UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

ÁREA TÉCNICA

TITULACIÓN DE INGENIERO EN SISTEMAS INFORMÁTICOS Y COMPUTACIÓN

Implementación de NOC para el monitoreo de Servicios e Infraestructura de Redes para el Banco de Loja, basado en Software Libre

TRABAJO DE FIN DE TITULACIÓN

AUTOR: Solís Álvarez, Camilo Javier

DIRECTOR: Aguilar Mora, Carlos Darwin, Ing.

LOJA – ECUADOR

2014

APROBACIÓN DEL DIRECTOR DEL TRABAJO DE FIN DE TITULACIÓN

Ingeniero
Carlos Darwin Aguilar Mora
DOCENTE DE LA TITULACIÓN

De mi consideración:

El presente trabajo de fin de titulación: “Implementación de NOC para el monitoreo de Servicios e Infraestructura de Redes para el Banco de Loja, basado en Software Libre” realizado por Solís Álvarez Camilo Javier, ha sido orientado y revisado durante su ejecución, por cuanto se aprueba la presentación del mismo.

Loja, Marzo 2014

Ing. Carlos Darwin Aguilar Mora
DOCENTE DE LA TITULACIÓN

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS

"Yo Solís Álvarez Camilo Javier declaro ser autor del presente trabajo de fin de titulación: "Implementación de NOC para el monitoreo de Servicios e Infraestructura de Redes para el Banco de Loja, basado en Software Libre", de la Titulación Sistemas Informáticos y Computación, siendo el Ingeniero Carlos Darwin Aguilar Mora director del presente trabajo; y eximo expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales. Además certifico que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de mi exclusiva responsabilidad.

Adicionalmente declaro conocer y aceptar la disposición del Art. 67 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que en su parte pertinente textualmente dice: "Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad"

_____

Camilo Javier Solís Álvarez
1104246291

DEDICATORIA

El presente trabajo tiene un poco de cada persona que me ha acompañado a lo largo de esta vida. Un par de ellas, son mis padres: Janneth y Julio quienes han sido mi ejemplo de superación y fuerza motora para cumplir mis metas.

A mis hermanos María Palmira e Israel quienes siempre me motivan para seguir adelante, con quienes he compartido grandes momentos. A los hermanos que me regaló la vida: Samantha, Juliana, Verito y Alejandro que por los caminos del destino formamos un vínculo de hermandad.

A mi Papito Pepe(†) y Mamita Palmira, mis abuelitos, quienes me enseñaron que con honestidad, constancia y trabajo se puede llegar lejos. A los que admiro por tener pensamientos adelantados a su época y por esa fuerza para buscar las oportunidades pese a la adversidad.

A mi otra mamá, Consuelo(†) quien siempre me motivo para seguir mis sueños.
A toda mi familia y amigos por sus consejos y apoyo incondicional en todo momento, a todas(os) ellas(os) mis infinitas gracias.

AGRADECIMIENTO

Gracias Dios por darme la vida, por la familia y por las bendiciones que he recibido para poder cumplir con este sueño.

A mis padres, por darme la oportunidad de vivir, por los sacrificios que han hecho para sacarnos adelante a mí y a mis hermanos. A ellos que por su perseverancia, su ejemplo de superación, por sus esfuerzo formaron un hogar de amor y armonía. Mis hermanos que siempre me brindaron su apoyo incondicional, sus consejos, sus risas y locuras que hemos compartidos.

A todos los profesores por haber compartido sus conocimientos y prepararme profesionalmente.

Al Ing. Carlos Aguilar y Carlos Córdova Erreis, director y codirector de tesis respectivamente quienes me supieron guiar en todo momento para el desarrollo de la tesis.

Al Banco de Loja que me acogió y en especial al Ing. Leonardo Burneo GERENTE GENERAL quién abrió las puertas para poder desarrollar la presente tesis. Al Ing. Manuel Lara e Ing. Boris Díaz del ÁREA DE SISTEMAS quienes siempre me apoyaron con los recursos e información necesarios para el desarrollo del proyecto. Además, a mis excompañeros del Centro de Cómputo por su disposición y ayuda.

A mis amigos(as) con quienes compartí anécdotas, amanecidas, farras, campeonatos, viajes….

ÍNDICE DE CONTENIDOS

CARATULA i
APROBACIÓN DEL DIRECTOR DEL TRABAJO DE FIN DE TITULACIÓN ii
DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS iii
DEDICATORIA iv
AGRADECIMIENTO v
ÍNDICE DE CONTENIDOS vi
ÍNDICE DE FIGURAS xi
ÍNDICE DE TABLAS xii
RESUMEN 1
ABSTRACT 2
INTRODUCCIÓN 3
OBJETIVOS 5
Objetivo General 5
Objetivos Específicos 5
1. MARCO TEÓRICO 6
1.1. Concepto de Administración de Redes 7
1.2. Elementos de un Sistema de Administración de Redes 7
1.2.1. El gestor. 8
1.2.2. El agente. 8
1.2.3. La MIB. 8
1.2.4. El protocolo. 8
1.3. Modelos de Gestión De Red 9
1.3.1. Modelo Aislado. 9
1.3.2. Modelo Coordinado. 9
1.3.3. Modelo Integrado. 9
1.4. Evolución de Los Sistemas de Administración 9
1.4.1. Redes Autónomas. 10
1.4.2. Redes Centralizadas 10
1.4.3. Redes Integradas 11
1.5. Estándares de Administración de Red 12
1.5.1. Gestión de Red OSI. 13
2. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED DEL BANCO DE LOJA 60
2.1. Introducción a la Empresa 61
2.1.2. Ubicación 61
2.2. Organigrama departamental del Área De Sistemas 63
2.3. Infraestructura Disponible 64

2.3.1. Servidores 64
2.3.2. Cuarto de Equipo 65
2.3.3. Equipos de Ruteo 65
2.4. Direccionamiento IP 66
2.5. Topología de Red 66
2.5.1. Cableado Estructurado 66
2.5.2. Cableado Vertical 67
2.6. Esquema de Red 67
2.7. Enlaces 69
2.7.1. Enlaces Internos 69
2.7.2. Enlaces Externos 70
2.7.3. Enlaces a Internet 70
2.8. Diagrama de una Agencia 71
2.9. Situación actual del Banco de Loja. 71
2.10. Herramientas Instaladas 74
2.10.1. PRTG. 74
2.10.2. ARANDA. 74
2.11. Administración de Seguridad 75
2.12. Problemática 75
2.13. Criterios de Evaluación para escogerl Herramienta de Monitoreo 76
2.14. Funcionalidades para escoger la herramienta de monitoreo 77
2.14.1. Funcionalidades Generales 77
2.14.2. Funcionalidades Específicas 78
3. PLAN DE APLICABILIDAD PARA EL CENTRO DE OPERACIONES DE RED DEL BANCO DE LOJA 79
3.1. Levantamiento de Requerimientos y Especificaciones 80
3.1.1. Descripción de Requerimientos. 80
3.1.1.1. Respuesta a Fallos. 80
3.1.1.2. Manejo de Infraestructura de Red. 80
3.1.1.3. Monitoreo de la Red. 81
3.1.1.4. Análisis de Datos. 81
3.1.1.5. Seguridad. 81
3.2. Definición de Roles de Usuarios 82
3.2.1. Gerente de Sistemas. 82
3.2.2. Jefe del Centro de Cómputo. 82
3.2.3. Supervisor Service Desk. 82
3.2.4. Técnico Infraestructura Tecnológica. 83

3.2.5. Técnico de Telecomunicaciones. 83
3.2.6. Operador y Soporte a Usuarios. 83
3.2.7. Supervisor de Seguridad. 84
3.3. Especificaciones de información y Equipos/Servicios a ser Monitoreados 84
3.3.1. Definición de Umbrales. 85
3.3.2. Métricas para el Servidor de Correos. 86
3.4. Descripción de Áreas Funcionales del NOC 87
3.4.1. Diseño de Análisis de Datos. 87
3.4.2. Diseño de Análisis de Configuración 88
3.4.3. Diseño de Análisis de Rendimiento 88
3.4.4. Diseño de Análisis de Contabilidad 88
3.4.5. Diseño de Gestión de Fallos 88
3.4.5.1. Monitoreo de Alarmas 89
3.4.5.2. Detección 90
3.4.5.3. Aislamiento 91
3.4.5.4. Diagnosticar 91
3.4.5.5. Corrección de Fallas 91
3.4.5.6. Tiempos de Solución a Fallos 92
3.4.5.7. Niveles de Criticidad en Fallas 92
3.4.5.8. Tiempos actuales de solución de requerimientos. 94
3.4.5.9. Documentación 95
4. DISEÑO DE INFRAESTRUCTURA IT 96
4.1. Aplicación del modelo de Gestión De Red 97
4.1.1. Creación del SLA para Manejo de Requerimientos por Problemas de Elementos de Red, Servicios y/o Servidores (Infraestructura de Red). 97
4.1.2. Implementación de la Metodología de Red. 99
4.1.3. Gestión de Rendimiento. 102
4.1.4. Gestión de Contabilidad. 105
4.1.5. Gestión de Seguridad. 108
4.1.6. Gestión de Configuración. 112
4.1.7. Gestión de Fallos. 116
4.2. Gestión de Incidentes 119
4.2.1. Proceso Gestión de Incidentes. 119
4.2.2. Registro y Clasificación de Incidentes. 119
4.2.3. Control del Proceso. 123
4.2.4. Clasificación del Incidente. 125
4.3. Infraestructura Física. 127

4.4. Infraestructura Tecnológica. 127
4.4.1. Servidores para instalación de NAGIOS. 127
4.4.2. Selección Herramientas a utilizar. 128
4.4.2.1. Definición y Evaluación de Herramientas. 128
4.4.2.1.1. Cumplimiento de Criterios de Evaluación para Escoger la Herramienta de Monitoreo. 131
4.4.2.1.2. Cumplimiento de Funcionalidades que debe tener la Herramienta de Monitoreo. 135
4.4.2.1.4. Funcionalidades Específicas. 136
4.4.2.1.5. Descripción de cada una de las funcionalidades que debe de cumplir la Herramienta de Monitoreo. 137
4.4.2.1.6. Cuadro de Evaluación Técnica de Herramientas. 140
4.4.2.1.7. Algunas otras características propuestas. 142
5. CONNOTACIONES FINALES 147
5.1. Discusión 148
5.2. Trabajos Futuros 150
CONCLUSIONES 151
RECOMENDACIONES 153
BIBLIOGRAFÍA 155
ANEXOS 160
1. ANEXO 1 160
1.1. Normas y Estándares Utilizados 160
2. ANEXO 2 163
2.1. Reportes De Monitoreo 163
3. ANEXO 3 172
3.1. Configurar SNMP en Gnu\Linux 172
4. ANEXO 4 186
4.1. Ingreso de Casos a Aranda 186
5. ANEXO 5 195
5.1. Plantilla para el Ingreso de Requerimientos. 195
6. ANEXO 6 196
6.1. Selección de la Distribución Linux 196
7. ANEXO 7 199
7.1. Sistemas de Gestión De Red 199
7.2. Herramientas Analizadas 199
7.3. Congruencia de Herramientas 215
8. ANEXO 8 216

8.1. Configuraciones generales de NAGIOS 216
En el Servidor 216
NAGIOS 216
En el Cliente 220
GLOSARIO DE TÉRMINOS 222

ÍNDICE DE FIGURAS

Ilustración 1: Elementos de Administración de una red 7
Ilustración 2: Redes Autónomas 10
Ilustración 3: Redes Centralizadas 11
Ilustración 4: Redes Integradas 12
Ilustración 5: División de Gestión de Redes. Tomada de (Electrónica, 1997) 13
Ilustración 6. Modelos arquitectura OSI 13
Ilustración 7: Submodelos Propuesto por (Irastorza, Gestión de Red, 2008) 14
Ilustración 8: Submodelo Funcional de la Arquitectura OSI (Alejandro, 2009) 15
Ilustración 9: Roles del Administrador y Agente 17
Ilustración 10: Dominio Organizacional y Dominio Organizativo 17
Ilustración 11. Áreas funcionales de un NOC 26
Ilustración 12: SLA's para ingreso de Falla en la red 28
Ilustración 13. Detección Proactiva – Reactiva 32
Ilustración 14. Detección Reactiva 33
Ilustración 15: Arquitectura CMIP 37
Ilustración 16: Sistema de Gestión de Red basada en el CMIP / CMIS 39
Ilustración 17: Sistema de Gestión CMIP / CMIS vs. SNMP 40
Ilustración 18: Ejes transversales para la implementación de un NOC (Diseño Personal) 42
Ilustración 19: Áreas Funcionales con respecto a modelo de capas 46
Ilustración 20: Árbol de la Infraestructura MIB 48
Ilustración 21: Ubicaciones a Nivel Nacional 61
Ilustración 22: Distribución de cada una de las Agencias 63
Ilustración 23: Organigrama Departamental Área de Sistemas 63
Ilustración 24: Esquema de Red 68
Ilustración 25: Diagrama Básico de una Agencia 71
Ilustración 26: Diagrama de Ingreso de Requerimientos 72
Ilustración 27: Gestión de Requerimientos (Diseño Propio) 73
Ilustración 28: Método del Percentil (Vicente, Análisis de Rendimiento - Servicios de Red) 86
Ilustración 29: Estadística SENDMAIL 86
Ilustración 30: Procesos de Detección de Fallas (Diseño Propio) 89
Ilustración 31: Localización de Problemas de Red (Irastorza, Grupo de Ingeniería Telemática, 2008) 90
Ilustración 32: Manejo de Incidentes de Red (Diseño Propio) 97
Ilustración 33: Workflow Ingreso de Requerimiento (Diseño Propio) 98
Ilustración 34: Gestión de Requerimientos (Diseño Propio) 99
Ilustración 35: Funciones de un NOC 99
Ilustración 36: Generalizando que es un NOC 101
Ilustración 37: Procedimiento de Gestión de Seguridad. 108
Ilustración 38: Proceso de Gestión de Incidentes basado en ITIL 119
Ilustración 39: Proceso de Manejo de Incidentes basado en ITIL 125
Ilustración 40: Severidad de las alarmas (IMPACTO)= URGENCIA 126
Ilustración 41: Reporte enviado por INTERNETVISTA. 166
Ilustración 42: Reporte enviado diariamente. 170
Ilustración 43: PRTG Instalado para monitoreo de BW. 171

ÍNDICE DE TABLAS

Tabla 1: *Estados de los Casos y su Descripción* 44
Tabla 2: *Tipos de Datos Primitivos ASN. 1* 59
Tabla 3: *Servidores Internos* 64
Tabla 4: *Servidores en cada Agencia* 65
Tabla 5: *Equipos de ruteo existentes* 65
Tabla 6: *Enlaces Locales* 69
Tabla 7: *Enlaces Remotos - Agencias* 70
Tabla 8: *Dispositivos a ser monitoreados (Diseño Propio)* 84
Tabla 9: *Umbrales Determinados (Diseño Personal)* 87
Tabla 10: *Niveles de Criticidad* 92
Tabla 11: *Valoración de Criticidad de acuerdo al tipo de falla* 93
Tabla 12: *Tiempo de Resolución de Requerimientos* 94
Tabla 13: *Gestión de Rendimiento* 103
Tabla 14: *Gestión de Contabilidad.* 106
Tabla 15: *Gestión de Seguridad* 110
Tabla 16: *Gestión de Configuración* 113
Tabla 17: *Gestión de fallos* 117
Tabla 18: *Colores de Casos ARANDA* 121
Tabla 19: *Estados usados por el Centro de Cómputo (de acuerdo a la Tabla 18)* 121
Tabla 20: *Niveles de Criticidad* 127
Tabla 21: *Tiempos resultantes al realizar Instalación NMS* 129
Tabla 22: *Historial de Actualización NAGIOS (Tomado de http://www.NAGIOS.org/projects/NAGIOScore/history/core-3x)* 130
Tabla 23: *Tabla de Escalas de Valoración* 135
Tabla 24: *Evaluación de Funcionalidades Generales* 135
Tabla 25: *Evaluación de Funcionalidades Específicas* 136
Tabla 26: *Plataformas Soportadas por NAGIOS* 138
Tabla 27: *Cuadro de cumplimiento de Funcionalidades Generales* 140
Tabla 28: *Evaluación Técnica de Herramientas* 140
Tabla 29: *Otras Características propuestas.* 142
Tabla 30: *Normas y estándares aplicables a la Gestión OSI* 160
Tabla 31: *Normas y estándares aplicables a la Gestión TMN* 161
Tabla 32: *Normas y estándares aplicables a la Gestión Internet* 162
Tabla 33: Evaluación del Sistema Operativo 197
Tabla 33: *Requerimientos de Hardware Zabbix* 202
Tabla 34: *Requerimientos de Software Zabbix* 202
Tabla 35: *Plataformas de ejecución de Servidor/Agente Zabbix* 203

Tabla 36: *Requerimientos de Hardware JFFNMS* 205
Tabla 37: *Requisitos Software JFFNMS* 205
Tabla 38: *Plataformas de ejecución de Servidor/Agente JFFNMS* 206
Tabla 39: *Requerimientos de Hardware Nagios* 209
Tabla 40: Requerimientos Software Nagios 209
Tabla 41: *Plataformas de ejecución de Servidor/Agente Nagios* 210
Tabla 42: *Requerimientos de Hardware Pandora FMS* 212
Tabla 43: *Requerimientos Software Pandora* 212
Tabla 44: *Plataformas de ejecución de Servidor/Agente Pandora* 212
Tabla 45: *Requerimientos de Hardware Zenoss* 214
Tabla 46: *Requerimientos de Software Zenoss* 214
Tabla 47: *Estados de los servicios* 220

RESUMEN

Hoy en día el desafío que tienen las empresas es que todos sus servicios estén disponibles 24 horas los 7 días de la semana (24/7); preocupándose siempre que éstos sean de calidad, eficientes y oportunos. Brindando siempre confianza, seguridad y corresponsabilidad a los clientes.

Analizando la realidad del Banco de Loja, se propone un Proyecto de Monitoreo de Servicios que ayude a solventar esta necesidad de forma: efectiva y controlada. Mantener una estadística de los servicios que posee el Banco permitiendo actuar rápida y oportunamente ante cualquier eventualidad que pueda suceder.

Toda la información histórica de: servicios, servidores, dispositivos de red, enlaces, etc.; tomada mediante el monitoreo permitirá tener una base de conocimiento sobre resolución de incidentes para estar preparados y priorizar aquellos servicios o infraestructura que se encuentren más sensibles a fallas y poder tomar a tiempo las medidas correctivas.

Lo que se contempla en este proyecto para el Banco de Loja S.A., se tiene previsto la utilización de Herramientas de Software Libre para todos los servicios que tiene; dando prioridad aquellos servicios que tenga que interactuar con clientes.

Palabras Claves: información, servicios, base de conocimiento

ABSTRACT

Today, the big challenge for companies is that all its services are available 24 hours - 7 days a week (24/7), provided that these are worrying quality, efficient and timely. Trying to bring confidence, security to customers.

Analyzing the reality at the Banco de Loja, is proposing a Project Monitoring Services to help address this need so: effective and controlled. Maintain statistical services held by the Bank allowing quick and timely respond to any eventuality that may happen.

All historical information, Services, servers, network devices, links, etc., taken by monitoring will have a knowledge base about solving incidents for be prepared and prioritize those services or infrastructure that are more sensitive to power failures and take time corrective measures.

What is contemplated in this project for Banco de Loja SA, plans to use Free Software Tools for all services having; prioritizing those services need to interact with customers.

Keyswords: information, services, knowledge base.

INTRODUCCIÓN

El presente proyecto nace como la necesidad primordial del Banco de Loja de tener un Sistema Integral de monitoreo para toda su infraestructura TI, que incluya características como: monitoreo de diferentes tipos de dispositivos, recursos, servicios y que la gestión de redes lo realice mediante el protocolo SNMP, logrando así conocer la salud de la red el mayor tiempo.

Además este proyecto permite integrar herramientas existentes en el Banco como es el ARANDA que es un Sistema para Manejo de Requerimientos (HELPDESK) que con este proyecto permite ayudar sustancialmente a las labores de la gestión de la red.

En este trabajo se recoge información sobre: estándares del NOC, SLA's para manejo de requerimientos, investigación y selección del NMS, instalación y configuración de la herramienta, pruebas y monitoreo, finalizando con algunas conclusiones y recomendaciones; seguidamente se hace mención de trabajos futuros relacionados con la gestión de redes. Todos estos temas se encuentran distribuidos en el presente documento de la siguiente manera:

Marco Teórico: se realiza un estudio de los conceptos referentes a la gestión de redes: componentes, protocolos, áreas funcionales, actividades de un NOC.

Situación actual: se muestra un vistazo a la situación actual del Banco de Loja, su infraestructura y organización, una vez conocida la situación actual se realiza una listado de necesidades y se especifica los requerimientos a cumplir en el presente proyecto.

Plan de aplicabilidad para el Centro de Operaciones de Red del Banco de Loja: se define requerimientos, los roles de los usuarios, se describe las áreas funcionales que debe tener el NOC, finalmente en base a ciertos criterios definidos por el Departamento de Sistemas se evalúa y selecciona la herramienta para el NOC.

Diseño de la infraestructura TI: se realiza una descripción de la aplicación a nivel general, cumplimiento de requerimientos, implementación de la herramienta en un entorno de pruebas, preparación del entorno, instalación y configuración de NAGIOS en un servidor del Centro de Cómputo, se realiza la documentación respectiva de las pruebas de monitoreo efectuadas en el servidor NOC.

Connotaciones Finales: en donse se incluye ropone algunos trabajos que se puedan desarrollar como proyectos dentro del Departamento de Sistemas o como futuras investigaciones. Finalmente, se determinan algunas conclusiones y recomendaciones del proyecto y citas bibliográficas en las que se ha sustentado el presente trabajo.

OBJETIVOS

Objetivo General

- Implementación de NOC para el monitoreo de servicios e infraestructura de redes para el Banco de Loja, basado en Software Libre.

Objetivos Específicos

- Levantar un estado del arte sintético de todos los conceptos, procesos, metodologías de un NOC.
- Analizar y conocer el esquema y estado actual de los Servicios de Red que posee el Banco de Loja S.A.
- Identificar herramientas de código abierto con buenas prestaciones para el monitoreo de la infraestructura que posee el Banco de Loja S.A.
- Definir Procedimientos para: monitoreo, fallas y seguimiento de incidentes con respecto a servicios que presta el Banco de Loja.
- Crear Políticas para: manejo de recursos de TI, Monitoreo de Servicios, Seguimiento de Incidentes. Además, crear polícas con la descripción de comptencias de Recurso Humano.
- Implementación y configuración de la solución de monitoreo (NOC) que mejor se adapten a la infraestructura que posee el Banco de Loja S.A.
- Levantar una base de datos estadística de los servicios que sirva para la toma de decisiones por parte de la Gerencia de Sistemas y Auditoria Informática.
- Efectivizar el uso de recursos tanto de Hardware, Software y de Red mediante la implementación del NOC.
- Levantar procesos que se realiza dentro del Área de Sistemas para el manejo de incidentes de infraestructura y de red, seguimiento de fallas y resolución de problemas dentro del monitoreo de servicios.
- Preparar al RR.HH. para que tenga conocimientos en:
    - Gestión de Monitoreo
    - Gestión de Análisis de Requerimientos
    - Gestión de Configuración de Herramientas
    - Gestión de Manejo de Fallas.

1. MARCO TEÓRICO

1.1. Concepto de Administración de Redes

Según (ALTAMIRANO, 2005)[1], la administración de redes es definida como la suma total de todas las políticas, procedimientos que intervienen en la planeación, configuración, control, monitoreo de los elementos que conforman a una red con el fin de asegurar el eficiente y efectivo empleo de sus recursos.

En lo personal, la administración de redes es un conjunto de técnicas que permita controlar, supervisar y mantener de forma operativa una red, mediante el uso de herramientas de gestión, control y monitoreo; además, permite diseñar procedimientos y ejecutar políticas para optimizar la infraestructura IT, manteniendo la continuidad y calidad de servicios de una organización.

La administración provee de lineamientos para estar preparados a posibles fallas o errores que pueda tener la infraestructura; así mismo, tomar medidas preventivas o correctivas para mitigar su mal funcionamiento.

1.2. Elementos de un Sistema de Administración de Redes

Los elementos de administración de redes (Ilustración 1: Elementos de Administración de una red) son:

- El gestor
- El agente
- La MIB
- El Protocolo

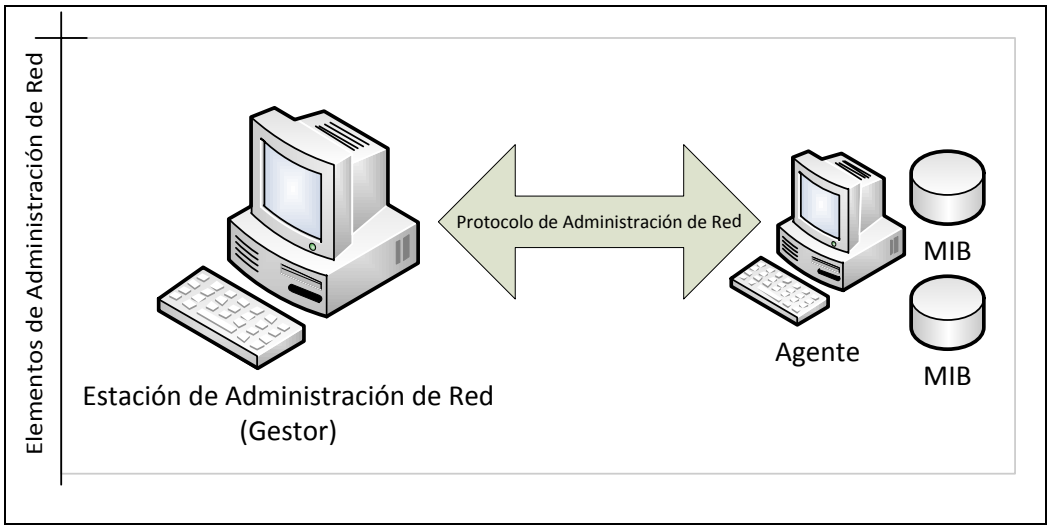


Ilustración 1: Elementos de Administración de una red[2]

[1]ALTAMIRANO, CARLOS VICENTE, "Un Modelo funcional para el Centro de operación de RedUNAM (NOCUNAM)", Julio 2003, UNAM - DGSCA.

[2]Adolfo Alberto Gomez Santos, «Gestion De Redes», accedido 23 de enero de 2012, http://www.slideshare.net/ing.adolfo/gestion-de-redes.

1.2.1. El gestor.

Es conocido como NMS (Nerwork Management Station), y es la parte que recibe e interpreta la información enviada desde los agentes de acuerdo a directivas y SLA's[3] configuradas. Además, es el que contiene la perspectiva global de todos los equipos monitoreados de la red.

Sus principales características son:

- Centralización de aplicaciones para análisis de datos.
- Entorno amigable para facilitar al administrador la gestión de red.
- Control remoto de dispositivos.
- Una Base de Datos que contiene las MIB's[4] extraídas de diferentes agentes.

1.2.2. El agente.

Es el que responde a las directivas y SLA's enviadas por el gestor.

Un agente puede realizar el seguimiento de[5]:

- Cantidad y estado de sus circuitos virtuales.
- Cantidad recibida de ciertos tipos de mensajes de error.
- Cantidad de bytes y de paquetes que entran y salen del dispositivo.
- Longitud máxima de la cola de entrada para los routers y otros dispositivos de internetworking.
- Mensajes de broadcast enviados y recibidos.
- Interfaces de red que se desactivan y que se activan.

1.2.3. La MIB[6].

Es el conjunto de objetos gestionados que representan a los recursos de la red que permiten algún tipo de gestión en una forma abstracta.[7]

1.2.4. El protocolo.

Es el conjunto de especificaciones y convenciones que preside la interacción de procesos y elementos dentro de un sistema de gestión.

---

[3] **SLA:** son las siglas de la frase en inglés Service Level Agreement, que significa Acuerdo de Nivel de Servicio y a veces se abrevia como ANS. Tomado de: «Definición De SLA -», s.f. http://soporte.epoint.es/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=134.

[4] Dr. Víctor J. SOSA-SOSA, «MIB.pdf», accedido 2 de febrero de 2012, http://www.tamps.cinvestav.mx/~vjsosa/clases/redes/MIB.pdf. La definición en el glosario de términos

[5] «Módulo 6: Introducción a la administración de redes», accedido 5 de noviembre de 2012, http://club.idecnet.com/~javcasta/webccna4/mod6.htm#6.2.3_Est%C3%A1ndares_SNMP_y_CMIP.

[6] Dr. Víctor J. SOSA-SOSA, «http://www.tamps.cinvestav.mx/~vjsosa/».

[7] Vea más información en el Anexo 1: MIB

1.3. Modelos de Gestión De Red

Para la gestión de red, según el grado de integración existen tres modelos de administración que son:

1.3.1. Modelo Aislado.

Este modelo posee esta denominación porque se crea una herramienta independiente para cada problema de administración, dichas herramientas trabajan de forma aislada, y la administración de la información se realiza con diferentes interfaces de usuario.
Si se tiene una red altamente distribuida no tiene sentido tener una administración de este tipo, ya que, es muy costosa y requiere de mucho personal.

1.3.2. Modelo Coordinado.

Este modelo permite relacionar herramientas que funcionan de manera aislada (por la forma en que proveen una función según el modelo explicado anteriormente) para complementarse con otras herramientas de acuerdo a las tareas en las que se las está utilizando.

El funcionamiento de este modelo lo describo de la siguiente manera: el resultado que genera una herramienta puede ser usado como los datos de entrada de otra. Una forma de lograr esto, es elaborar scripts para “programar” la interacción e integración entre diferentes herramientas.

En este enfoque podemos integrar diferentes interfaces de usuario, aplicaciones y herramientas de administración para ser controladas y manejadas sobre una interface de usuario común (GUI común).

1.3.3. Modelo Integrado.

El enfoque es integrado cuando los componentes que están siendo administrados son capaces de suministrar información que puede ser interpretada de tal forma que no dependa del fabricante. En esta información se puede acceder sobre interfaces y protocolos estándares diseñados para las comunicaciones de redes.

1.4. Evolución de Los Sistemas de Administración

La administración de redes surgió a la par con el origen de ellas, desde su existencia, siempre hubo la necesidad de controlar, configurar, monitorear, y otros, los recursos de conexión. Ahora bien, al igual que las redes, los sistemas de red también han ido evolucionando es por eso que según algunos autores se los ha dividido en las siguientes etapas evolutivas:

1.4.1. Redes Autónomas.

Esta gestión fue una de las primeras formas de agrupar y comunicar grupos de computadoras, en donde existían pocos equipos y cada equipo poseía un sistema de gestión local (Ver Ilustración 2: Redes Autónomas). Si existía la necesidad de comunicación con más nodos se tenía que realizar las gestiones con cada uno de los administradores de red. En estos sistemas la administración se realiza de forma local en cada elemento de red. Esto causa que existan tantos sistemas de administración como elementos de red, siendo una solución muy costosa. Sin embargo el tiempo de reacción ante fallos es resuelto rápidamente.

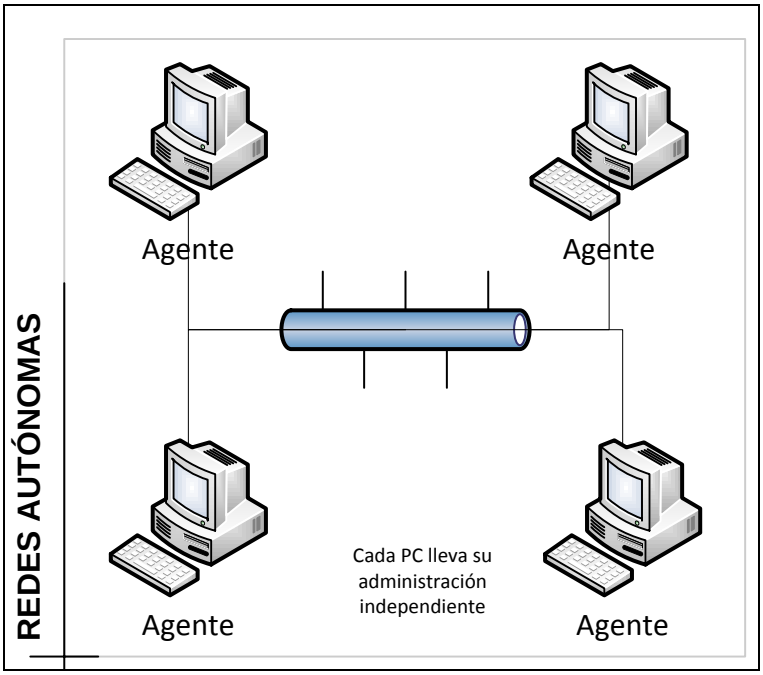


Ilustración 2: Redes Autónomas

1.4.2. Redes Centralizadas

Las redes fueron posteriormente aumentando de tamaño por lo que se necesitó que todos los equipos utilizaran un mismo protocolo dado por el fabricante de dispositivos y equipos de red. Cada fabricante poseía su propio sistema de gestión en donde existía un único nodo centralizado que trabajaba como nodo principal a manera de Servidor y uno o más nodos vinculados a manera de Clientes (Ver Ilustración 3: Redes Centralizadas).

En este tipo de sistemas existe una centralización de la administración de red, siendo única para todos los elementos de la red. El costo es inferior al de la solución previa, sin embargo, estos sistemas se ven limitados a la administración de elementos provenientes del mismo fabricante.

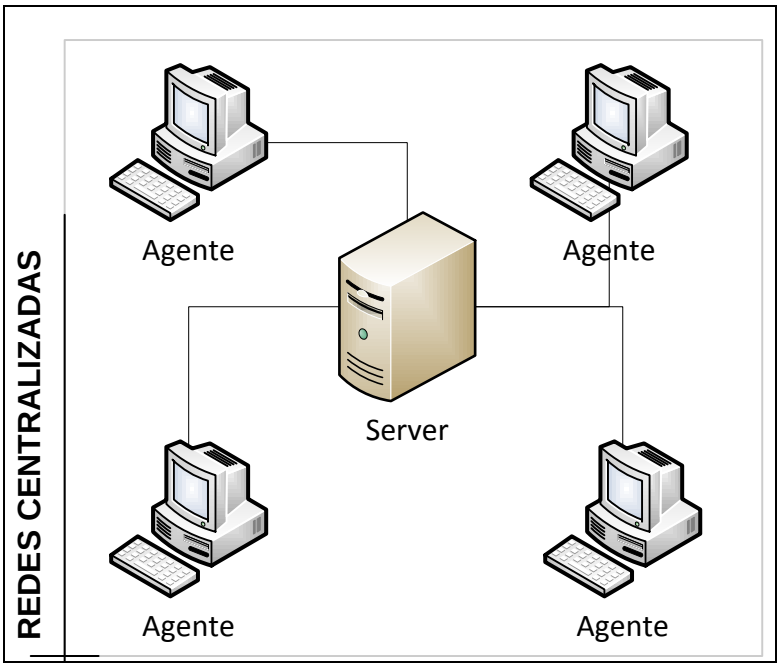


Ilustración 3: Redes Centralizadas

1.4.3. Redes Integradas

En la actualidad las redes han crecido de una manera astronómica con la incorporación de nuevas y variadas tecnologías. Ya no se puede hablar de entornos homogéneos sino que dentro de una misma red podemos encontrar una gran variedad de fabricantes y tecnologías que se encuentran interactuando entre sí. Este tipo de gestión ha permitido la generación de nuevas estructuras de funcionamiento de red, en donde puedan coexistir una gran variedad de topologías junto a diversas marcas y dispositivos dentro de un mismo esquema organizacional de red (Ver Ilustración 4: Redes Integradas).

Con este tipo de redes se descarta las desventajas en cuanto a la limitante por el fabricante y costos, porque la administración se centraliza y se puede administrar elementos de cualquier fabricante.

Un detalle importante que hay que destacar, es que se requiere de una normalización de comunicación a través de un protocolo específico en el gestor y los elementos gestionados. Además, se requiere que la información sea normalizada de tal manera que la central de administración de red conozca las propiedades de administración de cada elemento.

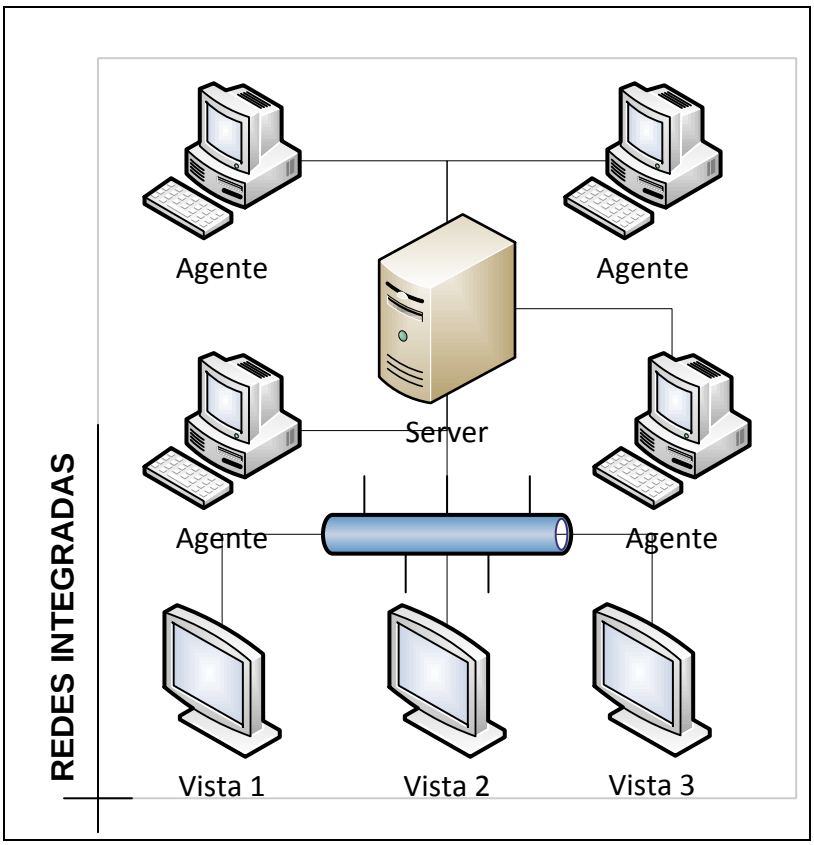


Ilustración 4: Redes Integradas

1.5. Estándares de Administración de Red

Los organismos de normalización han definido tres modelos principales para la gestión integrada de una red:

- ***Gestión de red OSI***[8]***:*** *(Open Systems Interconnection, Interconexión de Sistemas Abiertos)*
- ***Arquitectura TMN***[9]***:*** *(Telecommunications Management Network o Red de Gestión de las Telecomunicaciones)*. *Ver más en el Anexo 2: TMN.*
- ***Gestión Internet: Definida por la ISOC***[10] ***para gestión de redes TCP/IP.***

Para la Gestión rrectamente una red (Ilustración 5: División de Gestión de Redes. Tomada de) se utiliza la Gestión de Redes de computadores junto con la Gestión de

[8]Ing. William Marín Moreno, «Modelo OSI», s. f., http://www.ie.itcr.ac.cr/marin/mpc/redes/Modelo_osi_tcp_ip%28oficial%29.pdf; «Modelo_osi_tcp_ip(oficial).pdf», accedido 7 de noviembre de 2011, http://www.ie.itcr.ac.cr/marin/mpc/redes/Modelo_osi_tcp_ip(oficial).pdf.

[9]Telecomunications Management Network, «tmn.pdf», accedido 7 de febrero de 2012, http://www.hit.bme.hu/~jakab/edu/litr/TMN_EMS/tmn.pdf.***Más Información en el ANEXO 2***

[10]«La Internet Society (ISOC) es la organización dedicada al desarrollo estable y a la expansión global de Internet.- swissinfo», accedido 27 de julio de 2012, http://www.swissinfo.ch/spa/noticias/reportajes/Asegurar_la_evolucion_transparente_de_Internet.html?cid=915550.

Redes de Telecomunicaciones:

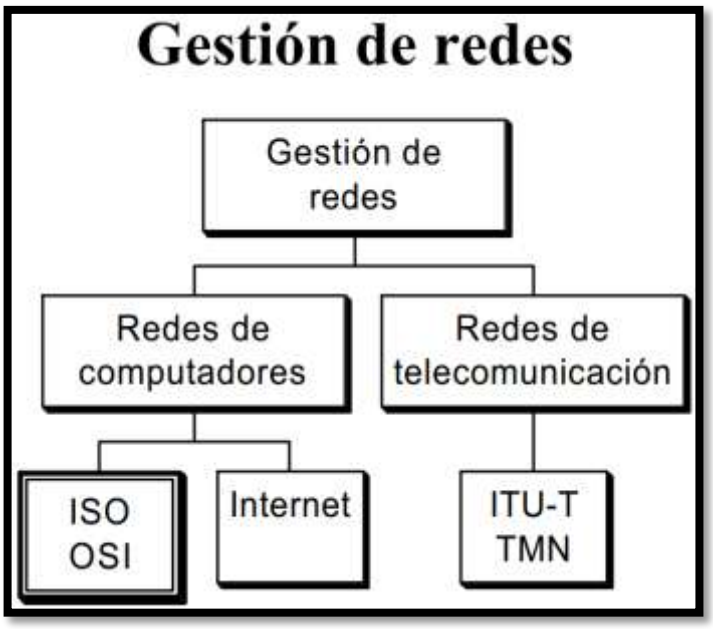


Ilustración 5: División de Gestión de Redes. Tomada de (Electrónica, 1997)[11]

Seguidamente se dará una explicación más amplia de cada uno de los modelos descritos anteriormente.

1.5.1. Gestión de Red OSI.

Es importante estudiar y explicar el modelo OSI para la administración de red por las siguientes razones:

1. La arquitectura OSI sirve como base de TMN (Telecommunications Management Network)
2. OSI puede tomarse como un estándar o como un modelo referencia de gestión de red.
3. La arquitectura OSI incluye los cuatro submodelos (información, organización, comunicación y funcional) y por tanto puede ser utilizada como una arquitectura de referencia.

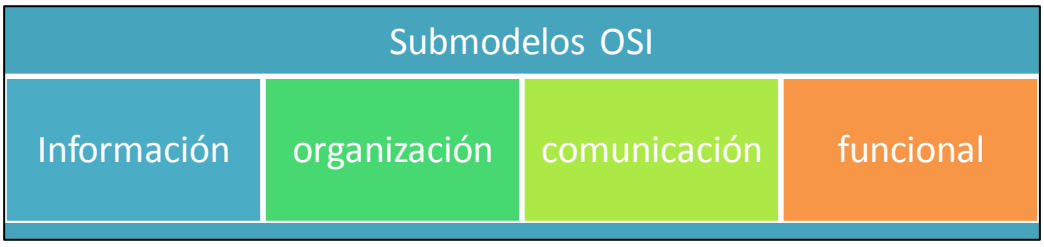


Ilustración 6. Modelos arquitectura OSI[12]

[11] «Gestión de Redes de Comunicaciones» (Dpto. de Tecnología Electrónica, 1997).
[12] Diseño personal

A continuación se explicará brevemente cada uno de estos submodelos:

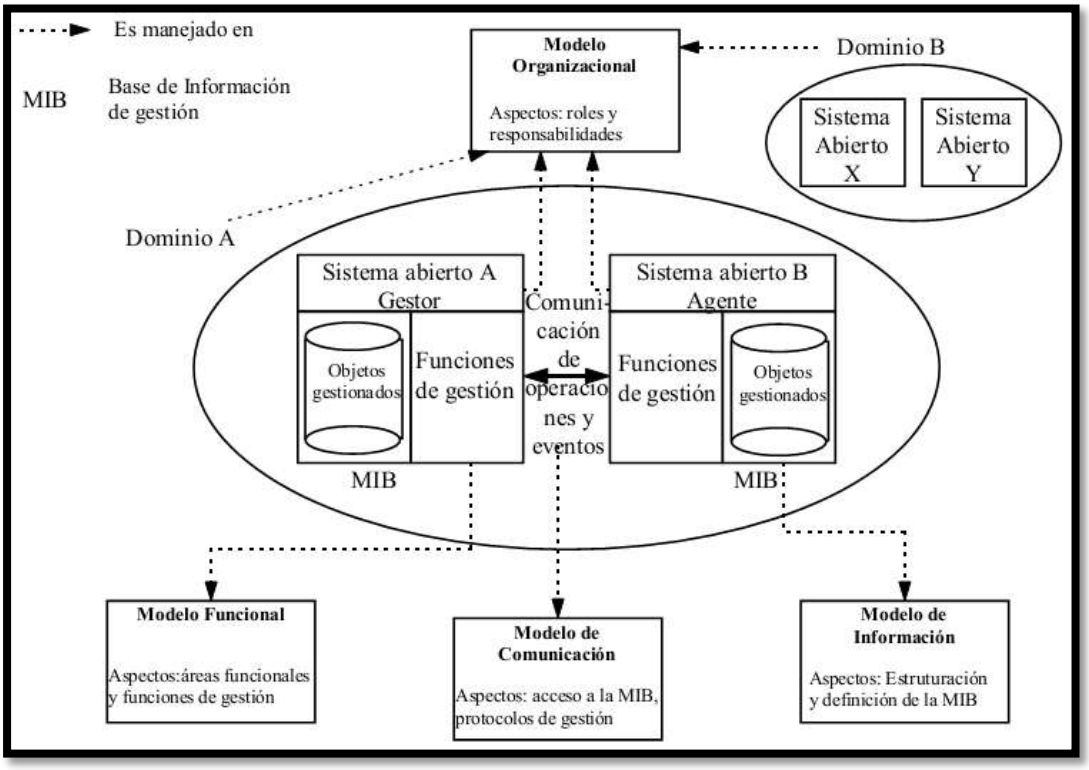


Ilustración 7: Submodelos Propuesto por (Irastorza, Gestión de Red, 2008)[13]

a) El submodelo de información utiliza un enfoque orientado a objetos en la abstracción de recursos relevantes a la administración. Este enfoque permite desarrollar un repertorio amplio para estructurar la base de información de administración (MIB). Para OSI, una MIB es la colección de información de administración que hace visible el sistema administrado.
b) El submodelo organizacional está basado en administración cooperativa distribuida en una red de sistemas abiertos. Los roles (manager o agente) se diferencian de acuerdo con "la actitud" que el sistema adopte frente a ciertos recursos (es decir, el rol puede cambiar dependiendo de los privilegios que tenga el usuario).
c) El submodelo de comunicaciones está soportado en el modelo de comunicaciones de siete capas de OSI. Este submodelo incorpora tres mecanismos para el intercambio de información de administración:
    1. Comunicación entre procesos de administración de la capa 7 (administración de los sistemas).

[13]IRASTORZA José Ángel, «Gestión de Redes», 2008, http://www.tlmat.unican.es/siteadmin/submaterials/509.pdf.

2. Comunicación entre entidades de administración específicas a una capa (administración de la capa).
3. Comunicación entre entidades de protocolo normal (operación de la capa).

d) El submodelo funcional subdivide el sistema de administración en cinco áreas funcionales FCAPS. (Fault, Configuration, Accounting, Performance y Security. Ver Ilustración 8: Submodelo Funcional de la Arquitectura OSI) busca definir funciones de administración genéricas que soporten uno o más áreas funcionales.

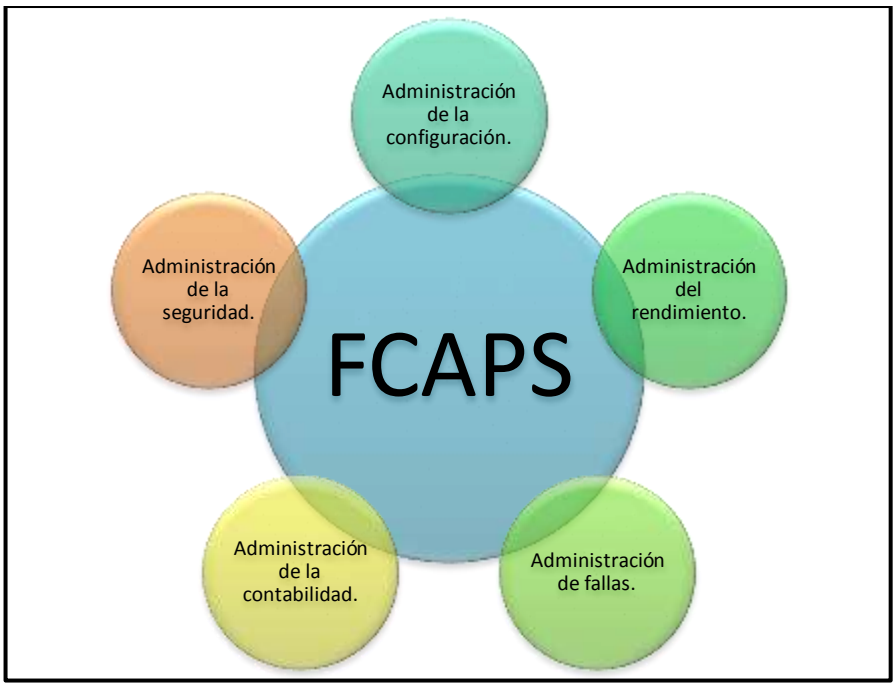


Ilustración 8: Submodelo Funcional de la Arquitectura OSI (Alejandro, 2009)[14]

1.5.1.1. Arquitectura de la Información.

El submodelo de información (de una arquitectura de administración) busca controlar los métodos utilizados para modelar y describir los objetos administrables. Además, *una definición estándar* de objetos administrables *es un prerrequisito para interoperabilidad* de la administración: permite a redes heterogéneas interactuar con propósitos de administración.

ISO aplica un enfoque totalmente orientado a objetos para construir su (complejo) modelo de información. Este modelo es llamado *Structure of Management Information* (**SMI**) (ISO 10165x). Los objetos administrables (*Managed Objets*: **MO**s) son instancias

[14]Alejandro MC, «Redes y Telecomunicaciones» (UNDAC, 2009).

de las clases *objeto administrable* (*Managed Object Classes*: **MOC**s) cuyas propiedades *visibles* externamente están descritas en la *managed object boundary* de la clase respectiva. Esta *managed object boundary* incluye los atributos, las operaciones definidas, notificaciones y descripciones de comportamiento de la clase. Esta *boundary* implementa una abstracción de los recursos desde el punto de vista de la administración. Los valores "reales" de los atributos y las operaciones se "mapean" del recurso real.

El modelo OSI incluye cinco componentes claves en la administración de red:

- **CMIS**: Common Management Information Services. Este es el servicio para la colección y transmisión de información de administración de red a las entidades de red que lo soliciten.
- **CMIP**: Common Management Information Protocol. Es el protocolo de OSI que soporta a CMIS, y proporciona el servicio de petición/respuesta que hace posible el intercambio de información de administración de red entre aplicaciones.
- **SMIS**: Specific Management Information Services. Define los servicios específicos de administración de red que se va a instalar, como configuración, fallas, contabilidad, comportamiento y seguridad.
- **MIB**: Management Information Base. Define un modelo conceptual de la información requerida para tomar decisiones de administración de red. La información en el MIB incluye: número de paquetes transmitidos, número de conexiones intentadas, datos de contabilidad, etc.
- **Servicios de Directorio**: Define las funciones necesarias para administrar la información nombrada, como la asociación entre nombres lógicos y direcciones físicas.

1.5.1.2. Arquitectura Organizacional[15].

El submodelo de organización (de una arquitectura de administración) define los actores (elementos que participan en la administración), sus roles y las reglas de cooperación entre ellos. Pueden definirse dominios para agrupar recursos que serán administrados. En estos dominios se definen políticas (reglas) específicas de administración. Los dominios y las políticas son objetos administrables. (Ver Ilustración 9: Roles del Administrador y Agente).

La arquitectura de administración OSI (ISO 10040)[16] define dos roles para los sistemas:

[15]«Submodelo-organizacional-OSI», accedido 27 de julio de 2012, http://www.arcesio.net/osinm/osinmorganizacion.html.
[16] Ver mas en el Anexo 4: Normas ISO y Estándares utilizados

un rol de *manager* y otro de agente (*agent*).

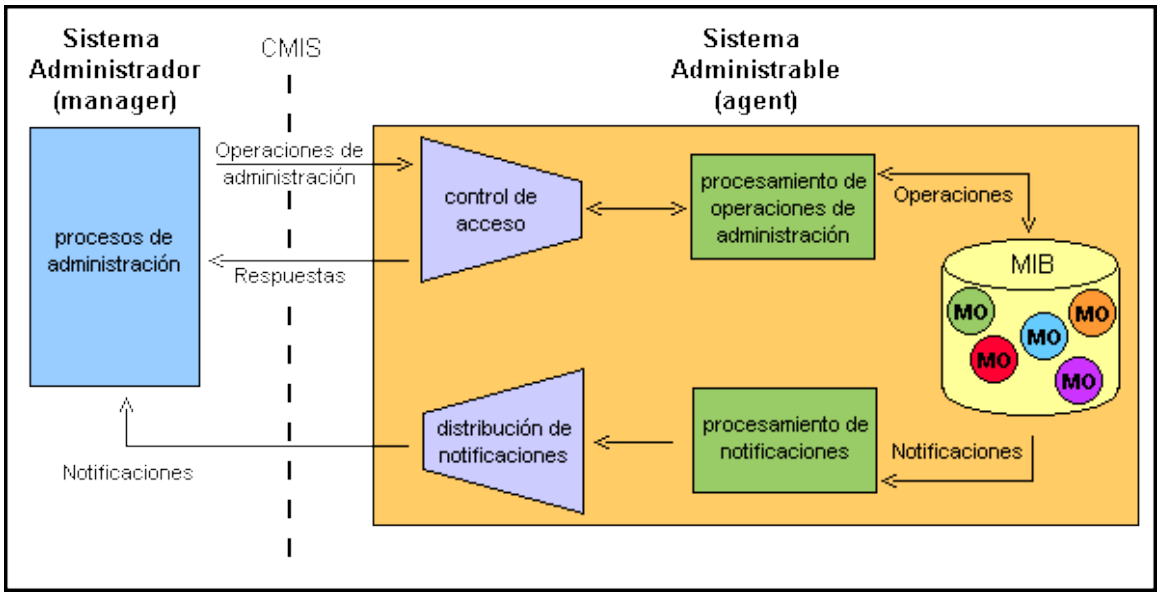


Ilustración 9: Roles del Administrador y Agente[17]

OSI provee un concepto de dominio extensible y flexible, en el cual se diferencia entre *dominio organizacional* y *dominio administrativo*.

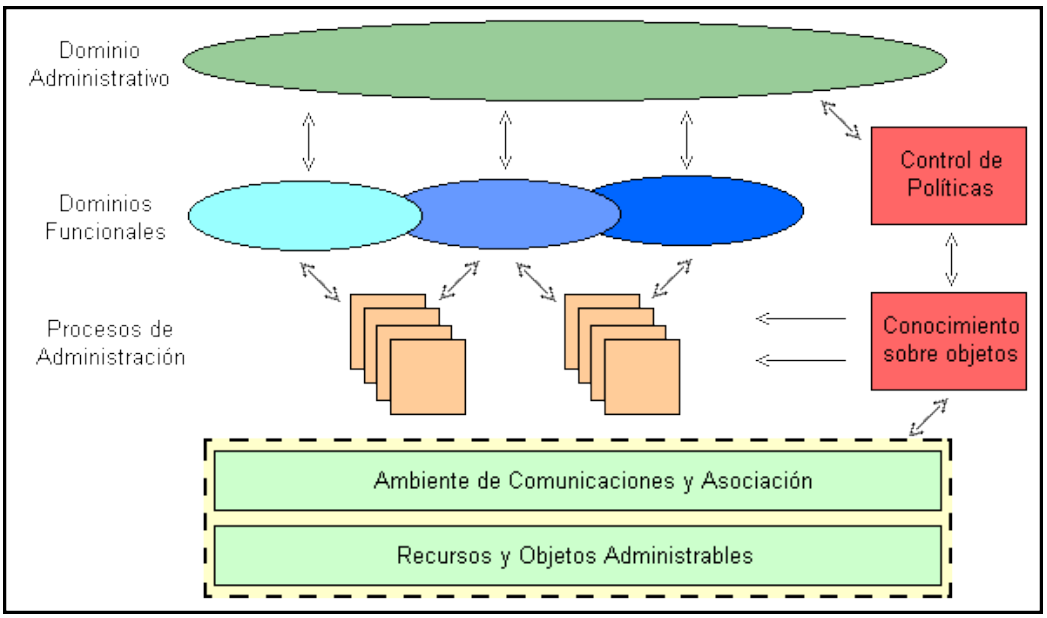


Ilustración 10: Dominio Organizacional y Dominio Organizativo[18]

Los ***dominios organizacionales*** son MOs (objetos administrables) agrupados de acuerdo a:

[17] "Submodelo-organizacional-OSI", n.d., http://www.arcesio.net/osinm/osinmorganizacion.html.
[18] «Submodelo-organizacional-OSI».,n.d., http://www.arcesio.net/osinm/osinmorganizacion.html.

- **Geográficos**: se agrupan por cercanía o que se puede agrupar por agencias ubicadas dentro de un mismo lugar.
- **Tecnológicos**: se agrupan por tecnología similar o compatible. También en esta parte se puede tomar en cuenta las caracteristicas de los equipos, como: servidores, switch, routers y demás elementos de red.
- **Organizativos**: se agrupan por departamentos dentro de una empresa.
- **Funcionales**: Se puede dividir también por la función que desempeñan. Como por ejemplo: Servidores de correo, Servidores de Actualización, etc.
    - Seguridad.
    - Facturación.
    - Gestión de fallos.

Los ***dominios administrativos*** agrupan los MOs (objetos administrables) que tienen la misma, y única, autoridad administrativa. Estos dominios se utilizan para:

- Crear y manipular dominios organizacionales.
- Controlar el flujo de acciones entre dominios (que pueden llegar a estar traslapados).

Un *dominio también es un objeto que se puede administrar* (es decir, un dominio es un MO (*Managed Object)*) y puede ser descrito con una especificación para una clase MOC[19].

Una política de administración, especificada como un conjunto de reglas, puede ser asignada a un dominio. Estas reglas pueden restringir el comportamiento de los objetos MOs a los cuáles se les aplique, pero dichas reglas no pueden contradecir el comportamiento "natural" del objeto MO. *Una política*, al igual que un dominio, *también es un objeto administrable* MO. Los dominios y las políticas se administran con la ayuda de las funciones de administración correspondientes que conforman el submodelo funcional.

Para lograr que los sistemas cooperen efectivamente, ellos deben conocer la funcionalidad relevante a la administración de los otros sistemas. El término *management knowledge* engloba el conocimiento que el *manager* y los agentes deben tener como soporte para ejecutar las diferentes aplicaciones de administración en forma distribuida. Incluye *protocolo knowledge* (el contexto de las aplicaciones), *functional knowledge* (unidades funcionales soportadas y las funciones de

[19] Ver definición en el Glosario de Términos

administración de sistemas) y *MO knowledge* (MOCs definidas, entidades de MOs). Debido a que muchas versiones concretas de *management knowledge* pueden existir, sería útil -donde se pueda- "predefinir" perfiles.

1.5.1.3. Arquitectura de Comunicaciones.

El submodelo de comunicaciones (de una arquitectura de administración) establece y define los elementos y conceptos necesarios para que los componentes del sistema (actores) puedan intercambiar información de administración (por ejemplo, quiénes pueden comunicarse, especificar los servicios y protocolos, definir la sintaxis y la semántica de los formatos de intercambio, además de los protocolos de administración que se colocarán dentro de la arquitectura de comunicaciones utilizada). La comunicación puede establecerse a través del intercambio de información de control, solicitudes de información de estado o generación de mensajes de eventos.

Los elementos que la componen son los siguientes:

- **ASCE** (Association Control Service Element): Establece la conexión y liberación de las operaciones realizadas entre los elementos de la red.
- **ROSE** (Remote Operate Service Elelement) realiza el control de las operaciones remotas.
- **CMISE** (Common Management Information Service Element): brinda las características acerca del protocolo basadas en dos elementos que son:
    - CMIP (Common Management Information Protocol)
    - CMIS (Common Management Information Services).

1.5.1.4. Modelo Funcional.

La norma ITU-M. 3400[20] y el modelo OSI divide el modelo de administración de red en Áreas Funcionales para la Administración de Sistemas más comúnmente llamados FCAPS. (Fault, Configuration, Accounting, Performance y Security).

1.5.1.4.1. Gestión de Fallas.

La administración de fallas está relacionada con la detección, aislamiento y eliminación de comportamientos anormales del sistema. Identificar y hacer el seguimiento de las fallas es un problema operacional importante en todos los sistemas de procesamiento de datos. Comparado con sistemas no conectados a una red, la administración de fallas en redes de computadores y sistemas distribuidos es más difícil por una diversidad de razones que incluyen, entre otros, el mayor número de componentes

[20] Ver más en el Anexo 4: Normas ISO y Estándares utilizados.

involucrados, la amplia distribución física de los recursos, la heterogeneidad de los componentes de hardware/software y los diferentes unidades de la organización involucradas (diferentes personas, áreas y departamentos que existen en la organización y de acuerdo a su estructura funcional).

La función de administración de fallas es detectar y corregir fallas rápidamente para asegurar un alto nivel de disponibilidad de un sistema distribuido y de los servicios que este presta. Las tareas que involucra son:

- Monitoreo del sistema y de la red.
- Respuesta y atención a alarmas.
- Diagnóstico de las causas de la falla (aislar la falla y analizar la causa que la origina).
- Establecer la propagación de errores.
- Presentar y evaluar medidas para recuperarse de los errores.
- Operación de sistemas de tiquetes de problemas (trouble tickets systems, TTS[21]).
- Proporcionar asistencia a usuarios mediante el área de TI (HELPDESK[22]).

Las siguientes capacidades técnicas pueden ayudar en el análisis de fallas:

- Auto identificación de los componentes del sistema.
- Poder realizar pruebas, por separado, con los componentes del sistema.
- Facilidades de seguimiento (tracking).
- Disponer de una base de datos de logs de errores.
- Alarmas de los mensajes en todas las capas de protocolo.
- Ambientes de pruebas para simular errores a propósito en partes sensibles del sistema.
- La posibilidad de iniciar rutinas de autoverificación y la transmisión de datos de prueba a puertos específicos (test de loops, test remotos) al igual que pruebas de asequibilidad con paquetes ICMP (ping o traceroute).
- Establecer valores máximos y mínimos que se tomados como umbral para realizar la evaluación de estado y funcionamiento de cada componente de la red.
- Interfaces de herramientas de administración de fallas a sistemas de tiquetes de problemas y HELPDESK (soporte técnico). Es decir, propagación automática de notificaciones y correcciones de fallas.

[21]«Trouble Ticket System», accedido 6 de septiembre de 2012, http://59.90.102.17/intranetuser/egroupware/rt.html.
[22]"¿Que Significa Help Desk En La Computación? - Yahoo! Respuestas", n.d., http://es.answers.yahoo.com/question/index?qid=20091103170048AA8MVxB.

1.5.1.4.2. Gestión de Configuración.

La configuración se define como el proceso de adaptación de los sistemas a un ambiente operativo, implica instalar nuevo software, actualizar software, conexión de dispositivos, cambios en la topología de la red o en el tráfico de la misma. Aunque la configuración se acompaña de establecimiento de umbrales, filtros de información, asignación de nombres a los objetos administrados, regula los cambios de configuración y exige la documentación detallada de los dichos cambios.

Dentro de esta gestión se debe tener en cuenta:

- El fácil acceso a la información.
- Inventario actualizado frecuentemente de los elementos de red y sus respectivos cambios y/o actualizaciones.
- Repositorio de configuraciones de sistemas.
- Disponibilidad de acceso remoto a los dispositivos.

1.5.1.4.3. Gestión de Contabilidad.

La administración de contabilidad incluye la recopilación de datos de uso (uso de recursos o de servicios basados en el monitoreo y la medición), definir unidades de contabilización, asignar cuentas, mantener bitácoras de contabilidad, asignar costos a las cuentas asignadas, asignar y monitorear las cuotas asignadas, mantener estadísticas de uso, y finalmente, definir políticas de contabilidad y tarifas, que permitirán generar facturas y cargos a los usuarios. Si varios proveedores están involucrados en la prestación de los servicios, las reglas de conciliación pertenecen a la administración de contabilidad. Este proceso puede realizarse por un procedimiento de repartir ingresos, mediante una tarifa plana o un precio para cierta unidad de tráfico.

Los parámetros "de uso" utilizados para calcular los costos incluye la cantidad de paquetes o bytes transmitidos, duración de la conexión, ancho de banda y QoS de la conexión, localización de los participantes en la comunicación, conversión de costos para servicios, uso de recursos en los servidores, y uso de productos de software (control de licencias). Además de los costos variables también se tienen en cuenta los costos fijos (espacio de oficina, costo del mantenimiento, depreciación de muebles y equipos, etc.).

En resumen, las funciones de administración de contabilidad comprenden al menos funciones de administración de consumo (generación, corrección de errores, acumulación, correlación, agregación y distribución de consumo; revisión de consumo y validación de llamadas de solicitudes de servicio), funciones de procesamiento de

contabilidad (pruebas, supervisión, administración del flujo y administración de la recopilación de datos de consumo), funciones de control (administración de tarifas, control de cambios en el sistema de tarifas, control de generación de registro, control de transferencia de datos, control de almacenamiento de datos), y funciones de cargos (generación de cargos, producción de facturas, proceso de pagos, recopilación de deudas, reconciliación externa, procesamiento de contratos).

1.5.1.4.4. Gestión de Rendimiento.

En términos de sus objetivos, la administración del rendimiento podría ser vista como una continuidad de la administración de fallas. Mientras la administración de fallas es la responsable de asegurar que una red esté operativa, no es suficiente para satisfacer los objetivos de *la administración de rendimiento*, que *busca que el sistema*, como un todo, *se comporte bien*.

Por lo tanto, la administración del desempeño incorpora todas las medidas requeridas para asegurar *que la calidad de servicio cumpla con un estándar de nivel de servicios*. Esto incluye:

- Establecer métricas y parámetros de calidad de servicio.
- Monitorear todos los recursos para detectar cuellos de botella en el desempeño y traspasos de los umbrales.
- Realizar medidas y análisis de tendencias para predecir fallas que puedan ocurrir.
- Evaluar bitácoras históricas (logs).
- Procesar los datos medidos y elaborar reportes de desempeño.
- Llevar a cabo planificación de desempeño y de capacidad. Esto implica proporcionar modelos de predicción simulados o analíticos utilizados para chequear los resultados de nuevas aplicaciones, mensajes de afinamiento y cambios de configuración.

Sistemas de monitoreo, analizadores de protocolos, paquetes estadísticos, generadores de reportes y software de modelamiento son algunas de las herramientas típicas en esta área de administración de redes (desempeño).

1.5.1.4.5. Gestión de Seguridad.

La administración de seguridad comprende tareas como administración de los accesos, direcciones IP, incluyendo los servicios relacionados con directorios, permisos para el uso de los recursos y tiempo de disponibilidad (horas laborables, o horarios especiales de fines de semana).

Para poder cumplir con la seguridad se puede implementar controles, políticas, procedimientos o funciones de software, dividiendo a los recursos dentro de áreas autorizadas y no autorizadas.

La gestión de seguridad se ocupa de los siguientes puntos:

- Determinar qué información se quiere proteger; donde se encuentra ubicada y las personas que tendrán privilegios para acceder a ésta.
- Identificación de los puntos de acceso a la información.
- Protección y mantenimiento de los puntos de acceso a la información.

1.5.2. Arquitectura de Gestión TCP/IP.

En los setenta el número de nodos de Internet era muy reducido se gestionaba Internet con las facilidades que ofrecía el protocolo ICMP, como el PING. Cuando Internet avanzó en complejidad, multiplicando el número de nodos se empezó a trabajar en tres soluciones diferentes, que se definieron en 1987:

SGMP (Simple Gateway Monitoring Protocol), Protocolo Simple de Monitorización de Pasarelas. Sencillo Protocolo orientado fundamentalmente a la gestión de pasarelas IP. Posteriormente pasaría a llamarse SNMP (Simple Network Management Protocol), Protocolo Simple de Gestión de Red.

HEMS (High-Level Entity Management System), Sistema de Gestión de Entidades de Alto Nivel. Nunca llegó a tener aplicación práctica.
CMOT (CMIP). Adopción de los estándares ISO como marco de gestión para Internet sobre una torre de protocolos TCP/IP.

En 1990 el SNMP se convirtió en el estándar de las redes TCP/IP y de Internet. En 1992, se comenzó el trabajo para especificar una nueva versión de SNMP, la SNMPv2; aunque hoy en día todavía continúan los trabajos de actualización.

1.5.3. Arquitectura de Gestión de Red en Internet.

Los sistemas de gestión de Internet están formados por cuatro elementos básicos: Gestores, Agentes, MIB y el protocolo de información de intercambio SNMP.

Existe un tipo de agente que permite la gestión de partes de la red que no comparten el modelo de gestión de Internet. Son los llamados Agentes Proxy. Estos agentes proxy proporcionan una funcionalidad de conversión del modelo de información y del

protocolo.

1.6. Centro de Administración de Red (Network Operation Center-NOC)

1.6.1. Definición.

Una definición de Centro de Operaciones de Red (NOC), según lo define searchnetworking.techtarget.com es un lugar desde donde los administradores monitorean, supervisan y dan mantenimiento a una red de comunicaciones.[23]

Un NOC es una o más localidades desde los cuales se puede: monitorear, controlar, supervisar y dar mantenimiento a toda la infraestructura IT de una compañía, y provee de mecanismos necesarios para mitigar fallas de hardware como software, riesgos de seguridad, falla de servicio entre otros, que puedan suscitarse en el desempeño de una red. Además permite tener un historial estadístico del comportamiento y estado de salud de la red, permitiendo analizar el estado de la infraestructura IT para desarrollar un plan de contingencia que permita estar preparse anticipadamente para posibles fallas y mitigar el impacto que se puede causar a los clientes finales.

1.6.2. Objetivos de un NOC.

Entre los objetivos que un NOC persigue se encuentran:

- *Alta disponibilidad de la red*: proveyendo eficiencia operacional, reduciendo los tiempos de caídas (downtime) de la red y del sistema y proveyendo tiempos de respuesta aceptables. Los problemas de la red deben ser rápidamente detectados y corregidos.
- *Reducción de costos operacionales de red*: este es uno de los motivos primarios detrás de la administración de redes. Como las tecnologías cambian rápidamente, es deseable la administración de sistemas heterogéneos y múltiples protocolos.
- *Reducción de cuellos de botella en la red*: dependiendo de cada caso en particular, puede ser deseable un monitor centralizado para administración y en otros casos esta tarea debe ser distribuida.
- *Incrementar flexibilidad de operación e Integración*: las tecnologías de redes están cambiando a velocidades mayores que los cambios de requerimientos y necesidades. Cuando se usa una nueva aplicación, los protocolos usados en redes deberán cambiar también. Debe ser posible absorber nueva tecnología con un costo mínimo y adicionar nuevo equipamiento sin mucha dificultad. Además, debe permitir lograr una fácil migración de un software de administración de redes a otra versión.
- *Alta eficiencia*: debemos incrementar la eficiencia en pérdida de otros objetivos de

[23]Tomado de: http://searchnetworking.techtarget.com/definition/network-operations-center

la administración pero dependerá de otros factores tales como utilización, costo operacional, costo de migración y flexibilidad.

- *Facilidad de uso*: las interfaces de usuario son críticas para el éxito de un producto. El uso de aplicaciones de administración de redes no debe incrementar la curva de aprendizaje.
- *Seguridad*: La seguridad es un aspecto a tener en lo que concierne a información de contaduría, información gerencial, informes financieros, reportes de inhabilitados, etc.

1.6.3. Funciones de un NOC.

Ver la Ilustración 11. Áreas funcionales de un NOC con sus respectivos elementos[24].

[24]«Aranda Software Aranda SERVICE DESK - Mesa de Servicios - Mesa de Ayuda», accedido 5 de marzo de 2012, http://www.arandasoft.com/solucion_asdk.php; Aranda Software, «Aranda SERVICE DESK - Datasheet», 22 de septiembre de 2011, http://www.slideshare.net/ArandaSoftware/aranda-service-desk.

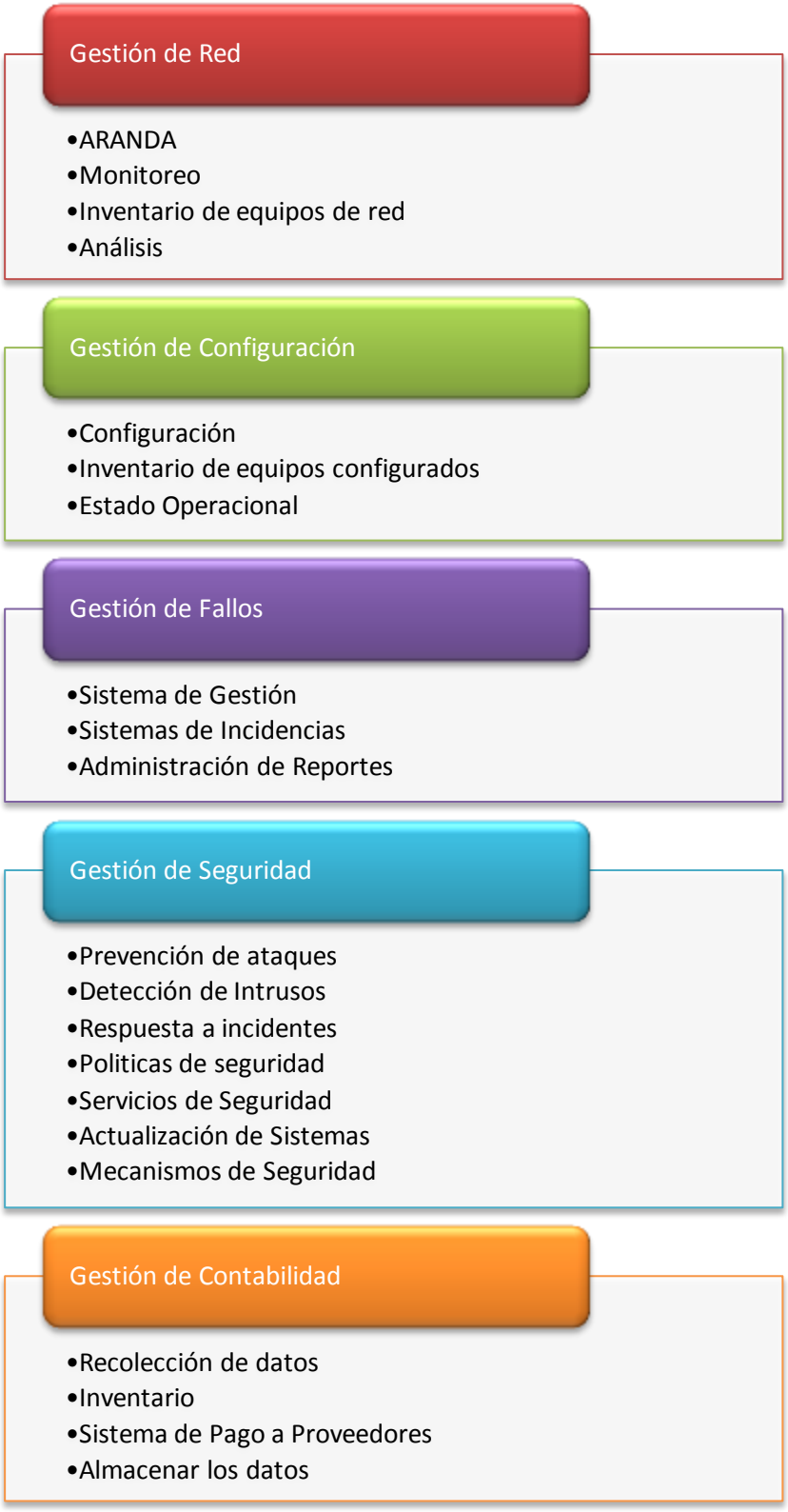


Ilustración 11. Áreas funcionales de un NOC

A continuación se detallará cada una de las áreas funcionales y sus elementos.

1.6.3.1. Gestión de Red[25].

Esta actividad abarca tanto tareas de monitorización, análisis y de ingreso de errores en la red. Esta gestión consiste en monitorear frecuentemente el estado de la red y ver su desempeño, así mismo, si existe un error reportarlo inmediatamente. Mediante el sistema ARANDA[26] se puede realizar el manejo de requerimientos, además, posee una Base de Datos de conocimiento en donde se van almacenando el historial de las soluciones a problemas que se hayan suscitado anteriormente.

Los elementos de la Gestión de red se los describe de la siguiente Manera:

1. **ARANDA[27].**

   Mediante este medio se va a realizar el ingreso de requerimientos, para lo cual se gestionó la integración de un nuevo SLA's para el manejo de los incidentes relacionados específicamente con las fallas en la infraestructura IT, enlaces, o problemas de red propiamente dicho. Aquí es donde se encontrará un seguimiento del estado del incidente desde la apertura hasta la solución (El funcionamiento del SLA se encuentra detallado en la Ilustración 12: SLA's para ingreso de Falla en la red). Además, existirá una documentación de seguimiento y de solución al incidente.

[25]Sergio Untiveros (suntiveros@aprendaredes.com), "Metodologías ParaAdministrar Redes."
[26]«Aranda Software Aranda SERVICE DESK - Mesa de Servicios - Mesa de Ayuda».
[27]Aranda Software, «Aranda SERVICE DESK - Datasheet».

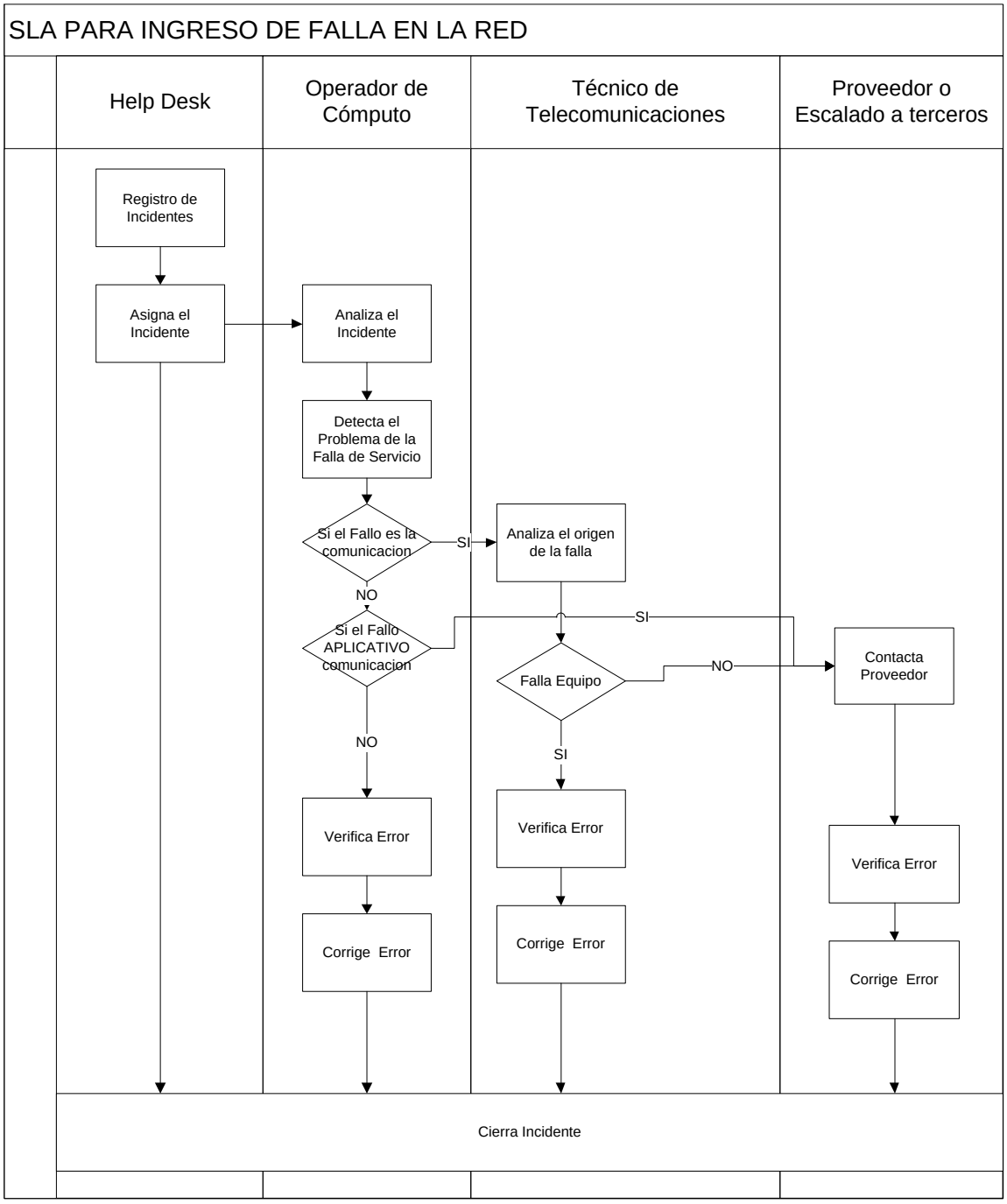


Ilustración 12: SLA's para ingreso de Falla en la red[28]

2. Monitoreo.

En esta parte se encarga de verificar el correcto funcionamiento y desempeño de todos los dispositivos que conforman la red en función de los datos recolectados mediante las actividades y procesos de observaciones de alarmas y procesos operativos dentro de la administración de red.

[28] Diseño propio

Entre las tareas se encuentra:

- Observar constantemente las alarmas de los dispositivos monitoreados.
- Identificar los elementos de red críticos dentro de la red.
- Establecer umbrales de medición basados en límites operacionales permitidos para el correcto funcionamiento de los elementos de la red[29].
- Análisis de los reportes históricos existentes sobre el funcionamiento de la red. (Estos reportes se realizan de manera semanal, y diaria. Más en el Anexo 5: Reportes Monitoreo)
- Conocer el estado actual de toda la red.
- Contar con sistemas de monitoreo que trabajen con protocolos estándares como son el SNMP y el MIB.
- Disponer de un sistema de monitoreo que se encuentre operativos 24x7 todo el año, todos los días de la semana y a toda hora del día.

3. Inventario de Equipos de Red.

Los elementos para tener encuenta dentro del inventario de equipos es: primero, se tiene que conocer la infraestructura IT disponibley segundo, los responsables que tienen asignados cada uno de los equipos. En esta parte se tiene que tener en cuenta tanto el software (programas, aplicativos), hardware (periféricos, capacidad) y configuraciones que tiene cada uno de los elementos de red.

4. Análisis.

Luego de tener la información recopilada del proceso de monitoreo, la base de datos de conocimiento de incidentes en el ARANDA [30] , conociendo la infraestructura (inventario de equipos) disponible, se procede a tomar medidas que permitan la optimización del rendimiento de la red. Dentro de lo que es análisis de debe detectar comportamiento relacionado a:

- *Utilización elevada.*

  Si se detecta que la utilización de un enlace es muy alta, se puede tomar la decisión de incrementar su ancho de banda o de agregar otro enlace para balancear las cargas de tráfico. También, el incremento en la utilización, puede ser el resultado de la saturación por tráfico generado maliciosamente, en este caso se debe contar con un plan de respuesta a incidentes de seguridad por problema de actualizaciones a nivel de sistema operativo o

[29] Los umbrales se dan explicación en el capítulo 3

[30]«Aranda Software Aranda SERVICE DESK - Mesa de Servicios - Mesa de Ayuda»; Aranda Software, «Aranda SERVICE DESK - Datasheet».

problemas de antivirus.

- ***Tráfico inusual.***

  Mediante el monitoreo detectar las aplicaciones que saturan/consumen los enlaces de comunicación de red, y de esta manera detectar el tráfico inusual; esto, permite obtener valiosa información en problemas que afecten el rendimiento de la red. Ej.: Saturación de enlace por la actualización del antivirus o por la generación de tráfico por actualizaciones de Windows del WSUS[31].

- ***Elementos principales de la red.***

  Un aspecto importante de conocer cuáles son los elementos que más reciben y transmiten información o consumen mayor ancho de banda, es el hecho de poder identificar los elementos a los cuales establecer un monitoreo más personalizado, debido a que seguramente son de importancia. Además, si se detecta un elemento que generalmente no se encuentra dentro del patrón de los equipos con más actividad, puede ayudar a la detección de posibles ataques a la seguridad de dicho equipo.

- ***Calidad de servicio.***

  Otro aspecto, es la Calidad de servicio, es decir, garantizar, mediante ciertos mecanismos, las condiciones necesarias, como ancho de banda, retardo, a aplicaciones que requieren de un trato especial, como Voz sobre IP (VoIP), el video sobre IP mediante H.323, etc.

- ***Control de tráfico.***

  El tráfico puede ser renviado o ruteado por otro canal, cuando se detecte saturación en los canales de comunicación de red, o al detectar que algún componente de la red se encuentra fuera de servicio, esto se puede hacer de manera automática ya que existen enlaces redundantes.

- ***Interacción con otras áreas***

  La administración del rendimiento se relaciona con la administración de fallas cuando se detectan anomalías en el patrón de tráfico dentro de la red y cuando se detecta saturación en los enlaces. Con la administración de la seguridad, cuando se detecta tráfico que es generado hacia un solo

[31] Sistema de Actualización de Software para Windows. WSUS (Windows Software Update System)

elemento de la red con más frecuencia que la común. Y con la administración de la configuración, cuando ante una falla o situación que atente contra el rendimiento de la red, se debe realizar alguna modificación en la configuración de algún elemento de la red para solucionarlo.

1.6.3.2. Gestión de Configuración.

Se encarga de mantener la información del diseño de la red y la configuración que posee cada uno de los elementos que integran la red. Además, de tener la información actualizada de todos los equipos y nodos que se van a gestionar y de los enlaces existentes para la comunicación interna y externa.

La gestión de red se maneja dentro de tres puntos importantes que son:

1. **Configuración**
   - Estar al tanto del estado actual de cada uno de los elementos de red.
   - Conocer la ubicación física de los equipos.
   - El personal responsable o custodio del equipo o equipos.
   - Poseer las descripciones del hardware (memoria, CPU, Disco Duro, etc.) y software (programas, aplicativos, parches de seguridad, sistema operativo) que requiere un determinado elemento de la red de acuerdo al rol que va a desempeñar o el servicio que va a brindar a los clientes.
   - Tener respaldos de los archivos de configuración.

2. **Inventario de Equipos Configurados**
   - Tener una base de datos de todos los elementos que conforman la red.
   - Tener una estructura organizativa para conocer la ubicación en la red. Ej.: Mediante el direccionamiento IP se puede conocer a que agencia pertenece.
   - Determinar mediante el direccionamiento IP el rol y las funciones que tiene cada nodo.

3. **Estado Operativo**
   - Llevar un inventario de cambios y/o actualizaciones de la información de los equipos. (cambio de ubicación, cambios en el SO, cambios de oficina, etc.).
   - Estadísticas de funcionamiento y consumo de recursos a nivel de hardware, software y de red.
   - Asegurar que el elemento de red se encuentre funcionando correctamente de acuerdo a las actividades y funciones para las que fue pensado.

1.6.3.3. Gestión de Fallas[32].

El objetivo de la gestión de fallas, es encontrar la mejor solución con la optimización de recursos tanto monetarios, RR.HH. y en el menor tiempo.

Las fallas son detectadas de acuerdo a las alarmas que se generen por distintos medios ya sean estos visuales, auditivos, mediante correos electrónicos que el personal del Centro de Cómputo genera para el seguimiento de un incidente dentro de la red desde su apertura y su posterior solución.

Existen dos métodos (Ver Ilustración 13. Detección Proactiva – Reactiva) para la detección de problemas que son:

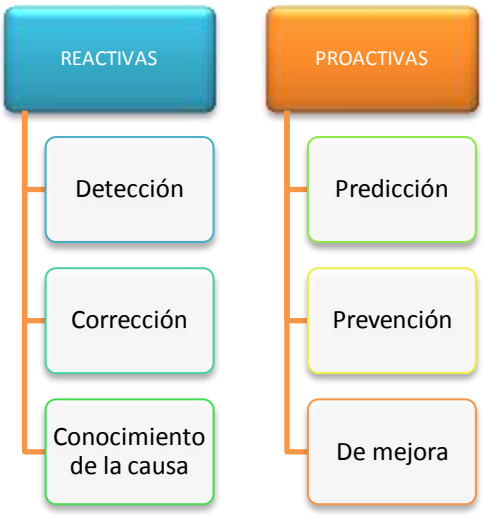


Ilustración 13. Detección Proactiva – Reactiva

- La detección proactiva: esta detección es la que se realiza antes que la falla se origine dentro de la red mediante el monitoreo continuo. Además, se puede verificar el comportamiento anormal pueda ocasionar alguna anomalía en la red.
- La detección reactiva: esta detección se realiza una vez que el fallo haya sucedido afectando el funcionamiento de un servicio o algún elemento en la red. En esta detección se realiza todo el proceso para controlar un incidente como se muestra en Ilustración 14. Detección Reactiva:

[32]Sergio Untiveros (suntiveros@aprendaredes.com), "Metodologías ParaAdministrar Redes"; ALTAMIRANO, CARLOS VICENTE, "Un Modelo funcional para el Centro de operación de RedUNAM (NOCUNAM)."

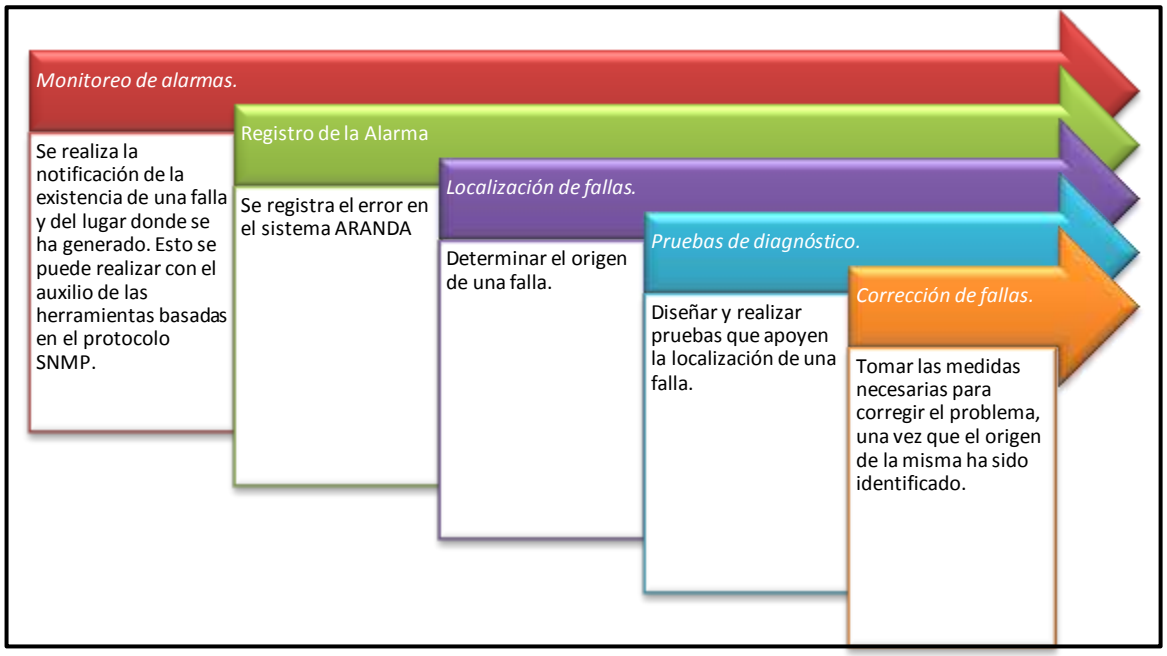


Ilustración 14. Detección Reactiva

1.6.3.4. Gestión de Seguridad[33].

Su objetivo es ofrecer servicios de seguridad a cada uno de los elementos de la red así como a la red en su conjunto, creando estrategias para la prevención y detección de ataques, así como para la respuesta ante incidentes de seguridad.

1.6.3.4.1. Prevención de ataques.

El objetivo es mantener los recursos de red fuera del alcance de potenciales usuarios maliciosos. Una acción puede ser la implementación de alguna estrategia de control de acceso. Obviamente, los ataques solamente se reducen pero nunca se eliminan del todo.

1.6.3.4.2. Detección de intrusos.

El objetivo es detectar el momento en que un ataque se está llevando a cabo. Hay diferentes maneras en la detección de ataques, tantas como la variedad de ataques mismo. El objetivo de la detección de intrusos se puede lograr mediante un sistema de detección que vigile y registre el tráfico que circula por la red apoyado en un esquema de notificaciones o alarmas que indiquen el momento en que se detecte una situación anormal en la red.

[33]Sergio Untiveros (suntiveros@aprendaredes.com), "Metodologías ParaAdministrar Redes"; ALTAMIRANO, CARLOS VICENTE, "Un Modelo funcional para el Centro de operación de RedUNAM (NOCUNAM)."

1.6.3.4.3. Respuesta a incidentes.

El objetivo es tomar las medidas necesarias para conocer las causas de un compromiso de seguridad en un sistema que es parte de la red, cuando éste haya sido detectado, además de tratar de eliminar dichas causas.

1.6.3.4.4. Políticas de Seguridad.

La meta principal de las políticas de seguridad es establecer los requerimientos recomendados para proteger adecuadamente la infraestructura de cómputo y la información ahí contenida. Una política debe especificar los mecanismos por los cuales estos requerimientos deben cumplirse. El grupo encargado de ésta tarea debe desarrollar todas las políticas después de haber hecho un análisis profundo de las necesidades de seguridad.

1.6.3.4.5. Servicios de seguridad.

Los servicios de seguridad definen los objetivos específicos a ser implementados por medio de *mecanismos de seguridad.*

De acuerdo a la Arquitectura de Seguridad OSI[34], un *servicio de seguridad* es una característica que debe tener un sistema para satisfacer una política de seguridad.

La arquitectura de seguridad OSI identifica cinco clases de servicios de seguridad[35]:

- Autenticación.- Confirma que la identidad de una o más entidades conectadas a una o más entidades sea verdadera. Entiéndase por entidad un usuario, proceso o sistema. De igual forma corrobora a una entidad que la información proviene de otra entidad verdadera.
- Control de acceso.- Protege a una entidad contra el uso no autorizado de sus recursos. Este servicio de seguridad se puede aplicar a varios tipos de acceso, por ejemplo el uso de medios de comunicación, la lectura, escritura o eliminación de información y la ejecución de procesos.
- Confidencialidad.- Protege a una entidad contra la revelación deliberada o accidental de cualquier conjunto de datos a entidades no autorizadas.
- Integridad.- Asegura que los datos almacenados en las computadoras y/o transferidos en una conexión no fueron modificados.
- No repudio: Este servicio protege contra usuarios que quieran negar falsamente que enviaran o recibieran un mensaje.

[34]Ing. William Marín Moreno, «Modelo OSI»; «Osi-NM», accedido 9 de diciembre de 2011, http://www.arcesio.net/osinm/osinm.html; «Modelo_osi_tcp_ip(oficial).pdf».
[35]Sergio Untiveros (suntiveros@aprendaredes.com), "Metodologías ParaAdministrar Redes."

La arquitectura de Seguridad OSI está basada en la recomendación X.800 y el RFC 2828.[36]

1.6.3.4.6. Mecanismos de seguridad.

Se deben definir las herramientas necesarias para poder implementar los servicios de seguridad dictados por las políticas de seguridad. Algunas herramientas comunes son: herramientas de control de acceso, cortafuegos (firewall[37]), TACACS+[38] o RADIUS[39]; mecanismos para acceso remoto como Secure Shell[40] o IPSec; mecanismos de integridad como MD5[41], entre otras.

1.6.3.5. Proceso.

Para lograr el objetivo perseguido se deben, al menos, realizar las siguientes acciones:

- Elaborar las políticas de seguridad donde se describan las reglas de administración de la infraestructura de red. Y donde además se definan las expectativas de la red en cuanto a su buen uso, y en cuanto a la prevención y respuesta a incidentes de seguridad.
- Definir, de acuerdo a las políticas de seguridad, cuales son los servicios necesarios y que pueden ser ofrecidos e implementados en la infraestructura de la red priorizando los que son de servicio al cliente.
- Implementar las políticas de seguridad mediante los mecanismos adecuados.

1.6.3.6. Gestión de Contabilidad[42]

Es el proceso de recolección de información acerca de los recursos utilizados por los elementos de la red, desde equipos de interconexión hasta usuarios finales. Esto se realiza con el objetivo de realizar los cobros correspondientes a los clientes del

[36] «La arquitectura de seguridad OSI», accedido 11 de junio de 2013, http://www.dragonjar.org/la-arquitectura-de-seguridad-osi.xhtml.
[37] «Qué es un firewall», accedido 29 de agosto de 2012, http://www.desarrolloweb.com/articulos/513.php.- Más en el Glosario de Términos.
[38] C. Finseth, «An Access Control Protocol, Sometimes Called TACACS», accedido 29 de agosto de 2012, http://tools.ietf.org/html/rfc1492; Wikipedia contributors, «TACACS», *Wikipedia, la enciclopedia libre* (Wikimedia Foundation, Inc., 2 de agosto de 2012), http://es.wikipedia.org/w/index.php?title=TACACS&oldid=58422643.- Más en el Glosario de Términos
[39] Wikipedia contributors, «RADIUS», *Wikipedia, la enciclopedia libre* (Wikimedia Foundation, Inc., 11 de agosto de 2012), http://es.wikipedia.org/w/index.php?title=RADIUS&oldid=58727330. - Más en el Glosario de Términos
[40] Ver definición en el Glosario de Términos.
[41] Ver definición en el Glosario de Términos.
[42] ALTAMIRANO, CARLOS VICENTE, "Un Modelo funcional para el Centro de operación de RedUNAM (NOCUNAM)"; Sergio Untiveros (suntiveros@aprendaredes.com), "Metodologías ParaAdministrar Redes."

servicio mediante tarifas establecidas. Este proceso, también llamado tarificación, es muy común en los proveedores de servicio de Internet o ISP[43].

Dentro de la contabilidad se incluye:

- Identificar el uso ineficiente de la red.
- Evitar sobrecargas dentro de la red y perjuicios a otros usuarios.
- Planificar el crecimiento de la red.
- Verificar los servicios a los usuarios en función de sus necesidades

1.7. Protocolos de Administración de Red[44].

1.7.1. CMIP (COMMON MANAGEMENT INFORMATION PROTOCOL)[45] [46]

Tras la aparición de SNMP como protocolo de gestión de red, a finales de los 80, gobiernos y grandes corporaciones plantearon el Protocolo Común de Gestión de Información CMIP (Common Management Information Protocol) que se pensó podría llegar a ser una realidad debido al alto presupuesto con que contaba. En cambio, problemas de implementación han retrasado su expansión de modo que solo está disponible actualmente de forma limitada y para desarrolladores.

CMIP [RFC 1189][47] fue diseñado teniendo en cuenta a SNMP, solucionando los errores y fallos que tenía SNMP y volviéndose un gestor de red más completo y más detallado. Su diseño es similar a SNMP por lo que se usan PDUs (Protocol Data Unit) como variables para monitorizar la red.

En CMIP las variables son estructuras de datos complejas con muchos atributos, que incluyen:

- Variables de atributos: representan las características de las variables.
- Variables de comportamiento: qué acciones puede realizar.
- Notificaciones: la variable genera una indicación de evento cuando ocurre un determinado hecho.

1.7.1.1. Arquitectura CMIP.

En la Ilustración 15: Arquitectura CMIP podemos observar como es la Arquitectura CMIP.

---

[43] Ver más en el Glosario de Términos

[44] «Administración de Redes - Protocolos de la familia Internet», accedido 14 de julio de 2012, http://personales.upv.es/rmartin/TcpIp/cap04s07.html.

[45] Daniel Arias Figueroa, «Herramientas de Gestión basada en Web» (Universidad Nacional de La Plata, 1999), http://postgrado.info.unlp.edu.ar/Carreras/Magisters/Redes_de_Datos/Tesis/Arias_Figueroa.pdf.

[46] Mauro, «CMIP», *CMIP*, 19 de febrero de 2010, http://maurocomputuacioningenieros.blogspot.com/; «CMIP», *Todoexpertos*, accedido 14 de julio de 2012, http://www.todoexpertos.com/categorias/tecnologia-e-internet/redes-de-computadores/respuestas/135528/cmip.

[47] Ver Anexo 4: Normas ISO y Estándares utilizados.

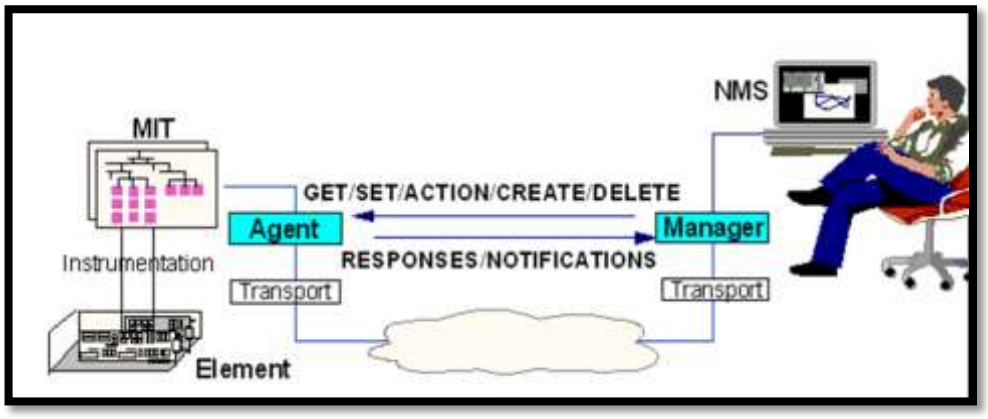


Ilustración 15: Arquitectura CMIP[48]

1.7.1.2. Fundamentos de CMIP.

CMIP es un protocolo de gestión de red que se implementa sobre el modelo de Interconexión de Redes Abiertas OSI (Open Systems Interconnection) que ha sido normalizado por la ISO (International Organization for Standardization) en sus grupos de trabajo OIW (OSI Implementors Workshop) y ONMF (OSI Network Management Forum). *Además existe una variante del mismo llamado CMOT [RFC 1095] que se implementa sobre un modelo de red TCP/IP.*

En pocas palabras, CMIP es una arquitectura de gestión de red que provee un modo de que la información de control y de mantenimiento pueda ser intercambiada entre un gestor (manager) y un elemento remoto de red. En efecto, los procesos de aplicación llamados gestores (managers) residen en las estaciones de gestión, mientras que los procesos de aplicación llamados agentes (agents) residen en los elementos de red.

CMIP define una relación igual a igual entre el gestor y el agente incluyendo lo que se refiere al establecimiento y cierre de conexión, y a la dirección de la información de gestión. Las operaciones CMIS (Common Management Information Services) se pueden originar tanto en gestores como en agentes, permitiendo relaciones simétricas o asimétricas entre los procesos de gestión. Sin embargo, la mayor parte de los dispositivos contienen las aplicaciones que sólo le permiten hacer de agente.

1.7.1.3. Estructura CMIP.

- El modelo de administración OSI define los sistemas administrados y los sistemas de administración.
- Cada nodo de comunicaciones debe tener una base de información de

[48]Emilio Hernández, «SNMP vs CMIP» (Redes 1, Universidad Simón Bolívar), accedido 5 de noviembre de 2012, ldc.usb.ve/~emilio/Portafolio/Exposiciones/SNMP-vs-CMIP.ppt.

administración (MIB)

- Un Proceso de Aplicación del Sistema de Administración (SMAP) proporciona el interfaz con la información compartida MIB. Los SMAPs dialogan con otros SMAPs a través de la red
- Una Entidad de Aplicación del Sistema de Administración (SMAE) soporta la comunicación de los SMAP y las SMAEs usan CMIP para intercambiar datos entre nodos.
- CMIP define la metodología para diseñar el sistema de administración de red y las especificaciones del interfaz están indicadas en CMIS (Servicio de Información de Administración Común).

1.7.1.4. Funciones CMIP.

Como CMIP es un protocolo de gestión de red implementado sobre OSI conviene introducir el marco de trabajo OSI en lo que respecta a gestión, ya que será la base para CMIP.

La gestión OSI posibilita monitorizar y controlar los recursos de la red que se conocen como "objetos gestionados". Para especificar la estandarización de la gestión de red se determina:

⇒ Modelo o grupo de modelos de la inteligencia de gestión, hay 3 principales:
  - Modelo de organización: describe la forma en que las funciones de gestión se pueden distribuir administrativamente. Aparecen los dominios como particiones administrativas de la red.
  - Modelo funcional: describe las funciones de gestión (de fallos, de configuración, de contabilidad, de seguridad y de rendimiento) y sus relaciones.
  - Modelo de información: provee las líneas a seguir para describir los objetos gestionados y sus informaciones de gestión asociadas. Reside en el MIB (Management Information Base).

⇒ Estructura para registrar, identificar y definir los objetos gestionados.

⇒ Especificación detallada de los objetos gestionados.

⇒ Serie de servicios y protocolos para operaciones de gestión remotas.

CMIP no especifica la funcionalidad de la aplicación de gestión de red, sólo se define el mecanismo de intercambio de información de los objetos gestionados y no cómo la información ha de ser utilizada o interpretada. El cuadro siguiente ofrece una imagen de alto nivel del sistema de gestión de red basada en el CMIP / CMIS:

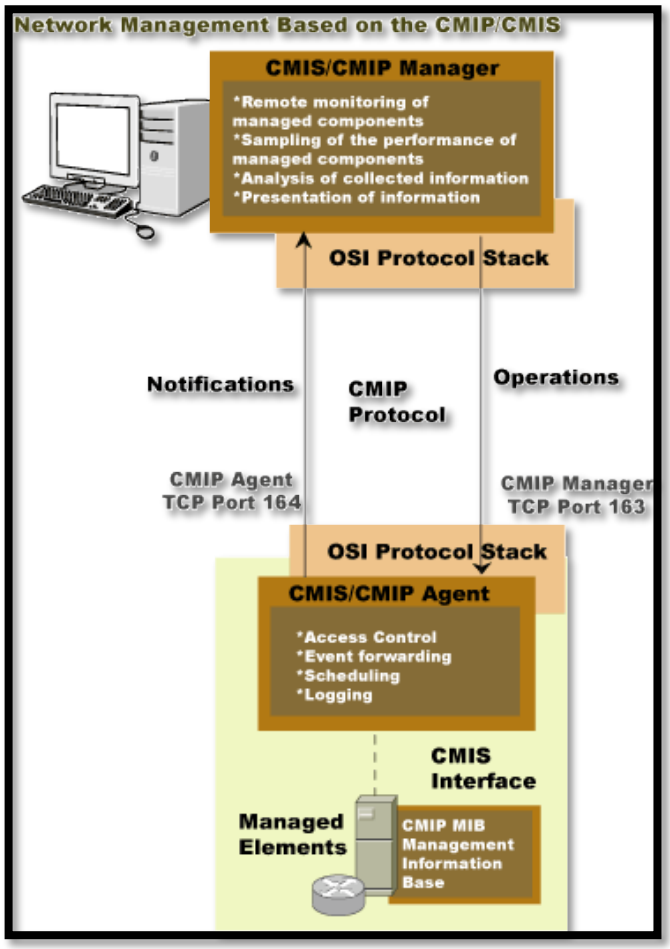


Ilustración 16: Sistema de Gestión de Red basada en el CMIP / CMIS[49]

1.7.1.5. Ventajas CMIP.

Las principales ventajas de CMIP a través de SNMP son:

- Variables CMIP de información no sólo de relevo, pero también puede ser utilizado para realizar las tareas de monitoreo de servicios. Esto es imposible en virtud de SNMP.
- CMIP es un sistema más seguro, ya que ha construido en la seguridad que soporta la autorización, control de acceso, y los registros de seguridad.
- CMIP proporciona capacidades de gran alcance que permite que las aplicaciones de gestión para lograr más con una sola solicitud.
- CMIP proporciona mejor información sobre las condiciones de red inusuales

El acceso a la información manejada en los objetos gestionados es proporcionado por el Servicio Común de Información de Gestión (Elemento CMISE) que utiliza CMIP (Common Management Information Protocol) para expedir las solicitudes de

[49]«CMIP: Common Management Information Protocol & CMIS: Common management Information Service (ISO 9595, 9596, X.700, X.711)», accedido 5 de noviembre de 2012, http://www.javvin.com/protocolCMIP.html.

servicios de gestión. Los servicios de gestión proporcionados por CMIP / CMISE se pueden organizar en dos grupos distintos, los servicios de gestión de la operación iniciada por un administrador para solicitar que un agente de prestación de determinados servicios o información, y servicios de notificación, utilizado por los agentes de administración para informar a los administradores de que algún evento o conjunto de eventos ocurridos.

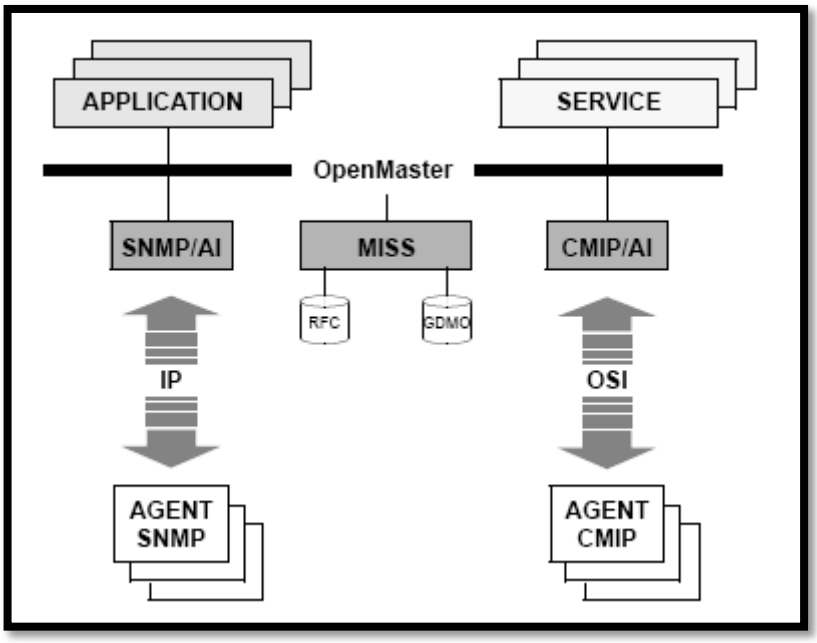


Ilustración 17: Sistema de Gestión CMIP / CMIS vs. SNMP[50]

1.7.1.6. CMI VS. SNMP.

- SNMP hace uso de un árbol de directorios estático CMIP hace uso de un árbol de directorios dinámico. SNMP utiliza un número mínimo de tipos de datos ASN.1 CMIP hace usa un rango extendido de tipos ASN.1.
- CMIP también es más seguro que el SNMP. CMIP obtiene un mayor rendimiento de los mensajes enviados ya que se reduce la señalización respecto al protocolo SNMP. CMIP utiliza conexiones con fuerte dependencia del estándar OSI. SNMP utiliza datagrama CMIP vs. SNMP
- SNMP que es más simple y que el personal requerido para su mantenimiento se reduce. CMIP se basa en una arquitectura jerárquicamente distribuida, lo que permite que el número de objetos supervisados sea mayor que en el protocolo SNMP. CMIP es más escalable, permite la herencia de atributos y es más flexible que el protocolo SNMP. SNMP es el utilizado por la gran mayoría de fabricantes y clientes, y existe una multitud de productos comerciales. CMIP vs. SNMP

[50]Mauro, «CMIP: CMIP», *CMIP*, 19 de febrero de 2010, http://maurocomputuacioningenieros.blogspot.com/2010/02/cmip.html.

1.7.2. CMOT (Common Management Information Protocol Over TCP/IP).

Protocolo de administración de información común basado en el modelo OSI; definen la comunicación entre las aplicaciones de la administración de red y administración de agentes, definidos en términos de objetos administrados y permite modificar las acciones sobre objetos manejados, similar al concepto X.500[51]. CMOT es simplemente una variante de CMIP implementado sobre un modelo de red TCP/IP, cumple las mismas funciones de intercambio de información de control, y mantenimiento de la red. CMOT[52] y SNMP utilizan los mismos conceptos básicos en la descripción y definición de la administración de la información llamado *Estructura e Identificación de Gestión de Información (SMI)* descrito en el RFC 1155 y *Base de Información de Gestión* (MIB) descritos en el RFC 1156[53].

1.7.3. Simple Network Manager Protocol (SNMP).

El Protocolo Simple de Administración de Red o SNMP, funciona en la capa de aplicación, facilita el intercambio de información administrativa entre diferentes dispositivos de red. Además, permite a los administradores supervisar el desempeño de la red, buscar/resolver problemas, y planificar su crecimiento.

Una ventaja importante es que posee un formato estándar de intercambio de información entre diferentes dispositivos de red independientemente del tipo y del fabricante.

1.8. Metodología A Utilizar

Para desarrollar la presente tesis se creyó conveniente tomar la norma TMN (Telecomunications Management Network) que fue introducida por la ITU-T (esta norma fue propuesta en el año 1998) para facilitar el desarrollo de entornos de gestión distribuidos y heterogéneos (teniendo en cuenta que se posee varios equipos, diferentes arquitecturas). Esta norma proporciona una arquitectura en capas para todas las funciones de las aplicaciones de gestión, además de los protocolos de comunicación entre los elementos de red y el gestor centralizado, entre distintos gestores de red, y entre estos gestores y los operadores humanos.

---

[51]"Definición De X.500 - ¿qué Es X.500?", n.d., http://www.alegsa.com.ar/Dic/x.500.php; "Protocolos X400 y X500", n.d., http://html.rincondelvago.com/protocolos-x400-y-x500.html; Wikipedia contributors, "X.500," *Wikipedia, la enciclopedia libre* (Wikimedia Foundation, Inc., Noviembre 8, 2011), http://es.wikipedia.org/w/index.php?title=X.500&oldid=51203068.

[52]L. Besaw y U. S. Warrier, «Common Management Information Services and Protocol over TCP/IP (CMOT)», accedido 5 de noviembre de 2012, http://tools.ietf.org/html/rfc1095#page-7.

[53]«RFC 1156 - Management Information Base for network management of TCP/IP-based internets», accedido 6 de febrero de 2012, http://tools.ietf.org/html/rfc1156.

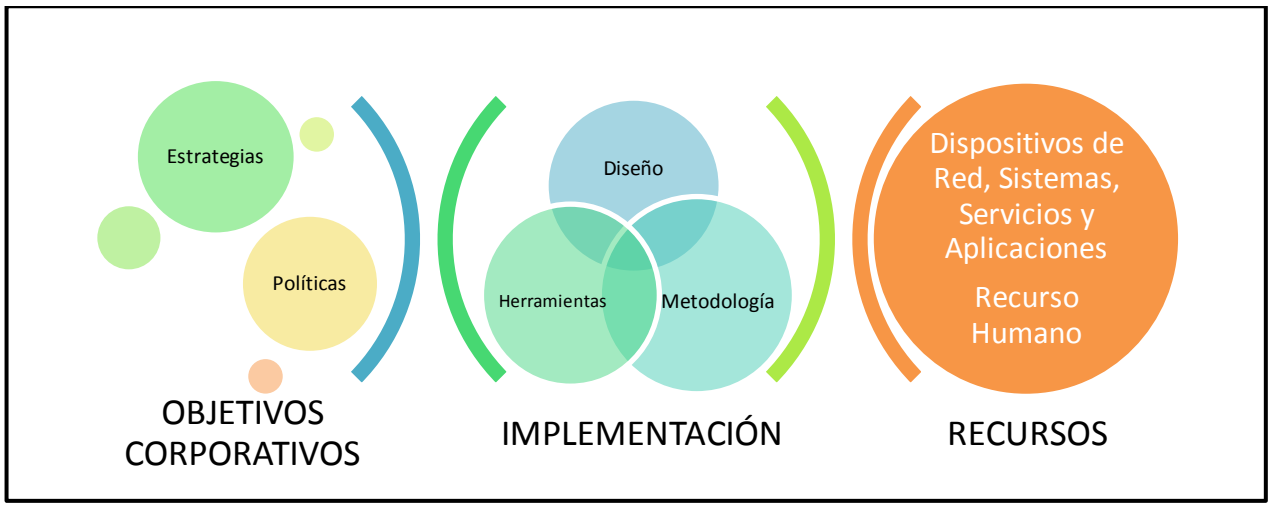


Ilustración 18: Ejes transversales para la implementación de un NOC (Diseño Personal)

Se ha propuesto el esquema anterior para reflejar de mejor manera la estructura de una empresa basada en tres ejes transversales para la implementación de un NOC son:

- **Objetivos Corporativos**

  Son los que permiten especificar los propósitos de la Organización e identificar los aspectos que se deben controlar y tomar en cuenta para lograr las metas, con el fin de colaborar en el cumplimiento de la Misión de la Institución.

  Dentro de los objetivos están:

  - **Estrategias**

    Es el conjunto de acciones planificadas sistemáticamente en el tiempo que se llevan a cabo para lograr un determinado fin.

  - **Políticas**

    Las políticas con directrices creadas en una empresa para dar una orientación de las actividades que se desarrollan de manera conjunta, como a nivel individual.

- **Implementación**

  En esta sección, una vez que se conoce como está estructurada la organización, se propuso el proyecto para desarrollo del NOC teniendo en cuenta que toda la puesta esté alienada a los objetivos corporativos.

Otro aspecto importante, son los beneficios que podría traer la implementación de un sistema de monitoreo en el Área de Sistemas y específicamente en el Centro de

Cómputo, se pueden mencionar los siguientes:

- Ofrecer soporte de monitoreo, gestión, resolución de problemas dentro de una infraestructura de red (servidores, clientes, routers, switches, etc.).
- Disponer de herramientas adecuadas que se adapten a la infraestructura para evaluar y detectar los eventos que pudieran afectar el desempeño de los elementos de la red.
- Mejorar los procesos operacionales para el adecuado control, monitoreo y resolución de problemas.
- Hacer uso eficiente de la red y optimizar los recursos.
- Asegurar la red, protegiéndola contra el acceso no autorizado.
- Controlar cambios y actualizaciones en la red de modo que disminuya la cantidad de interrupciones de servicio(s) a usuarios.

Es por eso, que se ha propuesto lo siguiente para la implementación del NOC:

- **Diseño**

  Para realizar el diseño se debe de conocer primero la estructura organizativa de la empresa y las necesidades que tiene.

  Para el diseño de Gestión de Redes existen cientos de funciones trabajando en forma interrelacionada para el logro de un fin común para el cumplimiento de la visión y misión de la organización.

- **Herramientas**

  La herramienta que se escoja debe de contar con:

  - **Procedimientos de notificación**:
    - ⇒ Configuración de SLA's para el NMS
    - ⇒ Tener un SLA específico para el manejo de errores o problemas del NOC
    - ⇒ Notificación al personal técnico del NOC
    - ⇒ Notificación de alarmas mediante la regla recomendada por Microsoft del 70% en el cumplimiento de umbrales.[54]
    - ⇒ Notificación a clientes, gerentes u otro personal de acuerdo al protocolo pre-establecido dentro de la organización
  - **Sistema de monitoreo y alarma**
    - ⇒ Sistema Automático de Monitoreo
  - **Establecer procedimientos de reparación/recuperación**

[54]«Descripción del rendimiento de Exchange», accedido 14 de mayo de 2012, http://technet.microsoft.com/es-es/library/bb124583%28EXCHG.65%29.aspx.

- ⇒ Documentar procedimientos estándares.
- ⇒ Entrenar al personal técnico,

➢ **Mantener un sistema de manejo de incidencias (ticketingsystem)**

- ⇒ Conocer cantidad, prioridad, y estado de resolución de cada problema
- ⇒ Excelente base de conocimiento, datos históricos
- ⇒ Regla de 80-20: 80% del tiempo se emplea en diagnóstico
- ⇒ Administrar carga de trabajo de ingenieros y operadores.
  - ✓ Ejemplo: RT (RequestTracker)

➢ **El sistema provee:**

- ⇒ Programación y asignación de tareas.
- ⇒ Registro de la notificación.
- ⇒ Registro de tiempo de notificación y otros pasos.
- ⇒ Comentarios, escalamiento, notas técnicas.
- ⇒ Análisis estadístico.
- ⇒ Supervisión y delimitación de responsabilidades. Tomar en cuenta el organigrama del departamento de TI existente en la empresa.

➢ **Crear un caso por cada incidente detectado**

- ⇒ Crear un caso por cada mantenimiento programado.
- ⇒ Enviar copia del caso a quién reporta, y a una lista de distribución.
- ⇒ Quién creó el caso determina cuándo debe ser cerrada la incidencia.
- ⇒ Los estados que puede tener el caso son:

Tabla 1: *Estados de los Casos y su Descripción*

ESTADO DE CASO	DESCRIPCIÓN
REGISTRADO	Este es el primer estado que tiene el caso. Se ingresa cuando se haya detectado algún error.
ASIGNADO	Segundo Estado, que es una vez que se encuentra registrado el caso el Supervisor HELPDESK de acuerdo al tipo de requerimiento lo asigna a la persona(as) responsables
EN PROCESO	Tercer Estado, que es cuando el Colaborador del HELPDESK empieza a desarrollar la solución
SUSPENDIDO	Si existe algún inconveniente, o cuando se

ESTADO DE CASO	DESCRIPCIÓN
	depende de algo que esta fuera del alcance de los Responsables de HELPDESK (pedido de piezas al proveedor, ayuda de soporte externo) se suspende para luego cerrarlo.
SOLUCIONADO	En este paso se realiza cuando se encuentre aplicada solución que de por CORREGIDO el caso o incidente.
ESCALADO A TERCEROS	Cuando se detecta que el problema depende del PROVEEDOR o por falla del APLICATIVO cuya SOLUCIÓN depende de SOPORTE EXTERNO

- **Metodología**

  Esas funciones genéricas están descriptas, en el marco del TMN, en la norma de la ITU-M.3400. Son llamadas *Áreas* Funcionales de los Sistemas de Gestión o SMFA (Systems Management Functional Areas), y se agrupan conformando lo que se conoce como procesos de la operación o FCAPS, estos se solapan verticalmente con el Modelo de Capas antes descripto, tal como se expone en la Ilustración 19.

  En la parte de las CAPAS (extensión de la recomendación ITU-T M.3010) trata de mostrar a quién afecta la administración de redes. Allí se puede observar que la administración técnica sólo es una parte de la pirámide. También debe quedar claro que, en la vida real, no todos los sistemas de administración operan todos los niveles de las CAPAS, aunque es deseable desde el punto de vista de administración integral.

  Lo que se hace evidente entre cada una de las CAPAS es que el éxito de la administración depende del éxito en todos los niveles (el nivel N no puede ser administrado efectivamente si el nivel N-1 no se opera efectivamente y, viceversa, si el nivel N no tiene claro qué quiere, el nivel N-1 no podrá apoyarlo correctamente).

Ilustración 19: Áreas Funcionales con respecto a modelo de capas[55]

- **Recursos**[56]

  Son todos aquellos bienes y servicios utilizados para ser transformados en productos o servicios. Hasta hace poco eran los llamados recursos reales o tangibles, específicamente los recursos humanos, físicos, y financieros.

Recursos reales o tangibles

a) Recursos humanos: los asignables a las personas, incluidas habilidades y talentos.
b) Recursos físicos: los asignables a las cosas, maquinarias, infraestructura, tierra, y recursos de la naturaleza.
c) Recursos financieros: los asignables al precio o valor monetario que se les asigna en las economías de intercambio. Como tal, pasan a constituir una reserva de los demás recursos en poder de las organizaciones.

Recursos intangibles

a) Recursos información y conocimientos: los asignables al conocimiento y a la tecnología de las organizaciones, al cómo se hacen las cosas y al por qué se hacen de esa manera.

[55] Diseño Personal. El modelo en capas esta descrito más a fondo en el Anexo 2. Metodología en Capas del Modelo TMN.
[56] «Los recursos en las organizaciones», *ZEN EN LA ORGANIZACIÓN*, s. f., http://zenempresarial.wordpress.com/2010/03/16/los-recursos-en-las-organizaciones/.

b) Recursos relaciones y alianzas: los asignables a la interacción entre las personas. Los negocios son relaciones sociales, se hacen entre personas, y el contacto personal constituye todo un recurso que puede o no ayudar a un negocio.

1.9. Base de Información para la Gestión[57]

También conocida como por sus siglas en inglés como MIB (Management Information Base) es un tipo de base de datos que contiene información representada en forma jerárquica, con estructura en forma de árbol de todos los dispositivos gestionados en una red de comunicaciones.

Cada objeto manejado en un MIB tiene un identificador único de objeto e incluye: el *tipo de objeto* (tal como contador, secuencia indicador), el *nivel de acceso* (tal como lectura y escritura), *restricciones de tamaño*, y la *información del rango del objeto*.

Los MIB tienen un formato común de modo que aun cuando los dispositivos sean de fabricantes distintos puedan ser administrados con un protocolo estándar.

Protocolo de administración: es el protocolo mediante el cual se consultan los objetos administrados enviando la información a la estación administradora.

Objeto MIB

De forma sencilla, un objeto MIB representa alguna característica del dispositivo administrado a través de una o más variables. Un objeto MIB se define especificando:

- ✓ **Sintaxis**: Especifica el tipo de datos de que manejará el objeto. Por ejemplo entero, cadena, dirección IP, etc.
- ✓ **Acceso**: Especifica el nivel de permiso para manejar el objeto. Este nivel puede ser de lectura, lectura y escritura, escritura, o no accesible
- ✓ **Estado**: Define si el uso del objeto es obligatorio u opcional.
- ✓ **Descripción**: Describe textualmente al objeto.

Según (SOSA-SOSA, 2008)[58], existen dos tipos de objetos MIB:

- ✓ Escalares: Son objetos que tienen una sola instancia de la variable que almacenan.
- ✓ Tabulares: Son objetos que definen múltiples instancias relacionadas a objetos

[57] Dr. Víctor J. SOSA-SOSA, «MIB.pdf», s. f., http://www.tamps.cinvestav.mx/~vjsosa/clases/redes/MIB.pdf. (SOSA-SOSA, 2008)
[58] Ibid. Dr. Víctor J. SOSA-SOSA, «MIB.pdf», s. f., http://www.tamps.cinvestav.mx/~vjsosa/clases/redes/MIB.pdf. (SOSA-SOSA, 2008)

contenidos en la MIB.

1.9.1. Jerarquía.

Los objetos asociados a variables están organizados en una jerarquía administrada por la ISO y por la ITU-T.

En esta jerarquía cada objeto posee un nombre simbólico y un identificador numérico asociado, de tal forma que, dentro de ese árbol jerárquico, esté determinado por un identificador único, que representa su localización relativa en la raíz del árbol.

Sólo una porción de esa jerarquía, que representa los objetos relativos al gerenciamiento de red, es conocida como MIB - Management Information Base, y su localización en la jerarquía puede ser visualizada en la siguiente figura:

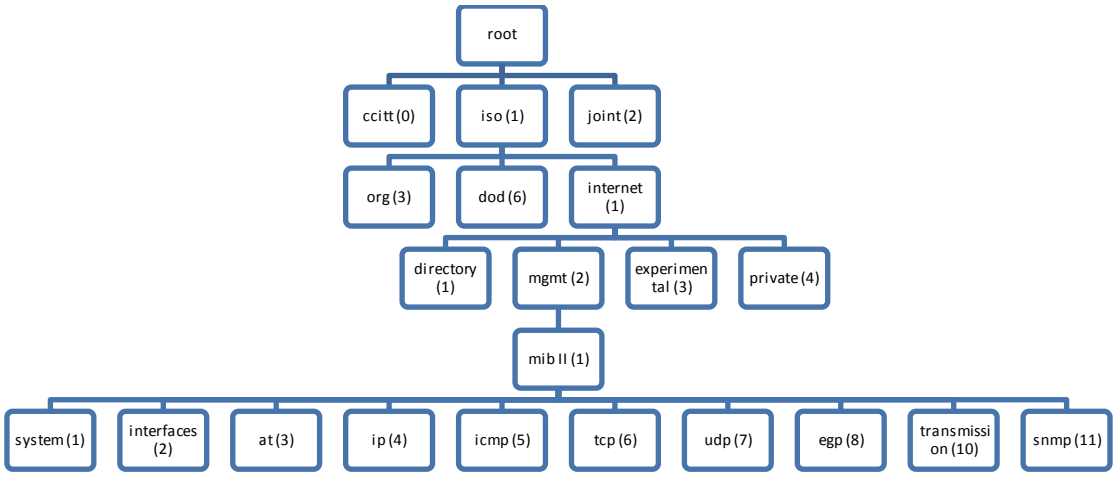


Ilustración 20: Árbol de la Infraestructura MIB[59]

Algunas descripciones de los objetos del MIB según ANS.1 del árbol presentado en la Ilustración 20: Árbol de la Infraestructura MIB.

- ***Subárbol OID de internet (1.3.6.1)***[60]

directory (1.3.6.1.1)

  - Uso futuro.
  - Previsto que contenga información sobre el servicio de directorio OSI, X.500.

mgmt (1.3.6.1.2)

[59] Dani Gutiérrez Porset, «Gestión de redes, SNMP y RMON», abril 1, 2011, http://www.slideshare.net/danitxu/snmp-rmon.

[60] VICTOR HINOJOSA, LUIS MADRUÑERO, y LUIS ORTEGA, «Sistema de gestión de red», Tesis, junio 6, 2011, http://repositorio.utn.edu.ec/handle/123456789/577; Víctor Hugo Hinojosa Jaramillo, Luis Vicente Ortega Pilco, y Luis Alberto Madruñero Padilla., «Sistema de gestión de red» (Universidad Técnica del Norte, 2011), http://repositorio.utn.edu.ec/bitstream/123456789/577/1/AnexoE.doc.

- Información de gestión para protocolos del DoD (Departamento de Defensa de los EEUU), en el subárbol **mib**(1).

experimental (1.3.6.1.3)

- Protocolos y MIBs experimentales, aún no son estándar.
- Se estandarizarán complementando a MIB II.

private (1.3.6.1.4)

- MIBs particulares de empresas (añaden funcionalidad).
- Cada empresa tiene su propio árbol a partir de private.
- Para una completa referencia consultar: http://www.mibcentral.com

- ***Subárbol OID mgmt (1.3.6.1.2)***

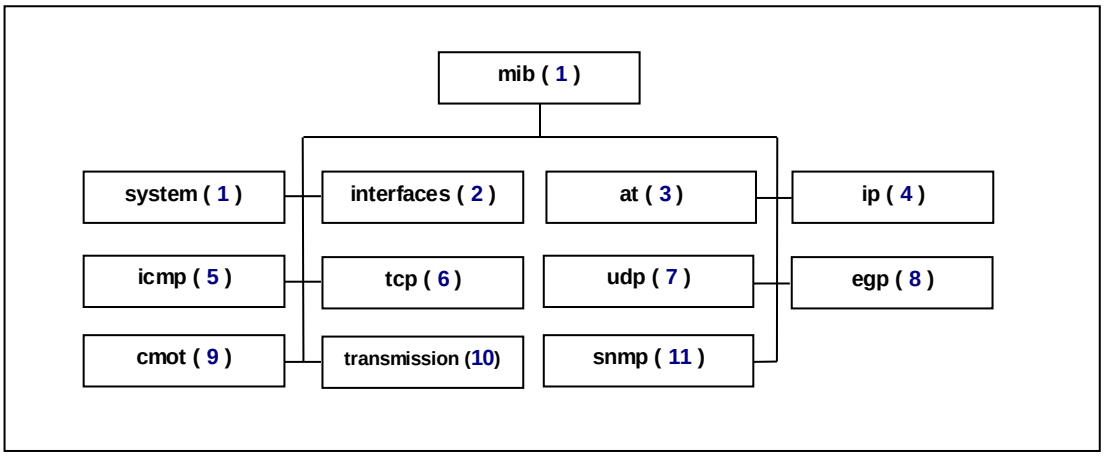
mib (1.3.6.1.2.1)

Contiene información de gestión para los protocolos del Departamento de defensa de los EEUU (DoD) en el sub-árbol MIB.

- Originalmente tenía MIB I (RFC-1052).
- Actualmente se ha ampliado con MIB II (RFC-1213).

Las diferencias fundamentales de MIB II con respecto a MIB I son:

- Los objetos del **grupo at**, se han trasladado a otros grupos, quedando este vacío.
- El grupo **cmot**, se mantiene por razones históricas; al principio se introdujo para ayudar a la transición a CMIS/CMIP.
- Ha aumentado el número de objetos de algunos grupos: **system**, **interfaces**, **ip** y **tcp**.
- Se han creado nuevos grupos: **transmission** (información sobre medios específicos de transmisión: Token Ring, FDDI)y **snmp**.
- Nuevos tipos predefinidos: **DisplayString** y **PhysAddress**.



Arbol OID – grupos de mib estándar

mib - system (1.3.6.1.2.1.1)

Contiene información sobre el sistema en el que se encuentra instalado el agente (entidad).

Este grupo contiene siete objetos:

- **sysDescr (1.3.6.1.2.1.1.1):** descripción del equipo/sistema.
- **sysObjectID (1.3.6.1.2.1.1.2):** Identificador asignado por el fabricante.
- **sysUptime (1.3.6.1.2.1.1.3):** tiempo de funcionamiento del servicio/agente SNMP en el equipo/sistema
- **sysContact (1.3.6.1.2.1.1.4):** persona responsable del equipo/sistema**.**
- **sysName (1.3.6.1.2.1.1.5):** nombre del equipo/sistema.
- **sysLocation (1.3.6.1.2.1.1.6):** localización física.
- **sysServices (1.3.6.1.2.1.1.7):** niveles OSI que soporta el equipo: $\Sigma\ 2^{L-1}$.

Estas variables MIB de sistema pueden ser empleadas para labores de:

GESTIÓN DE FALLOS:

- **sysObjectID (1.3.6.1.2.1.1.2), sysUptime(1.3.6.1.2.1.1.3)** y **sysServices (1.3.6.1.2.1.1.7)**

GESTIÓN DE LA CONFIGURACIÓN:

- **sysDescr (1.3.6.1.2.1.1.1), sysContact(1.3.6.1.2.1.1.4), sysName(1.3.6.1.2.1.1.5), sysLocation (1.3.6.1.2.1.1.6)**

mib - interfaces (1.3.6.1.2.1.2)

Contiene información sobre cada interfaz en un dispositivo de red.

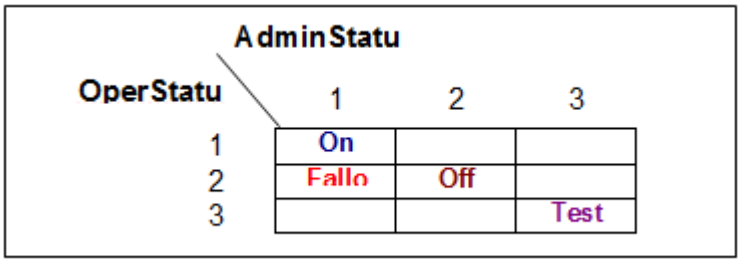
- **ifNumber (1.3.6.1.2.1.2.1):** número de interfaces de la entidad.
- **ifTable (1.3.6.1.2.1.2.2):** tabla de interfaces de la entidad.
  - **IfEntry (1.3.6.1.2.1.2.2.1):** Entradas para una interfaz específica.
    - **IfIndex (1.3.6.1.2.1.2.2.1.1):** valor único para cada interfaz, su valor se encuentra en el rango de 1 a ifNumber.
    - **IfDescr (1.3.6.1.2.1.2.2.1.2):** nombre de la interfaz.
    - **IfType (1.3.6.1.2.1.2.2.1.3):** tipo de interfaz (ej: 6=”ethernet CSMA/CD”).
    - **IfMtu (1.3.6.1.2.1.2.2.1.4):** tamaño del datagrama.
    - **IfSpeed (1.3.6.1.2.1.2.2.1.5):** velocidad en la interfaz en un momento dado (útil para interfaces que cambian de velocidad como módem; en ethernet = 10000000).
    - **IfPhysAddress (1.3.6.1.2.1.2.2.1.6):** direcciones físicas de las interfaces.
    - **IfAdminStatus (1.3.6.1.2.1.2.2.1.7):** estado administrativo de la interfaz (up=1 / down=2 / testing=3).
    - **IfOperStatus (1.3.6.1.2.1.2.2.1.8):** estado operacional actual de la interfaz (up=1 / down=2 / testing=3).
    - **IfLastChange (1.3.6.1.2.1.2.2.1.9):** tiempo desde el último cambio de estado de la interfaz (a estado operativo, guarda relación con el subsistema de gestión del equipo).
    - **IfInOctets (1.3.6.1.2.1.2.2.1.10):** número total de octetos(bytes) recibidos en la interfaz.
    - **IfInUcastPkts (1.3.6.1.2.1.2.2.1.11):** número de paquetes unicast enviados desde la capa de red hasta la capa de aplicación.
    - **IfInNUcastPkts (1.3.6.1.2.1.2.2.1.12):** número de paquetes no – unicast (broadcast y multicast) enviados desde la capa de red hasta la capa de aplicación.
    - **IfInDiscarts (1.3.6.1.2.1.2.2.1.13):** número de paquetes entrantes que fueron escogidos para ser descartados para prevenir errores en las capas más altas del modelo OSI.
    - **IfInErrors (1.3.6.1.2.1.2.2.1.14):** número de paquetes entrantes que contienen errores.
    - **IfInUnknownProtos (1.3.6.1.2.1.2.2.1.15):** número de paquetes recibidos a través de la interfaz, pero que son descartados por ser desconocidos o porque no son soportados por el protocolo.
    - **IfOutOctets (1.3.6.1.2.1.2.2.1.16):** número de octetos(bytes) transmitidos fuera de la interfaz.

- **IfOutUcastPkts (1.3.6.1.2.1.2.2.1.17):** número de paquetes unicast solicitados por las capas más altas del modelo OSI para ser transmitidos hacia direcciones unicasts.
- **IfOutNUcastPkts (1.3.6.1.2.1.2.2.1.18):** número de paquetes solicitados por las capas más altas del modelo OSI para ser transmitidos hacia direcciones no unicast (broadcast y multicast).
- **IfOutDiscarts (1.3.6.1.2.1.2.2.1.19):** número de paquetes salientes que fueron escogidos para ser descartados para prevenir errores en la transmisión de los paquetes.
- **IfOutErrors (1.3.6.1.2.1.2.2.1.20):** número de paquetes que no pueden ser transmitidos por causa de errores.
- **IfOutQLen (1.3.6.1.2.1.2.2.1.21):** número de paquetes en la cola de salida.
- **IfSpecific (1.3.6.1.2.1.2.2.1.22):** referencia a definiciones MIB específicas para medios particulares usados en la interfaz (ej: si la interfaz es realizada por ethernet, entonces el valor de este objeto se refiere al documento que define los objetos específicos de ethernet.).

Estas variables MIB de interfaces pueden ser empleadas para labores de:

GESTIÓN DE FALLOS:

- **ifAdminStatus(1.3.6.1.2.1.2.2.1.7), ifOperStatus (1.3.6.1.2.1.2.2.1.8)** y **ifLastChange (1.3.6.1.2.1.2.2.1.9)**



GESTIÓN DE LA CONFIGURACIÓN:

- **ifDescr (1.3.6.1.2.1.2.2.1.2), ifType(1.3.6.1.2.1.2.2.1.3), ifMtu(1.3.6.1.2.1.2.2.1.4), ifSpeed (1.3.6.1.2.1.2.2.1.5), ifAdminStatus(1.3.6.1.2.1.2.2.1.7)**

GESTIÓN DEL RENDIMIENTO:

- **ifInDiscart (1.3.6.1.2.1.2.2.1.13), IfOutDiscarts (1.3.6.1.2.1.2.2.1.19)**

- **IfInErrors (1.3.6.1.2.1.2.2.1.14), IfOutErrors (1.3.6.1.2.1.2.2.1.20)**
- **IfInOctets (1.3.6.1.2.1.2.2.1.10), IfOutOctets (1.3.6.1.2.1.2.2.1.16)**
- **IfInUcastPkts (1.3.6.1.2.1.2.2.1.11), IfOutUcastPkts (1.3.6.1.2.1.2.2.1.17)**
- **IfInNUcastPkts (1.3.6.1.2.1.2.2.1.12), IfOutNUcastPkts (1.3.6.1.2.1.2.2.1.18)**

Total Paquetes = Unicast + No Unicast

- **IfInUnknownProtos (1.3.6.1.2.1.2.2.1.15)**
- **IfOutQLen (1.3.6.1.2.1.2.2.1.21)**

mib - ip (1.3.6.1.2.1.4)

Contiene información de entidad IP, dividida en áreas:

- Información sobre errores y tipos de paquetes.
- Tabla de información sobre direcciones IP de la entidad.
- Tabla de rutas IP de la entidad.
- Mapa de traducción de direcciones IP con otros protocolos.

- **ipForwarding (1.3.6.1.2.1.4.1):** indica si el dispositivo está configurado para reenviar tráfico (comportamiento de router) (1) caso contrario (2).
- **ipDefaultTTL (1.3.6.1.2.1.4.2):** valor de "tiempo de vida" para la cabecera de los datagramas enviados por la entidad.
- **ipInReceives (1.3.6.1.2.1.4.3):** cantidad de datagramas recibidos.
- **ipInHdrErrors (1.3.6.1.2.1.4.4):** número de datagramas descartados debido a errores en las cabeceras IP.
- **ipAddrErrors (1.3.6.1.2.1.4.5):** número de datagramas entrantes descartados debido a que las direcciones IP en las cabeceras de destino no tienen direcciones válidas para ser recibidas en la entidad.
- **ipForwDatagrams (1.3.6.1.2.1.4.6):** número de datagramas reenviados a su destino final,
- **ipInUnknownProtos (1.3.6.1.2.1.4.7):** número de datagramas direccionados localmente recibidos con éxito, pero descartados debido a un protocolo desconocido o no soportado.
- **ipInDiscarts (1.3.6.1.2.1.4.8):** datagramas recibidos que se descartan.
- **ipInDelivers (1.3.6.1.2.1.4.9):** datagramas recibidos y entregados al nivel superior (sin error).

- **ipOutRequests (1.3.6.1.2.1.4.10):** datagramas enviados, no se cuentan los reenviados.
- **ipOutDiscarts (1.3.6.1.2.1.4.11):** datagramas de salida descartados.
- **ipOutNoRoutes (1.3.6.1.2.1.4.12):** datagramas descartados por falta de información de rutas.
- **ipReasmTimeout (1.3.6.1.2.1.4.13):** número máximo de segundos que los fragmentos recibidos son retenidos mientras esperan ser reensamblados en esta entidad.
- **ipReasmReqds (1.3.6.1.2.1.4.14):** fragmentos IP recibidos que necesitan ser reensamblados.
- **ipReasmOKs (1.3.6.1.2.1.4.15):** datagramas IP reensamblados satisfactoriamente.
- **ipReasmFails (1.3.6.1.2.1.4.16):** número de fallas durante el reensamblaje de fragmentos IP.
- **ipFragOKs (1.3.6.1.2.1.4.17):** número de datagramas IP que han sido fragmentados satisfactoriamente en la entidad.
- **ipFragFails (1.3.6.1.2.1.4.18):** datagramas IP que han sido descartados debido a que la bandera de no fragmentación ha sido establecida.
- **ipFragCreates (1.3.6.1.2.1.4.19):** número de datagramas IP que han sido generados debido a una fragmentación en la entidad.

- **ipAddrTable (1.3.6.1.2.1.4.20):** tabla de información de direccionamiento relevante a las direcciones IP de la entidad.
  - **IpAddrEntry (1.3.6.1.2.1.4.20.1):** Información específica de direccionamiento de las direcciones IP de la entidad.
    - **IpAdEntAddr (1.3.6.1.2.1.4.20.1.1):** dirección IP a la que esta entrada de direccionamiento pertenece.
    - **IpAdEntIfIndex (1.3.6.1.2.1.4.20.1.2):** valor que identifica de manera única a la interfaz a la que esta entrada es aplicable.
    - **IpAdEntNetMask (1.3.6.1.2.1.4.20.1.3):** máscara de subred asociada con la dirección IP de esta entrada.
    - **IpAdEntBCastAddr (1.3.6.1.2.1.4.20.1.4):** valor del bit menos significativo en la dirección de broadcast, usado para enviar datagramas en la interfaz asociada con la dirección IP de esta entrada.
    - **IpAdEntReasmMaxSize (1.3.6.1.2.1.4.20.1.5):** tamaño del datagrama más grande que esta interfaz puede reensamblar de los fragmentos de datagrama IP entrantes recibidos en esta interfaz.

- **IpRouteTable (1.3.6.1.2.1.4.21):** tabla de enrutamiento IP de las entidades.
  - **IpRouteEntry (1.3.6.1.2.1.4.21.1):** ruta para un destino particular.
    - **IpRouteDest (1.3.6.1.2.1.4.21.1.1):** dirección IP de destino de esta ruta.
    - **IpRouteIfIndex (1.3.6.1.2.1.4.21.1.2):** valor de índice único que identifica la interfaz local hasta que se alcance el siguiente salto de ruta.
    - **IpRouteMetric1 (1.3.6.1.2.1.4.21.1.3):** métrica de ruteo primaria para esta ruta.
    - **IpRouteMetric2 (1.3.6.1.2.1.4.21.1.4):** métrica de ruteo alternativa para esta ruta.
    - **IpRouteMetric3 (1.3.6.1.2.1.4.21.1.5):** métrica de ruteo alternativa para esta ruta.
    - **IpRouteMetric4 (1.3.6.1.2.1.4.21.1.6):** métrica de ruteo alternativa para esta ruta.
    - **IpRouteNextHop (1.3.6.1.2.1.4.21.1.7):** dirección IP del siguiente salto de esta ruta.
    - **IpRouteType (1.3.6.1.2.1.4.21.1.8):** tipo de ruta (1=otra, 2=no-válida, 3=directa, 4=indirecta).
    - **IpRouteProto (1.3.6.1.2.1.4.21.1.9):** mecanismo de ruteo mediante el cual la ruta es aprendida (**ej:** 2=local, 3=netmgmt, 4=icmp, 5=egp, 13=ospf, 14=bgp, etc).
    - **IpRouteAge (1.3.6.1.2.1.4.21.1.10):** número de segundos desde que esta ruta fue actualizada o determinada correcta.
    - **IpRouteMask (1.3.6.1.2.1.4.21.1.11):** muestra la máscara del AND lógico de la dirección de destino antes de ser comparada con el valor del campo ***IpRouteDest***.
      - **IpRouteMetric5 (1.3.6.1.2.1.4.21.1.12):** métrica de ruteo alternativa para esta ruta.
      - **IpRouteInfo (1.3.6.1.2.1.4.21.1.13):** referencia a definiciones MIB específicas al protocolo de ruteo que es responsable de la ruta, es determinado por el valor de ***IpRouteProto***.

  - **IpNetToMediaTable (1.3.6.1.2.1.4.22):** tabla de resolución de direcciones IP, usada para mapear las direcciones IP a direcciones físicas.
    - **IpNetToMediaEntry (1.3.6.1.2.1.4.22.1):** cada entidad contiene una dirección IP con su dirección física equivalente.
      - **IpNetToMediaIfIndex (1.3.6.1.2.1.4.22.1.1):** interfaz en la que esta equivalencia de entradas es válida.

- **IpNetToMediaPhysAddress (1.3.6.1.2.1.4.22.1.2):** dirección física dependiente del medio.
- **IpNetToMediaNetAddress (1.3.6.1.2.1.4.22.1.3):** dirección IP correspondiente a la dirección física dependiente del medio.
- **IpNetToMediaType (1.3.6.1.2.1.4.22.1.4):** tipo de mapeo (1=otro, 2=no-válido, 3= estático, 4=dinámico).

- **IpRoutingDiscards (1.3.6.1.2.1.4.23):** número de entradas de ruteo que se escogieron para ser descartadas mientras eran no-válidas.

Estas variables MIB IP pueden ser empleadas para labores de:

GESTIÓN DE FALLOS:

- IpRouteTable (1.3.6.1.2.1.4.21)
  - IpRouteIfIndex (1.3.6.1.2.1.4.21.1.2)
  - IpRouteMetric1 (1.3.6.1.2.1.4.21.1.3), IpRouteMetric2 (1.3.6.1.2.1.4.21.1.4), IpRouteMetric3 (1.3.6.1.2.1.4.21.1.5), IpRouteMetric4 (1.3.6.1.2.1.4.21.1.6), IpRouteMetric5 (1.3.6.1.2.1.4.21.1.12)
  - IpRouteNextHop (1.3.6.1.2.1.4.21.1.7)
  - IpRouteType (1.3.6.1.2.1.4.21.1.8) y IpRouteProto (1.3.6.1.2.1.4.21.1.9)

- IpNetToMediaTable (1.3.6.1.2.1.4.22)

GESTIÓN DE LA CONFIGURACIÓN:

- **ipForwarding (1.3.6.1.2.1.4.1), ipDefaultTTL (1.3.6.1.2.1.4.2), ipAddrTable (1.3.6.1.2.1.4.20), IpRouteTable (1.3.6.1.2.1.4.21)**

GESTIÓN DEL RENDIMIENTO:

- **ipInReceives (1.3.6.1.2.1.4.3), ipInHdrErrors (1.3.6.1.2.1.4.4), ipAddrErrors (1.3.6.1.2.1.4.5), ipForwDatagrams (1.3.6.1.2.1.4.6), ipInUnknownProtos (1.3.6.1.2.1.4.7), ipInDiscarts (1.3.6.1.2.1.4.8), ipInDelivers (1.3.6.1.2.1.4.9).**
- **ipOutRequests (1.3.6.1.2.1.4.10), ipOutDiscarts (1.3.6.1.2.1.4.11), ipOutNoRoutes (1.3.6.1.2.1.4.12)** e **IpRoutingDiscards (1.3.6.1.2.1.4.23)**

- **ipReasmReqds (1.3.6.1.2.1.4.14), ipReasmOKs (1.3.6.1.2.1.4.15), ipReasmFails (1.3.6.1.2.1.4.16), ipFragOKs (1.3.6.1.2.1.4.17), ipFragFails (1.3.6.1.2.1.4.18), ipFragCreates (1.3.6.1.2.1.4.19).**

ELEMENTOS A INSTALAR

La información a monitorizar puede encontrase en una de las siguientes categorías:

- **La información Estática**: Es generada y almacenada por el propio elemento de red (p.e. un ruteador almacena su propia configuración).
- **La información Dinámica:** Puede almacenarla el propio elemento, u otro encargado de ello (p.e. En una LAN cada elemento puede almacenar el número total de paquetes que envía, o un elemento de la LAN puede estar escuchando y recoger esa información (se denomina **Monitor remoto).** Un monitor remoto no puede recoger cierta información propia de un elemento (p.e. El número de sesiones abiertas).
- **La información Estadística**: Puede ser generada por cualquier elemento que tenga acceso a la información dinámica en base a dos opciones básicas:
  - Puede enviarse toda la información dinámica al gestor de red para que realice las estadísticas.
  - Si el gestor no necesita toda la información, ésta puede ser resumida por el propio elemento antes de enviarla al gestor, ahorrando procesamiento en el gestor y generando menos tráfico en la red.

1.9.2. Estructura

- Todos los objetos de la MIB de SNMP, se identifican de la siguiente forma: {iso identigfied-organization(3) dod(6) internet(1) mgmt(2) mib-2(1)...} o, de manera alternativa {1 3 6 1 2 1...}
- La MIB tiene 126 áreas de información sobre el estado del dispositivo, el desempeño del dispositivo, sus conexiones hacia los diferentes dispositivos y su configuración.
- El administrador SNMP consulta la MIB a través del software agente y puede especificar los cambios que se le hicieron a la configuración.
- La mayor parte de los administradores SNMP consultan a los agentes en un intervalo regular, 30 minutos por ejemplo, a menos que de acuerdo a los parámetros configurados de refresco de la información sea modificado por indicaciones de Gerencia de Sistemas. Además, con esto precautelamos que los enlaces no se saturen por la realización de consultas SNMP.

- El software agente SNMP por lo general es bastante pequeño (comúnmente de 64KB) dado que el protocolo SNMP es sencillo. SNMP está diseñado para ser un protocolo de sondeo (polling). Los mensajes SNMP se colocan dentro de un datagrama UDP y se enrutan vía IP (aunque podrían utilizarse otros protocolos).

1.9.3. Mensajes MIB

La estructura de mensajes que se utiliza para el envío y recepción de información solos los mismos del protocolo del SNMP, y son:

- **Get request (Obtener solicitud):** Utilizado para consultar una MIB.
- **Get next request (Obtener la siguiente solicitud):** Utilizado para leer secuencialmente a través de una MIB.
- **Get response (Obtener respuesta):** Utilizado para lograr una respuesta a un mensaje para obtener solicitud (getrequest).
- **Set request (Fijar solicitud):** Utilizado para fijar un valor en la MIB.
- **Trap (Trampa):** Utilizado para reportar fallas a eventos.

SINTAXIS

En el **RFC 1155**[61] están definidos los siguientes tipos de objetos:

- **Tipos primitivos**
  - **Integer:** para objetos que se representen con un número entero.
  - **Octet String:** para texto.
  - **Null:** cuando el objeto carece de valor.
  - **Object Identifier:** para nodos estructurales.
  - **Sequence y Sequence of:** para arrays.

- **Tipos Definidos**
  - **IpAddress:** para direcciones IP
  - **Counter:** para contadores.
  - **Gauge**
  - **Timeticks:** para medir tiempos. Cuenta en centésimas de segundos.
  - **Opaque:** para cualquier otra sintaxis ASN.1.

- **Tipos Constructor**
  - Las tablas son un tipo estructurado. se definen usando los tipos "Sequence" y "Sequence of" y la cláusula "index". La tabla consiste en un array ("secuence of") de filas, cada una formada por un "Sequence" que define la columna.

[61] «RFC 1155», s. f., https://datatracker.ietf.org/doc/rfc1155/.

1.9.4. FORMATOS

ASN.1 (Abstract Syntax Notation)

La definición de un objeto sigue un "lenguaje" conocido como ASN.1, que es una representación un tanto compleja a una primera vista, pero es extremadamente funcional y define los atributos de un objeto, permitiendo a el gestor (estación de administración) conocer de antemano como debe tratar tal objeto, además de definir como ese objeto debe ser implementado en un agente.

Tabla 2: *Tipos de Datos Primitivos ASN. 1*

TIPO PRIMITIVO	SIGNIFICADO	CÓDIGO
INTEGER	Entero de longitud arbitraria	2
BIT STRING	Cadena de cero o más bits	3
OCTED STRING	Cadena de cero o más bytes	4
NULL	Marcador de lugar	5
OBJECT IDENTIFIER	Tipo de datos definido oficialmente	6

Por ejemplo, la variable TAL de datagramas IP es definida en el documento RFC1213 de la siguiente forma:

ipDefault TTL OBJCT-TYPE

SYNTAX INTEGER

ACCESS read-write

STATUS mandatory

DESCRIPTION

"The default value inserted into the Time-To-Live field of the IP header of datagram originated at this entity, whenever aTTL value is not supplied by the transport layer protocol"

::= { ip 2 }

2. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED DEL BANCO DE LOJA

2.1. Introducción a la Empresa

En el capítulo presente, se dará una descripción del Banco de Loja, de cómo se lleva la administración de su infraestructura IT.

2.1.1. Historia[62]

El 1 de Julio de 1968 Banco de Loja abrió sus puertas al público, respondiendo así a la necesidad de los diversos sectores de la sociedad lojana de poseer un Banco propio, que atendiera la creciente demanda de crédito de la región sur del país.

2.1.2. Ubicación

Sus oficinas se encuentran distribuidas estratégicamente a lo largo de la provincia de Loja y también cuenta con agencias en provincias como: Pichincha, Zamora Chinchipe y Morona Santiago (Ver Ilustración 21: Ubicaciones a Nivel Nacional).

Ilustración 21: Ubicaciones a Nivel Nacional[63]

La oficina principal del Banco de Loja se encuentra ubicada en las calles Bolívar y Rocafuerte esquina en la capital provincial de Loja, cuya ciudad lleva el mismo nombre, además tiene 4 agencias distribuidas a lo largo de la ciudad que son: Agencia 1, Agencia Hipervalle, Agencia Norte y Agencia Sur.

También existen 4 ventanillas de extensión en las siguientes ubicaciones:

- Universidad Técnica Particular de Loja (UTPL).
    - Ubicado en la Marcelino Champagnat S/N y París.

[62]Tomada de la página institucional del Banco de Loja, Disponible en web: www.bancodeloja.fin.ec
[63]Tomada de la página institucional del Banco de Loja, Disponible en web: www.bancodeloja.fin.ec

- Universidad Nacional de Loja (UNL).
    - Ciudadela Universitaria.
- Mercado Centro Comercial.
    - Segunda Planta Alta, del Mercado Centro Comercial.
- Empresa Eléctrica (EERSSA)
    - En la Olmedo y Rocafuerte esquina.

A nivel de la provincia de Loja tiene 5 Agencias ubicadas en:

Alamor, Catacocha, Catamayo, Cariamanga y Macara.

En la Provincia de Zamora:

Zamora, Yantzatza, El Pangui.

En la Provincia de Macas:

San Juan Bosco y Gualaquiza.

Y posee dos agencias en la provincia de Pichincha y específicamente en la ciudad de Quito:

En el centro comercial el Recreo y en la Av. 6 de Diciembre y Whimper. (En la Ilustración 22: Distribución de cada una de las Agencias pordemos ver la distribución de agencias, ventanillas que tiene el banco de Loja)

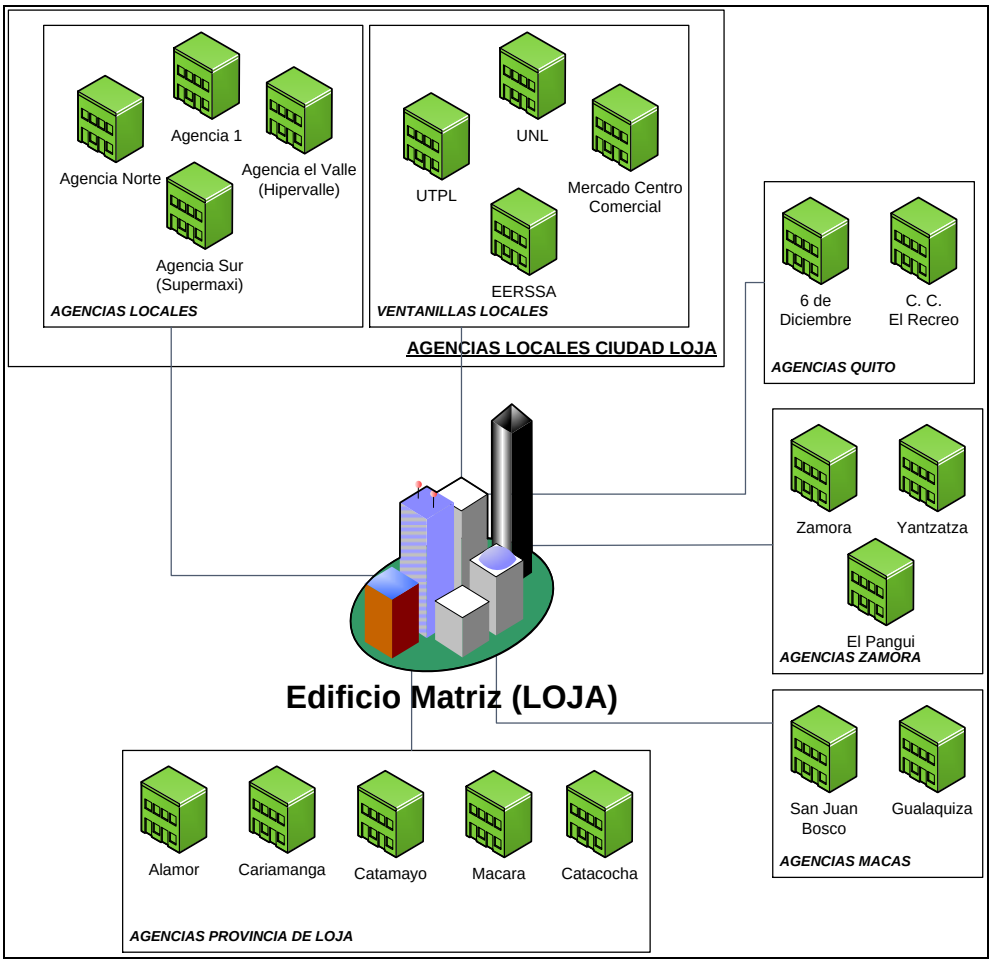


Ilustración 22: Distribución de cada una de las Agencias[64]

2.2. Organigrama departamental del Área De Sistemas

El organigrama se encuentra distribuido de la siguiente manera:

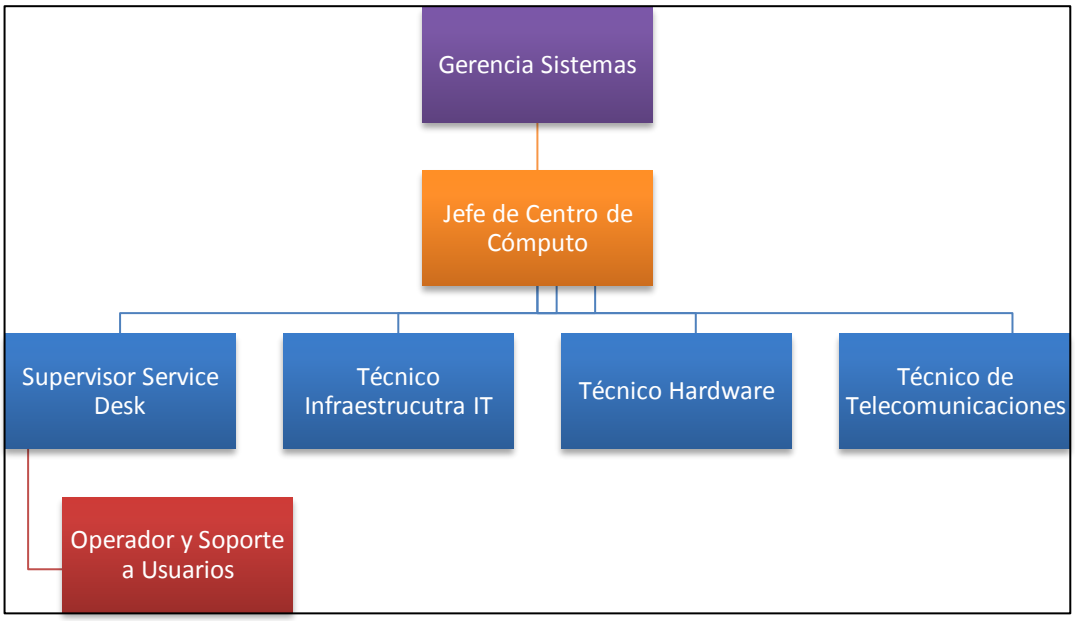


Ilustración 23: Organigrama Departamental Área de Sistemas

[64] Diseño Personal

2.3. Infraestructura Disponible

La infraestructura disponible del Banco de Loja se centraliza en la virtualización de servicios, dispone de tecnología nueva que cumple los más altos estándares internacionales de tecnología y se encuentra a la altura de grandes Bancos. El Banco de Loja posee la siguiente infraestructura:

2.3.1. Servidores

La infraestructura del Banco de Loja tiene importancia en la red, se destacan para efectos de este estudio equipos considerados críticos para las operaciones empresariales. Algunos de estos corresponden a dispositivos que ofrecen los servicios de mayor tráfico en la red, otros son considerados por aplicaciones cruciales que manejan de acuerdo al personal de la Coordinación de TIC. Así se mencionan además de servidores, dispositivos dentro de la red (networking) que poseen la mayor carga de información.

Tabla 3: *Servidores Internos*

SERVIDORES	IMPORTANCIA
CORE FINANCIERO	Alta
Correo	Alta
Página WEB	Alta
SERVICIO PAGUE YA, IEESS	Alta
SERVIDOR DE GIROS	Alta
SIM	Alta
UTPL	Alta
IVR-Elastix	Alta
Internet (navegación)	Alta
WAN	Alta
LAN	Alta
Proxy	Alta
Metaframe	Alta
Symantec	Alta
Swift	Alta
Facturación combustibles	Alta
Consola de Symantec	Alta
Consola de SMTP	Alta
Consola de Checkpoint	Alta
Consola de Swift	Alta

Tabla 4: *Servidores en cada Agencia*

SERVIDORES AGENCIAS	IMPORTANCIA
Agencia 1	Alta
Supermaxi	Alta
Agencia Norte	Alta
Agencia Alamor	Alta
Agencia Catacocha	Alta
Agencia Catamayo	Alta
Agencia Cariamanga	Alta
Agencia Macará	Alta
Agencia San Juan Bosco	Alta
Agencia Gualaquiza	Alta
Agencia Zamora	Alta
Agencia El Pangui	Alta
Agencia Yantzatza	Alta
Agencia 6 de Diciembre	Alta
Agencia C. C. el Recreo	Alta

2.3.2. Cuarto de Equipo

El cuarto de equipo se encuentra en la primera planta del edificio Matriz, acondicionado de acuerdo al estándar **ANSI/TIA/EIA-569-A**[65] para el mantenimiento de infraestructura IT. Aquí se encuentran los servidores que se especificó anteriormente.

Los equipos se encuentran montados sobre racks estándares de diecinueve pulgadas numerados, y en un BladeCenter H de 14 cuchillas. Los cuartos son administrados: por el Área de Sistemas, que se encarga de monitorear el funcionamiento de los equipos Tecnológicos; y, por otro lado, la parte el Área Administrativa que se encarga del buen funcionamiento de UPS's[66], Aire acondicionado y flujo de energía eléctrica.

2.3.3. Equipos de Ruteo

La infraestructura de red cuenta con los siguientes equipos de ruteo:

Tabla 5: Equipos de ruteo existentes

Equipo/Descripción	Cantidad
ROUTERS	5 routers Cisco.

[65] **ANSI/TIA/EIA-569-A.** Disponible en web: http://www.galeon.com/30008ceti/tarea3.html

[66] «Definición de UPS - ¿qué es UPS?», s. f., http://www.alegsa.com.ar/Dic/ups.php.

Equipo/Descripción	Cantidad
SWITCH	70 switch.
SERVIDORES	50 servidores.

2.4. Direccionamiento IP

El direccionamiento IP está seccionado de acuerdo al número de agencias que posee y se usa una red privada clase B y el direccionamiento es 172.*.*.*/24, para diferenciar sus departamentos, estaciones de trabajo, servidores y equipos activos. Se divide en subredes para cada una de las agencias tanto a nivel local y nacional. La máscara de subred está determinada en base al número de equipos que se tiene a una de las agencias.

Para los enlaces entre sucursales se emplea una red privada clase A 10.*.*.*/24 dividida en subredes con máscara /30 para asignar únicamente una dirección lógica a cada interfaz del Router extremo.

Todos los equipos del personal tanto de agencias locales como nacionales poseen una dirección estática dentro de cada subred, dependiendo del direccionamiento que sea dado por el Departamento de Sistemas.

2.5. Topología de Red

La topología de red es tipo estrella siendo su nodo principal la Matriz. Se tiene un Switch y un proxy-firewall Check-Point. Ver la
Ilustración 24.

2.5.1. Cableado Estructurado

Todo el edificio Matriz que tiene 6 Pisos posee un cableado UTP de cobre para la conexión con cada uno de los departamentos existente en cada uno de los pisos. Además posee un cableado de fibra óptica con conexión a la Agencia Uno para lo que es el Backup de Core Financiero. El cableado es de tipo par trenzado de cobre categoría 6 y 5e, se ha implementado UTP CAT6 sobre todo en el backbone, y en la conexión de servidores.

Todos los puntos de red de salida tanto en Matriz como en cada una de las agencias es doble tipo RJ-45 distribuido uno para lo que es datos y el otro para voz, con su etiqueta respectiva y la información correspondiente a cada punto.

Todas las instalaciones en donde se encuentra los servidores poseen cielo raso y piso flotante para que permita el paso del cableado.

2.5.2. Cableado Vertical

Las conexiones de cada uno de los pisos dentro del Edificio Matriz se encuentran conectados mediante cable UTP CAT6[67] desde el cuarto de equipos hasta los racks de distribución instalados en cada planta. Y todo los que son cables pasan por los ductos del edificio destinados para ese fin.

2.6. Esquema de Red

Como se puede apreciar el esquema de red en la
Ilustración 24: Esquema de Red.
Cada una de las agencias posee un servidor y uno o varios cajeros automáticos.

El servidor principal de la agencia trabaja como:

- Servidor de replicación de Directorio Activo.
- Servidor de Actualizaciones del Symantec.
- Servidor local de CORE FINANCIERO.

[67] «Cable de categoría 6», *Wikipedia, la enciclopedia libre*, 26 de septiembre de 2012, http://es.wikipedia.org/w/index.php?title=Cable_de_categor%C3%ADa_6&oldid=60005873.

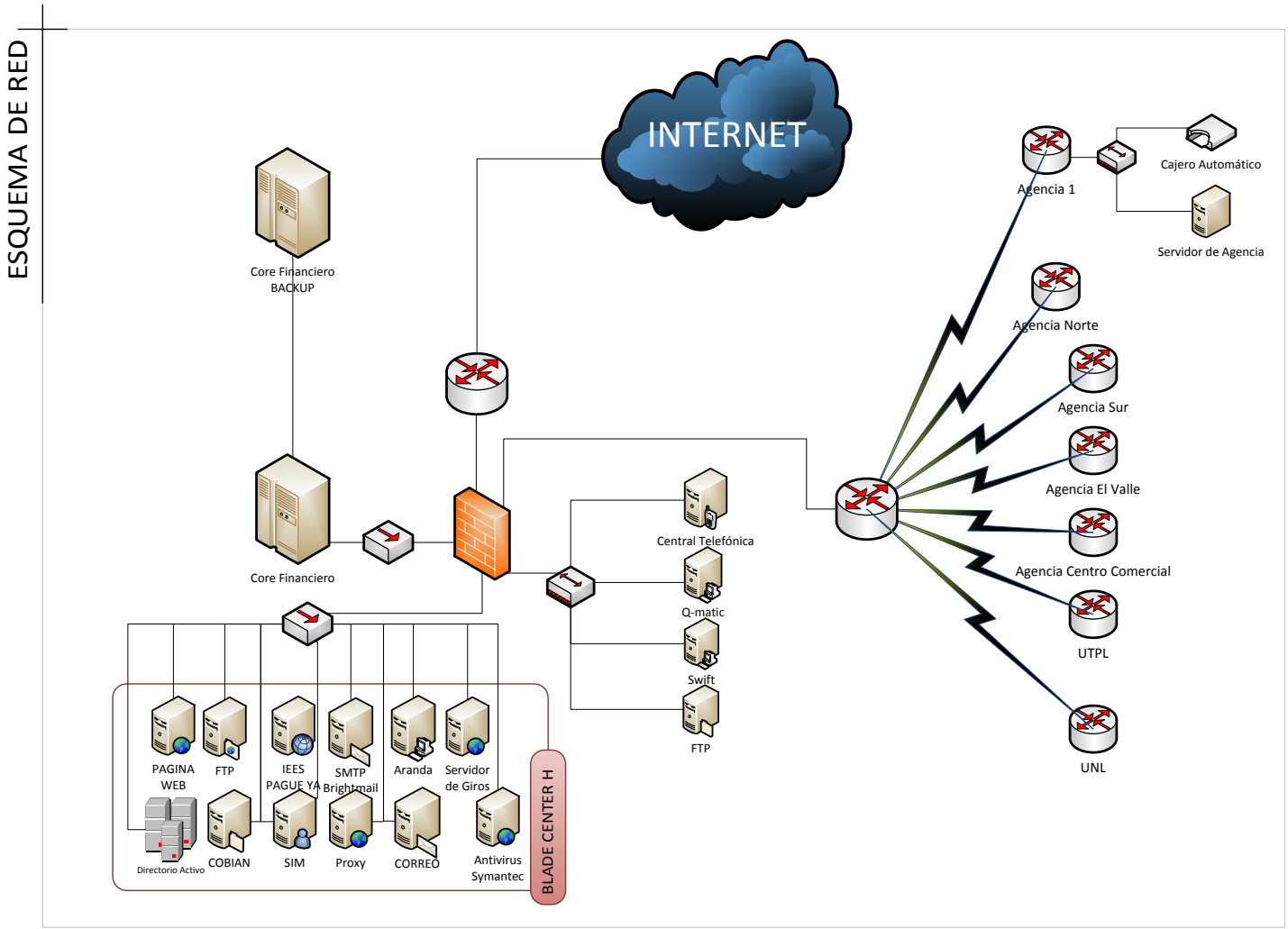


Ilustración 24: Esquema de Red

2.7. Enlaces

2.7.1. Enlaces Internos

Para la comunicación dentro de las agencias locales, ventanillas de extensión y cajeros automáticos se dispone de enlaces con CNT[68] y únicamente para lo que es la conexión con la Agencia Uno posee un enlace de Fibra Óptica de 1MB.

Tabla 6: *Enlaces Locales*

Oficinas Locales	
Agencia Locales y Cajeros Automáticos (Locales)	**Ancho De Banda (Kbps)**
18 de Noviembre (enlace datos)	1024
San Sebastián (enlace datos)	1024
Dispensario (línea dedicada)	1024
Gran Colombia (línea dedicada)	1024
Agencia Sur (línea dedicada)	1024
Agencia Norte (línea dedicada)	1024
Hipervalle (línea dedicada)	1024
UTPL (línea dedicada)	1024
EERSSA (línea dedicada)	1024
Centro Comercial (línea dedicada)	1024
Municipio (línea dedicada)	1024
La Tebaida (Cajero Automático)	1024
Centro Comercial	1024
EERSSA	1024
Agencia Sur	1024
Municipio	1024
UNL	1024
Agencia Hipervalle	1024
Agencia Norte	1024
UTPL	1024
Ciudadela Zamora (Cajero Automático)	1024
Solca (Cajero Automático)	1024
Terminal Terrestre (Cajero Automático)	1024

[68] Corporación Nacional de Telecomunicaciones – Empresa Pública

2.7.2. Enlaces Externos

Seguidamente detallamos los enlaces con las agencias y el ancho de banda.

Tabla 7: *Enlaces Remotos - Agencias*

Oficinas Remotas	
Agencia Locales y Cajeros Automáticos (Locales)	**Ancho De Banda (Kbps)**
Cariamanga	1024
Catamayo	1024
Catacocha	1024
Alamor	1024
Macara	1024
Zamora	1024
Yantzatza	1024
Gualaquiza	1024
San Juan Bosco	1024
6 de Diciembre	1024
El Recreo	1024
El Pangui	1024

2.7.3. Enlaces a Internet

El enlace a Internet es de 4 Mbps con una salida al exterior por medio de un enlace directo por fibra óptica contratado a la empresa BRAVCO.

2.8. Diagrama de una Agencia

A continuación se detalla el diagrama general de una Agencia y los elementos de red que ésta tiene:

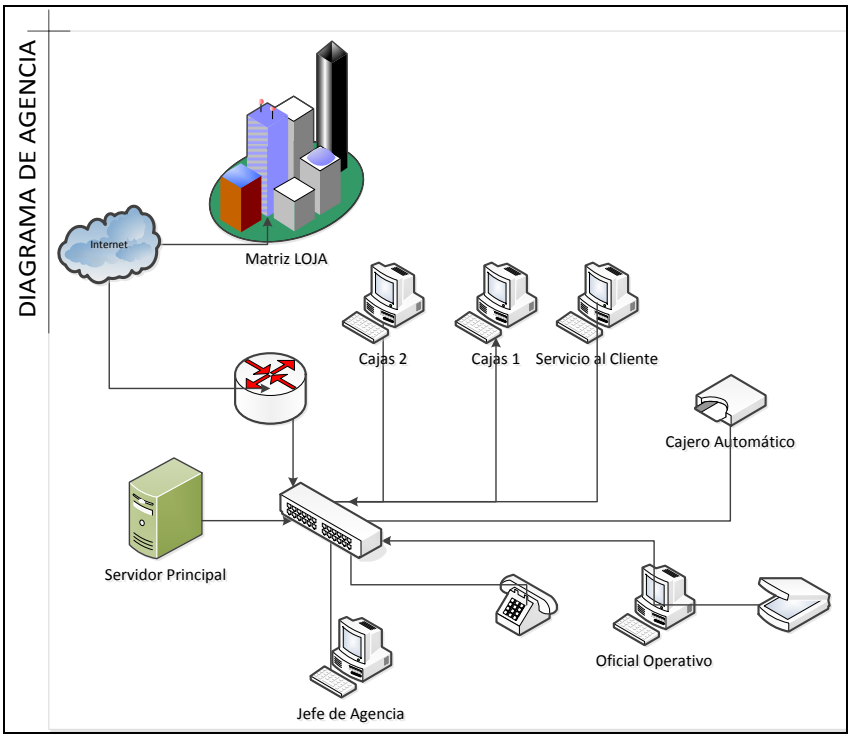


Ilustración 25: Diagrama Básico de una Agencia

2.9. Situación actual del Banco de Loja.

El Centro de Cómputo actualmente dispone de un proceso para el manejo de incidentes pero no posee un proceso formal para lo que es manejo de INCIDENTES DE INFRAESTRUCTURA. Por lo cual en el capítulo siguiente se procederá a proponer un proceso formal para el manejo de este tipo de casos.

2.9.1. Proceso de ingreso de incidentes:

Para el ingreso y administración de incidente el Banco posee un software especializado llamado ***ARANDA Software Service Desk***[69]y el procedimiento que se lleva para el registro y solución de incidentes es el siguiente:

[69]«Aranda Software Aranda SERVICE DESK - Mesa de Servicios - Mesa de Ayuda».

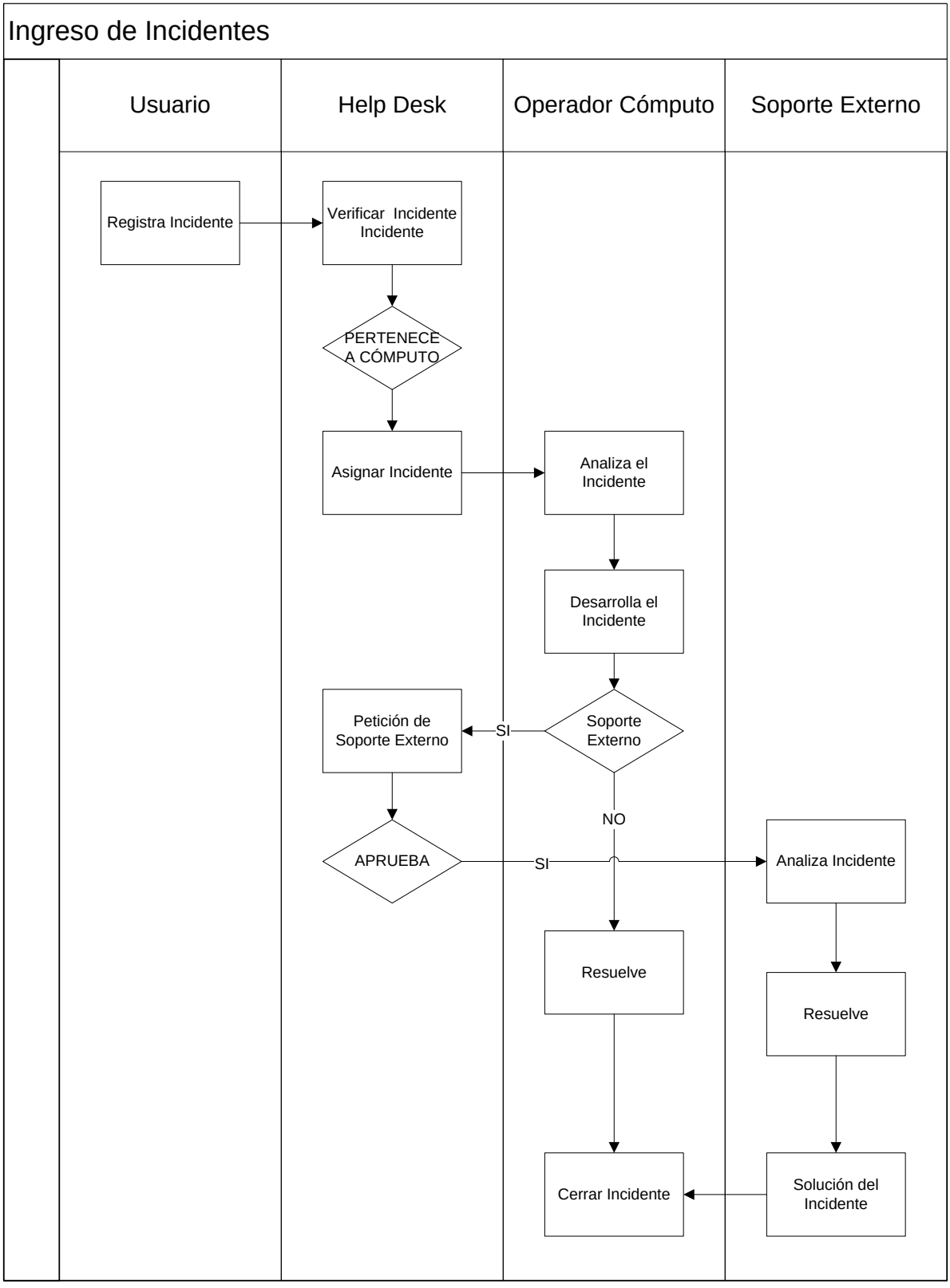


Ilustración 26: Diagrama de Ingreso de Requerimientos

A continuación (Ver Ilustración 27: Gestión de Requerimientos (Diseño Propio) se detalla el caso de uso para ingreso de requerimientos:

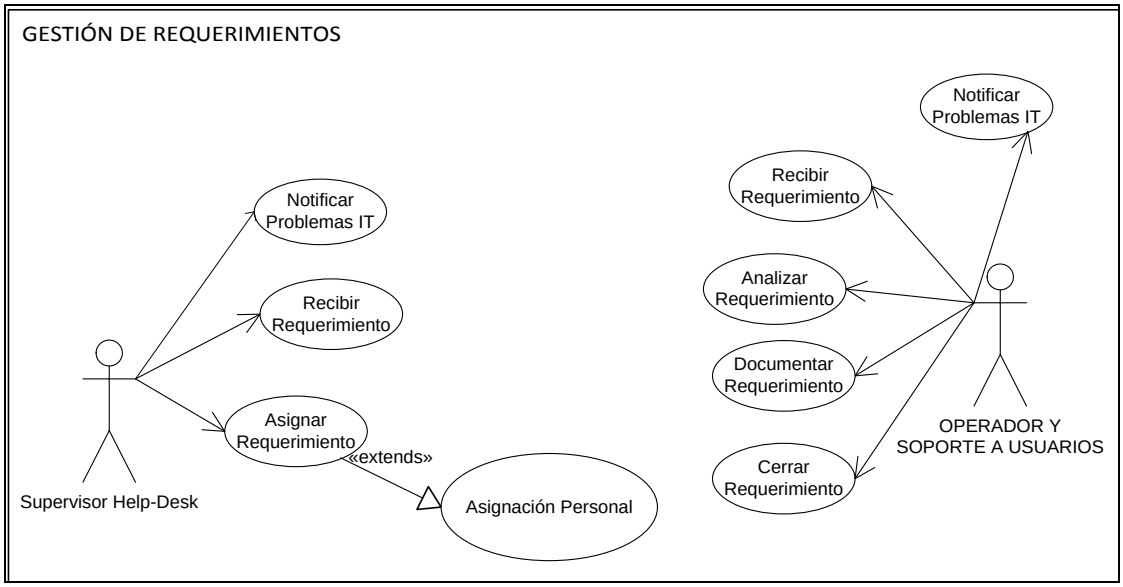


Ilustración 27: Gestión de Requerimientos (Diseño Propio)

1. NOTIFICAR EL PROBLEMA IT

   En este paso en donde se notifica la falla de un servicio/aplicativo/conexión ya sea por parte de un miembro del Centro de Cómputo (Jefe de Cómputo, Supervisor Service Desk, Operadores, etc.), usuario final o proveedor de servicios a SERVICE DESK.
2. RECIBIR EL REQUERIMIENTO

   El Supervisor Service Desk se encarga de ingresar el requerimiento al sistema ARANDA y detallar de forma clara y precisa el error.
3. ASIGNA REQUERIMIENTO

   El Supervisor Service Desk de acuerdo a tipo de problema se asignar el requerimiento a:

   OPERADOR

   - Problemas de Aplicaciones.
   - Instalación de Hardware o Software.

   TÉCNICO INFRAESTRUCTURA

   - Fallas en servidores
   - Fallas de Servicios

   TÉCNICO TELECOMUNICACIONES

   - Fallos en enlaces
   - Consumo de red

- Central telefónica

Y como algo que se debe de tomar en cuenta es el proceso que debe tener en caso de necesitar ayuda de terceros o del proveedor del servicio.

PROVEEDORES/TERCEROS

- Fallos en enlaces
- Consumo de red
- Central telefónica
- Problemas de aplicaciones
- Hardware o Software de terceros

4. SOLUCIÓN DE REQUERIMIENTO

   Posteriormente se realiza el proceso normal para la solución de requerimiento.

2.10. Herramientas Instaladas

Las herramientas instaladas se describen a continuación:

2.10.1. PRTG.

Es un programa para monitoreo de ancho de banda de una red basada en Windows, monitorizando parámetros de uso de red. Los datos de monitorización son guardados en una base de datos para poder generar reportes históricos.

Desde la interfaz de usuario permite configurar el equipo y los sensores que desea monitorizar. Además, puede generar reportes de uso y proveer colegas y clientes con acceso a gráficos y tablas de datos.

Una vez implementado este proyecto, se sustituirá esta herramienta.

2.10.2. ARANDA.

Poseen un Sistema de Gestión de Requerimientos HELPDESK propietario que se llama ARANDA[70]. En este sistema se registran todos los requerimientos, y es aquí,

[70]Aranda Software, «Aranda SERVICE DESK - Datasheet»; «Aranda Software Aranda SERVICE DESK - Mesa de Servicios - Mesa de Ayuda».

NOTA: *Es una poderosa herramienta de gestión de servicios que permite manejar eficientemente los*

donde se da seguimiento a todo CASO/REQUERIMIENTO desde que se inician con el ingreso por parte de usuario, hasta el cierre donde el OPERADOR/TÉCNICO o en su defecto un SOPORTE DE TERCEROS brinda la descripción de la solución.

2.11. Administración de Seguridad

Hay un Oficial de Seguridad que es el encargado de llevar un registro de todos los cambios que se efectúen en los siguientes aspectos:

- Autorizaciones para dar servicio de internet a empleados y terceros.
- Creación de Cuentas de Usuarios para Active Directory
- Creación de Cuentas de Correo
- Acceso para cada uno de los Sistemas que posee el banco.
- Auditoria de Usuarios y Permisos
- Control de Manejo de Dispositivos
- Horarios de trabajo por usuario para acceso a aplicaciones y/o sistemas que posee el Banco.

2.12. Problemática

Existen falencias en lo que es el monitoreo de servicios; esto se lo hace de manera manual y se envía un mail a las personas involucradas (Gerente de Sistemas, Jefe de Centro de Cómputo y Supervisor HELPDESK) y responsables de los servicios (Técnico de Infraestructura, Técnicos de Telecomunicaciones o Técnico de Hardware). Este reporte de monitoreo contiene la información descrita en el ANEXO Reportes De Monitoreo.

Dentro del análisis de servicios externos, el Banco tiene tercerisado mediante contrato con **Internetvista**[71] que es una compañía que se encarga de supervisar los servidores externos de una organización. A continuación se presenta un informe enviado diariamente por esta compañía mediante correo electrónico. Ver Anexo 5, en donde se detallan los reportes.

Luego de haber expuesto la Situación Actual del Banco de Loja, puedo decir que existe la necesidad de implementar un Centro de Administración de Red para manejar de mejor manera los requerimientos de infraestructura y de red que se susciten dentro

---

procedimientos de soporte de la organización de tal manera que aumente considerablemente su nivel de servicios.

[71] «internetVista® monitoring - Uptime is money», accedido 29 de febrero de 2012, http://www.internetvista.com/.

del Centro de Cómputo que posee el Banco. Además, de automatizar el proceso de monitoreo para mejorar la reacción a fallas, toma de decisiones y que todos los procesos cuenten con un estándar; además, de la elaboración de un manual de procedimientos pensado para la puesta en marcha dentro del Departamento de Sistemas.

2.13. Criterios de Evaluación para escogerl Herramienta de Monitoreo

Para realizar la evaluación de una herramienta se propuso los siguientes criterios basándose en el conocimiento de la red, las necesidades y la experiencia adquirida como Operador y Soporte a usuarios del Banco de Loja. Los aspectos tomados en cuenta son:

- Evaluar la estructura de la red.
- Determinar la cantidad de nodos a monitorear.
- Identificar los servicios principales para monitoreo.
- Analizar el soporte y documentación de la herramienta.
- Los costos:
    - Costo de inversión de licencia bajo o nulo.
    - Infraestructura IT.
        - Equipos (Servidor/es, switches, etc.)
        - Direcciones IP.
        - Cableado.
        - Ubicación y espacio físico.
    - Infraestructura Hardware.
        - Consumo de Recursos de Red.
        - Consumo de Recursos de Memoria, Procesador y Disco Duro.
    - Recurso Humano.
- Estudiar las características de la herramienta.
    - Capacidad de Integración con otras herramientas.
    - Generación de Reportes.
    - Medios de Notificación y alarmas.
    - Facilidad de Uso.
    - Registro de Eventos.
    - Documentación
    - Adaptabilidad a las necesidades e infraestructura del Banco.
    - Autodescubrimiento de la topología.

2.14. Funcionalidades para escoger la herramienta de monitoreo

2.14.1. Funcionalidades Generales.

Las funcionalidades generales fueron definidas tomando en cuenta el punto 2.13 de la presente tesis.

FUNCIONALIDADES GENERALES
Facilidad de Instalación
Facilidad de Configuración
Administración de Interfaz Web
Documentación
Integración con Plugins
Facilidad de Uso
Integración con otras herramientas
Alertas y Notificaciones
Creación Personalizada de Scripts
Soporte en Línea
Usado en la industria financiera
Actualizaciones
Monitoreo de Servicios

2.14.2. Funcionalidades Específicas.

De acuerdo a las funcionalidades generales propuestas en el apartado anterior, se define ciertas funcionalidades específicas que se desglosan de la siguiente manera:

FUNCIONALIDADES GENERALES

- Monitorear distintos sistemas operativos
- El servidor se instala en un entorno Linux
- Monitorear al menos 100 componentes
- Tener agentes de monitoreo que trabajan sobre los sistemas clientes
- Generación de reportes operativos y estadísticos
- Distribución de Usuarios por roles y responsabilidades
- Tener una pantalla central de administración y configuración

FUNCIONALIDAD DE HARDWARE

- Monitorear hardware (uptime servers, routers, etc,)
- Monitorear entornos Virtuales VMWare
- Enviar Alarma si no responde el equipo computacional (Server)
- Enviar Alarma si no responde el equipo de red (router, switch)

FUNCIONALIDADES A NIVEL DE SISTEMA OPERATIVO

- Enviar alarma si se llega a determinados umbrales de disco duro
- Enviar alarma si se llega a determinados umbrales de memoria
- Enviar alarma si se llega a determinados umbrales de CPU
- Controlar procesos (cantidad)
- Controlar archivos (tamaño)

FUNCIONALIDADES DE SERVICIOS Y APLICACIONES

- Monitorear software de base y generar alarmas ante caídas
- Monitorear software de aplicaciones y generar alarmas ante caídas
- Monitoreo de Enlaces y generar alarmas ante caídas

FUNCIONALIDADES DE NOTIFICACIONES

- Permitir el envío de notificaciones vía email
- Permitir el envío de notificaciones vía Correo Electrónico

3. PLAN DE APLICABILIDAD PARA EL CENTRO DE OPERACIONES DE RED DEL BANCO DE LOJA

3.1. Levantamiento de Requerimientos y Especificaciones

Una vez conocida la situación actual del Banco de Loja descrita en el Capítulo 2, en el presente capítulo se explicará los requerimientos para la puesta en marcha del NOC.

3.1.1. Descripción de Requerimientos.

Para el levantamiento de los requerimientos en el diseño del NOC se utilizó diálogos verbales, análisis de necesidades y la experiencia de dos años trabajando en el Departamento de Cómputo en áreas de Administración de Infraestructura y Soporte Técnico. Los aspectos tomados en cuenta para el levantamiento de requerimientos están orientados a las cinco áreas funcionales FCAPS[72] de la recomendación ITU-T M.3400. A continuación describo los requerimientos en cada una de dichas áreas:

3.1.1.1. Respuesta a Fallos.

- Dar solución en el menor tiempo posible a problemas y requerimientos que se presenten dentro de la red.
- Llevar una estadística y un control de aquellos elementos de red, servicios y activos informáticos que tienen una mayor incidencia de fallos.
- Los requerimientos y problemas que surgen en el equipo de hardware o en el del funcionamiento de red debe de tener: prioridad, recurso humano para la resolución y un tiempo que va desde el inicio hasta la resolución del problema.
- Un constante y continuo monitoreo de todos los equipos de red mediante alertas de sonido, alertas visuales (colores), correos electrónicos y notificaciones para estar preparados ante posibles problemas.

3.1.1.2. Manejo de Infraestructura de Red.

- Que posea un agente, componentes o programas que permita obtener información suficiente del estado de los equipos y/o servicios.
- Todos los equipos monitoreados deben constantemente alertar al servidor NMS[73] su mal funcionamiento o anormalidad en su operatividad.
- Llevar un control de cada equipo que ingresa o sale de la red.
- Configuración correcta de los equipos que van a ingresar; y también dar de baja aquellos que van a ser separados de la red.
- Sólo los administradores deben tener acceso a los parámetros configurables de los

[72]«IPPolicyHandbook-S.pdf (objeto application/pdf)», accedido 5 de marzo de 2012, http://www.itu.int/ITU-T/special-projects/ip-policy/final/IPPolicyHandbook-S.pdf.
[73]«Open Source NMS Tools - Network Management Wiki», accedido 9 de marzo de 2012, http://nms.gdd.net/index.php/Open_Source_NMS_Tools.

equipos.

3.1.1.3. Monitoreo de la Red.

- Monitorear el rendimiento, utilización y funcionamiento de los distintos elementos de red, teniendo una visión global de servidores, switches y routers que se encuentran activos dentro de la red, principalmente los que manejan un mayor volumen de información y aquellos servicios que son sensibles para la atención al cliente.
- Monitorear la cantidad de tráfico y ancho de banda para definir controles y mecanismos de medición y detectar un flujo excesivo o un mal funcionamiento en rendimiento de la red.
- Instalar herramientas que permitan llevar un control preventivo de los servidores y equipos de conectividad, garantizando la comunicación entre los distintos departamentos del banco.

3.1.1.4. Análisis de Datos.

- El NMS debe ser capaz de procesar la gran cantidad de información enviada por el agente y ser representada de tal manera que el Administrador de red pueda interpretarla con facilidad para la toma de decisiones.
- Los datos a contabilizar por parte de los agentes deben de regirse mediante políticas o SLA's para monitorear: capacidad de disco, utilización de memoria, uso del procesador, estados de las interfaces de red, procesos en ejecución, cantidad de paquetes enviados, entre otros.
- Establecer lineamientos del correcto funcionamiento de los dispositivos y definir umbrales que nos sirvan de base para poder tomar medidas preventivas ante posibles errores y fallas dentro de la red.
- Determinar las repercusiones que implica a la red el uso de recursos por parte de un equipo.
- Crear reportes personalizados de acuerdo a las necesidades que vayan surgiendo.

3.1.1.5. Seguridad.

- Establecer una base para la elaboración de un Plan de Monitoreo que defina los pasos a seguir por el Área Sistema y específicamente por el departamento del Centro de Cómputo.
- Implantar políticas de seguridad para el tratamiento y uso de la información dentro de las operaciones del Banco; además, asegurando el correcto funcionamiento de

la infraestructura física y la información empresarial.

- Identificar los principales riesgos y amenazas que afecten a los servidores más críticos.
- Controlar el acceso a las instalaciones del área de servidores, a los cuartos de equipos y a los racks de distribución ubicados en el Edificio Matriz y/o en cada agencia.
- Definir usuarios con privilegios específicos para cada rol de administración del NOC dentro del departamento.

3.2. Definición de Roles de Usuarios

3.2.1. Gerente de Sistemas.

- Cumplir y hacer cumplir las políticas y normativas tecnológicas para la administración del Área de Sistemas dentro de la Estructura de Responsabilidades de Recursos Humanos.
- Administrar todo el recurso humano del Área de Sistemas en función de las políticas del Banco.
- Seleccionar software y hardware, programación y operaciones.
- Autorizar nuevas funcionalidades y herramientas necesarias para el control de la red.

3.2.2. Jefe del Centro de Cómputo.

- Coordinar y administrar todo el recurso humano que maneje al Centro de Operaciones de Red en función de las políticas del Banco.
- Gestionar la administración del NOC haciendo cumplir las responsabilidades del personal.
- Establecer y mantener actualizados políticas, normas y estándares de tecnologías de información y comunicaciones para el Centro de Cómputo.
- Gestionar la capacitación integral y profesional del personal del NOC.
- Cumplir y hacer cumplir las políticas de buen uso de la infraestructura de red.
- Realizar una evaluación del funcionamiento de la red actual, sus características y brindar soluciones de mejoramiento.

3.2.3. Supervisor Service Desk.

- Ingreso, asignación y seguimiento de requerimientos desde su ingreso hasta el cierre de los mismos.
- Administrar el proceso de monitoreo de la red.

- Sugerir nuevas alarmas necesarias para el control de la red.
- Mantener actualizado el inventario de equipos de infraestructura
- Crear, modificar o eliminar SLA's del NMS en función de los dispositivos que ingresan a la intranet y características a ser monitoreadas.

3.2.4. Técnico Infraestructura Tecnológica.

- Coordinar el proceso de monitoreo de la red.
- Asegurar el óptimo funcionamiento del NMS.
- Adecuar el NMS según los protocolos que se requieran para controlar un nivel aceptable por debajo de los umbrales de rendimiento de la red.
- Añadir nuevos dispositivos y/o configurar los SLA's descritos por el Supervisor Service Desk.
- Establecer, evaluar y ejecutar las pruebas para detectar problemas de funcionamiento en infraestructura.

3.2.5. Técnico de Telecomunicaciones.

- Monitorear constantemente la capacidad operativa de los enlaces de la red y su correcto funcionamiento.
- Identificar y brindar soluciones a necesidades de comunicaciones asegurando la disponibilidad y confiabilidad de servicios con proveedores y conectividad con agencias.
- Implantar los planes de seguridad y contingencia elaborando planes de mantenimiento preventivo y correctivo.
- Administrar y coordinar el proceso de monitoreo de la red del Banco, ya sea interna o externa.
- Añadir nuevos dispositivos a la herramienta de administración en función de su ingreso a la intranet y habilitar las interfaces a ser monitoreadas.
- Configurar equipos de networking que se añaden a la red, corroborando su buen funcionamiento, seguridad y monitoreo remoto desde la NMS.
- Mantener el cableado estructurado en excelente estado.
- Realizar un mantenimiento continuo de los equipos de Red.

3.2.6. Operador y Soporte a Usuarios.

- Coordinar el proceso de monitoreo de la red.
- Monitorear constantemente los servicios y servidores de la red asegurando su correcto funcionamiento.

- Preparar informes detallados y reporte de Monitoreo.
- Reportar las fallas en la Infraestructura dividiéndolas de acuerdo al tipo de error en:
    - Si es falla en servicio y/o servidor, reportar a Supervisor Service Desk
    - Si es falla de interconectividad y/o enlaces, reportar a Técnico de Telecomunicaciones.

3.2.7. Supervisor de Seguridad.

- Diseñar políticas de seguridad para definición de roles de usuarios y administradores.
- Definir los controles necesarios para protección de información (gestión de contraseñas, métodos de autenticación apropiados, entre otros).

3.3. Especificaciones de información y Equipos/Servicios a ser Monitoreados

Para determinar los datos a ser monitoreados dentro de lo que son equipos y servicios se toma en cuenta las características propias de cada elemento gestionado.

Tabla 8: *Dispositivos a ser monitoreados (Diseño Propio)*

DISPOSITIVO/SERVICIO	PARÁMETROS	ESPECIFICACIÓN
SERVIDOR/EQUIPO	Memoria	Cantidad de Memoria utilizada
	Estado	Si esta encendido y/o apagado
	Uso CPU	Estadística del uso del CPU
	Disco Duro	Cantidad de disco duro ocupado y libre
	Procesos	Cantidad de Procesos ejecutándose
	Interfaces de Red	Número de Interfaces de Red que posee el Servidor
ENLACE	Capacidad	Cantidad ocupada, Picos máximos y mínimos
	Estado	Activo (Flujo de datos) o caído o inactivo (sin flujo de datos)
SWITCH	Procesador	Uso del procesador
	Interfaces	Interfaces ocupadas y desocupadas
ROUTER	Uso CPU	Estadística del uso del CPU
	Interfaces	Cantidad de interfaces ocupas y desocupadas.
	Disco Duro	Disco utilizado, para poder realizar futuras actualizaciones
	Memoria	Cantidad de memoria RAM utilizada

3.3.1. Definición de Umbrales.

Se realizó el análisis individual de las características comunes que pueden ser aplicadas a cada uno de los servidores/dispositivos y servicios, además, tomar en cuenta las funciones propias de cada dispositivo, los recursos físicos, su capacidad de memoria y procesamiento. Entonces, tomando en cuento lo expuesto anteriormente se ha propuesto asignar márgenes y/o porcentaje referencial para determinar los umbrales de medición.

El criterio que se va a utilizar es el dado por Microsoft[74]: "El uso del procesador de un servidor debe mantener una carga del 60 por ciento aproximadamente durante las horas de máxima actividad. Este porcentaje admite períodos de carga muy elevada. Si el uso del procesador está por encima del 75% de manera continua, el rendimiento del procesador se considera un cuello de botella"

Tomando como referencia la premisa anterior, se ha visto conveniente tener el porcentaje de 75% como línea base para conservar en condiciones óptimas todos los componentes de la red junto con los dispositivos de conexión. Entonces, una vez que supere este límite se recomienda tomar medidas correctivas en donde se observe que los equipos/servicios disminuyen su rendimiento para evitar la degradación de la red.

Para la memoria RAM se tendrá en cuenta también el 75% como escala para monitoreo.

En lo referente a la capacidad de discos duros, se estableció un umbral del 80% en el espacio usado.

Otro método a utilizar, es el método del percentil que establece un mayor máximo de acuerdo a una muestra. Se lo puede definir de la siguiente manera:

El percentil q (p_q). es un valor del recorrido de las observaciones tal que:
1º. A lo menos q% de las observaciones son menores o iguales que p_q.
2º. A lo menos (100-q)% de las observaciones son mayores o iguales que p_q.
En el siguiente gráfico se expresa de mejor manera.

[74]«Descripción del rendimiento de Exchange».

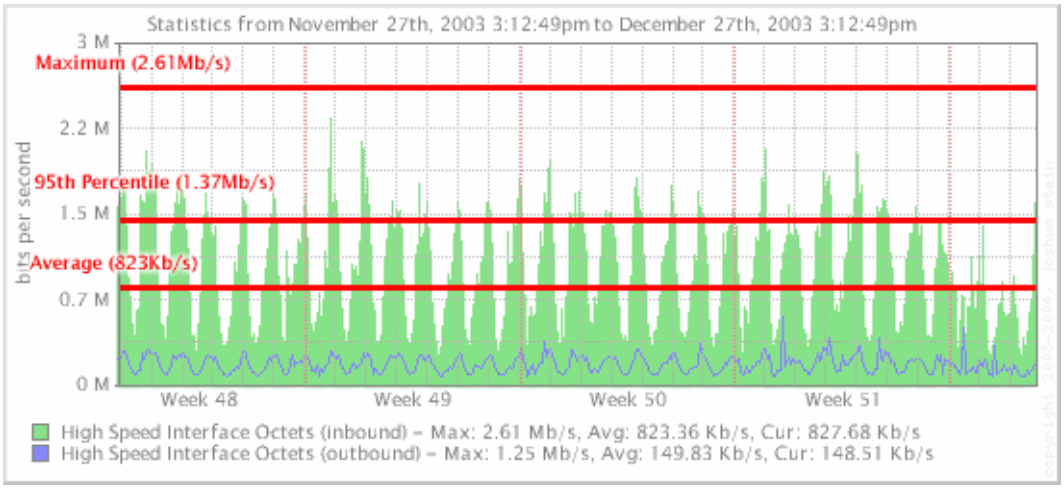


Ilustración 28: Método del Percentil (Vicente, Análisis de Rendimiento - Servicios de Red)[75]

3.3.2. Métricas para el Servidor de Correos

A más de las métricas descritas anteriormente se tomará en cuenta las siguientes:

- ✓ Número de mensajes recibidos/enviados
- ✓ Número de bytes recibidos/enviados
- ✓ Número de mensajes denegados
- ✓ Número de mensajes descartados
- ✓ Número de mensajes en cola

A continuación tomamos en cuenta la estadística de mensajes de SENDMAIL de una semana:

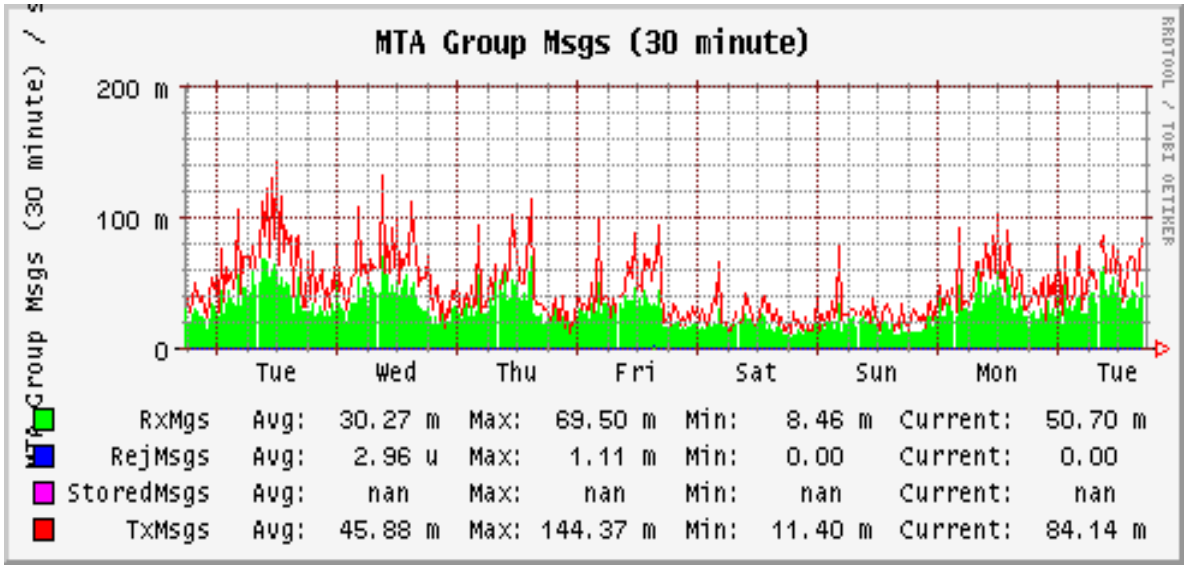


Ilustración 29: Estadística SENDMAIL

[75]Vicente, Carlos, «Análisis de Rendimiento - Servicios de Red», s. f.

Resumiendo los criterios expuestos anteriormente, se encuentran resumidos en la Tabla 9: Umbrales *Determinados*; vale recalcar las medidas son referenciales para que los administradores puedan tomar decisiones correctivas una vez que los equipos y/o servicios sobrepasen estos límites.

Tabla 9: *Umbrales Determinados (Diseño Personal)*

Elementos de Red	Parámetros Analizar	Umbrales
Router y Switchs	CPU	75%
	MEMORIA	75%
Enlaces	UTILIZACIÓN	75%
Servidor	CPU	75%
	RAM	75%
	DISCO	80%
FUNCIONAMIENTO RECOMENDABLE		< 60%
UMBRAL GENERAL		61 – 75 %

3.4. Descripción de Áreas Funcionales del NOC

3.4.1. Diseño de Análisis de Datos.

Esta sección permite medir la cantidad de información dentro de la red empresarial de acuerdo a los parámetros planteados en el punto 3.3.

- Tráfico entrante y saliente en todos los enlaces, especialmente entre dispositivos de conectividad principal y todos los servicios.
- Capacidad de CPU utilizada en los servidores y equipos de la red, esto permitirá conocer que equipos están funcionando lentamente y aquellos que necesitan cambiarse por su bajo rendimiento.
- Cantidad ocupada de los discos duros de servidores, permitirá identificar el momento de inserción de nuevos módulos de almacenamiento para la información.
- Porcentaje de uso del procesador del equipo, permitirá especificar si el equipo está en óptimas condiciones para soportar la carga informática actual. Al mismo tiempo será una herramienta de planificación en la adquisición de dispositivos que remplacen aquellos que no soporten la carga actual.
- Tener un registro de alarmas (logs) que van generando los dispositivos de red, también un registro de eventos para saber el tiempo y la solución a los distintos errores suscitados en la red.

- El control de seguridad en cuanto al acceso, se debe de contabilizar las entradas de cada miembro del NOC a los servidores, cuarto de equipos y el número de veces que chequea los servidores y servicios que tiene a su cargo.
- Reportes personalizados del funcionamiento de equipos durante periodos de tiempos.

3.4.2. Diseño de Análisis de Configuración

En este punto se realiza la configuración del NMS y de cada uno de los agentes en los equipos y servidores a monitorear de acuerdo al sistema operativo instalado. También se configura en los dispositivos de conectividad como son routers y Switchs.

Las configuraciones de cada uno de los elementos se describen en el ANEXO 6[76].

- ✓ Hacerle seguimiento a los dispositivos de red y sus configuraciones (hacer respaldo de las configuraciones)
- ✓ Mantener un inventario de todos los dispositivos que posee la red
- ✓ Registrar las versiones de los sistemas de operación y las aplicaciones

3.4.3. Diseño de Análisis de Rendimiento

Tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo. Esto permitirá tomar las decisiones pertinentes de acuerdo al comportamiento encontrado.

3.4.4. Diseño de Análisis de Contabilidad

Es el proceso de recolección de información acerca de los recursos utilizados por los elementos de la red, desde equipos de interconexión hasta usuarios finales. Esto se realiza con el objetivo de realizarlos cobros correspondientes a los clientes del servicio mediante tarifas establecidas. Este proceso, también llamado tarificación, es muy común en los proveedores de servicio de Internet o ISP.

3.4.5. Diseño de Gestión de Fallos

A continuación se realiza un plan para el manejo de errores y el procedimiento a seguir para solucionarlo o mitigarlo.

[76] Anexo 6: Configuración cliente SNMP

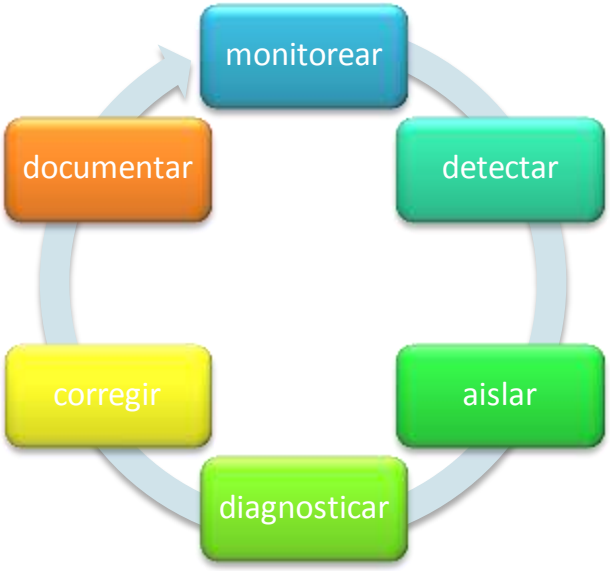


Ilustración 30: Procesos de Detección de Fallas (Diseño Propio)

3.4.5.1. Monitoreo de Alarmas

Cuando una alarma ha sido generada mediante el NMS, esta debe ser detectada casi en el instante de haber sido emitida para poder atender el problema de una forma inmediata, incluso antes de que el usuario del servicio pueda percibirla. Además, cada requerimiento detectado debe ser registrado en el SISTEMA ARANDA para el manejo y seguimiento.

Las alarmas pueden ser caracterizadas desde al menos dos perspectivas, su tipo y su severidad.

Tipo de las Alarmas

- **Alarmas en las comunicaciones**. Son aquellas que tiene que ver con el transporte de la información, Ej. Caídas de enlaces, mal funcionamiento del punto de red.
- **Alarmas de procesos**. Son las asociadas con las fallas en el software o los procesos asociados a un programa. Ej. No respuesta del IIS, SQL Server, Antivirus, etc.
- **Alarmas de equipos**. Como su nombre lo indica, son las asociadas con los equipos y/o sus partes. Uso de CPU, falta de disco duro.
- **Alarmas en el servicio**. Relacionadas con la degradación del servicio en cuanto a límites predeterminados. Ej. utilización del ancho de banda para el internet, pagos en línea SRI, etc.

3.4.5.2. Detección

Este segundo elemento de la administración de fallas es importante para identificar las causas que han originado una falla. La alarma indica el lugar del problema, pero las pruebas de diagnóstico adicionales son las que ayudan a determinar el origen de la misma. Una vez identificado el origen, se tienen que tomar las acciones suficientes para reparar el daño. Para lo cual se realizará las siguientes pruebas:

Según (Irastorza, Grupo de Ingeniería Telemática, 2008) [77] propone el siguiente esquema para localizar de problemas en la red:

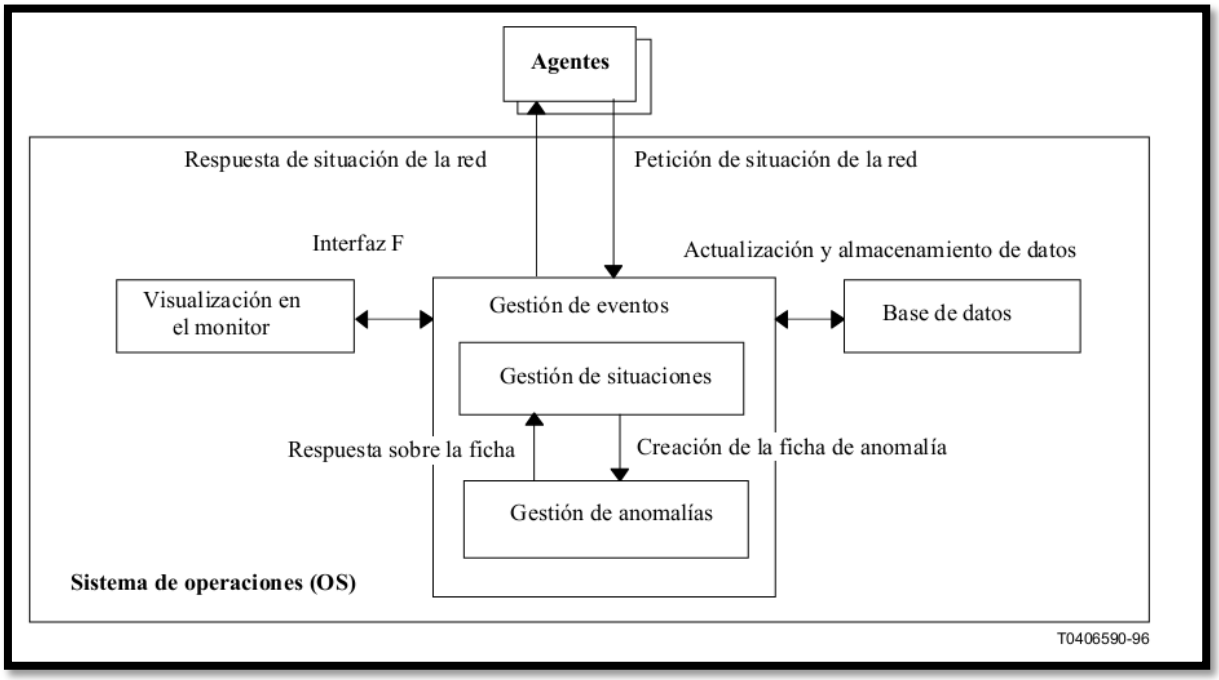


Ilustración 31: Localización de Problemas de Red (Irastorza, Grupo de Ingeniería Telemática, 2008)[78]

Pruebas de conectividad física.

Son pruebas que se realizan para verificar que los medios de transmisión se encuentran en servicio, nos referimos a tarjeta de red, routers, switches o cable de red.

Pruebas de conectividad lógica.

Son pruebas que se pueden realizar punto a punto, o salto por salto. Las pruebas punto a punto se realizan entre entidades finales, y las salto por salto se realizan entre la entidad origen y cada elemento intermedio en la

[77] IRASTORZA José Ángel, «Gestión de Redes».
[78] Ibid.

comunicación. Los comandos usualmente utilizados para la realización de estas pruebas son “ping” y “traceroute”.

Pruebas de medición.

Esta prueba va de la mano con la anterior, donde, además de revisar la conectividad, se miden: los tiempos de respuesta en ambos sentidos de la comunicación, la pérdida de paquetes y las rutas que sigue la información desde el origen hasta el destino.

3.4.5.3. Aislamiento

Se debe tratar de que otros servicios o equipos no se vean afectados a causa del mismo problema, tratando siempre de minimizar el impacto y hallar una solucionar al problema rápidamente asegurando que el resto de los elementos de la red pueden seguir funcionando. Por ejemplo: si se cae el enlace en la agencia Catamayo, los funcionarios de dicha agencia se pueden movilizar hasta la agencia más cercana, en este caso, a la Matriz en Loja para realizar los procedimientos de cierre y cuadre de caja sin ocasionar que en el siguiente día existan variaciones en el efectivo del CORE FINANCIERO.

3.4.5.4. Diagnosticar

En el diagnóstico se debe tener en cuenta que equipos o servicios se vieron afectados por la falla en la red.

3.4.5.5. Corrección de Fallas

Entre los mecanismos más recurrentes y más utilizados por los administradores de red se encuentran los siguientes:

- Remplazo de recursos dañados. Hay equipos de red que permiten cambiar módulos en lugar de cambiarlo totalmente.
- Contingencia. Si se cuenta con un recurso redundante, el servicio se cambia hacia este elemento.
- Recarga del sistema. Muchos sistemas se estabilizan si son reiniciados.
- Instalación de software. Sea una nueva versión de sistema operativo, una actualización, un parche que solucione un problema específico, etc.
- Cambios en la configuración. También es algo muy usual cambiar algún parámetro en la configuración del elemento de la red.

3.4.5.6. Tiempos de Solución a Fallos

- **Tiempo de detección:** Es el tiempo que transcurre entre el origen del problema y su detección. Hay una relación entre el tiempo de detección y el tiempo de resolución total: cuanto antes se detecte la avería, en general, habrá causado menos daño y será más fácil y más económica su reparación. Es posible reducir este tiempo si se revisa constantemente los sistemas del NOC y comprobar los parámetros de funcionamiento para detectar más rápidamente el problema.
- **Tiempo de comunicación:** Es el tiempo que transcurre entre la detección del problema y localización del equipo de mantenimiento. Este periodo se ve muy afectado por los sistemas de información y de comunicación con el personal de mantenimiento y con sus responsables.
- **Diagnóstico del problema:** Es el tiempo necesario para que el operador determine que está ocurriendo en el equipo y como solucionarlo.
- **Reparación de la avería:** Es el tiempo necesario para solucionar el problema surgido, de manera que el equipo quede en disposición para producir. Se ve muy afectado por el alcance del problema y por los conocimientos y habilidad del personal encargado de su resolución. Para optimizar este tiempo es necesario disponer de un sistema de mantenimiento preventivo que evite averías de gran alcance, y disponer de un personal eficaz, motivado y muy bien formado.
- **Puesta en servicio:** Es el tiempo que transcurre entre la solución completa del problema y la puesta en servicio del equipo. Está afectado por la rapidez y agilidad de las comunicaciones.
- **Documentación:** El sistema documental de mantenimiento debe recoger al menos los incidentes más importantes de la planta, con un análisis en el que se detallen los síntomas, la causa, la solución y las medidas preventivas adoptadas.

3.4.5.7. Niveles de Criticidad en Fallas

Los niveles críticos se van a utilizar los que ya se tenían descritos dentro del manejo de requerimientos en el Centro de Cómputo y estos son:

Tabla 10: *Niveles de Criticidad*

NIVEL CRITICIDAD	NIVEL CRITICIDAD	DESCRIPCIÓN
1	Bajo	Problemas que a pesar de su ocurrencia la red se mantiene en funcionamiento.
2	Medio	Mal funcionamiento de equipos de red.
3	Alto	Operaciones relacionadas con el

NIVEL CRITICIDAD	NIVEL CRITICIDAD	DESCRIPCIÓN
		mantenimiento de Equipos, configuraciones de programas o llegada a los límites de los umbrales.
4	Crítico	Problemas relacionados con el tráfico de red, problemas de software, hardware, afectación de servicios.

Tabla 11: *Valoración de Criticidad de acuerdo al tipo de falla*

FALLA	CRITICIDAD				RESPONSABLE
	1	2	3	4	
Caída de enlace con alguna de las agencias.				X	Técnico de Telecomunicaciones
Caída del enlace de internet				X	Técnico de Telecomunicaciones
Caída del Servidor Página Web				X	HELPDESK-Operador y Soporte a Usuarios-Técnico de Infraestructura
Caída de Servidor Active Director				X	HELPDESK-Operador y Soporte a Usuarios
Caída de Servidores de uso general Ej.: Webmail, Antivirus, SMTP, Directorio Telefónico, Aranda, TurboSwif				X	HELPDESK-Operador y Soporte a Usuarios-Técnico de Infraestructura
Problema de saturación de enlace				X	HELPDESK-Operador y Soporte a Usuarios-Técnico de Telecomunicaciones
Problema con Switchs				X	Técnico de Telecomunicaciones
Problema de Router				X	Técnico de Telecomunicaciones
Problema con Puntos de red o del cableado estructurado			X		Técnico de Telecomunicaciones
Problema de Hardware de los			X		Técnico de Hardware

FALLA	CRITICIDAD				RESPONSABLE
	1	2	3	4	
equipos de los colaboradores del banco					
Problema de Software o mal funcionamiento de aplicativos de terceros instalados en los equipos de los colaboradores del banco			X		HELPDESK-Operador y Soporte a Usuarios

3.4.5.8. Tiempos actuales de solución de requerimientos.

Para definir los tiempos de respuesta en cuanto a los fallos se lo hizo mediante diálogos verbales y el estudio de la Matriz de Respuesta a Fallas llevada dentro del Centro de Cómputo.

Tabla 12: *Tiempo de Resolución de Requerimientos*

Nro.	DESCRIPCIÓN DEL FALLO	TIEMPOS DE RESPUESTA				
		5-15 MIN	**16-30 MIN**	**31-60 MIN**	**61-120 MIN**	**MAYOR A 120 MIN**
1.	Caída enlace WAN interno					
2.	Caída enlace WAN externo					
3.	Caída enlace internet					
4.	Caída Servidor de Área Operativa					
5.	Caída servidor Active Directory					
6.	Caída servidor ARANDA					
7.	Problema en el CORE FINANCIERO					
8.	Problemas en la red de transporte					
9.	Fuera de servicio de HW o SW en los puntos de red de las agencias					
10.	Problemas Switchs Acceso					
11.	Problemas Switchs Core					
12.	Problemas con un Router					
13.	Problemas con cableado estructurado					
14.	Problemas HW o SW de usuario.					

Nro.	DESCRIPCIÓN DEL FALLO	TIEMPOS DE RESPUESTA				
		5-15 MIN	**16-30 MIN**	**31-60 MIN**	**61-120 MIN**	**MAYOR A 120 MIN**
15.	No se pueden leer las MIB's de un equipo					
16.	Equipo no responde a SNMP pero si a ping.					
17.	No existe conectividad en un dispositivo					
18.	Dispositivo fuera de servicio por problema eléctrico.					

3.4.5.9. Documentación

La documentación será registrada con todo el procedimiento realizado para solucionar todos los problemas que se registren dentro del ARANDA. Como se muestra en el ANEXO 7: INGRESO DE CASOS AL ARANDA.

4. DISEÑO DE INFRAESTRUCTURA IT

4.1. Aplicación del modelo de Gestión De Red

4.1.1. Creación del SLA para Manejo de Requerimientos por Problemas de Elementos de Red, Servicios y/o Servidores (Infraestructura de Red).

Se implementó un nuevo SLA para manejar los problemas de: elementos de red, servicios y/o servidores. En el SLA permite crear incidentes que que se deriven del sistema monitoreo para posteriormente sean reportados en el sistema ARANDA.

A continuación se explica gráficamente este proceso:

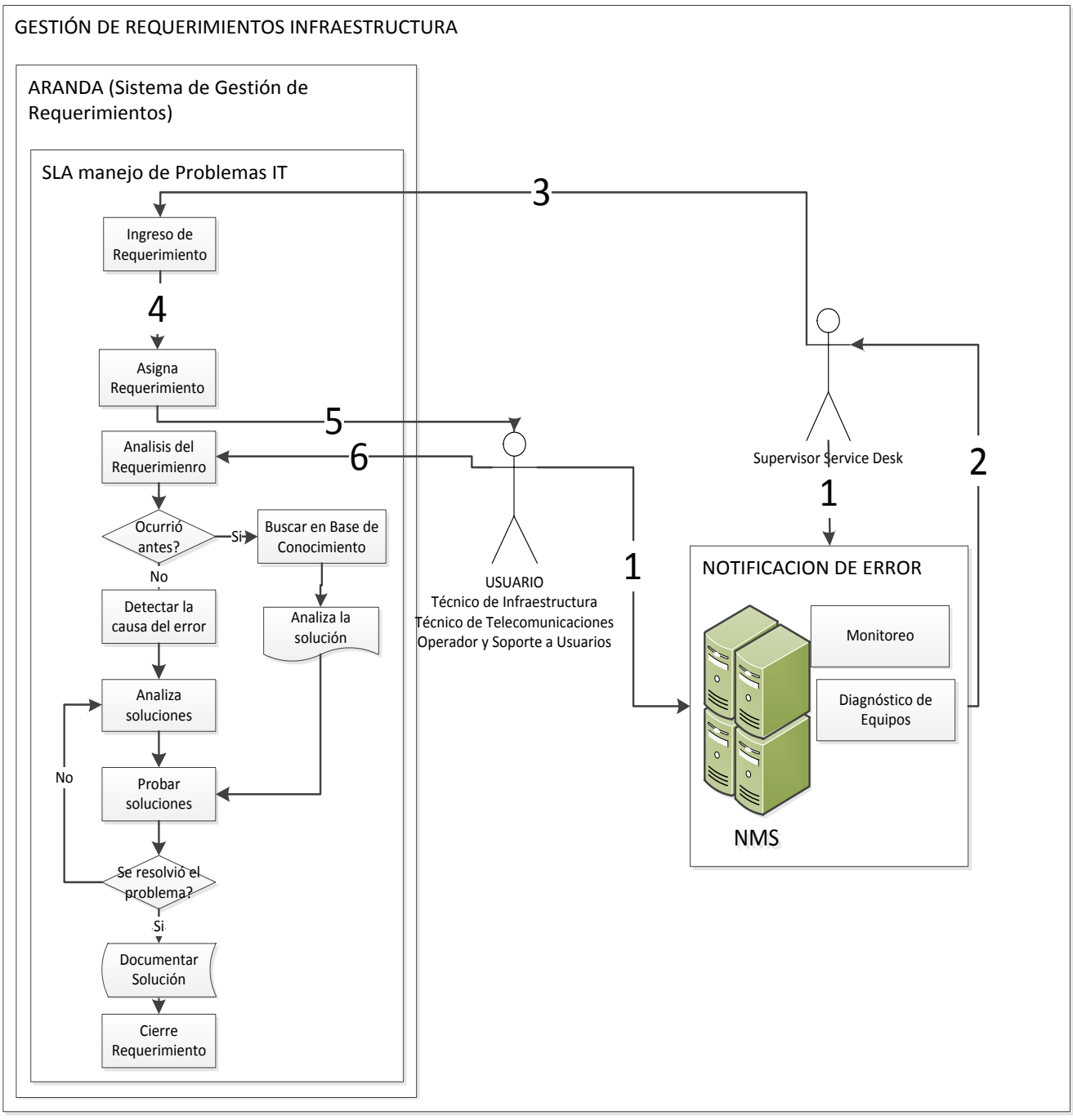


Ilustración 32: Manejo de Incidentes de Red (Diseño Propio)

A continuación se detalla el proceso para el ingreso de requerimiento que el Workflow contendrá y en donde se introducirá la plantilla como documento final del proceso para realizar una estadística y un registro de incidentes en la infraestructura de red, problemas con los servicios o fallas en los servidores.

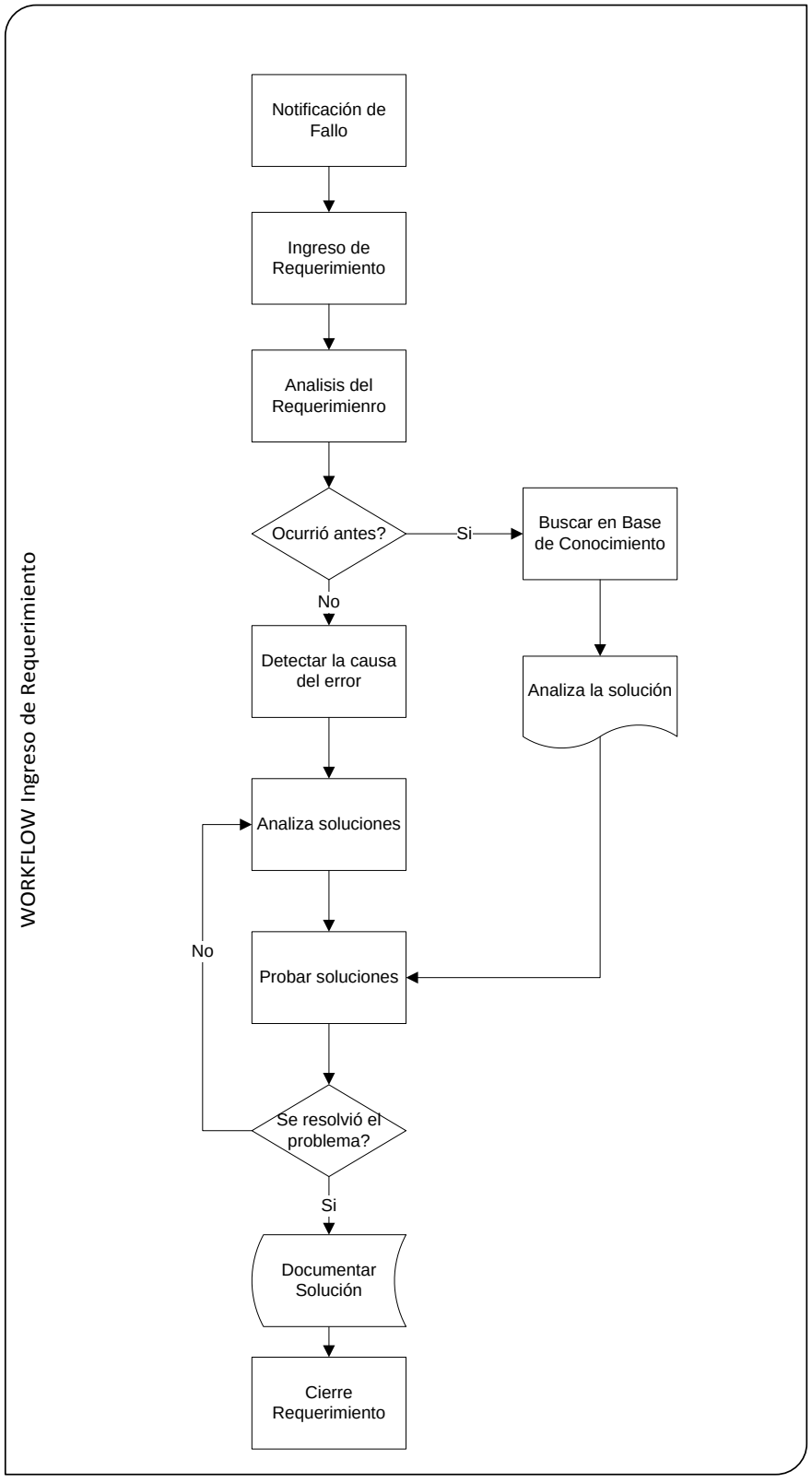


Ilustración 33: Workflow Ingreso de Requerimiento (Diseño Propio)

De acuerdo a lo expuesto en la Ilustración 33 Workflow Ingreso de Requerimiento (Diseño Propio) se desarrolla el presente CASO DE USO para determinar las principales actividades de la Gestión de Requerimientos:

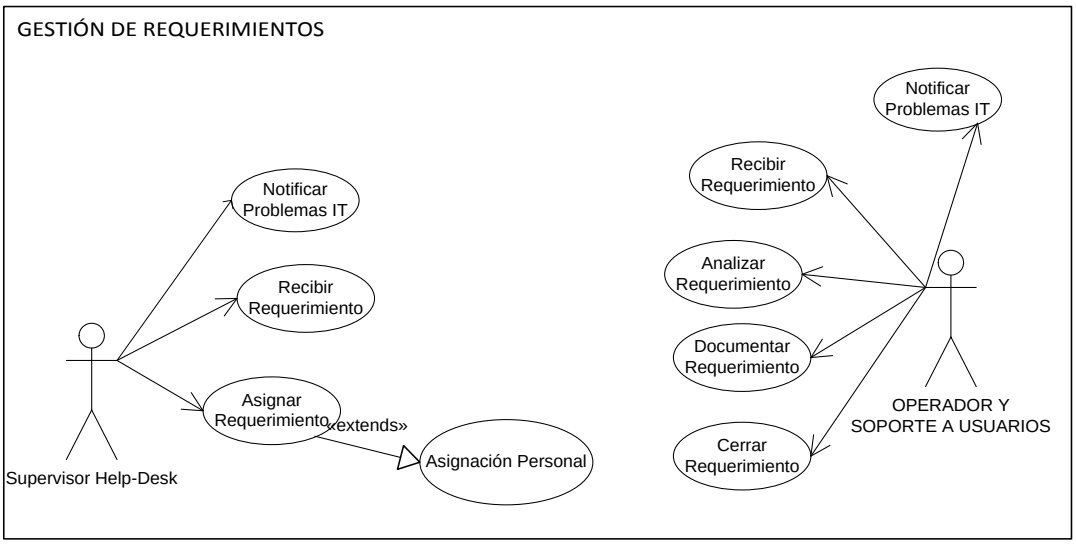


Ilustración 34: Gestión de Requerimientos (Diseño Propio)

4.1.2. Implementación de la Metodología de Red.

Las funcionalidades de un NOC están dadas por las normas ITU y las normas ISO, basadas en el modelo propuesto FCAPS.

Ilustración 35: Funciones de un NOC

Entre las principales actividades tenemos:

- El monitoreo de Alarmas

- Ingreso de Requerimientos.

Siempre que exista alguna alarma o la necesidad de ingresar un requerimiento siempre se generará un ticket en el sistema ARANDA.

Las quejas de los clientes o los incidentes externos que tengan que ver con tecnología también generaran un ticket.

Siempre cada ticket tiene que tener los procesos y almacenarse una base de conocimiento de cómo fue resuelto el incidente.

Al realizar todo este proceso permitirá la solución de problemas.

A continuación se detalla estas actividades gráficamente:

Ilustración 36: Generalizando que es un NOC

4.1.3. Gestión de Rendimiento.

Proporciona información en forma ordenada para determinar la carga del sistema y de la red bajo condiciones naturales y artificiales, proporcionando estadísticas y permitiendo actividades de planeación de configuración.

Su objetivo es medir y proveer la información disponible del desempeño de la red para mantener el funcionamiento de la red interna en un nivel aceptable.

Para la administración del rendimiento tenemos que tener claros tres aspectos:

1. El funcionamiento es una de labor primordial dentro del Departamento de Centro de Cómputo. Mediante esta actividad lo que se prioriza es aquellos servidores, servicios y elementos de red que permiten la conectividad con el Sistema Financiero Nacional y enlaces de comunicaciones.
2. Verificar constantemente que los límites de umbrales que hemos determinado en el punto 3.3.1 se cumplan correctamente dentro de los parámetros establecidos para su medición.
3. Además, debemos seguir correctamente el procedimiento desde el inicio al cierre de un problema y documentar mediante la plantilla de registro todo el proceso que se realiza de acuerdo al flujo de trabajo del punto anterior.

Seguidamente se detalla los procesos actividades y los responsables para llevar la Gestión de Rendimiento dentro del NOC del Banco de Loja:

Tabla 13: *Gestión de Rendimiento*

BANCO DE LOJA SIEMPRE SEGURO Y NUESTRO	**SISTEMA DE GESTIÓN DE RED - NOC BL**		
	GESTIÓN DE RENDIMIENTO	**VERSIÓN:**	1
		AÑO:	2012
Nro.	**PROCESO**	**ACTIVIDADES**	**RESPONSABLE(S)**
1.	Recolección de información del estado de la red y determinación de indicadores de rendimiento	1. Almacenamiento de información de la utilización actual de la red, dispositivos y enlaces en una Base de Datos histórica. 2. Determinación de los siguientes indicadores del desempeño: a. Estado de los dispositivos gestionados (Disponibilidad) b. Tiempo total, retardos en la red y en los nodos (Tiempo de respuesta) c. Calidad del enlace (Exactitud) d. Mediciones dinámicas de la utilización de la red (Grado de utilización) e. Utilización de recursos de red por parte de los dispositivos y/o aplicaciones (Demanda) f. Relación entre la utilización y la demanda de un	HELPDESK Técnico de Infraestructura Operadores del Centro de Cómputo

		recurso de la red (Throughput)	
2.	Monitoreo y Rendimiento de la red	1. Almacenamiento de información de fallas 2. Definición de límites/umbrales de utilización de la red 3. Manipulación de límites e indicadores del rendimiento en la red. 4. Definición de nuevos SLA's para el mantenimiento y generación de nuevas políticas de monitoreo.	HELPDESK Técnico de Infraestructura Operadores del Centro de Cómputo
3.	Análisis y perfeccionamiento	1. Analizar datos relevantes de la información almacenada para detectar las tendencias de uso de recursos 2. Usar simulaciones para determinar cómo la red puede alcanzar máximo rendimiento	HELPDESK Técnico de Infraestructura Operadores del Centro de Cómputo

4.1.4. Gestión de Contabilidad.

Su objetivo es medir los parámetros de utilización en la red para regular apropiadamente las aplicaciones de un usuario o grupo en la red. Tal regulación reduce al mínimo los problemas de la red y controla el acceso de los usuarios a la red.

Además, consiste en actividades de recolección de información de contabilidad y su procesamiento para propósitos de cobranza, consumo y facturación. Estas actividades establecen un límite contable para que un conjunto de costos se combinen con recursos múltiples y se utilicen en un contexto de servicio.

Seguidamente se detalla los procesos actividades y los responsables para llevar la Gestión de Contabilidad dentro del NOC del Banco de Loja:

Tabla 14: *Gestión de Contabilidad.*

BANCO DE LOJA SIEMPRE SEGURO Y NUESTRO	SISTEMA DE GESTIÓN DE RED - NOC BL		
	GESTIÓN DE CONTABILIDAD	**VERSIÓN:**	1
		AÑO:	2012
Nro.	**PROCESO**	**ACTIVIDADES**	**RESPONSABLE(S)**
1.	Llevar una contabilidad de activos	1. Tener un registro de las personas que manipulan y acceden a la información sensible de la empresa. 2. Estadísticas de equipos, servicios, enlaces y consumo de recursos de hardware y software de cada uno de los componentes de la red. 3. Infraestructura de interconexión utilizada para los servicios. 4. Determinar el impacto que tiene dentro de la organización por el mal funcionamiento de la red o equipo. 5. Cambios y modificaciones de la red. 6. Reportes de Activos y equipos. 7. Utilización de servicios y equipos. 8. Control de gastos con respecto de los servicios instalados y los servicios utilizados.	Operador y Soporte a Usuarios HELPDESK Técnico de Telecomunicaciones Técnico de Hardware Técnico de Infraestructura

		9. Facturación con respecto de lo utilizado.	
2.	Inventarios y estadísticas	1. Tener un control de activos y sus respectivos responsables. 2. Actualizar los responsables y equipos cuando se realizan las transferencias de activos. 3. Colocar un serial único a cada dispositivo. 4. Archivar las facturas de cada uno de los equipos adquiridos. 5. Realizar el proceso de devaluación respectiva cada año	Área Financiero - Administrativo

4.1.5. Gestión de Seguridad[79].

Está relacionada con 2 aspectos de la seguridad del sistema: La gestión de seguridad misma, la cual requiere la habilidad para supervisar y controlar la disponibilidad de facilidades de seguridad, y reportar amenazas y rupturas en la seguridad. Y la seguridad de la gestión, la cual requiere la habilidad para autentificar usuarios y aplicaciones de gestión, con el fin de garantizar la confidencialidad e integridad de intercambios de operaciones de gestión y prevenir accesos no autorizados a la información.

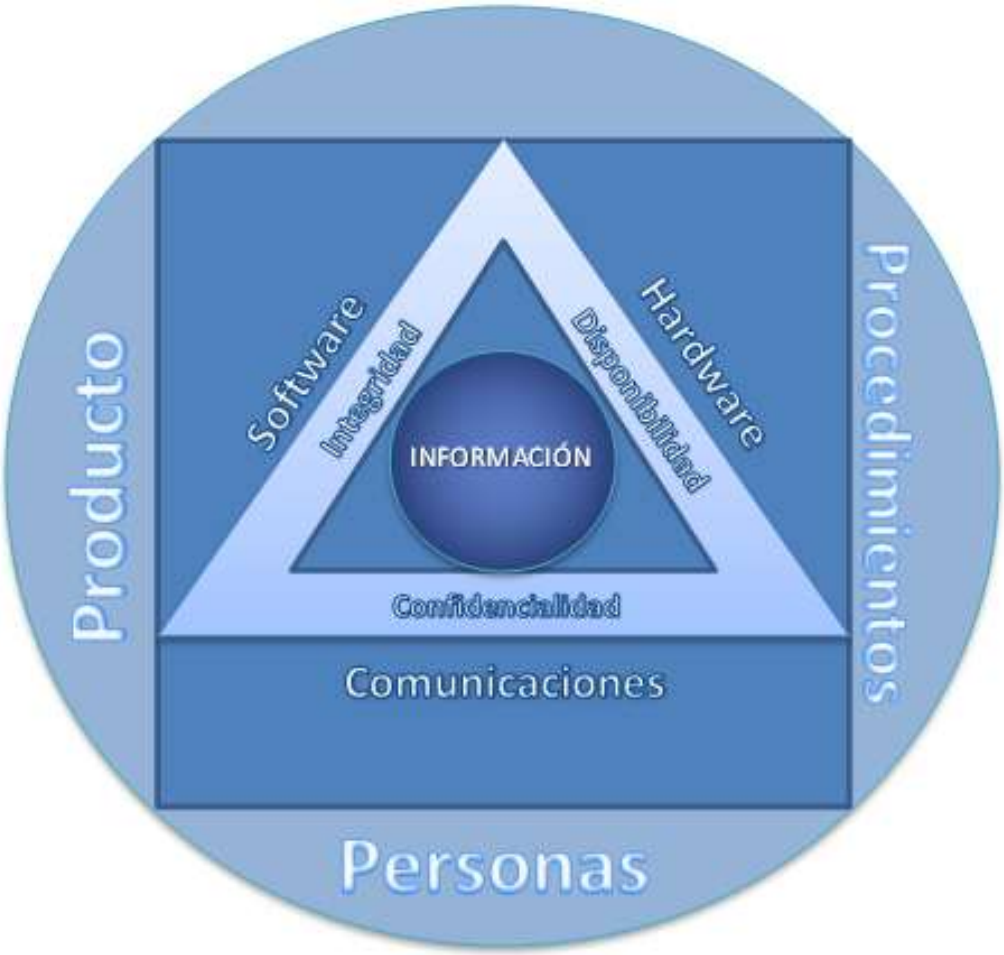


Ilustración 37: Procedimiento de Gestión de Seguridad.[80]

Procedimientos: En la capa más externa del gráfico se refiere a las políticas y normas internas del BANCO para el manejo de todo el departamento de SISTEMAS, también, se tiene que tener en cuenta los roles que desempeñan cada rol dentro del Organigrama del área y sus respectivas responsabilidades.

[79]Hervey Allen y Carlos Armas, «Introducción a la Gestión de Redes», s. f.
[80]Hervey Allen y Carlos Armas, «Introducción a la Gestión de Redes», s. f.

Personas: Es la persona que se realiza para las personas que tiene acceso a los distintos departamentos o códigos de acceso. Como ejemplo: el uso de sistemas biométricos para acceso a sala de servidores o. También, el resguardo de la información sensible en el custodio de valores del Banco.

Producto: Son las seguridad que tenemos para acceso a los sistemas, servicios o servidores dentro del BANCO. Ej.: claves compartidos para acceso a Bases de Datos. En esta parte comprende:

- ***Hardware***: Los equipos que se debe de tener siempre deben estar siempre disponibles a todo momento.
- ***Software***: Los sistemas que se utilizan deben ser confiable.
- ***Comunicaciones***: Los canales de comunicación deben de proteger la confidencialidad de la información.

Información: El valor más grande que tiene una empresa es la información y sobre todo la rigurosidad para mantener la información resguardada y sobre todo si este es un Banco en donde se vincula por parte sistemas financiero y servicios a clientes.

Integridad: Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) *La integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.*

Confidencialidad: Es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados. En otras palabras*, la confidencialidad es el acceso a la información únicamente por personas que cuenten con la debida autorización.*

Disponibilidad: La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. *La disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que lo requieran.*

Seguidamente se detalla los procesos actividades y los responsables para llevar la Gestión de Seguridad dentro del NOC del Banco de Loja:

Tabla 15: *Gestión de Seguridad*

BANCO DE LOJA SIEMPRE SEGURO Y NUESTRO	**SISTEMA DE GESTIÓN DE RED - NOC BL**		
	GESTIÓN DE SEGURIDAD	**VERSIÓN:**	1
		AÑO:	2012
Nro.	**PROCESO**	**ACTIVIDADES**	**RESPONSABLE(S)**
1.	Análisis de riesgos	1. Creación, eliminación y mantenimiento de servicios y mecanismos de seguridad de acuerdo a una política de seguridad establecida 2. Distribución de información de seguridad 3. Las contraseñas deben de constar de dos partes. Una colocada por el oficial de riesgo y otra por el Jefe de Cómputo. 4. Guardar las contraseñas en sobre cerrado y guardarlas en el custodio de valores. 5. Información de los intentos de violación de la seguridad en los equipos activos de comunicación	Riesgo Informático Custodio de Valores Gerencia de Sistemas Jefe del Centro de Cómputo
2.	Evaluación de los servicios de seguridad	1. Comprobación de la autenticidad de la información 2. Control de acceso hacia los objetos gestionados	Auditoria Informática
3.	Evaluación de las soluciones de gestión de seguridad	1. Encriptación 2. Establecer políticas de creación de claves	Riesgo Informático Gerencia de Sistema

		3. Utilización de claves para la identificación de usuarios	Jefe del Centro de Cómputo

4.1.6. Gestión de Configuración.

Su objetivo es supervisar la información de la configuración de la red y de los sistemas para rastrear y manejar los efectos sobre el desempeño de las versiones del software y hardware de la red.

Se distribuye en actividades de inicialización, instalación, y abastecimiento.
Esto permite la colección de información de configuración y estado en demanda, proporcionando facilidades de inventario y además soporta el anuncio de cambios de configuración a través de notificaciones relevantes.

En la configuración es importante designar los responsable de cada uno de los equipos y las responsabilidades que va a desempeñar, teniendo en cuenta que puede tener a cargo un determinado número de servicios y/o servidores para el monitoreo.

Seguidamente se detalla los procesos actividades y los responsables para llevar la Gestión de Configuración dentro del NOC del Banco de Loja:

Tabla 16: *Gestión de Configuración*

BANCO DE LOJA SIEMPRE SEGURO Y NUESTRO	SISTEMA DE GESTIÓN DE RED - NOC BL	
	GESTIÓN DE CONFIGURACIÓN	**VERSIÓN:** 1
		AÑO: 2012

Nro.	PROCESO	ACTIVIDADES	RESPONSABLE(S)
1.	Análisis del estado actual de la red	1. Realizar un inventario general de equipos que se encuentran en la red y las características que tiene cada uno. 2. Conocer la ubicación física de los equipos. 3. Saber el direccionamiento IP que tiene cada máquina. 4. Mantener actualizado los registros del direccionamiento IP de cada una de las agencias y oficinas.	Operador y Soporte a Usuarios HELPDESK Técnico de Telecomunicaciones Técnico de Hardware Técnico de Infraestructura
2.	Determinar la topología de red general que posee el Banco.	1. Definición de nuevos recursos a gestionar 2. Manejo de correspondencia de nombres entre dispositivos y sus direcciones de red 3. Asignación y gestión de nombres a los recursos gestionados 4. Creación, modificación y destrucción de relaciones entre los recursos 5. Determinación de los conflictos reales y potenciales al	Operador y Soporte a Usuarios HELPDESK Técnico de Telecomunicaciones Técnico de Hardware Técnico de Infraestructura

		realizar cambios en las configuraciones 6. Descubrimiento automático de dispositivos	
3.	Control de Configuración	1. Registrar las versiones de los sistemas operativos y las aplicaciones que utiliza cada servicio o servidor de acuerdo a sus rol específico. 2. Respaldar las configuraciones de cada uno de los dispositivos de red como lo son: routers, switches, proxy, firewall. 3. Fijarse que se realices las réplicas del directorio activo. 4. Revisar que los respaldos hechos de cada uno de los dispositivos o servicios se encuentren bien realizadas. 5. Controlar que los respaldos diarios o incrementales realizados por se realicen correctamente.	Operador y Soporte a Usuarios HELPDESK Técnico de Telecomunicaciones Técnico de Hardware Técnico de Infraestructura
4.	Control de inventarios	1. Borrado y actualización de los dispositivos instalados 2. Obtención de informes de la identidad, condiciones de funcionamiento, de los objetos gestionados 3. Determinación de cambios en el software instalado 4. Identificación de cambios en los archivos de configuración 5. Recopilación de datos hardware y software 6. Distribución electrónica de software	Operador y Soporte a Usuarios HELPDESK Técnico de Telecomunicaciones Técnico de Hardware Técnico de Infraestructura
5.	Definición de Grupos para	Se definen los siguientes parámetros:	Operador y Soporte a Usuarios

	el correcto funcionamiento de SNMP v2	1. COMUNIDAD de Lectura y Escritura: gr_bl_rw. 2. COMUNIDAD de Solo Lectura: gr_bl_r. 3. GRUPO de Escritura y Lectura: blnoc_rw. 4. GRUPO únicamente de Lectura: blnoc_ro. a. MIB's permitidas para las Vistas: MIB-2, cisco, snmpv2.	HELPDESK Técnico de Telecomunicaciones Técnico de Hardware Técnico de Infraestructura

4.1.7. Gestión de Fallos.

Establece la generación de notificaciones específicas de error (alarmas), el registro de las notificaciones de error y la verificación de los recursos de red para trazar e identificar fallas.

Seguidamente se detalla los procesos actividades y los responsables para llevar la Gestión de Contabilidad dentro del NOC del Banco de Loja:

Tabla 17: *Gestión de fallos*

BANCO DE LOJA SIEMPRE SEGURO Y NUESTRO	SISTEMA DE GESTIÓN DE RED - NOC BL		
	GESTIÓN DE FALLOS	**VERSIÓN:**	1
		AÑO:	2012
Nro.	**PROCESO**	**ACTIVIDADES**	**RESPONSABLE(S)**
1.	Detección e informe de problemas	1. Presentación del estado de la red, e indicación de la falla, su naturaleza y gravedad 2. Empleo de rutinas para la localización de la falla 3. Almacenamiento de los eventos generados en los recursos gestionados en una Base de Datos de reportes históricos 4. Generación de alarmas para indicar el mal funcionamiento	Operador y Soporte a Usuarios HELPDESK Técnico de Telecomunicaciones Técnico de Hardware Técnico de Infraestructura
2.	Detección de la causa o problema	1. Determinación de la ubicación exacta de cuellos de botella y problemas de red 2. Aislamiento del recurso hardware, medio de transporte o causa externa causante de la falla	Operador y Soporte a Usuarios HELPDESK Técnico de Telecomunicaciones Técnico de Hardware Técnico de Infraestructura
3.	Diagnóstico y resolución de problemas	1. Seguimiento y control del problema desde su detección hasta su resolución de un incidente y/o problema. 2. Determinación de las posibles soluciones para el problema detectado. 3. Respaldo de las configuraciones para mantener la integridad de la topología de red.	Operador y Soporte a Usuarios HELPDESK Técnico de Telecomunicaciones Técnico de Hardware Técnico de Infraestructura

4. Tratar de minimizar o eliminar temporalmente los efectos de los fallos en la red.

4.2. Gestión de Incidentes

4.2.1. Proceso Gestión de Incidentes[81].

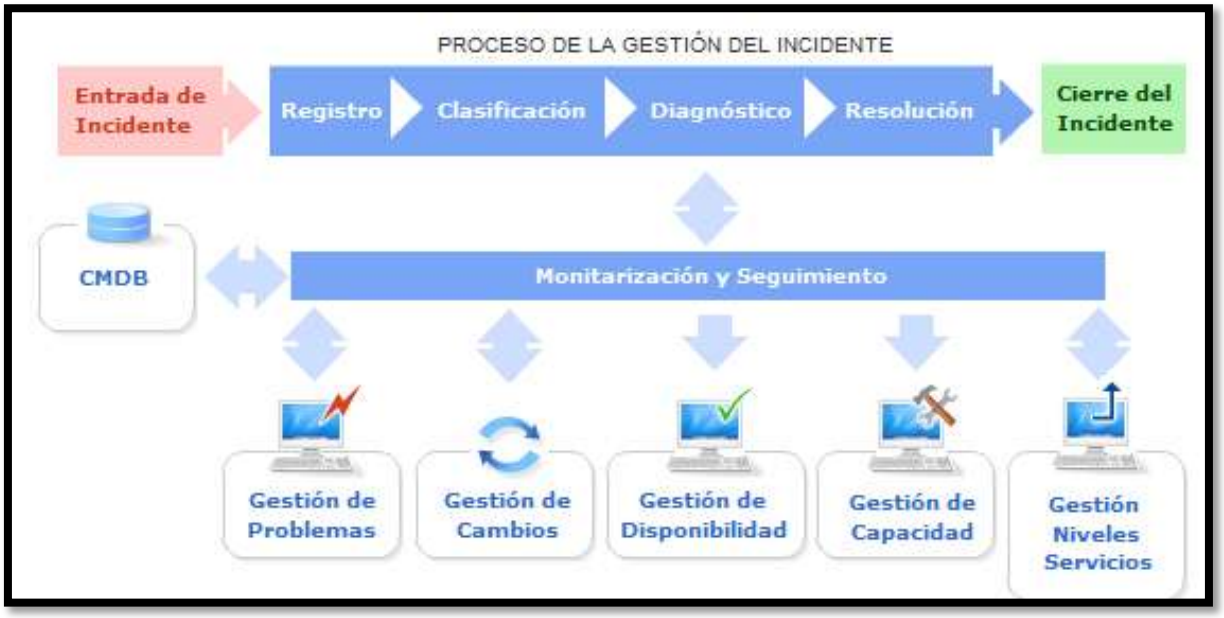


Ilustración 38: Proceso de Gestión de Incidentes basado en ITIL[82]

4.2.2. Registro y Clasificación de Incidentes.

Registro

La admisión y registro del incidente es el primer y necesario paso para una correcta gestión del mismo.

Las incidencias pueden provenir de diversas fuentes tales como usuarios, gestión de aplicaciones, del mismo **HELPDESK**, entre otros.

El proceso de registro debe realizarse inmediatamente pues resulta mucho más costoso hacerlo posteriormente y se corre el riesgo de que la aparición de nuevas incidencias demore indefinidamente el proceso.

- La admisión a trámite del incidente: el **HELPDESK** debe de ser capaz de evaluar en primera instancia si el servicio requerido se incluye en el SLA del cliente y/o en caso contrario canalizarlo con la persona encargada de la Supervisión HELPDESK.
- Comprobación de que ese incidente aún no ha sido registrado: es reportado con frecuencia y que más de un usuario notifique la misma incidencia. Con ésto se evita duplicaciones innecesarias.

[81] Ibid.

[82] «Gestión de Incidentes - Proceso», accedido 23 de mayo de 2012, http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/proceso_gestion_de_incidentes/proceso_gestion_de_incidentes.php.

- **Asignación de referencia**: al incidente se le asignará una referencia que le identificará unívocamente tanto en los procesos internos como en las comunicaciones con el cliente.
- **Registro inicial**: se han de introducir en la base de datos asociada la información básica necesaria para el procesamiento del incidente (hora, descripción del incidente, sistemas afectados...).
- **Información de apoyo**: se incluirá cualquier información relevante para la resolución del incidente que puede ser solicitada al cliente a través de un formulario específico, o que pueda ser obtenida de la propia CMDB (hardware interrelacionado), etc.
- **Notificación del incidente**: en los casos en que el incidente pueda afectar a otros usuarios estos deben ser notificados para que conozcan como esta incidencia puede afectar su flujo habitual de trabajo.

Clasificación

La clasificación de un incidente tiene como objetivo principal el recopilar toda la información que pueda ser de utilidad para la resolución del mismo.

El proceso de clasificación debe implementar, al menos, los siguientes pasos:

- **Categorización**: se asigna una categoría (que puede estar a su vez subdividida en más niveles) dependiendo del tipo de incidente o del grupo de trabajo responsable de su resolución. Se identifican los servicios afectados por el incidente.
- **Establecimiento del nivel de prioridad**: dependiendo del impacto y la urgencia se determina, según criterios preestablecidos, un nivel de prioridad.
- **Asignación de recursos**: si el **HELPDESK** no puede resolver el incidente en primera instancia designara al personal de soporte técnico responsable de su resolución (segundo nivel).
- **Monitorización del estado y tiempo de respuesta esperado**: se asocia un estado al incidente (por ejemplo: registrado, activo, suspendido, resuelto, cerrado) y se estima el tiempo de resolución del incidente en base al SLA correspondiente y la prioridad.
- **Estados de los Incidentes**

  Los colores de cada uno de los estados que puede tener un requerimiento dentro del Área de Sistemas se los describe a continuación:

Tabla 18: *Colores de Casos ARANDA*[83]

Pero los estados y colores utilizados dentro del departamento del Centro de Cómputo para el manejo de requerimientos son:

Tabla 19: *Estados usados por el Centro de Cómputo (de acuerdo a la Tabla* 18*)*

ESTADO DE CASO	DESCRIPCIÓN
REGISTRADO	Este es el primer estado que tiene el caso. Se ingresa cuando se haya detectado algún error
ASIGNADO	Segundo Estado, que es una vez que se encuentra registrado el caso el Supervisor HELPDESK de acuerdo al tipo de requerimiento lo asigna a un operador.
EN PROCESO	Tercer Estado, que es cuando el

[83] Son los colores que se recogió del sistema de manejo de requerimientos ARANDA disponible al momento de realizar el presente proyecto Enero 2012.

ESTADO DE CASO	DESCRIPCIÓN
	OPERADOR empieza a desarrollar la solución
SUSPENDIDO	Si existe algún inconveniente, o cuando se depende de algo que esta fuera del alcance de los operadores (pedido de piezas al proveedor, ayuda de soporte externo) se suspende para luego cerrarlo.
SOLUCIONADO	En este paso se realiza cuando se encuentre aplicada solución que de por CORREGIDO el caso o incidente.
ESCALADO A TERCEROS	Cuando el OPERADOR detecte que el problema depende del PROVEEDOR o por falla del APLICATIVO cuya SOLUCIÓN depende de SOPORTE EXTERNO

Análisis, Resolución y Cierre de Incidentes

En primera instancia se examina el incidente con ayuda de la KB para determinar si se puede identificar con alguna incidencia ya resuelta y aplicar el procedimiento asignado.

Si la resolución del incidente se escapa de las posibilidades del **HELPDESK** éste se escala a un nivel superior para su investigación con expertos asignados. Si los expertos no son capaces de resolver el incidente se seguirán los protocolos de escalado a proveedores o fabricantes dependiendo del caso.

Durante todo el ciclo de vida del incidente se debe actualizar la información almacenada en las correspondientes bases de datos para que los agentes implicados dispongan de cumplida información sobre el estado del mismo.

Si fuera necesario se puede emitir una **Petición de Cambio** (RFC). Si la incidencia fuera recurrente y no se encuentra una solución definitiva al mismo se deberá informar igualmente a la **Gestión de Problemas** para el estudio detallado de las causas subyacentes.

Cuando se haya solucionado el incidente se:

- Confirma con los usuarios la solución satisfactoria del mismo.

- Incorpora el proceso de resolución a la KB.
- Reclasifica el incidente si fuera necesario.
- Actualiza la información en la CMDB sobre los elementos de configuración (CI) implicados en el incidente.
- Cierra el incidente.

4.2.3. Control del Proceso.

La correcta elaboración de informes forma parte esencial en el proceso de **Gestión de Incidentes**.

Estos informes deben aportar información esencial para, por ejemplo:

- La **Gestión de Niveles de Servicio**: es esencial que los clientes dispongan de información puntual sobre los niveles de cumplimiento de los SLA's y que se adopten medidas correctivas en caso de incumplimiento.
- Monitorizar el rendimiento del **HELPDESK**: conocer el grado de satisfacción del cliente por el servicio prestado y supervisar el correcto funcionamiento de la primera línea de soporte y atención al cliente.
- Optimizar la asignación de recursos: los gestores deben conocer si el proceso de escalado ha sido fiel a los protocolos prestablecidos y si se han evitado duplicidades en el proceso de gestión.
- Identificar errores: puede ocurrir que los protocolos especificados no se adecuen a la estructura de la organización o las necesidades del cliente por lo que se deban tomar medidas correctivas.
- Disponer de Información Estadística: que puede ser utilizada para hacer proyecciones futuras sobre asignación de recursos, costes asociados al servicio, etc.

Por otro lado una correcta **Gestión de Incidentes** requiere de una infraestructura que facilite su correcta implementación. Entre ellos cabe destacar:

- Un correcto sistema automatizado de registro de incidentes y relación con los clientes
- Una Base de Conocimiento (KB) que permita comparar nuevos incidentes con incidentes ya registrados y resueltos. Una (KB) actualizada permite:
    - Evitar escalados innecesarios.
    - Convertir el "know-how" de los técnicos en un recurso reutilizable y activo dentro de la empresa para ser utilizado de manera continua.
    - Poner directamente a disposición del cliente parte o la totalidad de estos datos (a la manera de FAQ's) en una Extranet. Lo que puede

permitir que a veces el usuario no necesite siquiera notificar la incidencia.

- Una CMDB que permita conocer todas las configuraciones actuales y el impacto que estas puedan tener en la resolución del incidente.

Para el correcto seguimiento de todo el proceso es indispensable la utilización de métricas que permitan evaluar la forma más objetiva posible el funcionamiento del servicio. Algunos de los aspectos clave a considerar son:

- Número de incidentes clasificados temporalmente y por prioridades.
- Tiempos de resolución clasificados en función del impacto y la urgencia de los incidentes.
- Nivel de cumplimiento del SLA.
- Costes asociados.
- Uso de los recursos disponibles en el **Centro de Cómputo**.
- Porcentaje de incidentes, clasificados por prioridades, resueltos en primera instancia por los **Operadores y Soporte a Usuarios**.
- Grado de satisfacción del cliente.

Escalado y Soporte

Puede suceder que el **HELPDESK o los Operadores de Centro de Cómputo** se vean imposibilitados de resolver en primera instancia un incidente y para ello deba recurrir a un especialista o a algún superior que pueda tomar decisiones que se requieren de autorización de una jerarquía superior.

Básicamente hay dos tipos diferentes de escalado:

- **Escalado funcional**: Se requiere el apoyo de un especialista de más alto nivel para resolver el problema.
- **Escalado jerárquico:** Debemos acudir a un responsable de mayor autoridad para tomar decisiones que se escapen de las atribuciones asignadas a ese nivel, como, por ejemplo, asignar más recursos para la resolución de un incidente específico o si existe un problema con el sistema se puede contactar con el departamento de Desarrollo para ayudar a solucionar el incidente.

El proceso de escalado puede resumirse como sigue:

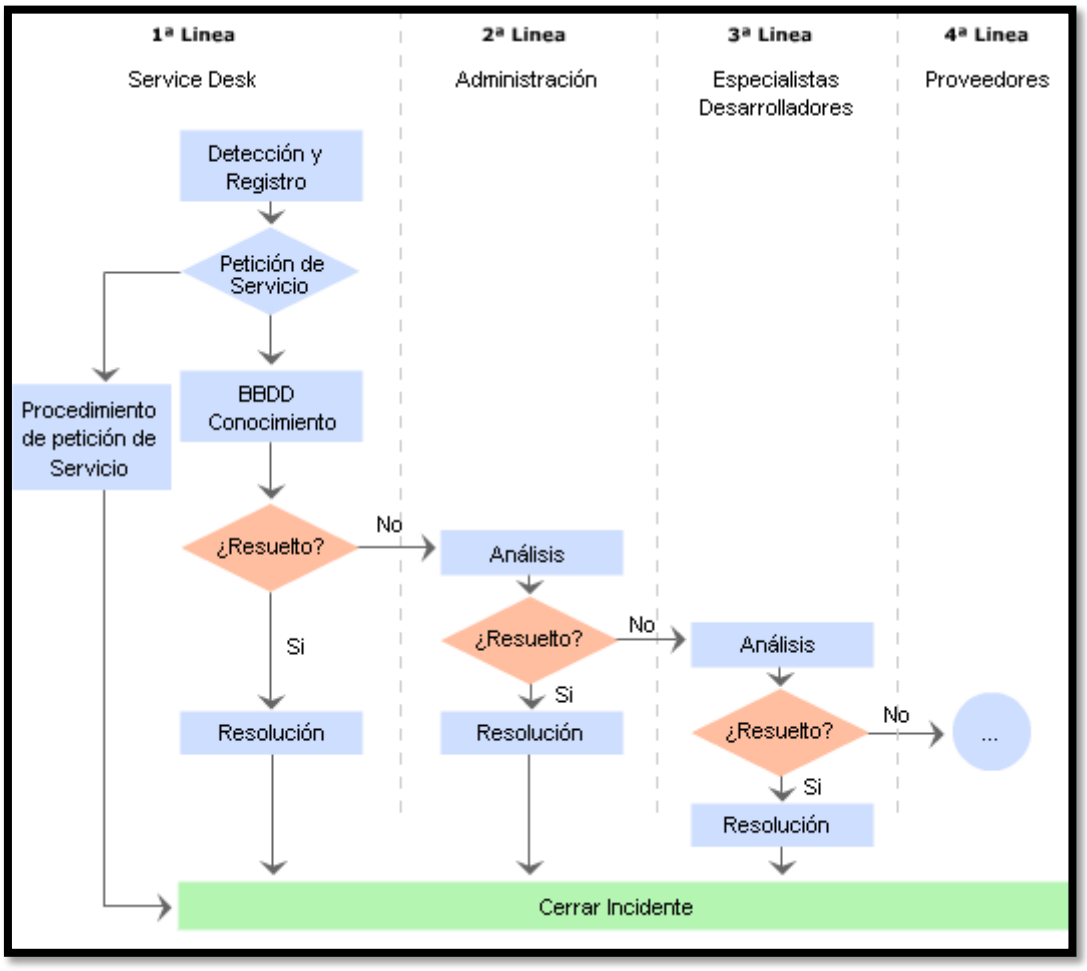


Ilustración 39: Proceso de Manejo de Incidentes basado en ITIL[84]

4.2.4. Clasificación del Incidente.

A diario siempre existen múltiples incidencias concurrentes por lo que es necesario determinar un nivel de prioridad para la resolución de las mismas.

El nivel de prioridad se basa esencialmente en dos parámetros:

- **Impacto:** determina la importancia del incidente dependiendo de cómo éste afecta a los procesos de negocio y/o del número de usuarios afectados.
- **Urgencia:** depende del tiempo máximo de demora que acepte el cliente para la resolución del incidente y/o el nivel de servicio acordado en el SLA.

[84]www.osiatis.es. «Gestión de Incidentes - Visión General». Gestión de Incidentes. Accedido 13 de marzo de 2012. http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/vision_general_gestion_de_incidentes/vision_general_gestion_de_incidentes.php.

También se deben tener en cuenta factores auxiliares tales como el tiempo de resolución esperado y los recursos necesarios: los incidentes "sencillos" se tramitarán cuanto antes.

Dependiendo de la prioridad se asignarán los recursos necesarios para la resolución del incidente.

La prioridad del incidente puede cambiar durante su ciclo de vida. Por ejemplo, se pueden encontrar soluciones temporales que restauren aceptablemente los niveles de servicio y que permitan retrasar el cierre del incidente sin graves repercusiones.

Es conveniente establecer un método para determinar, en primera instancia, la prioridad del incidente. El siguiente diagrama nos muestra un posible "diagrama de prioridades" en función de la urgencia e impacto del incidente:

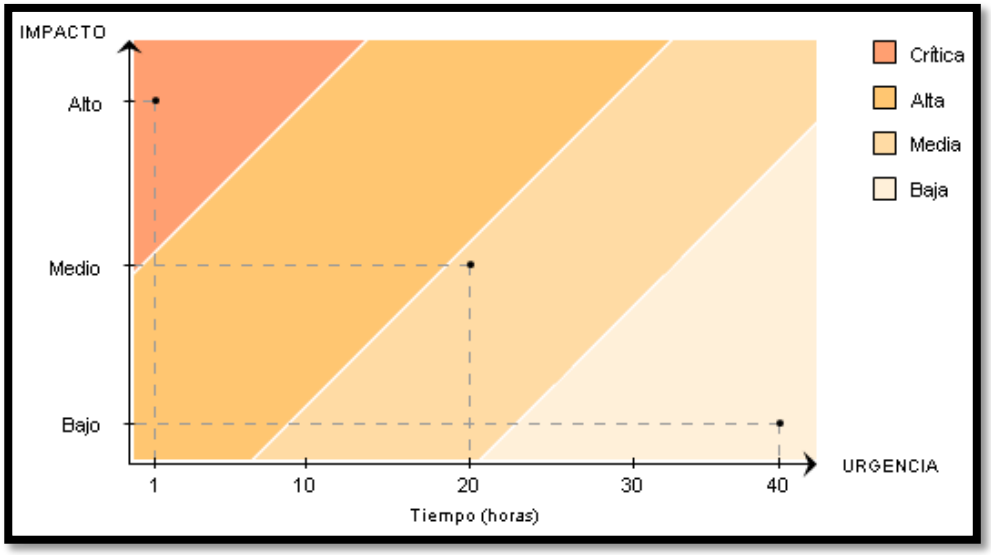


Ilustración 40: Severidad de las alarmas **(IMPACTO)= URGENCIA**[85]

De acuerdo al diagrama anterior podemos definir 4 niveles de criticidad como se explica a continuación:

[85]www.osiatis.es. «Gestión de Incidentes - Visión General». Gestión de Incidentes. Accedido 13 de marzo de 2012. http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/vision_general_gestion_de_incidentes/vision_general_gestion_de_incidentes.php.

Tabla 20: *Niveles de Criticidad*

NIVEL CRITICIDAD	NIVEL CRITICIDAD	DESCRIPCIÓN
4	*Crítico*	*Problemas relacionados con el tráfico de red, problemas de software, hardware, afectación de servicios.*
3	*Alto*	*Operaciones relacionadas con el mantenimiento de Equipos, configuraciones de programas o llegada a los límites de los umbrales.*
2	*Medio*	*Mal funcionamiento de equipos de red.*
1	*Bajo*	*Problemas que a pesar de su ocurrencia la red se mantiene en funcionamiento.*

4.3. Infraestructura Física.

Toda la infraestructura física del sistema de Monitoreo se encontrará alojada dentro del Cuarto de equipos se encuentra en la primera planta del edificio Matriz, la cual se encuentra acondicionada de acuerdo al estándar **ANSI/TIA/EIA-569-A** [86] para el mantenimiento de infraestructura IT.

Todo lo que es monitores y pantallas de monitoreo se encontraran dentro del centro de Cómputo en el lugar destinado para el efecto.

4.4. Infraestructura Tecnológica.

4.4.1. Servidores para instalación de NAGIOS.

Sistema Operativo del Servidor:

- Sistema Operativo Base VMWare ESXi 3.5
- Máquina Virtual con Sistema Operativo CENTOS Versión 6

Especificaciones Mínimas del Servidor:

- 1.x GHz Procesador
- 1 GB RAM
- 120 GB HD

[86] **ANSI/TIA/EIA-569-A.** Disponible en web: http://www.galeon.com/30008ceti/tarea3.html

Especificaciones Recomendadas del Servidor:

- 2.x GHz Procesador
- 3 GB RAM
- 320 GB HD

Especificaciones mínimas para el equipo de monitoreo

- Procesador CORE i3 3.2 GHz
- 500 GB de disco duro
- 4 GB de Memoria RAM
- Tarjeta de Video DDR3 de 2 GB
- 3 Monitores LCD de 32 pulgadas

4.4.2. Selección Herramientas a utilizar.

4.4.2.1. Definición y Evaluación de Herramientas[87].

El análisis que se llevó a cabo para poder escoger NAGIOS fue el de comparar esta herramienta con otras existentes en el mercado que prestan el servicio de monitoreo, como lo son: PANDORA FMS, JFFNMS, ZENOSS Y ZABBIX.

La Evaluación realizada es en base a los criterios dados en el punto 2.13 CRITERIOS DE EVALUACIÓN PARA ESCOGER LA HERRAMIENTA DE MONITOREO, y los Cuadros de las Funcionalidades Puntos 2.14.1 y 2.14.2 que se recogieron del análisis hecho por el Departamento de Sistemas, se procedió a escoger NAGIOS para desarrollo del presente proyecto.

Seguidamente en los puntos 4.4.2.1.1 y 4.4.2.1.2 se explicarán detalladamente los criterios evaluados que se tomaron en cuenta para escoger dicha herramienta y en la Tabla 28: Evaluación Técnica de ***Herramientas*** se muestra las principales características de NAGIOS frente a otras herramientas comparadas (más información del análisis sobre la realización de esta tabla se encuentra en el ANEXO 6).

La herramienta escogida es muy sencilla para manejar y presenta la información de tal forma que es más fácil de interpretar para el administrador, presenta un historial de eventos en el monitoreo de equipos y servicios.

Según el análisis realizado en el punto 3.4.5.8 los tiempos de solución de requerimientos se vieron disminuidos por el uso de esta herramienta de hasta un 30%.

[87] Ver más en el ANEXO 9: Análisis de Herramientas

Al realizar el monitoreo síncrono de equipos NAGIOS es el que menos recursos de hardware consume. Entonces, podemos decir que el tiempo de ejecución de ciertas tareas y procesos se van a realizar más rápidamente por el bajo consumo de recursos hardware.

NAGIOS es el sistema que ofrece un mayor número de opciones como mapas, iconos descriptivos fáciles de entender, representación gráfica de datos, distintos colores según el nivel de gravedad del evento. Es un sistema sencillo de instalar y configurar lo que permite al departamento de sistema en caso de una contingencia del sistema de monitoreo tener el equipo funcionando en 62 minutos de acuerdo a la siguiente tabla:

Tabla 21: *Tiempos resultantes al realizar Instalación NMS*[88]

DESCRIPCIÓN NMS	TIEMPO DE INSTALACIÓN (min)
ZENOSS	136
JFFNMS	117
PANDORA FMS	146
ZABBIX	151
NAGIOS	62

Permite asignar roles de acuerdo a las tareas desempeñadas por los usuarios. Por ejemplo: unos encargados del estado de los servicios y otros usuarios encargados de los recursos del equipo, a los que se envían diferentes mensajes de acuerdo a sus responsabilidades. Múltiples usuarios pueden acceder a la interface web, además cada usuario puede tener una vista personalizada, única y restringida.

NAGIOS permite definir notificaciones mediante correo electrónico y/o SMS muy específicas y granulares; tales como: tipo de servicio, criticidad, horario de monitoreo, cantidad de alertas, tiempo de espera para enviar las alertas, etc.; estas configuraciones de las alertas son necesarias para que no sean excesivas y tener un entorno de monitorización más apegado a la realidad del funcionamiento de los sistemas de TI para no saturar nuestro buzón de correo y el consumo de recursos de hardware.

[88] Tabla realizada de acuerdo a los tiempos de instalación de cada una de las herramientas.

Dispone de gran cantidad de plugins y programas que se pueden integrar para robustecer su funcionamiento como: SNMP + MRTG (para mejorar las gráfica), Cacti + NPC Plugin, PNP4Nagios, entre otros. Además, del control de nuevos servicios como una variedad de los gestores de bases de datos MySQL o PostgreSQL. Para programarlos, podemos utilizar el lenguaje que prefiramos, ya que NAGIOS funciona como una plataforma transparente para enviar mensajes con las salidas de los programas. Facilidad de poder configurar nuevas alertas y personalización de scripts para nuevas alertas y/o reglas de monitoreo.

NAGIOS es un sistema Open Source y con coste de licencia cero y funciona sobre sistema operativo Linux. El NAGIOS es usado en gran cantidad de entornos financieros por sus prestaciones y robustez. (De acuerdo a la cantidad de clientes que se puedo verificar en la página web http://users.nagios.org/).
Una de las características que hace la diferencia de NAGIOS con otras herramientas es el envío de notificaciones mediante SMS siendo esta característica, única en este sistema de monitoreo.

NAGIOS posee también Interfaces para monitoreo desde móvil mediante aplicaciones de integración con BlackBerry, iPhone y Android.
El equipo de desarrolladores de NAGIOS realiza constantes actualizaciones al sistema NAGIOS, de acuerdo al registro de actualizaciones que se encuentra en la tabla siguiente, se podría decir que las actualizaciones son bimensuales cuando se trata de corregir fallos o errores en la seguridad. A continuación se coloca un historial de actualizaciones:

Tabla 22: *Historial de Actualización NAGIOS*[89] *(Tomado de http://www.NAGIOS.org/projects/NAGIOScore/history/core-3x)*

VERSION	FECHA
3.3.1.	2011/07/25
3.2.3	2010/10/03
3.2.2	2010/09/01
3.2.1	2010/03/09
3.2.0	2009/08/12
3.1.2	2009/06/23

[89] Tomado de: http://www.nagios.org/projects/nagioscore/history/core-3x

VERSION	FECHA
3.1.1	2009/06/22
3.1.0	2009/01/25

Otro aspecto importante por escoger NAGIOS es la gran cantidad de información y documentación que se puede encontrar y el soporte de una comunidad que va creciendo en internet para compartir experiencias, conocimiento, nuevos plugins.

Además, NAGIOS posee integrado el servicio para monitoreo de servicios que los otros NMS como PANDORA se tiene solo en la versión pagada.

NAGIOS es un sistema que cuenta con más de 10 años en desarrollo, es un sistema que permite escalar hasta monitorear más de 100.000 nodos, cuenta con gran reconocimiento, ganador de múltiples premios. Actualmente cuenta con más de 250.000 usuarios alrededor del mundo. Tiene una amplia comunidad de usuarios a través del sitio web.
Por lo tanto de acuerdo al análisis realizado, se escogió NAGIOS para el desarrollo del presente proyecto, de acuerdo a un estudio detallado junto con el departamento de sistemas es la herramienta que más se ajusta a los requerimientos expuesto en el 2.13 CRITERIOS DE EVALUACIÓN PARA ESCOGER LA HERRAMIENTA DE MONITOREO; y también, en las funcionalidades específicos expuesto en el apartado 2.14.1 y 2.14.2. Prueba de esto es el detalle que se ofrece a continuación:

Por todo lo explicado anteriormente NAGIOS es muy superior a los demás NMS comparados. En los anexos se encuentra el acta firmada de determinación de la herramienta.

4.4.2.1.1. Cumplimiento de Criterios de Evaluación para Escoger la Herramienta de Monitoreo.

Los criterios de Evaluación definidos en el apartado 2.13 de la presente tesis se detallan a continuación el cumplimiento de cada uno de ellos.

- Estudiar las características de la herramienta
    - **Capacidad de Integración con otras herramientas**
      Se puede integrar con varios plugins o con programas similares como Cacti, Centreon, O.T.R.S. (Open-source Ticket Request System), etc.

- **Costos de la Herramienta**

  Se han analizaron dos opciones de SO, como son Linux y Windows, en ambos casos todo el software para la implementación de NAGIOS estaba disponible para ambos sistemas operativos. Y se pudo concluir lo siguiente: NAGIOS funciona correctamente en las dos plataformas.

  - *En Linux no necesitamos licencia, ya que la versión utilizada para la implementación es CENTOS 6.*
  - *Linux se puede configurar para que sólo invierta recursos en lo que realmente necesitamos, quitando todos los componentes en la instalación que no creamos oportuno tener.*

  La implementación se ha realizado sobre Linux. La opción que se escogió fue CentOS 6, debido a que ya se había trabajado con esta distribución y que revisando, todos los paquetes necesarios para la implementación estaban disponibles. Esto permite en gran medida disminuir el coste final del producto.

  Linux gestionará mejor los procesos y no invierte muchos recursos en la interface gráfica, la cual no necesitamos para nada. Además nos interesa tener un SO multiusuario que nos gestione múltiples sesiones de terminal (Windows) o ssh (Linux); en Windows necesitaríamos una versión server, lo cual al escoger Linux como plataforma base del SO nos ahorra costos en la licencia.

  Además, con la idea a futuro es tener una imagen que se pueda instalar en diferentes equipos de manera de poder distribuir el monitoreo en aquellas agencias con mayor número de usuarios nos será mucho más útil Linux por el tema de las licencias.

- **Generación de Reportes**

  NAGIOS dispone de una gran cantidad de reportes visuales, reportes de estadísticas y de reportes para envío mediante mail; además, permite asignar reportes de acuerdo a los roles y responsabilidades de cada usuario.

- **Medios de notificación y alarmas**

  NAGIOS posee dos sistemas de notificaciones:

Notificaciones pasivas: *Bajo este concepto se entiende la visualización del estado de la monitorización en la página web de NAGIOS. Esta visualización debe ser observada permanentemente por el usuario o administrador. NAGIOS no ejecuta ninguna acción en caso de cambio de estado de un observable, por ello se denominan notificaciones "pasivas".*

Notificaciones activas: *En este caso se le exige al sistema tomar una medida o ejecutar una acción determinada en caso de cambio de estado para informar a un usuario (contacto). Una notificación activa implica la ejecución de un comando y puede, por lo tanto, adoptar diversas formas. Dentro de estas notificaciones se encuentran las notificaciones mediante SMS.*

El caso general, en caso de existir un problema detectado por la monitorización, bien sea en un observable como en un componente, se genera y envía un e-mail y/o SMS automáticamente.

- **Interface de usuario**

  La interface de usuario permite observar de forma gráfica cuando ocurre un problema y ejecutar un diagnóstico de los recursos remotos desde NAGIOS. También, se pueden ejecutar diagnósticos de sistema operativo, consultas, y ver el estado del servidor.

  Uso de su interface web permite ver información detallada de los estados de los distintos componentes, reconocer problemas de forma rápida.

  - *Estado de la monitorización: Muestra los estados de los distintos observables y, con ello, de los distintos componentes monitorizados. Según el estado se asignan colores para informar al usuario de posibles problemas y advertencias de un modo claro y directo.*
  - *Evolución temporal: Los cambios de estado de los observables se almacenan en archivos en el servidor, los cuales pueden ser evaluados posteriormente para mostrar la evolución temporal de los observables o de la accesibilidad de un componente a través de la red en la página web. Dado que NAGIOS solo almacena datos en los cambios de estado, esta visualización es bastante limitada.*
  - *Configuración de la monitorización: Para contribuir a la administración del sistema, se ofrece una opción de visualización de las configuraciones de los distintos objetos (componentes, consultas a observables, contactos, etc.)*

- **Facilidad de Uso**

  Tiene una interface de usuario muy útil y visual, con la que a partir de colores, podemos ver el estado de la red y ver los cambios de estado que se producen.

  Además posee una interfaz web muy descriptiva con colores en cuando a la criticidad de los eventos, notificaciones mediante alertas visuales y fácil configuración del sistema.

- **Registro de Eventos**

  El demonio syslog en el sistema nos permite tener un servicio a la espera de recibir logs de cualquier tipo de sistema, que previamente haya sido configurado, y que envíe eventos que ocurran en su funcionamiento, dependiendo del nivel de logs que le configuremos y los umbrales que tengamos.

- **Documentación**

  Existe una extensa documentación en la web y soporte, además, posee una gran comunidad de usuarios y desarrolladores.

- **Personalización de nuevas alertas e ingresos de nuevas métricas y umbrales de medición.**

  Se pueden personalizar nuevas alertar y nuevas notificaciones de acuerdo al crecimiento de la organización.

- **Adaptabilidad a las necesidades e infraestructura del Banco.**

  Como software Open Source, está desarrollado para ser adaptado y configurado y adaptado a cualquier necesidad dependiendo del cliente. Los usuarios pueden organizar los dashboard, la visualización de métricas, y agrupar recursos para que representen sus roles, intereses y responsabilidades.

- **Autodescubrimiento de la topología**

  Incluye soporte para reconocer más de 75 productos y tecnologías. Descubre automáticamente y crea el inventario, y registra las métricas de

desempeño de sus servicios a través de la infraestructura física, virtual y servicios.

Este sistema permite monitorear una importante cantidad de dispositivos y sistemas como por ejemplo: Sistemas Operativos Windows, Sistemas Operativos Linux/Unix, Routers, Switches, Firewalls, Impresoras, Servicios y Aplicaciones.

4.4.2.1.2. Cumplimiento de Funcionalidades que debe tener la Herramienta de Monitoreo.

Las funcionalidades descritas en el punto 2.14.1 y 2.14.2 se evaluaron de acuerdo a la siguiente escala de valoración:

Tabla 23: *Tabla de Escalas de Valoración*

Escala	Valor
0	Malo/No existe
1	Regular
2	Bueno
3	Muy bueno
4	Excelente

4.4.2.1.3. Funcionalidades Generales.

Tomando como referencia la

Tabla 23: Tabla de Escalas de *Valoración* se realizó la evaluación del punto 2.14.1, para lo cual el análisis está apoyado en los resultados que se obtuvieron después de las pruebas de instalación realizadas.

Tabla 24: *Evaluación de Funcionalidades Generales*

DESCRIPCIÓN	ZENOSS	JFFNMS	PANDORA FMS	ZABBIX	NAGIOS
Facilidad de Instalación	2	3	3	2	3
Facilidad de Configuración	2	3	3	2	3
Administración de Interfaz Web	2	3	2	2	3

DESCRIPCIÓN	ZENOSS	JFFNMS	PANDORA FMS	ZABBIX	NAGIOS
Documentación	3	3	3	3	4
Integración con Plugins	2	3	2	3	3
Facilidad de Uso	2	3	3	3	3
Integración con otras herramientas	2	3	2	2	3
Alertas y Notificaciones	2	2	2	2	3
Creación Personalizada de Scripts	2	3	1	2	3
Soporte en Línea	3	3	3	3	3
Usado en la industria financiera	2	2	1	2	3
Actualizaciones	2	2	2	2	3
Monitoreo de Servicios	2	2	1	2	3
TOTAL	**41**	**48**	**41**	**43**	**53**

4.4.2.1.4. Funcionalidades Específicas.

Tomando en cuenta la Tabla 23: Tabla de Escalas *de Valoración* se realizó la evaluación del punto 2.14.2, para lo cual el análisis está apoyado en los resultados que se iban obteniendo a lo largo del desarrollo de la presente investigación.

Tabla 25: *Evaluación de Funcionalidades Específicas*

ANÁLISIS DE FUNCIONALIDADES					
FUNCIONALIDADES GENERALES					
DESCRIPCIÓN	**ZENOSS**	**JFFNMS**	**PANDORA FMS**	**ZABBIX**	**NAGIOS**
Monitorear distintos sistemas operativos	3	3	2	3	3
El servidor se instala en ambiente Linux	3	3	3	3	3
Monitorear al menos 100 componentes	3	3	3	3	4
Tener agentes de monitoreo que trabajan sobre los sistemas clientes	3	3	3	3	3
Generación de reportes operativos y estadísticos	2	2	2	2	3
Distribución de Usuarios por roles y responsabilidades	2	2	2	2	3

ANÁLISIS DE FUNCIONALIDADES					
FUNCIONALIDADES GENERALES					
DESCRIPCIÓN	**ZENOSS**	**JFFNMS**	**PANDORA FMS**	**ZABBIX**	**NAGIOS**
Tener una pantalla central de administración y configuración	2	2	2	2	2
FUNCIONALIDAD DE HARDWARE					
Monitoreo de hardware (uptime servers, routers, etc.,)	3	3	3	3	3
Monitoreo entornos Virtuales VMWare	1	0	0	0	4
Enviar Alarma si no responde el equipo computacional (Server)	3	3	3	3	3
Enviar Alarma si no responde el equipo de red (router, switch)	3	3	3	3	3
FUNCIONALIDADES A NIVEL DE SISTEMA OPERATIVO					
Enviar alarma si se llega a determinados umbrales de disco duro	3	3	3	3	3
Enviar alarma si se llega a determinados umbrales de memoria	3	3	3	3	3
Enviar alarma si se llega a determinados umbrales de CPU	3	3	3	3	3
Controlar procesos (cantidad)	3	3	2	2	3
Controlar archivos (tamaño)	2	2	2	2	2
FUNCIONALIDADES DE SERVICIOS Y APLICACIONES					
Monitorear software de base y generar alarmas ante caídas	3	3	3	3	3
Monitorear software de aplicaciones y generar alarmas ante caídas	3	3	3	3	3
Monitoreo de Enlaces y generar alarmas ante caídas	3	3	3	3	3
FUNCIONALIDADES DE NOTIFICACIONES					
Permitir el envío de notificaciones vía email	3	3	3	3	3
Permitir el envío de notificaciones vía Correo Electrónico	3	3	3	3	3
TOTAL	**57**	**56**	**54**	**55**	**63**

4.4.2.1.5. Descripción de cada una de las funcionalidades que debe de cumplir la Herramienta de Monitoreo.

Según las Funcionalidades Generales descritas en el apartado 2.14.1 se puede describir cada una de las funcionalidades como sigue:

A. Evaluar el tipo de licencia, el sistema debe ser de código abierto (Open Source).
   El tipo de licencia que tiene NAGIOS es Open Source GPL.

B. El Sistema debe poder monitorear al menos 100 componentes de red.
Es un sistema que en su versión NAGIOS Core permite el monitoreo de más de 100 componentes de red.

C. Debe monitorear: Servidores (uso de memoria, uso de CPU, uso de disco, etc.), aplicaciones (servidores de base de datos, etc.), y dispositivos de red (routers, etc.).
Mediante la configuración del servicio SNMP se puede realizar el monitoreo del estado de los dispositivos y mediante la instalación del agente permite monitorear los recursos de memoria, uso del CPU, Disco Duro, además, se puede verificar el estado de aplicaciones y que servicios se tiene corriendo a nivel de software cada equipo.

D. El servidor se debe poder instalar en Linux.
El servidor del NMS NAGIOS permite instalar tanto en Windows como en LINUX.

Tabla 26: *Plataformas Soportadas por NAGIOS*

PLATAFORMA	SERVER	AGENT
Linux **Se puede Instalar en:** **Ubuntu, RH4, Centos, Fedora**	*	Instalación del Servicio SNMP y NRPE para Linux Instalación de Cliente NSCliente++ para Windows
Windows 2003, Windows 2008	*	Instalación del Servicio SNMP y NRPE para Linux Instalación de Cliente NSCliente++ para Windows

E. Debe monitorear servidores con sistemas operativos Windows, Linux y VMWare.
NAGIOS es la única plataforma de monitoreo que puede realizar el monitoreo de las tres plataformas.

F. Debe generar alertas cuando se identifican situaciones que así lo ameriten.
Las alertas se pueden presentar de varias maneras:
- *VISUALES: Se las puede observar dentro del dashboard, se las puede revisar las alertas en el mail.*

- *AUDITIVAS: Mediante la generación de sonidos cuando se genera alguna caída de enlace o pérdida de conexión con algún servidor y/o servicio.*

G. Los datos se deben poder exportar a una base relacional Open Source.
Las Base de Datos se puede exportar a Flat file, SQL, Oracle, MySQL, PostgreSQL, IBM DB2, SQLite. Un detalle importante es que NAGIOS es el que más integración tiene con la mayoría de Base de Datos existentes en el mercado.

H. El sistema debe trabajar con agentes instalados en los equipos clientes.
Si puede trabajar con agente instalado (En este caso se tiene instalado el NSClient++) o con el servicio SNMP para monitoreo.

I. Disponer de un Agente para realizar el monitoreo:
El agente que se instala es el NSCliente++-0.3.9; es un software libre y que se encuentra disponible para arquitecturas de 32 y 64 bits, consume poca cantidad en memoria y el espacio de instalación en el disco es de 16MB.

J. Permite generar complementos (plugins) y brinda información de cómo desarrollarlos.
Permite diseñar plugins, o complementos, para desarrollar chequeos personalizados. No están limitados a ningún lenguaje de programación específico. Existe documentación suficiente y clara disponible del sistema.

K. El sistema es muy conocido o utilizado. Existencia de empresas clientes o usuarios a los que se puede referenciar.
Actualmente cuenta con más de 250.000 usuarios alrededor del mundo. Además, posee un gran portafolio de clientes pertenecientes al Sector Financiero.

L. Existen soluciones a errores encontrados. Se han publicado nuevas versiones o nuevos paquetes en el último año.
Las soluciones a errores son periódicas y cuando existe algún error o problema podemos utilizar los foros o documentación existente. También las nuevas versiones son por lo general cada 2 meses. Veamos la Tabla 22: Historial de Actualización NAGIOS (Tomado de http://www.NAGIOS.org/projects/NAGIOScore/history/core-3x).

De acuerdo a las Funcionalidades Específicas dadas en el punto 2.14.1 se puede resumir en lo siguiente.

Tabla 27: *Cuadro de cumplimiento de Funcionalidades Generales*

Criterio de Evaluación	ZENOSS	JFFNMS	PANDORA FMS	ZABBIX	NAGIOS
A.	SI	SI	SI	SI	SI
B.	SI	SI	SI	SI	SI
C.	SI	SI	SI	SI	SI
D.	NO	NO	NO	NO	SI
E.	SI	SI	SI	SI	SI
F.	SI, en parte	SI, en parte	SI, en parte	SI, en parte	SI
G.	SI	SI	SI	SI	SI
H.	SI	SI	SI	SI	SI
I.	SI	SI	SI	SI	SI
J.	NO, medianamente	NO, medianamente	NO	NO, medianamente	SI
K.	SI	SI	SI	SI	SI
L.	SI, medianamente	SI, medianamente	SI, medianamente	SI, medianamente	SI

4.4.2.1.6. Cuadro de Evaluación Técnica de Herramientas.

El presente cuadro fue recopilado con el análisis realizado para escoger la herramienta NMS. Todo el detalle se encuentra especificado en el **ANEXO 7.**

Tabla 28: *Evaluación Técnica de Herramientas*

CARACTERÍSTICAS	ZENOSS	JFFNMS	PANDORA FMS	ZABBIX	NAGIOS
AUTODESCUBRIMIENTO	**SI**	**SI**	**SI**	**SI**	**SI, Detalle completo**
GRAFICAS	**SI**	**SI**	**SI**	**SI**	**SI**
ESTADÍSTICAS	**SI**	**SI**	**SI**	**SI**	**SI**
SNMP	**SI**	**SI**	**SI**	**SI**	**SI**
SYSLOG	**SI**	**SI**	**SI**	**SI**	**SI**

CARACTERÍSTICAS	ZENOSS	JFFNMS	PANDORA FMS	ZABBIX	NAGIOS
OPTIMIZACIÓN DE RECURSOS DE HARDWARE	NO	NO	NO	NO	SI
MONITOREO DE ENTORNOS VIRTUALES	NO	NO	NO	NO	SI
SCRIPTS EXTERNOS	SI	SI	SI	SI	SI
ALERTAS	SI	SI	SI	SI	SI, hasta con SMS
INTERFAZ WEB	Control Total	Control Total	Control Total	Control Total	Control Total
BASE DE DATOS	RRDTOOL y MySQL	RRDTOOL, MySQL y PostgreSQL	SQL	SQL	SQL, PostgreSQL, Oracle
EVENTOS	SI	SI	SI	SI	SI
LICENCIA	GPL	GPL	GPL2	GPL	GPL
COMPLEMENTOS	SI	SI	SI	SI	SI
SEGURIDAD	SI	SI	SI	SI	SI

4.4.2.1.7. Algunas otras características propuestas.

En la presente tabla se presenta un resumen de todas las funcionalidades expuestas anteriormente que se han tomado en cuenta lo siguiente:

Tabla 29: *Otras Características propuestas.*

Nombre	Reportes Mediante IP SLA	Agrupación Lógica	Tendencia	Predicción de Tendencia	Auto Descubrimiento	Agente	ESX/ESXi	Nombre	Reportes Mediante IP SLA	Agrupación Lógica	Tendencia	Predicción de Tendencia
ZENOSS	Si	Si	Si	Si	Si	Soportado	No	Si	Si	Si	Si	Control Total
JFFNMS	Si	Si	Si	Si	Si	Soportado	No	Si	Si	Si	Si	Control Total
Pandora FMS	Si	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	Control Total
ZABBIX	Si	Si	Si	No	Si	Soportado	No	Si	Si	Si	Si	Control Total
NAGIOS	Si	Si	Si	Si	Si	Si	Soportado mediante plugins ***	Si	Si	Si	Si	Control Total

***Una de las características que tiene NAGIOS es el soporte para el monitoreo de sistemas virtuales como el VMWare ESX/ESXi, dicha tecnología el Banco tiene implementada dentro de su infraestructura de Servidores y para manejo de algunos servicios.

Nombre	Monitoreo de Procesos	Monitoreo Distribuido	Inventario	Plataforma	Base de Datos	Licencia	Mapas	Control de Acceso	IPv6
Zenoss	SI	Si	Si	Python	ZODB, MySQL, RRDtool	GPL	Si	Si	Si
JFNMS	SI	Si	Si	Python	ZODB, MySQL, RRDtool	GPL	Si	Si	Si
Pandora FMS	Solo en la versión PAGADA	Si	Si	Perl	MySQL, PostgreSQL, Oracle	GPLv2; (Enterprise edition available)	Si	Si	Si
Zabbix	SI	Si	Si	C, PHP	Oracle, MySQL, PostgreSQL, IBM DB2,	GPL	Si	Si	Si
NAGIOS	SI	Si	Si	C, PHP	Flat file, SQL, Oracle, MySQL, PostgreSQL, IBM DB2, SQLite	GPL	Si	Si	Si

LEYENDA

La presente leyenda corresponde a la descripción de cada uno de los registros en la Tabla 29: Otras Características propuestas.

Nombre del Producto

Nombre del producto que se está analizando.

IP SLA's Reports (Referencia https://supportforums.cisco.com/docs/DOC-26665)

Sirve para poder reunir información detallada de algún tipo de tráfico específico de lado a lado dentro de una red. Básicamente, un equipo que tiene configurado IP SLA corre una prueba previamente configurada hacia un equipo en algún punto remoto de la red, de este modo, al recibir la respuesta a la prueba enviada al equipo remoto, IP SLA reúne información acerca del estado del camino por el cuál pasaron los paquetes.

Grupos Lógicos

Se puede realizar agrupaciones mediante grupos, de acuerdo a ubicación, prestación de servicios o el tipo de equipo que brinda.

Predicciones

Provee líneas de tendencia de la red durante el tiempo de funcionamiento de la herramienta.

Predicción de Tendencia

El software posee algoritmos diseñados para predecir el futuro de la red mediante estadísticas.

Auto Descubrimiento

Detección Automática de todos los equipos o dispositivos que están conectados a la red.

Agente

Permite la instalación de software que trabaja como agente recolector de información de cada uno de los dispositivos que se encuentran en la red.

ESX/ESXi

Compatible con la virtualización y tecnología VMWare ESX/ESXi.

SNMP

Capacidad de recuperar e informar sobre las estadísticas sobre protocolo SNMP.

Syslog

Nos ayuda para el envío de mensajes de registro en una red.

La introducción de este daemon en el sistema nos permite tener un servidor a la espera de recibir logs de cualquier tipo de sistema, que previamente haya sido configurado, y que envíe eventos que ocurran en su funcionamiento, dependiendo del nivel de logs que le configuremos.

El software escuchará por un puerto TCP y/o UDP o ambos y escribirá en un directorio lo que el equipo afectado le envíe.

Plugins

Capacidad que tiene el NAGIOS para integrarse con programas de terceros (plugins).

Triggers/Alertas

Tiene la capacidad para detector errores o violación de las reglas de configuración de los umbrales configurados. Permitiendo alertar al administrador del error que ha ocurrido.

WebApp

Se ejecuta como una aplicación basada en web.

- Visualización: datos de la red se pueden ver en una interfaz gráfica basada en web.
- Reconocer: Los usuarios pueden interactuar con el software a través de la interfaz basada en web para reconocer las alarmas o manipular otras notificaciones.
- Reportes: informes específicos sobre datos de la red pueden ser configurados por el usuario y se ejecutan a través de la interfaz basada en web.
- Control total: todos los aspectos del producto se pueden controlar a través de la interfaz basada en la web, incluidas las tareas de mantenimiento de bajo nivel, tales como la configuración del software y las actualizaciones.

Monitoreo distribuido

Posibilidad de distribuir el balanceo de la carga para el monitoreo de la red.

Inventario

Mantiene todo inventario del hardware, software y de los dispositivos que se esté monitoreando.

Data Storage Method

Main method used to store the network data it monitors.

Principal método para guardar los datos de la red monitoreada.

Licencia

Bajo que licencia se basa el software.

Mapas

Característica gráfica para representar la red mediante el uso de mapas.

Control del Acceso

Es el nivel de seguridad que le permite al administrador tener un control de acceso por usuario, productos, dispositivos que se están monitoreando dentro de la red.

IPv6

Soporte de monitoreo IPv6.

4.4.2.2. Selección de la distribución Linux.

CentOS es estable y eficaz en el manejo de los recursos. Se ha optimizado para correr Apache, PHP, MySQL, y una variedad de otros programas necesarios para el funcionamiento de NAGIOS. Además esta distribución está aprobada por parte de los desarrolladores del proyecto NAGIOS para el correcto funcionamiento y desempeño.

La principal ventaja de CentOS es el hecho de que es Open Source y se adapta a los requerimientos que necesita el Banco de Loja como software de bajo coste de manteamiento y de licenciamiento sin costo.

NSCLIENT++

NSClient proviene de la unión de NAGIOS y Client. Este *addon* es uno de los imprescindibles en nuestro caso, está preparado para instalarse en los sistemas operativos de Windows y una vez configurado pasa a ser un servicio (programa en segundo plano) más de la lista que Windows ejecuta cuando se enciende el PC.

La finalidad de este programa es recoger la información del ordenador donde se ha instalado y enviarla a NAGIOS cada vez que este la requiera siempre y cuando se trate de un ordenador con un sistema operativo basado en Windows.

Dado que casi todos los elementos que se deberán monitorizar basan su funcionamiento en el sistema de Microsoft el NSClient++ se vuelve una herramienta indispensable para este proyecto.

NSClient++ se descarga desde su página oficial (ver bibliografía) y se instala como cualquier otro programa pensado para la plataforma de Windows. Una vez instalado se debe modificar el archivo de configuración NSC.ini ubicado en el directorio de instalación del *addon*. Este archivo es el que gobierna completamente al *addon* y es donde se pueden modificar todas las opciones permitidas. Seguidamente se muestran las premisas más importantes a modificar para su correcto funcionamiento:

- **Direcciones permitidas:** En esta premisa de declarar la IP del servidor donde se ejecuta NAGIOS para que el *addon* de permiso para la comunicación.
- **Contraseña de verificación:** Se asigna una contraseña en el addon y en el plugin check_nt, no es de vital importancia en este marco dado que solo existe un sistema de monitorización.

5. CONNOTACIONES FINALES

5.1. Discusión

Esta investigación contiene una base para la implementación de un sistema de Monitoreo de Red (NOC), para lo cual se analizó las necesidades y requerimientos que tenía el Departamento de Sistemas y específicamente el Centro de Cómputo del Banco de Loja para la detección, análisis, resolución y documentación de los problemas de red en general. También, los planes de mitigación y contingencia; y la manera en cómo se maneja los recursos para solucionar los incidentes.

Todo este proceso debe estar enmarcado dentro de las Políticas de manejo de Infraestructura IT y sobre todo deben estar acoplados a las estrategias corporativas como un medio para mejorar los servicios y aumentar su portafolio de servicios a los clientes.

Dentro de este contexto como se mencionó anteriormente primero se analizó la problemática y requerimientos, para posteriormente hacer un levantamiento de todos los procesos que se vinculaban para el manejo de requerimiento, seguidamente se propuso en el capítulo 3 una metodología para el Monitoreo de Eventos en cuanto a problema de red tomando en cuenta los actores, procedimientos a seguir y herramientas a utilizar para solucionar los problemas.

Se tomó la norma TMN (Telecomunications Management Network) fue introducida por la ITU-T en 1988 para facilitar el desarrollo de entornos de gestión distribuidos y heterogéneos (teniendo en cuenta que se posee varios equipos, diferentes arquitecturas). Esta norma proporciona una arquitectura en capas para todas las funciones de las aplicaciones de gestión, además de los protocolos de comunicación entre los elementos de red y el gestor centralizado, entre distintos gestores de red, y entre estos gestores y los operadores humanos.

Para escoger la Herramienta para la gestión de red, se realizó el análisis de las herramientas más usadas por administradores de red a nivel corporativo que cumpla con requerimientos planteados en el Capítulo 3, y decidiendo finalmente por NAGIOS como herramienta de monitoreo para el NOC del Banco de Loja por cumplir con los requisitos del punto 2.13 y el Análisis Realizado en el ANEXO 9. Entonces, al haber escogido esta herramienta se procedió a la implementación de NAGIOS en un ambiente de pruebas en donde se instaló de dos formas desde código fuente y mediante instalación de Appliance; posteriormente se procedió a la implementación de NAGIOS en un entorno de producción.

Durante toda la implementación de este proyecto se logró la estandarización del proceso de monitoreo basando toda la Gestión de Red dentro de la norma ITU 3400 y la norma TMN para la organización. Se tomó como referencias estas dos normas ya que por una parte la Norma ITU 3400 te ayudaba con las Áreas Funcionales FCAPS y la norma TMN[90]. Finalmente se involucró las áreas de la Norma ITU 3400 con las fases organizativas de la Pirámide de Administración de TMN.

Con la implementación del NMS se ha logrado potenciar la atención a los requerimientos de monitoreo, optimizar las tareas y llevar un mejor control de la gestión de red. Una vez, incorporado este proyecto al Área de Sistemas del Banco de Loja ha permitido disminuir en un 30% del tiempo dedicado para las tareas del NOC (un total mensual de 60 horas mensuales[91]) que implica: revisión del estado de todos los enlaces, revisión del estado de los recursos en los servidores, revisión de los dispositivos de red, atención de requerimientos de monitoreo, recuperación a fallas y generación de reportes manualmente (se suprimió todos los reportes manuales).

Un detalle importante a ser tomando encuenta dentro de la presente tesis se puede decir: Toda la información recopilada para la realización del NOC ha servido para la creación de un Manual de Procesos para seguir de forma paralela con la Gestión de Red del NMS, aportando para ello al NOC del Banco de Loja un manual de procesos de gestión de red, sobre la implementación de un Sistema de Gestión de Red (NAGIOS) en el servidor del NOC, un manual de administración correspondiente a la herramienta implementada.

[90] Telecomunications Management Network, «tmn.pdf».
[91] Ver Anexo 5. Reportes de Monitoreo.

5.2. Trabajos Futuros

1. Implementación de un servicio de mensajería de alertas mediante SMS en caso de no existir internet o servidor de correos.
2. Hacer uso de la funcionalidad que tiene NAGIOS para distribuir el monitoreo en servidores centralizados en cada una de las agencias con el fin de no tener sobrecargado el servidor principal y mantener estable el ancho de banda de cada una de las agencias/sucursales.
3. Desarrollo de una interfaz para monitoreo en TELÉFONOS MÓVILES ya sea para BlackBerry o iPhone.
4. Aislamiento de la base de datos, colocándola en un servidor aparte, por si existe un desperfecto en el front-end del programa se encuentre salvaguarda las configuraciones y logs de toda la red.
5. Implementar un NETFLOW para el control del ancho de banda y análisis de tráfico de la red basada en la Web y que se integre fácilmente al NAGIOS.
6. Realizar un sistema de calendarización mediante BATCH para Backups y limpieza de log ya sea diario, semanal o mensual.
7. Creación de mayor número de reportes personalizados de acuerdo a los requerimientos.

CONCLUSIONES

1. Este proyecto permitió al Banco potenciar el Área de Sistemas y específicamente al Centro de Cómputo un mecanismo efectivo para llevar de mejor manera los incidentes de infraestructura y problemas en la red.

2. Gracias a la implementación del NOC se redujo en un 30% el tiempo de solución de requerimientos de la gestión de red.

3. La administración de redes esta enfocada en todas las actividades de planeación y control, enfocadas a mantener una red eficiente y con altos niveles de disponibilidad. Dentro de estas actividades hay diferentes responsabilidades fundamentales como el monitoreo, la atención a fallas, configuración, la seguridad, entre otras.

4. La elección de la herramienta NAGIOS como NMS a utilizar se basó en un previo análisis por parte del Centro de Cómputo de acuerdo a las necesidades del departamento que se encuentra propuestas en 2.13 y el análisis de la herramienta que se encuentran descritas en 4.4.2.1 complementada con el Anexo 9. Así mismo las funcionalidades generales y específicas descritas en el punto 2.14.1 y 2.14.2 que se explican a detalle en los puntos 4.5.2.1.3 y 4.5.2.1.4 respectivamente.

5. La implementación de NAGIOS se encuentra actualmente monitoreando cada uno de los elementos descritos en el Capítulo 2 y en el Capítulo 3; toda la información recogida se encuentra almacenándose en una base de datos para poder tener un reporte histórico del funcionamiento y el estado de salud de la red. Gracias a estos datos es posible desplegar en forma automática gráficos, eventos, estadísticas de cada uno de los elementos de la red. Se han generado además procedimientos que permitan compartir datos con otras áreas dentro del Banco y además, la posibilidad de utilizar dichos datos tomar decisiones; como por ejemplo, el Área de Proyectos puede pedir información de los recursos e infraestructura existente para abrir una nueva agencia.

6. El NOC es toda una metodología que cubre las necesidades para la administración de red y brinda los lineamientos para el manejo de infraestructura, recurso humano y requerimientos.

7. En los puntos anteriores se describió una propuesta de administración para redes de datos. La propuesta se basó en la recomendación de la ITU-T, el modelo TMN y en el modelo OSI-NM de ISO. Se presentó una propuesta global que enfatiza en todos los aspectos relacionados a la buena operación de una red, como lo son el control sobre los sucesos en la red, la visualización de los tipos

de tráfico, la detección y atención oportuna de problemas, aspectos de seguridad, etc.

8. La metodología presentada se basa en un modelo con tareas bien definidas y complementarias. Esta modularidad permite su mejor entendimiento y facilita su implementación y actualización.

RECOMENDACIONES

1. Disponer de dos servidores distribuidos de la siguiente manera:
   i. Uno para el NMS, en este caso el NAGIOS.
   ii. Y otro, para el almacenamiento de la Base de Datos.
2. Tener configurado un RAID 1 en los equipos que se dispongan tanto para el NMS, como para la Base de Datos de Almacenamiento de configuraciones e información histórica (mencionado en el punto anterior (1)); por si existe algún desperfecto en el disco pueda existir contingencia.
3. Mediante los lineamientos del Capítulo 3. Establecer formalmente el equipo de MONITOREO.
4. Que el servidor del NAGIOS cuente con todos los requisitos de hardware necesario para el correcto funcionamiento.
5. Establecer como software autorizado la instalación del agente de NSClient++ y el servicio de SNMP en todas las máquinas y servidores del banco.
6. Que se añada las responsabilidades descritas en el Capítulo II al rol de cada uno de los integrantes del equipo del Centro de Cómputo para la administración del NOC.
7. Crear una política para que el agente NSClient++ y el servicio de SNMP sean instalados como software necesarios en la configuración inicial de un equipo y/o servidor, o en su defecto en aquellos equipos que sea posible de instalar el servicio o el software del NSClient++
8. Seguir el procedimiento descrito en el presente proyecto de tesis.
9. Crear una base de datos de conocimiento para el archivo de requerimientos.
10. En caso de existir saturación en el envío de mensajes y/o alertar por parte del NMS, implementar NMS Locales para el monitoreo.
11. De acuerdo al crecimiento de la red, ir aumentando las capacidad en cuando a hardware del Servidor de Monitoreo.
12. Crear alertas esenciales y definir correctamente las alertas mediante correo electrónico, ya que podemos saturar este servidor por eventos innecesarios.
13. Tener un servidor de contingencia en caso de algún problema o falla en el servidor principal del NAGIOS.
14. Una recomendación para automatización del ingreso y registro de los requerimientos en la plantilla que se detalla en el ANEXO 5

15. Plantilla para el Ingreso de Requerimientos. se ingresen como Workflow dentro del SharePoint.

BIBLIOGRAFÍA

Abadi, M. (Marzo de 2012). *[NAGIOS] - O que RSZDT significa?* Obtenido de http://marcosabadi.blogspot.com: http://marcosabadi.blogspot.com/2012/03/nagios-o-que-rszdt-significa.html

Abeck , S., & Farrel, A. (2008). *Network Management: Know It All.* Morgan Kaufmann.

Agudelo, O. (2011). *Arquitecturas.* Obtenido de Arcesio.net: http://www.arcesio.net/administracion/arquitecturas.ppt

Agudelo, O. (s.f.). *Osi-NM.* Recuperado el 9 de Diciembre de 2011, de Arcesio.net: http://www.arcesio.net/osinm/osinm.html

Agudelo, O. (s.f.). *Otros enfoques para clasificar las funciones de administración.* Recuperado el 11 de Noviembre de 2012, de Arcesio.net: http://www.arcesio.net/osinm/otrasfunciones.html#piramide

Agudelo, S. (s.f.). *OSI.* Recuperado el 1 de Febrero de 2012, de Arcesio.net: http://www.arcesio.net/arquitecturas/osi.ppt

Alejandro, M. (2009). *Redes y Telecomunicaciones.* UNDAC.

ALTAMIRANO, C. V. (2005). *Un Modelo funcional para el Centro de operación de RedUNAM (NOCUNAM).* México.

Anónimo. (25 de Julio de 2011). *Importar Virtual Appliance Astaro v8 a ESX.* Obtenido de http://www.eiweb.es/vmware/importar-virtual-appliance-astaro-v8-a-esx/

Anónimo. (24 de mayo de 2011). *SCRIBD.* Recuperado el 2011, de http://es.scribd.com/doc/56183621/admoredest: http://es.scribd.com/doc/56183621/admoredest

Arias Figueroa, D. (1999). *Herramientas de Gestión basada en Web.* Recuperado el 2012, de http://postgrado.info.unlp.edu.ar/Carreras/Magisters/Redes_de_Datos/Tesis/Arias_Figueroa.pdf

Arias Figueroa, D. (1999). *Herramientas de Gestión basada en Web.* Obtenido de http://postgrado.info.unlp.edu.ar/Carreras/Magisters/Redes_de_Datos/Tesis/Arias_Figueroa.pdf

Armas, C., & Vicente, C. (s.f.). *SlideShare*. Recuperado el 6 de Marzo de 2012, de Analisis de rendimiento de red: http://www.slideshare.net/Comdat4/analisis-de-rendimiento-de-red.

Badger, M. (2008). *Zenoss Core Network and System Monitoring: A step-by-step guide to configuring, using, and adapting this free Open Source network monitoring system.* Packt Publishing.

Barba A, B. (2008). *Gestión de red.* Edicions UPC .

Barba Martí, A. (2005). *Gestión de red.* Colombia: Edicions UPC.

Barrientos Arias, I., & Beites de Pedraza, J. (14 de Marzo de 2006). NAGIOS Un sistema de monitorización de servicios de red. *NAGIOS Un sistema de monitorización de servicios de red*.

Bastidas, J. (s.f.). *FCAPS.* Recuperado el 10 de Marzo de 2012, de www.scribd.com: http://www.slideshare.net/JhenniferBastidas/fcaps-7220464

Bert, W., Presuhn, R., & Harrington, D. (s.f.). *An Architecture for Describing SNMP Management Frameworks.* Recuperado el 17 de Enero de 2012, de An Architecture for Describing SNMP Management Frameworks: http://tools.ietf.org/html/rfc2571#page-4

Casares Stacey, D. (2001). *GESTION DE RED.* Obtenido de ftp://ftp.puce.edu.ec/Facultades/Ingenieria/Sistemas/Network%20news/Gestion%20de%20Redes/GESTION%20DE%20RED.ppt

Case, J. D., Fedor, M., Schoffstall, M. L., & Davin, J. R. (Mayo de 1990). *A Simple Network Management Protocol (SNMP).* Obtenido de http://www.ietf.org/rfc/rfc1157.txt

Castañeda Espindola, D. (s.f.). *FUNDACIÓN UNIVERSITA RIA KONRAD LORENZ.* Recuperado el 8 de Febrero de 2012, de TELETRABAJO: http://www.konradlorenz.edu.co/images/stories/articulos/TELETRABAJO.pdf

Chan, K. H., Baker, F., & Smith, A. (s.f.). *Management Information Base for the Differentiated Services Architecture.* Recuperado el 17 de Enero de 2012, de http://www.ietf.org/html/rfc3289: http://tools.ietf.org/html/rfc3289

Davin, J., Case, J. D., Fedor, M., & Schoffstall, M. L. (s.f.). *Simple Network Management Protocol (SNMP).* Recuperado el 17 de Enero de 2012, de www.ietf.org: http://tools.ietf.org/html/rfc1157

Desconocido. (2008-03-28). *MIB MANAGER INFORMATION BASE.*

Díaz, E. J. (26 de 11 de 2008). Análisis y Desarrollo de Conceptos Fundamentales de Redes Autónomas. *Análisis y Desarrollo de Conceptos Fundamentales de Redes Autónomas*. Madrid, Madrid, España.

Díaz, E., & y García, J. (2008). Análisis y Desarrollo de Conceptos Fundamentales de Redes Autónomas. Madrid.

Ding, J. (2009). *Advances in Network Management.* NW: Auerbach Publications.

Domínguez, J. A. (s.f.). *Introducción a la Gestión de Redes.* Recuperado el 9 de Junio de 2012, de www.lacnic.net: http://lacnic.net/documentos/lacnicx/Intro_Gestion_Redes.pdf.

Dpto. de Ingeniería Electrónica, d. T. (2005). *Tema 5. GESTIÓN DE REDES DE TELECOMUNICACIONES.* Jaén: Universidad de Jaén.

Electrónica, D. d. (1997). Gestión de Redes de Comunicaciones.

Finseth, C. (s.f.). *An Access Control Protocol, Sometimes Called TACACS.* Recuperado el 29 de Agosto de 2012, de An Access Control Protocol, Sometimes Called TACACS: http://tools.ietf.org/html/rfc1492

García Díaz, E. J. (2008). Análisis y Desarrollo de Conceptos Fundamentales de . Madrid: Departamento de Ingeniería Informática .

Gomez Santos, A. (s.f.). *«Gestion De Redes».* Recuperado el 23 de Enero de 2012, de Slideshare: http://www.slideshare.net/ing.adolfo/gestion-de-redes

Gutiérrez Porset, D. (Noviembre de 2010). Gestión de redes, SNMP RMON. *Redes y Servicios II*. ETSI Bilbao/DET/Telemática/5º Ing. Telecomunicación. Obtenido de Gestión de redes,.

Gutiérrez Porset, D. (1 de Abril de 2011). *Gestión de redes, SNMP y RMON.* Recuperado el 15 de Noviembre de 2012, de SLIDESHARE: http://www.slideshare.net/danitxu/snmp-rmon

Gutiérrez Porset, Dani. (s.f.). *Gestión de redes, SNMP y RMON.* Recuperado el 1 de Abril de 2011, de SLIDESHARE: http://www.slideshare.net/danitxu/snmp-rmon

Heinz-Gerd Hegering, Sebastian, A., & Bernhard , N. (2001). *Integrated Management of Networked Systems.* San Francisco, USA: Morgan Kauffman Publisher.

Hernández, E. (s.f.). *SNMP vs CMIP.* Recuperado el 5 de Noviembre de 2012, de ldc.usb.ve/~emilio/Portafolio/Exposiciones/SNMP-vs-CMIP.ppt

Hernando Velasco, R. (7 de Julio de 2002). *Gestión de redes.* Obtenido de http://www.rhernando.net/modules/tutorials/doc/redes/Gredes.html.

Hervey, A., & Armas, C. (s.f.). Introducción a la Gestión de Redes.

Irastorza, J. A. (21 de 02 de 2008). *Gestión de Red.* Obtenido de Modelo de arquitectura ISO/OSI.

Irastorza, J. A. (2008). Grupo de Ingeniería Telemática. UC.

Jose, J. (2004). *revista FMI.* Quito: flacso.

Kemp, J. (s.f.). Harramientas MLM. *Harramientas MLM(41)*. www.linux-magazine.es. doi:020-023

Kirch, O., & Dawson, T. (2000). *Guía de Administración de Redes con Linux.* O'Reilly & Associates.

Kirch, O., & Dawson, T. (2000). Guía de Administración de Redes con Linux. O'Reilly & Associates.

Kirch, O., & Dawson, T. (2002). *Guía de Administración de Redes con Linux.* O'Reilly (printed version) (c) 2000 O'Reilly & Associates. Obtenido de http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/: http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/

Kovács, K. (s.f.). *Zabbix vs Nagios comparison.* Obtenido de http://kkovacs.eu/zabbix-vs-nagios

Kurose, J., & Ross, K. (2002). *Computer Networking: A Top Down Approach Featuring the Internet.* Addison-Wesley.

Kurose, J., & Ross, K. (2002). *Computer Networking: A Top Down Approach Featuring the Internet.* Addison-Wesley.

Lerena Urrea, S., Villanueva Jiménez, D., & González González, J. (s.f.). *Manual del Administrador.* Obtenido de Pandorafms: pandorafms.com/downloads/doc/PandoraFMS_Manual_3.2_ES.pdf

Levi, D. B., Stewart, B., & Meyer, P. (s.f.). *SNMP Applications.* Recuperado el 17 de Enero de 2012, de http://tools.ietf.org/html/rfc2573

Luque, J. (2003). *Gestión de Redes de Comunicación.* Sevilla: Departamento de Tecnología Electrónica-Facultad de Informatica-Universidad de Sevilla.

Luque, J. (2003). *Gestión de Redes de Comunicación.* Sevilla.

Marín Moreno, W. (s.f.). *Modelo OSI.* Obtenido de Modelo OSI: http://www.ie.itcr.ac.cr/marin/mpc/redes/Modelo_osi_tcp_ip%28oficial%29.pdf

Martin, R. (s.f.). *Administración de Redes - Protocolos de la familia Internet.* Recuperado el 14 de Julio de 2013, de Protocolos de la familia Internet (TCP/IP): http://personales.upv.es/rmartin/TcpIp/cap04s07.html

Mikker, F. (15 de Jun de 2012). *Agents Home.* Obtenido de op5: http://www.op5.com/agents/nsclient/

Mikker, F. (15 de Jun de 2012). *NSClient++.* Obtenido de op5: http://www.nsclient.org/nscp/

Miranda Orozco, V. R., Enrique, M., & Conor, G. (5 de Febrero de 2012). *Universidad de San Carlos de Guatemala.* Obtenido de Configuracion Protcolo SNMP: http://carlos8rg.files.wordpress.com/2008/08/onto_snmp.pdf

Muria, D., Moreno, K., Barrios, G., Solórzano, B., Perazzo, D., Baptista, A., & Suarez, D. (s.f.). *NAGIOS.* Recuperado el 12 de Marzo de 2012, de SCRIBD: http://es.scribd.com/doc/21931635/NAGIOS

NESTOR. (2006). *Redes de Computadoras II.* Recuperado el Mayo de 2011, de Administracion de Redes: http://www.ciudadranelagh.com.ar/unlz/unocursada/Redes%20de%20Computadoras/ClaseAdmRedes_unlz.pdf

Orozco, P. (22 de Febrero de 2012). *Gestión De Red.* Recuperado el 15 de Marzo de 2012, de SLIDESHARE: http://www.slideshare.net/pakus/gestion-de-red

Ortiz Olague, M. (s.f.). *Formato de documentacion ieee 830.* Recuperado el 20 de Marzo de 2012, de http://www.slideshare.net: http://www.slideshare.net/MauricioOrtizOlague/formato-de-documentacion-ieee-830

PARRA CARABALLO, A., & MENDIETA BUENO, S. (2005). *Universidad Tecnológica de Bolívar.* Recuperado el Mayo de 2011, de Facultad de Ingeniería Eléctrica y

Electrónica Cartagena De Indias D.T: http://biblioteca.unitecnologica.edu.co/notas/2005-12-12/0032134.pdf

Román, A., & Utard, M. (14 de Julio de 2002). Obtenido de http://www.fiuba6662.com.ar/6662/papers/SNMP.pdf.

Romero, M. d. (s.f.). *sac-gestionderedes.* Recuperado el 1 de Febrero de 2012, de http://www.dte.us.es: http://www.dte.us.es/personal/mcromero/docs/sac/sac-gestionderedes.pdf

Rose, M. T., & McCloghrie, K. (s.f.). *Structure and identification of management information for TCP/IP-based internets.* Recuperado el 17 de Enero de 2012, de http:/www.ietf.org: http://tools.ietf.org/html/rfc1155

Sepúlveda, M. (13 de Julio de 2009). *Herramientas de Administacion de Redes: Las cinco capas funcionales de la administración de redes (FCAPS).* Obtenido de Integrared Herramientas de Administacion de Redes: http://integrared.blogspot.com/2009/07/las-cinco-capas-funcionales-de-la.html

Software, A. (s.f.). *Aranda SERVICE DESK - Datasheet.* Recuperado el 22 de Septiembre de 2012, de Aranda SERVICE DESK: http://www.slideshare.net/ArandaSoftware/aranda-service-desk

SOSA-SOSA, D. V. (2008). MIB (Manager Information Base). DF, DF, Mexico.

Terplan, K. (1995). *Client/Server Management Datacom.* Buchverlag Bergheim: Prentice-Hall.

Untiveros, S. (Junio de 2004). *Metodologías para Administrar Redes.* Recuperado el 12 de Julio de 2012, de www.aprendaredes.com: http://www.aprendaredes.com/downloads/Como_Administrar_Redes.pdf

Vicente, C. (2004). *Servicios y Aplicaciones de un Centro de Operaciones de Red.* Obtenido de https://nsrc.org/workshops/2004/CEDIA2/material/NOC.pdf

Vicente, C. (s.f.). Análisis de Rendimiento - Servicios de Red. Oregon.

ANEXOS

1. ANEXO 1

1.1. Normas y Estándares Utilizados[92]

Las normas y estándares aplicables a la gestión de redes se muestran a continuación:

Tabla 30: *Normas y estándares aplicables a la Gestión OSI*

GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS (Gestión OSI)	Recomendación
Marco y Arquitectura de la Gestión de Sistemas:	
Marco de la Gestión OSI – Arquitectura de Gestión OSI	ITU-T X.700
Visión General de la Gestión de Sistemas OSI	ITU-T X.701
Servicio y Protocolo de Comunicación de Gestión:	
Servicio Común de Información de Gestión (CMIS)	ITU-T X.710
Protocolo Común de Información de Gestión (CMIP)	ITU-T X.711
Estructura de la Información de Gestión:	
Modelo de Información de Gestión	ITU-T X.720
Definición de la Información de Gestión	ITU-T X.721
Directrices para la Definición de Objetos Gestionados (GDMO)	ITU-T X.722
Información de Gestión Genérica	ITU-T X.723
Directrices para la implantación de Proformas relacionadas con la Gestión OSI	ITU-T X.724
Modelo General de Relación	ITU-T X.725
Funciones de Gestión de Sistemas:	
Función de Gestión de Objetos	ITU-T X.730
Función de Gestión de Estados	ITU-T X.731
Atributos para la Representación de Relaciones	ITU-T X.732
Función Señaladora de Alarmas	ITU-T X.733
Función de Gestión de Informes de Evento	ITU-T X.734
Función de Control de Archivos de Registro Cronológico	ITU-T X.735
Función Señaladora de Alarmas de Seguridad	ITU-T X.736
Categorías de Prueba de Confianza y de Diagnóstico	ITU-T X.737
Función de Sumario	ITU-T X.738
Objetos Métricos y Atributos	ITU-T X.739

[92] Víctor Hugo Hinojosa Jaramillo, Luis Vicente Ortega Pilco, y Luis Alberto Madruñero Padilla., «Sistema de gestión de red» (Universidad Técnica del Norte, 2011), http://repositorio.utn.edu.ec/bitstream/123456789/577/1/TesisFinal.doc; VICTOR HINOJOSA, LUIS MADRUÑERO, y LUIS ORTEGA, «Sistema de gestión de red», Thesis, junio 6, 2011, http://repositorio.utn.edu.ec/handle/123456789/577.

Función de Pista de Auditoría de Seguridad	ITU-T X.740
Objetos y Atributos para el Control de Acceso	ITU-T X.741
Función de Cómputo de Utilización para la Contabilidad	ITU-T X.742
Función de Gestión del Tiempo	ITU-T X.743
Función de Gestión del Soporte Lógico	ITU-T X.744
Función de Gestión de Prueba	ITU-T X.745
Función de Planificación	ITU-T X.746
Función de Monitorización del Tiempo de Respuesta	ITU-T X.748

Tabla 31: *Normas y estándares aplicables a la Gestión TMN*[93]

GESTIÓN DE LAS TELECOMUNICACIONES (Modelo TMN)	**Recomendación**
Arquitectura del Modelo TMN:	
Visión de Conjunto de las Recomendaciones Relativas a la Red de Gestión de las Telecomunicaciones	ITU-T M.3000
Principios para una Red de Gestión de las Telecomunicaciones	ITU-T M.3010
Consideraciones sobre una Red de Gestión de las Telecomunicaciones	ITU-T M.3013
Metodología de Especificación de Interfaces TMN:	
Metodología de especificación de interfaz de la Red de Gestión de las Telecomunicaciones.	ITU-T M.3020
Modelos y Catálogo de Información de Gestión:	
Modelo Genérico de Información de Red	ITU-T M.3100
Catálogo de Información de Gestión de la Red de Gestión de las Telecomunicaciones	ITU-T M.3180
Servicios de Gestión:	
Introducción a los Servicios de Gestión de las Telecomunicaciones	ITU-T M.3200
Requisitos de la Interfaz F de la Red de Gestión de las Telecomunicaciones	ITU-T M.3300
Funciones de Gestión:	
Funciones de Gestión de la Red de Gestión de las Telecomunicaciones	ITU-T M.3400
Protocolos de Comunicación:	
Perfiles de Protocolo de capa inferior para las Interfaces Q3 y X	ITU-T Q.811
Perfiles de Protocolo de capa superior para las Interfaces Q3 y X	ITU-T Q.812

[93] Víctor Hugo Hinojosa Jaramillo, Luis Vicente Ortega Pilco, y Luis Alberto Madruñero Padilla., «Sistema de gestión de red»; HINOJOSA, MADRUÑERO, y ORTEGA, «Sistema de gestión de red».

Servicios de Gestión de Sistemas y Mensajes de Gestión:	
Descripción de la etapa 2 y la etapa 3 para la interfaz Q3: Vigilancia de Alarmas	ITU-T Q.821
Descripción de la etapa 1, la etapa 2 y de la etapa 3 para la interfaz Q3: Gestión de la calidad de funcionamiento	ITU-T Q.822

Tabla 32: *Normas y estándares aplicables a la Gestión Internet*[94]

GESTIÓN INTERNET (Modelo SNMP)	Recomendación
Recomendaciones del IAB (Internet Activities Board) para el desarrollo de estándares de gestión de red para Internet.	RFC 1052
Base de Información de gestión para Redes basadas en TCP/IP	RFC 1066
Estructura e Identificación de la Información de Gestión para Redes basadas en TCP/IP	RFC 1155
Protocolo SNMP	RFC 1157
Definición concisa de MIB	RFC 1212
Base de la Información de Gestión para Redes basadas en TCP/IP: MIB-II	RFC 1213
Definición de Traps para uso en SNMP	RFC 1215
Estructura de información de gestión SNMPv2	RFC 1902
Nomenclatura en SNMPv2	RFC 1903
Reglas de conformidad para SNMPv2	RFC 1904
Operaciones del protocolo SNMPv2	RFC 1905
Mapeados de transporte SNMPv2	RFC 1906
MIB para SNMPv2	RFC 1907
Compatibilidad entre las versiones 1 y 2 de SNMP	RFC 1908
Arquitectura de las plataformas SNMP	RFC 2271
Procesamiento y envío de mensajes en SNMP	RFC 2272
Aplicaciones SNMPv3	RFC 2273
Modelo de seguridad basado orientada al usuario en SNMPv3	RFC 2274
Modelo de control de acceso SNMP	RFC 2275

[94] Víctor Hugo Hinojosa Jaramillo, Luis Vicente Ortega Pilco, y Luis Alberto Madruñero Padilla., «Sistema de gestión de red»; HINOJOSA, MADRUÑERO, y ORTEGA, «Sistema de gestión de red».

2. ANEXO 2

2.1. Reportes De Monitoreo

Dentro del análisis de servicios externos, el Banco tiene tercerizado mediante contrato con **Internetvista**[95] que es una compañía que encarga de supervisar los servidores externos de una organización. A continuación se presenta un informe enviado diariamente por esta compañía mediante correo electrónico:

InternetVista®

Estimado/Estimada -----,

Le adjuntamos el informe de rendimiento referente a todas sus aplicaciones controladas durante el periodo de 02/01/2012 00:00:00 a 08/01/2012 23:59:59.

aplicación	*% up*	*tiempo en error*	*activo*	*frec.*
Frontal (Apache) Pagina Web	100%	0 segundo	sí	5 min.
iis Server IESS	100%	0 segundo	sí	5 min.
imap Server Correo	100%	0 segundo	sí	5 min.
Página Web	100%	0 segundo	sí	5 min.
ping Server Pagina Web	100%	0 segundo	sí	5 min.
pop Server Info	100%	0 segundo	sí	5 min.
Página Web Segura	100%	0 segundo	sí	5 min.
smtp Server Correo Autenticado	100%	0 segundo	sí	5 min.
smtp Server Info	100%	0 segundo	sí	5 min.
smtp Server SMTP	100%	0 segundo	sí	5 min.
webmail	100%	0 segundo	sí	5 min.

aplicación Frontal (Apache) Pagina Web: (*.*.*.* en el puerto 8080)

% up	100%
% down	0%
tiempo en error	0 segundo
tiempo sin error	7 días
tiempo medio de respuesta	0,181 segundo
tiempo de respuesta más rápido	0,093 segundo
tiempo de respuesta más lento	3,196 segundos
número de verificaciones	2016
número de éxitos	2016
número de errores	0
fecha de inicio	02/01/2012 00:00:00
fecha de fin	08/01/2012 23:59:59

top

aplicación iis Server IESS: (*.***.***.*** en el puerto 80)**

% up	100%

[95] «internetVista® monitoring - Uptime is money», accedido febrero 29, 2012, http://www.internetvista.com/.

% down	0%
tiempo en error	0 segundo
tiempo sin error	7 días
tiempo medio de respuesta	0,181 segundo
tiempo de respuesta más rápido	0,093 segundo
tiempo de respuesta más lento	3,195 segundos
número de verificaciones	2019
número de éxitos	2019
número de errores	0
fecha de inicio	02/01/2012 00:00:00
fecha de fin	08/01/2012 23:59:59

top

aplicación imap Server Correo: (*.***.***.*** en el puerto 143)**

% up	100%
% down	0%
tiempo en error	0 segundo
tiempo sin error	7 días
tiempo medio de respuesta	0,910 segundo
tiempo de respuesta más rápido	0,476 segundo
tiempo de respuesta más lento	4,574 segundos
número de verificaciones	2017
número de éxitos	2017
número de errores	0
fecha de inicio	02/01/2012 00:00:00
fecha de fin	08/01/2012 23:59:59

top

aplicación Pagina Web: (http://www.bancodeloja.fin.ec)

% up	100%
% down	0%
tiempo en error	0 segundo
tiempo sin error	7 días
tiempo medio de respuesta	0,481 segundo
tiempo de respuesta más rápido	0,199 segundo
tiempo de respuesta más lento	3,623 segundos
número de verificaciones	2016
número de éxitos	2016
número de errores	0
fecha de inicio	02/01/2012 00:00:00
fecha de fin	08/01/2012 23:59:59

top

aplicación ping Server Pagina Web: (ping *.***.***.***)**

% up	100%
% down	0%
tiempo en error	0 segundo
tiempo sin error	7 días
tiempo medio de respuesta	0,176 segundo
tiempo de respuesta más rápido	0,093 segundo
tiempo de respuesta más lento	0,282 segundo
número de verificaciones	2017
número de éxitos	2017
número de errores	0

fecha de inicio	02/01/2012 00:00:00
fecha de fin	08/01/2012 23:59:59

top

aplicación pop Server Info: (*.***.***.*** en el puerto 110)**

% up	100%
% down	0%
tiempo en error	0 segundo
tiempo sin error	7 días
tiempo medio de respuesta	1,454 segundo
tiempo de respuesta más rápido	0,753 segundo
tiempo de respuesta más lento	7,195 segundos
número de verificaciones	2016
número de éxitos	2016
número de errores	0
fecha de inicio	02/01/2012 00:00:00
fecha de fin	08/01/2012 23:59:59

top

aplicación Página Web Segura: (https://www.bancodeloja.fin.ec)

% up	100%
% down	0%
tiempo en error	0 segundo
tiempo sin error	7 días
tiempo medio de respuesta	1,056 segundo
tiempo de respuesta más rápido	0,488 segundo
tiempo de respuesta más lento	5,422 segundos
número de verificaciones	2016
número de éxitos	2016
número de errores	0
fecha de inicio	02/01/2012 00:00:00
fecha de fin	08/01/2012 23:59:59

top

aplicación smtp Server Correo Autenticado: (*.***.***.*** en el puerto 587)**

% up	100%
% down	0%
tiempo en error	0 segundo
tiempo sin error	7 días
tiempo medio de respuesta	0,926 segundo
tiempo de respuesta más rápido	0,439 segundo
tiempo de respuesta más lento	25,673 segundos
número de verificaciones	2016
número de éxitos	2016
número de errores	0
fecha de inicio	02/01/2012 00:00:00
fecha de fin	08/01/2012 23:59:59

top

aplicación smtp Server Info: (*.***.***.*** en el puerto 25)**

% up	100%
% down	0%
tiempo en error	0 segundo
tiempo sin error	7 días
tiempo medio de respuesta	0,804 segundo

tiempo de respuesta más rápido	0,438 segundo
tiempo de respuesta más lento	13,633 segundos
número de verificaciones	2018
número de éxitos	2018
número de errores	0
fecha de inicio	02/01/2012 00:00:00
fecha de fin	08/01/2012 23:59:59

top

aplicación smtp Server SMTP: (*.***.***.*** en el puerto 25)**

% up	100%
% down	0%
tiempo en error	0 segundo
tiempo sin error	7 días
tiempo medio de respuesta	0,964 segundo
tiempo de respuesta más rápido	0,367 segundo
tiempo de respuesta más lento	10,529 segundos
número de verificaciones	2017
número de éxitos	2017
número de errores	0
fecha de inicio	02/01/2012 00:00:00
fecha de fin	08/01/2012 23:59:59

top

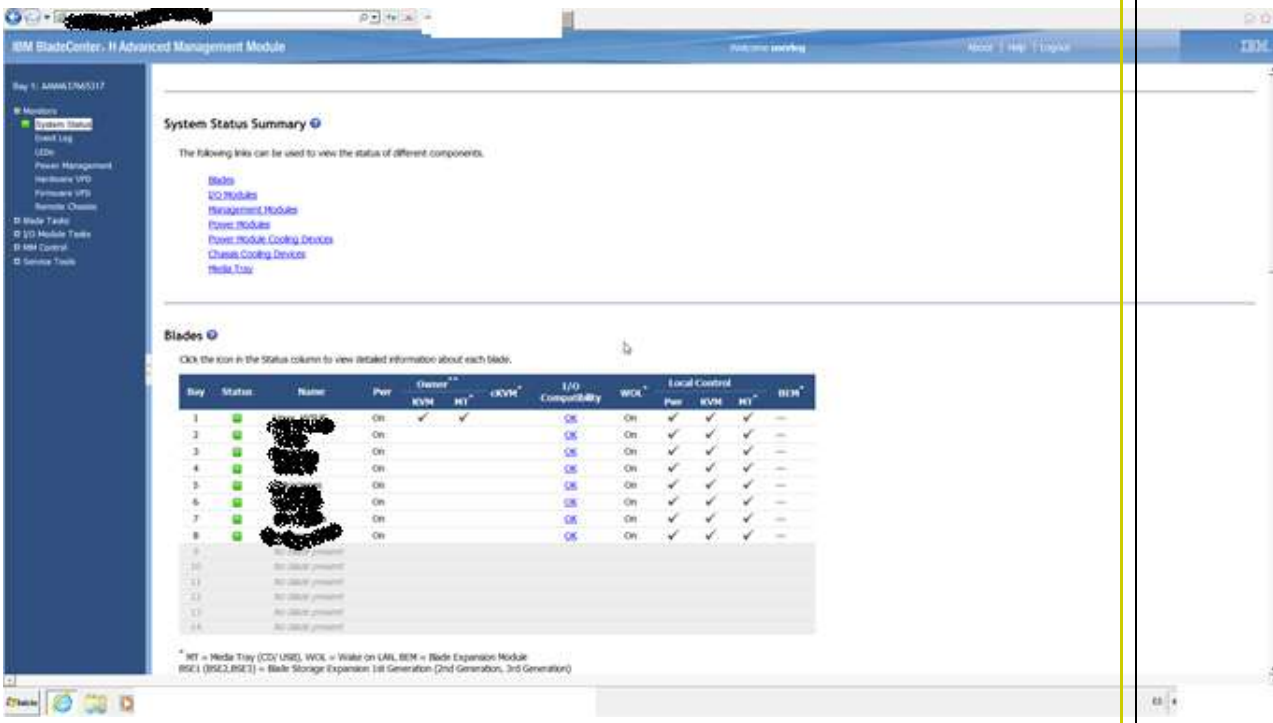
aplicación webmail: (https://webmail.bancodeloja.fin.ec)

% up	100%
% down	0%
tiempo en error	0 segundo
tiempo sin error	7 días
tiempo medio de respuesta	1,013 segundo
tiempo de respuesta más rápido	0,426 segundo
tiempo de respuesta más lento	4,431 segundos
número de verificaciones	2016
número de éxitos	2016
número de errores	0
fecha de inicio	02/01/2012 00:00:00
fecha de fin	08/01/2012 23:59:59

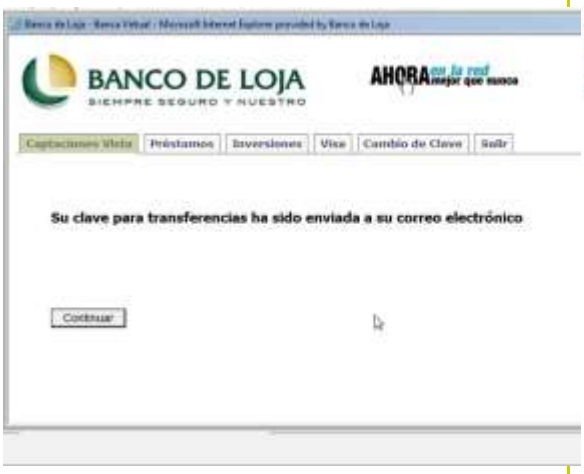
top

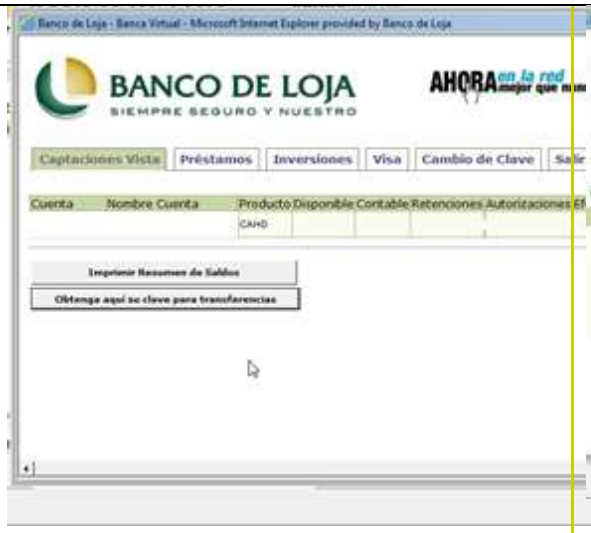
Ilustración 41: Reporte enviado por INTERNETVISTA.

Para el monitoreo interno de los servidores se realiza un correo electrónico dos veces al día distribuidos de la siguiente manera: uno en la mañana a las 10h00 y otro a las 20h00. La información contenida en dicho correo es la que se detallada a continuación:

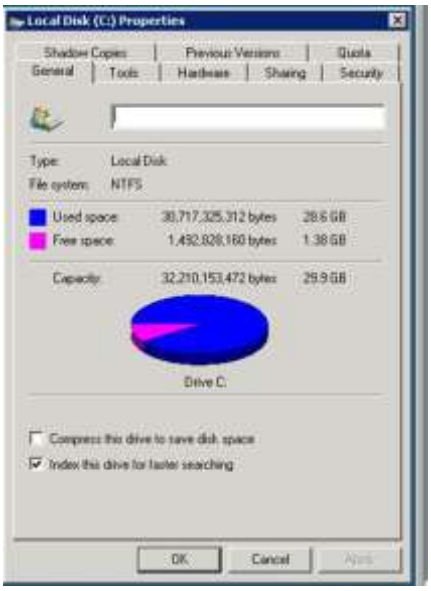


2- Pruebas de acceso a la banca electrónica, en la cual no se detecta ningún error:

Prueba de solicitud de clave para transferencias:	Correo de confirmación de clave:
	
Prueba consulta en Banca electrónica:	

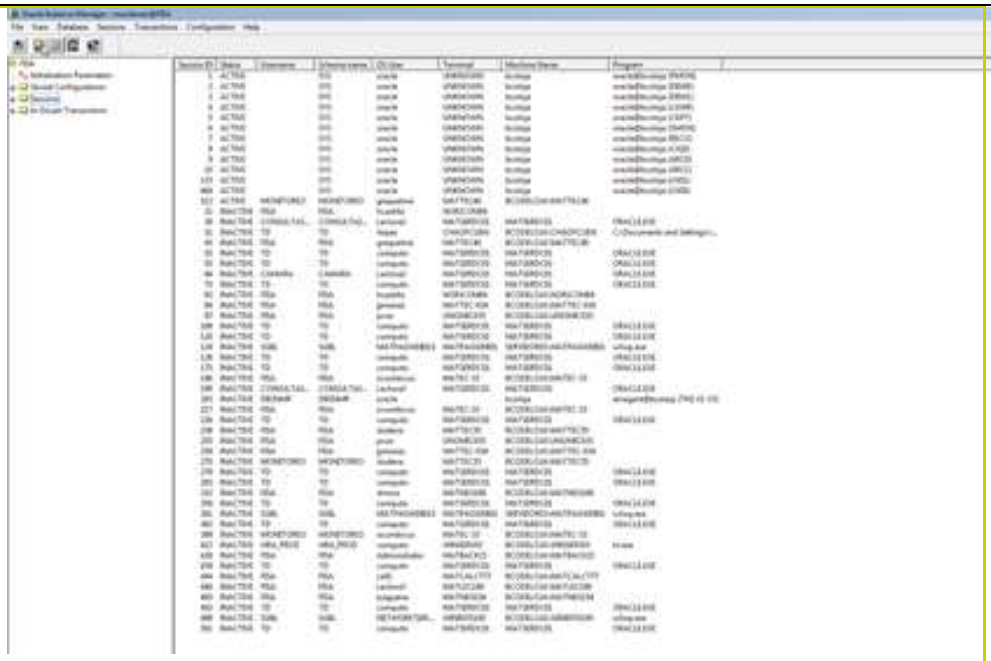


Disco Server XXXX



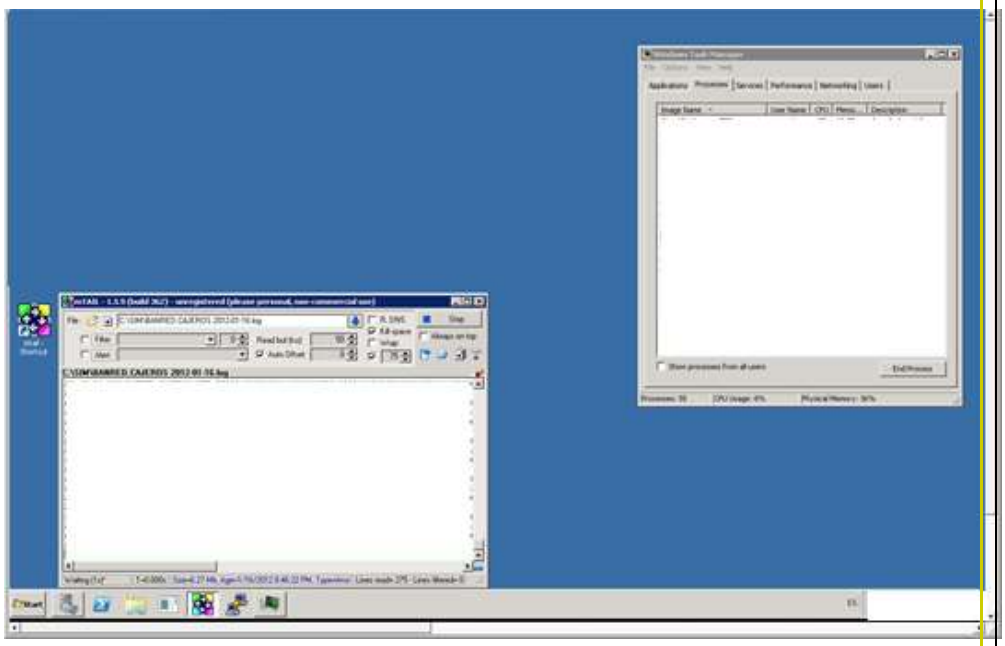
3- Sesiones activas en el ORACLE INSTANCE, esto varia constantemente, pero se mantienen un numero de sesiones normal[96]:

[96] El número de sesiones normal oscila de 50 a 500 sesiones de usuarios.

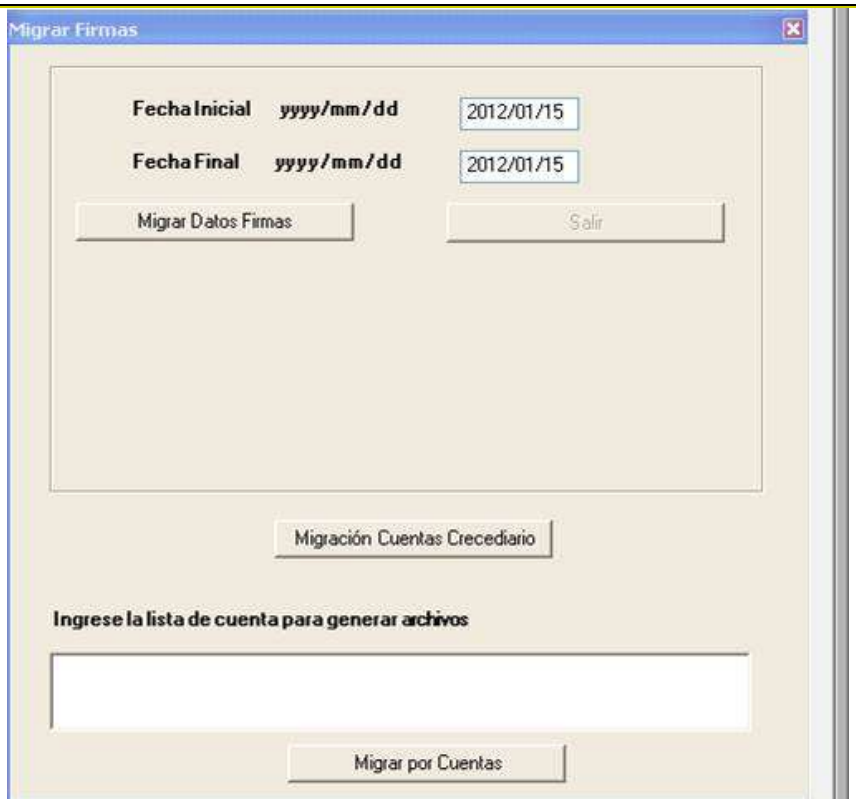


4- Transacciones Cajeros, e instancias levantadas del SIM:

Transacciones Cajeros:	Instancias levantadas SIM:



5- Se verifica usuario del Sistema de Gestión de Base de Datos, se verifica que no esté bloqueado, ejecutando cada 5 minutos el software de carga de firmas:



6- Espacio en disco del servidor principal

Cómputo

```
Filesystem             size   used  avail capacity  Mounted on
/dev/dsk/c0t0d0s0      5.9G   3.0G   2.8G    52%    /
/devices                 0K     0K     0K     0%    /devices
ctfs                     0K     0K     0K     0%    /system/contract
proc                     0K     0K     0K     0%    /proc
mnttab                   0K     0K     0K     0%    /etc/mnttab
swap                    14G   1.2M    14G     1%    /etc/svc/volatile
objfs                    0K     0K     0K     0%    /system/object
/dev/dsk/c0t0d0s5      5.9G   3.4G   2.4G    59%    /usr
/platform/SUNW,Sun-Fire-T200/lib/libc_psr/libc_psr_hwcap1.so.1
                       5.9G   3.0G   2.8G    52%    /platform/sun4v/lib/libc_psr.
so.1
/platform/SUNW,Sun-Fire-T200/lib/sparcv9/libc_psr/libc_psr_hwcap1.so.1
                       5.9G   3.0G   2.8G    52%    /platform/sun4v/lib/sparcv9/l
ibc_psr.so.1
fd                       0K     0K     0K     0%    /dev/fd
swap                    14G   112K    14G     1%    /tmp
swap                    14G    48K    14G     1%    /var/run
/dev/dsk/c2t0d1s0      118G   105G    12G    90%    /datos02
/dev/dsk/c2t0d0s0      118G    68G    49G    59%    /datos01
/dev/dsk/c2t0d8s0      274G   132G   139G    49%    /datos06
/dev/dsk/c2t0d2s0      118G    88G    29G    76%    /datos03
/dev/dsk/c2t0d4s0      7.9G   6.4G   1.4G    83%    /base
/dev/dsk/c2t0d3s0      118G    43G    74G    37%    /datos04
/dev/dsk/c2t0d7s0      274G    61G   210G    23%    /datos05
/dev/dsk/c2t0d6s0       51G    52M    51G     1%    /respaldo
/dev/dsk/c2t0d9s0      492G   133G   355G    28%    /datos07
/dev/dsk/c2t0d5s0      4.9G   4.2G   676M    87%    /oracle
/dev/dsk/c2t0d10s0     332G    64M   328G     1%    /datos08
/dev/dsk/c0t0d0s6       47G    31G    16G    66%    /export/home
/export/home/grequelme
                        47G    31G    16G    66%    /home/grequelme
```

Ilustración 42: Reporte enviado diariamente.[97]

[97] Este reporte se lo realiza de forma manual y 2 veces al día.

Adicional a esto, se posee una licencia de PRTG para lo que es monitoreo de enlaces y de conexión con las agencias como se detalla en la Ilustración siguiente:

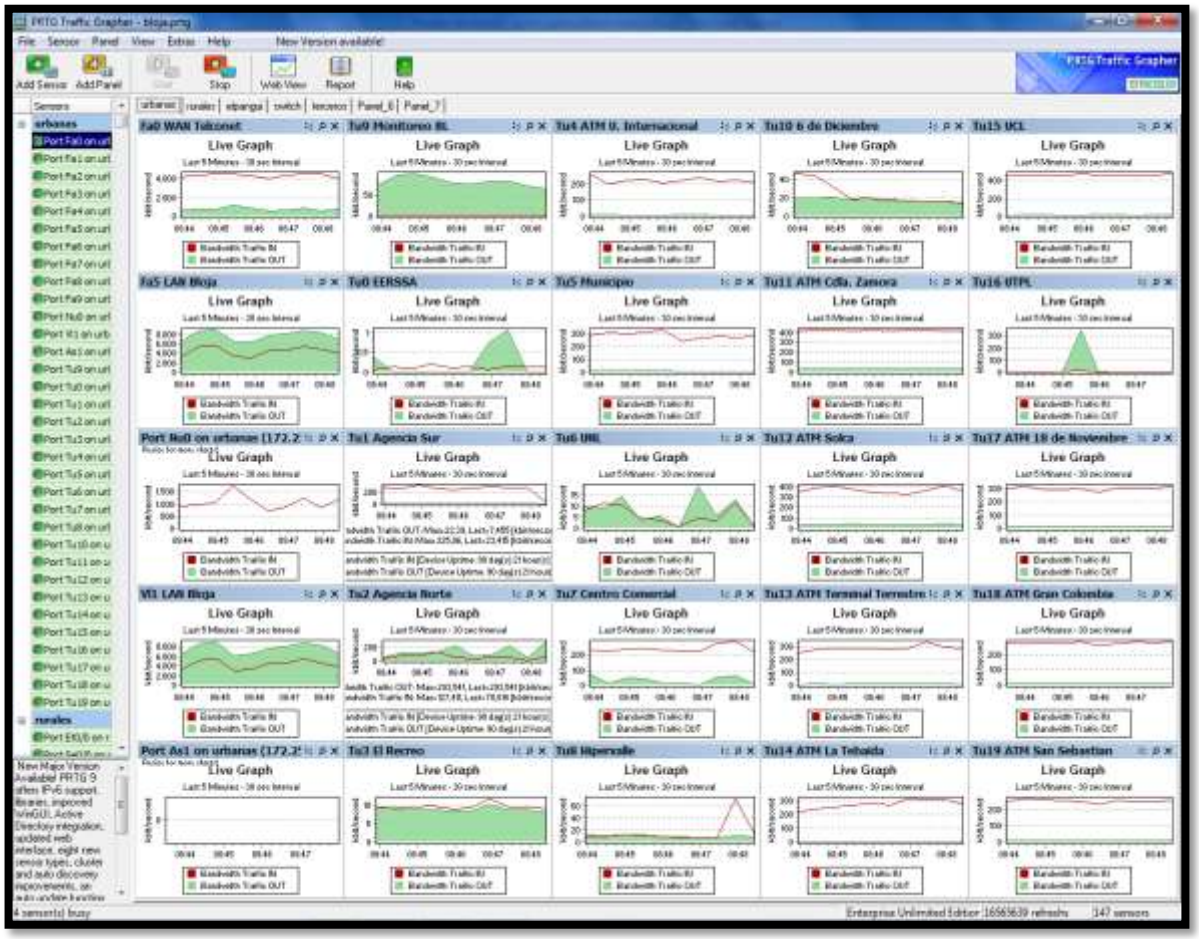


Ilustración 43: PRTG Instalado para monitoreo de BW.

3. ANEXO 3

3.1. Configurar SNMP en Gnu\Linux

Si seguimos el tutorial de instalación de NAGIOS, ya tenemos instalado SNMP-Net. Para configurar el servidor NAGIOS y que sea monitorizado con SNMP debemos seguir este procedimiento. Este procedimiento se sigue para instalarlo en otro GNU\Linux que queramos monitorizar.

Los paquetes a instalar son

```
sudo aptitude install snmp snmpd
```

Esto nos instala el agente snmpd que recoge datos del equipo GNU\Linux y los envía al gestor cuando este lo pida o envía traps asíncronas y notificaciones. También instala las aplicaciones como snmpwalk, etc. que sirven para usar snmp o testearlo.

```
Lo primero es configurar /etc/default/snmpd,
$ vi /etc/default/snmpd

# This file controls the activity of snmpd and snmptrapd

# MIB directories. /usr/share/snmp/mibs is the default, but
# including it here avoids some strange problems.
# Directorio donde están los mibs
export MIBDIRS=/usr/share/snmp/mibs

# snmpd control (yes means start daemon).
# Yes. para que se inicie snmpd
SNMPDRUN=yes

# snmpd options (use syslog, close stdin/out/err).
# Opciones del servidor, debeis añadir la interfaz donde queréis que snmp este activo.
# Si dejáis solo 127.0.0.1 no enviaréis recibiréis nada más que en localhost, no por la red.
# Pongo aquí la ip 172.*.*.*, puesto que el host Server lo tengo añadido a
# NAGIOS con esta IP. Si en NAGIOS añades hosts GNU\Linux con sus IPs y queréis
# monitorizarlos con snmp debéis poner la IP aquí (en cada host, en este archivo)

#SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid 127.0.0.1'
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid 172.*.*.* 127.0.0.1'

# snmptrapd control (yes means start daemon). As of net-snmp version
# 5.0, master agentx support must be enabled in snmpd before snmptrapd
# can be run. See snmpd.conf(5) for how to do this.
# Para el control de traps.
TRAPDRUN=yes
```

```
# snmptrapd options (use syslog).
TRAPDOPTS='-Lsd -p /var/run/snmptrapd.pid'

# create symlink on Debian legacy location to official RFC path
SNMPDCOMPAT=yes
```

Por otro lado configuramos el archivo /etc/snmp/snmpd.conf que es donde está el grueso de la configuración.

```
####
# First, map the community name (COMMUNITY) into a security name

# Aquí ponemos la configuración del nombre de seguridad que vamos a usar
# (una especie de usuario) y la contraseña que tiene (community)
# com2sec vale para cualquier dirección ip IPv4 de origen "default" que es de cualquier
# origen. Para IPv6 podemos poner com2sec6. Son ACLs o listas de control de acceso.

# sec.name source  community
#com2sec paranoid default  public

# El nombre de seguridad readonly con contraseña "mipasswordpublica"
# se usará para datos de lectura que enviará el agente (snmpd) al gestor.
# Se permite coger datos desde cualquier origen (default)
com2sec readonly default  mipasswordpublica

# El nombre de seguridad readwrite con contraseña "mipasswordprivada"
# se usará para datos de lectura que enviará el agente (snmpd) al gestor
# y escritura para modificar las variables snmp del dispositivo gestionado
# (gnu\linux en este caso) desde cualquier origen (default)
com2sec readwrite default  mipasswordprivada

# Voy a crear una ACL.
# El nombre de seguridad redlocal permite, desde la red 172.*.*.*/24 y con
# la contraseña mipasswordredlocal, recoger datos de este dispositivo.
com2sec redlocal 172.*.*.*/24 mipasswordredlocal

# También para localhost.
com2sec lhostacc 127.0.0.1/32 mipasswordlocal

####
# Second, map the security names into group names:

# Los nombres de seguridad (usuarios, nombres de ACL, o como queramos
# llamarlos) se asignan a un grupo.

# readonly lo hemos asignado a MyROGroup para las versiones
# del protocolo snmp 1 y v2c y usm
```

```
# Lo mismo hacemos con el nombre de seguridad readwrite
# Obviamente, podemos cambiar los nombres por los nuestros propios
# pero yo los he dejado por defecto.
# Añado también redlocal al grupo de solo lectura.
# Añado lhostacc al grupo de lectura escritura

#  sec.model sec.name
group MyROSystem v1 paranoid
group MyROSystem v2c paranoid
group MyROSystem usm paranoid
group MyROGroup v1  readonly
group MyROGroup v2c readonly
group MyROGroup usm readonly
group MyRWGroup v1  readwrite
group MyRWGroup v2c readwrite
group MyRWGroup usm readwrite

group MyROGroup v1  redlocal
group MyROGroup v2c redlocal
group MyROGroup usm redlocal

group MyRWGroup v1  lhostacc
group MyRWGroup v2c lhostacc
group MyRWGroup usm lhostacc

####
# Third, create a view for us to let the groups have rights to:

# Aquí se crean vistas para después permitir verlas o no a los
# grupos. Las vistas son partes de los arboles MIBS. Por ejemplo
# La vista all es todo el árbol a partir de.1 (.iso)
# La vista system solo recorre la parte del árbol a partir de.system.*

#  incl/excl subtree    mask
view all included .1    80
view system included .1.3.6.1.2.1.1
#view system included .iso.org.dod.internet.mgmt.mib-2.system

####
# Finally, grant the 2 groups access to the 1 view with different
# write permissions:

# Por último, le damos permisos a los grupos que creamos.
# MyROSystem tiene acceso con cualquier sec.model (version protocolo)y
# puede leer la vista system (solo el árbol system) pero no escribir ni notificar.
# A este grupo pertenece el "usuario/ACL" paranoid que estaba comentado así que no se aplica.
```

```
# MyROGroup puede leer la vista all, es decir, obtener todos los datos pero no
# puede escribir ni notificar.

# MyRWGroup puede leer, escribir y notificar en todo el árbol con la vista all
# y con cualquier versión del protocolo (sec.model)

#  context sec.model sec.level match read write notif
access MyROSystem "" any noauth exact system none none
access MyROGroup "" any noauth exact all none none
access MyRWGroup "" any noauth exact all all all

# -----------------------------------------------------------------------------

###############################################################################
# System contact information
#
# Información del sistema

syslocation Sistema Nagios con nombre de host linux.bancodeloja.fin.ec
syscontact Administrador NOC

# También vamos a monitorizar los procesos mysql y postfix como ejemplo.
# El nombre de los procesos debemos ponerlo exacto a como saldría
# con ps -e (no es igual mysql que mysqld
# Esto nos dice si los procesos están corriendo en la máquina.
# Podemos monitorizar los que queramos incluso el número que tiene que haber
# corriendo como mínimo o como máximo.

# Mysql
proc mysqld

# Postfix
proc master
proc qmgr
proc pickup
...
###############################################################################
# Subagent control
#
# The agent can support subagents using a number of extension mechanisms.
# From the 4.2.1 release, AgentX support is being compiled in by default.
# To use this mechanism, simply uncomment the following directive.
#
master agentx
```

Ahora podemos probar si recibimos datos con snmpwalk y testear si funciona la configuración

```
$ snmpwalk -v 1 -c mipasswordredlocal 172.*.*.* prName
UCD-SNMP-MIB::prNames.1 = STRING: mysqld
UCD-SNMP-MIB::prNames.2 = STRING: master
UCD-SNMP-MIB::prNames.3 = STRING: qmgr
UCD-SNMP-MIB::prNames.4 = STRING: pickup
```

Vemos como los procesos que hemos configurado se muestran. Hemos dicho a snmpwalk que use la version 1 del protocolo, la community "mipasswordredlocal" que recoja datos de 172.*.*.* y que recoja los nombres de procesos. También podemos decirle que recoja los datos del sistema

```
$ snmpwalk -v 2c -c mipasswordredlocal 172.*.*.* system
SNMPv2-MIB::sysDescr.0 = STRING: Linux linux 2.6.32-24-server #41-Linux SMP Thu Aug 19 02:47:08
UTC 2010 x86_64
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-TC::linux
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (130841) 0:21:48.41
SNMPv2-MIB::sysContact.0 = STRING: Administrador NOC
SNMPv2-MIB::sysName.0 = STRING: Linux
SNMPv2-MIB::sysLocation.0 = STRING: Sistema Nagios con nombre de host linux
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (1) 0:00:00.01
...
```

Si no le decimos nada, ni tabla de procesos o system o system,sysUptime... nos saldrá todos los datos que recoge del host. Algún dato más.

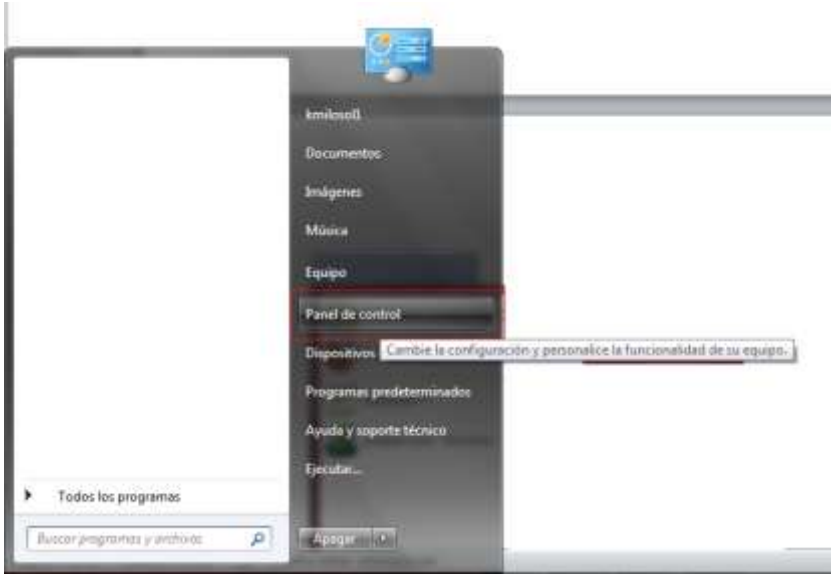
```
$ snmpwalk -v 2c -c mipasswordlocal localhost sysUptime
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (138707) 0:23:07.07

$ snmpwalk -v 1 -c mipasswordlocal localhost interfaces
IF-MIB::ifNumber.0 = INTEGER: 2
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifDescr.1 = STRING: lo
IF-MIB::ifDescr.2 = STRING: eth2
IF-MIB::ifType.1 = INTEGER: softwareLoopback(24)
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
```

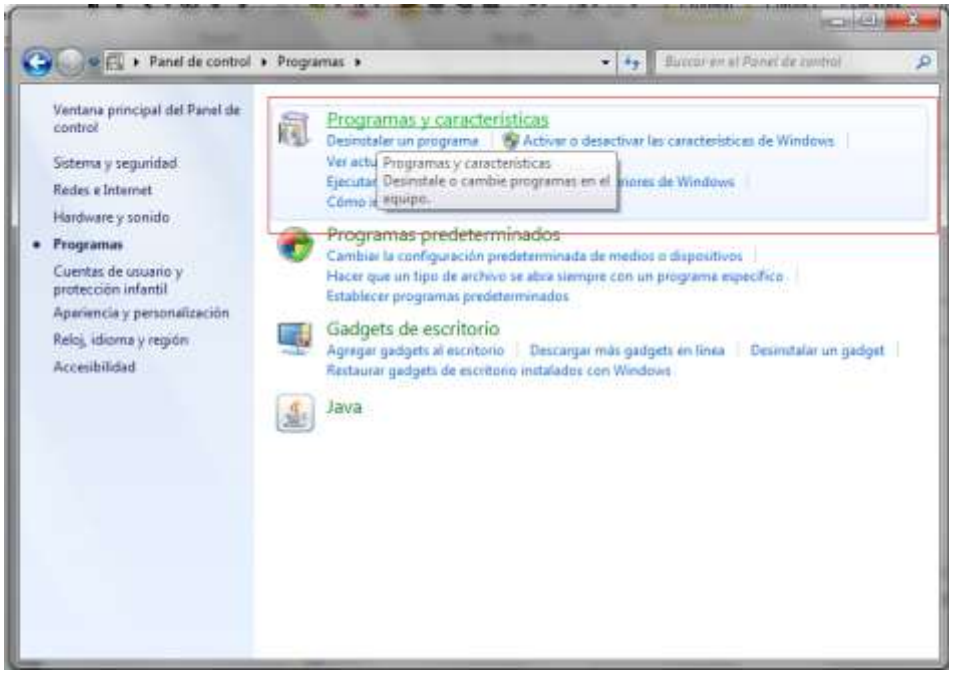
CONFIGURAR SNMP EN WINDOWS 7

Para configurar SNMP en Windows 7 (es algo similar en XP) debemos añadir una característica o servicio que no trae activa por defecto.

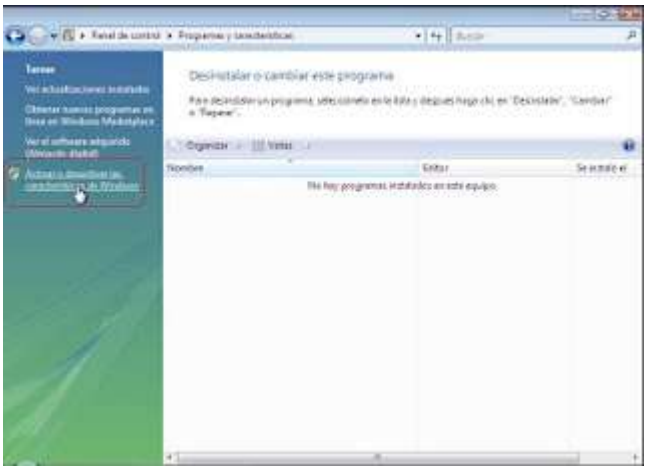
Damos clic en INICIO luego nos dirigimos a PANEL DE CONTROL y damos nuevamente clic.



Cuando estemos dentro de la ventana panel de control, damos clic en Programas y características:

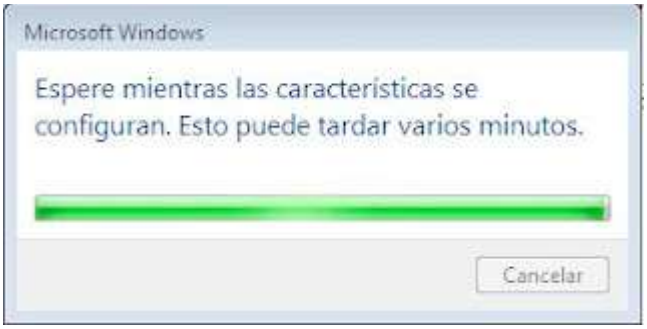


Luego de hacer clic en programas y características el sistema nos mostrara un asistente que nos permite desinstalar o cambiar programas, dentro de este debemos escoger la opción activar o desactivar las características de Windows:

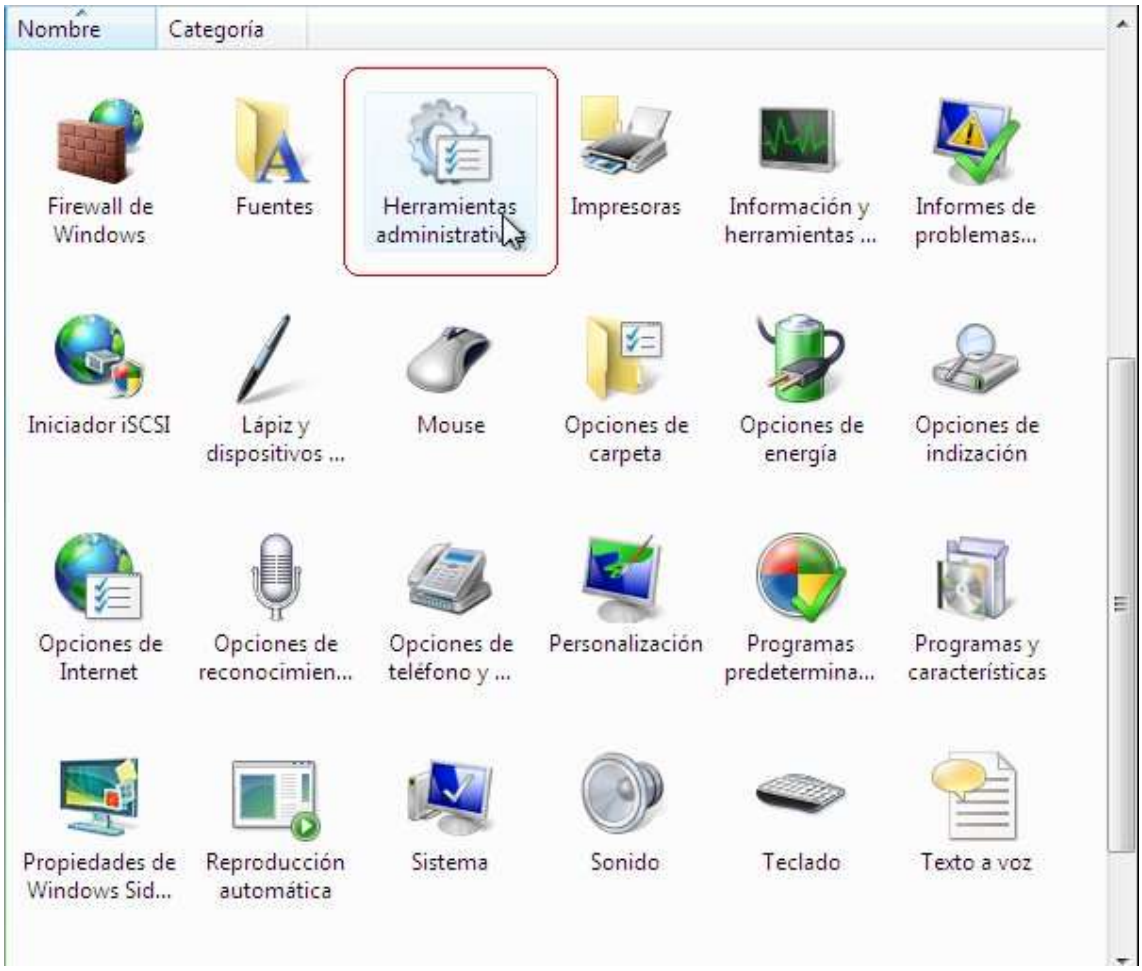


Luego de dar clic en la opción activar o desactivar las características de Windows, debemos buscar la característica o programa que queremos instalar, en nuestro caso será SNMP:

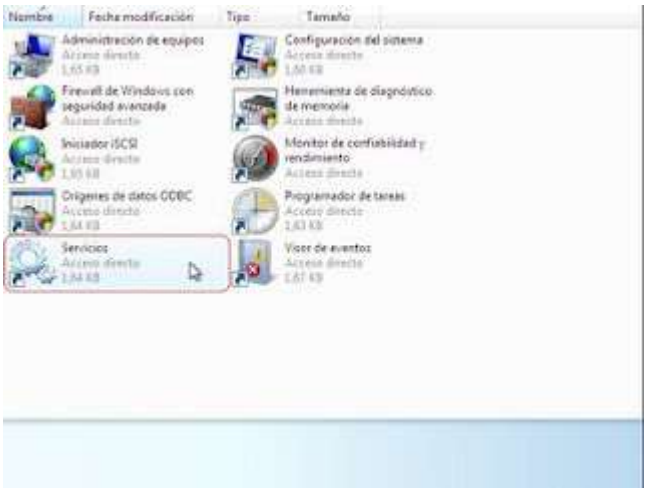
Inmediatamente hacemos clic en aceptar en el pantallazo, anterior el asistente comenzara a copiar los archivos necesarios para que el programa funcione correctamente:



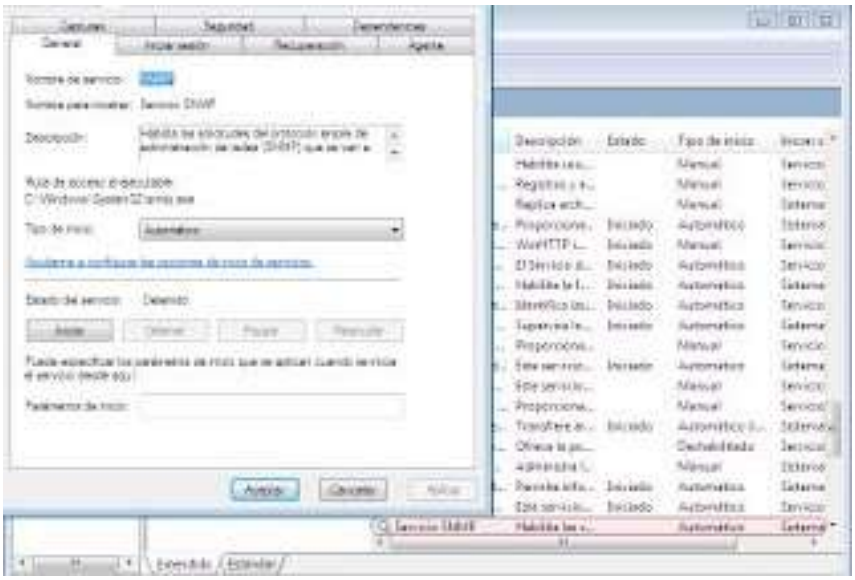
En este paso vamos a configurar el agente SNMP en nuestro equipo para que el servidor pueda monitorearlo, abrimos el panel de control y seleccionamos Herramientas administrativas:



cuando estemos dentro de la ventana de configuración de las herramientas administrativas de Windows vista, hacemos clic en servicios:



En la siguiente pantalla aparecen todos los servicios que tiene instalado el sistema operativo, debemos buscar el servicio que vamos a configurar que es SNMP y damos doble clic sobre el:

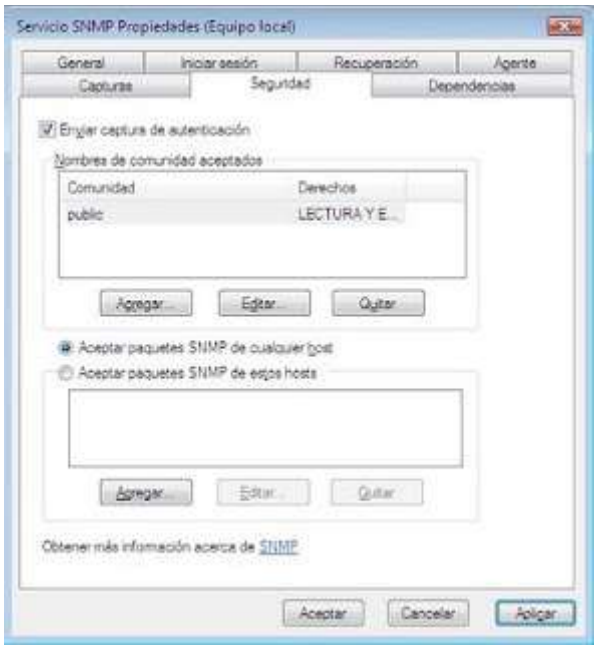


En la pantalla propiedades de SNMP, seleccionamos la pestaña capturas y agregamos el Nombre de la comunidad "public" y el destino de la captura que será la IP del servidor "192.168.0.11[98]".Dar clic en aceptar:

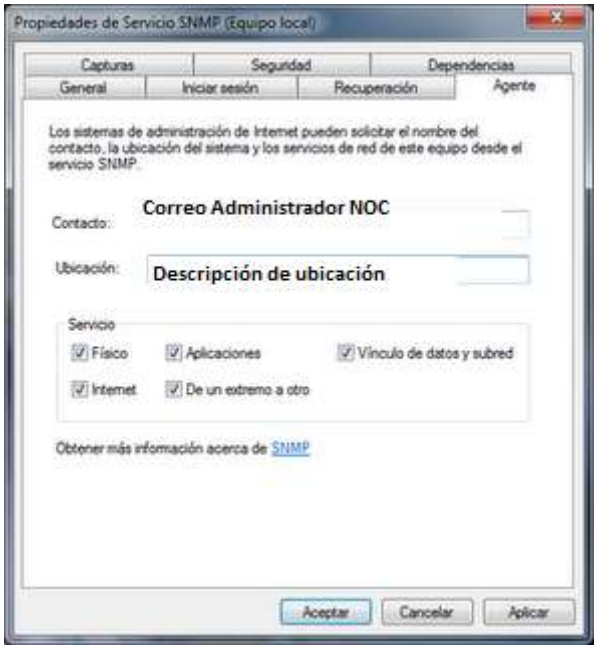
Luego damos clic en la pestaña seguridad, en el apartado nombre de comunidad aceptados damos clic en agregar y añadimos el nombre de nuestra comunidad "public".

[98] Se utilizó la red 192.168.0.* para lo que el entorno de pruebas y el entono de producción la red 172.25.*.*

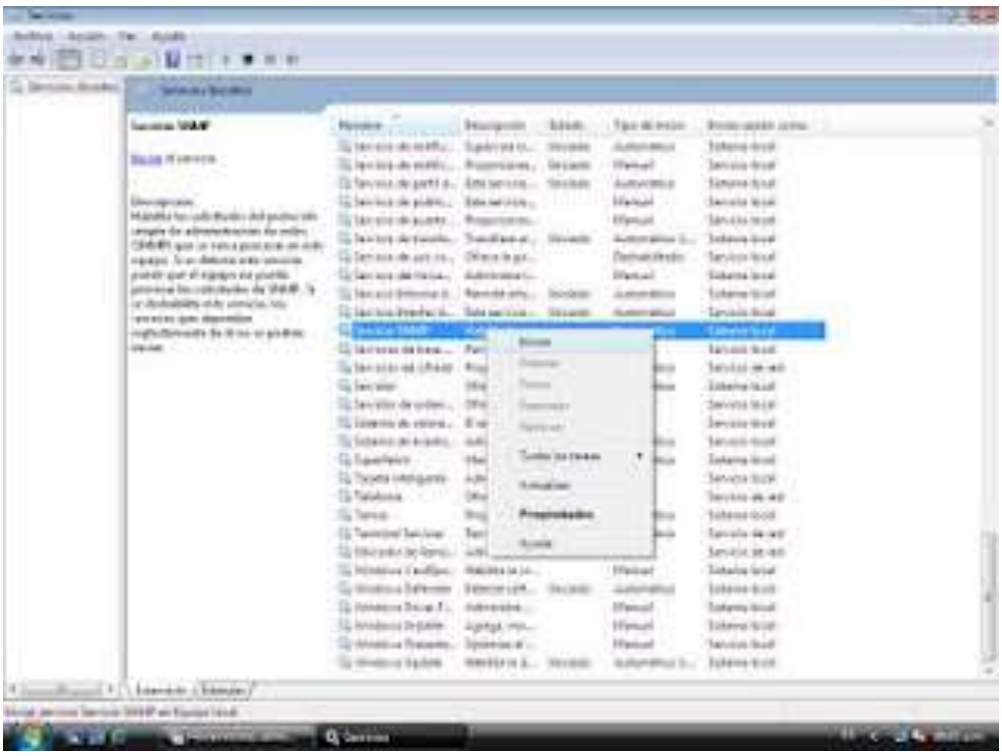
Luego activamos la opción Aceptar paquetes SNMP de cualquier host.



Configuramos el agente con la información de lo que queremos monitorizar, la localización y el contacto.



Por ultimo iniciamos el servicio SNMP, nos vamos a panel de control, herramientas administrativas y hacemos clic en servicios, luego buscamos el servicio de SNMP damos clic derecho sobre éste y activamos la opción iniciar:



Desde el servidor NAGIOS podemos probar con snmpwalk si vemos a nuestro agente en Windows. Esto se puede usar para todos los Windows.

```
$ snmpwalk -v 2c -c mipasswordredlocal NOMBRE_EQUIPO_WINDOWS system
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: Intel64 Family 6 Model 37 Stepping 2 AT/AT
COMPATIBLE - Software: Windows Version 6.1 (Build 7600 Multiprocessor Free)
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.311.1.1.3.1.1
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (27311) 0:04:33.11
SNMPv2-MIB::sysContact.0 = STRING: monitor@bancodeloja.fin.ec
SNMPv2-MIB::sysName.0 = STRING: EQUIPO_WINDOWS
SNMPv2-MIB::sysLocation.0 = STRING: Escritorio Windows con nombre de host EQUIPO_WINDOWS
SNMPv2-MIB::sysServices.0 = INTEGER: 79
```

CONFIGURACIÓN DEL AGENTE SNMP EN LINUX/DEBIAN

Primero instalaremos los paquetes del servidor snmp.

#apt-get install snmpd

Ahora uniremos el equipo debían a una comunidad existente.

Vamos al archivo

nano /etc/snmp/snmpd.conf

Y buscamos las siguientes líneas

sec.name source community

com2sec notConfigUser default public

Public es el nombre de la comunidad al que va pertenecer nuestro equipo

Y agregamos debajo la siguiente línea.
com2sec public 192.168.*.*/24 N@giosBL

Nota: las letras “o”, sustitúyalas por “ceros”.

Donde *public* es el nombre del grupo al que pertenecemos, 192.168.*.*/24 es el identificador de la red que va a ser monitoreada por el gestor snmp y N@giosBL es la clave de acceso.

Después buscamos la siguiente línea
sec.model sec.name

Y agregamos debajo las siguientes líneas.

group mygroup v1 public
group mygroup v2c private

Y agregamos debajo la siguiente línea, que sirve para definirle a la comunidad public los permisos de solo lectura.

rocomumunity public

En este punto el archivo debería lucir de este modo:

```
  GNU nano 2.0.2                          Fichero: /etc/snmp/snmpd.conf

# For more information, read the FAQ as well as the snmpd.conf(5)
# manual page.

####
# First, map the community name (COMMUNITY) into a security name
# (local and mynetwork, depending on where the request is coming
# from):

#       sec.name  source          community
com2sec mynetwork 192.168.0.0/24  public
com2sec paranoid  default         public
#com2sec readonly  default         public
#com2sec readwrite default         private

####
# Second, map the security names into group names:

#               sec.model  sec.name
group mynetwork v1
group mynetwork v2
group mynetwork usm
recommunity                public
group MyROSystem v1        paranoid
group MyROSystem v2c       paranoid
group MyROSystem usm       paranoid
group MyROGroup v1         readonly
group MyROGroup v2c        readonly
group MyROGroup usm        readonly
group MyRWGroup v1         readwrite
group MyRWGroup v2c        readwrite
group MyRWGroup usm        readwrite
```

Por ultimo iniciamos el demonio snmpd, para que nuestra configuración tenga efecto.

#/etc/init.d/snmpd start

Nota: Si queremos comprobar que todo haya salido bien, podemos descargar la herramienta scli.

#apt-get install scli

Después de que hayamos instalado la herramienta scli, procedemos a ejecutar el siguiente el comando.

scli localhost

Y nos debe aparecer algo similar a esto.

100-scli versión 0.2.12 (c) 2001-2002 juergen Schoenwaelder

100-scli trying SNMPv2c ... good

(localhost) scli >

Y escribimos la palabra monitor

Y nos aparecerán unos datos básicos.

CONFIGURAR EL AGENTE SNMP EN UN SWITCH Y EN UN ROUTER

Switch>

Switch>enable

Entramos al dispositivo a modo configuración global

Switch#configure terminal

Switch (config) #snmp-server enable traps

Habilitamos las interrupciones para alertar al SNMP sobre la situación en la red.

Switch (config) #snmp-server community public ro

Especificamos la comunidad y damos permisos, ya sean de lectura y escritura (rw) o de solo lectura (ro)

Switch (config) # snmp-server enable traps

Habilitamos las interrupciones

Los mismos pasos hacemos en un ROUTER.

Router>

Router> enable

Entramos como configuracion global

Router# configure terminal

Router (config) # snmp-server community public ro

Especificamos la comunidad y damos permisos, ya sean de lectura y escritura (rw) o de solo lectura (ro).

Router (config) # snmp-server enable traps

Habilitamos las interrupciones.

4. ANEXO 4

4.1. Ingreso de Casos a Aranda

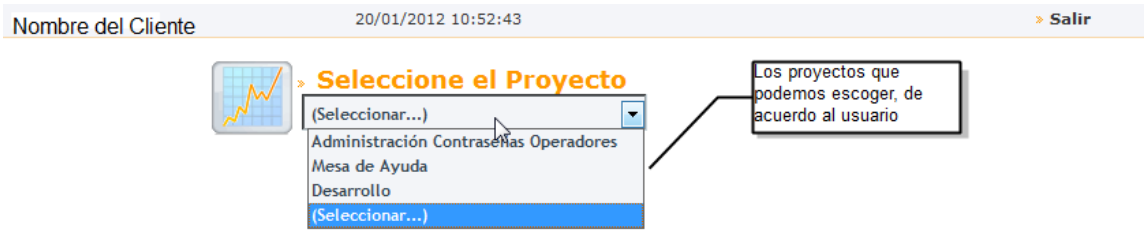
A continuación detallo como se registra los casos en el sistema ARANDA por parte del USUARIO o por parte de HELPDESK:

PRIMERA PARTE

1. El usuario ingresa al sistema http://aranda/usdk

2. Ubica su nombre y su contraseña

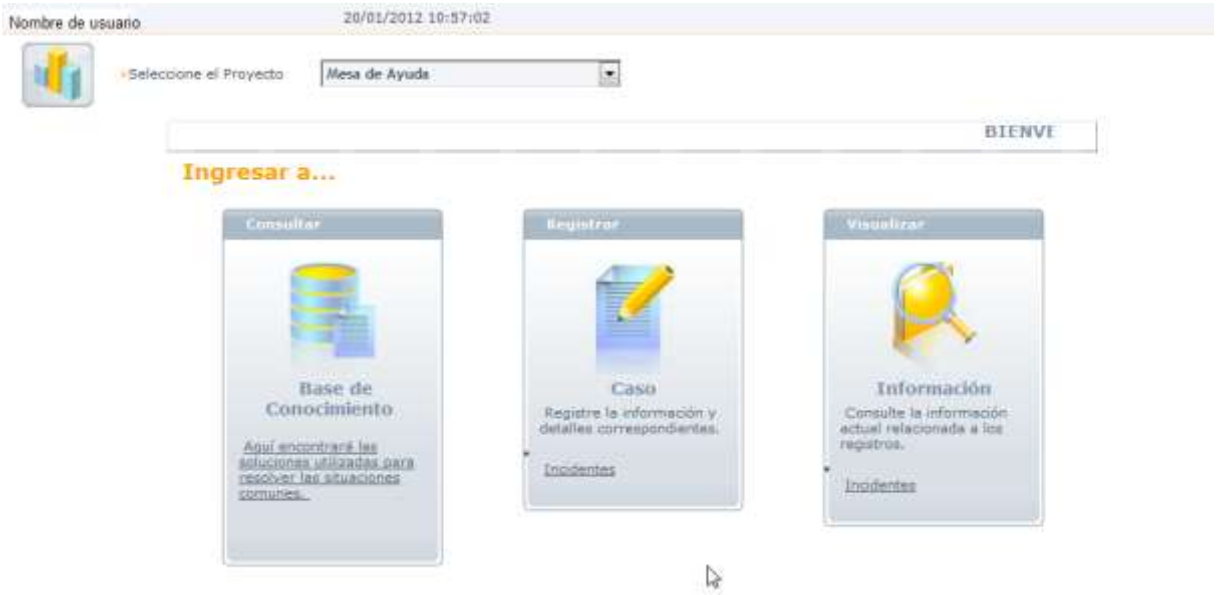
3. Escoge el proyecto



PROYECTOS:

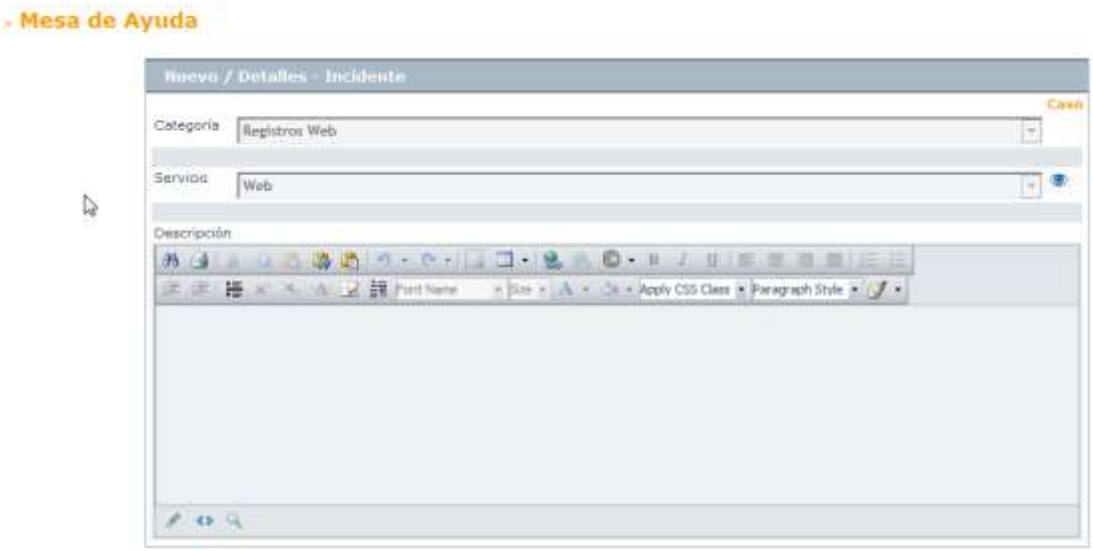
- **Administración de Contraseñas:** Es para solicitar claves de acceso para los distintos sistemas e interfaces que tiene el BANCO.
- **Mesa de Ayuda:** Es el soporte Service Desk
- **Desarrollo:** Son problemas causado por problemas en el CORE DEL BANCO o en aplicativos desarrollado dentro del BANCO.

4. Escogemos el tipo de proyecto al que queremos revisa/asignar el requerimiento.



a. BASE DE CONOCIMIENTO: Encontraras toda la Base de Ayuda si el problema ya ha ocurrido anteriormente, y si el usuario se encuentra en capacidad para poder resolverlo. Caso contrario tiene que registrar el caso.
b. CASO: Aquí es donde se procede a registrar el caso o problema que tengamos de acuerdo al tipo de proyecto que hayamos escogido anteriormente. En este caso específico se seleccionó MESA DE AYUDA y procedemos al paso 5.
c. INFORMACIÓN: En esta parte se encuentra un histórico de todos los casos e incidentes registrados por el usuario. Con toda la información requerida como aparece en el siguiente gráfico.

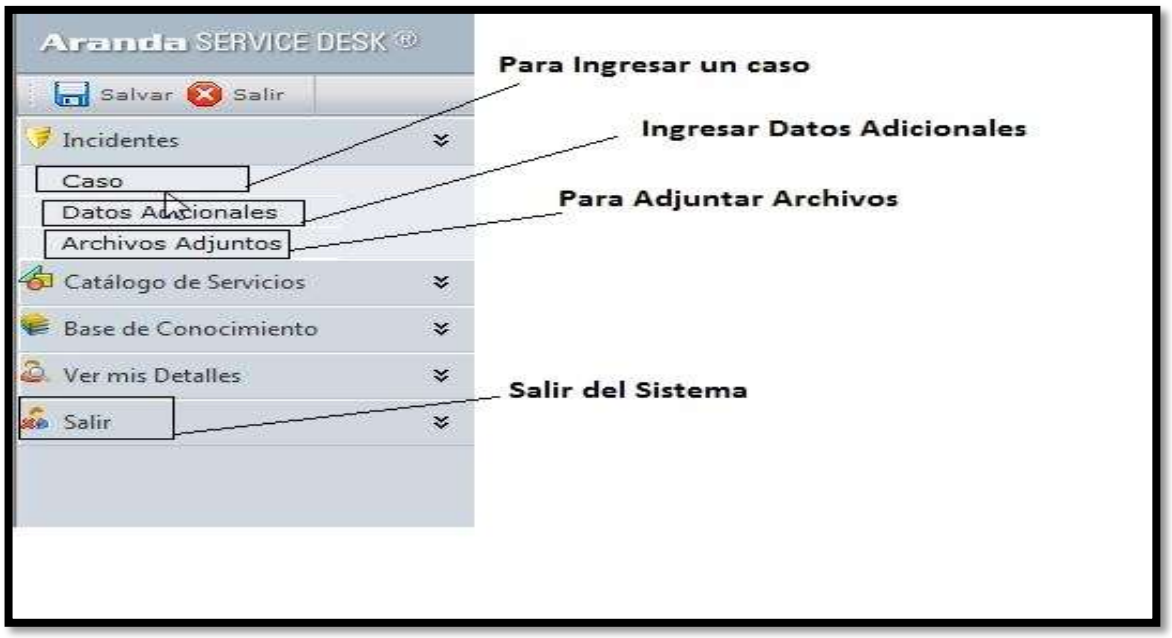
5. Escogemos el ingresar un nuevo requerimiento:



En la parte de DESCRIPCIÓN detallamos el tipo incidente y/o inconveniente que tengamos.

Una vez que terminemos de detallar nuestro incidente y/o requerimiento procedemos a guardar la información presionando SALVAR. Como se muestra en la imagen a continuación:

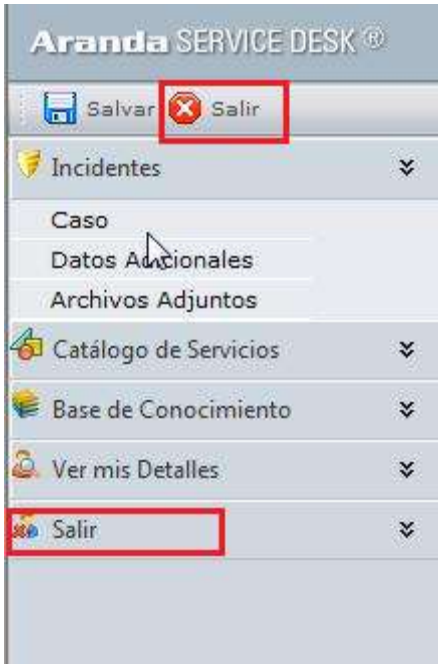
Los demás botones se los específica a continuación



Datos Adicionales ARANDA

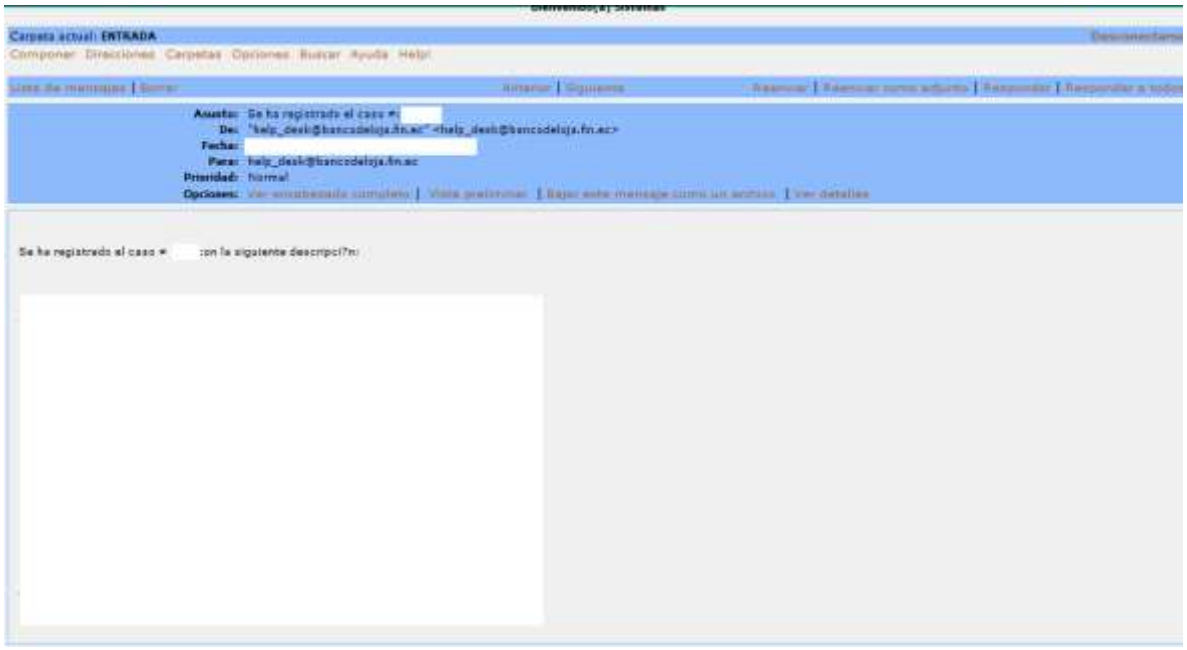
Adjuntar Archivos ARANDA

Cualquier de los dos botones SALIR sirve para para cerrar la sesión y salir del sistema ARANDA.



SEGUNDA PARTE

1. Una vez que se haya registrado el caso nos llega un MAIL describiendo toda la información del requerimiento al SUPERVISOR SERVICE DESK.



2. Luego el SUPERVISOR DE SERVICE DESK canaliza y asigna el caso a un OPERADOR DEL CENTRO DE CÓMPUTO.
3. Una vez asignado llega un mail al OPERADOR confirmando que se la asignado un caso.

TERCERA PARTE

1. Una vez asignado llega un mail al OPERADOR confirmando que se la asignado un caso.
2. El usuario ingresa al sistema http://aranda/asdk

3. Ubica su nombre y su contraseña

4. El OPERADOR SE DIRIGE AL CASO y visualiza la siguiente imagen:

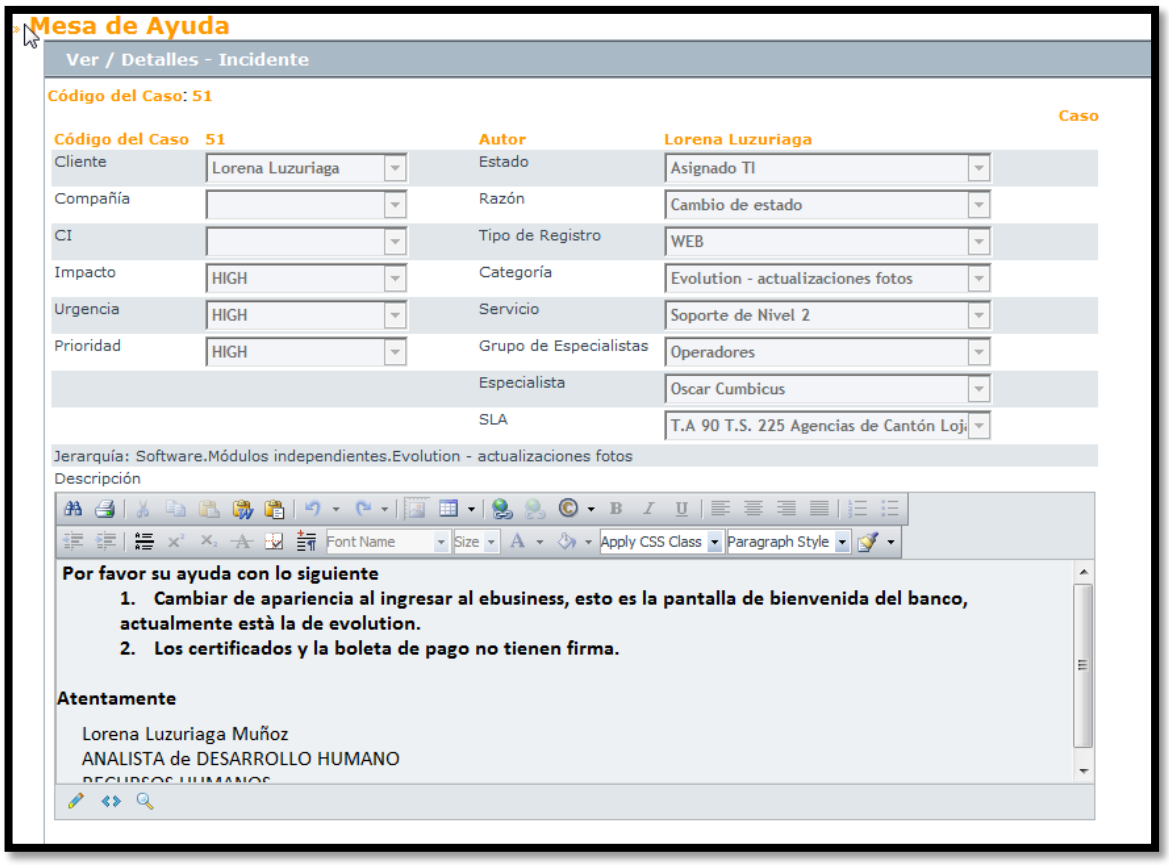
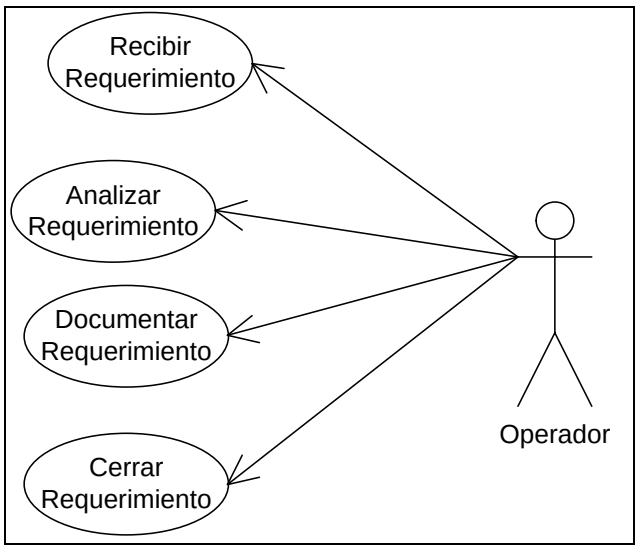


Ilustración 8: Detalles de Requerimiento de Mesa de ayuda HELPDESK SISTEMA ARANDA

6. Además, una vez que se le asigna al OPERADOR, el SISTEMA ARANDA envía un correo al USUARIO PETITORIO sobre qué persona le fue asignado el caso.
7. EL OPERADOR puede realizar cualquier de las siguiente actividades:



8. Una vez que se resuelve y se cierra el caso el SISTEMA ARANDA envía una notificación al SUPERVISOR SERVICE DESK que se encuentre cerrado el CASO.

5. ANEXO 5

5.1. Plantilla para el Ingreso de Requerimientos.

Esta plantilla servirá para llevar un control y seguimiento a las fallas que se vayan suscitando en la red.

INGRESO DE INCIDENTES DE SERVIDOR/SERVICIOS	CASO NRO.

Fecha:		Hora Incidente:	
Asignado a:			

Nombre del Servidor/Servicio	
Tiempo Aproximado de Solución	
Descripción de Error	

Tipo de Falla	Red □	Servicio□	Seguridad□	Otro□

Equipos o Servicios Afectados				
Criticidad	Ninguna□	Baja□	Media□	Alta □
Estado	Iniciado□	Pendiente□	Finalizado□	Escalado a Terceros □
				Responsable de Solución:

Descripción de la Solución:

Recomendaciones y/o Sugerencias:

FIRMA DEL RESPONSABLE

6. ANEXO 6

6.1. Selección de la Distribución Linux

Considerando para el análisis de la selección de la distribución Linux a emplear para instalar la herramienta NMS en este caso el NAGIOS, se ha tomado en cuenta la NORMA IEEE 830 para definir un Sistema Operativo que posea las siguientes características:

- Debe de poseer repositorios de versiones para mantener actualizado el software.
- Tener un nivel de seguridad que garantice la integridad del núcleo del sistema.
- El Sistema tiene que ser OpenSource y que tenga unas licencias GNU/GPL o similares.
- Poseer soporte de una comunidad para realizar actualizaciones y buscar ayuda.
- Permita la fácil integración con nuevas herramientas de gestión de red.

REQUERIMIENTOS

Dentro de los requerimientos para el analisis de herramienta se tuvo en cuenta:

1. Debe de ser software libre y tener una licencia GPL sin costo.
2. La versión que se va a usar debe ser actualizada y estable. Además, de poseer repositorios públicos para la descarga.
3. La velocidad de arranque del sistema operativo debe ser muy rapida para disminuir los tiempos de inicio y puesta en marcha de un servicio cuando se realizan mantenimientos o cuando existen fallas que requieren reinicio del sistema.
4. El envio de información y de paquetes a través de la red debe de ser lo mas eficiente posible.
5. El sistema operativo tiene que poseer documentación sufiente y soporte de una comunidad de desarrolladores para siempre tener actualizaciones y terner un medio de consulta.
6. Rendimiento del NMS teniendo en cuenta el hardware instalado y la ejecución del Software.
7. El sistema debe de disponer de una inteface de administración mediante consola para que permita a los administradores acceder con facilidad, configurar todas las funcionalidades y funciones que tiene el Sistema Operativo.

Tabla 33: Evaluación del Sistema Operativo

Nro. Requerimiento	UBUNTU	FEDORA	CENTOS	DEBIAN	OPENSUSE
1	8	8	8	8	8
2	5	5	8	8	5
3	5	5	10	8	5
4	8	8	8	8	8
5	10	10	10	10	10
6	6	7	8	7	8
7	9	5	10	8	5
TOTAL	51	48	62	57	49

De acuerdo a lo expuesto en los puntos anteriores se procede a escoger CENTOS basándose en las siguientes condiciones:

1. Cumple con los requerimientos antes mencionados.
2. Según la norma IEEE 830[99] lo ubica como una de las mejores características basadas en OpenSource.
3. Es un sistema utilizado ampliamente por las organizaciones para lo que implementación de servidores.
4. Adaptabilidad del sistema operativo frente a las herramientas de monitoreo que se va a instalar.
5. La superioridad en el rendimiento y estabilidad por el NMS (NAGIOS) instalado.
6. Posee estabilidad y ejecución de comandos a través de consola.
7. Tiene una gran comunidad de soporte, documentación, foros y manuales web.

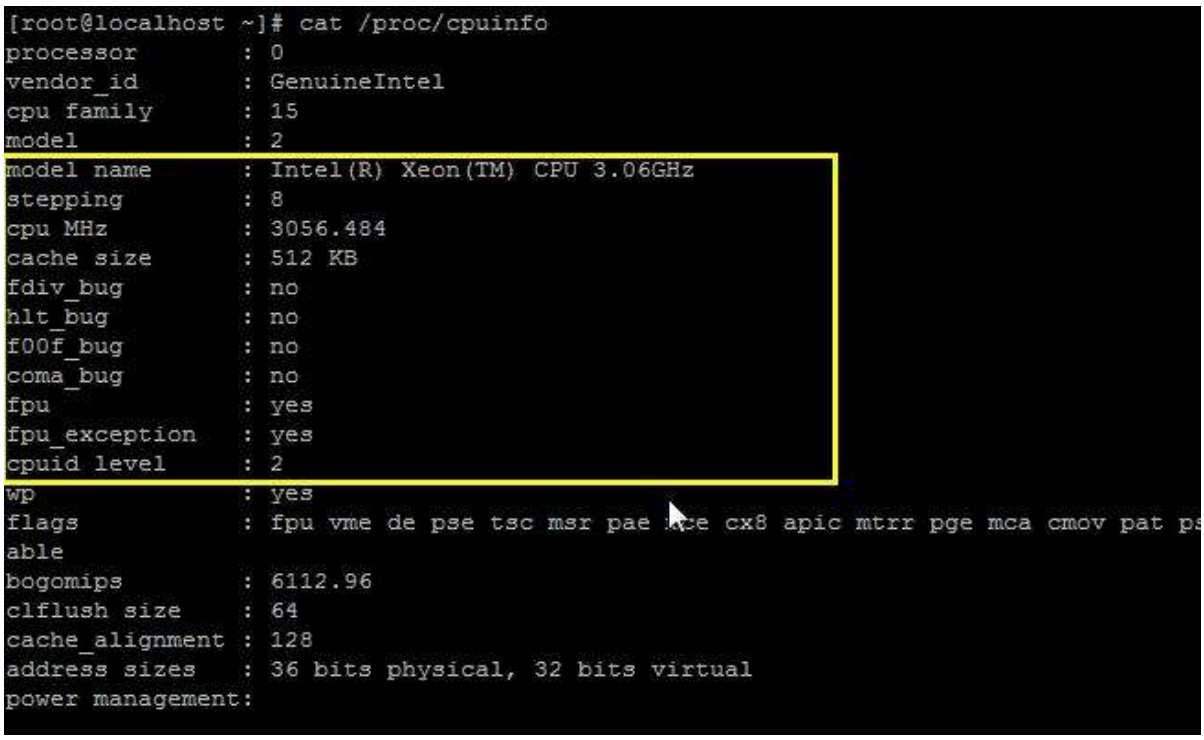
SISTEMA DE PRODUCCIÓN

La implementación del NOC, se enmarcan dentro de las pruebas realizadas en el Capítulo 3 y en el Anexo 9: de Análisis de Herramientas.

SERVIDOR DE MONITOREO

De acuerdo a los recursos existentes, se implementó el Sistema de Monitoreo en un equipo de las siguientes características:

[99] LauC2457, «Ieee 830 srs», enero 25, 2011, http://www.slideshare.net/LauC2457/ieee-830-srs; Mauricio Ortiz Olague, «Formato de documentacion ieee 830», marzo 20, 2012, http://www.slideshare.net/MauricioOrtizOlague/formato-de-documentacion-ieee-830; «ieee830.pdf (objeto application/pdf)», s. f., http://www.fdi.ucm.es/profesor/gmendez/docs/is0809/ieee830.pdf.


[root@localhost ~]# cat /proc/cpuinfo
processor : 0
vendor_id : GenuineIntel
cpu family : 15
model : 2
model name : Intel(R) Xeon(TM) CPU 3.06GHz
stepping : 8
cpu MHz : 3056.484
cache size : 512 KB
fdiv_bug : no
hlt_bug : no
f00f_bug : no
coma_bug : no
fpu : yes
fpu_exception : yes
cpuid level : 2
wp : yes
flags : fpu vme de pse tsc msr pae cx8 apic mtrr pge mca cmov pat
able
bogomips : 6112.96
clflush size : 64
cache_alignment : 128
address sizes : 36 bits physical, 32 bits virtual
power management:

7. ANEXO 7

7.1. Sistemas de Gestión De Red

Un Sistema de Gestión de Red o NMS (Nerwork Manager System) por sus siglas en inglés, son herramientas que permiten la administración de una red organizacional y facilita el monitoreo, inventarios de equipos, reportes y nos ayuda también a la toma de decisiones en cuanto a la estabilidad la red. Otro objetivo de estos sistemas es el de ayudar a los administradores a tener siempre el control de los eventos de la red y detectar anticipadamente los problemas antes de que los usuarios los perciban, y tomar la iniciativa para hacer que las cosas no sucedan.

El presente capítulo se describirá cada una de las herramientas evaluadas y se expondrá las características, ventajas, desventajas, recursos de Hardware y Software. Tomando en cuenta los criterios de evaluación tomados en la el capítulo 2.

7.2. Herramientas Analizadas

Para el análisis de la herramienta se buscó un NMS que cumpla con los requerimientos de la empresa y que los costos de adquisición e implementación sean bajos; es por eso, que todas las herramientas poseen licencia GNU (General Public License), la cual es una licencia de Software Libre con bajo coste de instalación, que nos asegura que siempre tendremos actualizaciones disponibles y soporte por parte de una gran comunidad de desarrolladores.

Para este proceso se utilizó el método analítico-sintético para poder recopilar información de las siguientes herramientas:

ZABBIX

- Kristóf Kovács. “Zabbix Vs Nagios Comparison.” Kristóf Kovács, n.d. http://kkovacs.eu/zabbix-vs-nagios.
- “Manual_zabbix.pdf”, n.d.
- Olups, Richards. Zabbix 1.8 Network Monitoring. PACKT PUB, 2010.
- “ZABBIX Manual V1.6.pdf”, n.d.

JFFNMS

- Installing jffnms [Internet]. [cited 2012 Mar 12]. Available from: http://www.jffnms.org/docs/installing.html#sec:hwreqs
- Craig Small csmall@small.dropbear.id.au, Javier Szyszlican javier@szysz.com. JFFNMS Manual. 2008.

- jffnms.pdf.
- JFFNMS Manual [Internet]. [cited 2012 Mar 9]. Available from: http://www.jffnms.org/docs/jffnms.html
- ProyectoJFFNMS.pdf.

PANDORA

- Artica Soluciones Tecnológicas 20052010, Sancho Lerena Urrea, David Villanueva Jiménez, and Jorge González González. "Manual Del Administrador." Translated by Julia Lerena Urrea (Traducción), Pablo de la Concepción, Ramón Novoa, Miguel de Dios, Sergio Zarzuelo, and Darío Rodríguez, n.d.
- "PandoraFMS_Releasenote_3.2_ES.pdf", n.d.

ZENOSS

- Badger, Michael. Zenoss Core Network and System Monitoring: A Step-by-step Guide to Configuring, Using, and Adapting This Free Open Source Network Monitoring System -... Mark R. Hinkle, VP of Community Zenoss Inc. Packt Publishing, 2008.
- ces1227. "Zenoss Manual." SlideShare, n.d. http://www.slideshare.net/ces1227/zenoss-manual-presentation.
- "Zenoss_Administration_06-102009-2.5-v01.pdf", n.d.

NAGIOS

- Dennys Muria, Kirian Moreno, Germán Barrios, Bárbara Solórzano, Domingo Perazzo, Anthony Baptista, Dennys Suarez. "Nagios", n.d. http://es.scribd.com/doc/21931635/NAGIOS.
- Ethan Galstad. "Nagios Core Version 3.x Documentation", n.d.
- Ignacio Barrientos Arias, and José Beites de Pedraza. "NAGIOS Un Sistema De Monitorización De Servicios De Red", March 14, 2006.
- Kristóf Kovács. "Zabbix Vs Nagios Comparison." Kristóf Kovács, n.d. http://kkovacs.eu/zabbix-vs-nagios.
- "Manuales: nagios [Cayu - Wiki De Sergio Cayuqueo]", n.d. http://cayu.com.ar/wiki/doku.php?id=manuales:nagios.
- "Nagios En Español: Definiciones De Objetos", n.d. http://nagioses.blogspot.com/2011/07/definiciones-de-objetos.html.
- "Nagios.pdf", n.d. https://nsrc.org/workshops/2008/walc/presentaciones/nagios.pdf.

- Sergio Cayuqueo. “Monitoria y Análisis De Red Con Nagios”, n.d.

Una vez analizada la bibliografía expuesta anteriormente se pudo recopilar la información de cada una de las herramientas:

ZABBIX[100]

Zabbix es una herramienta creada por Alexei Vladishev, y actualmente es un activo desarrollador y aporta para Zabbix SIA.

Zabbix tiene la licencia GPL, está basado en PHP, las librerías están realizadas en C y utiliza Apache como motor de Servidor Web; sirve para conocer el estado e integridad de los servidores, además, poseen un mecanismo que permite tener notificaciones flexibles y tener una rápida reacción a los problemas.

La página oficial es: http://www.zabbix.com

Características:

- Zabbix supervisa todos los principales protocolos (HTTP, FTP, SSH, SMTP, POP3, SMTP, SNMP, MySQL, etc)
- Alertas de correo electrónico y / o SMS
- Muy buena Interfaz Web
- Agente nativo disponible en Windows, OS X, Linux, FreeBSD, etc
- Monitoreo web de la aplicación (contenidos, la latencia, velocidad)
- Se puede visualizar y comparar cualquier valor que controla
- Sistema de "plantillas"
- Poderes locales de seguimiento
- Pantallas personalizables tablero de instrumentos
- En tiempo real de informes SLA

Ventajas

- Administración completamente web.
- Escalabilidad. Probado hasta 10.000 dispositivos.
- Posibilidad de monitorizar redes internas y externas.
- Sistema de alertas (email, SMS, Jabber)

[100] Richards Olups, *Zabbix 1.8 Network Monitoring* (PACKT PUB, 2010).

- Creación de plantillas de configuración exportables/importables.
- Autodescubrimiento de dispositivos.
- Multiplataforma (Windows, Linux, AIX, FreeBSD, HP-UX, Solaris)
- Base de datos (Oracle, MySQL, PostgreSQL o SQLite).

Desventajas

- Zabbix es más complejo de configurar
- La escalada es un poco extraño
- Sin detección de aleteo
- La documentación es irregular a veces,
- Utiliza una base de datos (como MySQL)

Hardware:

Tabla 34: *Requerimientos de Hardware Zabbix*

Tamaño	CPU/Memoria	Disco Duro	Número de host
Pequeña	PII 350MHz/256MB	40 GB*	20
Mediana	AMD Athlon 3200/2GB	80 GB*	500
Grande	Intel Dual Core 6400/4GB	100 GB*	>1000
Muy Grande	Intel Xeon 2xCPU/8GB	120 GB*	>10000

Software

Tabla 35: *Requerimientos de Software Zabbix*

Software	Descripción
Apache	Servidor Web
PHP	
PHP modules: php-gd	PHP GD module must support PNG images.
PHP TrueType support	--with-ttf
PHP bc support	php-bcmath, --enable-bcmath
PHP XML support	php-xml or php5-dom, if provided as a separate package by the distributor
PHP session support	php-session, if provided as a separate package by the distributor
PHP socket support	php-net-socket, --enable-sockets. Required for user

Software	Descripción
	script support.
PHP multibyte support	php-mbstring, --enable-mbstring
PHP gettext support	php-gettext, --with-gettext
IBM DB2 ibm_db2	Required if IBM DB2 is used as Zabbix back end database.
MySQL php-mysql	Required if MySQL is used as Zabbix back end database.
Oracle oci8	Required if Oracle is used as Zabbix back-end database.
PostgreSQL php-pgsql	Required if PostgreSQL is used as Zabbix back-end database. It is suggested to use at least PostgreSQL 8.3, which introduced much better VACUUM performance.
SQLite php-sqlite3	Required if SQLite is used as Zabbix back-end database.

Plataformas[101]

Tabla 36: *Plataformas de ejecución de Servidor/Agente Zabbix*

PLATAFORMA	ZABBIX SERVER	ZABBIX AGENT
AIX	*	*
FreeBSD	*	*
HP-UX	*	*
Linux	*	*
Mac OS X	*	*
Novell Netware		*
Open BSD	*	*
SCO Open Server	*	*
Solaris	*	*
Tru64/OSF	*	*
Windows NT 4.0, Windows 2000, Windows 2003, Windows XP, Windows Vista		*

[101] Ibid. Richards Olups, *Zabbix 1.8 Network Monitoring* (PACKT PUB, 2010).

JFFNMS[102]

JFFNMS son las siglas de Just For Fun Network Management System que se traduciría como: una forma divertida de gestionar un sistema de red; es un programa que utiliza el lenguaje PHP scripting para recolectar y mostrar información acerca de varios dispositivos que pueden ser encontrados en una red de computadores de una organización.

JFFNMS es muy modular y extensible lo que significa que se pueden programar extensiones en caso de que no se disponga de soporte para los elementos específicos de la red.

La página oficial es: http://www.jffnms.org

Características:

- Permite monitorizar una red IP mediante SNMP.
- Puede ser utilizado para monitorizar cualquier dispositivo SNMP (servidor, router, puerto TCP y UDP
- JFFNMS está escrito en PHP, el cual funciona en Sistemas
- Operativos GNU/Linux, FreeBSD y Windows 2000/XP.
- Tiene soporte de base de datos (MySQL o PostgreSQL

Ventajas

- Alarmas de syslog y eventos SNMP trap.
- Representación gráfica de datos estadísticos de interfaces de red.
- Notificaciones vía email basadas en la configuración de alarmas.
- Permite monitorizar una red IP mediante SNMP, Siglo y TACACS+ (Terminal Access Controller Access Control System).

Desventajas[103]

Se han encontrado múltiples vulnerabilidades en Justa For Fun Network Management System. Las vulnerabilidades son descritas a continuación:

[102] Craig Small csmall@small.dropbear.id.au y Javier Szyszlican javier@szysz.com, «JFFNMS Manual», julio 3, 2008.

[103] «Inseguridades.pdf (objeto application/pdf)», s. f., http://www.linux-magazine.es/issue/08/Inseguridades.pdf; Tim Brow, «Boletines de Vulnerabilidades», s. f., https://www.ccn-cert.cni.es/index.php?option=com_vulnerabilidades&task=view&id=3424&Itemid=0&lang=ca.

- Se ha encontrado una vulnerabilidad del tipo cross-site scripting en Just For Fun Network Management System 0.8.3. La vulnerabilidad reside en un error no especificado. Un atacante remoto podría inyectar código script web o HTML mediante el parámetro user.
- Se han encontrado múltiples vulnerabilidades del tipo inyección SQL en Just For Fun Network Management System 0.8.3 en el archivo auth.php. La vulnerabilidad yace cuando se desactiva magic_quotes_gpc. Un atacante remoto podría ejecutar comandos SQL de forma arbitraria a través de los parámetros user y pass.
- Se ha encontrado una vulnerabilidad en Just For Fun Network Management System 0.8.3. La vulnerabilidad reside en un error no especificado. Un atacante remoto podría obtener información sobre la configuración del sistema mediante una petición directa a admin/adm/test.php.

Hardware

Tabla 37: *Requerimientos de Hardware JFFNMS*

Tamaño	CPU/Memoria	Disco Duro	Número de host
Pequeña	PII 266MHz 128MB	40 GB*	20
Mediana	Xeon 3.4GHz + 1GB	80 GB*	500
Grande	Dual Xeon 2GHz + 4GB	100 GB*	>1000
Muy Grande	Dual Xeon 3.4 GHz 2xCPU 8GB	120 GB*	>10000

Software

Tabla 38: *Requisitos Software JFFNMS*

Software	Descripción
Apache	Apache web server, essential.
PHP	Needs to have MySQL, GD and SNMP enabled.
net snmp	Optional if you want SNMP alerts so you use snmptrapd. You can use an alternative one if you prefer, but it has to be able to call an external program.
MySQL	Need this for the libraries (eg to enable PHP MySQL) as well as to supply the main database.
rrdtool	Round Robin Database, for MRTGlike graphs.

Software	Descripción
	See http://www.rrdtool.org/.
nmap	Provides TCP ports discovery
tac plus	TACACS+ Server for AAA. Optional but handy to have. (get it from the jffnms site)
msyslog	Modular syslog daemon to insert syslog lines into MySQL or PostgreSQL databases. (get it from the jffnms site)

Plataformas

Tabla 39: *Plataformas de ejecución de Servidor/Agente JFFNMS*

PLATAFORMA	SERVER	AGENT
Linux • **Ubuntu** • **RH4** • **Centos** • **Fedora**	*	Instalación del Servicio SNMP
Mac OS X	*	Instalación del Servicio SNMP
Novell Netware		Instalación del Servicio SNMP
Open BSD	*	Instalación del Servicio SNMP
SCO Open Server	*	Instalación del Servicio SNMP
Solaris	*	Instalación del Servicio SNMP

NAGIOS[104]

Fue creado por Ethan Galstad, y es actualmente él se encuentra frente al proyecto junto con un grupo de desarrolladores de software.

Nagios está escrito en C y se trata de un software que proporciona una gran versatilidad para consultar cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables correspondientes mediante correo electrónico y mensajes SMS, cuando estos parámetros exceden de los márgenes definidos por el administrador de red.

[104] Ethan Galstad, «Nagios Core Version 3.x Documentation», s. f.

Como un poco de historia podemos decir que anteriormente Nagios se llamaba Netsaint y por problemas comerciales y de copyright se cambió definitivamente por el nombre actual NAGIOS[105].

La página oficial es: http://www.nagios.org

Características[106]:

- Gestión de servicios (SMTP, POP3, HTTP, PING, etc.).
- Monitorización de recursos de sistemas.
- Gestión de servicios pasivos generados por aplicaciones o comandos externos (servicios pasivos)
- Monitorización de factores ambientales a través de sondas físicas (temperatura, humedad relativa, luminosidad, líneas de tensión, etc.)
- Arquitectura simple de integración que permita a los usuarios desarrollar fácilmente sus propios agentes de chequeo de servicios y recursos.
- Definición de arquitecturas jerárquicas de los elementos gestionados que nos permitan identificar rápidamente las caídas de servicios.
- Diferentes notificaciones de errores por tipo de contacto (vía email, SMS u otros servicios de notificación)
- Escalado y distribución de servicios, recursos y nodos gestionados por grupos de contacto.
- Definición de acciones reactivas que permitan solventar un problema de forma inmediata.
- Soporte de arquitecturas de servidor redundantes y distribuidas.
- Retención del último estado de los servicios y recursos que permite paliar pérdidas del sistema gestor.
- Programación de intervalos de tiempo sin notificaciones.
- Visión rápida y sencilla de los elementos gestionados.
- Portal web que permite consultar el estado de los elementos gestionados, las notificaciones realizadas, los problemas acontecidos, el estado de los servidores, la administración básica, etc.
- Definición de usuarios de lectura y administración del portal web.

[105] «Nagios - Wikipedia, la enciclopedia libre», s. f., http://es.wikipedia.org/wiki/Nagios.
[106] Dennys Muria, Kirian Moreno, Germán Barrios, Bárbara Solórzano, Domingo Perazzo, Anthony Baptista, Dennys Suarez, «NAGIOS», s. f., http://es.scribd.com/doc/21931635/NAGIOS.

Ventajas

- Nagios controla todos los principales protocolos (HTTP, FTP, SSH, SMTP, POP3, SMTP, SNMP, MySQL, etc)
- Alertas de correo electrónico y / o SMS
- Múltiples niveles de alerta: ERROR, WARNING, OK
- Visualización automática de la topografía
- Totalmente independiente, ningún otro software es necesario
- Control de contenidos web
- Posee cliente nagios para Windows NSClient++, y el cliente para linux es NRPE.
- Nagios Core puede monitorear cualquier dispositivo que tenga una dirección IP.
- Para monitorear un dispositivo no es necesario instalar un agente en el dispositivo sino simplemente agregar la dirección IP de este a la consola de Nagios la cual lo detectará automáticamente.
- La actualización de los datos y las pantallas de mapas de red es automática.
- Es la herramienta de monitoreo libre más usada, razón por la cual existe extensa documentación sobre su configuración, ayuda sobre problemas, librerías para la consola de monitoreo entre otros aspectos que la hacen una herramienta muy robusta de monitoreo.
- La consola de administración es de fácil manejo.
- Permite monitorear varios parámetros a la vez.
- Permite ver mapas de red por grupos.
- Permite la asignación de roles de usuarios de acuerdo a sus responsabilidades y equipos asignados para el monitoreo.

Desventajas

- Nagios tiene acceso SSH para controlar a distancia internos del sistema (archivos abiertos, procesos en ejecución, memoria, etc).
- La versión libre no cuenta con soporte oficial, solo con la documentación que se pueda encontrar en la página oficial, en los foros de discusión y en general todo el material que se pueda encontrar en internet.
- Interfaz web es en su mayoría de sólo lectura.

Hardware[107]

Tabla 40: *Requerimientos de Hardware Nagios*

Name	CPU/Memoria	Disco Duro	Número de host
Pequeña	PII 266MHz 128MB	20	20
Mediana	Xeon 2.4GHz + 1GB	40	500
Grande	Dual Xeon 1GHz + 4GB	80	>1000
Muy Grande	Dual Xeon 2 GHz 2xCPU 8GB	>=120	>10000

Software[108]

Tabla 41: Requerimientos Software Nagios

PAQUETE	DESCRIPCIÓN
Perl	Interprete para el lenguaje de script Perl
Net::SNMP	Módulo de Perl para consultas SNMP
Crypt::DES	Módulo de Perl para encriptación DES, necesario para consultas SNMPv3
Digest::HMAC	Keyed-Hashing for Message Authentication
Digest::SHA1	Perl interface to the SHA-1 algorithm
RRDTool	Utilitario para generación de gráficas de red y además su módulo de integración con el lenguaje Perl
Zlib	Librería de compresión utilizada por las utilidades graficas
LibJPEG	Librería para exportación jpg
LibPNG	Librería para exportación png
Freetype2	Librería para procesamiento de fuentes
Graphviz	Utilitario para generación de graficas
XFree86-libs	Librerías gráficas generales
Apache 2	Servidor Web
PHP	Interprete de lenguaje de script
MySQL	Sistema de base de datos
Postfix	SMTP para enviar mail
GD	Librería para generación de formatos gráficos
Nagvis	Aditivo para la generación de diagramas dinámicos

[107] «Nagios_XI_Hardware_Requirements.pdf (objeto application/pdf)», s. f., http://assets.nagios.com/downloads/nagiosxi/docs/Nagios_XI_Hardware_Requirements.pdf.
[108] Ignacio Barrientos Arias y José Beites de Pedraza, «NAGIOS Un sistema de monitorización de servicios de red», marzo 14, 2006; Sergio Cayuqueo, «Monitoria y análisis de Red con Nagios», s. f.; Ethan Galstad, «Nagios Core Version 3.x Documentation».

PAQUETE	DESCRIPCIÓN
PNP4Nagios	Aditivo para la generación de gráficos estadísticos y reportes visuales
NDO	Agregado para articular Nagios con MySQL
Plugins	Plugins de chequeo standard de Nagios
SNMP Plugins	Plugins para la integración de chequeos SNMP de Nagios
Nagios	Sitio de descarga oficial
NagiosQL	Herramienta visual de configuración de Nagios vía Web
Dokuwiki	Herramienta de documentación colaborativa
Syslog-Ng	Logueo de eventos del sistema
SNARE	Agente Syslog para clientes Windows
MK Livestatus	Aditivo para obtener los datos de Nagios en Vivo vía Socket (muy útil para abandonar NDO)

Plataformas[109]

Tabla 42: *Plataformas de ejecución de Servidor/Agente Nagios*

PLATAFORMA	SERVER	AGENT
Linux • **Ubuntu** • **RH4** • **Centos** • **Fedora**	*	• Instalación del Servicio SNMP y NRPE para Linux • Instalación de Cliente NSCliente++ para Windows

PANDORA[110]

El proyecto original de Pandora FMS fue mentalizado por Sancho Lerena en el año 2003. En la actualidad hay muchas otras personas trabajando en él y el proyecto es dirigido y financiado por Ártica Soluciones Tecnológicas.

Pandora FMS es código abierto, y aparece recogida bajo Licencia GPL2.

La página oficial es: http://www.pandora.sourceforge.net

[109] «Nagios Support Wiki - Nagios XI:FAQs», s. f., http://support.nagios.com/wiki/index.php/Nagios_XI:FAQs#Hardware_Requirements; Dennys Muria, Kirian Moreno, Germán Barrios, Bárbara Solórzano, Domingo Perazzo, Anthony Baptista, Dennys Suarez, «NAGIOS».

[110] «PandoraFMS_Releasenote_3.2_ES.pdf», s. f.

Características:

- Es sistema es muy modular y se puede dividir las carga en diferente servidores.
- Permite crear informes, estadísticas, niveles de adecuación de servicio (SLA).
- Se puede recolectar información mediante el Agente o mediante el protocolo SNMP
- Retención del último estado de los servicios y recursos que permite paliar pérdidas del sistema gestor.
- Existe una herramienta que facilita a migración de Nagios a Pandora FMS.
- Instalación del agente de manera distribuida o de forma local.
- Algo importante dentro de este NMS es puede medir: sistemas operativos, servidores, aplicaciones y sistemas hardware tal como cortafuegos, proxies, bases de datos, servidores web, VPN, routers, switches, procesos, servicios, acceso remoto a servidores, etc.
- Programación de intervalos de tiempo para que no se envíen notificaciones.

Ventajas

- Es una herramienta de monitoreo libre
- La consola de administración es de fácil manejo.
- Permite monitorear varios parámetros a la vez.
- Permite ver mapas de red por grupos.
- Existe documentación en español e inglés
- Permite crear alertas personalizadas para cada módulo.
- Sus agentes pueden ser instalados en cualquier sistema operativo.

Desventajas

- La versión libre no contiene todos los módulos de monitoreo.
- Solo la versión pagada o Enterprise permite monitorear servicios de los sistemas operativos.
- Pandora no es un sistema de monitoreo en tiempo real ya que la actualización de sus datos tiene que ser configurado manualmente teniendo un error de más menos 5 segundos

Hardware[111]

Tabla 43: *Requerimientos de Hardware Pandora FMS*

Name	CPU/Memoria	Disco Duro	Número de host
Pequeña	Core 2 GHz/2 GB	300GB	20
Mediana	Dual core 2.5 GHz/4 GB	400GB	500
Grande	Quad core 6 GHz/6 GB	500GB	>1000
Muy Grande	Quad core 12 GHz/8 GB	600GB	>10000

Software

Tabla 44: *Requerimientos Software Pandora*

Paquete	Descripción
Perl	Interprete para el lenguaje de script Perl
SSH	
XML	Procesado y gestión de datos en formato XML.
DBI::DB	Interfaz con MySQL.
Apache 2	Servidor Web
PHP	Interprete de lenguaje de script
MySQL	Sistema de base de datos
Net::SNMP	Módulo de Perl para consultas SNMP
Crypt::DES	Módulo de Perl para encriptación DES, necesario para consultas SNMPv3
Postfix	SMTP para enviar mail

Plataformas

Tabla 45: *Plataformas de ejecución de Servidor/Agente Pandora*

PLATAFORMA	PANDORA FMS SERVER	PANDORA FMS AGENT
Windows 2000 SP3	*	*
Windows 2003	*	*
Windows XP	*	*
Windows Vista	*	*
Windows 7	*	*
Windows 2008	*	*
Debian	*	*

[111] «Pandora FMS: Free System Monitoring Software || Free Software», s. f., http://www.ilovefreesoftware.com/13/windows/system-utils/pandora-fms-free-system-monitoring-software.html.

PLATAFORMA	PANDORA FMS SERVER	PANDORA FMS AGENT
Fedora	*	*
FreeBSD	*	*
Gentoo	*	*
OS X	*	*
Red Hat	*	*
Solaris	*	*
SUSE	*	*
Ubuntu	*	*

ZENOSS

Erik Dahl es el creador de Zenoss y comenzó su desarrollo desde el 2002.[112]
Es un software bajo licencia GLP, escrito en Pythón y corre en una plataforma zope. (Zope es un código abierto del servidor de aplicaciones para la construcción de sistemas de gestión de contenidos, intranets, porta les y aplicaciones personalizadas). Zenoss crea una base de datos llamada (CMDB) para guardar los registros de los recursos-servidores, redes, y otros dispositivos en su entorno de TI[113].

Características:

- Permite monitorizar una red IP mediante SNMP.
- Puede ser utilizado para monitorizar cualquier dispositivo SNMP (servidor, router, puerto TCP y UDP
- JFFNMS está escrito en PHP, el cual funciona en Sistemas
- Operativos GNU/Linux, FreeBSD y Windows 2000/XP.
- Tiene soporte de base de datos (MySQL o PostgreSQL)
- Gestión de bases de datos de configuración (CMDB)
- De inventario y cambio
- Vigilancia de Red
- Disponibilidad de Vigilancia

[112] Michael Badger, *Zenoss Core Network and System Monitoring: A step-by-step guide to configuring, using, and adapting this free Open Source network monitoring system -... Mark R. Hinkle, VP of Community Zenoss Inc.* (Packt Publishing, 2008).
[113] ces1227, «Zenoss Manual», *SlideShare*, s. f., http://www.slideshare.net/ces1227/zenoss-manual-presentation.

- Monitoreo del rendimiento

Ventajas

- Vigilancia de la disponibilidad de dispositivos de red mediante SNMP
- Seguimiento de los servicios de red (HTTP, POP3, NNTP, SNMP, FTP)
- Seguimiento de acogida de los recursos (procesos, el uso de disco) en la mayoría de los sistemas operativos de red.
- Series cronológicas de la supervisión de la ejecución de los dispositivos
- Descubrir automáticamente los recursos de la red y los cambios en la configuración de la red
- Sistema de alerta basado en las notificaciones de conjuntos de reglas y de atención cíclica.

Desventajas

- La instalación es monolítica
- Necesita hardware de altas prestaciones

Hardware[114]

Tabla 46: *Requerimientos de Hardware Zenoss*

Name	CPU/Memoria	Disco Duro	Número de host
Pequeña	2 Cores/4GB	100 GB	20
Mediana	4 Cores/8GB	200 GB	500
Grande	8 Cores/16GB	300 GB	>1000
Muy Grande	**[115]	> 400 GB	>10000

** Si tiene planeado monitorear más de 1000 dispositivos, Zenoss recomienda distribuir el método de monitoreo en varios servidores y/o áreas organizativas. Además, se puede contactar con el Servicio Profesional de Zenoss para asistencia en el desarrollo de un plan de distribución de Monitoreo[116].

Software

Tabla 47: *Requerimientos de Software Zenoss*

Paquete	Descripción
Perl	Interprete para el lenguaje de script Perl y procesa la información enviada por los agentes

[114] Zenoss, Inc, «1.1 Hardware Requirements - Open Source Network Monitoring and Systems Management», s. f., http://community.zenoss.org/docs/DOC-7387.
[115] « 1.4. Deployments Larger than 1000 Monitored Devices», s. f., nota Descripción Adicional.
[116] Zenoss, Inc, «1.2 Hardware Requirements - Open Source Network Monitoring and Systems Management», s. f., http://community.zenoss.org/docs/DOC-10206#d0e152.

Paquete	Descripción
SSH	Es usado para el envío de transferencia de archivos entre servidor/agente y usado por el nuevo proyecto Tentacle
XML	Procesado y gestión de datos en formato XML.
DBI::DB	Interfaz con MySQL.
Apache 2	Servidor Web
PHP	Interprete de lenguaje de script. Se recomienda la versión 5.x
MySQL	Sistema de base de datos
Net::SNMP	Módulo de Perl para consultas SNMP
Crypt::DES	Módulo de Perl para encriptación DES, necesario para consultas SNMPv3
gcc/g++	Librería para la compilación de documento
Postfix	SMTP para enviar mail

7.3. Congruencia de Herramientas

Algunas de las congruencias que tienen la mayoría de NMS son:

- Monitoreo de servicios como: SMTP, POP3, HTTP, PING, etc.
- Monitoreo de recursos de sistemas.
- Diferentes tipos de notificaciones de errores como: sms, alertar visibles, alertas auditivas, correos electrónicos entre otras.
- Soporte de arquitecturas de servidor redundantes y distribuidas.
- Documentación web y soporte de comunidades de desarrolladores.
- Retención del último estado de los servicios y recursos que permite paliar pérdidas del sistema gestor.
- Poseen licencias OpenSource.
- Utilizan base de datos MySQL para el almacenamiento de eventos.
- Programación de intervalos de tiempo sin notificaciones.
- Visión rápida y sencilla de los elementos gestionados.
- Portal web que permite consultar el estado de los elementos gestionados, las notificaciones realizadas, los problemas acontecidos, el estado de los servidores, la administración básica, etc.

8. ANEXO 8

8.1. Configuraciones generales de NAGIOS

En el Servidor

Configuraciones necesarias en el servidor de monitoreo.

NAGIOS

Algunos puntos básicos previos a la instalación:

PATH: Esta es la ruta de instalación. Por defecto es /usr/local/nagios

Usuario: Usuario que va a usar nagios para ejecutarse. Debe crearse con adduser especificarle el PATH de NAGIOS como *su directorio home de inicio*, usualmente deberemos llamarlo nagios y debe estar dentro del grupo nagios

Grupo: Grupo de usuario que va a usar NAGIOS. Este grupo tendrá permisos sobre todos los ficheros y directorios de NAGIOS. Por defecto es nagios. Puede crearse con groupadd.

URL: NAGIOS utiliza una interfaz web para ejecutarse. Esta URL determina cual va a ser el directorio virtual que debe usar para instalarse. Por defecto /nagios, es decir, las peticiones irán dirigidas a http://host/nagios

Estructura de archivos

Una vez que compilamos e instalamos el paquete NAGIOS nos termina quedando una nomenclatura de directorios como la siguiente:

bin

Aquí se almacenan los binarios ejecutables

etc

Guarda la configuración de NAGIOS

libexec

Se almacenan los plugins que efectuaran los chequeos a monitorear

sbin

Dentro de este directorio se mantienen los ejecutables CGI de la interfaz web

share

Organiza el contenido web a mostrar, iconos, html, php, etc

var

Guarda los datos de ejecución del monitoreo, estado de servicios, hosts, y logs

bin

Dentro de este directorio encontramos los ejecutable principales, como el binario *nagios* que es el que se ejecuta como proceso en segundo plano, el

objeto *ndomod.o* que es el modulo que se encarga de traducir las estadísticas de nagios en formato de consultas *MySQL*, y *ndo2db*que el proceso en segundo plano que se encarga conectarse con la base de datos para posteriormente ejecutar esas consultas, **etc**

Este directorio guarda la configuración de NAGIOS, sus componentes, hosts/servicios a chequear, comandos de ejecución, contactos de notificación, intervalos de chequeos. Dentro del hay diferentes subdirectorios y archivos.

libexec

Allí se contienen lo ejecutables de los plugins que efectúan los chequeos, SNMP, SAP, Oracle, SSH, que pueden ser binarios, scripts en Perl, PHP, Shell, Java, etc.

sbin

Aquí se almacenan los ejecutables cgi que se ejecutaran para la visualización por web de la consola NAGIOS.

share

Aquí encontramos el contenido web, imágenes, logos, los aditivos como PNP, Nagvis y los datos que necesitan para funcionar estos.

var

Aquí se guardan los datos internos de NAGIOS, estadísticas de los chequeos, información de ejecución actual, archivos de sockets, registros de logs, colas de ejecución de chequeos.

Archivos de configuración nagios/etc

cgi.cfg

Definir archivo de configuración principal de NAGIOS

main_config_file=/usr/local/nagios/etc/nagios.cfg

Ruta donde se ubican los archivos a mostrar vía web

physical_html_path=/usr/local/nagios/share

Ruta del url a donde ubicar NAGIOS desde el navegador

url_html_path=/nagios

Mostrar o no el icono de ayuda en la interfaz web

show_context_help=0

Mostrar objetos pendientes de chequeo

use_pending_states=1

Usar autenticacion para acceder a NAGIOS

use_authentication=1

Tener usuario logueado por default (no recomendado, dejar comentado)

#default_user_name=guest

Usuarios con acceso permitido para ver la información de objetos (separados por comas)

authorized_for_system_information=nagiosadmin

Usuarios con acceso permitido para ver la informacion de configuracion (separados por comas)

sauthorized_for_configuration_information=nagiosadmin

Usuarios con acceso permitido ejecución de comandos nagios (separados por comas)

authorized_for_system_commands=nagiosadmin

Usuarios permitidos a ver informacion de hosts y servicios (separados por comas)

authorized_for_all_services=nagiosadmin

authorized_for_all_hosts=nagiosadmin

Usuarios permitidos para ejecutar comandos sobre hosts y servicios (separados por comas)

authorized_for_all_service_commands=nagiosadmin

authorized_for_all_host_commands=nagiosadmin

Tasa de refresco para la interfaz web en segundos

refresh_rate=90

htpasswd.users

Archivo con passwords encriptados de los usuarios que se autentificaran por HTTP

nagios.cfg

Archivo de configuración principal de NAGIOS, aquí se especifican los directorios de trabajo y se incluyen los archivos de configuración extra a utilizar por NAGIOS

Con diversos parámetros:

log_file se especifica el archivo de log a utilizar por NAGIOS

cfg_file se especifica un archivo de configuración extra a incluir en la ejecución de NAGIOS

cfg_dir se especifica un directorio con archivos de configuración extra a incluir recursivamente en la ejecución de NAGIOS

log_archive_pathpath dónde se alojaran los archivos de log

use_syslog integración con syslog

ndo2db.cfg

Archivo de configuración del daemon que se encarga de introducir las consultar generadas por el módulo ndomod

ndomod.cfg

Módulo de NAGIOS que se encarga de traducir la información de ejecución de NAGIOS en consultas MySQL, disponiéndolas por medio de un socket

resource.cfg

Archivo de configuración donde se definen macros de ejecución

objects/

Directorio de archivos generales de configuración

objects/commands.cfg

Definición de comandos de ejecución por default, con los alias que queremos usar

objects/contacts.cfg

Definición de contactos de notificación

objects/localhost.cfg

Plantilla inicial para el chequeo del host local

objects/printer.cfg

Plantilla de ejemplo de chequeo de impresoras por SNMP

objects/switch.cfg

Plantilla de ejemplo de chequeo de switchs por SNMP

objects/templates.cfg

Plantillas generales de host, contactos, y servicios

objects/timeperiods.cfg

Plantilla inicial para definir periodos de chequeos, aquí se definen los rangos de tiempo donde son válidos el envío de alertas y las verificaciones de los servicios que están funcionando

objects/windows.cfg

Plantilla de ejemplo de chequeo de equipos Windows

services/

Aquí vamos a definir los servicios que usaremos en los chequeos. Se define la métrica o el servicio a monitorizar y el host/grupo de hosts sobre el que se ejecuta

var/rw/

Allí se encuentra un archivo especial del socket que realiza la comunicación de los comandos y órdenes de la interfaz web hacia NAGIOS, como cambiar horarios de chequeo, deshabilitar notificaciones etc.

El archivo que allí se encuentra *nagios.cmd* debe tener permisos de escritura y lectura por el propietario y el grupo de pertenencia *nagios: nagcmd (660)*,

nagcmd es un grupo especial en el cual vamos a incluir al usuario que ejecuta el servido, y así poder enviar ordenes desde la interfaz web CGI. Esta es una característica avanzada de NAGIOS es que permite vía web la ejecución de ciertas tareas más allá del propio conjunto de CGI's que vienen de serie, como por ejemplo la caída o el reinicio del propio NAGIOS, etcétera. Para poder ejecutar este tipo de comandos es necesario también configurar el sistema de una forma un tanto especial. No hay que olvidar que al configurar NAGIOS de este modo se está permitiendo desde la web activar o desactivar opciones que en principio sólo estaban disponibles desde la consola del sistema. Para configurar NAGIOS de esta forma, hay que editar el fichero principal *nagios.cfg* y añadir (o modificar si ya existen) las siguientes líneas:

check_external_commands=1

command_check_interval=-1

command_file=/usr/local/nagios/var/rw/nagios.cmd

Lo que hará que NAGIOS active el chequeo para buscar comandos externos, con tanta frecuencia como sea posible por el sistema y buscará los comandos en el archivo *nagios.cmd*.

En el siguiente gráfico detalla la organización recomendada de la configuración de NAGIOS.

En el Cliente

Deberemos conocer bien lo que queremos chequear y conocer los indicadores que nos mostraran si deberemos expresarlos como un OK, un WARNING o un CRITICAL.
Luego deberemos reflejar esos estados en su código de retorno o Exit status, dependiendo del código del mismo NAGIOS entenderá que debe mostrar.

Tabla 48: *Estados de los servicios*

Exit status	Estado de Servicio	Estado de Host	Descripción
0	OK	UP	El plugin es capaz de verificar el servicio y que parece estar funcionando correctamente
1	WARNING	UP/DOWN/UNREACHABLE	El plugin es capaz de verificar el servicio, pero que parecía estar por encima de un umbral de "advertencia" o parece no estar funcionando correctamente

Exit status	Estado de Servicio	Estado de Host	Descripción
2	CRITICAL	DOWN/UNREACHABLE	El plugin detecta que o bien el servicio no funciona o que está por encima de un umbral “crítico”
3	UNKNOWN	DOWN/UNREACHABLE	Argumentos de línea de comandos no válida o fallas internas del plugin (por ejemplo error en un socket o DNS) que le impiden realizar las operaciones especificadas

GLOSARIO DE TÉRMINOS

- **ADSL:** Sistema de trasmisión digital sobre hilo de cobre o fibra óptica, que por sus características puede alcanzar velocidades muy superiores a las actuales, gracias al aumento y división del ancho de banda.
- **Alias:** Apodo o Pseudónimo. Nombre corto y fácil de recordar que se utiliza normalmente en los chats.
- **Antivirus:** Programa cuya finalidad es prevenir los virus informáticos, así como curar los ya existentes en el sistema. Estos programas deben actualizarse periódicamente. Ejemplos de antivirus: McAfee, Norton.
- **Aplicación:** Cada uno de los programas que, una vez ejecutados, permiten trabajar con el ordenador. Son aplicaciones los procesadores de textos, hojas de cálculo, bases de datos, programas de dibujo, paquetes estadísticos, etc.
- **BIT:** Es la unidad de información más pequeña. Puede tener sólo dos valores o estados: 0 o 1, encendido o apagado.
- **Byte:** Ocho bits que representan un carácter. Unidad básica de información con la que operan los ordenadores.
- **Caché:** Es una de las memorias del ordenador, muy rápida, que contiene las operaciones más frecuentes o las últimas realizadas con lo que aumenta considerablemente la velocidad de los procesos al evitar en muchos casos el acceso a memorias más lentas.
- **Chip:** Utilizado habitualmente como sinónimo de procesador, se trata de una oblea de silicio sobre la que se imprime un microcircuito.
- **Chip de Memoria:** Chip que contiene programas y datos, ya sea de manera temporal (RAM), permanente (ROM, PROM) o permanentemente hasta que se cambien (EPROM, EEPROM).
- **CL**: (Control Language) y un sistema operativo basado en objetos y bibliotecas, OS/400.
- **CLI**: Command line interface - Línea de comandos.
- **Cliente:** En la filosofía Cliente/Servidor el Cliente es el "solicitante", el que pide datos al servidor.
- **Cliente/Servidor:** Se le suele llamar así a la arquitectura a dos capas, es decir, una capa servidor, u ordenador que contendrá los datos y los programas gestores asociados, y capas clientes, u ordenadores que se dirigirán al anterior para obtener la información.

- **CMIP**[117]: Acrónimo de Common Management Information Protocol - Common Management Information Services
- **CMISE**: Common Management Information Service Element - Elemento de Servicio Común de Información de Gestión
- **CMOT**: Common Management Information Protocol over TCP/IP
- **COBIT**: Control Objectives for Information and related Technology.
- **Cookies:** (Galletas) Cuando se visita una página Web, es posible recibir una Cookie. Este es el nombre que se da a un pequeño archivo de texto, que queda almacenado en el disco duro del ordenador. Este archivo sirve para identificar al usuario cuando se conecta de nuevo a dicha página Web.
- **Cortafuegos**[118]**:** También llamado FIREWALL. Es un ordenador o un programa que conecta una red a Internet pero impide el acceso no autorizado desde Internet.
- **CPU:** Conocida como Unidad Central de Proceso o procesador, es el "cerebro" del ordenador y se encuentra encajado en la Placa Base. Es una de las partes fundamentales del PC y, junto con una serie de chips de apoyo, es el responsable de realizar las operaciones de cálculo que le solicitan los programas y el sistema operativo. También se le denomina Microprocesador.
- **DMZ**: Demilitarized Zone - Zona Desmilitarizada
- **DNS:** Domain Name System. Son unas direcciones simbólicas utilizadas en Internet y que sustituyen a las cadenas de números que son las verdaderas direcciones. Se le conoce también con el nombre de "dominio", aunque no es del todo exacto.
- **Dominio:** Hay dos sistemas principalmente de incluir una dirección de páginas Web en Internet, la utilización de espacios generalmente gratuitos y que "cuelgan" de una empresa de suministros o el alta de una propia. Tanto la suministradora de servicios en su momento como el registro de una dirección propia lo que hacen es registrar un dominio, o un nombre registrador en un ordenador al efecto y que asigna un IP propio.
- **Demo:** Es una "demostración" de un software. Es decir, un programa generalmente de libre reparto para que compruebes su utilidad y la diferencia entre ésta y el programa comercial depende del fabricante.

[117] «CMIP», *Todoexpertos*, accedido 14 de julio de 2012, http://www.todoexpertos.com/categorias/tecnologia-e-internet/redes-de-computadores/respuestas/135528/cmip.
[118] «Qué es un firewall», accedido 29 de agosto de 2012, http://www.desarrolloweb.com/articulos/513.php.

- **Dirección IP:** (Dirección de protocolo de Internet). La forma estándar de identificar un equipo que está conectado a Internet. Consta de cuatro números separados por puntos y cada número es menor de 256; por ejemplo 192.200.44.69. El administrador del servidor Web o su proveedor de servicios de Internet asignará una dirección IP a su equipo.
- **E-mail:** Servicio de comunicaciones que permite el intercambio y almacenamiento de mensajes. En muchos casos sustituye al sistema FTP ya que acepta el envío de ficheros, imágenes, etc. aparte del texto.
- **Enlace:** (Link). Refiriéndonos a Internet y páginas Web es un unión entre varios documentos dentro de un mismo servidor, o con mayor frecuencia, la posibilidad de acceder mediante la pulsación de una palabra o frase, generalmente resaltada y subrayada, a otra página situada en un ordenador distinto y ubicado en cualquier lugar del mundo, ya que en el momento de la creación de ese enlace se le ha asignado la dirección o URL a la que ha de dirigirse.
- **FAQ:** (Frequently Asked Questions). Son las colecciones de preguntas más frecuentes que se realizan y publican las empresas de programación o similares, foros de discusión, etc.
- **FCAPS**[119]: Faults, Configuration, Accounting, Performance, Security
- **Firmware:** Son programas, generalmente responsables de un dispositivo, que tienen como característica común que están almacenados en memoria ROM (Memoria de sólo lectura).
- **Freeware:** Programas, generalmente distribuidos por la red, que se pueden utilizar libremente.
- **FTP:** (File Transfer Protocol). Protocolo para la transferencia de ficheros.
- **Gb:** Mil millones de bits. También Gb, Gbit y G-bit. File Transfer Protocol - Protocolo de Transferencia de Archivos
- **GB:** Es una unidad de medida de memorias. Equivale a 1.024 Mb. También GB, Gbyte y G-byte.
- **GNU**[120]**:** Licencia Publica General. Software desarrollado para distribución sin fines de lucro.

  El proyecto GNU (GNU es un acrónimo recursivo para "GNU No es Unix")

[119] Jhennifer Bastidas, «Fcaps», 10 de marzo de 2011, http://www.slideshare.net/JhenniferBastidas/fcaps-7220464; Wikipedia contributors, «FCAPS», *Wikipedia, la enciclopedia libre* (Wikimedia Foundation, Inc., 24 de junio de 2012), http://es.wikipedia.org/w/index.php?title=FCAPS&oldid=57280262; «FCAPS», accedido 22 de julio de 2012, http://es.scribd.com/doc/17243959/FCAPS; «Fcaps», accedido 22 de julio de 2012, http://www.slideshare.net/JhenniferBastidas/fcaps-7220464.

[120] Wikipedia contributors, «GNU General Public License», *Wikipedia, la enciclopedia libre* (Wikimedia Foundation, Inc., 28 de agosto de 2012), http://es.wikipedia.org/w/index.php?title=GNU_General_Public_License&oldid=59185383.

comenzó en 1984 para desarrollar un sistema operativo tipo Unix completo, que fuera Software Libre. La gente a menudo se refiere erróneamente a estos sistemas como "Linux", cuando es más preciso y concreto llamarlos "GNU/Linux".

- **GNU-GPL**[121]: GNU General Public License - Licencia Pública General de GNU.
- **Hacker:** Informático especializado o con inquietudes de salvar determinados retos complejos. Popularmente se le considera dedicado a la infiltración en sistemas informáticos con fines destructivos.
- **Hardware:** Se denomina así al conjunto de componentes físicos dentro de la informática (un teclado, una placa, por ej.).
- **Hosting:** Palabra del Ingles que quiere decir dar hospedar o alojar. Aplicado al Internet, significa poner una página web en un servidor de Internet para que esta pueda ser vista en cualquier lugar del mundo entero con acceso al Internet.
- **HTML:** Es el lenguaje estándar para describir el contenido y la apariencia de las páginas en el WWW.
- **HTTP**: HyperText Transfer Protocol - Protocolo de Transferencia de Hipertexto. Es el protocolo o las reglas de funcionamiento de los servidores WWW, que son los encargados de mantener este tipo de páginas.
- **HTTPS**: Hypertext Transfer Protocol Secure - Protocolo de Transferencia de Hipertexto Seguro.
- **IEEE**: Instituto de Ingenieros Electricistas y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización.
- **IETF**: Internet Engineering Task Force.
- **IOS**: Sistema de Entrada y Salida (Input Output System). Es el sistema operativo de switches y ruteadores.
- **IPsec**[122]: (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.
- **ISO**: International Organization for Standardization - Organización Internacional para la Estandarización.
- **ISP**: Internet Service Provider - Proveedor de servicios de Internet.
- **ITIL**[123]: Information Technology Infrastructure Library - Biblioteca de Infraestructura de Tecnologías de Información.
- **JFFNMS**[124]: Just For Fun Network Management System.

---

[121] Ibid.

[122] «IPsec», *Wikipedia, la enciclopedia libre*, 1 de noviembre de 2012, http://es.wikipedia.org/w/index.php?title=IPsec&oldid=61021937.

[123] «Service Desk Software– Incident & Problem Management | ITIL V 3.1 Service Desk», accedido 29 de agosto de 2012, http://www.arandasoft.com/solucion_asdk.php.

- **Log**[125]: Notificaciones que envía un agente a un gestor, sin que este le haya solicitado información.
- **Medidas de almacenamiento:**
  - Bit: es la unidad básica de información y sólo dos unidades posibles el 0 y el 1.
  - Byte: es una unidad de información compuesta generalmente por 8 bits.
  - Kilobyte: se abrevia como K o KB y equivale a 1.024 bytes.
  - Megabyte: se abrevia como MB y es igual a 1.024 KB.
  - Gigabyte: se abrevia GB y equivale a 1.024 MB.

- **Megabytes:** Megas o Mb. Unidad de almacenamiento que equivale a 1.024 Kb.
- **Memoria:** Lugar donde se almacenan datos o programas mientras se están utilizando.
- **Memoria RAM:** Es el elemento del ordenador donde se encuentran los datos mientras el usuario los está ejecutando. Cuando apagamos el ordenador la información contenida en la memoria RAM se borra; es por eso por lo que hay que guardar aquello con lo que estamos trabajando (por ejemplo, el texto que estamos escribiendo) en el disco duro justo al empezar, ya que de lo contrario, si el ordenador se apagara accidentalmente, perderíamos todo lo que hemos hecho.
- **Memoria ROM:** Contiene la información necesaria para que el ordenador pueda reconocer todos sus periféricos y arrancar el sistema operativo. Se encuentra en la BIOS y, a diferencia de la memoria RAM, no se llena y se vacía; no se "escribe" en ella, sino que sólo se "leen" sus órdenes.
- **Mhz:** Megahercios. Medida de velocidad del reloj de un ordenador. Un Mhz equivale a un millón de ciclos por segundo.
- **MD5**[126]**:** es un algoritmo de reducción criptográfico de 128 bits ampliamente usado (abreviatura de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5).
- **MIB**[127]: Management Information Base - Base de Información de Gestión
- NMS: Network Monitoring System - Sistema de Monitoreo de Red
- **ODF**: Distribuidor de fibra óptica. Elemento usado como punto de interconexión entre cable de fibra. O también es la extensión de Documentos de OpenOffice, abreviatura de Open Document File.

---

[124] «ProyectoJFFNMS.pdf», s. f.
[125] «Los logs», accedido 29 de agosto de 2012, http://www.desarrolloweb.com/faq/408.php.
[126] «MD5», *Wikipedia, la enciclopedia libre*, 4 de noviembre de 2012, 5, http://es.wikipedia.org/w/index.php?title=MD5&oldid=61091647.
[127] Dr. Víctor J. SOSA-SOSA, «MIB.pdf», accedido 2 de febrero de 2012, http://www.tamps.cinvestav.mx/~vjsosa/clases/redes/MIB.pdf; Desconocido, «MIB.pdf», accedido 17 de enero de 2012, http://www.tamps.cinvestav.mx/~vjsosa/clases/redes/MIB.pdf.

- **OID** Object identifier – identificador de objeto.
- **OSI**[128]: Open Systems Interconnection - Interconexión de Sistemas Abiertos.
- **NOC**[129]: Network Operation Center
- **Nombre de usuario:** Username. No tiene por qué ser el nombre real sino cualquier identificador para el programa que se esté utilizando.
- **NSClient++**[130].- Es un agente para monitoreo de sistemas operativos Windows, este agente tiene la habilidad para funcionar junto con el servicio SNMP para enviar información de procesos, procesador, rendimiento de CPU, etc., hacia el NMS NAGIOS.
- **On-Line:** En línea. Se refiere a cualquier documento, archivo o servicio de la red.
- **P2P**: Point to Point: Es transferencia compartida de archivos entre usuarios de una red. Compartición de archivos de igual a igual
- **Password:** (Contraseña). Se denomina así al método de seguridad que se utiliza para identificar a un usuario.
- **PDU**[131]: Protocol Data Units - Unidades de Datos de Protocolo.
- **PHP**: Hypertext Preprocessor - lenguaje de programación interpretado, diseñado originalmente para la creación de páginas web dinámicas.
- **Proxy:** Dispositivo que realiza una acción en representación de otro. La finalidad más habitual es la del servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.
- **RADIUS** [132] : Remote Authentication Dial-In User Server - protocolo de autenticación y autorización para aplicaciones de acceso a la red.
- **RFC**: Request For Comments - "Petición De Comentarios", serie de notas sobre Internet

[128] Ing. William Marín Moreno, «Modelo OSI», s. f., http://www.ie.itcr.ac.cr/marin/mpc/redes/Modelo_osi_tcp_ip%28oficial%29.pdf; «osi.ppt», accedido 1 de febrero de 2012, http://www.arcesio.net/arquitecturas/osi.ppt; «Modelo_osi_tcp_ip(oficial).pdf», accedido 7 de noviembre de 2011, http://www.ie.itcr.ac.cr/marin/mpc/redes/Modelo_osi_tcp_ip(oficial).pdf.

[129] «NOC.pdf», accedido 6 de enero de 2012, https://nsrc.org/workshops/2004/CEDIA2/material/NOC.pdf; «Centro de Comando - NOC (Centro de Operaciones de Red) (CommandCenter-NOC) por Raritan Americas, Inc. - reporte y descarga», accedido 25 de enero de 2012, http://www.freedownloadmanager.org/es/downloads/CommandCenter-NOC_51971_p/.

[130] «NSClient++», accedido 15 de junio de 2013, http://www.op5.com/agents/nsclient/; «NSClient++», accedido 15 de junio de 2013, http://www.nsclient.org/nscp/.

[131] «Definicion de PDU - ¿qué es PDU?», accedido 6 de septiembre de 2012, http://www.alegsa.com.ar/Dic/PDU.php.

[132] Wikipedia contributors, «RADIUS», *Wikipedia, la enciclopedia libre* (Wikimedia Foundation, Inc., 11 de agosto de 2012), http://es.wikipedia.org/w/index.php?title=RADIUS&oldid=58727330.

- **Router:** Se denomina así al dispositivo capaz de dirigir la información, dividida en paquetes, por el camino más idóneo, examinando la dirección y el destino y utilizando mapas de red.
- **RRDTool**: Round Robin Database tool - herramienta que trabaja con una base de datos que maneja planificación según Round-Robin.
- **Servidor:** Se denomina así al ordenador que se encarga de suministrar lo necesario a una red, dependiendo de cuál sea la finalidad de ésta.
- **SLA**[133]: Service Level Agreement - Acuerdo de nivel de servicio
- **SMFA**: Systems Management Functional Areas
- **SMTP**[134]: Simple Mail Transfer Protocol - Protocolo Simple de Transferencia
- **SNMP**: Simple Network Management Protocol - Protocolo de Gestión de Red Simple.
- **Software:** Conjunto de programas de distinto tipo (sistema operativo y aplicaciones diversas) que hacen posible operar con el ordenador.
- **Spam:** Se denomina con este término al correo electrónico que se recibe de forma indeseada, generalmente con carácter comercial.
- **SSH**[135]: (Secure SHell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.
- **STP**: Spanning Tree Protocol - protocolo de red de nivel 2 de la capa OSI.
- **SysLog**: Estándar de facto para el envío de mensajes de registro en una red informática IP
- **TACACS**[136]: Terminal Access Controller Access Control System - Sistema de Control de Acceso mediante Control del Acceso desde Terminales
- **TCP-IP:** (Transmision Control Protocol-Internet Protocol). Protocolo en el que se basa Internet y que en realidad consiste en dos. El TCP, especializado en fragmentar y recomponer paquetes, e IP para direccionarlos hasta su destino.

---

[133] «Definición De SLA -», accedido 31 de enero de 2012, http://soporte.epoint.es/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=134.

[134] Jeffrey D. Case et al., «A Simple Network Management Protocol (SNMP)», mayo de 1990, http://www.ietf.org/rfc/rfc1157.txt; «¿Que es SNMP, RMON y SMON? - Yahoo! Respuestas», accedido 29 de agosto de 2012, http://es.answers.yahoo.com/question/index?qid=20070618183354AADS2ca; «Tutorial - Simple Network Management Protocol (SNMP)», accedido 4 de julio de 2012, http://www.eogogics.com/talkgogics/tutorials/SNMP/.

[135] «Secure Shell», *Wikipedia, la enciclopedia libre*, 11 de octubre de 2012, http://es.wikipedia.org/w/index.php?title=Secure_Shell&oldid=59882808.

[136] C. Finseth, «An Access Control Protocol, Sometimes Called TACACS», accedido 29 de agosto de 2012, http://tools.ietf.org/html/rfc1492; Wikipedia contributors, «TACACS», *Wikipedia, la enciclopedia libre* (Wikimedia Foundation, Inc., 2 de agosto de 2012), http://es.wikipedia.org/w/index.php?title=TACACS&oldid=58422643.

- **Throughput**: Tasa de transferencia, rendimiento o throughput, se refiere a la tasa efectiva de bits.
- **TIC**: Tecnologías de la Información y Comunicaciones
- **TMN**[137]: Telecommunication Management Network - Red de Gestión de las Telecomunicaciones
- **TOM**: Telecommunication Operation Map - Mapa de Operaciones de Telecomunicaciones
- **Trap**: Una trap es generado por el agente para reportar ciertas condiciones y cambios de estado a un proceso de administración
- **Troubleshooting**[138]: Es la forma sistemática de buscar el origen de un problema para que éste pueda ser resuelto
- **Tutorial:** Libro de instrucciones o programa que guía al usuario a través de una secuencia predeterminada de pasos con el fin de aprender un producto.
- **UDP**: User Datagram Protocol - Protocolo de Datagrama de Usuario
- **UIT-T**: International Telecommunications Union – Telecomunications
- **UNIX:** Es una familia de sistemas operativos para ordenadores personales. Soporta gran número de usuarios y posibilita la ejecución de distintas tareas de forma simultánea (multiusuario y multitarea). Su facilidad de adaptación a distintas plataformas y la portabilidad de las aplicaciones (está escrito en lenguaje C) que ofrece hacen que se extienda rápidamente.
- **URL:** Se conoce por este nombre a las direcciones dentro de Internet, normalmente, aunque no necesariamente, refiriéndonos a páginas Web. El tipo más común de dirección URL es http://direcciónweb, que proporciona la dirección Internet de una página Web.
- **USB:** Bus serie universal. La característica principal de este bus reside en que los periféricos pueden conectarse y desconectarse con el equipo en marcha, configurándose de forma automática.
- **USM**: User-Based Security Model.
- **Web:** Por éste término se suele conocer a WWW (World Wide Web), creado por el Centro Europeo de Investigación Nuclear como un sistema de intercambio de información y que Internet ha estandarizado. Supone un medio cómodo y elegante, basado en multimedia e hipertexto, para publicar información en la red. Inicial y básicamente se compone del protocolo http y del lenguaje HTML.
- **WebMail:** Es un email basado en web. Una cuenta de correo que puede enviar, recibir y leerse desde cualquier lugar mediante un navegador web.

[137] Telecomunications Management Network, «tmn.pdf», accedido 7 de febrero de 2012, http://www.hit.bme.hu/~jakab/edu/litr/TMN_EMS/tmn.pdf.
[138] «Service Desk Software– Incident & Problem Management | ITIL V 3.1 Service Desk».

- **Webmaster:** Es la persona o personas que crean, diseñan, organizan y gestionan una página web (lo que vemos en Internet).
- **WI-FI:** (Wireless Fidelity). Tecnología relativamente estandarizada para redes inalámbricas que utilizan ondas de radio de corto alcance.
- **Wireless:** Redes sin hilos. Las redes sin cables permiten compartir periféricos y acceso a Internet.
- **Windows:** Sistema operativo de 32 bits, de Microsoft, elaborado al estilo de ventanas y sistema gráfico (tradicionalmente utilizado por otros sistemas). El más utilizado actualmente es el Windows XP.
- **WWW:** (World Wide Web). Telaraña o malla mundial. Sistema de información con mecanismos de hipertexto creado por investigadores del CERN. Los usuarios pueden crear, editar y visualizar documentos de hipertexto.