Colocar unidad fuera de servicio. -OA30
  - Informe de unidad puesta fuera de servicio. –NA11
  - Anular reestablecimiento automático. –OA31
  - Activar restablecimiento automático. –OA32
  - Informe de activación de reestablecimiento automático. –NA12
  - Informe de Anulación de reestablecimiento automático. –NA13

3.1.5 Funciones de pruebas

- **Conjunto de funciones de control y recuperación de red de acceso de prueba:**
  - Informe de inicialización del sistema de prueba. –N9
  - Inicialización y restablecimiento del sistema de acceso. –O26
- **Conjunto de funciones de configuración de acceso de prueba:**
  - Conexión de acceso de prueba. –O27
  - Liberación del acceso de prueba. –O28
  - Inicio de Comprobación de un Elemento de Red. -OA33
  - Notificación de Inicio de Comprobación de un Elemento de Red. -NA14
  - Informe de Comprobación de un Elemento de Red. -NA15
- **Conjunto de funciones de informe de resultados y situaciones:**
  - Petición de resultados de prueba. –O29
  - Comunicación de resultados de prueba. –N10

3.1.6 Administración de anomalías

- **Conjunto de funciones de señalamiento de anomalías:**

  - Denuncia de la anomalía. –O30
  - Adición de información relativa a la anomalía. –O31
  - Cancelación de anomalías. –O32
- **Conjunto de funciones de notificación de cambio de la situación del informe de anomalías:**
  - Informe de cambio de situación de la anomalía. –N11
- **Conjunto de gestiones de indagación de información sobre anomalías:**
  - Comprobación de la situación de la anomalía. –O33
  - Examen del historial de anomalías. –O34
- **Conjunto de funciones de administración de fichas de anomalías:**
  - Búsqueda de informe de anomalía o tique de anomalía. –OA34
  - Informe de seguimiento de corrección de averías. –NA16
  - Notificación de desaparición de informe o tique de anomalía. –NA17
  -

3.1.7 Grupos de funciones

Para la definición de las funciones que se emplean en el sistema de operaciones y demás entidades del OSS, los anteriores conjuntos de funciones de gestión de TMN se dividen en los siguientes grupos:

Grupo1: N9, NA14, NA15, NA6
Grupo2: O26, O27, O28, OA33
Grupo3: O23
Grupo4: N7, NA3, NA7
Grupo5: O12, O14, OA11, OA14, OA15, OA16, OA17, OA18, OA19, OA20, OA29
Grupo6: OA13
Grupo7: N1, N7, N9, NA14, NA15, NA7
Grupo8: N10, N2, N3, N5, N6, NA1, NA11, NA2, NA3, NA5, NA8, NA9
Grupo9: N10, N2, N3, N5, N6, N8, NA1, NA11, NA12, NA13, NA2, NA3, NA4, NA5, NA8, NA9
Grupo10: O24, OA3, OA4, OA9
Grupo11: O1, O10, O11, O13, O2, O21, O22, O25, O29, O3, O4, O5, O6, O7, O8, O9, OA10, OA12, OA21, OA22, OA30, OA31, OA32, OA5, OA6, OA7, OA8
Grupo12: O1, O11, O21, O22, O29, O3, O7, OA10, OA21, OA22, OA30, OA5, OA8
Grupo13: O30, O31, O32, OA28
Grupo14: OA1, OA2
Grupo15: O33, O34, OA34
Grupo16: N11, NA16, NA17
Grupo17: N11, NA10, NA16, NA17
Grupo18: N11, NA10, NA16, NA17
Grupo19: OA26

Grupo20: O33, O34, OA23, OA24, OA25, OA34
Grupo21: O33, O34, OA27, OA28, OA34

Los mensajes que circulan entre los puntos/interfaces de referencia entre los bloques de función de gestión están agrupados de la siguiente forma:

Grupo I: N9, NA14, NA15, NA6, O23.
Grupo II: N1, N7, N9, NA14, NA15, NA7.
Grupo III: O1, O10, O11, O13, O2, O21, O22, O25, O29, O3, O4, O5, O6, O7, O8, O9, OA10, OA12, OA21, OA22, OA30, OA31, OA32, OA5, OA6, OA7, OA8.
Grupo IV: N10, N2, N3, N5, N6, N8, NA1, NA11, NA12, NA13, NA2, NA3, NA4, NA5, NA8, NA9, O1, O10, O11, O13, O2, O21, O22, O25, O29, O3, O4, O5, O6, O7, O8, O9, OA10, OA12, OA21, OA22, OA30, OA31, OA32, OA5, OA6, OA7, OA8.
Grupo V: N10, N2, N3, N5, N6, NA1, NA11, NA2, NA3, NA5, NA8, NA9, O1, O11, O21, O22, O29, O3, O7, OA10, OA21, OA22, OA30, OA5, OA8.
Grupo VI: O33, O34, OA34.
Grupo VII: O1, O11, O21, O22, O29, O3, O7, OA10, OA21, OA22, OA30, OA5, OA8.
Grupo VIII: O30, O31, O32, OA28, N11, NA16, NA17.
Grupo IX: N11, NA10, NA16, NA17, O33, O34, OA23, OA24, OA25, OA34.
Grupo X: N11, NA10, NA16, NA17.
Grupo XI: O33, O34, OA27, OA28, OA34.

3.2 ARQUITECTURA FUNCIONAL

Para poder tratar la complejidad del sistema de Soporte de operaciones para la red de 3G, la funcionalidad de gestión puede considerarse dividida en capas lógicas, estas capas lógicas han sido obtenidas de acuerdo a TMN y las divisiones de nivel 0 del eTOM.

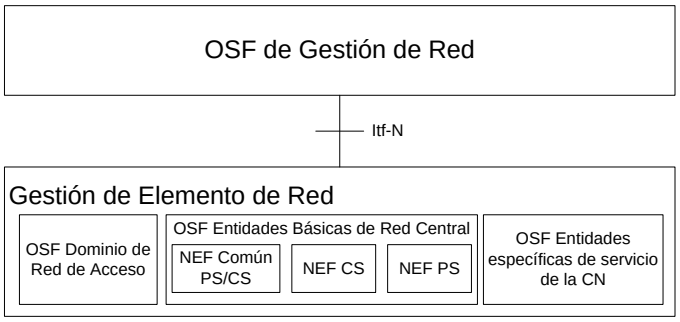
Tabla 1. Capas lógicas de la arquitectura funcional

Capas lógicas eTOM	Capas lógicas TMN
Mercado, producto y cliente Proveedor/Asociado	Capa de gestión empresarial
Servicio	Capa de gestión de servicio
Recursos (Aplicaciones, informática y red)	Capa de gestión de red Capa de gestión de elemento Capa de elemento de red

3.2.1 Recursos (Aplicación, Informática y Red)

3.2.1.1 Arquitectura Funcional de Capa de Elementos de Red y Gestión de Elementos de Red. Como se vio anteriormente los recursos gestionados son aquellas entidades de la red móvil de 3G que componen el dominio de infraestructura. Esos recursos gestionados cumplen con las Funciones de Elemento de Red (NEF, Network Element Function) y se dividen como se muestra en la Figura 6.

Figura 6. Nivel de gestión de elementos de red y red.



Para lograr la gestión de fallas en las capas de gestión de elemento red y de gestión de elemento se propone la arquitectura que se muestra en la Figura 7.

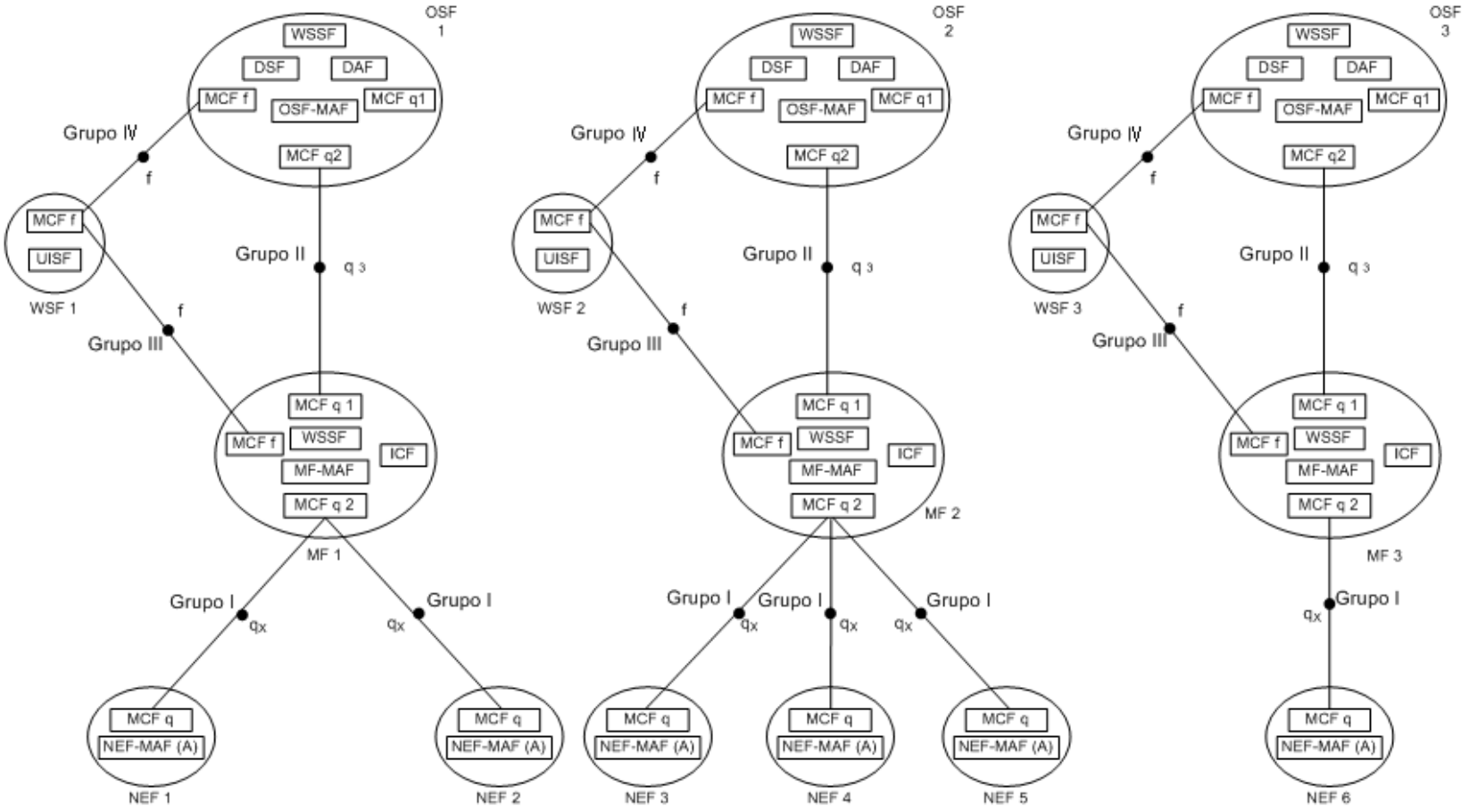
Gestión de fallas en la red de acceso. La gestión de fallas de la red de acceso esta conformada por los siguientes bloques funcionales:

NEF 1: este bloque funcional lleva a cabo funciones de telecomunicaciones involucradas con la Red de acceso radio terrestre UMTS (UTRAN, UMTS Terrestrial Radio Access Network), y las funciones relacionadas con el envió de eventos para su pertinente gestión. Se conforma de las siguientes funciones:

- **NEF–MAF (A**): como soporte al cometido de agente del NEF este bloque esta conformado por operaciones realizadas en elementos (RNS, Nodo B y RNC) de la UTRAN, que generan eventos para su respectiva gestión. Se utilizan las funciones del ***Grupo 1*****.**
- **MCF q:** esta función de comunicación de mensajes es la encargada de hacer las notificaciones y envío de los eventos que ocurren en este segmento de la red hacia el OSF gestor. Las funciones utilizadas en este bloque son las que corresponden al ***Grupo 2.***

NEF 2: este bloque funcional lleva a cabo funciones de telecomunicaciones involucradas con Red de Acceso Radio Terrestre GSM/EDGE (GERAN, GSM/EDGE Radio Access Network), y las funciones relacionadas con el envió de eventos para su pertinente gestión. Se conforma de las siguientes funciones:

Figura 7. Arquitectura Funcional Capa de Elementos de Red y Gestión de Elementos de Red



- **NEF–MAF (A):** como soporte al cometido de Agente del NEF este bloque esta conformado por operaciones realizadas en elementos (BSS conformado por la BSC y la BTS) de GERAN, que generan eventos para su respectiva gestión. Se utilizan las funciones del ***Grupo 1*****.**
- **MCF q:** esta función de comunicación de mensajes es la encargada de hacer las notificaciones y envío de los eventos que ocurren en este segmento de la red hacia el OSF gestor. Las funciones utilizadas en este bloque son las que corresponden al ***Grupo 2.***

MF 1: este bloque actúa sobre la información que pasa entre el OSF1, NEF1 y NEF2 con el fin de, adaptar, filtrar, y condensar información. Está conformado por:

- **MCF q1:** esta función de comunicación de mensajes es la encargada de hacer las notificaciones hacia el gestor d elementos de red, definidas en el ***Grupo 7.***
- **MF–MAF:** como soporte de los cometidos de agente y de gestor de la función de mediación en este bloque se encuentran las funciones de aplicación incluidas en el: ***Grupo 5.***
- **ICF:** para el cumplimiento del objetivo de la función de conversión de información (ICF, Information Conversion Function) que afecta la transformación y adaptación de los mensajes por medio de la traducción a nivel sintáctico y/o semántico para su ulterior gestión se utilizan las funciones del ***Grupo 6.***
- **WSSF:** función que proporciona soporte al bloque de función de estación de trabajo (WSF), incluido el acceso y la manipulación de datos, la invocación y confirmación de acciones.
- **MCF f:** esta función de comunicación de mensajes se encarga de recibir las peticiones hechas por el usuario de la WSF y enviar notificaciones hacia él. Usa las funciones del ***Grupo 4.***
- **MCF q2:** esta función de comunicación de mensajes es la encargada recibir las notificaciones enviadas desde el agente para su respectivo filtraje, y adaptación (eventos) y conducir las peticiones mapeadas del OSF gestor por medio de las funciones del: ***Grupo 3.***

OSF 1:

- **MCF q1:** esta función de comunicación de mensajes es la encargada de hacer las notificaciones hacia el gestor de red, al igual que recibir las peticiones provenientes de este. Los mensajes que se intercambian en este bloque están representados en el: ***Grupo 8.***
- **OSF–MAF:** como soporte de los cometidos de gestor y de agente este bloque utiliza el grupo de funciones: ***Grupo 10.***
- **DAF:** la función de acceso al directorio está asociado con los bloques OSF y WSF que necesitan tener acceso al directorio. Se utiliza para acceder a, (leer, enumerar, buscar, añadir, modificar, suprimir), y/o mantener información relativa a la TMN representada en la DSF.
- **DSF:** la función de sistema de directorio contiene en su interior las bases de datos referentes a
    - Historial de Alarmas
    - Inventario
    - Pruebas
- **WSSF:** como soporte al bloque de trabajo WSF (función de estación de trabajo) esta sección

del OSF permite el acceso y la manipulación de datos.

- **MCF f:** esta función de comunicación de mensajes es la encargada de recibir las peticiones y enviar las notificaciones e informes al usuario de la WSF: ***Grupo 9.***
- **MCF q2**: esta función de comunicación de mensajes es la encargada recibir las notificaciones enviadas desde el agente para su respectiva gestión y de enviar las peticiones requeridas por el gestor. Las funciones que representan esta interacción de mensajes son las correspondientes al ***Grupo 3.***

WSF 1:

- **UISF:** esta función traduce la información proveniente del OSF, recibida por el MCFf, a un formato visualizable para la interfaz persona–máquina, y traduce lo introducido por el usuario al modelo de información de la red de gestión TMN.
- **MCF f:** esta función de comunicación de mensajes es la encargada de hacer las peticiones del usuario de la WSF y recibir las notificaciones e informes. Utiliza las funciones del: ***Grupo 11.***

Gestión de fallas en las Entidades Básicas de la Red Central.La gestión de fallas de las entidades básicas de la red central se conforma de los siguientes bloques funcionales:

NEF 3: este bloque funcional lleva a cabo funciones de telecomunicaciones involucradas con el dominio de conmutación de paquetes (PS), y las funciones relacionadas con el envió de eventos para su pertinente gestión.

- **NEF–MAF (A):** como soporte al cometido de Agente del NEF este bloque esta conformado por operaciones que generan eventos para su respectiva gestión, en elementos que conforman la el dominio PS (SGSN, GGSN y BG). Se utilizan las funciones del ***Grupo 1.***
- **MCF q:** esta función de comunicación de mensajes es la encargada de hacer las notificaciones y envio de los eventos que ocurren en este segmento de la red hacia el OSF gestor. Las funciones utilizadas en este bloque son las que corresponden al ***Grupo 2.***

NEF 4: este bloque funcional lleva a cabo funciones de telecomunicaciones involucradas con el dominio de conmutación de circuitos (CS), y las funciones relacionadas con el envió de eventos para su pertinente gestión.

- **NEF–MAF (A):** como soporte al cometido de Agente del NEF este bloque esta conformado por operaciones que generan eventos para su respectiva gestión, en elementos que conforman la el dominio CS (MSC, GMSC y IWF). Se utilizan las funciones del ***Grupo 1.***
- **MCF q:** esta función de comunicación de mensajes es la encargada de hacer las notificaciones y envio de los eventos que ocurren en este segmento de la red hacia el OSF gestor. Las funciones utilizadas en este bloque son las que corresponden al ***Grupo 2.***

NEF 5: este bloque funcional lleva a cabo funciones de telecomunicaciones involucradas con la

entidades comunes PS/CS, y las funciones relacionadas con el envió de eventos para su pertinente gestión.

- **NEF–MAF (A):** como soporte al cometido de Agente del NEF este bloque esta conformado por operaciones que generan eventos para su respectiva gestión, en elementos que conforman las entidades comunes PS/CS. Se utilizan las funciones del ***Grupo 1.***
- **MCF q:** esta función de comunicación de mensajes es la encargada de hacer las notificaciones y envio de los eventos que ocurren en este segmento de la red hacia el OSF gestor. Las funciones utilizadas en este bloque son las que corresponden al ***Grupo 2.***

MF 2: este bloque actúa sobre la información que pasa entre el OSF2, NEF3, NEF4 y NEF 5 con el fin de, adaptar, filtrar, y condensar información.

- **MCF q1:** esta función de comunicación de mensajes es la encargada de hacer las notificaciones hacia el OSF gestor de elementos de red definidas en el ***Grupo 7.***
- **MF–MAF:** como soporte de los cometidos de agente y de gestor de la función de mediación en este bloque se encuentran las funciones de aplicación incluidas en el: ***Grupo 5.***
- **ICF:** para el cumplimiento del objetivo de la función de conversión de información (ICF, Information Conversion Function) que afecta la transformación y adaptación de los mensajes por medio de la traducción a nivel sintáctico y/o semántico para su ulterior gestión, se utilizan las funciones del ***Grupo 6.***
- **WSSF:** función que proporciona soporte al bloque de función de estación de trabajo (WSF), incluido el acceso y la manipulación de datos, la invocación y confirmación de acciones.
- **MCF f:** esta función de comunicación de mensajes es la encargada de recibir las peticiones hechas por el usuario de la WSF y enviar notificaciones hacia este. Usa la funciones del ***Grupo 4.***
- **MCF q2:** esta función de comunicación de mensajes es la encargada recibir las notificaciones enviadas desde el agente para su respectivo filtraje, y adaptación (eventos) y conducir las peticiones mapeadas del OSF gestor por medio de las funciones del: ***Grupo 3.***

OSF 2:

- **MCF q1:** esta función de comunicación de mensajes es la encargada de hacer las notificaciones hacia el gestor, al igual que recibir las peticiones provenientes de este. Los mensajes que se intercambian en este bloque están representados en el: ***Grupo 8.***
- **OSF–MAF:** como soporte de los cometidos de gestor y de agente este bloque utiliza el grupo de funciones ***Grupo 10.***
- **DAF:** la función de acceso al directorio está asociado con los bloques OSF y WSF que necesitan tener acceso al directorio. Se utiliza para acceder a, (leer, enumerar, buscar, añadir, modificar, suprimir), y/o mantener información relativa a la TMN representada en la DSF.
- **DSF:** la función de sistema de directorio contiene en su interior las bases de datos referentes

a**:**

- Historial de Alarmas
- Inventario
- Pruebas

- **WSSF:** como soporte al bloque de trabajo WSF (función de estación de trabajo) esta sección del OSF permite el acceso y la manipulación de datos.
- **MCF f:** esta función de comunicación de mensajes es la encargada de recibir las peticiones y enviar las notificaciones e informes al usuario de la WSF: ***Grupo 9.***
- **MCF q2**: esta función de comunicación de mensajes es la encargada recibir las notificaciones enviadas desde el agente para su respectiva gestión y de enviar las peticiones requeridas por el gestor. Las funciones que representan esta interacción de mensajes son las correspondientes al ***Grupo 3.***

WSF 2:

- **UISF:** esta función traduce la información Proveniente del OSF, recibida por el MCFf, a un formato visualizable para la interfaz persona–máquina, y traduce lo introducido por el usuario al modelo de información de la red de gestión TMN.
- **MCF f:** esta función de comunicación de mensajes es la encargada de hacer las peticiones del usuario de la WSF y recibir las notificaciones e informes. Utiliza las funciones del: ***Grupo 11.***

Gestión de fallas en las Entidades Específicas de Servicios de la Red Central. La gestión de fallas de las entidades específicas de servicio de la red central se conforma de los siguientes bloques funcionales:

NEF 6: este bloque funcional lleva a cabo funciones de telecomunicaciones involucradas con las entidades específicas de servicio de la red central, y las funciones relacionadas con el envió de eventos para su pertinente gestión

- **NEF–MAF (A):** Como soporte al cometido de Agente del NEF este bloque esta conformado por operaciones que generan eventos para su respectiva gestión, en elementos que conforman las entidades específicas de servicio de la red central. Se utilizan las funciones del: ***Grupo 1.***
- **MCF q:** esta función de comunicación de mensajes es la encargada de hacer las notificaciones y envio de los eventos que ocurren en este segmento de la red hacia el OSF gestor. Las funciones utilizadas en este bloque son las que corresponden al ***Grupo 2.***

MF 3: Este bloque actúa sobre la información que pasa entre el OSF3 y NEF 6 con el fin de, adaptar, filtrar, y condensar información.

- **MCF q1: e**sta función de comunicación de mensajes es la encargada de hacer las notificaciones hacia el gestor definidas en el ***Grupo 7.***

- **MF–MAF:** como soporte de los cometidos de agente y de gestor de la función de mediación en este bloque se encuentran las funciones de aplicación incluidas en el: ***Grupo 5.***
- **ICF:** para el cumplimiento del objetivo de la función de conversión de información (ICF, Information Conversion Function) que afecta la transformación y adaptación de los mensajes por medio de la traducción a nivel sintáctico y/o semántico para su ulterior gestión se utilizan las funciones del ***Grupo 6.***
- **WSSF:** función que proporciona soporte al bloque de función de estación de trabajo (WSF), incluido el acceso y la manipulación de datos, la invocación y confirmación de acciones.
- **MCF f: e**sta función de comunicación de mensajes es la encargada de recibir las peticiones hechas por el usuario de la WSF. Usa la funciones del ***Grupo 4.***
- **MCF q2:** esta función de comunicación de mensajes es la encargada recibir las notificaciones enviadas desde el agente para su respectivo filtraje, y adaptación (eventos) y conducir las peticiones mapeadas del OSF gestor por medio de las funciones del: ***Grupo 3.***

OSF 3:

- **MCF q1:** Esta función de comunicación de mensajes es la encargada de hacer las notificaciones hacia el gestor, al igual que recibir las peticiones provenientes de este. Los mensajes que se intercambian en este bloque están representados en el: ***Grupo 8.***
- **OSF–MAF:** Como soporte de los cometidos de gestor y de agente este bloque utiliza el grupo de funciones: ***Grupo 10.***
- **DAF:** la función de acceso al directorio está asociado con los bloques OSF y WSF que necesitan tener acceso al directorio. Se utiliza para acceder a, (leer, enumerar, buscar, añadir, modificar, suprimir), y/o mantener información relativa a la TMN representada en la DSF.
- **DSF:** La función de sistema de directorio contiene en su interior las bases de datos referentes a
    - Historial de Alarmas
    - Inventario
    - Pruebas
- **WSSF:** como soporte al bloque de trabajo WSF (función de estación de trabajo) esta sección del OSF permite el acceso y la manipulación de datos.
- **MCF f:** Esta función de comunicación de mensajes es la encargada de recibir las peticiones y enviar las notificaciones e informes al usuario de la WSF: ***Grupo 9.***
- **MCF q2**: esta función de comunicación de mensajes es la encargada recibir las notificaciones enviadas desde el agente para su respectiva gestión y de enviar las peticiones requeridas por el gestor. Las funciones que representan esta interacción de mensajes son las correspondientes al ***Grupo 3.***

WSF 3:

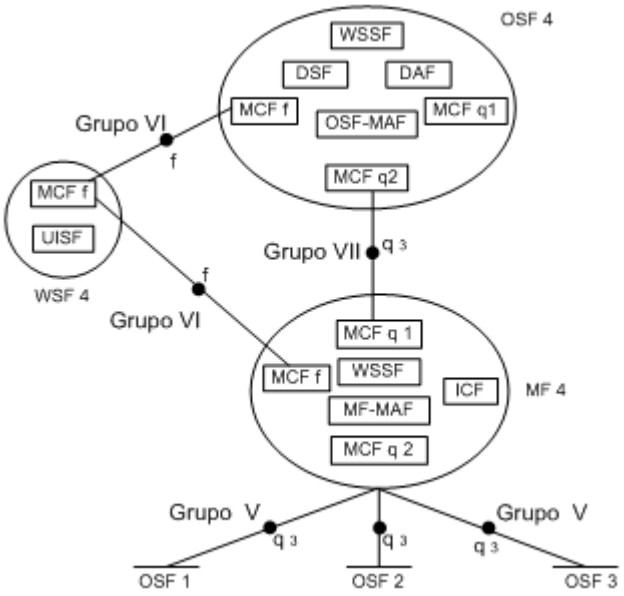
- **UISF:** Esta función traduce la información Proveniente del OSF, recibida por el MCFf, a un

formato visualizable para la interfaz persona–máquina, y traduce lo introducido por el usuario al modelo de información de la red de gestión TMN.

- **MCF f:** Esta función de comunicación de mensajes es la encargada de hacer las peticiones del usuario de la WSF y recibir las notificaciones e informes. Utiliza las funciones del: ***Grupo 11.***

3.2.1.2 Arquitectura Funcional de la Capa de Gestión de Red. Para obtener una gestión completa de la red es necesario unir los OSF que gestionan la red Central (OSF1, OSF2 y OSF3) al OSF que maneja las fallas de la red en conjunto, y soporta el OSF de nivel superior (OSF 5), encargado de gestionar los informes de dificultades generados por interrupciones de la red y del servicio. Para lograr esta unión se utiliza Función de mediación (MF) que representa a la Interfaz N, concepto del que ya se había expuesto anteriormente.El OSS para gestión de fallas en esta capa esta compuesto se muestra en la Figura 8.

Figura 8. Arquitectura Funcional de la Capa de Gestión de Red



MF 4: este bloque de mediación representa la interfaz N y se encarga de recibir notificaciones y hacer peticiones de alarmas, inventario y pruebas, con el fin de comunicar la capa de gestión de elemento de red (OSF 1, OSF2 y OSF3) con la capa de gestión de red (OSF 4). Está constituido por los siguientes bloques.

- **MCF q1:** esta función de comunicación de mensajes es la encargada de hacer las notificaciones de alarmas, inventario y pruebas hacia el gestor ubicado en la capa de red (OSF4).
- **MF–MAF:** como soporte de los cometidos de agente y de gestor de la función de mediación en

este bloque se encarga de adaptar la información proveniente del Gestor IRP o AgenteIRP con el fin de dar a la red la capacidad de trabajar con multi-proveedores en la capa de gestión de red y Elemento de red.

- **ICF:** realiza la traducción a nivel sintáctico y/o semántico de los mensajes de alarmas, inventario y pruebas para su ulterior gestión.
- **WSSF:** función que proporciona soporte al bloque de función de estación de trabajo (WSF), incluido el acceso y la manipulación de datos, la invocación y confirmación de acciones.
- **MCF f:** esta función de comunicación de mensajes es la encargada de recibir las peticiones de alarmas, inventario y pruebas, hechas por el usuario de la WSF.
- **MCF q2:** esta función de comunicación de mensajes es la encargada recibir las notificaciones de alarmas, inventario y pruebas enviadas desde los agentes para su respectivo filtraje, y adaptación. Usa la funciones del ***Grupo 12.***

OSF 4:

- **MCF q1:** esta función de comunicación de mensajes es la encargada de recibir las peticiones y hacer las notificaciones hacia la capa de Gestión de servicios definidas en el ***Grupo 13*****.**
- **OSF–MAF:** como soporte de los cometidos de gestor y de agente este bloque utiliza el grupo de funciones: ***Grupo 14.***
- **DAF:** la función de acceso al directorio está asociado con los bloques OSF y WSF que necesitan tener acceso al directorio. Se utiliza para acceder a, (leer, enumerar, buscar, añadir, modificar, suprimir), y/o mantener información relativa a la TMN representada en la DSF.
- **DSF:** la función de sistema de directorio contiene en su interior las bases de datos referentes a**:**
    - Informe de dificultades
- **WSSF:** como soporte al bloque de trabajo WSF (función de estación de trabajo) esta sección del MF suministra al cliente interno que opera en la estación de trabajo un puente o camino hacia la función de acceso al directorio y otras funciones.
- **MCF f:** esta función de comunicación de mensajes es la encargada de recibir las peticiones y enviar al usuario de la WSF las notificaciones e informes resultantes de la gestión de la red.
- **MCF q2:** esta función de comunicación de mensajes es la encargada recibir las notificaciones enviadas desde la función de mediación (MF4) y enviar las peticiones y notificaciones referentes a alarmas, inventario y pruebas definidas en el ***Grupo 12.***

WSF 4:

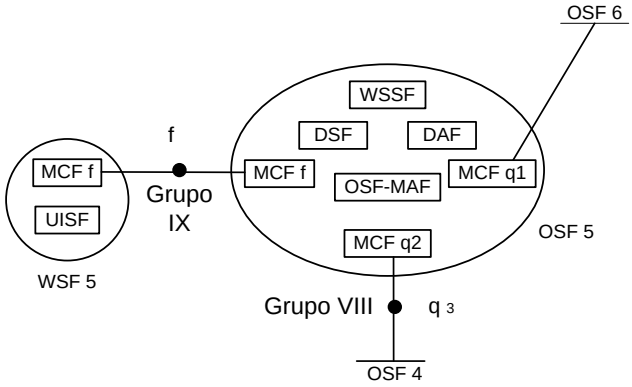
- **UISF:** Esta función traduce la información Proveniente del OSF, recibida por el MCFf, a un formato visualizable para la interfaz persona–máquina, y traduce lo introducido por el usuario al modelo de información de la red de gestión TMN.
- **MCF f:** Esta función de comunicación de mensajes es la encargada de recibir las notificaciones e informes y hacer las peticiones del usuario de la WSF referentes a la capa de red. Utiliza las

funciones del: ***Grupo 15.***

3.2.1.3 Servicios: Arquitectura Funcional de la Capa de Gestión de Servicios. En esta capa del Sistema de Soporte de Operaciones se realiza la gestión de dificultades que se presentan en la red y traen como consecuencia la degradación del servicio que se presta, adicionalmente en esta capa también se gestiona las reparaciones necesarias para la solución de la dificultad presentada..

El OSF5 que compone esta capa sirve de soporte a la capa de Gestión empresarial (OSF6) y algunas de sus funcionalidades están basadas en la información enviada desde la capa de Red (OSF4).

Figura 9. Arquitectura Funcional de la Capa de Gestión de Servicios



OSF 5:

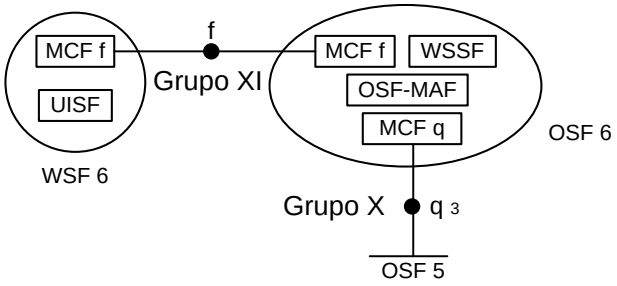
- **MCF q1:** esta función de comunicación de mensajes es la encargada de recibir las peticiones realizadas desde el nivel superior y también hacer las notificaciones pertinentes a esas peticiones por medio de las funciones del: ***Grupo 17.***
- **OSF–MAF:** como soporte de los cometidos de gestor y de agente este bloque utiliza las funciones del: ***Grupo 19.***
- **DAF:** la función de acceso al directorio está asociado con los bloques OSF y WSF que necesitan tener acceso al directorio. Se utiliza para acceder a, (leer, enumerar, buscar, añadir, modificar, suprimir), y/o mantener información relativa a la TMN representada en la DSF.
- **DSF:** la función de sistema de directorio contiene en su interior las bases de datos referentes a
    - Historial de dificultades
- **WSSF:** función que proporciona soporte al bloque de función de estación de trabajo (WSF), incluido el acceso y la manipulación de datos, la invocación y confirmación de acciones.
- **MCF f:** esta función de comunicación de mensajes es la encargada de recibir las peticiones y enviar las notificaciones e informes al usuario de la WSF representados en el*:* ***Grupo 18.***
- **MCF q2:** esta función de comunicación de mensajes es la encargada recibir las notificaciones enviadas desde el agente para su respectiva gestión. Esos mensajes son los encontrados en el: ***Grupo 16.***

WSF 5:

- **UISF**: esta función traduce la información proveniente del OSF, recibida por el MCFf, a un formato visualizable para la interfaz persona–máquina, y traduce lo introducido por el usuario al modelo de información de la red de gestión TMN.
- **MCF f:** esta función de comunicación de mensajes es la encargada de recibir las notificaciones e informes y hacer las peticiones del usuario de la WSF. Utiliza las funciones del: ***Grupo 20.***

3.2.1.4 Mercado, Producto y Cliente/Proveedor/Asociado: Arquitectura Funcional de la Capa Empresarial

Figura 10. Arquitectura Funcional de la Capa Empresarial



OSF 6:

- **MCF q**: esta función de comunicación de mensajes es la encargada recibir las notificaciones enviadas desde el agente para realizar la gestión correspondiente en este nivel, y de enviar las peticiones necesarias para obtener información de gestión.
- **MCF f:** esta función de comunicación de mensajes es la encargada de recibir las peticiones del usuario de la WSF en la capa empresarial.
- **OSF–MAF:** como soporte de los cometidos de gestor y de agente este bloque se encarga de procesar la información proveniente de los clientes.
- **WSSF:** función que proporciona soporte al bloque de función de estación de trabajo (WSF), incluido el acceso y la manipulación de datos, la invocación y confirmación de acciones.

WSF 6:

- **UISF:** esta función traduce la información proveniente del OSF, recibida por el MCFf, a un formato visualizable para la interfaz persona–máquina, y traduce lo introducido por el usuario al modelo de información de la red de gestión TMN.
- **MCF f:** esta función de comunicación de mensajes es la encargada de hacer las peticiones del usuario de la WSF y recibir las notificaciones e informes. Utiliza las funciones del: ***Grupo 21.***

3.3 ARQUITECTURA FÍSICA

Para el desarrollo de la arquitectura física del sistema de Soporte de operaciones para la red de 3G se parte de la arquitectura funcional obtenida y se seguirán los lineamientos de la recomendación del 3GPP TS 32.102. [32]

Se debe tener en cuenta que en la transmisión de mensajes entre los diferentes bloque del sistema de gestión es necesario emplear una Red de Comunicación de Datos (RCD), la cual debe ser independiente tecnológicamente y dado el tamaño y distribución de las redes de 3G puede emplear combinaciones de tecnologías de transmisión (ISDN, ATM, SDH,…) y estar constituida de un número de subredes individuales interconectadas entre si (punto a punto, estrella, bus, anillo), que permitan el transporte de tráfico IP.

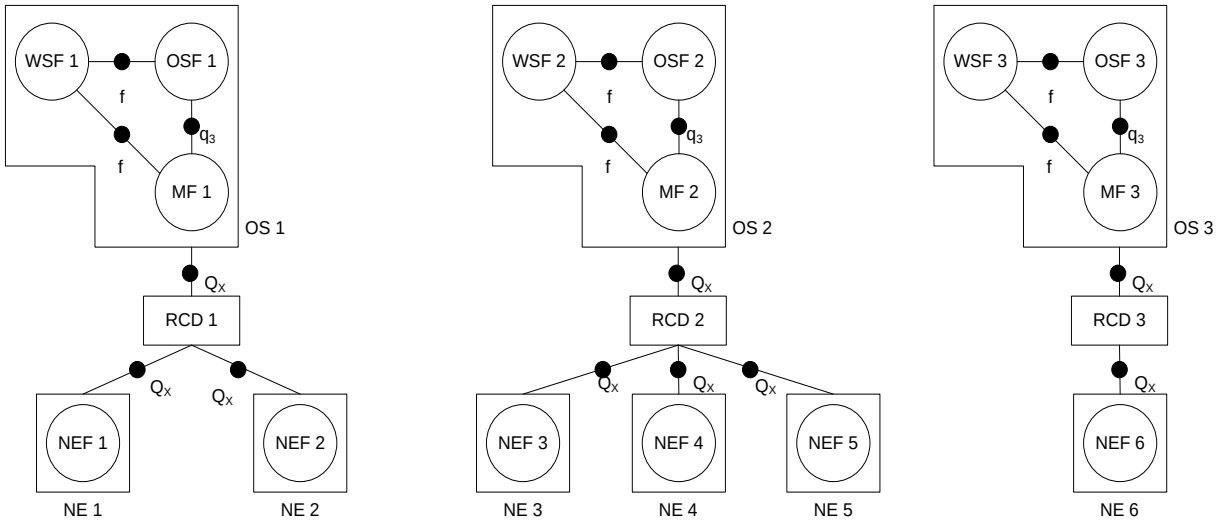
3.3.1 Arquitectura Física de Gestión de Elemento de Red

En la arquitectura planteada los Sistemas de operaciones (OS) de las capas superiores (Red, Servicio, Empresarial) acceden a los Elementos de Red por medio del OS de gestión de elemento de red.

Para que los Elementos de Red (NE) sean compatibles a las interfaces del OSS se deben cumplir las siguientes condiciones:

- Los NEs deben implementar el grupo de soluciones IRP de gestión CMIP/GDMO.
- El protocolo de la capa de red para la gestión debe ser IP.

Figura 11. *Arquitectura Física de la Capa* de Elementos de Red y Gestión de Elementos de Red



Gestión de fallas en la red de acceso:

NE 1: Este elemento representa los equipos de telecomunicaciones (grupos/partes de equipos de telecomunicación) involucrados en la Red de Acceso Radio Terrestre UMTS (UTRAN), que ejecutan las funciones del bloque funcional NEF 1.

NE 2: Este elemento representa los equipos de telecomunicaciones (grupos/partes de equipos de telecomunicación) involucrados en la Red de Acceso Radio Terrestre GSM/EDGE (GERAN), que ejecutan las funciones del bloque funcional NEF 1.

OS 1: En este sistema se ejecutan las funcionalidades de sistema de operaciones del bloque funcional OSF 1 y se integran las funcionalidades de los bloques de función de estación de trabajo WSF 1 y de función de medicación 1 (no se encuentran distribuidos). Los puntos de referencia f y q_3 son internos a este sistema.

RCD 1: Esta red comunicación permite el transporte de datos entre los elementos de red de la red de acceso (NE 1 y NE 2) y el sistema de operaciones OS 1.

Gestión de fallas en la Red Central

NE 3: Este elemento representa los equipos de telecomunicaciones (grupos/partes de equipos de telecomunicación) involucrados en las entidades del dominio de conmutación de paquetes, que ejecutan las funciones del bloque funcional NEF 3.

NE 4: Este elemento representa los equipos de telecomunicaciones (grupos/partes de equipos de telecomunicación) involucrados en las entidades del dominio de conmutación de circuitos, que ejecutan las funciones del bloque funcional NEF 4.

NE 5: Este elemento representa los equipos de telecomunicaciones (grupos/partes de equipos de telecomunicación) involucrados en las entidades comunes a los dominios de conmutación de paquetes y circuitos, que ejecutan las funciones del bloque funcional NEF 5.

OS 2: En este sistema se ejecutan las funcionalidades de sistema de operaciones del bloque funcional OSF 2 y se integran las funcionalidades de los bloques de función de estación de trabajo WSF 2 y de función de medicación 2 (no se encuentran distribuidos). Los puntos de referencia f y q_3 son internos a este sistema.

RCD 2: Esta red comunicación permite el transporte de datos entre los elementos de las redes NE 2, NE 4 y NE 5 y el sistema de operaciones OS 2.

Gestión de fallas en Entidades Específicas de Servicios de la Red Central

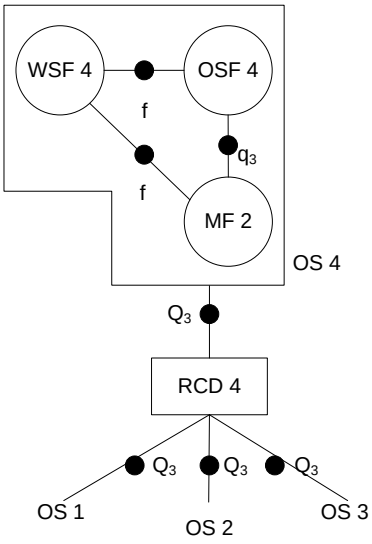
NE 6: Este elemento representa los equipos de telecomunicaciones (grupos/partes de equipos de telecomunicación) involucrados en las entidades específicas de servicios de la Red Central, que ejecutan las funciones del bloque funcional NEF 6.

OS 3: En este sistema se ejecutan las funcionalidades de sistema de operaciones del bloque funcional OSF 3 y se integran las funcionalidades de los bloques de función de estación de trabajo WSF 3 y de función de medicación 3 (no se encuentran distribuidos). Los puntos de referencia f y q_3 son internos a este sistema.

RCD 3: Esta red comunicación permite el transporte de datos entre entidades específicas de servicios de la Red Central (NE 6) y el dispositivo de mediación MD 2.

3.3.2 Arquitectura Física de la Capa de Gestión de Red:

Figura 12. ***Arquitectura Física de la*** **Capa de Gestión de Red**

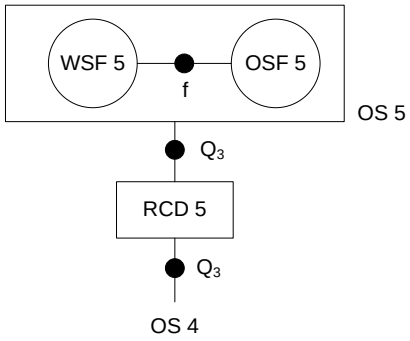


OS 4: En este sistema se ejecutan las funcionalidades de sistema de operaciones del bloque funcional OSF 4 y se integran las funcionalidades del bloque de función de estación de trabajo WSF 4 (no se encuentra distribuido). El punto de referencia f es interno a este sistema.

RCD 4: Esta red comunicación permite el transporte de datos entre los sistemas de operaciones OS 1, OS 2 y OS 3 y el sistema de operaciones OS 4

3.3.3 Arquitectura Física de la Capa de Gestión de Servicios

Figura 13. ***Arquitectura Física de la*** **Capa de Gestión de Servicios**

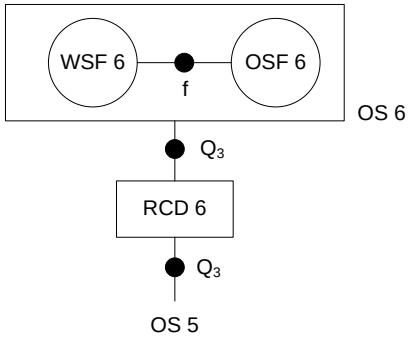


OS 5: En este sistema se ejecutan las funcionalidades de sistema de operaciones del bloque funcional OSF 5 y se integran las funcionalidades del bloque de función de estación de trabajo WSF 5 (no se encuentra distribuido). El punto de referencia f es interno a este sistema.

RCD 5: Esta red comunicación permite el transporte de datos entre el sistema de operaciones OS 4 y el sistema de operaciones OS 5

3.3.4 Arquitectura Funcional de la Capa Empresarial

Figura 14. ***Arquitectura Física de la*** **Capa Empresarial**



OS 6: En este sistema se ejecutan las funcionalidades de sistema de operaciones del bloque funcional OSF 6 y se integran las funcionalidades del bloque de función de estación de trabajo WSF 6 (no se encuentra distribuido). El punto de referencia f es interno a este sistema.

RCD 6: Esta red comunicación permite el transporte de datos entre el sistema de operaciones OS 5 y el sistema de operaciones OS 6

4. ARQUITECTURA DE LA INFORMACIÓN

El diseño de la arquitectura de la información del OSS para gestión de fallas en redes móviles de 3G, esta basado en un planteamiento orientado al objeto, en la cual los diferentes bloques de función de soporte de operaciones (OSF) localizados en cada uno de los niveles de gestión TMN, intercambian información de gestión modelada en términos de objetos gestionados, donde se entiende por objeto gestionado “las visiones conceptuales de los recursos sometidos a gestión o de los recursos que podrían existir para soportar ciertas funciones de gestión” [9], y están definidos mediante atributos, comportamiento, operaciones, aplicables a él y notificaciones emitidas por él.

La gestión de fallas en una red de telecomunicaciones móviles de 3G al igual que cualquier tipo de gestión involucra procesamiento de información, pero en este tipo de red es evidente que ese procesamiento de información se hace de forma distribuida debido al tamaño y cantidad de componentes de red, tanto físicos como lógicos que la conforman.

Esta información de gestión se encuentra almacenada en diferentes bases de datos en la red de gestión. Esta colección de información es definida como directorio y a la información contenida en él se le denomina base de información del directorio (DIB, Directory Information Base) de acuerdo a la recomendación ITU-T X.500 [33] “Redes de datos y comunicación entre sistemas abiertos. Directorio”.

Los usuarios del directorio, pueden ser los clientes internos del sistema de soporte de operaciones o programas de computador, los cuales pueden leer o modificar la información contenida en el directorio. Estos usuarios de directorio están representados según la recomendación ITU-T X.500 [33] por un Agente de usuario de directorio (DUA, Directory User Agent) y funcionalmente por los WSSF, y los OSF-MAF (G, gestores) de cada nivel. El acceso al directorio por parte de estos usuarios es proporcionado por un agente de sistema de directorio (DSA, Directory System Agent) el cual atiende las peticiones hechas por estos y se encuentra representado funcionalmente por las DAFs descritas en la arquitectura funcional.

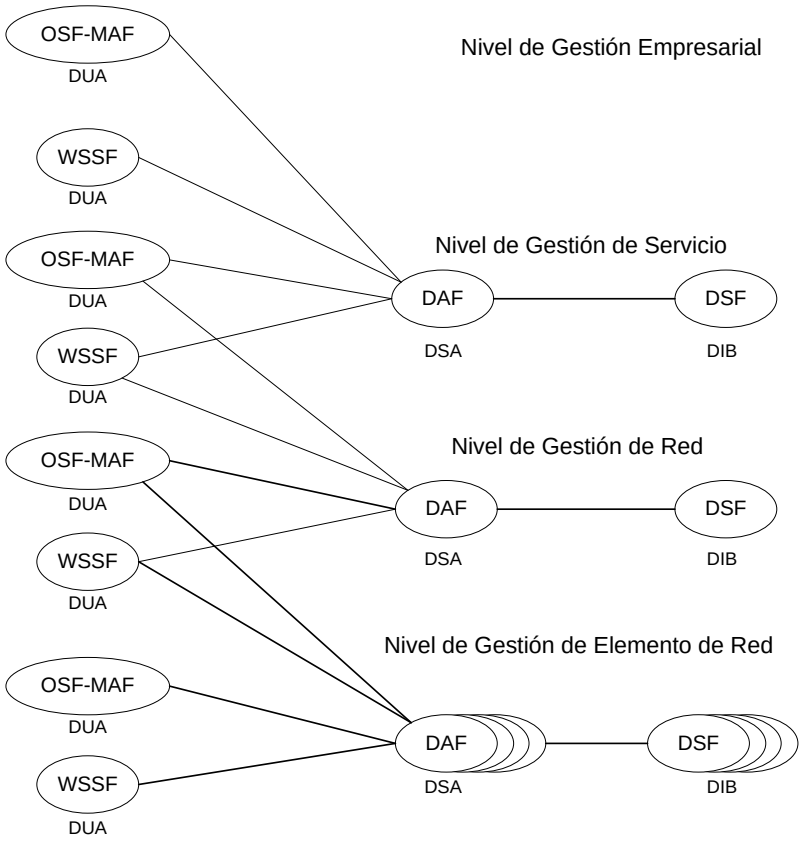
Como se vio anteriormente en la arquitectura funcional, el nivel de gestión de Elemento de red se encuentra distribuido de acuerdo a las subredes que conforman el dominio de infraestructura de la arquitectura de referencia para un red UMTS, por lo tanto la información que se procesa en este nivel se encuentra distribuida en un número de directorios (representados funcionalmente por las DSF) igual al número de bloques OSF que componen esta capa de gestión, cada uno con su respectiva DAF. Esos directorios podrán ser manipulados y accedidos tanto por usuarios del mismo nivel, como por usuarios del nivel superior (nivel de red) que requieren la información contenida en estos directorios (Ver figura 15).

En el nivel de gestión de Red solo se implementa un directorio que puede ser accedido desde usuarios del mismo nivel, o usuarios del nivel superior. De forma similar ocurre en el nivel de Servicio.

En la capa de gestión empresarial no se implementan directorios, los usuarios de esta capa acceden al directorio de nivel inferior (nivel de red).

La información contenida en cada directorio, es aquella que se almacena en los ficheros de registro cronológico manejados en el Sistema de Soporte de Operaciones los cuales se especificarán posteriormente.

Figura 15. Arquitectura del sistema de directorio distribuido



Continuando con la "Metodología de Especificación de Interfaz de la Red de Gestión de las Telecomunicaciones" a continuación se llevará a cabo las tareas 3 y 4 para hacer el modelado de la información y la consolidación de la información intercambiada en el OSS.

4.1 TAREA 3: MODELADO DE INFORMACIÓN

En la tarea 3 se identifican las clases de objeto existentes y nuevas, que sean necesarias para

soportar las funciones de gestión de los cometidos planteados en la tarea 2.

Para satisfacer los requerimientos de esta tarea se debe hacer un análisis del modelo de información de forma genérica, y posteriormente se debe determinar que clases de objetos existentes son aplicables al modelo recurriendo a relaciones de herencia.

Si las clases de objeto existentes no satisfacen las funciones de gestión especificadas, entonces se debe crear nuevas clases de objeto que cubran esas funcionalidades o cometidos.

En este modelo genérico de información de red se describe también las relaciones entre clases de objeto en forma de diagramas de relación entre entidades.

En la Figura 16 se puede observar el mapa de clases de objetos de información, que representa el modelo de información para el OSS para gestión de fallas.

Estas clases serán tratadas de acuerdo a la actividad que desarrollan dentro del Sistema de Soporte de Operaciones como se muestra a continuación:

- Entidad Monitoreada
- Discriminador de Envío de Eventos
- Registro Cronológico
- Inventario
- Punto de Referencia de Integración de Alarmas
- Punto de Referencia de Integración de Pruebas
- Trouble Ticket o Gestión de Dificultades

Se debe tener en cuenta que las clases de objetos de información que pertenecen a la capa de Gestión de Elemento de Red, se aplican a cada una de las subdivisiones que se realizaron en la arquitectura funcional. Es decir que tanto para la Red de Acceso como para el conjunto de Entidades Básicas de la Red Central y el conjunto de las Entidades Especificas de la Red Central se implementa el Punto de Referencia de Integración de Pruebas, Punto de Referencia de Integración de Alarmas e Inventario. De igual forma en la capa de Elemento de Red se debe implementar tantas entidades monitoreadas como Funciones de Elemento de Red (NEFs) se implemento en la Arquitectura funcional.

4.1.1 Calificadores Obligatorio, Opcional y Condicional.

En el modelo de información diseñado para el sistema de soporte de operaciones planteado, se utiliza un número de términos que califican la relación entre la arquitectura de la información y su impacto en la implementación.

En la Tabla 2 se encuentran los significados de estos calificadores, pero se debe tener en cuenta

que la utilización de estos se hará por medio de las iniciales de sus significados en inglés, de la siguiente forma:

- Mandatory M = Obligatorio
- Conditional C = Condicional
- Optional O = Opcional

Tabla 2. Definiciones de los calificadores Mandatory, Optional y Conditional usados en la Arquitectura de la información.

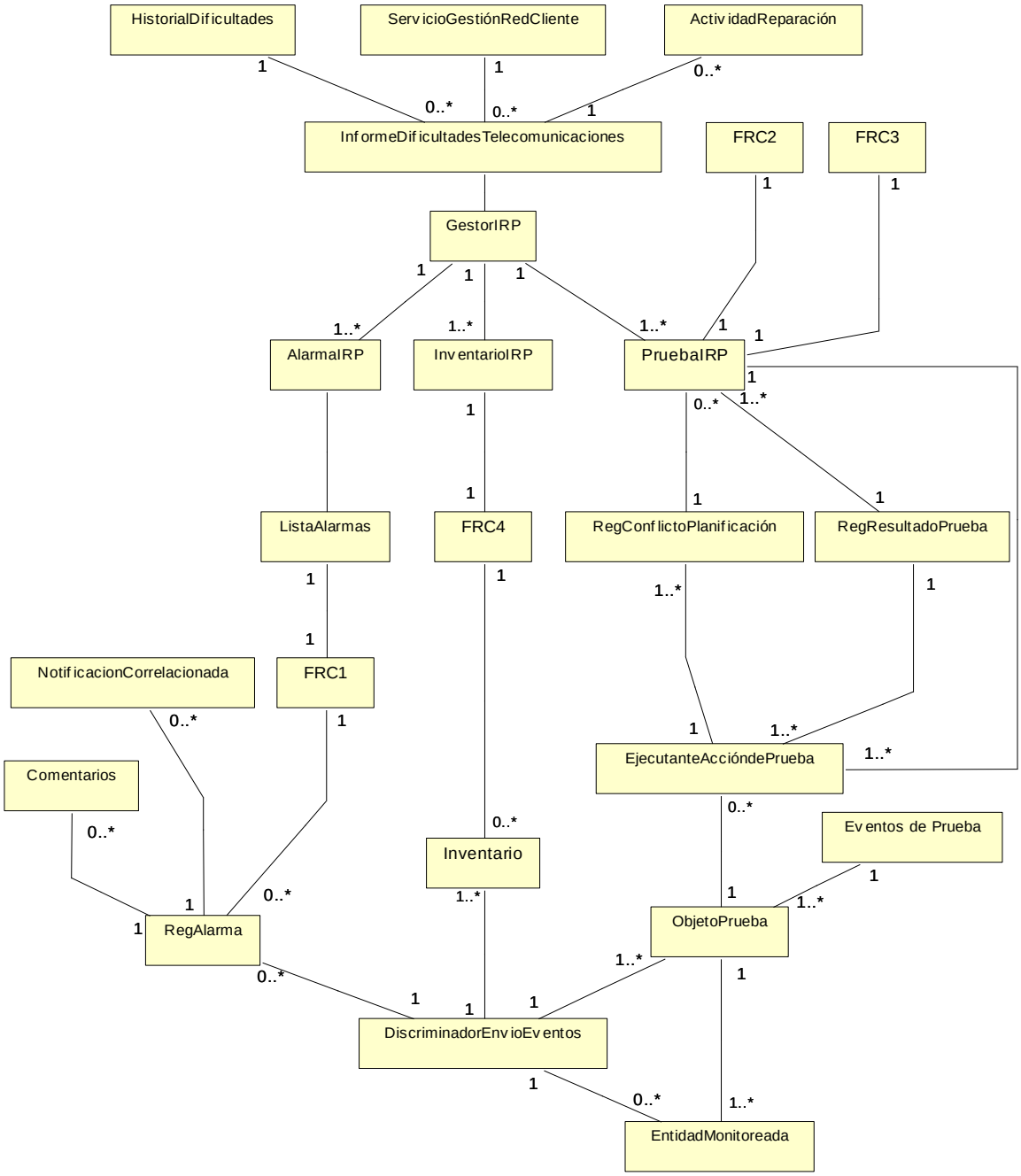
	Mandatory (M)	**Conditional (C)**	**Optional (O)**
Parámetros de Entrada y Salida	El parámetro deberá ser implementado de forma obligatoria, para la operación o notificación que lo contenga.	El parámetro deberá ser implementado de acuerdo a condiciones externas que afecten su existencia o no, dentro de una operación o una notificación.	El parámetro deberá ser implementado al criterio del desarrollador y necesidades del entorno, Por lo general estos parámetros sirven para ampliar información.
Atributos	El atributo deberá ser implementado de forma obligatoria, para la clase de objeto de información.	El atributo deberá ser implementado de acuerdo a condiciones externas que afecten su existencia o no, dentro de una clase de objeto de información.	El atributo deberá ser implementado al criterio del desarrollador y necesidades del entorno. Por lo general estos parámetros sirven para ampliar información.

4.1.2 Definición e Información Correspondiente.

Para la explicación de las clases de Objetos de Información se utiliza en las tablas de atributos la columna *Definición* en la cual se encuentra la descripción del atributo y adicionalmente se encuentra la referencia a la recomendación de donde fue tomado. De igual forma para la explicación de los parámetros de las interfaces usadas, se encuentra la Columna información correspondiente, donde se expone el significado del parámetro y su equivalente en el Servicio de Información de Gestión Común (CMISE, Common Management Information Service Element) o la referencia a la recomendación en donde fue encontrado.

4.2 CLASES DE OBJETOS DE INFORMACIÓN GENERAL

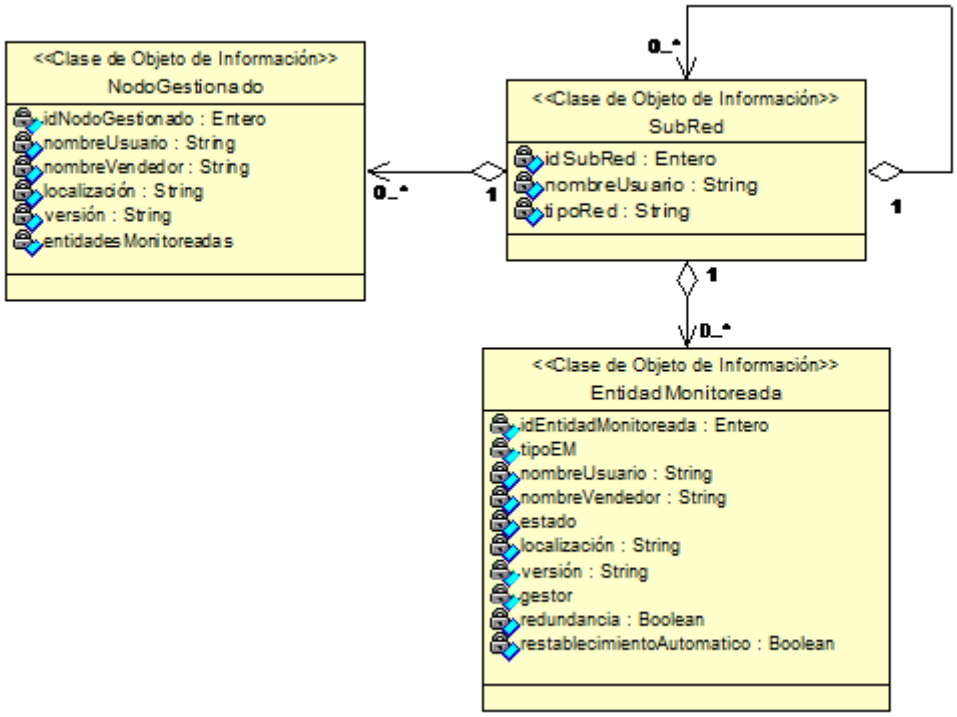
Figura 16. Diagrama de clases de Objetos de Información General



4.2.1 Entidad Monitoreada.

4.2.1.1 Clases de Objetos de Información.

Figura 17. Diagrama de Clases de Objetos de Información Entidad Monitoreada



EntidadMonitoreada

- **Definición:** representa los equipos de telecomunicaciones o entidades de la red de gestión dentro de la red de telecomunicaciones que ejecutan funciones de elementos gestionados (Ver figura 17).
- **Atributos:**

Tabla 3. Atributos EntidadMonitoreada

Nombre de Atributo	Calificador Soportado	Definición	Valores Legales
idEntidad Monitoreada	M	Este atributo contiene el identificador de la Entidad Monitoreada. 3GPP 32.622 ManagedElement.managedElementId [28]	Entero
tipoEM	M	Define el tipo de elemento gestionado. 3GPP 32.622 ManagedElement.managedElementType [28]	Instancia
nombreUsuario	M	Nombre asignado por el usuario. 3GPP 32.622 ManagedElement.userLabel [28]	String

nombreVendedor	M	Nombre asignado por el vendedor. 3GPP 32.622 ManagedElement.vendorName [28]	String
estado	M	Define el estado para uso específico del operador. 3GPP 32.622 ManagedElement.userDefinedState [28]	String
localización	M	Localización del elemento. 3GPP 32.622 ManagedElement.locationName [28]	String
versión	M	Versión del elemento. 3GPP 32.622 ManagedElement.swVersion [28]	String
gestor	M	Contiene la lista de instancias de nodos gestionados. 3GPP 32.622 ManagedElement.managedBy [28]	Instancia de nodos gestionados
redundancia	O	Representa si el Elemento gestionado tiene elementos redundantes.	Boolean
restablecimiento Automático	O	Indica si el Elemento gestionado tiene capacidad de restablecimiento automático.	Boolean

NodoGestionado

- **Definición:** representa un sistema de gestión de telecomunicaciones dentro del TMN que contiene funcionalidades para gestionar un número de Entidades Monitoreadas (Ver figura 17).
- **Atributos:**

Tabla 4. Atributos NodoGestionado

Nombre de Atributo	Calificador Soportado	Definición	Valores Legales
idNodoGestionado	M	Este atributo contiene el identificador del Nodo Gestionado. 3GPP 32.622 ManagedElement.managementNodeId [28]	Entero
nombreUsuario	M	Nombre asignado por el usuario. 3GPP 32.622 ManagedElement.userLabel [28]	String
nombreVendedor	M	Nombre asignado por el vendedor. 3GPP 32.622 ManagedElement.vendorName [28]	String
localización	M	Localización del elemento. 3GPP 32.622 ManagedElement.locationName [28]	String
Versión	M	Versión del elemento. 3GPP 32.622 ManagedElement.swVersion [28]	String
Entidades Monitoreadas	M	Contiene la lista de instancias de entidades monitoreadas. 3GPP 32.622 ManagedElement.managedElements [28]	Lista

SubRed

- **Definición:** representa un grupo de Entidades Monitoreadas como se ven sobre la interfaz-N (Ver figura 17).

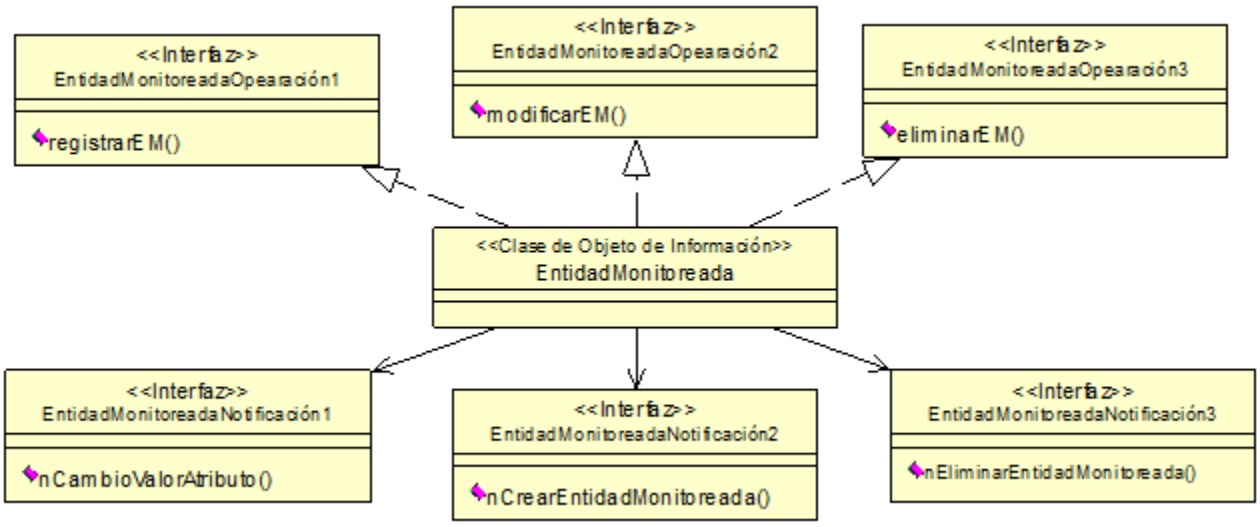
- **Atributos:**

Tabla 5. Atributos SubRed

Nombre de Atributo	Calificador Soportado	Definición	Valores Legales
idSubRed	M	Contiene el identificador de la SubRed. 3GPP 32.622 ManagedElement.subNetworkId [28]	Entero
nombreUsuario	M	Nombre asignado por el usuario. 3GPP 32.622 ManagedElement.userLabel [28]	String
TipoRed	M	Información relativa al tipo de red. 3GPP 32.622 ManagedElement.userDefinedNetworkType [28]	String

4.2.1.2 Definición de interfaces.

Figura 18. Diagrama de Interfaces Entidad Monitoreada



Interfaz EntidadMonitoreadaIRPNotificacion1

nCambioValorAtributo

Definición: el agente notifica el cambio del valor de un atributo (Ver figura 18).

Interfaz EntidadMonitoreadaIRPNotificacion2

nCrearEntidadMonitoreada

Definición*:* el agente notifica la creación de una Entidad Monitoreada (Ver figura 18).

Interfaz EntidadMonitoreadaIRPNotificacion3

nEliminarEntidadMonitoreada

Definición: el agente notifica la eliminación de una Entidad Monitoreada (Ver figura 18).

Interfaz EntidadMonitoreadaIRPOperación1

registrarEM

Definición: el gestor utiliza esta operación para crear una Entidad Monitoreada (Ver figura 18).

Interfaz EntidadMonitoreadaIRPOperación2

modificarEM

Definición: el gestor utiliza esta operación para modificar un atributo de una Entidad Monitoreada (Ver figura 18).

Interfaz EntidadMonitoreadaIRPOperación3

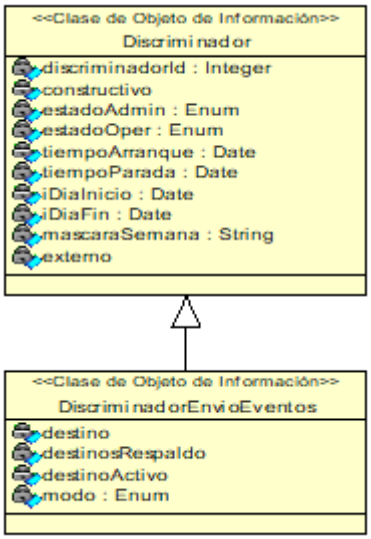
eliminarEM

Definición: el gestor utiliza esta operación para eliminar una Entidad Monitoreada (Ver figura 18).

4.2.2 Discriminador de Envío de Eventos.

4.2.2.1 Clases de Objetos de Información.

Figura 19. Diagrama de Clases de Objetos de Información Discriminador de Envío de Eventos.



Discriminador

- **Definición:** objeto de soporte de gestión que permite determinar los informes que deberán ser enviados a un determinado destino en periodos de tiempo definidos (Ver figura 19).
- **Atributos:**

Tabla 6. Atributos Discriminador

Nombre de Atributo	Calificador Soportado	Definición	Valores Legales
discriminadorId	M	Contiene el identificador del discriminador.	Entero

		CCITT X.734 discriminator.discriminatorId [16]	
Constructivo	M	Especifica pruebas para la información que procesa el discriminador. CCITT X.734 discriminator.discriminatorConstruct [16]	
estadoAdmin	M	Define el estado administrativo del discriminador. En estado desbloqueado se permite el procesamiento de información, mientras en bloqueado no. CCITT X.734 discriminator.administrativeState [16]	Enum: - Desbloqueado - Bloqueado
estadoOper	M	Define el estado operativo del discriminador. En estado habilitado el discriminador se encuentra en estado operacional y en deshabilitado el discriminador no se encuentra en estado operacional. CCITT X.734 discriminator.operationalState [16]	Enum: - Habilitado - Deshabilitado
tiempo Arranque	C	Define la fecha y hora en el que el discriminador desbloqueado y habilitado comienza a funcionar. CCITT X.734discriminator.startTime [16]	Date
tiempo Parada	C	Define la fecha y hora en el que el discriminador deja de funcionar. CCITT X.734 discriminator.stopTime [9]	Date
iDiaInicio e iDiaFin	O	Definen el intervalo de tiempo en el cual se encuentra en condición de servicio, fuera de este periodo se encuentra fuera de servicio. CCITT X.734 discriminator.intervalsOfDay [16]	Date
mascara Semana	O	Define los días de la semana en los cuales el discriminador se encontrará en servicio. Si no se especifica el discriminador estará disponible toda la semana. CCITT X.734 discriminator.weekMask [16]	Lista de días
Externo	O	Proporciona el nombre de un objeto gestionado encargado de realizar la planificación.	String

DiscriminadorEnvioEventos

- **Definición:** objeto utilizado para determinar los informes de eventos que deberán ser enviados a un determinado destino en un periodo de tiempo especificado. Este objeto hereda de Discriminador (Ver figura 19).
- **Atributos:**

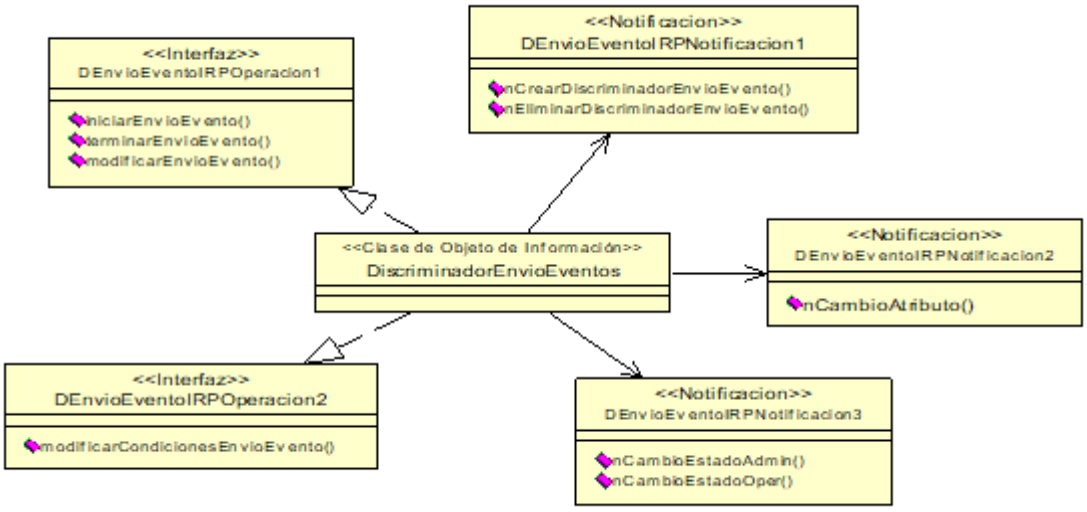
Tabla 7. Atributos DiscriminadorEnvíoEventos

Nombre de Atributo	Calificador Soportado	Definición	Valores Legales
destino	M	Define el destino o los destinos a los que se envían informes de eventos. CCITT X.734 eventForwardingDiscriminator.	Entero

		Destination [16]	
destinosRespaldo	O	Define destinos de respaldo en caso de que falle el destino especificado en el atributo destino. CCITT X.734 eventForwardingDiscriminator. backUpDestinationList [16]	Entero
destinoActivo	O	Identifica el destino al que el discriminador está enviando la información. CCITT X.734 eventForwardingDiscriminator. activeDestination [16]	Entero
modo	M	Determina el modo de señalización de eventos. CCITT X.734 eventForwardingDiscriminator.mode [16]	Enum: • Confirmado • No Confirmado

4.2.2.2 Definición de interfaces

Figura 20. Diagrama de Interfaces de DiscriminadorEnvioEventos.



Interfaz DEnvioEventoIRPNotificacion1

- **nCrearDiscriminadorEnvioEvento**

  Definición: el agente notifica al gestor que se ha creado un nuevo Discriminador de Envió de Eventos (Ver figura 20).
- **nEliminarDiscriminadorEnvioEvento**

  Definición: el agente notifica al gestor que se ha eliminado un Discriminador de Envió de Eventos (Ver figura 20).

Interfaz DEnvioEventoIRPNotificacion2

- **nCambioAtributo**

  Definición: el agente notifica al gestor la modificación de un atributo del Discriminador de Envió de Eventos (Ver figura 20).

Interfaz DEnvioEventoIRPNotificacion3

- **nCambioEstadoAdmin**
  Definición: el agente notifica al gestor la modificación el estado administrativo (atributo estadoAdmin) del Discriminador de Envió de Eventos (Ver figura 20).
- **nCambioEstadoOper**
  Definición: el agente notifica al gestor la modificación el estado operativo (atributo estadoOper) del Discriminador de Envió de Eventos (Ver figura 20).

Interfaz DEnvioEventoIRPOperacion1

- **iniciarEnvioEvento**
  Definición: el gestor utiliza esta operación para que se cree un discriminador de envío de evento, e imponer controles de envíos de eventos, ingresando el identificador (Ver figura 20).
- **terminarEnvioEvento**
  Definición: el gestor utiliza esta operación para que se elimine un discriminador de envío de eventos, y termine el control de envíos de eventos (Ver figura 20).
- **modificarEnvioEvento**
  Definición: el gestor utiliza esta operación para modificar el estado administrativo o atributos del discriminador de envío de eventos (Ver figura 20).

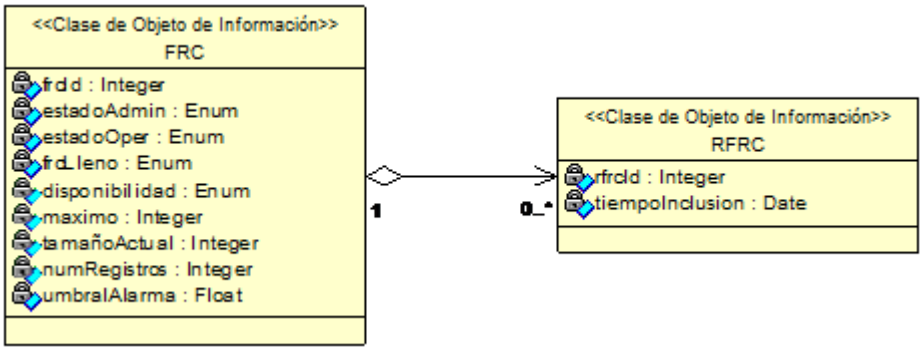
Interfaz DEnvioEventoIRPOperacion2

- **recuperarCondicionesEnvioEvento**
  Definición: el gestor utiliza esta operación para recuperar atributos del discriminador de envío de eventos (Ver figura 20).

4.2.3 Fichero Registro Cronológico (FRC).

4.2.3.1 Clases de Objetos de Información.

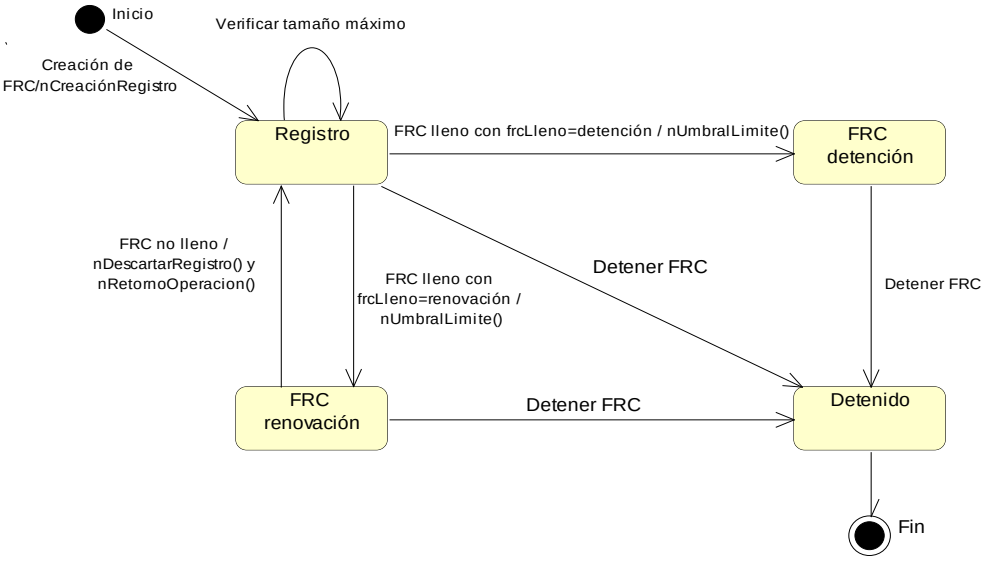
Figura 21. Diagrama de Clases de Objetos de Información Fichero Registro Cronológico (FRC).



FRC

- **Definición:** representa una clase de soporte de gestión que modela recursos utilizados como un depositario para registros de fichero registro cronológico (Ver figura 21). [17]
- **Diagrama de estados:**

Figura 22. Diagrama de estados Fichero Registro Cronológico (FRC).



- **Atributos:**

Tabla 8. Atributos FRC

Nombre de Atributo	Calificador Soportado	Definición	Valores Legales
frcId	M	Contiene el identificador del FRC. CCITT X.735 log.logId [17]	Entero
estadoAdmin	M	Define el estado administrativo del FRC. En estado Desbloqueado se permite la utilización y se puede recuperar información de registros dependientes y crear nuevos registros. En estado Bloqueado no se permite la utilización, se puede recuperar información de registros dependientes y suprimir registros, no se pueden crear nuevos registros. CCITT X.735 log.administrativeState [17]	Enum: • Desbloqueado • Bloqueado
estadoOper	M	Define el estado operativo del FRC. En estado Habilitado el FRC se encuentra en estado operacional y se puede utilizar, se puede recuperar información de registros dependientes y crear nuevos registros. En estado Deshabilitado el FRC no se encuentra en estado operacional y no se	Enum: • Habilitado • Deshabilitado

		pueden crear nuevos registros. CCITT X.735 log.operationalState [17]	
frcLleno	M	Indica la acción que será tomada cuando el tamaño máximo del FRC se ha alcanzado. CCITT X.735 log.logFullAction [17]	Enum: • Renovación: se suprimen los registros más antiguos. • Detención: el Fichero Registro Cronológico se detiene, no se hacen más registros.
disponibilidad	M	Indica el estado actual del FRC. CCITT X.735 log.availabilityStatus [17]	Enum: • Lleno • Detenido • Registrando • Deshabilitado • Habilitado
maximo	M	Determina el tamaño máximo en bytes del FRC. CCITT X.735 log.maxLogSize [17]	Entero, cero para indicar que no tiene límite
tamañoActual	M	Determina el número de byte utilizados por el FRC. CCITT X.735 log.currentLogSize [17]	Entero
numRegistros	M	Determina el número de registros del FRC. CCITT X.735 log.numberOfRecords [17]	Entero
umbralAlarma	M	Determina cuando se genera un evento (porcentaje) de alarma que indique que esta próximo a llenarse el FRC. CCITT X.735 log.capacityAlarmThreshold [17]	Entero

RFRC

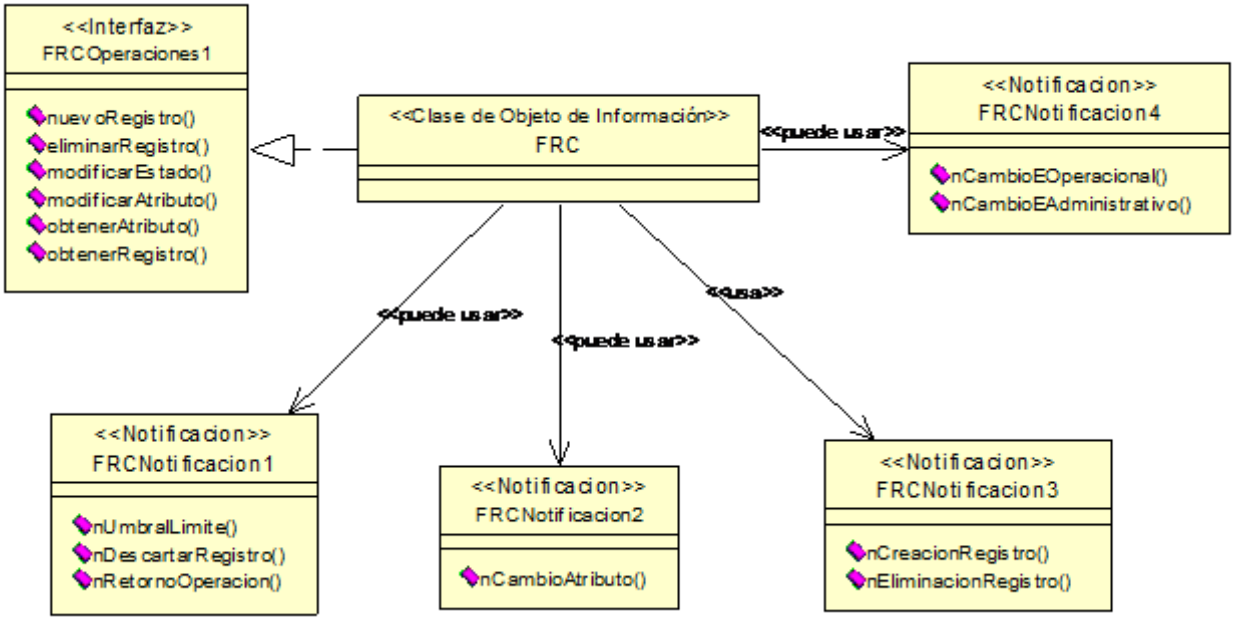
- **Definición:** representa una clase de soporte de gestión que modela unidades de información almacenadas en un fichero registro cronológico (Ver figura 21). [17]
- **Atributos:**

Tabla 9. Atributos RFRC

Nombre de Atributo	Calificador Soportado	Definición	Valores Legales
rfrcId	M	Contiene el identificador de un Registro de Fichero Registro Cronológico. CCITT X.735 logRecord.logRecordId [17]	Entero
tiempoInclusion	M	Determina la fecha y hora en que se ingresó el registro al Fichero Registro Cronológico. CCITT X.735 logRecord.loggingTime [17]	Date

4.2.3.2 Definición de interfaces

Figura 23. Diagrama de Interfaces de FRC.



Interfaz FRCNotificacion1

nUmbralLimite

Definición: el agente notifica al gestor que el nivel del Fichero Registro Cronológico ha llegado o cruzado el umbral (Ver figura 23).

nDescartarRegistro

Definición: el agente notifica al gestor que se ha suprimido un registro del Fichero Registro Cronológico, para poder ingresar un nuevo registro (Ver figura 23).

nRetornoOperacion

Definición: el agente notifica al gestor que se ha reducido la cantidad de registros y se ha retomado la actividad en el Fichero Registro Cronológico (Ver figura 23).

Interfaz FRCNotificacion2

nCambioAtributo

Definición: el agente notifica al gestor la modificación de un atributo del Fichero Registro Cronológico (Ver figura 23).

Interfaz FRCNotificacion3

nCreacionRegistro

Definición: el agente notifica al gestor que se ha agregado un nuevo Registro al Fichero

Registro Cronológico (Ver figura 23).

nEliminacionRegistro

Definición: el agente notifica al gestor que se ha eliminado un Registro del Fichero Registro Cronológico (Ver figura 23).

Interfaz FRCNotificacion4

nCambioEOperacional

Definición: el agente notifica al gestor la modificación el estado operaciones (atributo estadoOper) del Fichero Registro Cronológico (Ver figura 23).

nCambioEAdministrativo

Definición: el agente notifica al gestor la modificación el estado administrativo (atributo estadoAdmin) del Fichero Registro Cronológico (Ver figura 23).

Interfaz FRCOperaciones1

nuevoRegistro

Definición: el gestor utiliza esta operación para ingresar un nuevo Registro en el Fichero Registro Cronológico, ingresando en identificador del registro a crear, la disponibilidad (Ver figura 23).

eliminarRegistro

Definición: el gestor utiliza esta operación para eliminar un Registro del Fichero Registro Cronológico, ingresando en identificador del registro a eliminar (Ver figura 23).

modificarEstado

Definición: el gestor utiliza esta operación para modificar el estado del Fichero Registro Cronológico (Ver figura 23).

modificarAtributo

Definición: el gestor utiliza esta operación para modificar un atributo del Fichero Registro Cronológico (Ver figura 23).

obtenerAtributo

Definición: el gestor utiliza esta operación para obtener un atributo del Fichero Registro Cronológico (Ver figura 23).

obtenerRegistro

Definición: el gestor utiliza esta operación para obtener un registro del Fichero Registro Cronológico completo o parcial (Ver figura 23).

4.2.4 Inventario.

4.2.4.1 Clases de Objetos de Información.

Figura 24. Diagrama de Clases de Objetos de Información de Inventario.

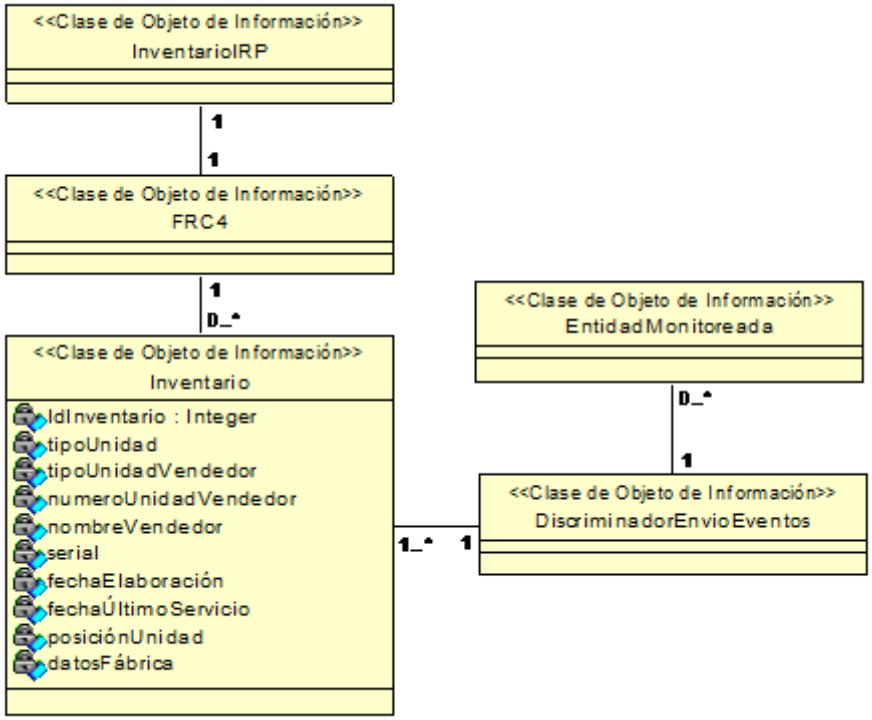
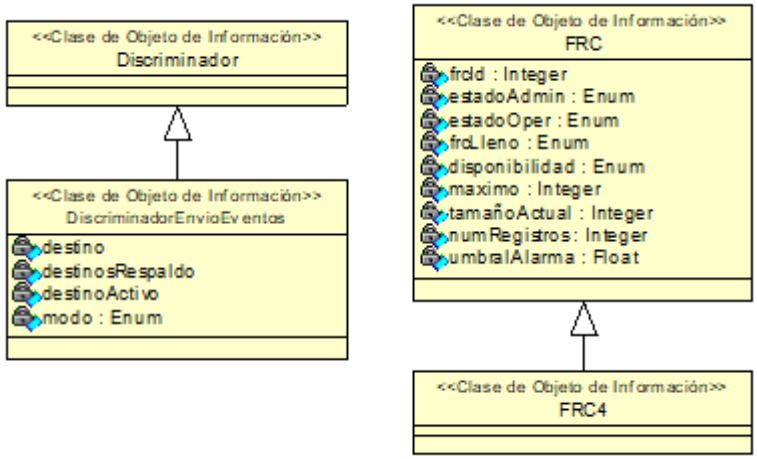


Figura 25. Diagrama de herencia.



Inventario

- **Definición:** representa la información de un inventario de un recurso de la red de 3G y hereda de la clase RFRC (Ver figura 24).

- **Atributos:**

Tabla 10. Atributos Inventario

Nombre de Atributo	Calificador Soportado	Definición	Valores Legales
IdInventario	M	Este atributo contiene el identificador del Inventario. 3GPP 32.692 InventoryUnit.inventoryUnitId [29]	Entero
tipoUnidad	M	Define el tipo de la Unidad de inventario. 3GPP 32.692 InventoryUnit.inventoryUnitType [29]	String
tipoUnidadVendedor	M	Tipo de unidad asignado por el vendedor. 3GPP 32.692 InventoryUnit.vendorUnitFamilyType [29]	String
númeroUnidad Vendedor	M	Número con el identificador y versión de la unidad asignado por el vendedor.vendorUnitTypeNumber	String
nombreVendedor	M	Nombre asignado por el vendedor. 3GPP 32.692 InventoryUnit.vendorName [29]	String
serial	M	Número del serial de la unidad. 3GPP 32.692 InventoryUnit.serialNumber [29]	String
fechaElaboración	O	Fecha de elaboración de la unidad. 3GPP 32.692 InventoryUnit.dateOfManufacture [29]	Date
fechaÚltimoServicio	O	Fecha del último servicio o de reparación. 3GPP 32.692 InventoryUnit.dateOfLastService [22]	Date
posiciónUnidad	O	Posición de la unidad. 3GPP 32.692 InventoryUnit.unitPosition [29]	Enum: • Soporte • Estante • Ranura • Otra
datosFábrica	O	Información adicional de fábrica. 3GPP 32.692 InventoryUnit.manufacturerData [29]	String

FRC4

- **Definición:** clase de objeto de información hereda de Fichero de Registro Cronológico FRC, y se crea para almacenar los inventarios (Ver figura 24).

DiscriminadoEnvioEventos

- **Definición:** esta clase de objeto de información hereda de la clase DiscriminadorEnvioEventos, y se implementa para garantizar el filtraje de eventos desde la entidad monitoreada hacia el proceso de gestión de Inventario (Ver figura 24).

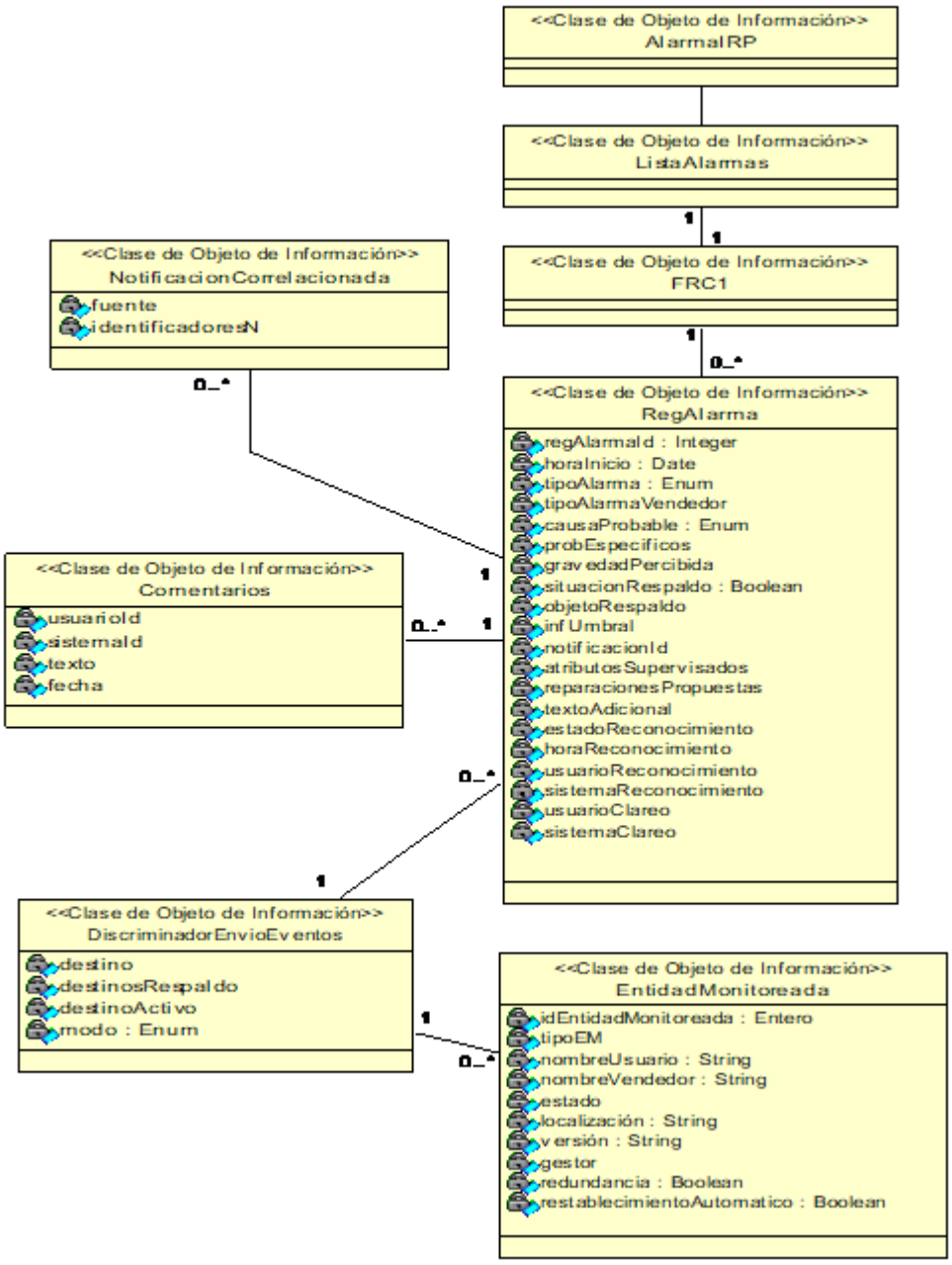
InventarioIRP

- **Definición:** esta clase de objeto de información representa las capacidades de gestión del Inventario y hace parte de la Interfaz-N existente entre la capa de gestión de Elementos de Red y la capa de Red de TMN. El inventario emplea este objeto para intercambiar información entre las capas superiores y el Fichero Registro Cronológico de Inventario (FRC4) (Ver figura 24).

4.2.5 Punto de Referencia de Integración de Alarmas.

4.2.5.1 Clases de Objetos de Información.

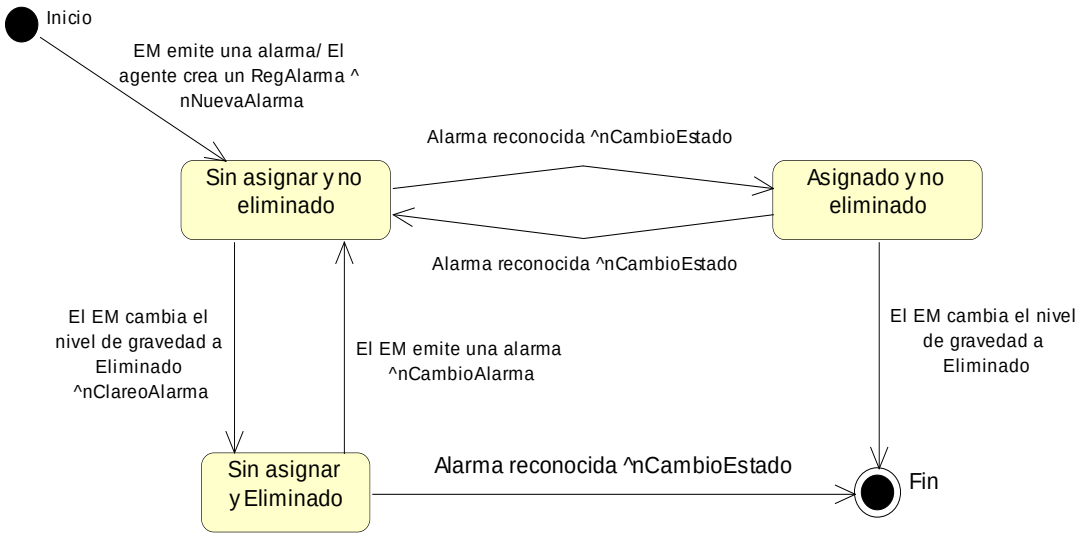
Figura 26. Diagrama de Clases de Objetos de Información de Punto de Referencia de Integración de Alarmas.



RegAlarma

- **Definición:** contiene información de una alarma de una Entidad monitoreada. Hereda del Registro de Fichero Registro Cronológico (Ver figura 26).
- **Diagrama de estados**

Figura 27. Diagrama de estados RegAlarma



- **Atributos:**

Tabla 11. Atributos RegAlarma

Nombre de Atributo	Calificador Soportado	Definición	Valores Legales
regAlarmaId	M	Contiene el identificador del registro de alarma. 3GPP 32.111-2 AlarmInformation.alarmId [24]	Entero
horaInicio	M	Indica la fecha y hora en la que la alarma fue iniciada por el Objeto Gestionado. 3GPP 32.111-2 AlarmInformation.startTime [24]	Date
tipoAlarma	M	Este parámetro clasifica la alarma. 3GPP 32.111-2 AlarmInformation.eventType [24]	Ver anexo C
tipoAlarma Vendedor	O	Indica la alarma específica del vendedor que identifica el tipo de alarma de NE o el tipo de alarma relacionada de NE. 3GPP 32.111-2 AlarmInformation.vendorSpecificAlarmType [24]	String
causaProbable	O	Este parámetro da una descripción detallada de la causa probable de la alarma. 3GPP 32.111-2	Ver anexo C

		AlarmInformation.probableCause [24]	
probEspecificos	O	Este parámetro entrega mas detalles de la causa del problema. 3GPP 32.111-2 AlarmInformation.specificProblem [24]	String
gravedad Percibida	M	Indica en que cantidad se ha afectado el objeto gestionado. 3GPP 32.111-2 AlarmInformation.perceivedSeverity [24]	Enum: • Crítico • Mayor • Menor • Aviso • Indeterminado • Eliminado
situación Respaldo	O	Determina si el objeto que emitió la alarma está respaldado o no. 3GPP 32.111-2 AlarmInformation.backedUpStatus [24]	Boolean
objetoRespaldo	C	Determina el objeto que respaldo al objeto que emite la alarma en caso de que situaciónRespaldo se verdadero. [24]	Entero
infoUmbral	O	Este parámetro tiene información del umbral en caso que la alarma se de rebasamiento de este. 3GPP 32.111-2 AlarmInformation.thresholdInfo [24]	String
notificacionId	C	Contiene los identificadores de las notificaciones correlacionadas. 3GPP 32.111-2 AlarmInformation.notificationId [24]	Entero
atributos Supervisados	C	Contiene los atributos y sus valores del objeto gestionado en el momento de la alarma. 3GPP 32.111-2 AlarmInformation.monitoredAttributes [24]	
reparaciones Propuestas	O	Presenta una sugerencia de reparaciones. 3GPP 32.111-2 AlarmInformation.proposedRepairActions [24]	String
textoAdicional	O	Descripción libre. 3GPP 32.111-2 AlarmInformation.additionalText [24]	String
estado Reconocimiento	M	Determina el estado de reconocimiento de la alarma. 3GPP 32.111-2 AlarmInformation.ackState [24]	Enum: • Reconocida • No reconocida
hora Reconocimiento	C	Contiene la hora de reconocimiento. 3GPP 32.111-2 AlarmInformation.ackTime [24]	Date
usuario Reconocimiento	C	Contiene el identificador del último usuario que cambio el estado de reconocimiento. 3GPP 32.111-2 AlarmInformation.ackUserId [24]	Entero
sistema Reconocimiento	C	Contiene el identificador del sistema del que se identificó la alarma. 3GPP 32.111-2 AlarmInformation.ackSystemId [24]	Entero

usuarioClareo	C	Contiene el identificador del usuario que eliminó la alarma. 3GPP 32.111-2 AlarmInformation.clearUserId [24]	Entero
sistemaClareo	C	Contiene el identificador del sistema desde el cual se eliminó la alarma. 3GPP 32.111-2 AlarmInformation.clearSystemId [24]	Entero

ListaAlarmas

- **Definición:** Esta objeto tiene todas las alarmas activas actualmente (gravedadPercibida diferente de Eliminado) y las alarmas que son Clareadas pero todavía no reconocidas. Hereda de Fichero Registro Cronológico (Ver figura 26).

Comentarios

- **Definición:** este objeto tiene información adicional asociada a una alarma (Ver figura 26).
- **Atributos:**

Tabla 12. Atributos Comentarios

Nombre de Atributo	Calificador Soportado	Definición	Valores Legales
usuarioId	M	Contiene el identificador del usuario que realizó el comentario. 3GPP 32.111-2 Comment.commentUserId [24]	Entero
sistemaId	O	Contiene el identificador del sistema desde el que hizo el comentario. 3GPP 32.111-2 Comment.commentSystemId [24]	Entero
texto	M	Contiene el comentario. 3GPP 32.111-2 Comment.commentText [24]	String
fecha	O	Contiene la hora en que se realizó el comentario. 3GPP 32.111-2 Comment.commentTime [24]	Date

NotificaciónCorrelacionada

- **Definición:** este objeto identifica un conjunto de notificaciones con las que se considera que la alarma está correlacionada (Ver figura 26).
- **Atributos:**

Tabla 13. Atributos NotificaciónCorrelacionada

Nombre de Atributo	Calificador Soportado	Definición	Valores Legales
fuente	M	Contiene el identificador del objeto gestionado. 3GPP 32.111-2 CorrelatedNotification.source [24]	Entero
identificadoresN	M	Contiene los identificadores de las notificaciones. 3GPP 32.111-2 CorrelatedNotification.notificationIdSet [24]	Entero

FRC1

- **Definición:** clase de objeto de información hereda de Fichero de Registro Cronológico FRC, y se crea para almacenar los Registros de Alarmas (RegAlarma) (Ver figura 26).

DiscriminadoEnvioEventos

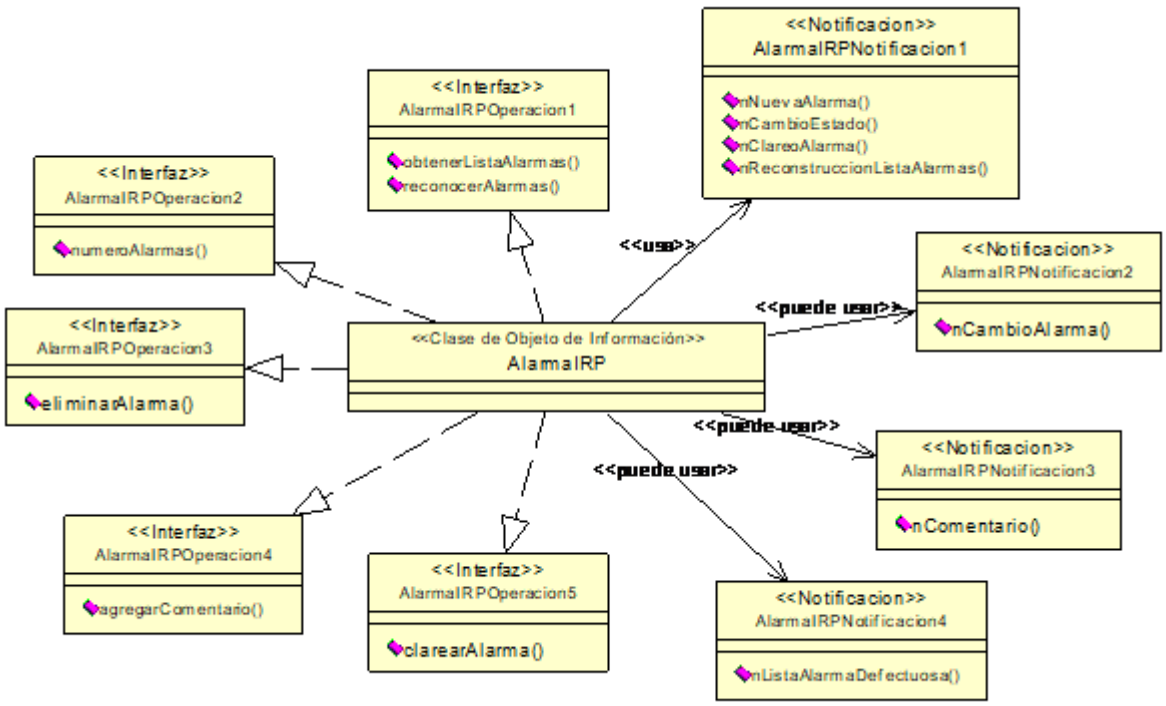
- **Definición:** esta clase de objeto de información hereda de la clase DiscriminadorEnvioEventos, y se implementa para garantizar el filtraje de eventos desde la entidad monitoreada hacia el proceso de gestión de Alarmas (Ver figura 26).

AlarmaIRP

- **Definición:** esta clase de objeto de información representa las capacidades de gestión de las alarmas y hace parte de la Interfaz-N existente entre la capa de gestión de Elementos de Red y la capa de Red de TMN. Se emplea para intercambiar información entre las capas superiores y la lista de alarmas activas (ListaAlarmas) (Ver figura 26).

4.2.5.2 Definición de interfaces

Figura 28. Diagrama de Interfaces de AlarmaIRP.



Interfaz AlarmaIRPNotificacion1

nNuevaAlarma

Definición: se ha agregado un nuevo registro de alarma (RegAlarma) en ListaAlarma (Ver figura 28).

Parámetros de entrada

Tabla14. Parámetros de entrada nNuevaAlarma

Nombre	Calificador	Información correspondiente
Instancia de Objeto	M	EntidadMonitoreada.ClaseObjeto
Id Notificación	M	
Hora de evento	M	RegAlarma.horaInicio
Tipo de Notificación	M	“Notificar Nueva Alarma”
Causa probable	M	RegAlarma.causaProbable
Severidad Percibida	M	RegAlarma.gravedadPercibida
Tipo de Alarma	M	RegAlarma.tipoAlarma
Tipo de Alarma del vendedor	O	RegAlarma.tipoAlarmaVendedor
Problemas Específicos	O	RegAlarma.probEspecificos
Notificaciones Correlacionadas	O	NotificacionCorrelacionada asociada al Registro de Alarmas
Situación de respaldo	O	RegAlarma.situacionRespaldo
Objeto de respaldo	O	RegAlarma.objetoRespaldo
Información de umbral	O	RegAlarma.infUmbral
Atributos monitoreados	O	RegAlarma.atributosSupervisados
Reparaciones propuestas	O	RegAlarma.reparacionesPropuestas
Texto adicional	O	RegAlarma.textoAdicional
Identificador de registro de alarma	M	RegAlarma.regAlarmaId

nCambioEstado

Definición: se notifica al gestor el cambio de estado (atributo estadoReconocimiento) (Ver figura 28).

Parámetros de entrada

Tabla 15. Parámetros de entrada nCambioEstado

Nombre	Calificador	Información correspondiente
Instancia de Objeto	M	EntidadMonitoreada.ClaseObjeto
Id Notificación	M	
Hora de evento	M	RegAlarma.horaInicio
Tipo de Notificación	M	"Notificar Cambio de Estado"
Causa probable	M	RegAlarma.causaProbable
Severidad Percibida	M	RegAlarma.gravedadPercibida
Tipo de Alarma	M	RegAlarma.tipoAlarma
Identificador de registro de alarma	M	RegAlarma.regAlarmaId
Estado de reconocimiento	M	RegAlarma.estadoReconocimiento
Usuario de reconocimiento	M	RegAlarma.usuarioReconocimiento
Sistema de reconocimiento	O	RegAlarma.sistemaReconocimiento

nClareoAlarma

Definición: el agente notifica al gestor el cambio del nivel de gravedad a Eliminado (Ver figura 28).

Parámetros de entrada

Tabla 16. Parámetros de entrada nClareoAlarma

Nombre	Calificador	Información correspondiente
Instancia de Objeto	M	EntidadMonitoreada.ClaseObjeto
Id Notificación	M	
Hora de evento	M	RegAlarma.horaInicio
Tipo de Notificación	M	"Notificar Clareo de Alarma"
Causa probable	M	RegAlarma.causaProbable
Severidad Percibida	M	RegAlarma.gravedadPercibida
Tipo de Alarma	M	RegAlarma.tipoAlarma
Notificaciones Correlacionadas	O	NotificacionCorrelacionada asociada al Registro de Alarmas
Usuario de Clareo	O	RegAlarma.clearUserId
Sistema de clareo	O	RegAlarma.usuarioClareo
Identificador de registro de alarma	M	RegAlarma.sistemaClareo

nReconstruccionListaAlarmas

Definición: el agente notifica la reconstrucción de la lista de alarmas (Ver figura 28).

Parámetros de entrada

Tabla 17. Parámetros de entrada nReconstrucciónListaAlarmas

Nombre	Calificador	Información correspondiente
Instancia de Objeto	M	EntidadMonitoreada.ClaseObjeto
Id Notificación	M	
Hora de evento	M	RegAlarma.horaInicio
Tipo de Notificación	M	"Notificar Reconstrucción de Lista de Alarmas"
Razones	M	

Interfaz AlarmaIRPNotificacion2

nCambioAlarma

Definición: se notifica al gestor el cambio del atributo gravedadPercibida (Ver figura 28).

Parámetros de entrada

Tabla 18. Parámetros de entrada nCambioAlarma

Nombre	Calificador	Información correspondiente
Instancia de Objeto	M	EntidadMonitoreada.ClaseObjeto
Id Notificación	M	
Hora de evento	M	RegAlarma.horaInicio
Tipo de Notificación	M	"Notificar Cambio de Alarma"
Causa probable	M	RegAlarma.causaProbable
Severidad Percibida	M	RegAlarma.gravedadPercibida
Tipo de Alarma	M	RegAlarma.tipoAlarma
Identificador de registro de alarma	M	RegAlarma.sistemaClareo

Interfaz AlarmaIRPNotificacion3

nComentario

Definición: se notifica al gestor la adición de un comentario a un Registro de Alarma(Ver figura 28).

Parámetros de entrada

Tabla 19. Parámetros de entrada nComentario

Nombre	Calificador	Información correspondiente
Instancia de Objeto	M	EntidadMonitoreada.ClaseObjeto
Id Notificación	M	
Hora de evento	M	RegAlarma.horaInicio
Tipo de Notificación	M	"Notificar Comentarios"
Tipo de Alarma	M	RegAlarma.tipoAlarma
Causa probable	M	RegAlarma.causaProbable
Severidad Percibida	M	RegAlarma.gravedadPercibida
Comentarios	M	Comentarios relacionados a la alarma
Identificador de registro de alarma	M	RegAlarma.sistemaClareo

Interfaz AlarmaIRPNotificacion4

nListaAlarmaDefectuosa

Definición: el agente notifica la pérdida de confidencialidad en la integración de la Lista de Alaramas (Ver figura 28).

Parámetros de entrada

Tabla 20. Parámetros de entrada nListaAlarmaDefectuosa

Nombre	Calificador	Información correspondiente
Instancia de Objeto	M	EntidadMonitoreada.ClaseObjeto
Id Notificación	M	
Hora de evento	M	RegAlarma.horaInicio
Tipo de Notificación	M	"Notificar Lista de Alarma Defectuosa"

Interfaz AlarmaIRPOperacion1

obtenerListaAlarmas

Definición: el gestor invoca esta operación para solicitar un a lista completa o parcial (activas, activas y reconocidas, activas y desconocidas, Eliminadas y reconocidas, no reconocidas) de los registros de alarmas de la Lista de Alarmas (Ver figura 28).

reconocerAlarmas

Definición: el gestor invoca esta operación para reconocer una o mas alarmas, ingresando la lista de identificadores de los registros, la gravedad percibida y los datos del usuario y del sistema (Ver figura 28).

Interfaz AlarmaIRPOperacion2

numeroAlarmas

Definición: el gestor pide la cantidad de Registros de Alarmas que hay en una Lista de Alarmas, puede emplear un filtro (todas, activas, activas y reconocidas, activas y desconocidas, Eliminadas y reconocidas, no reconocidas) (Ver figura 28).

Interfaz AlarmaIRPOperacion3

eliminarAlarma

Definición: el gestor invoca esta operación para eliminar información de uno o mas Registros de Alarmas, ingresando el identificador de los registros de alarmas (Ver figura 28).

Interfaz AlarmaIRPOperacion4

agregarComentario

Definición: el gestor invoca esta operación para agregar un comentario a un Registro de Alarma, ingresando el identificador de los registros de alarmas y los datos que se agregarán (usuarioId, sistemaId, texto) (Ver figura 28).

Interfaz AlarmaIRPOperacion5

clarearAlarma

Definición: el gestor invoca esta operación para clarear (gravedadPercibida = Eliminado) un Registro de Alarma de la Lista de Alarmas, ingresando el identificador de los registros de alarmas (Ver figura 28).

4.2.6 Punto de Referencia de Integración de Pruebas.

4.2.6.1 Clases de Objetos de Información.

Figura 29. Diagrama de Clases de Objetos de Información de Punto de Referencia de Integración de Pruebas.

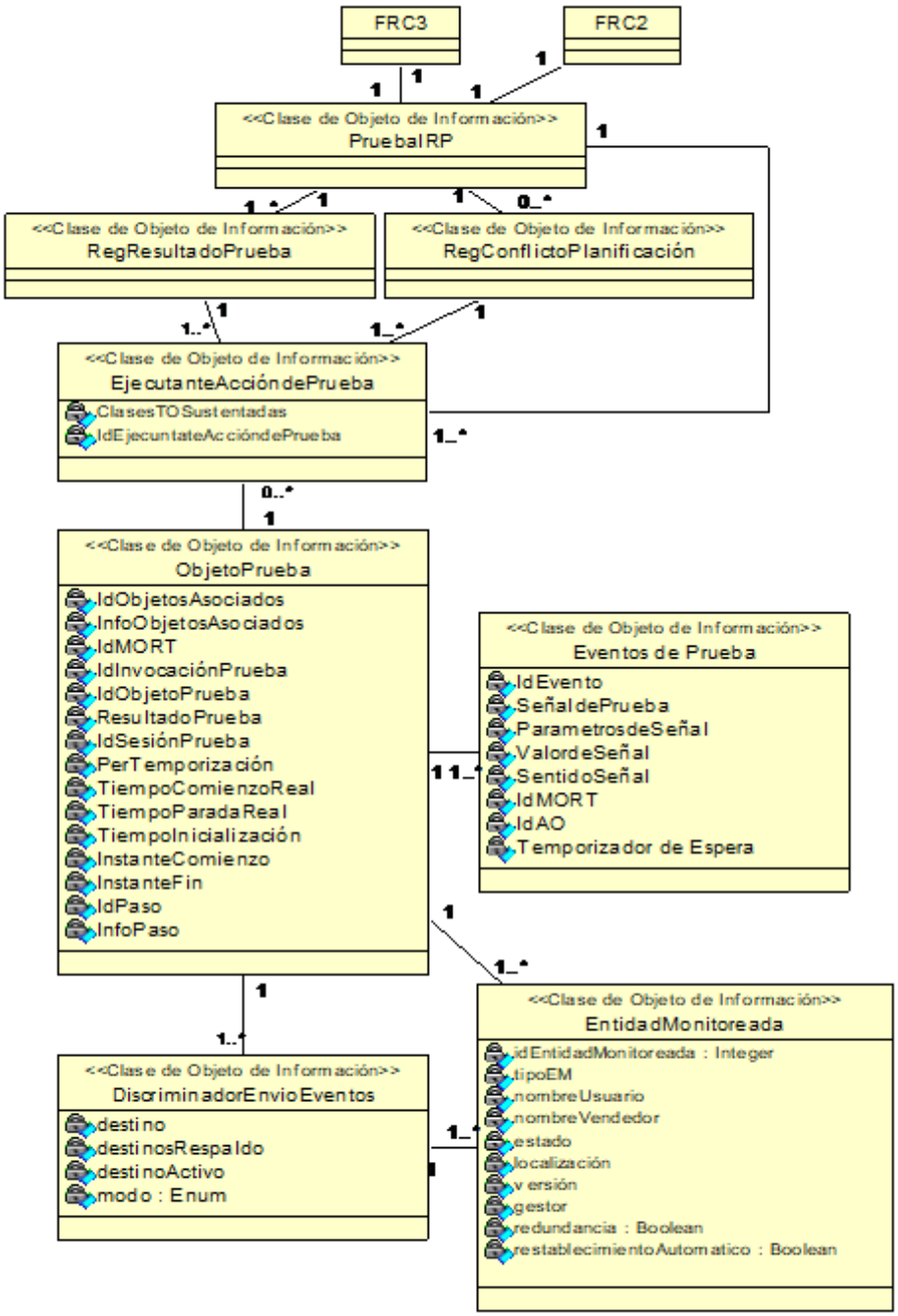
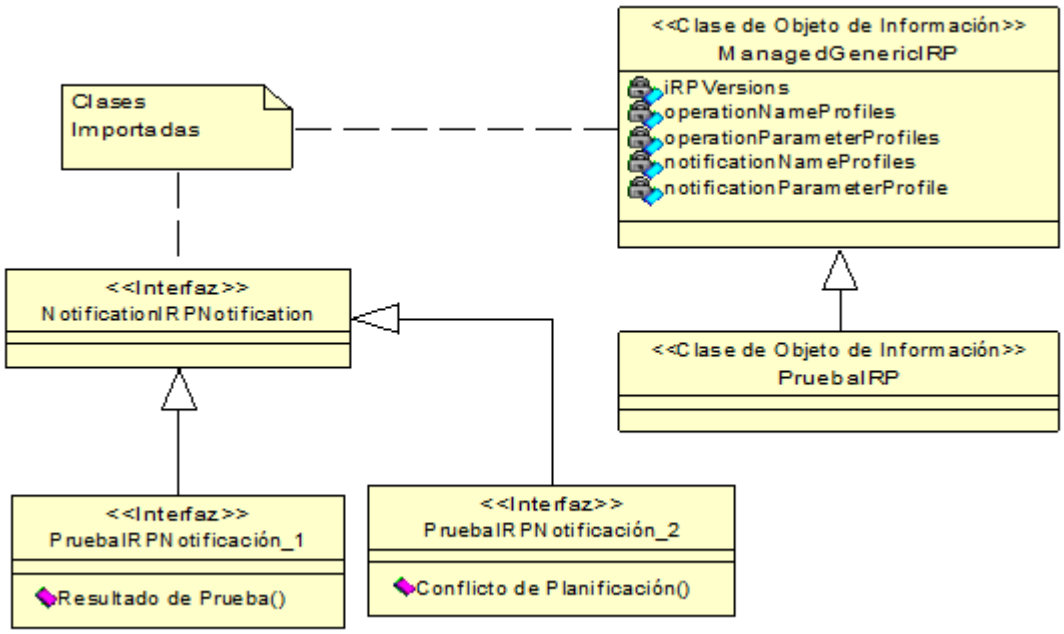


Figura 30. Diagrama de herencia Prueba IRP.



PruebaIRP

- **Definición:** PruebaIRP es la representación de las capacidades de Gestión de Pruebas del OSS y hace parte de la Interfaz-N existente entre la capa de gestión de Elementos de Red y la capa de Red de TMN. Esta Clase Objeto de Información (IOC, Information Object Class) hereda de la IOC ManagedGenericIRP especificada en la recomendación 3GPP TS 32.312 [26]. (Ver figura 29).

Ejecutante de Acción de Prueba

- **Definición:** cumple la función de AgenteIRP. Esta clase de objeto de información tiene la funcionalidad de recibir y responder peticiones de prueba y esta representado en la arquitectura funcional por los OSF-MAF agentes de cada OSF planteado en la capa de gestión de elementos de red. Además es la que crea y controla los objetos de Prueba a partir de Peticiones del gestor de la Prueba. ITU-T X.745 Objetos testActionPerformer [19]. (Ver figura 29).

- ***Atributos:***

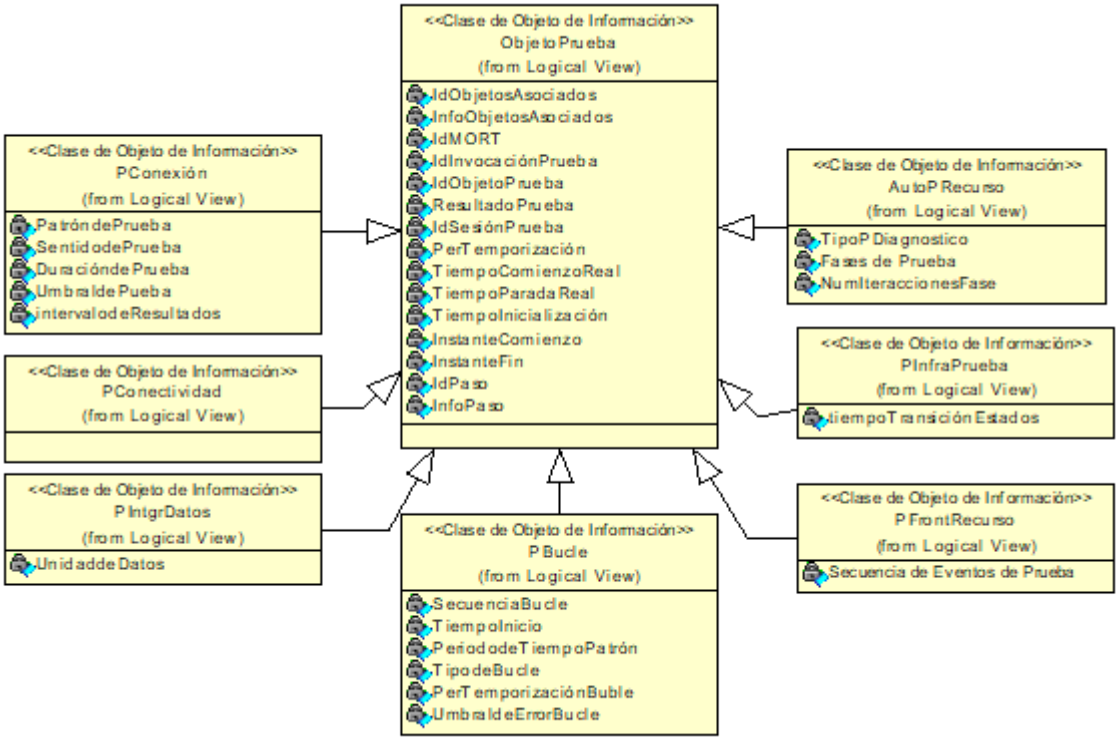
Tabla 21. Atributos Ejecutante de Acción de Prueba

Nombre de Atributo	Calificador	Definición	Valores Legales
ClasesTOSustentadas	C	Atributo usado para identificar las clases de Objetos de Prueba sustentados por un Ejecutante de Acción de Prueba. ITU-T X.745 supportedTOClassesPackage.	Lista

		supportedTOClasses [19]	
IdEjecutanteAcción dePrueba	C	Utilizado para identificar un sistema ejecutante de una acción de prueba. ITU-T X.745 testActionPerformerPackage testActionPerformerId [19]	Entero

ObjetoPrueba

Figura 31. Diagrama de herencia de Objeto Prueba.



- **Definición:** ObjetoPrueba contiene información perteneciente a una prueba controlada, como las condiciones en las cuales se ejecutará, suspenderá, reanudará y terminará. Su existencia se debe a una sola petición de prueba hecha por el gestor GestorIRP(en este caso la OSF-MAF que cumple el papel de gestor en la capa de gestión de Red de TMN) hacia la Entidad Monitoreada la cual es gestionada por ejecutante de acción de prueba que desempeña el papel de AgenteIRP (representado en la arquitectura funcional por los OSF-MAF agentes, de cada OSF planteado en la capa de gestión de elementos de red) y tiene la función de recibir las peticiones y responder a las mismas. El AgenteIRP asigna el Identificador de invocación de Prueba que identifica la invocación de la prueba. ITU-T X.745 Objetos testObject [19]. (Ver figura 31).

  Los Objetos de Prueba se pueden clasificar para definir pruebas más específicas de acuerdo a

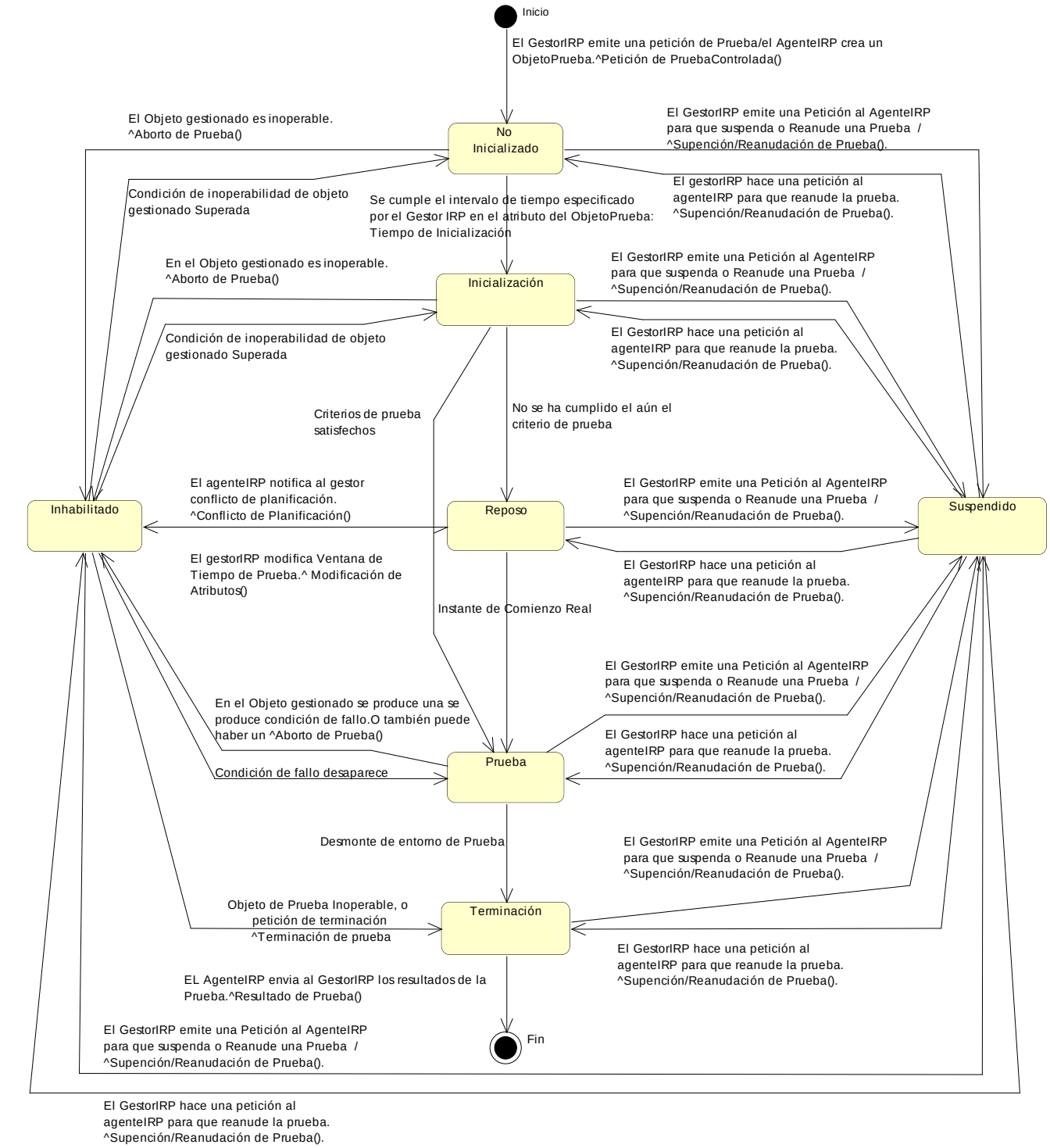
su especialización, a continuación se definen cada una de las Categorías de Prueba que se obtienen (herendan) de la Clase Objeto de Información ObjetoPrueba (Ver figura 31).

- PConexión: este tipo de Prueba permite conocer las condiciones del trayecto de comunicaciones real o virtual para soportar un servicio. En esta se definen dos objetos Asociados que representan los recursos en los extremos del trayecto de telecomunicaciones. [18]
- PConectividad: se utiliza para verificar que puede establecerse conectividad entre dos entidades (ObjetoGestionado-Objeto Asociado) en un plazo especificado. [18]
- PIntrDatos: permite comprobar si dos entidades pueden intercambiar datos sin degradación alguna y mide el tiempo que dura la degradación de datos. [18]
- PBucle: esta prueba permite verificar que los datos pueden ser enviados y recibidos por un trayecto de comunicaciones en un periodo de temporizaron de bucle especificado, con una tasa de error aceptable. [18]
- AutoPRecurso: permiten comprobar la aptitud de un recurso para realizar la función que se le ha adjudicado en un momento dado. [18]
- PInfraPrueba: se utiliza para verificar aspectos de implementación de una Prueba, que permiten iniciar pruebas, devolver resultados y responder a acciones de supervisión y control. [18]
- PFrontRecurso: esta especialidad de ObjetoPrueba se utiliza para verificar el correcto comportamiento de los diversos recursos internos al sistema, Esto se realiza insertando señales de prueba en puntos de control y observación, que permitan determinar si las señales generadas por el recurso son conformes a la especificación del comportamiento del Recurso. [18]

- ***Diagramas de Estados***

  Las pruebas tienen estados. La información de estado de una prueba es capturada en cada una de las categorías de Objeto de Prueba, representado como el atributo de EstadoPrueba. EL icono del circulo negro relleno representa el estado de inicial. El doble círculo representa el estado final de la prueba (Ver figura 32).

Figura 32. Diagrama de estados Objeto Prueba.



- **Atributos:**
  - Objeto Prueba

Tabla 22. Atributos Objeto Prueba

Nombre de Atributo	Calificador	Definición	Valores Legales
IdObjetosAsociados	M	Identifica el objeto u objetos gestionados (entidades monitoreadas) que representan otros recursos que intervienen en la prueba. ITU-T X.745 associatedObjectsPackage. associatedObjects [19]	Entero
InfoObjetosAsociados	M	Información adicional de los Objetos Asociados. ITU-T X.745 associatedObjectsPackage [19]	String
IdMORTS	M	Identifica Objeto gestionado referenciador de una prueba (MORT, Managed Object Referring to Test), es decir el objeto u objetos gestionados (entidades monitoreadas) que identifican el recurso que se prueba o se probará. Parámetro obligatorio. ITU-T X.745 mORTsPackage .mORTS [19]	Entero
IdInvocaciónPrueba	M	Identificador único de una prueba devuelto en respuesta al petición de prueba, obligatorio para todos los objetos de Prueba. ITU-T X.745 testInvocationIdPackage. testInvocationId [19]	Entero
EstadodePrueba	M	Este atributo refleja el estado actual de la Prueba 3GPP 32.322-610 TesterObject.testState [27]	Enum: No Inicializado, Inicializada, Inhabilitado, Reposo, Suspendido, Prueba, Terminación
IdObjetoPrueba	M	Identifica de manera única un Objeto de Prueba. Puede ser asignado por el GestorIRP o AgenteIRP. ITU-T X.745 testObjectPackage.testObjectId [19]	Entero
ResultadoPrueba	M	Proporciona una visión normalizada del resultado de la prueba. ITU-T X.745 testOutcomePackage.testOutcome [19]	Enum: • Éxito •Fracaso •No concluyente •Temporizada •Terminación Prematura

IdSesiónPrueba	O	Identifica una sesión de prueba (conjunto de invocaciones de prueba). Asignado por el GestorIRP y proporcionado en la petición de prueba. ITU-T X.745 testSessionPackage.testSessionId [19]	Entero+identificador de objeto
PerTemporización	M	Define la cantidad máxima de tiempo que puede durar una prueba. ITU-T X.745 timeoutPeriod	Date
TiempoComienzoReal	M	Indica la hora de comienzo real de la prueba es asignado por el AgenteIRP. Junto con TiempoParadaReal indican el tiempo que durará la prueba. ITU-T X.745 actualTestTimePackage. actualStartTime [19]	Date Tiempo absoluto
TiempoParadaReal	M	Indica la hora de parada real de la prueba es asignado por el AgenteIRP. ITU-T X.745 actualTestTimePackage.actualStopTime [19]	Date: Tiempo absoluto
TiempoInicialización	M	Indica el instante en el que el objeto de prueba pasa al estado de inicilización. Puede ser absoluto o relativo con respecto al instante en el que el objeto de prueba pasará al estado de prueba. ITU-T X.745 initializingTimePackage. initializingTime [19]	Date
InstanteComienzo	M	Junto con Instante de fin permite a un gestorIRP controlar la ventana de tiempo dentro de la cual un Objeto de Prueba ejecutará la prueba. ITU-T X.745 requestedWindowPackage [19]	Date Por defecto: NULL
InstanteFin	M	Permite a un gestorIRP controlar la ventana de tiempo dentro de la cual un Objeto de Prueba ejecutará la prueba. ITU-T X.745 requestedWindowPackage. endTime [19]	Date Por defecto: NULL
IdPaso	M	Identifica un paso de prueba dentro de uno de los estados de prueba. ITU-T X.745. testStepsPackage.testStep [19]	Entero
InfoPaso	M	Información de paso calificadora relativa a ese paso. ITU-T X.745 testStepsPackage. testStepQualifier [19]	String

- **Atributos Adicionales**
  - PConexión

Tabla 23. Atributos adicionales PConexión

Nombre de Atributo	Calificador	Definición	Valores Legales
PatróndePrueba	C	Ejercicio o serie de ejercicios aplicados al trayecto, acordado por los Objetos Asociados que participan en la prueba. Si este no esta presente patrón de prueba será especifico a la implementación. ITU-T X.737 connectionTestObject.testPatterns [18]	Lista
SentidodePrueba	C	Este atributo es utilizado, cuando el trayecto gestionado soporta dos sentidos, entonces los ejercicios de la prueba se realizan por separado en cada sentido de la comunicación. ITU-T X.737 Prueba de conexión.El sentido de la prueba aplicada al MORT[18]	Enum
DuracióndePrueba	C	Tiempo de duración de la prueba. ITU-T X.737 Prueba de conexión. La duración de la prueba aplicada a la prueba [18]	Date
UmbraldePrueba	C	Debe utilizarse para determinar el resultado de la prueba. Especifica el umbral de error. Al cruzarse el umbral, se terminará la prueba asociada y el resultado de la prueba será fracaso. ITU-T X.737 Prueba de conexión. El umbral de prueba que debe utilizarse para determinar el resultado de prueba [18]	Date

  - PConectividad: no tiene atributos adicionales a los heredados por el ObjetoPrueba.
  - PIntrDatos

Tabla 24. Atributos adicionales PIntrDatos

Nombre de Atributo	Calificador	Definición	Valores Legales
UnidaddeDatos	C	Este atributo se utiliza para especificar el tipo y la cantidad de las unidades de datos que hay que enviar durante la prueba. Este atributo sólo se usa si la prueba soporta la especificación por el gestor del tipo y/o la cantidad de unidades de datos. ITU-T X.737 dataIntegrityTestObject.dataUnits [18]	String

  - PBucle

Tabla 25. Atributos adicionales PBucle

Nombre de Atributo	Calificador	Definición	Valores Legales
Secuencia Bucle	C	Contiene los datos de bucle que van a utilizarse durante la prueba, incluyen el tráfico de prueba para una prueba de	Lista

		bucle. ITU-T X.737 loopbackTestObject.testPatterns [18]	
Periodo de Tiempo Patrón	C	Cantidad de tiempo durante el cual cada patrón de prueba es transmitido. ITU-T X.737 loopbackTestObject.timeoutPeriod [18]	Date segundos reales bits/octetos en forma de lotes/bloques
TipodeBucle	C	Identifica el tipo de bucle. ITU-T X.737 loopbackTestObject.loopbackType [18]	Enum: Físico, Eco, Analógico, Digital
PerTemporiza-ción Bucle	C	Tiempo en el que debe completarse la totalidad de la prueba. ITU-T X.737 loopbackTestObject. loopbackTimeoutPkg [18]	Date= # de Patrones*Periodo de Tiempo del Patrón+Tiempo de Retardo de Transmisión de Bucle
UmbraldeError Bucle	C	Especifica el tiempo que un ejecutante de prueba esperará para que vuelvan los datos transmitidos. Se mide entre la transmisión del patrón de prueba y la recepción de los datos devueltos por el circuito de bucle. Si el retardo de transmisión de bucle es mayor que el valor especificado, se obtendrá un fallo intermedio de toda la prueba y se devolverá un resultado fracaso. ITU-T X.737 loopbackTestObject. loopbackThreshold [18]	Date

- AutoPRecurso

Tabla 26. Atributos adicionales AutoPRecurso

Nombre de Atributo	Calificador	Definición	Valores Legales
TipoPDiagnostico	C	Tipo de Prueba de Diagnostico a Realizar. Si el tipo de diagnostico no esta incluido en la petición de prueba, el tipo de diagnostico es especifico y conocido por el MORT. ITU-T X.737 Auto Prueba de Recurso. El tipo de prueba de diagnóstico a realizar. [18]	String
FasesdePrueba	C	Usado para especificar los ejercicios específicos que se llevarán a cabo del sistema continente. ITU-T X.737 Auto Prueba de Recurso.Fases de la Prueba a realizar [18]	Lista
NumIteraciones Fase	C	Numero de veces que se realizará un ejercicio específico de forma insistente. ITU-T X.737 Auto Prueba de Recurso.Número de iteraciones para cada fase [18]	Entero

- PInfraPrueba

Tabla 27. Atributos adicionales PInfraPrueba

Nombre de Atributo	Calificador	Definición	Valores Legales
TiempoTransición Estados	C	Intervalo de tiempo necesario entre transiciones de estados de prueba. ITU-T X.737 testInfrastructureTestObject. stateTransitionTimeIntervalPkg [18]	Date

- PFrontRecurso

Tabla 28. Atributos adicionales PFronteraRecurso

Nombre de Atributo	Calificador	Definición	Valores Legales
SecuenciaEventos Prueba	C	Este atributo especifica una secuencia de señales que han de insertarse o recibirse en el Objeto Gestionado y en el Objeto Asociado especificados. ITU-T X.737 resourceBoundaryTestObject. sequenceOfEvents [18]	Lista

Eventos de Prueba

- **Definición:** Esta clase de objeto de información solo existe cuando el objeto de Prueba es creado a partir de una petición de prueba catalogada como una prueba de Frontera de Recurso. En esta se especifica la información de los eventos que conforman la Secuencia de eventos utilizada en la clase ObjetoPrueba.PFrontRecurso (Ver figura 29).
- **Atributos:**

Tabla 29. Atributos Eventos de Prueba

Nombre de Atributo	Calificador	Definición	Valores Legales
IdEvento	C	Identificador del evento. ITU-T X.737 resourceBoundaryTestObject. sequenceOfEvents.eventId [18]	Entero
SeñaldePrueba	C	Identifica un tipo de señal particular que ha de insertarse o recibirse. ITU-T X.737 ResourceBoundaryTestObject. sequenceOfEvents.signalType [18]	String
Parámetrosy ValordeSeñal	O	Especifica los valores y parámetros de la señal que es insertada o recibida del recurso sometido a prueba. ITU-T X.737 resourceBoundaryTestObject. sequenceOfEvents.signalValue [18]	Enum
SentidoSeñal	O	Atributo que especifica si la señal es insertada al recurso sometido a prueba o si es recibida es decir generada por el recurso a prueba. ITU-T X.737 resourceBoundaryTestObject.	Enum: • Insertada • recibida

		sequenceOfEvents.signalDirection [18]	
IdMORT	C	Identificador del objeto gestionado en el cual ha de insertarse o recibirse determinada señal. ITU-T X.737 resourceBoundaryTestObject. sequenceOfEvents.mORTs [18]	Entero
IdAO	C	Identificador del o los objetos asociados que actúan como Puntos de control y observación, en los cuales ha de insertarse y observarse determinada señal. ITU-T X.737 resourceBoundaryTestObject. sequenceOfEvents.associatedObjects [18]	Entero
Temporizador de Espera	C	Si la señal es recibida: tiempo que se espera la señal, Si señal es insertada: tiempo que se espera antes de que se inserte la señal después de finalizar el evento anterior. ITU-T X.737 resourceBoundaryTestObject. sequenceOfEvents.waitDuration [18]	Date

RegResultadoPrueba

- **Definición:** esta clase de objeto de información se crea para informar al gestor de las Pruebas, los resultados de esta, y se crea como una notificación del Ejecutante de la Prueba cuando se da por terminada la Prueba. La información que contiene este registro depende del tipo de prueba que se requiera. Hereda del Registro de Fichero Registro Cronológico RFRC. ITU-T X.745 Objetos. testResultsRecord [19]. (Ver figura 29).

RegConflictoPlanificación

- **Definición:** esta clase de objeto de información se crea para informar al gestor de pruebas, de la presencia de un conflicto en la planificación de estas, y se crea como una notificación del Ejecutante de la Prueba cuando ha ocurrido un conflicto de este tipo. Hereda del Registro de Fichero Registro Cronológico RFRC. ITU-T X.745 Objetos schedulingConflictRecord [19]. (Ver figura 29).

FRC2

- **Definición:** esta clase de objeto de información hereda de Fichero de Registro Cronológico FRC, y se crea para almacenar los registros de conflicto de planificación generados por el ejecutante de prueba como notificación de un conflicto en la información de planificación de una prueba. Este fichero hace parte de la función de sistema de directorio (DSF), del OSF de la capa de gestión de red en la arquitectura funcional (Ver figura 29).

FRC3

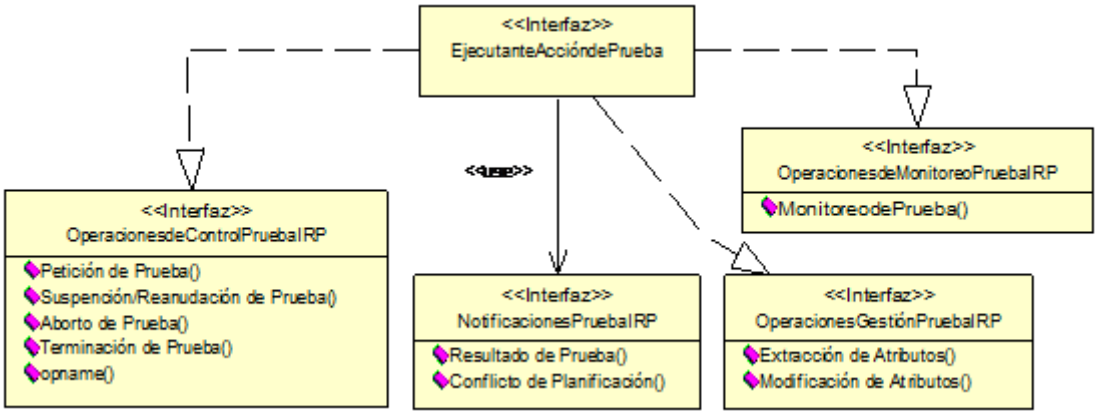
- **Definición:** esta clase de objeto de información hereda de Fichero de Registro Cronológico FRC, y se crea para almacenar los registros de resultado de prueba generados por el ejecutante de prueba cuando esta se concluye. Este fichero hace parte de la función de sistema de directorio (DSF), del OSF de la capa de gestión de red en la arquitectura funcional (Ver figura 29).

DiscriminadorEnvioEventos1

- **Definición:** esta clase de objeto de información hereda de la clase DiscriminadorEnvioEventos, y se implementa para garantizar el filtraje de eventos desde la entidad monitoreada hacia el proceso de gestión de Pruebas. En la Arquitectura funcional esta clase de objeto de información se encuentra representada por las funciones de mediación existentes entre las funciones de elemento de Red (capa de Elemento de Red) y los OSFs pertenecientes a la capa de gestión de Elemento de Red (Ver figura 29).

4.2.6.2 Definición de interfaces

Figura 33. Diagrama de Interfaces de Punto de referencia de pruebas.



Para la definición y explicación de las interfaces utilizadas en este cometido de pruebas es necesario definir primero los siguientes parámetros:

Tabla 30. Parámetros generales de las interfaces del cometido de pruebas

Nombre de parámetro	Información correspondiente
IdInvocación	Especifica el identificador asignado a la operación. Puede utilizarse para distinguir esta operación de otras notificaciones u operaciones ***Equivalente CMIP:*** *CMISE servicio M-ACCIÓN ITU-T X.710* [14]
Modo	Especifica el modo solicitado para la operación. Confirmado o no confirmado. ***Equivalente CMIP:*** *CMISE servicio M- ACCIÓN ITU-T X.710 [14]*
ClaseObjetoBase	Especifica la clase del objeto gestionado que ha de utilizarse como punto de partida para la selección de los objetos gestionados a los cuales ha de aplicarse el filtro (cuando se suministre). ***Equivalente CMIP:*** *CMISE servicio M- ACCIÓN ITU-T X.710 [14]*
CasoObjetoBase	Especifica la manifestación o instancia del objeto gestionado que ha de utilizarse como punto de partida para la selección de los objetos gestionados a los cuales ha de aplicarse el filtro (cuando se suministre). ***Equivalente CMIP:*** *CMISE servicio M- ACCIÓN ITU-T X.710 [14]*

Alcance	Indica el subárbol, enraizado en el objeto gestionado de base, en que ha de buscarse. ***Equivalente CMIP:*** *CMISE servicio M- ACCIÓN ITU-T X.710 [14]*
Filtro	Especifica el conjunto de aserciones que define la prueba de filtro que ha de aplicarse al objeto (u objetos) gestionados delimitados. ***Equivalente CMIP:*** *CMISE servicio M- ACCIÓN ITU-T X.710 [14]*
ControlAcceso	Contiene información de control de acceso con miras a la obtención del permiso de realizar la acción en el objeto o los objetos gestionados especificados. ***Equivalente CMIP:*** *CMISE servicio M- ACCIÓN ITU-T X.710 [14]*
Sincronización	Indica cómo desea el usuario invocador del servicio que se sincronicen las operaciones de a través de las manifestaciones del objeto seleccionado. Puede ser: atómica, la mejor posible. ***Equivalente CMIP:*** *CMISE servicio M- ACCIÓN ITU-T X.710 [14]*
TipoPeticiónPrueba	Identifica que la petición pertenece a una sola prueba compuesta de TO relacionados (una prueba relacionada) o a múltiples pruebas, cada una de las cuales comprende un solo TO (pruebas independientes). ***Equivalente CMIP:*** *CMISE servicio M- ACCIÓN ITU-T X.710 [14]*
IdEnlazado	Si han de enviarse múltiples respuestas para esta operación, este parámetro especifica la identificación que es proporcionada por el usuario realizador del servicio cuando se devuelven estas respuestas. ***Equivalente CMIP:*** *CMISE servicio M- ACCIÓN ITU-T X.710 [14]*
IdInvocaciónNotifi	Especifica el identificador asignado a la notificación. Puede utilizarse para distinguir esta notificación de otras notificaciones u operaciones que el proveedor del servicio CMISE tenga en curso. ***Equivalente CMIP:*** *CMISE servicio M-INFORME-EVENTO ITU-T X.710* [14]
TipoEvento	Especifica el tipo de evento del que se informa. Puede incluirse en la confirmación de éxito, y se incluirá si se incluye el parámetro respuesta al evento. ***Equivalente CMIP:*** *CMISE servicio M-INFORME-EVENTO ITU-T X.710* [14]
TiempoEvento	Contiene la hora de generación del evento. ***Equivalente CMIP:*** *CMISE servicio M-INFORME-EVENTO ITU-T X.710* [14]
InfEvento	Contiene la respuesta al informe de evento. Puede incluirse en la confirmación de éxito. ***Equivalente CMIP:*** *CMISE servicio M-INFORME-EVENTO ITU-T X.710* [14]
ResdeEvento	Contiene la respuesta al informe de evento. Puede incluirse en la confirmación de éxito. ***Equivalente CMIP:*** *CMISE servicio M-INFORME-EVENTO ITU-T X.710* [14]
Errores	Este parámetro contiene la notificación de errores para la operación. Se incluirá en la confirmación de fracaso. Pueden producirse los errores siguientes: duplicación de invocación, valor de argumento no válido, argumento mal tipificado, no hay tal argumento es decir la información especificada no estaba reconocida, no hay tal tipo de evento, no hay tal clase de objeto, no hay tal manifestación de objeto, fallo de procesamiento de la notificación, no se procesó la notificación por limitación de recursos, operación no reconocida. ***Equivalente CMIP:*** *CMISE servicio M-INFORME-EVENTO ITU-T X.710* [14]

Interfaz OperacionesGestiónPruebaIRP

- **Extracción de Atributos**
  Definición: se puede utilizar para extraer cualquiera de los atributos legibles de un TO. CCITT | ISO/CEI 10164-1 X.730 PT-OBTENCIÓN [34]. (Ver figura 33).
- **Modificación de Atributos**
  Definición: se puede utilizar para fijar cualquiera de los atributos que pueden fijarse de un TO. CCITT | ISO/CEI 10164-1 X.730 PT-FIJACIÓN [34]. (Ver figura 33).

- **Aborto de Prueba**
  Definición: se puede utilizar para que un sistema abierto pueda abortar una prueba controlada. Cuando está disponible, se recomienda que el parámetro alcance incluya todos los ObjetoPrueba identificador de invocación de prueba y que el parámetro filtro seleccione los ObjetoPrueba identificador de invocación de prueba CCITT | ISO/CEI 10164-1 X.730 PT-SUPRESION [34]. (Ver figura 33).

Interfaz OperacionesdeControlPruebaIRP

- **Petición de Prueba**
  Definición: el servicio de petición de prueba controlada permite a un gestor (GestorIRP) pedir que otro sistema abierto (agenteIRP) inicie una prueba controlada.
  Este tipo de servicio comprende varias categorías, debido a las diferentes especializaciones existentes del Objeto Prueba. CCITT | ISO/CEI 9595 X.710 M-ACCIÓN. ITU-T X.745 acciones testRequestControlledAction [19]. (Ver figura 33).

  Parámetros de Entrada:

Tabla 31. Parámetros de Entrada Petición de Prueba

Nombre de parámetro	Calificador	Información correspondiente
Identificador de invocación	M	M-ACCIÓN parámetro IdInvocación
Modo	M	M-ACCIÓN parámetro Modo
Clase objeto de base	M	M-ACCIÓN parámetro ClaseObjetoBase
Caso de objeto de base	M	M-ACCIÓN parámetro CasoObjetoBase
Alcance	M	M-ACCIÓN parámetro Alcance
Filtro	M	M-ACCIÓN parámetro Filtro
Control de acceso	M	M-ACCIÓN parámetro ControlAcceso
Sincronización	M	M-ACCIÓN parámetro Sincronización
Tipo de petición de prueba controlada	M	M-ACCIÓN parámetro TipoPeticiónPrueba
Información de petición de prueba controlada: ITU-T X.745 TestRequestControlledInfo		

– Información de categoría de prueba	M	Este parámetro facultativo indica la información específica de prueba asociada con una petición de prueba. ITU-T X.745 TestRequestControlledInfo.testCategoryInformation [19]
– Tipo de petición de prueba controlada	M	Este parámetro identifica que la petición pertenece a una sola prueba compuesta de TO relacionados (una prueba relacionada) o a múltiples pruebas, cada una de las cuales comprende un solo TO (pruebas independientes). ITU-T X.745 TestRequestControlledInfo.controlledTestRequestType [19]
– Identificador de sesión de prueba	M	ObjetoPrueba.IdSesiónPrueba
– MORT que han de probarse	M	ObjetoPrueba.IdMORTS
– Objetos asociados	M	ObjetoPrueba.IdObjetosAsociados
– Periodo de temporización	M	ObjetoPrueba.PerTemporización
– Lista de objetos de prueba	M	El parámetro lista de objetos de prueba, cuando está presente, específica los TO que han de crearse como resultado de una petición de prueba controlada. ITU-T X.745 TestRequestControlledInfo.testObjectList [19]
• Clase de TO	M	Nombre de la Categoría de prueba a la que pertenecen el o los Objetos de Prueba. ITU-T X.745 TestRequestControlledInfo.TestObjectList.tOClass [19]
• Lista de atributos iniciales	M	Contendrá los valores iniciales de sólo aquellos atributos especificados que han de ser devueltos por el comportamiento del TO. ITU-T X.745 TestRequestControlledInfo.TestObjectList. initialAttributeList [19]

Parámetros de entada adicionales.

- **Prueba de conexión.**

Tabla 32. Parámetros de entrada Prueba de conexión

Nombre de parámetro	Calificador	Información correspondiente
Patrón de Prueba	C	ObjetoPrueba.PConexión.PatróndePrueba
Sentido de Prueba	C	ObjetoPrueba.PConexión.SentidodePrueba
Duración de Prueba	C	ObjetoPrueba.PConexión.DuracióndePrueba
Umbral de Prueba	C	ObjetoPrueba.PConexión.UmbraldePrueba

- **Prueba de conectividad.**

  No hay parámetros adicionales a los utilizados en la petición de Prueba General.

- **Prueba de integridad de datos**

Tabla 33. Parámetros de entrada Prueba de integridad de datos

Nombre de parámetro	Calificador	Información correspondiente
Unidad de Datos	C	ObjetoPrueba.PIntrDatos.UnidaddeDatos

- **Prueba de bucle**

Tabla 34. Parámetros de entrada Prueba de bulce

Nombre de parámetro	Calificador	Información correspondiente
Secuencia de Bucle	C	ObjetoPrueba.PBucle.SecuenciadeBucle
TiempoInicio	C	ObjetoPrueba.PBucle.TiempoInicio
Periodo de Tiempo de Patrón	C	ObjetoPrueba.PBucle.PeriododeTiempoPatrón
Tipo de Bucle	C	ObjetoPrueba.PBucle.TipodeBucle
PerTemporizaciónBucle	C	ObjetoPrueba.PBucle.PerTemporizaciónBucle
Umbral de Error del Bucle	C	ObjetoPrueba.PBucle.UmbraldeErrorBucle

- **Autoprueba de recurso**

Tabla 35. Parámetros de entrada Autoprueba de recursos

Nombre de parámetro	Calificador	Información correspondiente
TipoPDiagnostico	C	ObjetoPrueba.AutoPRecurso.TipoPDiagnostico
Fases de Prueba	C	ObjetoPrueba.AutoPRecurso.FasesdePrueba
NumIteraciones Fase	C	ObjetoPrueba.AutoPRecurso.NumIteracionesFase

- **Prueba de infraestructura de prueba**

Tabla 36. Parámetros de entrada Prueba de infraestructura de prueba

Nombre de parámetro	Calificador	Información correspondiente
Tiempo de transición de Estados	C	ObjetoPrueba.PInfraPrueba. TiempoTransiciónEstados

- **Prueba de frontera de Recurso**

Tabla 37. Parámetros de entrada Prueba de frontera de recursos

Nombre de parámetro	Calificador	Información correspondiente
Secuencia de Eventos de Prueba	C	ObjetoPrueba.PFrontRecurso. SecuenciaEventosPrueba

Parámetros de Salida:

Tabla 38. Parámetros de salida Prueba de frontera de recursos

Nombre de parámetro	Calificador	Información correspondiente
Identificador de invocación	M	M-ACCIÓN parámetro IdInvocación
Identificador enlazado	M	M-ACCIÓN parámetro IdEnlazado
Clase objeto gestionado	M	M-ACCIÓN parámetro ClaseObjetoBase
Caso de objeto gestionado	M	M-ACCIÓN parámetro CasoObjetoBase
Tipo de petición de prueba controlada	C	Identifica que la petición pertenece a una sola prueba compuesta de TO relacionados (una prueba relacionada) o a múltiples pruebas, cada una de las cuales comprende un solo TO (pruebas independientes). ITU.T X.745 TestRequestControlledInfo. ControlledTestRequestType [19]
Respuesta a petición de prueba controlada	C	Estará presente en una respuesta positiva; en los demás casos estará presente el parámetro errores. ITU.T X.745 TestRequestControlledInfo. TestRequestControlledResponse. [19]
- Respuesta de prueba independiente	C	Indica que todos los TO de la petición de prueba han sido ejemplificados y que el parámetro tipo de petición de prueba controlada se especificó como independiente. El parámetro devuelve información sobre los TO que han sido ejemplificados satisfactoriamente, incluidos sus identificadores de invocación de prueba y, si es especificado por el comportamiento del TO, los valores de los atributos de TO. ITU.T X.745 TestRequestControlledInfo. TestRequestControlledResponse. IndependentTestResponse. [19]
• Identificador de invocación de prueba	M	ObjetoPrueba.IdInvocaciónPrueba
• Lista de atributos de TO	C	Lista de atributos de los TO ejemplificados. ITU.T X.745 TestRequestControlledInfo. TestRequestControlledResponse. IndependentTestResponse.tOAttributeList [19]
- Respuesta de prueba relacionada	C	Indica que todos los TO especificados en la petición de prueba han sido ejemplificados. Este parámetro se utiliza si el parámetro de tipo de petición de prueba controlada se especificó como relacionado. El parámetro devuelve el identificador de invocación de prueba para la prueba, los nombres de los TO que han sido ejemplificados y, si es especificado por el comportamiento del TO, los valores de atributos de TO. La información sobre los TO está en el mismo orden que en la petición de prueba. ITU.T X.745 TestRequestControlledInfo. TestRequestControlledResponse.relatedTestResponse [19]

• Identificador de invocación de prueba	M	ObjetoPrueba.IdInvocaciónPrueba
• Lista de respuesta de objeto de prueba	M	Transporta los nombres de los TO creados como resultado de una petición de prueba controlada. La información de TO estará en la misma secuencia dada en la petición de prueba para que el ejecutante de la prueba pueda correlacionar la petición y la respuesta. ITU.T X.745 TestRequestControlledInfo. TestRequestControlledResponse.RelatedTestResponse. testObjectResponseList. [19]
– Atributo de TO	C	Información de inicialización de atributo de TO. ITU.T X.745 Servicio de petición de prueba controlada. Parámetros de petición de prueba controlada. Atributo de TO [19]
Errores	C	Contiene la notificación de errores para la operación. Se incluirá en la confirmación de fracaso. Pueden producirse los siguientes errores: acceso denegado, conflicto de manifestación de clase, limitación por complejidad, duplicación de invocación, valor de argumento no válido, filtro no válido, delimitación no válida, argumento mal tipificado, no hay tal acción: el tipo de acción especificado no estaba admitido, no hay tal clase de objeto, no hay tal manifestación de objeto, fallo de procesamiento, limitación de recursos, sincronización no soportada, operación no reconocida. ITU.T X.745 controlledTestRequestPackage. independentTestInvocationError, ITU.T X.745 controlledTestRequestPackage.relatedTOError; [19]

Pre-Condición

- Se necesita al menos un IdMORT (identificadores de los objetos gestionados, en este caso el trayecto de comunicaciones a probar) y se necesita también colocar este en el estado apropiado (por ejemplo reservado para pruebas). De lo contrario la prueba de conexión abortará
- Es necesario definir dos Objetos Asociados (que representan los recursos en los extremos del trayecto de comunicaciones que impulsan y reciben señales a este) y colocarlos en el estado apropiado. De lo contrario la prueba de conexión abortará

- **Suspensión/Reanudación de Prueba**

  Definición: el servicio de suspensión/reanudación de prueba permite a un gestor (GestorIRP) pedir que otro sistema abierto (AgenteIRP) suspenda o reanude una prueba o sesión de pruebas. Parámetros de Entrada generales de todas las categorías de Prueba. CCITT | ISO/CEI 9595 X.710 M-ACCIÓN. ITU-T X.745 acciones testSuspendResumeAction [19]. (Ver figura 33).

Parámetros de Entrada

Tabla 39. Parámetros de entrada Suspensión/Reanudación de Prueba

Nombre de parámetro	Calificador	Información correspondiente
Identificador de invocación	M	M-ACCIÓN parámetro IdInvocación
Modo	M	M-ACCIÓN parámetro Modo
Clase de objeto de base	M	M-ACCIÓN parámetro ClaseObjetoBase
Caso de objeto de base	M	M-ACCIÓN parámetro CasoObjetoBase
Alcance	M	M-ACCIÓN parámetro Alcance
Filtro	M	M-ACCIÓN parámetro Filtro
Control de acceso	M	M-ACCIÓN parámetro ControlAcceso
Sincronización	M	M-ACCIÓN parámetro Sincronización
Tipo de suspensión/ reanudación de prueba	M	Específica una acción particular que ha de realizarse puede ser suspensión o reanudación. ITU-T X. Servicio de suspensión/reanudación de prueba. Parámetros de suspensión/reanudación de prueba. Tipo de suspensión/reanudación de prueba
Información de suspensión/ reanudación de prueba	M	Especifica información suplementaria sobre el servicio de suspensión/reanudación. . ITU-T X.745 testSuspendResumeAction.TestSuspendResumeInfo [19]
− Pruebas indicadas	M	Indica las pruebas que son el objeto de una petición de control, por medio de identificador de sesión de prueba o en un conjunto de identificadores de invocación de prueba. ITU-T X.745 testSuspendResumeAction. TestSuspendResumeInfo.indicatedTests [19].
− Elección de suspensión/ reanudación	M	Este parámetro indica si ha de suspenderse o reanudarse la prueba o pruebas indicadas. ITU-T X.745 TestSuspendResumeInfo. SuspendResumeChoice [19]

Parámetros de Salida

Tabla 40. Parámetros de salida Suspensión/Reanudación de Prueba

Nombre de parámetro	Calificador	Información correspondiente
Identificador de invocación	M	M-ACCIÓN parámetro IdInvocación
Identificador enlazado	M	M-ACCIÓN parámetro IdEnlazado
Clase de objeto gestionado	M	M-ACCIÓN parámetro ClaseObjetoBase
Caso de objeto gestionado	M	M-ACCIÓN parámetro CasoObjetoBase

Tipo de suspensión/ reanudación de prueba	C(□)	Específica una acción particular que ha de realizarse puede ser suspensión o reanudación. ITU-T X.745 Servicio de suspensión/reanudación de prueba. Parámetros de suspensión/reanudación de prueba. Tipo de suspensión/reanudación de prueba [19]
Tiempo vigente	M	. Este parámetro contiene la hora a la que se generó la respuesta. ITU-T X.745 Servicio de suspensión/reanudación de prueba. Parámetros de suspensión/reanudación de prueba. Tiempo vigente. [19]
Resultado de suspensión/reanudación de prueba	C	Indica que el objeto gestionado con funcionalidad de Receptor de petición de acción de prueba pudo suspender o reanudar todas las pruebas solicitadas. ITU-T X.745 TestSuspendResumeResult [19]
− Identificador de invocación de prueba	M	ObjetoPrueba.IdInvocaciónPrueba
− Estado de objetos de prueba: ITU-T X.745 TestSuspendResumeElement.tOsStates		
• Caso de TO	C	Especifica la manifestación o instancia del objeto de Prueba. ITU-T X.745 TestSuspendResumeElement. tOsStates.tOInstance [19]
• Estado de prueba	M	Indica el estado de prueba de un TO afectado antes de la suspensión/reanudación de la prueba. ITU-T X.745 TestSuspendResumeElement.tOsStates.testState [19]
Errores	C	Indica que el objeto con funcionalidad Receptor de petición de acción de prueba no pudo suspender o reanudar una o más de las pruebas especificadas. ITU-T X.745 testSuspendResumeError [19]

- **Terminación de Prueba**

  Definición: el servicio de terminación de prueba permite a un gestor (el conductor de la prueba) pedir que otro sistema abierto (el sistema gestionado) termine una prueba o sesión de pruebas. CCITT | ISO/CEI 9595 X.710 M-ACCIÓN. ITU-T X.745 acciones testTerminateAction [19]. (Ver figura 33).

  Parámetros de Entrada

Tabla 41. Parámetros de entrada terminación de Prueba

Nombre de parámetro	Calificador	Información correspondiente
Identificador de invocación	M	M-ACCIÓN parámetro IdInvocación
Modo	M	M-ACCIÓN parámetro Modo
Clase de objeto de base	M	M-ACCIÓN parámetro ClaseObjetoBase
Caso de objeto de base	M	M-ACCIÓN parámetro CasoObjetoBase
Alcance	M	M-ACCIÓN parámetro Alcance
Filtro	M	M-ACCIÓN parámetro Filtro

Control de acceso	M	M-ACCIÓN parámetro ControlAcceso
Sincronización	M	M-ACCIÓN parámetro Sincronización
Tipo de terminación de prueba	M	Específica la terminación particular que ha de realizarse puede ser terminación .implícita o explícita. ITU-T X.745 Servicio de terminación de prueba. Parámetros de terminación de prueba. Tipo de terminación de prueba. Tiempo vigente. [19]
Información de terminación de prueba	M	Especifica información suplementaria sobre el servicio de terminación de prueba. ITU-T X.745 TestTerminateInfo [19]
− Pruebas indicadas	M	Indica las pruebas que son el objeto de una petición de control, por medio de identificador de sesión de prueba o en un conjunto de identificadores de invocación de prueba. ITU-T X.745 TestTerminateInfo IndicatedTests [19]

Parámetros de Salida

Tabla 42. Parámetros de salida terminación de Prueba

Nombre de parámetro	Calificador	Información correspondiente
Identificador de invocación	M	M-ACCIÓN parámetro IdInvocación
Identificador enlazado	M	M-ACCIÓN parámetro IdEnlazado
Clase de objeto gestionado	M	M-ACCIÓN parámetro ClaseObjetoBase
Caso de objeto gestionado	M	M-ACCIÓN parámetro CasoObjetoBase
Tipo de terminación de prueba	C(□)	Específica la terminación particular que ha de realizarse puede ser terminación .implícita o explícita. ITU-T X.745 Servicio de terminación de prueba. Parámetros de terminación de prueba. Tipo de terminación de prueba. Tiempo vigente. [19]
Tiempo vigente	M	Este parámetro contiene la hora a la que se generó la respuesta. ITU-T X.745 Servicio de terminación de prueba. Parámetros de terminación de prueba. Tipo de terminación de prueba. Tiempo vigente [19]
Resultado de terminación de prueba	C	Especifica el resultado de la petición de terminación de Prueba. ITU-T X.745 TestTerminateResult [19]
− Identificador de invocación de prueba	M	ObjetoPrueba.IdInvocaciónPrueba
Errores	C	Indica que el objeto gestionado con funcionalidad Receptor de petición de acción de prueba no pudo terminar una o más de las pruebas especificadas. Especifica el identificador de invocación de prueba de cada prueba que no se terminó, y los identificadores de invocación de prueba de las que se terminaron satisfactoriamente. ITU-T X.745 testTerminateError [19]

Pre-Condiciónes

- **Prueba de conexión**
  - Conclusión normal de la prueba
  - La prueba no puedo concluirse normalmente
  - Vencimiento del intervalo concedido para a conclusión de la prueba
  - Cuando se ha llevado a cabo una petición de terminación

- **Prueba de conectividad integridad de datos**
  - Recibo de confirmación del objeto asociado antes de que expire el periodo de temporización;
  - Vencimiento del periodo de temporización

- **Prueba de bucle**
  - Conclusión de la prueba;
  - Se ha excedido el umbral de error;
  - Se ha excedido el periodo de temporización de bucle;
  - Se ha excedido el periodo de temporización de prueba.

- **Prueba de frontera de recursos**
  - Recibo de una petición de terminación, enviada por el director de prueba.

- **Autoprueba de recurso**
  - Conclusión de la prueba;
  - La prueba no puede concluir normalmente;
  - Expiración del plazo concedido para la conclusión de la prueba

- **Prueba de infraestructura de prueba**
  - Conclusión del ejercicio;
  - Temporización;
  - El ejercicio no puede concluirse debido a la detección de un error.

OperacionesdeMonitoreoPruebaIRP

- **Monitoreo de Prueba**

  Definición: el GestorIRP será capaz de recuperar información sobre la prueba como es contemplada por los atributos del Objeto de Prueba asociado, durante la ejecución de esta. También después de la ejecución de la prueba el gestor será capaz de leer los atributos mientras el Objeto de Prueba exista. Los atributos que dan a conocer información sobre la ejecución de la prueba son estado de Prueba y Resultado de Prueba. Dependiendo de la categoría de prueba especificada otros atributos pueden también contener información sobre la ejecución de la prueba, en este caso se podrá permitir leer los valores de esos atributos también. 3GPP TS 32.322 interfaz testManagementIRPMonitorOperations.monitorTest [20].

Parámetros de Entrada:

Tabla 43. Parámetros de entrada Monitoreo de Prueba

Nombre del parámetro	Calificador	Información correspondiente
IdObjetoPrueba	M	ObjetoPrueba.IdObjetoPrueba
Atributos Monitoreados	M	Este parámetro especifica los identificadores de los atributos cuyos valores serán leídos. 3GPP TS 32.322 interfaz testManagementIRPMonitorOperations. monitorTest.toBeMonitoredAttributes [27]

Parámetros de Salida

Tabla 44. Parámetros de salida Monitoreo de Prueba

Nombre de parámetro	Calificador	Información correspondiente
Valores de Atributos Monitoreados	M	Este parámetro será retornado si todos los atributos fueron leídos exitosamente. Los valores a ser retornados son aquellos que prevalecen en el tiempo de recepción de la operación sujeta. 3GPP TS 32.322 interfaz testManagementIRPMonitorOperations.monitorTest. monitoredAttributeValues [27]
Error	M	Este parámetro será retornado si la instancia de objeto de prueba especificado no existe o en caso de que la instancia de objeto de prueba exista, al menos un atributo no pueda ser leído. 3GPP TS 32.322 interfaz testManagementIRPMonitorOperations.monitorTest.error

Pre-Condiciónes

La instancia del objeto de Prueba ha ser monitoreado, indicado por la operación sujeta, existe. Esta condición debe ser verdadera antes que la operación de monitoreo sea invocada.

NotificacionesPruebaIRP

Resultado de Prueba

Definición: el servicio de resultado de prueba permite a un sistema abierto (el sistema gestionado), informar los resultados de pruebas controladas. Los resultados de una prueba se hacen disponibles al GestorIRP por una o más notificaciones NotificacionesPruebaIRP emitidas por el Ejecutante de Acción de Prueba (AgenteIRP) que esta relacionado a la invocación de prueba. (Ver figura 33).

Dependiendo de la naturaleza de la prueba y de la especificación del comportamiento del TO relacionado, el Ejecutante de Acción de Prueba podrá necesitar conducir o transportar al GestorIRP un conjunto de datos de resultado. Esto se hace por medio del uso del parámetro Información Adicional de la notificación, en el cual se transfieren resultados de prueba que no son finales. En este tipo de notificaciones, el parámetro de resultado de prueba estará ausente.

El Ejecutante de Acción de Prueba deberá emitir al menos una notificación para la petición o invocación de Prueba. La última notificación relativa a una invocación de prueba en particular será indicada para incluir el parámetro resultado de prueba en la notificación. CCITT | ISO/CEI 9595 X.710. M-INFORME DE EVENTO ITU-T. X.745 Notificaciones schedulingConflictNotification testResultNotification.

Parámetros de Salida

Tabla 45. Parámetros de salida Resultado de Prueba

Nombre de parámetro	Calificador	Información correspondiente
Identificador de invocación	M	M-ACCIÓN parámetro IdInvocación
Modo	M	M-ACCIÓN parámetro Modo
Clase de objeto gestionado	M	M-ACCIÓN parámetro ClaseObjetoBase
Caso de objeto gestionado	M	M-ACCIÓN parámetro CasoObjetoBase
Tipo de resultado de prueba	C	*M-INFORME-EVENTO* parámetro TipoEvento
Tiempo de evento	M	*M-INFORME-EVENTO* parámetro TiempoEvento
Información de resultado de prueba	C	*M-INFORME-EVENTO* parámetro InfEvento
▪ Identificador de invocación de prueba	C	ObjetoPrueba.IdInvocaciónPrueba
▪ Identificador de sesión de prueba	C	ObjetoPrueba.IdSesiónPrueba
▪ Resultado de prueba	C	ObjetoPrueba.ResultadoPrueba
▪ MORT	C	ObjetoPrueba.IdMORTS
▪ Objetos asociados	C	ObjetoPrueba.IdObjetosAsociados
▪ Atributos supervisados	C	ObjetoPrueba.IdObjetoPrueba
▪ Acciones de reparación propuestas	C	Acciones de reparación suministradas por el usuario ITU-T X.733 alarmRecord.proposedRepairActions [15]
▪ Texto adicional	C	Información suministrada por el usuario como diagnostico de una falla o información adicional de una Prueba ITU-T X.733 alarmRecord.additionalText[15]
▪ Información adicional	C	Información suministrada por el usuario como diagnostico de una falla o información adicional de un resultado ITU-T X.733 alarmRecord.additionalInformation [15]
▪ Identificador de notificación	C	*M-INFORME-EVENTO* parámetro IdInvocaciónNotifi

▪ Notificaciones correlacionadas	C	Conjunto de identificadores de notificación que define un conjunto de todas las notificaciones con las cuales se considera que esta notificación está correlacionada. ITU-T X.733 alarmRecord.correlatedNotification [15]
Tiempo vigente	M	Este parámetro contiene la hora a la que se generó la respuesta.
Respuesta de evento	C	M-INFORME-EVENTO parámetro ResdeEvento
Errores	C	M-INFORME-EVENTO parámetro Errores

Parámetros de salida adicionales.

- **Prueba de Conexión.**

Tabla 46. Parámetros de salida adicionales Prueba de Conexión

Nombre de parámetro	Calificador	Información correspondiente
SeñaldePruebaRecibida	C	ITU-T X.737 Prueba de Conexión - Información de Resultados -parámetro Señal de prueba recibida [18]
TasadeErrores	C	ITU-T X.737 Prueba de Conexión - Información de Resultados -parámetro Tasa de errores detectada durante la prueba[18]
SentidodePrueba	C	ITU-T X.737 Prueba de Conexión - Información de Resultados -parámetro Sentido de la prueba[18]
TiempoDuraciónPrueba	C	ITU-T X.737 Prueba de Conexión - Información de Resultados -parámetro Tiempo de duración de la prueba [18]
InfoResultadosPrueba	C	ITU-T X.737 Prueba de Conexión - Información de Resultados -parámetro Info de resultados de prueba [18]
Diagnostico	C	ITU-T X.737 Prueba de Conexión - Información de Resultados -parámetro Diagnostico [18]

- **Prueba de conectividad.**

Tabla 47. Parámetros de salida adicionales Prueba de conectividad

Nombre de parámetro	Calificador	Información correspondiente
TiempoEstablecimiento	C	ITU-T X.737 Prueba de conectividad - Información de Resultados -parámetro Tiempo de Establecimiento [18]
TiempoConfirmación	C	ITU-T X.737 Prueba de conectividad - Información de Resultados -parámetro Tiempo entre petición y recibo de confirmación [18]
InformaciónAdicional	C	ITU-T X.737 Prueba de conectividad - Información de Resultados -parámetro Información adicional [18]

- **Prueba de integridad de datos**

Tabla 48. Parámetros de salida adicionales Prueba integridad de datos

Nombre de parámetro	Calificador	Información correspondiente
TiempoPruebaEfectivo	C	ITU-T X.737 Prueba de integridad de datos- Información de Resultados -parámetro Tiempo de prueba efectivo para el intercambio de datos [18]
TiempoConfirmación	C	ITU-T X.737 Prueba de integridad de datos- Información de Resultados- parámetro Tiempo entre petición y recibo de confirmación [18]
DatosCausantesde Fracaso	C	ITU-T X.737 Prueba de integridad de datos- Información de Resultados -Datos recibidos causantes de fracaso [18]
InformaciónAdicional	C	ITU-T X.737 Prueba de integridad de datos- Información de Resultados -Información adicional [18]

- **Prueba de bucle**

Tabla 49. Parámetros de salida adicionales Prueba de bucle

Nombre de parámetro	Calificador	Información correspondiente
DatosdeBucle	C	ITU-T X.737 Prueba de bucle - Información de Resultados - parámetro Datos devueltos por el bucle.[18]
ErrordeBucle	C	ITU-T X.737 Prueba de bucle - Información de Resultados - parámetro Error del bucle. [18]
Causa Fallo	C	ITU-T X.737 Prueba de bucle - Información de Resultados - parámetro Causa de Fallo. [18]
Información Adicional	C	ITU-T X.737 Prueba de bucle - Información de Resultados - parámetro Información adicional. [18]

- **Autoprueba de recurso**

Tabla 50. Parámetros de salida adicionales Autoprueba de recurso

Nombre de parámetro	Calificador	Información correspondiente
InfoEjercicios	C	ITU-T X.737 Autoprueba de recurso - Información de Resultados -parámetro Información especifica de prueba Ejercicios [18]
InfoAdicional	C	ITU-T X.737 Autoprueba de recurso - Información de Resultados -parámetro Información adicional [18]

- **Prueba de infraestructura de prueba**

Tabla 51. Parámetros de salida adicionales Prueba de infraestructura de prueba

Nombre de parámetro	Calificador	Información correspondiente
InfoPrueba	C	ITU-T X.737 Prueba de infraestructura de prueba - Información de Resultados -parámetro Información especifica de la Prueba [18]

- **Prueba de frontera de Recurso**

Tabla 52. Parámetros de salida adicionales Prueba de frontera de recurso

Nombre de parámetro	Calificador	Información correspondiente
TipoSeñalRecibida	C	ITU-T X.737 Prueba de frontera de Recurso - Información de Resultados -parámetro Tipo de la señal recibida [18]
TipoyValoresSeñal	C	ITU-T X.737 Prueba de frontera de Recurso - Información de Resultados -parámetro Valores y Tipo de Señal [18]
IdMORTSeñal	C	ITU-T X.737 Prueba de frontera de Recurso - Información de Resultados -parámetro IdMORT de los que se recibió la señal [18]
IdObjetosAsociados Señal	C	ITU-T X.737 Prueba de frontera de Recurso - Información de Resultados -parámetro Id Objetos Asociados donde se recibió la señal [18]
IdEventodePrueba Fallido	C	ITU-T X.737 Prueba de frontera de Recurso - Información de Resultados -parámetro Id evento de prueba fallido [18]

Eventos de Activación.

- **Prueba de Conexión.**
  - Conclusión del ejercicio (o ejercicios) de prueba efectuado en un solo sentido de comunicación;
  - Conclusión de la prueba;
  - Temporización;
  - Recibo de una petición de terminación.

- **Prueba de conectividad.**
  - Recibo de confirmación del objeto asociado antes de que expire el periodo de temporización;
  - Vencimiento del periodo de temporización.

- **Prueba de integridad de datos**
  - Recibo de confirmación del o de los objetos asociados antes de que expire el periodo de temporización;
  - Vencimiento del periodo de temporización.

- **Prueba de bucle**
  - Recepción de todos los datos enviados antes de que expire el tiempo de duración de la prueba;
  - Temporización del valor del periodo de temporización de bucle;
  - Temporización del periodo de temporización de prueba incluidos el tiempo de establecimiento y los periodos de temporización de bucle;
  - Intervalo de tiempo especificado para el informe;
  - Recepción de la petición de terminación, si se trata de una prueba controlada.

- **Autoprueba de recurso**
  - Cualquier punto durante el ejercicio de la función, normalmente al final de las fases apropiadas, si se definen;
  - Conclusión del ejercicio de la función.

- **Prueba de infraestructura de prueba**
  - Transición entre estados de prueba (si son proporcionados por la implementación);
  - Conclusión del ejercicio.
- **Prueba de frontera de Recurso**
  - Caso 1 – conclusión de la última señal en secuencia de eventos de prueba (si es indicado por el indicador de informe de resultados).
  - Caso 2 – recibo de una señal en un punto de control y observación (PCO, Point Of Control and Observation) mientras no hay activa ninguna secuencia de eventos y por tanto no ha de concordarse ninguna señal de recepción.
  - Caso 3 – recibo de una señal en un PCO mientras que ha de concordarse otra señal de recepción conforme a la lista de secuencia de eventos activos.
  - Caso 4 – expiró el temporizador de duración de espera en el caso de una señal de recepción.

Conflicto de Planificación

Definición: El servicio de conflicto de planificación permite a un sistema abierto (el sistema gestionado) informar un conflicto de planificación de pruebas. CCITT | ISO/CEI 9595 X.710 M-INFORME DE EVENTO. ITU-T X.745 Notificaciones schedulingConflictNotification. (Ver figura 33).

Parámetros de Salida

Tabla 53. Parámetros de salida Conflicto de planificación

Nombre de parámetro	Calificador	Información correspondiente
Identificador de invocador	M	M-ACCIÓN parámetro IdInvocación
Modo	M	M-ACCIÓN parámetro Modo
Clase de objeto gestionado	M	M-ACCIÓN parámetro claseObjetoBase
Caso de objeto gestionado	M	M-ACCIÓN parámetro CasoObjetoBase
Tipo de informe de conflicto de planificación	C	M-INFORME-EVENTO parámetro TipoEvento
Tiempo de evento	M	M-INFORME-EVENTO parámetro TiempoEvento
Información de conflicto de planificación	C	M-INFORME-EVENTO parámetro InfEvento
• Identificador de invocación de prueba	C	ObjetoPrueba.IdInvocaciónPrueba

• Identificador de sesión de prueba	C	ObjetoPrueba.IdSesiónPrueba
• Instante de comienzo	C	ObjetoPrueba.InstanteComienzo
• Instante de fin	C	ObjetoPrueba.InstanteFin
• Instante de comienzo real	C	ObjetoPrueba.TiempoComienzoReal
• Instante de parada real	C	ObjetoPrueba.TiempoParadaReal
• Texto adicional	C	ITU-T X.733 alarmRecord.additionalText [15]
• Información adicional	C	ITU-T X.733 alarmRecord.additionalInformation [15]
• Identificador de notificación	C	M-INFORME-EVENTO parámetro IdInvocaciónNotifi
• Notificaciones correlacionadas	C	ITU-TX.733 alarmRecord.correlatedNotification [15]
Tiempo vigente	M	Este parámetro contiene la hora a la que se generó la respuesta. ITU-T X.745 Servicio de conflicto de planificación. Parámetros de conflicto de planificación. Tiempo vigente [19]
Respuesta de evento	C	M-INFORME-EVENTO parámetro ResdeEvento
Errores	C	M-INFORME-EVENTO parámetro Errores

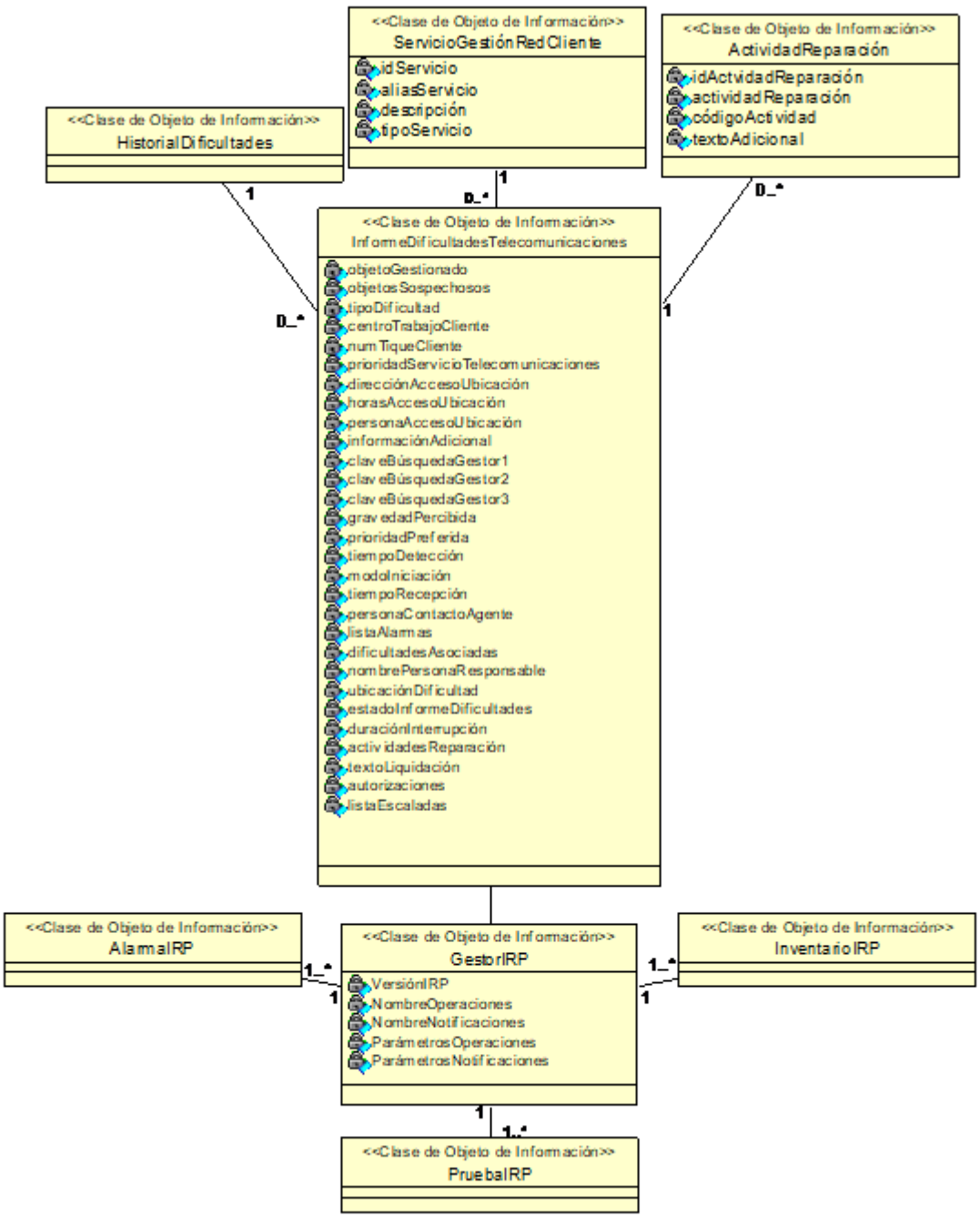
Eventos de Activación

- Si el tiempo de parada real es mayor que el solicitado o el tiempo de comienzo real es anterior al solicitado, el Objeto de Prueba cesará la ejecución (si se está ejecutando) y emitirá una notificación de conflicto de planificación.
- Si se especifica que el instante de comienzo será posterior al instante de fin, el TO emitirá una notificación de conflicto de planificación.

4.2.7 Trouble Ticketing.

4.2.7.1 Clases de Objetos de Información de Trouble Ticketing.

Figura 34. Diagrama de Clases de Objetos de Información de Trouble Ticketing.



InformeDificultades

Definición: describe la naturaleza del problema así como su estado actual. [13] (Ver figura 34).

- **Atributos:**

Tabla 54. Atributos Informe de dificultades

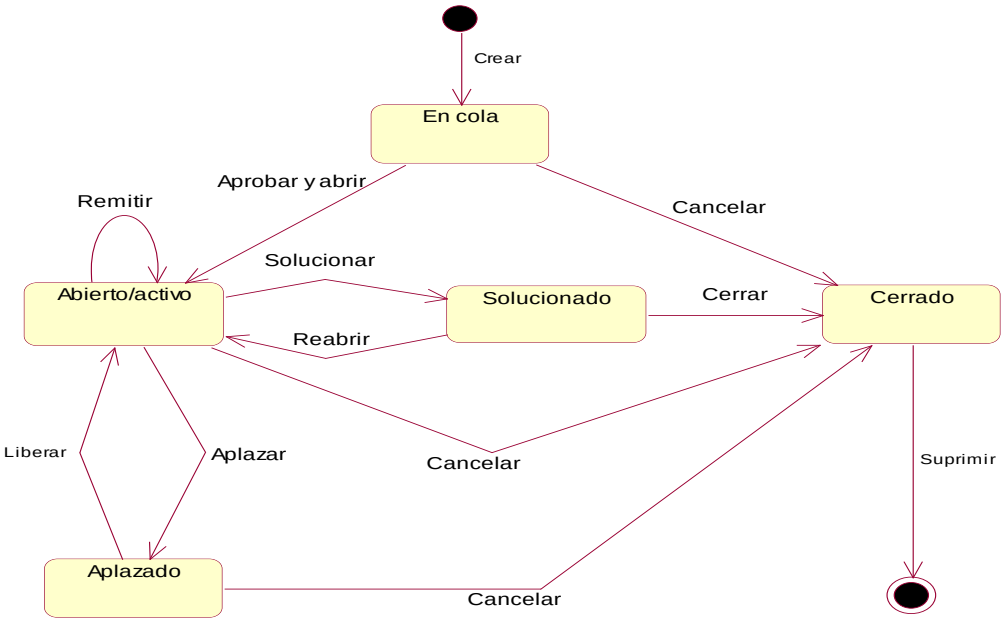
Nombre de Atributo	Calificador	Definición	Valores Legales
idInformeDificultades	M	Contiene el identificador del Informe de dificultades. ITU-T X.790 troubleReport.troubleReportID [20]	Entero

InformeDificultadesTelecomunicaciones

Definición: representa dificultades informadas sobre servicios o recursos de telecomunicaciones. Las instancias de esta clase describen la naturaleza del problema así como la situación actual. [20] (Ver figura 34).

- **Diagrama de estados:**

Figura 35. Diagrama de estados InformeDificultadesTelecomunicaciones.



- **Atributos:**

Tabla 55. Atributos InformeDificultadesTelecomunicaciones

Nombre de Atributo	Calificador	Definición	Valores Legales
objetoGestionado	M	Indica la instancia del objeto ServicioGestiónRedCliente o recurso de red de telecomunicación asociado con un informe de dificultades determinado. ITU-T X.790	Instancia de objeto

		telecommunicationsTroubleReport. managedObjectInstance [20]	
objetos Sospechosos	O	Indica los objetos gestionados que pueden ser la causa subyacente de la dificultad. ITU-T X.790 telecommunicationsTroubleReport. suspectObjectList[20]	Instancias de objetos
tipoDificultad	M	Identifica la categoría de dificultad que se está informando en un ServicioGestiónRedCliente u objeto gestionado. ITU-T X.790 telecommunicationsTroubleReport. troubleType [20]	Entero [20]
centroTrabajo Cliente	M	Identifica el centro de trabajo del gestor desde el cual se introdujo la dificultad. ITU-T X.790 telecommunicationsTroubleReport. customerWorkCenter [20]	String
numTiqueCliente	M	Contiene el número de ficha de dificultades interno del cliente. Permite al cliente acceder a dificultades informadas al proveedor de servicio con el número de ficha local. ITU-T X.790 telecommunicationsTroubleReport. custTroubleTickNum [20]	String
prioridadServicio Telecomunicaciones	M	Transporta códigos de prioridad de servicio de telecomunicaciones, si es aplicable, entre el gestor y el agente. ITU-T X.790 telecommunicationsTroubleReport. tspPriority [20]	Entero
direcciónAcceso Ubicación	M	Identifica la dirección para la cual son válidos los respectivos valores del atributo horas de acceso a ubicación. ITU-T X.790 telecommunicationsTroubleReport. aLocationAccessAddress [20]	String
horasAcceso Ubicación	M	Define las horas específicas de cada día de la semana durante las cuales es posible acceder a la ubicación. ITU-T X.790 telecommunicationsTroubleReport. aLocationAccessHours [20]	Intervalo de tiempo
personaAcceso Ubicación	M	Permite al gestor especificar los detalles de la persona en la ubicación. ITU-T X.790 telecommunicationsTroubleReport. aLocationAccessPerson [20]	String
informaciónAdicional	O	Describe más detalladamente el tipo de dificultad seleccionada. ITU-T X.790 telecommunicationsTroubleReport.	String

		additionalTroubleInfoList [20]	
claveBúsqueda Gestor1	O	Permiten al gestor filtrar informes de dificultades, por ejemplo, por cuenta o por identidad de cliente. ITU-T X.790 telecommunicationsTroubleReport. managerSearchKey1 [20]	String
claveBúsqueda Gestor2	O		
claveBúsqueda Gestor3	O		
gravedadPercibida	M	Permite al gestor indicar el efecto de la dificultad en el objeto gestionado sobre el que se informa. ITU-T X.790 telecommunicationsTroubleReport. perceivedTroubleSeverity [20]	Enum: • Fuera de servicio • Retroceso del servicio • Servicio deteriorado • Servicio no afectado
prioridadPreferida	M	Define la urgencia con la cual el gestor requiere que se resuelva el problema. ITU-T X.790 telecommunicationsTroubleReport. preferredPriority [20]	Enum: • Indeterminado • Menor • Mayor • Crítica
tiempoDetección	M	Indica el momento en el cual se detectó la dificultad. Puede ser diferente del momento en el que se creó el informe de dificultades. ITU-T X.790 telecommunicationsTroubleReport. troubleDetectionTime [20]	Date
modoIniciación	M	Especifica el modo de iniciación del informe de dificultades. ITU-T X.790 telecommunicationsTroubleReport. initiatingMode [20]	Enum: • gestor directo • gestor indirecto • e-mail • fax • personal • teléfono • agente • alarma
tiempoRecepción	C	Indica la fecha y hora en que se introdujo un informe de dificultades. ITU-T X.790 telecommunicationsTroubleReport. receivedTime [20]	Date
personaContacto Agente	O	Identifica a un individuo con el que se puede comunicar en la organización del agente en relación con la dificultad informada. ITU-T X.790 telecommunicationsTroubleReport agentContactPerson [20]	String
listaAlarmas	O	Señala instancias de alarmas disponibles en el sistema del agente. Una condición necesaria para que	Instancias de alarmas

		este atributo esté presente es que el informe de dificultades haya sido generado como resultado de una alarma. Sin embargo, ésta no es una condición suficiente puesto que algunas Administraciones pueden elegir no admitir este atributo, incluso si el informe de dificultades fue generado como resultado de una alarma recibida o generada en el agente. ITU-T X.790 telecommunicationsTroubleReport. alarmRecordPtrList [20]	
dificultadesAsociadas	O	Identifica otros informes de dificultades asociados. ITU-T X.790 telecommunicationsTroubleReport. relatedTroubleReportList [20]	Instancias de informes de dificultades
nombrePersona Responsable	O	Indica la persona que tiene la responsabilidad general de resolver el problema indicado por el informe de dificultades. Esta puede no ser la persona que realiza las actividades de reparación, pero es la persona responsable del proceso de solución de la dificultad, que incluye el seguimiento del problema, el aislamiento del problema y la corrección del problema. ITU-T X.790 telecommunicationsTroubleReport. responsiblePersonName [20]	String
ubicaciónDificultad	O	Indica dónde radica la dificultad. Esta información podría no ser conocida en el momento en que se crea el informe de dificultades. ITU-T X.790 telecommunicationsTroubleReport. troubleLocation [20]	String
estadoInforme Dificultades	O	Indica el estado vigente de un informe de dificultades. ITU-T X.790 telecommunicationsTroubleReport. troubleReportState [20]	Enum: • Cola • Abierto/activo • Aplazado • Solucionado • Cerrado • Inhabilitado
duraciónInterrupción	C	Indica intervalo de tiempo entre el momento en que se solucionó el informe de dificultades y el momento en que se recibió el informe de dificultades ITU-T X.790 telecommunicationsTroubleReport. outageDuration [20]	Intervalo de tiempo
actividades	C	Contiene una lista de los	Lista de:

Reparación		identificadores de las actividades de reparación realizadas. ITU-T X.790 telecommunicationsTroubleReport. repairActivityList [20]	• Tiempo de entrada (Date) • Información de actividad (String) • Personal (String)
textoLiquidación	O	Especifica información adicional sobre el problema. Este campo proporciona un lugar para que la persona que resolvió el problema documente cualquier información adicional relativa a la liquidación del informe de dificultades ITU-T X.790 telecommunicationsTroubleReport. closeOutNarr[20]	String
autorizaciones	O	Identifica si la autorización es solicitada por el agente y concedida por el gestor. Especifica también el tipo de actividades que son autorizadas y, facultativamente, la persona que autoriza y el tiempo de autorización. ITU-T X.790 telecommunicationsTroubleReport. authorizationList [20]	
listaEscaladas	O	Indica si la escalada es solicitada por el gestor y concedida por el agente. Especifica facultativamente el nivel de escalada y la persona a la cual se ha llegado. ITU-T X.790 telecommunicationsTroubleReport. escalationList [20]	

ServicioGestiónRedCliente

- **Definición:** representa la funcionalidad específica que un proveedor suministra a los clientes. El objeto ServicioGestiónRedCliente desacopla la relación entre servicios ofrecidos al cliente y los componentes de red específicos que proporcionan el servicio (Ver figura 34).
- **Atributos:**

Tabla 56. Atributos ServicioGestiónRedCliente

Nombre del atributo	Calificador	Definición	Valores Legales
idServicio	M	Contiene el identificador del Servicio de Gestión de Red de Cliente. ITU-T X.790 Service.serviceID	Entero
aliasServicio	M	Identifica el Servicio de Gestión de Red de Cliente mediante una terminología de telecomunicaciones comúnmente utilizada (número telefónico, número de servicios especiales). ITU-T X.790 cnmService.serviceAliasList [20]	String

descripción	O	Describe el servicio en forma textual. ITU-T X.790 cnmService.serviceDescription [20]	String
tipoServicio	M	Identifica la categoría del servicio. ITU-T X.790[20] Service.serviceType	String

ActividadReparación

- **Definición:** contiene parámetros y texto que describen las funciones de reparación específicas ejecutadas, quién las ejecutó y cuándo se ejecutaron (Ver figura 34).
- **Atributos:**

Tabla 57. Atributos ActividadReparación

Nombre de Atributo	Calificador	Definición	Valores Legales
idActividad Reparación	M	Contiene el identificador de la Actividad de Reparación. ITU-T X.790 repairActivity.repairActivityID	Entero
Actividad Reparación	M	Describe la actividad de reparación en forma textual. ITU-T X.790 repairActivity.activityInfo	String
códigoActividad	M	Identifica una categoría de actividad de reparación general. ITU-T X.790 repairActivity.activityCode	Enum: Aprobado, Asignar, Cancelar, Clarear, Cerrar, Diferir, Despachar, Referir, Lanzar, Reabrir, Reparar, Probar, Transferir
textoAdicional	O	Contiene información adicional.	String

GestorIRP

- **Definición:** el GestorIRP es el encargado de analizar y procesar la información que envían los agentes y determinar la acción a tomar.

  Cuando es detectada una alarma, el GestorIRP debe analizarla para poder determinar el origen. Una vez que el GestorIRP detecta el origen de la alarma procede a notificar y hacer los cambios al inventario sobre el estado actual del dispositivo afectado. En el caso que no se pueda determinar el elemento que originó la alarma o se desea hacer mantenimiento, se realizan los procedimientos de pruebas que permitan determinar el origen de esta. El GestorIRP también se encarga de comunicarse con InformeDificultadesTelecomunicaciones, ya sea para analizar notificaciones de los informes de dificultades o para enviar información a estos (Ver figura 34).

- **Atributos:**

Tabla 58. Atributos GestorIRP

Nombre de Atributo	Califa cador	Definición	Valores Legales
VersiónIRP	M	Contine el grupo de elementos relacionados al gestor	Intancia
NombreOperaciones	O	Contiene un grupo de elementos. El elemento n de este grupo contiene las operaciones soportadas por el elemento n del atributo VersiónIRP	Arreglo de elementos
NombreNotificaciones	O	Contiene un grupo de elementos. El elemento n de este grupo contiene las notificaciones soportadas por el elemento n del atributo VersiónIRP	Arreglo de elementos
ParámetrosOperaciones	O	Contiene un grupo de elementos. El elemento n de este grupo contiene los parámetros del elemento n del atributo NombreOperaciones	Arreglo de elementos
ParámetrosNotificaciones	O	Contiene un grupo de elementos. El elemento n de este grupo contiene los parámetros del elemento n del atributo NombreNotificaciones	Arreglo de elementos

4.2.7.2 Definición de interfaces.

Figura 36. Diagrama de Interfaces de *informeDificultadesTelecomunicaciones*.

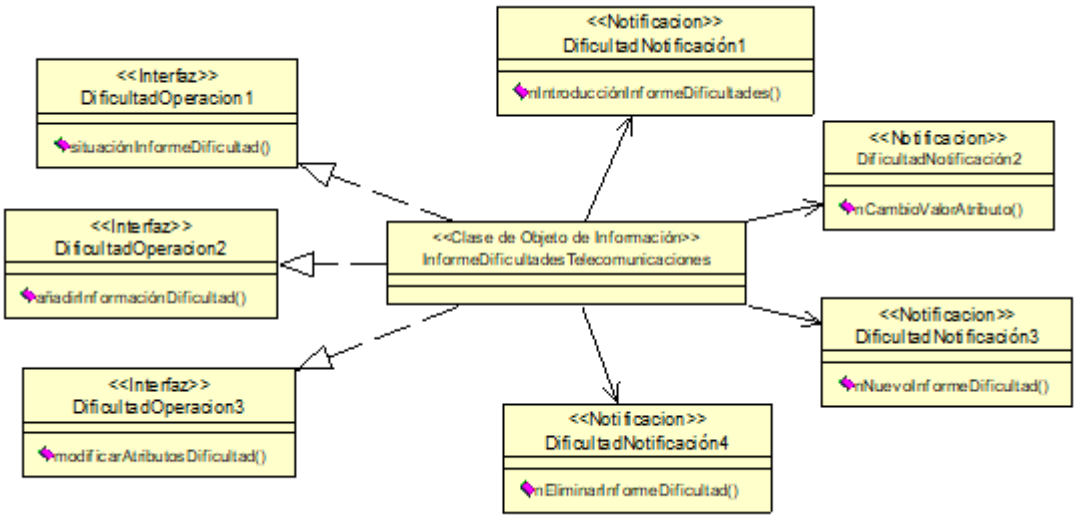
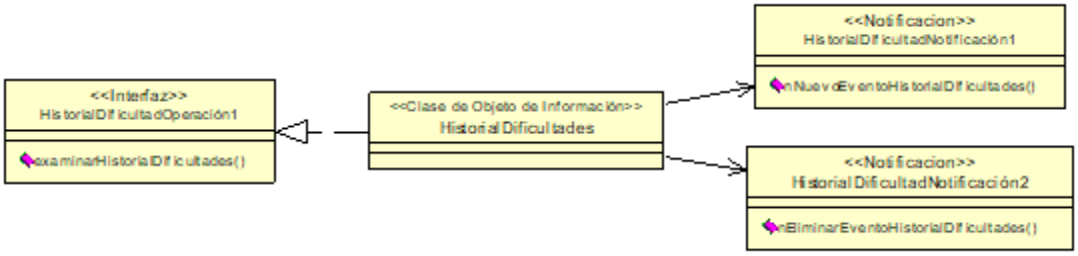


Figura 37. Diagrama de Interfaces de *HistorialDificultades*



Interfaz DificultadOperacion1

- **situaciónInformeDificultad**
  Definición: La red de gestión pide información de situación sobre un informe de dificultades introducido previamente (Ver figura 36).

Interfaz DificultadOperacion2

- **añadirInformaciónDificultad**
  Definición: La red de gestión añade información a un informe de dificultades que ha sido introducido (Ver figura 36).

Interfaz DificultadOperacion3

- **modificarAtributosDificultad**
  Definición: La red de gestión modifica los atributos que pueden escribirse de un informe de dificultades que no están cubiertos específicamente en otras funciones (Ver figura 36).
  Parámetros de entrada:

Tabla 59. Parámetros de entrada modificarAtributosDificultades

Nombre	Calificador	Información correspondiente
dirección de acceso a ubicación	M	InformeDificultadesTelecomunicaciones. direcciónAccesoUbicación
horas de acceso a ubicación	M	InformeDificultadesTelecomunicaciones. horasAccesoUbicación
persona de acceso a ubicación	M	InformeDificultadesTelecomunicaciones. personaAccesoUbicación
lista de autorizaciones	M	InformeDificultadesTelecomunicaciones. autorizaciones
lista de escalada	O	InformeDificultadesTelecomunicaciones. listaEscaladas
gravedad de dificultad percibida	O	InformeDificultadesTelecomunicaciones. gravedadPercibida

Interfaz DificultadNotificación1

- **nIntroducciónInformeDificultades**
  Definición: La red de gestión notifica a otra red de gestión que un servicio proporcionado por esa red de gestión necesita reparación (Ver figura 36).

Parámetros de entrada:

Tabla 60. Parámetros de entrada nIntroducciónInformeDificultades

Nombre	Calificador	Información correspondiente
instancia de objeto gestionado	M	Especifica la instancia del objeto gestionado que ha de utilizarse como punto de partida para la selección de los objetos gestionados. ***Equivalente CMIP***: CMISE servicio M- ACCIÓN ITU-T X.710 [14]
tipo de dificultad	M	Identifica el tipo de dificultad del evento. ***Equivalente CMIP:*** *CMISE servicio M- ACCIÓN ITU-T X.710 [14]*
lista de informaciones adicionales sobre dificultades	M	Lista de InformeDificultadesTelecomunicaciones.*atributos*, donde atributos representa la información que se quiere enviar.

Interfaz DificultadNotificación2

- **nCambioValorAtributo**
  Definición: La red de gestión notifica a la red de gestión que originó un informe de dificultades que otros atributos de interés para ese informe han cambiado (Ver figura 36).

Interfaz DificultadNotificación3

- **nNuevoInformeDificultad**
  Definición: La red de gestión notifica a la red de gestión que originó normalmente un informe de dificultades que se ha creado un informe de dificultades como resultado de una petición o como resultado de una acción interna de la red de gestión notificante (Ver figura 36).

Interfaz DificultadNotificación4

- **nEliminarInformeDificultad**
  Definición: La red de gestión notifica a la red de gestión que originó normalmente un informe de dificultades que éste ha sido suprimido, como resultado de una petición o como resultado de una petición interna de la red de gestión notificante (Ver figura 36).

Interfaz HistorialDificultadOperación1

- **examinarHistorialDificultades**
  Definición: La red de gestión pide información sobre dificultades pasadas que ha informado (Ver figura 37).

Interfaz HistorialDificultadNotificación1

- **nNuevoEventoHistorialDificultades**
  Definición: la red de gestión notifica a la red de gestión que originó el informe de dificultades que éste ha sido liquidado o que mantiene la información de liquidación en un registro interno (Ver figura 37).

Parámetros de entrada:

Tabla 61. Parámetros de entrada nNuevoEventoHistorialDificultades

Nombre	Calificador	Información correspondiente
Identificador de invocación	M	Especifica el identificador asignado a la operación. Puede utilizarse para distinguir esta operación de otras notificaciones u operaciones ***Equivalente CMIP:*** *CMISE servicio M-ACCIÓN ITU-T X.710*
Modo	M	"confirmado"
Tipo de evento	M	"Notificación de evento de historial de dificultades"
Tiempo de evento	M	Fecha actual del sistema
Instancia de objeto gestionado	M	InformeDificultadesTelecomunicaciones.objetoGestionado
Tiempo de recepción	O	InformeDificultadesTelecomunicaciones.tiempoRecepción
Lista de informaciones adicionales de dificultades	O	InformeDificultadesTelecomunicaciones.informaciónAdicional
Lista de autorizaciones	O	InformeDificultadesTelecomunicaciones.autorizaciones
Texto de liquidación	O	InformeDificultadesTelecomunicaciones.textoLiquidación
Número de ficha de dificultad de cliente	O	InformeDificultadesTelecomunicaciones.numTiqueCliente
gravedad de la dificultad percibida	O	InformeDificultadesTelecomunicaciones.gravedadPercibida
tipo de dificultad	O	InformeDificultadesTelecomunicaciones.tipoDificultad
Tiempo vigente	O	Contiene la hora de generación del evento. ***Equivalente CMIP:*** CMISE servicio M-INFORME-EVENTO ITU-T X.710 [14]

Interfaz HistorialDificultadNotificación2

- **nEliminarEventoHistorialDificultades**

  Definición: La red de gestión notifica que se ha eliminado información de liquidación de un registro interno (Ver figura 37).

Interfaz GestorIRPOperación

- **obtenerOperación**

  Definición: el gestor utiliza esta operación para obtener las operaciones del elemento relacionado (Ver figura 37).

Parámetros de entrada:.

Tabla 62. Parámetros de entrada obtenerOperación

Nombre	Calificador	Información correspondiente
VersiónIRP	M	GestorIRP.VersiónIRP

Parámetros de salida:

Tabla 63. Parámetros de salida obtenerOperación

Nombre	Calificador	Información correspondiente
NombreOperaciones	M	GestorIRP.NombreOperaciones
ParámetrosOperaciones	M	GetorIRP.ParámetrosOperaciones

- **obtenerNotificación**
  Definición: el gestor utiliza esta operación para obtener las notificaciones del elemento relacionado (Ver figura 37).

Tabla 64. Parámetros de entrada obtenerNotificación

Nombre	Calificador	Información correspondiente
VersiónIRP	M	GestorIRP.VersiónIRP

Parámetros de salida:

Tabla 65. Parámetros de salida obtenerNotificación

Nombre	Calificador	Información correspondiente
NombreNotificaciones	M	GestorIRP.NombreNotificaciones
ParámetrosNotificaciones	M	GestorIRP.ParámetrosNotificaciones

4.3 TAREA 4: CONSOLIDACIÓN DE LA INFORMACIÓN DISPONIBLE

En la tarea 4 se hace una comprobación entre las funciones que conforman los cometidos y las funcionalidades generales de las clases de objetos creados.

Tabla 66. Relación Funciones de gestión de fallas/actividades arquitectura de la información

Actividades de la arquitectura de la información	Funciones de gestión de fallas relacionadas
Entidad Monitoreada	• Envió de eventos de Elementos de Red
Discriminador de Envío de Eventos	• Envió de eventos adaptados o mapeados para objeto de gestión • Establecer la identidad única de un evento • Establecimiento de condiciones de Mapeo de Eventos • Adaptar un evento proveniente de un agente para el posterior manejo en el gestor • Filtrar eventos • Suprimir eventos transitorios de ocurrencia rara o intermitente • Suprimir eventos redundantes • Mantenimiento de interdependencias de evento • Gestionar eventos de orden de llegada erróneo • Gestionar las condiciones del entorno • Activación/desactivación de acciones automáticas • Ejecutar acción en base a la no llegada de un evento dentro de un periodo de tiempo especificado • Recepción de datos brutos • Detección de restablecimiento automático • Informe de restablecimiento automático • Procedimiento de auxilio inmediato • Procedimiento de recarga • Informe de recarga
Fichero Registro Cronológico	• Adicionar/Eliminar informe de alarma en fichero cronológico • Autorización/inhibición de inscripción en el fichero-registro cronológico • Inscripción condicional en el fichero-registro cronológico • Informe de asignación vigente de atributos especificados del fichero-registro cronológico • Petición de condición de fichero-registro cronológico
Inventario	• Colocar unidad fuera de servicio • Informe de unidad puesta fuera de servicio. • Anular reestablecimiento automático • Activar restablecimiento automático • Informe de activación de reestablecimiento automático • Informe de Anulación de reestablecimiento automático
Punto de Referencia de Integración de Alarmas	• Detección de interrupción de elemento de red • Informe de interrupción del elemento de red • Finalización de interrupción de elemento de red • Informe de finalización de interrupción del elemento de red • Adición de información relativa a interrupciones del elemento de red • Establecimiento de condiciones de anulación de una señal de

	alarma en un cuadro • Establecimiento del nivel de gravedad que se ha de asignar a unas condiciones de alarma específicas en un cuadro • Informe de alarma • Encaminamiento de informes de alarma • Petición de encaminamiento de informes de alarma • Asignar atributos del discriminador de remisión de los eventos especificados por el gestor • Señalamiento de alarma condicional • Informe de asignación vigente de los atributos especificados de informe de alarmas • Petición de condición de control de informe de alarma • Autorización/inhibición de señalamiento de alarma • Informe de historial de Alarmas • Petición de historial de alarmas • Reconstrucción de historial de alarmas o de un segmento de este • Informe de resumen de alarmas vigentes • Autorización/inhibición de resumen de alarmas vigentes • Petición de resumen de alarmas vigentes • Acondicionamiento de criterios de eventos de alarma • Detección de Alarma
Punto de Referencia de Integración de Pruebas	• Detectar interrupción del servicio • Detectar interrupción de la red o un segmento de red • Petición de datos de diagnóstico • Informe de diagnóstico • Análisis del estado operacional en una unidad o elemento de red • Informe del estado operacional de una unidad o elemento de Red • Cambio de Estado Operacional de una unidad o elemento de Red • Informe de cambio de estado operacional de una unidad o elemento de Red • Planificación de pruebas de rutina • Comienzo/detención de pruebas de rutina. • Informe de plan de pruebas de rutina. • Informe de inicialización del sistema de prueba • Inicialización y restablecimiento del sistema de acceso • Conexión de acceso de prueba • Liberación del acceso de prueba • Inicio de Comprobación de un Elemento de Red. • Notificación de Inicio de Comprobación de un Elemento de Red • Informe de Comprobación de un Elemento de Red • Petición de resultados de prueba • Comunicación de resultados de prueba
Trouble Ticket o Gestión de Dificultades	• Mensaje al cliente • Apertura/cierre de tiques del sistema • Anulación/supresión de tiques de anomalía • Actualización de la situación de anomalía • Selección de una alternativa • Selección de un problema • Examen de la base de datos de anomalías • Adición de reparación • Reporte de finalización de reparación

	• Asignación de personal a reparación • Asignación de tiempo de reparación • Calculo de tiempo medio de reparaciones • Adicionar demanda de cliente. • Cerrar o finalizar demanda del cliente. • Denuncia de la anomalía • Adición de información relativa a la anomalía • Cancelación de anomalías • Informe de cambio de situación de la anomalía • Comprobación de la situación de la anomalía • Examen del historial de anomalías • Búsqueda de informe de anomalía o tique de anomalía • Informe de seguimiento de corrección de averías • Notificación de desaparición de informe o tique de anomalía

Dado que la arquitectura de la información se hizo a partir de la arquitectura funcional, se ha cumplido con todas la funciones propuestas en el capítulo 3.

5. OSS A TRAVES DE OSS/J

OSS a través de la iniciativa JavaTM (OSS/J), nace debido a la carencia de tecnología para afrontar el rápido incremento de escala de redes, la diversidad de tecnologías de comunicaciones, la reducción de tiempo para la comercialización de nuevos servicios y el aumento de expectativas en cuanto a disponibilidad y fiabilidad.

OSS/J define un conjunto de interfaces de programación de aplicaciones (APIs, Application Program Interfaces) que integran una total solución OSS que soporta el flujo a través del desempeño, aseguramiento y facturación del servicio, basado en el éxito de la plataforma Java, Java 2 Enterprise Edition (J2EE), XML y en las tecnologías de los servicios Web en las aplicaciones empresariales. Las metas de esta iniciativa son desarrollar, a través del programa Java Community Process (JCP), especificaciones de APIs, implementaciones de referencia, kits de compatibilidad tecnológica, y código fuente, libre de costos, para integración y desarrollo OSS.

Los APIs de OSS/J ayudan al proveedor del servicio a dar un salto hacia el despliegue de servicios end-to-end sobre redes de próxima generación, impulsando la convergencia de soluciones de telecomunicaciones y soluciones basadas en Internet.

Desde su principio en septiembre del 2000, OSS/J ha tenido el respaldo de algunos de los proveedores de equipos de redes (NEPs, Network Equipment Providers), vendedores de software independientes (ISVs, Independent Software Vendors) e integradores de sistemas (SIs, System Integrators) líderes en el mundo.

En el 2004, el TeleManagement forum anunció una unión de fuerza de trabajo con OSS/J, asociación que ofrece una efectiva y rápida opción de implementación para desarrolladores de soluciones quienes están alineados al marco de los sistemas y software de Operaciones de próxima generación (NGOSS, Next Generation Operations Systems and Software) del TMForum y quienes escogen implementar en tecnología Java y Web Services.

Los APIs OSS/J han sido derivados de muchos escenarios OSS, notas de aplicaciones, y ejemplos publicados por el TeleManagement Forum con respecto al TOM y al eTOM. Además de forma similar a las especificaciones del eTOM, las especificaciones de los APIs OSS/J son derivadas de la aplicación de estándares relevantes de telecomunicaciones como lo son los de la ITU-T.

La principal diferencia entre el alcance de la guía básica de los APIs de OSS/J y el eTOM, es que la guía define APIs que son esencialmente para automatizar flujos a través de la gestión de servicios y cubren determinados bloques de funciones del eTOM, el cual identifica procesos

generales independiente de si ellos son automáticos o si pueden ser llevados a cabo por humanos. [35]

En la Figura 38 se puede observar como los APIs de OSS a través de Java son mapeados a los procesos del eTOM (cuadros con relleno amarillo). Esta figura resalta el enfoque de la iniciativa OSS/J en la automatización de operaciones de los proveedores de servicios de telecomunicaciones y también resalta la cobertura de la automatización con respecto a los elementos identificados en el marco del eTOM.

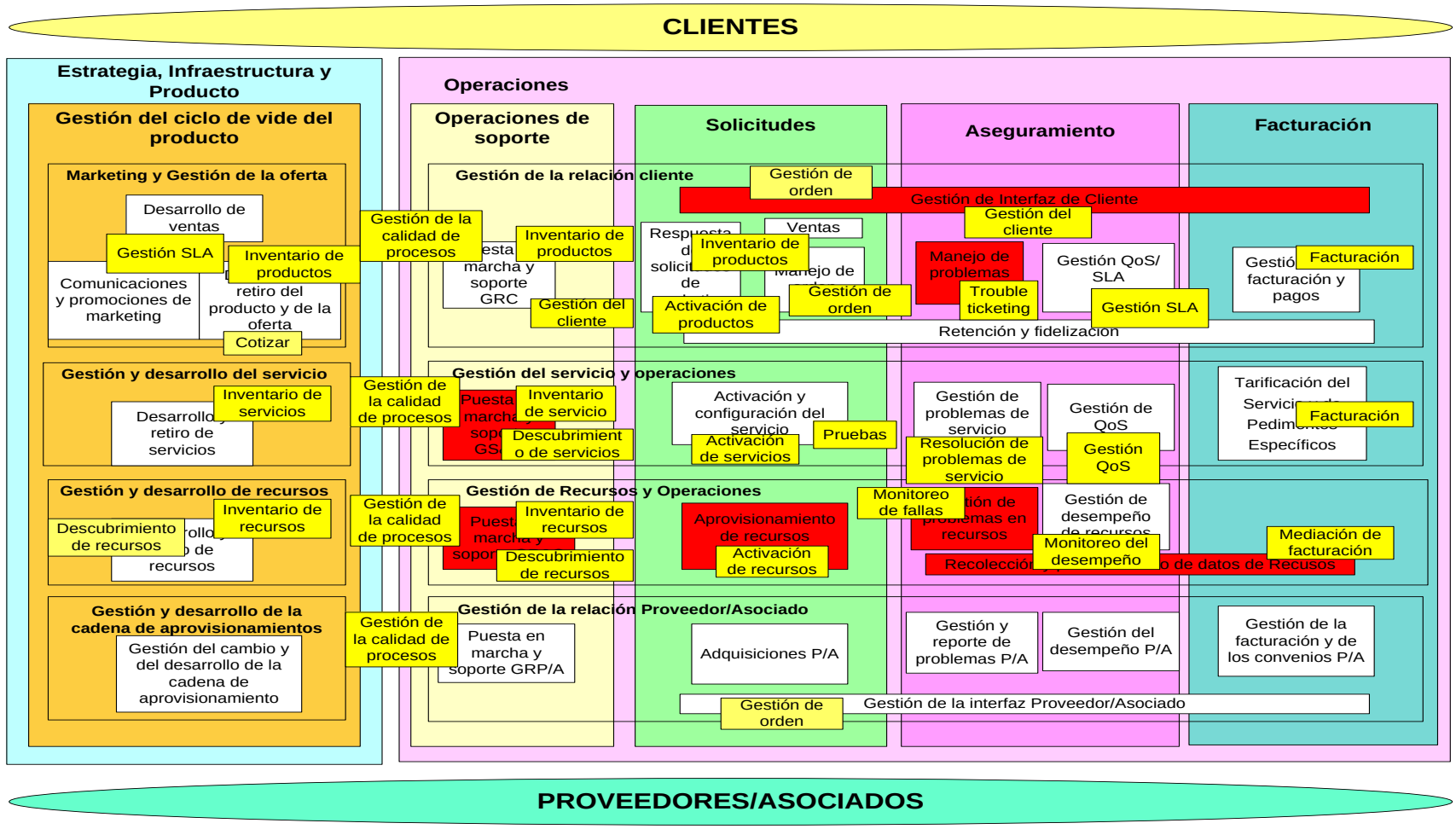
5.1 APLICACIÓN DE OSS/J AL OSS PARA GESTIÓN DE FALLAS EN REDES MÓVILES DE 3G

Como se vio en el capitulo dos, los cometidos tenidos en cuenta para el diseño del OSS para gestión de fallas en redes móviles de 3G, se obtuvieron a partir del mapa de operaciones de telecomunicaciones mejorado eTOM. Posteriormente se obtuvo el mapeo de los bloques involucrados en gestión de fallas hacia los conjuntos de funciones de la recomendación ITU-T M.3400 para determinar las operaciones, notificaciones y flujo de información que se implementarían para el diseño del OSS. Estos cometidos son mapeados en este capitulo con el fin de observar la aplicación que pueda tener la iniciativa OSS/J en el diseño propuesto para el OSS.

El hecho, que los APIs de OSS/J se basen en el eTOM y este a su vez en las recomendaciones de la ITU-T, hacen que la tecnología presentada por la JCP a través de Java, sea una opción atractiva para la implementación de los componentes diseñados para gestión de fallas en una red UMTS, debido a que tanto el diseño desarrollado, como los APIs OSS/J están basados en los mismos conceptos de gestión. Adicionalmente otra razón que se suma a la escogencia de esta tecnología es la expectativa generada en el mercado de los OSS, a causa de las facilidades que brinda en cuanto a integración de este tipo de sistemas con otros componentes de gestión, y a que es uno de los lenguajes más conocidos por los desarrolladores actualmente.

Otro factor tenido en cuenta para optar por OSS/J es que el diseño que se plantea en este proyecto, esta enfocado hacia una red de tercera generación lo que implica complejos sistemas de procesamiento de datos distribuidos, por lo cual se hace indispensable analizar la utilización de una tecnología que permita el desarrollo de componentes independientes, que conforme pase el tiempo puedan ser integrados para construir una solución de gestión cada vez más robusta y eficiente.

Figura 38. Mapeo APIs OSS/J a eTOM



OSS through Java Initiative. OSS/J API Roadmap. OSS/J 2005. p.14.:il(OSS-J API Roadmap) [35]

Una ventaja que presenta OSS/J frente a otras tecnologías en el desarrollo de componentes OSS para redes de tercera generación, es que esta ha tomado como referencia varios de los requerimiento de gestión de redes UMTS expuestos en las recomendaciones del 3GPP con el fin de dar un cubrimiento mayor a redes de tercera generación, permitiendo a los desarrolladores agilizar procesos en la implementación de los sistemas de soporte, por medio de APIs como el común donde incluye el concepto de puntos de referencia IRP, al igual que el API de Calidad de Servicio y Gestión de Fallas.

De acuerdo a los cometidos y el diseño planteado para la arquitectura de la información del sistema de soporte de operaciones para gestión de fallas en redes móviles de tercera generación, los APIs de OSS/J que se presentan en la Tabla 67 son los que pueden ser aplicados al proyecto:

Tabla 67. APIs OSS/J para Gestión de Fallas

API	Java Specification Requests (JSR) Correspondiente
API Común	(JSR 144: OSS Common API)
API Inventario	(JSR 142: OSS Inventory API)
API Calidad de servicio	(JSR 90: OSS Quality of Service API)
API Gestión de Fallas	(JSR 263: Fault Management API)
API Pruebas	(Aún no desarrollado)
API Trouble Ticket	(JSR 162: OSS Trouble Ticket API)

A continuación se hace una breve explicación de cada uno de los APIs de OSS/J aplicables al diseño.

5.1.1 API Común (JSR 144: OSS Common API). Este API surge ante la necesidad de las APIs OSS de un JSR común para capturar interfaces y clases comunes para evitar la duplicación de estas y de código, y mantener la consistencia a través de los APIs.

En este API se encuentra la definición más genérica de las clases, de la cual se basan los APIs actuales y se basarán los que están por desarrollarse, por lo que aquellas clases de Objetos de información y atributos, así como las operaciones, notificaciones y parámetros, definidos en el Capitulo 4, para la arquitectura de la Información del OSS serán mapeados a este API, siempre y cuando no exista un API especifico que los cubra.

Este JSR esta basado en el estándar de servicios J2EE, esencialmente en:

- **EJB (Enterprise Java Beans):** es usada debido a su aceptación por la industria de la información y de las comunicaciones, para facilitar la integración de componentes OSS, los APIs OSS/J definen interfaces estándar EJB.

- **JMS (Java Message Service):** además de la capacidad para ejecutar llamadas a métodos de forma sincrónica (EJB), exite también la necesidad de enviar mensajes asíncronos. Por esta

razón es considerada la tecnología JMS como la solución más viable.

Esta especificación define clases e interfaces así como un conjunto de patrones que pueden ser aplicados a la plataforma J2EE para la especificación de componentes básicos de gestión de redes, servicios, y negocios.

Las entidades de red central (CBE, Core Business Entities), también parte de esta especificación, definen interfaces que son reusables a través de múltiples componentes OSS tales como: activación, facturación, Inventario, Trouble Ticket, Calidad de servicio (QoS), etc. CBE también define un modelo de información central, de objetos de transferencia de datos compartibles alineados al modelo de datos e información compartida TMF (SID, Shared Information and Data).

La clave de esta especificación es el concepto de componentes básicos software. Un componente básico software es una colección de componentes software, que junto con otro componente software (para los propósitos de desarrollo), satisfacen una o más necesidades de negocios. Un componente básico OSS/J comprende piezas software, como:

- EJB Session Beans con Java Value Types (JVT)
- Message Driven Beans
- EJB Entity Beans
- Core Business Entities (CBE)

En OSS/J, una entidad gestionada o un objeto de negocios esta representado por un EJB Entity Bean, un objeto Java Value Type (JVT), un documento XML o una entidad de negocios.

Este API esta enfocado a los siguientes elementos:

- un mecanismo para implementar un modelo de interacción asíncrono y débilmente acoplado que depende de mensajes basados en XML;
- un mecanismo para fuerte tipeado, y eventos basados en objetos;
- un mecanismo para eventos basados en XML;
- mecanismos de Suscripción de eventos y mensajes basados en la especificación Java™ Messaging Service (JMS);
- un mecanismo para facilitar la ubicación de elementos de la arquitectura OSS/J, por ejemplo, tópicos, Session Beans, y Colas que utilizan la especificación Java™ Naming and Directory Interface (JNDI);

Un componente básico OSS/J provee interfaces para la gestión de un conjunto específico de entidades u objetos de negocios de telecomunicaciones. La funcionalidad OSS esta implementada dentro de componentes software que soportan el contrato de interfaces definidas que representan la lógica de la aplicación.

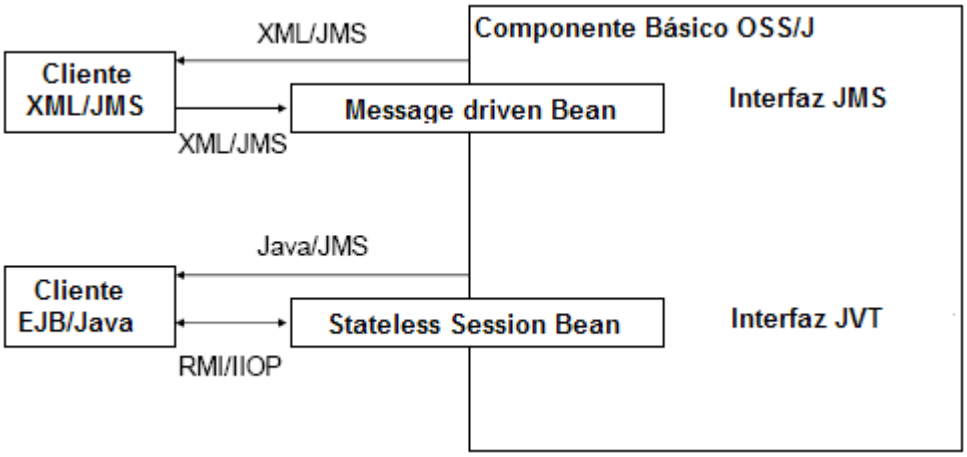
Entidades Gestionadas. Un tipo entidad describe un tipo de "cosa" en el mundo real con una existencia independiente. Un tipo entidad puede ser un objeto con una existencia física como por ejemplo un paquete de circuitos, un elemento gestionado, o una ranura de tiempo (slot)- o puede ser un objeto con una existencia conceptual como una alarma, un conjunto de políticas, un SLA, una orden de servicio, un trouble ticket, un escáner, una subred, un punto de terminación, etc. Cada tipo entidad tiene propiedades particulares y atributos los cuales describen la entidad. Una instancia de entidad describe una instancia particular de un tipo de entidad. Los atributos de cada entidad son descritos por valores particulares que representan el estado de esa instancia. Adicionalmente, cada entidad puede ser identificable excepcionalmente.

Las definiciones de las entidades centrales, modelos de información y especificaciones (CBE), son una implementación del TMForum SID, y son usadas como la piedra angular para el desarrollo de algunos de APIs OSS/J.

Patrones de Interacción .Un patrón de interacción define al naturaleza de las interacciones (por ejemplo la interacción de interfaces) expuestas por los componentes básicos de OSS/J.

La definición de los diferentes patrones de interacción depende del tipo de actor que accede el sistema gestionado. Para el API común se definen dos patrones de interacción. Si el uso pretendido es para fuerte integración de aplicaciones OSS/J el tipo de patrón interacción recomendado es Java Value Type Session Bean (JVT), si por el contrario lo que se pretende es la baja integración con aplicaciones OSS/J el patrón de interacción recomendado es XML Messaging.

Figura 39. Patrones de Interacción



OSS through Java Initiative. OSS Common API Overview. OSS/J 2005. p.14.:il(OSS Common API) [36]

Java Value Type Session Beans (JVT): las instancias de un conjunto de tipos de entidades son accedidas por medio de una interfaz singular por ejemplo un Stateless Session Bean. La mayoría de operaciones son definidas en la aplicación de interfaces Session, las cuales comunican

identidades y estados de entidades gestionadas usando parámetros de operación que usan los objetos Java Value Type. El estilo de interfaces JVT son propuestas para el uso por clientes Java que desean fuerte integración con aplicaciones OSS/J.

XML/JMS Messaging: las instancias de un conjunto de tipos de entidades son accedidas por medio de peticiones XML enviadas a destinos de mensajes (MD, Messaging Destinations), las peticiones son enrutadas a la aplicación Message Driven Beans específica. Las operaciones son definidas en mensajes XML Request, los cuales comunican identidades y estados de entidades gestionadas usando parámetros de operación definidos por un esquema XML que emplea el mapeo XML de objetos Java. Se espera que los Stateless Session Beans XML sean usados para implementar las interfaces que soportan mensajes XML.

Interfaces JVT. Las JVT Session Bean proveen acceso a las entidades gestionadas usando objetos Java™ Value Type (JVT) como parámetros y caracteres de retorno. En este patrón de interacción, las entidades gestionadas son representadas como Objetos JVT basados en el modelo de objetos. El JVT Session Bean soporta interfaces para crear, recuperar, actualizar, consultar y borrar un objeto JVT.

En una interacción típica entre un cliente y un JVT Session Bean el cliente obtiene la instancia del ManagedEntityValue correspondiente al identificador del objeto dado. Este fija solo los atributos apropiados desde el ManagedEntityValue retornado y llama al método setManagedEntity() usando la ManagedEntityValue actualizada.

Todos los objetos tipo valor (ManagedEntityValue class) siguen este patrón de nombramiento específico:

- Una interfaz tipo valor siempre termina con la cadena ”Value”.
- Una interfaz de identificador que permite identificar excepcionalmente el objeto tipo valor, siempre finalizando con la cadena “Key”

Por ejemplo:
javax.oss.cbe.product.ProductValue
javax.oss.cbe.product.ProductKey

La interfaz Tipo valor incluye siempre un método industrial para crear, y retornar la interfaz de identificador correspondiente por defecto.

XML Messaging
Los patrones de interacción entre XML Messaging proveen accesos a las entidades gestionadas a través del paradigma requerimiento/respuesta basado en XML. En este patrón de interacción, las

entidades gestionadas son representadas por instancias XML basadas en un esquema de definiciones XML desarrollado por los grupos de trabajo de OSS/J. Los documentos XML intercambiados a través de esta interfaz, son peticiones y respuestas XML que contienen el mapeo XML de los objetos de valor de la entidad gestionada encontrados en el JVT Session Bean.

Debe notarse que el modo de interacción de mensajes XML soporta esencialmente las mismas operaciones que el JVT Session Bean.

Los clientes pueden interactuar con aplicaciones OSS/J para crear documentos de instancia de una petición o requerimiento XML y comunicar este documento a la aplicación por medio de un JMS Text Message enviado a una cola de mensajes especifica. El cliente entonces espera una respuesta XML o una excepción escuchando en un JMS Reply Destination suministrado. [36]

5.1.2 API Inventario de Recursos (JSR 142: OSS Inventory API). Las funciones de inventario son una parte central de una solución OSS y un factor clave para la rápida implementación de nuevos servicios. Ellas proveen almacenamiento de datos de equipos físicos y configuraciones, topología de red, recursos lógicos, definición de servicios e instancias, información de cuenta del cliente, etc.

La variedad de información de inventario puede ser clasificada en varios grupos que definen diferentes funciones de inventario (por ejemplo: Inventario de Red, Inventario de Servicio). Cada función contiene su conjunto específico de relaciones y entidades de inventario, su lógica de negocios especifica e interactúa con diferentes subconjuntos de componentes OSS.

La integración de productos que implementan funciones de inventario específicas en una solución OSS end-to-end no es un propósito directo, y usualmente requiere funcionalidad basada en el cliente, difícil de extender y mantener. El intercambio de relaciones entre entidades de inventario almacenadas en diferentes repositorios es muy complejo debido a la incompatibilidad de APIs y diferentes modelos de información.

La meta primaria del API de inventario OSS es reducir el costo de integración de inventario de productos con otros componentes OSS y permitir el intercambio de información a través de los límites de los componentes de inventario.

El API de inventario provee interfaces basadas en J2EE/EJB para crear, remover, actualizar, buscar entidades de inventario, plantillas y asociaciones de entidades, permite también la búsqueda de meta datos y a los clientes recibir notificaciones de eventos de inventario. Adicionalmente soporta el monitoreo de utilización de recursos. [37]

5.1.3 API de Pruebas (Aún no desarrollado). El API de pruebas provee interfaces, para crear, modificar, suspender, y cancelar los trabajos de pruebas. El API de Pruebas podrá retornar

resultados de pruebas brutos o sino aplicar alguna computación de algoritmos a los resultados de pruebas brutos para producir un resultado más significativo. Desde la perspectiva del TMF eTOM, el API de gestión de pruebas provee interfaces que permiten a los clientes: crear modificar suspender y cancelar trabajos de pruebas, preguntar sobre trabajos de pruebas y su estado, ser informado del progreso de las pruebas, preguntar por el tipo de pruebas disponibles, preguntar por los resultados de las pruebas y recuperar resultados de pruebas almacenados.

5.1.4 API de Trouble Ticketing (JSR 162: OSS Trouble Ticket API). Un número de sistemas trouble ticket esta disponible en el mercado pero cada uno es accedido por un conjunto de APIs diferentes que necesitan integración con el cliente dentro del OSS. La meta del JSR es definir un API estándar, basado en J2EE que permita el rápido desarrollo de sistemas de trouble ticket comerciales.

EL API trouble ticket reúne los siguientes requerimientos funcionales:

- permite al cliente crear, remover o cancelar trouble tickets;
- permite a los clientes cambiar valores de los parámetros de los trouble tickets;
- permite a los clientes ser informados de cambios en los trouble tickets mediante notificaciones;
- permite recibir cualquier información desde el cliente o desde el servicio y desde aplicaciones de gestión de red como lo son el análisis de impacto del servicio y el análisis de causa raíz del sistema de monitoreo de alarmas y fallas;
- permite el rastreo del problema hasta la resolución y notificación de clientes cuando el problema ha sido resuelto y el ticket de problema clareado.

La especificación del API trouble ticket direcciona los siguientes aspectos:

- la especificación de los Enterprise Java Beans que exportan interfaces para los sistemas trouble ticket;
- la especificación del mecanismo para localizar interfaces;
- la especificación de mensajes basados en XML que podrán ser enviados a, y recibidos desde, un sistema trouble ticket;
- la especificación de eventos basados en objetos fuertemente tipiados y eventos basados en XML emitidos por un sistema trouble ticket, y
- la especificación de mecanismos de suscripción de eventos.[38]

5.1.5 API de Gestión de Fallas (JSR 263: Fault Management API). El API de gestión de Fallas (FM, Fault Management), es el API que esta orientado hacia la red. Este API interactuará con gestores de elementos, y/o gestores de sistemas y/o gestores de subred que proveen información de fallas cuando un evento indeseadado ocurre. Este API especifica la interfaz de configuración para detección de fallas incluyendo el formato y reporte de alarmas para permitir el descubrimiento, aislamiento, y corrección de problemas en la red.

Dentro de los APIs que han sido definidos por la iniciativa OSS a través de Java, la funcionalidad de gestión de fallas ha sido embebida dentro del API OSS de Calidad de Servicio. EL JSR del API FM es el primero de dos JSRs para separar la funcionalidad de gestión de fallas del API OSS de Calidad de Servicio. [39]

5.1.6 API de Calidad de Servicio (JSR 90: OSS Quality of Service API). Actualmente en el mercado se encuentran varios productos que gestionan partes de Calidad de Servicios. Ellos pueden ser integrados dentro de soluciones end-to-end, pero estos estilos de soluciones integradas son complejos y difíciles de lograr, debido a la carencia de estándares de integración. Por lo tanto la capacidad para reducir los esfuerzos de integración vía un conjunto de estándares y componentes de software reusables para ensamblar aplicaciones OSS en un tiempo muy corto es una atractiva perspectiva de todos los jugadores en el mercado de OSS.

Los proveedores de servicio que ofrecen servicios con una garantía de calidad requieren sistemas de gestión que puedan recuperar, calcular, y presentar datos de QoS desde las 4 áreas de desempeño de servicio (soporte, operabilidad, servilidad, operabilidad). Estos sistemas de gestión tienen que controlar los acuerdos de nivel de servicio (SLA, Service Level Agreements), entre los clientes y los proveedores de servicio, y reaccionar sobre violaciones de calidad de servicio de acuerdo a las reglas de negocio. Hoy en día existen productos para gestionar esto, pero no existen estándares de facto para facilitar la integración de sistemas de gestión de calidad de servicio con otros sistemas de gestión tales como mediación, facturación y activación del servicio, como parte de una solución total de gestión.

Para hacer más fácil la integración y desarrollo de soluciones de QoS totales, un número de interfaces pueden ser acordadas. Estas interfaces son definidas dentro de la Especificación del API OSS de QoS que permite la construcción de una solución total OSS de Calidad de servicio para ensamblar componentes comerciales.

Las soluciones de QoS requieren la especificación de muchas interfaces. La primera prioridad de la especificación de este API es dar frente a la red es decir estar orientada a ella. El API de QoS interactuará con sistemas gestores de red o con gestores de elemento de red que proveen información de QoS. [40]

5.2 MAPEO DE LA ARQUITECTURA DE LA INFORMACIÓN A APIS OSS/J

Para observar de forma mas clara la aplicación que tienen los APIs de OSS/J anteriormente mencionados, en el diseño del sistema de soporte de operaciones para gestión de fallas en redes móviles de 3G, se presenta un mapeo de las clases de objetos de información, e interfaces

presentadas en la arquitectura de la información del OSS.

5.2.1 EntidadMonitoreada

5.2.1.1 Clases de Objetos de Información

- **Entidad Monitoreada.** El equivalente en OSS/J de la Clase de Objeto de Información EntidadMonitoreada es la Interfaz ManagedElementValue del paquete ossj.inventory.infomodel.resource, el cual se encuentra en el API de Inventario OSS (JSR 142)[42]. La relación de atributos se muestra en la tabla 68.

Tabla 68. Atributos EntidadMonitoreada

Nombre de Atributo	Equivalente OSS/J
idEntidadMonitoreada	KEY
tipoEM	No hay equivalente
nombreUsuario	USER_LABEL
nombreVendedor	RESOURCE_BUSINESS_NAME
estado	No hay equivalente
localización	LOCATION_NAME
Versión	SYS_LEVEL_VERSION
Gestor	No hay equivalente
Redundancia	No hay equivalente
restablecimientoAutomático	No hay equivalente

- **NodoGestionado.** No se encontró equivalente con OSS/J

- **Subred.** El equivalente en OSS/J de la Clase de Objeto de Información SubRed es la Interfaz SubnetworkValue del paquete ossj.inventory.infomodel.resource, el cual se encuentra en el API de Inventario OSS (JSR 142)[42]. La relación de atributos se muestra en la tabla 69.

Tabla 69. Atributos Subred

Nombre de Atributo	Equivalente OSS/J
idSubRed	KEY
nombreUsuario	USER_LABEL
TipoRed	RESOURCE_BUSINESS_NAME

5.2.1.2 Interfaces Entidad Monitoreada

- **Interfaz EntidadMonitoreadaNotificacion1**
  nCambioValorAtributo. El equivalente en OSS/J de la interfaz nCambioValorAtributo es la Interfaz EntityValueAttributeChangeEvent del paquete javax.oss.inventory, el cual se encuentra en el API de Inventario OSS (JSR 142)[42].

- **Interfaz EntidadMonitoreadaNotificacion2**
  nCrearEntidadMonitoreada. El equivalente en OSS/J de la interfaz nCrearEntidadMonitoreada es la Interfaz EntityValueCreateEvent del paquete javax.oss.inventory, el cual se encuentra en el API de Inventario OSS (JSR 142)[42].

- **Interfaz EntidadMonitoreadaNotificacion3**
  nEliminarEntidadMonitoreada. El equivalente en OSS/J de la interfaz nEliminarEntidadMonitoreada es la Interfaz EntityValueRemoveEvent del paquete javax.oss.inventory, el cual se encuentra en el API de Inventario OSS (JSR 142)[42].

5.2.2 DiscriminadorEnvioEventos. El Discriminador de Envío de Eventos no se encuentra definido por OSS/J.

Las notificaciones nCrearDiscriminadorEnvioEvento, nEliminarDiscriminadorEnvioEvento, nCambioAtributo, nCambioEstadoAdmin y nCambioEstadoOper pueden ser implementadas a partir de la Interfaz IRPEvent del paquete javax.oss.util del API Común de OSS.

Las operaciones iniciarEnvioEvento, terminarEnvioEvento, modificarEnvioEvento y recuperarCondicionesEnvioEvento pueden ser implementadas a partir de la Interfaz JVTSession del paquete javax.oss del API Común de OSS [41].

5.2.3 FRC y RFRC. El Fichero Registro Cronológico y los Registros de Fichero Registro Cronológicos no están definidos en OSS/J, pero pueden ser implementados en Bases de Datos.

Las notificaciones del Registro de Fichero Registro nUmbralLimite, nDescartarRegistro, nRetornoOperacion, nCambioAtributo, nCreacionRegistro, nEliminacionRegistro, nCambioEOperacional y nCambioEAdministrativo pueden ser implementadas a partir de la Interfaz IRPEvent del paquete javax.oss.util del API Común de OSS[41].

Las operaciones nuevoRegistro, eliminarRegistro, modificarEstado, modificarAtributo, obtenerAtributo y obtenerRegistro pueden ser implementadas a partir de la Interfaz JVTSession del paquete javax.oss del API Común de OSS[41].

5.2.4 Inventario. El equivalente en OSS/J de la Clase de Objeto de Información Inventario es la Interfaz ResourceSpecificationValue del paquete javax.oss.cbe.resource, el cual se encuentra en el API de Inventario OSS (JSR 142)[42]. La relación de atributos se muestra en la tabla 70.

Tabla 70. Atributos Inventario

Nombre de Atributo	Equivalente OSS/J
IdInventario	KEY
tipoUnidad	PART_NUMBER
tipoUnidadVendedor	RESOURCE_BUSINESS_NAME
númeroUnidadVendedor	MODEL_NUMBER
nombreVendedor	VENDOR_NAME
Serial	SKU_NUMBER
fechaElaboración	No hay equivalente
fechaÚltimoServicio	No hay equivalente
posiciónUnidad	No hay equivalente
datosFábrica	No hay equivalente

5.2.5 AlarmaIRP

5.2.5.1 Clases de Objetos de Información AlarmaIRP

- **RegAlarma.** El equivalente en OSS/J de la Clase de Objeto de Información RegAlarma es la Interfaz AlarmValue del paquete javax.oss.fm.monitor, el cual se encuentra en el API de Calidad del Servicio OSS. La relación de atributos se muestra en la tabla 71.

Tabla 71. Atributos RegAlarma

Nombre de Atributo	Equivalente OSS/J
regAlarmaId	KEY
horaInicio	No hay equivalente
tipoAlarma	ALARM_TYPE
tipoAlarmaVendedor	No hay equivalente
causaProbable	PROBABLE_CAUSE
probEspecificos	SPECIFIC_PROBLEM
gravedadPercibida	PERCEIVED_SEVERITY
situaciónRespaldo	BACKED_UP_STATUS
objetoRespaldo	BACK_UP_OBJECT
infoUmbral	THRESHOLD_INFO
notificacionId	NOTIFICATION_ID
atributosSupervisados	MONITORED_ATTRIBUTES
reparacionesPropuestas	PROPOSED_REPAIR_ACTIONS
textoAdicional	ADDITIONAL_TEXT
estadoReconocimiento	ALARM_ACK_STATE
horaReconocimiento	ACK_TIME
usuarioReconocimiento	ACK_USER_ID
sistemaReconocimiento	ACK_SYSTEM_ID
usuarioClareo	No hay equivalente
sistemaClareo	No hay equivalente

- **Comentarios.** El equivalente en OSS/J de la Clase de Objeto de Información Comentarios es la Interfaz CommentValue del paquete javax.oss.fm.monitor, el cual se encuentra en el API de

Calidad del Servicio OSS [44]. La relación de atributos se muestra en la tabla 72.

Tabla 72. Atributos Comentarios

Nombre de Atributo	Equivalente OSS/J
usuarioId	Para el manejo de este atributo se emplea • setCommentUserId(String user_Id) • getCommentUserId()
sistemaId	Para el manejo de este atributo se emplea • setCommentSystemId(String system_Id) • getCommentSystemId()
texto	Para el manejo de este atributo se emplea • setCommentText(String text) • getCommentText()
fecha	Para el manejo de este atributo se emplea • setCommentTime(Date time) • getCommentTime()

- **NotificaciónCorrelacionada.** El equivalente en OSS/J de la Clase de Objeto de Información NotificaciónCorrelacionada es la Interfaz CorrelatedNotificationValue del paquete javax.oss.fm.monitor, el cual se encuentra en el API de Calidad del Servicio OSS [44].. La relación de atributos se muestra en la tabla 73.

Tabla 73. Atributos NotificaciónCorrelacionada

Nombre de Atributo	Equivalente OSS/J
fuente	Para el manejo de este atributo se emplea • setManagedObjectInstance(String moi) • getManagedObjectInstance()
identificadoresN	Para el manejo de este atributo se emplea • setNotificationIds(String[] ids) • getNotificationIds()

5.2.5.2 Interfaces AlarmaIRP

- **Interfaz AlarmaIRPNotificacion**

nNuevaAlarma. El equivalente en OSS/J de la interfaz nNuevaAlarma es la Interfaz NotifyNewAlarmEvent del paquete javax.oss.fm.monitor, el cual se encuentra en el API de Calidad del Servicio OSS [44]. La relación de atributos se muestra en la tabla 74.

Tabla 74. Atributos nNuevaAlarma

Nombre de Atributo	Equivalente OSS/J
Instancia de Objeto	MANAGED_OBJECT_INSTANCE
Id Notificación	NOTIFICATION_ID
Hora de evento	EVENT_TIME

Tipo de Notificación	No hay equivalente
Causa probable	PROBABLE_CAUSE
Severidad Percibida	PERCEIVED_SEVERITY
Tipo de Alarma	ALARM_TYPE
Tipo de Alarma del vendedor	No hay equivalente
Problemas Específicos	SPECIFIC_PROBLEM
Notificaciones Correlacionadas	CORRELATED_NOTIFICATIONS
Situación de respaldo	BACKED_UP_STATUS
Objeto de respaldo	BACK_UP_OBJECT
Información de umbral	THRESHOLD_INFO
Atributos monitoreados	MONITORED_ATTRIBUTES
Reparaciones propuestas	PROPOSED_REPAIR_ACTIONS
Texto adicional	ADDITIONAL_TEXT
Identificador de registro de alarma	No hay equivalente

nCambioEstado. El equivalente en OSS/J de la interfaz nCambioEstado es la Interfaz NotifyAckStateChangedEvent del paquete javax.oss.fm.monitor, el cual se encuentra en el API de Calidad del Servicio OSS [44]. La relación de atributos se muestra en la tabla 75.

Tabla 75. Atributos nCambioEstado

Nombre de Atributo	Equivalente OSS/J
Instancia de Objeto	MANAGED_OBJECT_INSTANCE
Id Notificación	NOTIFICATION_ID
Hora de evento	EVENT_TIME
Tipo de Notificación	No hay equivalente
Causa probable	PROBABLE_CAUSE
Severidad Percibida	PERCEIVED_SEVERITY
Tipo de Alarma	ALARM_TYPE
Identificador de registro de alarma	No hay equivalente
Estado de reconocimiento	ALARM_ACK_STATE
Usuario de reconocimiento	ACK_USER_ID
Sistema de reconocimiento	ACK_SYSTEM_ID

nClareoAlarma. El equivalente en OSS/J de la interfaz nClareoAlarma es la Interfaz NotifyClearedAlarmEvent del paquete javax.oss.fm.monitor, el cual se encuentra en el API de Calidad del Servicio OSS [44]. La relación de atributos se muestra en la tabla 76.

Tabla 76. Atributos nClareoAlarma

Nombre de Atributo	Equivalente OSS/J
Instancia de Objeto	MANAGED_OBJECT_INSTANCE
Id Notificación	NOTIFICATION_ID
Hora de evento	EVENT_TIME
Tipo de Notificación	No hay equivalente
Causa probable	PROBABLE_CAUSE
Severidad Percibida	PERCEIVED_SEVERITY

Tipo de Alarma	ALARM_TYPE
Notificaciones Correlacionadas	CORRELATED_NOTIFICATIONS
Usuario de Clareo	No hay equivalente
Sistema de clareo	No hay equivalente
Identificador de registro de alarma	No hay equivalente

nReconstruccionListaAlarmas. El equivalente en OSS/J de la interfaz nReconstruccionListaAlarmas es la Interfaz NotifyAlarmListRebuiltEvent del paquete javax.oss.fm.monitor, el cual se encuentra en el API de Calidad del Servicio OSS [44]. La relación de atributos se muestra en la tabla 77.

Tabla 77. Atributos nReconstrucciónListaAlarmas

Nombre de Atributo	Equivalente OSS/J
Instancia de Objeto	MANAGED_OBJECT_INSTANCE
Id Notificación	NOTIFICATION_ID
Hora de evento	EVENT_TIME
Tipo de Notificación	No hay equivalente
Razón	REASON

- **Interfaz AlarmaIRPNotificacion2**

nCambioAlarma. El equivalente en OSS/J de la interfaz nCambioAlarma es la Interfaz NotifyChangedAlarmEvent del paquete javax.oss.fm.monitor, el cual se encuentra en el API de Calidad del Servicio OSS [44]. La relación de atributos se muestra en la tabla 78.

Tabla 78. Atributos nCambioAlarma

Nombre de Atributo	Equivalente OSS/J
Instancia de Objeto	MANAGED_OBJECT_INSTANCE
Id Notificación	NOTIFICATION_ID
Hora de evento	EVENT_TIME
Tipo de Notificación	No hay equivalente
Causa probable	PROBABLE_CAUSE
Severidad Percibida	PERCEIVED_SEVERITY
Tipo de Alarma	ALARM_TYPE
Identificador de registro de alarma	RegAlarma.sistemaClareo

- **Interfaz AlarmaIRPNotificacion3**

nComentario. El equivalente en OSS/J de la interfaz nComentario es la Interfaz NotifyAlarmCommentsEvent del paquete javax.oss.fm.monitor, el cual se encuentra en el API de Calidad del Servicio OSS [44]. La relación de atributos se muestra en la tabla 79.

Tabla 79. Atributos nComentario

Nombre de Atributo	Equivalente OSS/J
Instancia de Objeto	MANAGED_OBJECT_INSTANCE
Id Notificación	NOTIFICATION_ID
Hora de evento	EVENT_TIME
Tipo de Notificación	No hay equivalente
Tipo de Alarma	ALARM_TYPE
Causa probable	PROBABLE_CAUSE
Severidad Percibida	PERCEIVED_SEVERITY
Comentarios	COMMENTS
Identificador de registro de alarma	No hay equivalente

- **Interfaz AlarmaIRPNotificacion4**

  nListaAlarmaDefectuosa. El equivalente en OSS/J de la interfaz nListaAlarmaDefectuosa es la Interfaz NotifyPotentialFaultyAlarmListEvent del paquete javax.oss.cbe.alarm, el cual se encuentra en el API Común de OSS [41]. La relación de atributos se muestra en la tabla 80.

Tabla 80. Atributos nListaAlarmaDefectuosa

Nombre de Atributo	Equivalente OSS/J
Instancia de Objeto	MANAGED_OBJECT_INSTANCE
Id Notificación	NOTIFICATION_ID
Hora de evento	EVENT_TIME
Tipo de Notificación	No hay equivalente

- **Interfaz AlarmaIRPOperacion 1, 2, 3, 4.** El equivalente en OSS/J de las operaciones de las Interfaces AlarmaIRPOperacion1, AlarmaIRPOperacion2, AlarmaIRPOperacion3 y AlarmaIRPOperacion4 se encuentra en la interfaz JVTAlarmMonitorSession del paquete javax.oss.fm.monitor del API de Calidad del Servicio OSS [44] y se muestran en la tabla 81.

Tabla 81. Operaciones Interfaz AlarmaIRPOperacion1-4

Operación	Equivalente OSS/J
obtenerListaAlarmas	queryAlarmList(QueryValue[] query, String[] attributes)
reconocerAlarmas	tryAcknowledgeAlarms(AlarmKey[] alarmReferenceList, String ackUserId, String ackSystemId)
numeroAlarmas	queryAlarmCounts(QueryValue[] query)
eliminarAlarma	tryUnacknowledgeAlarms(AlarmKey[] alarmReferenceList, String ackUserId, String ackSystemId)
agregarComentario	tryCommentAlarms(AlarmKey[] alarmReferenceList, String commentUserId, String commentText, String commentSystemId)

- **Interfaz AlarmaIRPOperacion5**

  clarearAlarma. Para esta operación no se encontró equivalente.

5.2.6 PruebasIRP. OSS/J no ha implementado el API de Pruebas, por tanto no se encuentran

definidas las clases de Objetos de Información de PruebaIRP, Ejecutante de Acción de Prueba, ObjetoPrueba ni Eventos de Prueba.

Las operaciones de las Interfaces OperacionesGestiónPruebaIRP (Extracción de Atributos, Modificación de Atributos y Aborto de Prueba) OperacionesdeControlPruebaIRP (Petición de Prueba, Suspención/Reanudación de Prueba y Terminación de Prueba) y OperacionesdeMonitoreoPruebaIRP (Monitoreo de Prueba, Resultado de Prueba y Conflicto de Planificación) pueden ser implementadas a partir de la Interfaz JVTSession del paquete javax.oss del API Común de OSS [41].

5.2.7 Trouble Ticketing

5.2.7.1 Clases de Objetos de Información Trouble Ticketing

- **InformeDificultades.** El equivalente en OSS/J de la Clase de Objeto de Información InformeDificultades es la Interfaz TroubleTicketValue del paquete javax.oss.trouble, el cual se encuentra en el API de Trouble Ticket OSS (JSR 91)[43]. La relación de atributos se muestra en la tabla 82.

Tabla 82. Atributos InformeDificultades

Nombre de Atributo	Equivalente OSS/J
idInformeDificultades	TROUBLETICKETKEY

- **InformeDificultadesTelecomunicaciones.** El equivalente en OSS/J de la Clase de Objeto de Información InformeDificultadesTelecomunicaciones es la Interfaz TroubleTicketValue del paquete javax.oss.trouble, el cual se encuentra en el API de Trouble Ticket OSS (JSR 91) [43]. La relación de atributos se muestra en la tabla 83.

Tabla 83. Atributos InformeDificultadesTelecomunicaciones

Nombre de Atributo	Equivalente OSS/J
objetoGestionado	TROUBLEDOBJECT
objetosSospechosos	SUSPECTOBJECTLIST
tipoDificultad	TROUBLETYPE
centroTrabajoCliente	No hay equivalente
numTiqueCliente	CUSTOMERTROUBLENUM
prioridadServicioTelecomunicaciones	No hay equivalente
direcciónAccesoUbicación	TROUBLELOCATIONINFOLIST
horasAccesoUbicación	
personaAccesoUbicación	
informaciónAdicional	ADDITIONALTROUBLEINFOLIST
claveBúsquedaGestor1	No hay equivalente
claveBúsquedaGestor2	
claveBúsquedaGestor3	

gravedadPercibida	PERCEIVEDTROUBLESEVERITY
prioridadPreferida	PREFERREDPRIORITY
tiempoDetección	TROUBLEDETECTIONTIME
modoIniciación	INITIATINGMODE
tiempoRecepción	RECEIVEDTIME
personaContactoAgente	SPROLEASSIGNMENTLIST
listaAlarmas	RELATEDALARMLIST
dificultadesAsociadas	RELATEDTROUBLETICKETKEYLIST
nombrePersonaResponsable	No hay equivalente
ubicaciónDificultad	TROUBLELOCATION
estadoInformeDificultades	TROUBLESTATE
duraciónInterrupción	OUTAGEDURATION
actividadesReparación	REPAIRACTIVITYLIST
textoLiquidación	CLOSEOUTNARR
autorizaciones	AUTHORIZATIONLIST
listaEscaladas	ESCALATIONLIST

- **ServicioGestiónRedCliente.** El equivalente en OSS/J de la Clase de Objeto de Información ServicioGestiónRedCliente es la Interfaz ServiceSpecificationValue del paquete javax.oss.cbe.service, el cual se encuentra en el API Común de OSS [41]. La relación de atributos se muestra en la tabla 84.

Tabla 84. Atributos ServicioGestiónCliente

Nombre de Atributo	Equivalente OSS/J
idServicio	No hay equivalente
aliasServicio	NAME
descripción	DESCRIPTION
perfilServicio	No hay equivalente
tipoServicio	No hay equivalente

- **ActividadReparación.** El equivalente en OSS/J de la Clase de Objeto de Información ActividadReparación es la Interfaz RepairActivity del paquete javax.oss.trouble, el cual se encuentra en el API de Trouble Ticket OSS (JSR 91) [43]. La relación de atributos se muestra en la tabla 85.

Tabla 85. Atributos ActividadReparación

Nombre de Atributo	Equivalente OSS/J
idActvidadReparación	No hay equivalente
actividadReparación	Para el manejo de este atributo se emplea • setActivityInfo(String activityInfo) • getActivityInfo()
códigoActividad	Para el manejo de este atributo se emplea • setActivityCode(int activityCode) • getActivityCode()
textoAdicional	No hay equivalente

5.2.7.2 Mapeo de Interfaces Trouble Ticket

- **Interfaz DificultadOperacion1**

  situaciónInformeDificultad. Para obtener la situación de un Informe de dificultades la Interfaz JVTTroubleTicketSession del paquete javax.oss.trouble, proporciona tres operaciones que permiten ver los atributos de uno varios informes, las cuales se muestran en la tabla 86.

Tabla 86. Operaciones situaciónInformeDificultad

Operación	Descripción
getTroubleTicketByKey(TroubleTicketKey key, String[] attrNames)	Obtiene un informe de dificultades dando el identificador y retorna solo los atributos pedidos.
getTroubleTicketsByKeys(TroubleTicketKey[] keys, String[] attrNames)	Obtiene varios informes de dificultades dando los identificadores y retorna solo los atributos pedidos.
getTroubleTicketsByTemplate(TroubleTicketValue template, String[] attrNames)	Obtiene varios informes de dificultades relacionados con el parámetro template y retorna solo los atributos pedidos.

- **Interfaces DificultadOperacion2 y DificultadOperacion3.** Para agregar (añadirInformaciónDificultad) o modificar (modificarAtributosDificultad) un informe de dificultades la interfaz JVTTroubleTicketSession del paquete javax.oss.trouble se tienen las siguientes operaciones de la tabla 87.

Tabla 87. Operaciones DifucultadOperación2 y DifucultadOperación3

Operación	Descripción
setTroubleTicketByValue(TroubleTicketValue value, boolean resyncRequired)	Fija un informe de dificultades dando los valores.
setTroubleTicketsByValues(TroubleTicketValue[] values, boolean resyncRequired)	Fija varios informes de dificultades cada uno con diferentes valores.
setTroubleTicketsByKeys(TroubleTicketKey[] keys, TroubleTicketValue value)	Fija varios informes de dificultades dando los identificadores y con los mismos valores.
setTroubleTicketsByTemplate(TroubleTicketValue template, TroubleTicketValue value)	Fija varios informes de dificultades relacionados con el parámetro template con los mismos valores
setTroubleTicketsByTemplates(TroubleTicketValue[] templates, TroubleTicketValue value)	Fija varios informes de dificultades relacionados con al menos uno de los parámetros template con los mismos valores
trySetTroubleTicketsByValues(TroubleTicketValue[] values, boolean resychRequired)	Mejor esfuerzo para fija varios informes de dificultades cada uno con diferentes valores.
trySetTroubleTicketsByKeys(TroubleTicketKey[] keys, TroubleTicketValue value)	Mejor esfuerzo para fija varios informes de dificultades con los mismos valores.
trySetTroubleTicketsByTemplate(TroubleTicketValue template, TroubleTicketValue value, boolean failuresOnly)	Mejor esfuerzo para fija varios informes de dificultades relacionados con el parámetro template con los mismos

	valores.
trySetTroubleTicketsByTemplates(TroubleTicketValue[] templates, TroubleTicketValue value, boolean failuresOnly)	Mejor esfuerzo para fija varios informes de dificultades relacionados con al menos uno de los parámetros template con los mismos valores.

- **Interfaz DificultadNotificación1**
  nIntroducciónInformeDificultades. La interfaz nIntroducciónInformeDificultades no se encuentra definida en OSS/J.

- **Interfaz DificultadNotificación2**
  nCambioValorAtributo. El equivalente en OSS/J de la interfaz nCambioValorAtributo es la Interfaz TroubleTicketAttributeValueChangeEvent del paquete javax.oss.trouble, el cual se encuentra en el API de Trouble Ticket OSS (JSR 91) [43].

- **Interfaz DificultadNotificación3**
  nNuevoInformeDificultad. El equivalente en OSS/J de la interfaz nNuevoInformeDificultad es la Interfaz TroubleTicketCreateEvent del paquete javax.oss.trouble, el cual se encuentra en el API de Trouble Ticket OSS (JSR 91) [43].

- **Interfaz DificultadNotificación4**
  nEliminarInformeDificultad. El equivalente en OSS/J de la interfaz nEliminarInformeDificultad es la Interfaz TroubleTicketCloseOutEvent del paquete javax.oss.trouble, el cual se encuentra en el API de Trouble Ticket OSS (JSR 91) [43].

5.2.8 HistorialDificultad. El Historial de dificultades no está definido por OSS/J, pero las operaciones examinarHistorialDificultades, nNuevoEventoHistorialDificultades y nEliminarEventoHistorialDificultades, pueden ser implementadas a partir de la Interfaz JVTSession del paquete javax.oss del API Común de OSS [41].

5.3 FUTURAS IMPLEMENTACIONES

Como se muestra en este capitulo, OSS/J tiene una alta compatibilidad en el diseño realizado del OSS para gestión de fallas y permite un fácil mapeo. Además deja observar claramente la aplicación que tiene esta tecnología en una futura implementación del diseño planteado, y la aplicación en general en este tipo de soluciones para redes de telecomunicaciones.

Queda en espera el API de Pruebas que aún no ha sido desarrollado por el JCP, pero se encuentra en la lista de sus próximas especificaciones a desarrollar. Por lo pronto este cometido del diseño

realizado para gestión de fallos puede ser implementado tomando como referencia el API Común.

En cuanto al API de Gestión de fallas, todavía no ha sido liberado, pero como se dijo anteriormente, este surge a partir de la separación de las clases de gestión de fallas que se encontraban antes en el API de Calidad de Servicio. Por lo tanto este cometido del diseño propuesto, puede ser realizado con el API de Calidad de Servicio mientras se espera su liberación.

Los demás APIs aplicables al OSS diseñado se encuentran disponibles en la página Web del Java Community Process, libres de costos.

6. CONCLUSIONES

- TMN es un modelo de gestión estandarizado que representa la mejor opción para la implementación de soluciones de gestión en redes de 3G debido a ventajas, como la concepción de una red de gestión separada de la red que se gestiona y el intercambio y procesamiento de la información sobre gestión que permite realizar actividades comerciales de manera eficaz.

- La Metodología de Especificación de Interfaz de Red de Gestión de Telecomunicaciones permite mediante sus tareas obtener resultados de forma ordenada y eficiente, llevando al diseñador por una serie de procesos como generación de directrices, descripción de servicios y objetivos de gestión, descripción del contexto de gestión, modelado de información y consolidación de la información disponible, hacia el diseño óptimo de la solución de gestión por medio de la utilización de estándares o normas internacionales que rigen en este campo, asegurando su real utilidad en una futura implementación.

- La utilización de estándares para el desarrollo del diseño del OSS para gestión de fallos permite asegurar que aunque en la actualidad en nuestro país no se han desarrollado redes de 3G, el diseño puede ser realmente implementable, ya que esta basado en normas Internacionales que le dan el respaldo y la fiabilidad. Adicionalmente permiten también que el diseño sea fácilmente adaptable a otro tipo de redes, haciendo los respectivos ajustes al nivel de elementos de red específico para cada una de estas.

- El eTOM es una herramienta excepcional que está en auge, utilizada por muchos desarrolladores de OSS para la implementación de soluciones de gestión, que proporcionó al diseño del OSS la información necesaria sobre los procesos que conforman la gestión de fallos facilitando la definición de los servicios y objetivos de gestión así como la definición de los cometidos de gestión. Una de los principales ventajas que presento la utilización de este marco de gestión fue dar al diseño la capacidad de reflejar la gestión de fallas hacia el cliente, al mismo tiempo que permite a la red obtener del cliente información que le da al OSS la posibilidad de una gestión integral en todas las capas de gestión.

- El estudio de los requerimientos de gestión en redes de 3G permite concluir que los cuatro pilares básicos en una solución de gestión de fallos son la gestión de alarmas, la gestión de inventario, la gestión de pruebas, y para reflejar toda esta información hacia los clientes de la red, la gestión de dificultades o trouble ticket.

- Dada la especificación de la versión 6 de la arquitectura UMTS de una red física soportada en

IP, el diseño de la arquitectura física se desarrollo sobre este protocolo que es de gran ventaja a la hora de construir la red de gestión, dado que en la actualidad existen gran cantidad de dispositivos que soportan esta tecnología, y que actualmente tiene gran difusión y es de conocimiento global.

- Al analizar que tecnología es la más conveniente para la posible implantación del OSS diseñado, se observa que no puede haber tecnología, más compatible que la suministrada por la iniciativa OSS/J para este tipo de desarrollos, ya que al igual que el diseño, esta orientada a objetos y basada en el marco del eTOM y la arquitectura TMN, de tal forma que suministra APIs con clases que se adaptan fácilmente al modelo de información presentado para el sistema de soporte de operaciones, y que además constituye una opción económica.

7. RECOMENDACIONES

- Aunque la información disponible sobre gestión de redes de comunicaciones es basta en cuanto a recomendaciones e investigaciones plasmadas en documentos, no se encuentra muchas soluciones en el mercado de las telecomunicaciones, ya que es un tema que esta aún emergiendo en cuanto a implementación. Actualmente la gestión de las redes de telecomunicaciones ha tomado mayor importancia, y es necesario que la en comunidad educativa del Programa de Ingeniería Electrónica y Telecomunicaciones de la Universidad del Cauca, se siga investigando y desarrollando implementaciones que permitan el crecimiento de la base de conocimientos en este campo.

- Este proyecto deja al grupo de Nuevas Tecnologías en Telecomunicaciones de la Universidad del Cauca, un diseño basado en estándares que permite una fácil integración con otros módulos además de su escalabilidad, por lo que se invita a la implementación de los cometidos de este diseño en soluciones independientes como por ejemplo: OSSs para gestión de Alarmas, OSSs para gestión de inventario, OSSs para gestión de pruebas, y soluciones para gestión de trouble tickets, teniendo en cuenta que el diseño desarrollado no solo es aplicable a redes de 3G sino a todas las redes de telecomunicaciones a las que se desee implementar un sistema de gestión basado en la arquitectura TMN, pero teniendo en cuenta lógicamente las adaptaciones necesarias en cuanto a la arquitectura funcional y física que se requieran, para dar cubrimiento a los elementos de gestión que presenta cada red.

- La gestión de fallas dentro del contexto de una red de gestión de Telecomunicaciones, es la base para que otros módulos de gestión desarrollen sus cometidos. Unos de estos módulos es la gestión de Calidad del Servicio y Aseguramiento del Servicio, que es uno de los propósitos esenciales por los cuales se gestiona fallas en las redes. Aunque este no era uno de los objetivos del proyecto, el OSS para gestión de fallos se realizó pensando en la continuidad de su desarrollo, en cuanto a su aplicación dentro de un Sistema integral de Gestión de Calidad y Aseguramiento del Servicio, por lo que se invita a seguir haciendo este desarrollo.

REFERENCIAS BIBLIOGRAFICAS

[1] Notas sobre TMN [en línea]. Argentina: Escuela de Ingeniería Electrónica, Universidad Nacional de Rosario. Mayo 2004. Disponibilidad en Internet: <www.eie.fceia.unr.edu.ar/ftp/Tecnologias%20de%20banda%20angosta/Notas_sobre_TMN.pdf>.

[2] SAUVE, Bernard. OSS integration and services [en línea]. ALCATEL. Francia: 2003.

[3] MARTINS, Vergílio Antonio y TUDE, Eduardo. Mapa de Processos de uma Operadora de Telecomunicações (eTOM) [en línea]. Teleco. Brasil. Noviembre de 2003. Disponibilidad en Internet: < http://www.teleco.com.br/tutoriais/tutorialetom/default.asp>.

[4] TeleManagement Forum. Mapa de Operaciones Telecom ampliado (eTOM) [en línea]. Versión 4.0. Febrero 2004. GB921.

[5] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES [CD-ROM]. Marco general para la gestión de las telecomunicaciones móviles internacionales-2000 (IMT-2000). UIT-R. 1995. 34p.: (UIT-R M.1168)

[6] HUÉLAMO PLATAS, Javier. Opciones Tecnológicas para la Gestión de Redes de Telecomunicaciones [en línea]. Micro/bit. Ediciones Técnicas Rede. España: enero 2002.

[7] LACUNZA PRIETO, Fernando. MAGAÑA LIZARRONDO, Eduardo. y MARTÍNEZ DE LIZARRONDO, Alfonso. Ventajas y desventajas del SNMP [en línea]. Disponiblilidad en Internet: < http://www.arrakis.es/~gepetto/redes/rog08p6.htm>.

[8] LOPEZ DE VERGARA, Jorge Enrique. Diseño e implementación de un sistema para la gestión de un aplicación distribuida de intermediación electrónica. Universidad Politécnica de Madrid. Madrid: septiembre de 1998. p 36-37.

[9] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES [CD-ROM]. Principios para una red de gestión de las telecomunicaciones. UIT-T. 1996. 87p.: (UIT-T M.3010)

[10] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES [CD-ROM]. Funciones de gestión de la red de gestión de las telecomunicaciones. UIT-T. 1997. 109p.: (UIT-T M.3400)

[11] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES [CD-ROM]. Metodología de

especificación de interfaz de la red de gestión de las telecomunicaciones. UIT-T. 1995. 34p.: (UIT-T M.3020)

[12] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES [CD-ROM]. Servicios de gestión de red de gestión de las telecomunicaciones y sectores gestionados de las telecomunicaciones: panorama general. UIT-T. 1997. 31p.: (UIT-T M.3200)

[13] INTERNATIONAL TELECOMMUNICATION UNION [CD-ROM]. Enhanced Telecom Operations Map® (eTOM) - The business process framework. ITU-T. 2004. 55p.: (ITU-T M.3050)

[14] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES [CD-ROM]. Tecnología de la información – Interconexión de sistemas abiertos – Servicio común de información de gestión. UIT-T. 1997. 43p.: (UIT-T X.710)

[15] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES [CD-ROM]. Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función señaladora de alarmas. CCITT. 1992. 26p.: (CCITT X.733)

[16] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES [CD-ROM]. Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de gestión de informe de evento. CCITT. 1993. 29p.: (CCITT X.734)

[17] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES [CD-ROM]. Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función control de ficheros registro cronológico. CCITT. 1993. 33p.: (CCITT X.735)

[18] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES [CD-ROM]. Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: categorías de pruebas de confianza y de diagnóstico. UIT-T. 1997. 73p.: (ITU-T X.737)

[19] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES [CD-ROM]. Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de gestión de prueba. UIT-T. 1995. 64p.: (ITU-T X.745)

[20] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES [CD-ROM]. Función de gestión de dificultades para aplicaciones del sector de normalización de las telecomunicaciones de la unión internacional de telecomunicaciones (UIT-T). UIT-T. 1996. 142p.: (ITU-T X.790)

[21] 3rd GENERATION PARTNERSHIP PROJECT [en línea]. Architecture Principles for Release 2000. 3GPP. 2000. 62p.: (TR 23.821). Disponibilidad en Internet:

<http://www.3gpp.org/ftp/Specs/archive/23_series/23.821/23821-101.zip>

[22] 3rd GENERATION PARTNERSHIP PROJECT [en línea]. Telecommunication management; Principles and high level requirements (Release 6). 3GPP. 2004. 45p.: (TS 32.101). Disponibilidad en Internet: <http://www.3gpp.org/ftp/Specs/archive/32_series/32.101/32101-610.zip>

[23] 3rd GENERATION PARTNERSHIP PROJECT [en línea]. Telecommunication management; Fault Management; Part 1: 3G fault management requirements (Release 6). 3GPP. 2003. 19p.: (TS 32.111-1). Disponibilidad en Internet: <http://www.3gpp.org/ftp/Specs/archive/32_series/32.111-1/32111-1-601.zip>

[24] 3rd GENERATION PARTNERSHIP PROJECT [en línea]. Telecommunication management; Fault Management; Part 2: Alarm Integration Reference Point (IRP): Information Service (IS) (Release 6). 3GPP. 2004. 40p.: (TS 32.111-2). Disponibilidad en Internet: <http://www.3gpp.org/ftp/Specs/archive/32_series/32.111-2/32111-2-650.zip>

[25] 3rd GENERATION PARTNERSHIP PROJECT [en línea]. Telecommunication management; Fault Management (FM); Part 4: Alarm Integration Reference Point (IRP): Common Management Information Protocol (CMIP) Solution Set (SS) (Release 6). 3GPP. 2005. 43p.: (TS 32.111-4). Disponibilidad en Internet: <http://www.3gpp.org/ftp/Specs/archive/32_series/32.111-4/32111-4-650.zip>

[26] 3rd GENERATION PARTNERSHIP PROJECT [en línea]. Telecommunication management; Generic Integration Reference Point (IRP) management: Information Service (IS) (Release 6). 3GPP. 2004. 15p.: (TS 32.312). Disponibilidad en Internet: <http://www.3gpp.org/ftp/Specs/archive/32_series/32.312/32312-620.zip>

[27] 3rd GENERATION PARTNERSHIP PROJECT [en línea]. Telecommunication management; Test management Integration Reference Point (IRP); Information Service (IS) (Release 6). 3GPP. 2005. 25p.: (TS 32.322). Disponibilidad en Internet: <http://www.3gpp.org/ftp/Specs/archive/32_series/32.322/32322-610.zip>

[28] 3rd GENERATION PARTNERSHIP PROJECT [en línea]. Telecommunication management; Configuration Management (CM); Generic network resources Integration Reference Point (IRP); Network Resource Model (NRM) (Release 6). 3GPP. 2005. 24p.: (TS 32.622). Disponibilidad en Internet: <http://www.3gpp.org/ftp/Specs/archive/32_series/32.622/32622-640.zip>

[29] 3rd GENERATION PARTNERSHIP PROJECT [en línea]. Telecommunication management; Inventory Management (IM) network resources Integration Reference Point

(IRP): Network Resource Model (NRM) (Release 6). 3GPP. 2005. 11p.: (TS 32.692). Disponibilidad en Internet: <http://www.3gpp.org/ftp/Specs/archive/32_series/32.692/32692-610.zip>

[30] HUÉLAMO PLATAS, Javier. Visión Arquitectural de la Tercera Generación de Móviles UMTS [en línea]. Centro de Investigación Corporativo Alcatel. Artículo publicado en la Revista Española de Electrónica. Madrid (España): Octubre de 2000. Disponibilidad en Internet: < http://www.umtsforum.net/mostrar_articulos.asp?u_action=display&u_log=15>

[31] MORENO, Manuel. ÁLVAREZ, Martín Manuel. y SANZ, Joan Vinyes. Propuesta de utilización de SIP como protocolo de señalización en la red de acceso radio de sistemas [en línea]. UMTS. AHCIET, 2002. p 74.

[32] 3rd GENERATION PARTNERSHIP PROJECT [en línea]. Telecommunication management; Architecture (Release 6). 3GPP. 2004. 40p.: (TS 32.102). Disponibilidad en Internet: <http://www.3gpp.org/ftp/Specs/archive/32_series/32.102/32102-630.zip>

[33] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES [CD-ROM]. Tecnología de la información – Interconexión de sistemas abiertos – El directorio: visión de conjunto de conceptos, modelos y servicios. UIT-T. 1995. 29p.: (ITU-T X.500)

[34] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES [CD-ROM]. Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de gestión de objetos. CCITT. 1993. 32p.: (CCITT X.730)

[35] RAYMER, Dave. The OSS through Java™ API Roadmap [en línea]. OSS through JAVA Initiative. Version 3.0.1. March 2005. Disponibilidad en Internet: <http://www.ossj.org/downloads/docs/wp_ossj_api_roadmap.pdf>.

[36] PERROT, Vincent. OSS Common API Overview [en línea]. OSS through Java™ Initiative. Version 1.1. 2005. Disponibilidad en Internet: <http://jcp.org/en/jsr/detail?id=144>.

[37] JSR 142: OSS Inventory API [en línea]. Java Community Process. 2002.<http://jcp.org/en/jsr/detail?id=142>.

[38] JSR 162: OSS Trouble Ticket API [en línea]. Java Community Process. 2001. <http://jcp.org/en/jsr/detail?id=162>.

[39] JSR 263: Fault Management API [en línea]. Java Community Process. 2004. <http://jcp.org/en/jsr/detail?id=144>.

[40] JSR 90: OSS Quality of Service API [en línea]. Java Community Process. 2001. <http://jcp.org/en/jsr/detail?id=90>.

[41] PERROT, Vincent. OSS Common API. OSS through Java™ Initiative. Version 1.1. 2005. Disponibilidad en Internet: <http://jcp.org/en/jsr/detail?id=144>. JSR 144.

[42] GAUTHIER, Pierre. OSS Inventory API. User's Guide (Part 2). OSS through Java™ Initiative. Version 1.0. 2005. Disponibilidad en Internet: <http://jcp.org/en/jsr/detail?id=142>. JSR 142.

[43] GAUTHIER, Pierre. Trouble Ticket API. Trouble Ticket API Interface Definitions. OSS through Java™ Initiative. Version 1.0. February, 2002. Disponibilidad en Internet: <http://jcp.org/en/jsr/detail?id=91>. JSR90.

[44] ABERG Stefan, OSS Quality of Service API. Java Reference Part 3. OSS through Java™ Initiative. Versión 1.0. 2001. Disponibilidad en Internet: <http://jcp.org/en/jsr/detail?id=91>. JSR162.