



**UNIVERSIDAD DE LA FRONTERA
FACULTAD DE INGENIERÍA, CIENCIAS Y ADMINISTRACIÓN
DEPARTAMENTO DE INGENIERÍA DE SISTEMAS**

**PROGRAMA DOCENTE ESPECIAL INGENIERIA INFORMATICA PARA INGENIEROS DE
EJECUCIÓN EN INFORMÁTICA Y/O COMPUTACIÓN**

**SISTEMA DE MONITOREO DE SERVICIOS INTERNET
DE ALTA DISPONIBILIDAD**

SYLVIA ELIANA ALARCÓN CASTILLO

- 2009 -

II
A321 s
2009
C.1



**UNIVERSIDAD DE LA FRONTERA
FACULTAD DE INGENIERÍA, CIENCIAS Y ADMINISTRACIÓN
DEPARTAMENTO DE INGENIERÍA DE SISTEMAS**

**PROGRAMA DOCENTE ESPECIAL INGENIERÍA INFORMÁTICA PARA INGENIEROS DE
EJECUCIÓN EN INFORMÁTICA Y/O COMPUTACIÓN**

**SISTEMA DE MONITOREO DE SERVICIOS INTERNET
DE ALTA DISPONIBILIDAD**

**TRABAJO PARA OPTAR AL TÍTULO DE
INGENIERO INFORMÁTICO**

87845



Profesor Guía: Sr. RICARDO A. RIVERA N.

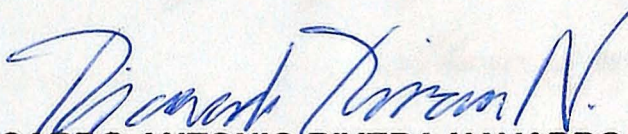
SYLVIA ELIANA ALARCÓN CASTILLO

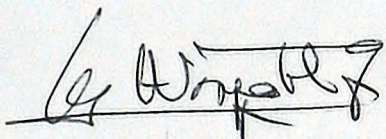
- 2009 -

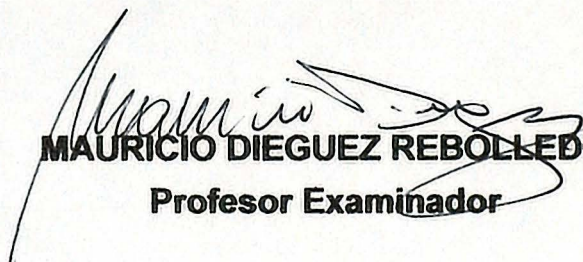
**SISTEMA DE MONITOREO DE SERVICIOS INTERNET
DE ALTA DISPONIBILIDAD**

SYLVIA ELIANA ALARCÓN CASTILLO

COMISIÓN EXAMINADORA


RICARDO ANTONIO RIVERA NAVARRO
Profesor Guía


GERARDO VORPHAL GROLLMUS
Profesor Examinador


MAURICIO DIEGUEZ REBOLLEDO
Profesor Examinador

Nota trabajo escrito	: 6,3
Nota examen	: 6,3
Nota final	: 6,3

Dedicatoria

A Jesús, por su infinito e incondicional amor por mí.

*Al único y sabio Dios, nuestro Salvador,
Sea gloria y majestad, imperio y potencia,
Ahora y por todos los siglos.
Amén.*

Judas 1:25

AGRADECIMIENTOS

Un par de líneas no alcanzan a contener y reflejar los sentimientos
que se producen al finalizar una etapa,
y todo lo que se involucró en ella.

Agradezco a la empresa Datacare Ltda
por permitir mi desarrollo profesional y personal.

Al equipo coordinador de este Programa Académico, por su apoyo y ayuda.

A Ricardo Rivera, mi profesor guía,
por su dedicación y apoyo ... gracias por creer en mí.

A cada persona que de una u otra forma se hizo parte de este proyecto.

A mi familia y a todos

Gracias!

RESUMEN

En este Trabajo de Título se explica la implementación de un sistema de monitoreo de servicios de alta disponibilidad para la empresa Datacare Ltda. Se detallan las características que debe tener y lo que se espera obtener de él.

Este trabajo está estructurado en los siguientes capítulos:

1. Introducción: Este capítulo describe la problemática del proyecto, se describe la empresa en la que se realiza este trabajo, se enuncian los objetivos, límites y fronteras del proyecto.
2. Fundamentos Teóricos: Este capítulo describe la terminología y los fundamentos teóricos relacionados con la gestión de servicios, y en particular con el monitoreo de redes y servicios, los cuales se necesitan conocer para el desarrollo del presente proyecto.
3. Desarrollo: Este capítulo describe las alternativas revisadas y la que finalmente fue escogida para la implementación. Se presentan también las funcionalidades esenciales a implementar en este esquema.
4. Discusión y Resultados: En este capítulo se explican algunos problemas encontrados en la instalación del software y los resultados obtenidos.
5. Conclusiones y Trabajo Futuro: Este capítulo resume las conclusiones respecto del trabajo realizado y describe aspectos a considerar para el desarrollo de trabajos posteriores relacionados con el tema.

ÍNDICE DE CONTENIDOS

CAPITULO I - INTRODUCCIÓN

1. Introducción	1
1.1 Antecedentes del Problema	2
1.1.1 Exposición General del Problema	2
1.1.2 Nivel Actual del Problema	3
1.2 Antecedentes de la Empresa	11
1.2.1 Estructura Organizacional de Datacare Ltda.	12
1.3 Objetivos	14
1.3.1 Objetivo General	14
1.3.2 Objetivos Específicos	14
1.4 Límitaciones y Fronteras	14
1.5 Conclusión del Capítulo	14

CAPÍTULO II - FUNDAMENTOS TEÓRICOS

2. Fundamentos Teóricos	15
2.1 Marco Teórico	15
2.2 Conclusión del Capítulo	27

CAPÍTULO III - DESARROLLO

3. Desarrollo	28
3.1 Requerimientos de la aplicación	28
3.2 Requerimientos de plataforma	30
3.3 Alternativas de solución	30
3.3.1 Monitoreo Externo	30
3.3.2 Monitoreo Externo Internacional	32
3.4 Implementación	38
3.5 Conclusión del Capítulo	44

CAPÍTULO IV – DISCUSIÓN Y RESULTADOS

4 Discusión y Resultados	45
4.1 Resultados	45
4.2 Estimación de Costos	45
4.3 Conclusión del Capítulo	46

CAPÍTULO V – CONCLUSIONES Y TRABAJO FUTURO

5 Conclusiones y Trabajo Futuro	47
5.1 Conclusiones	47
5.2 Trabajo Futuro	48

BIBLIOGRAFÍA

Bibliografía Referenciada	50
Bibliografía Consultada	51

ANEXOS

ANEXO A - Inicio de Datacare Ltda	52
ANEXO B – Instalación de Nagios	54
ANEXO C – Screenshots de Nagios	59

ÍNDICE DE FIGURAS

Figura 1.1 Registro detallado de incidentes	7
Figura 1.2 Organigrama de la Empresa	13
Figura 2.1 Interacción de los procesos de negocios	20
Figura 2.2 Fases del manejo de incidentes	22
Figura 2.3 Fases del control de errores	23
Figura 2.4 Proceso de manejo de configuraciones	24
Figura 2.5 Proceso de manejo de cambios	25
Figura 2.6 Proceso de manejo de liberaciones	26
Figura 3.1 Presentación Atentus.com	31
Figura 3.2 Red Operativa Atentus	32
Figura 3.3 Interfaz de acceso	33
Figura 3.4 Archivos de configuración de Nagios	40
Figura 3.5 Funcionamiento Addon NRPE	41
Figura 3.6 Funcionamiento Addon NSCA	42
Figura 3.7 Funcionamiento Addon NDOUtils	42
Figura 3.12 Esquema de Fallas para Servidor Maestro	36

ÍNDICE DE TABLAS

Tabla 1.1 Tiempos de uptime	9
Tabla 1.2 Cálculo de uptime	10
Tabla 3.1 Recopilación herramientas en Wikipedia	34
Tabla 3.2 Comparativa herramientas según Wiki	36

CAPÍTULO I INTRODUCCIÓN

INTRODUCCIÓN

En el contexto del mundo actual, en el que la informática gira en torno al concepto de red, el trabajo de los administradores de red es muy complejo, al punto de volverse inmanejable para ciertos tamaños de red sin un buen sistema de supervisión o monitoreo. La misión de los administradores de red consiste en mantener en funcionamiento recursos tales como encaminadores (routers), concentradores de cableado (hubs o switches), servidores, así como cada dispositivo crítico que conforma la red y principalmente mantener en funcionamiento algunas aplicaciones y servicios. Estos dispositivos y aplicaciones deben funcionar en forma continua y si se trata de dispositivos o aplicaciones muy críticas, es importante actuar rápidamente frente a fallas o síntomas de fallas. En otras palabras, la misión de un administrador de red es mantener funcionando en condiciones óptimas la red durante el mayor tiempo posible.

Para lograr esto es importante contar con la información al instante de lo que está sucediendo y ser alertado en caso de eventos negativos, es por eso que el monitoreo constante de los sistemas de comunicación y aplicaciones es fundamental para mantener la disponibilidad de los servicios.

Hay gran cantidad de motivos por los cuales un administrador necesita monitorear sus redes y servicios, entre otros: la utilización del ancho de banda, el estado de funcionamiento de los enlaces, la detección de cuellos de botella y problemas con el cableado, administrar la información de enrutamiento entre máquinas, funcionamiento de los servicios, etc.. Además el monitoreo de los servicios en la red es un buen punto desde el cual comenzar el estudio de los problemas de seguridad.

En el presente trabajo se toma como punto de partida el sistema de monitoreo que ya existe en la empresa, para conocer sus falencias y sus virtudes, con el fin de que el nuevo sistema responda a las necesidades de acuerdo a la evolución que el mercado requiere.

Antecedentes del Problema

1.1.2 Nivel Actual del Problema

1.1.1 Exposición General del Problema

Para una empresa cuyo negocio es la prestación de servicios, tanto o más importante que instalar y dejar operativo uno de ellos, es asegurarse que funcione correctamente, y en caso de presentarse una falla o interrupción detectarla a tiempo y reaccionar rápidamente. Es por eso que este trabajo surge de la necesidad de mejorar el sistema de monitoreo de la red de servidores y servicios de la empresa.

La palabra “monitoreo” no tiene una definición exacta, pero en el contexto computacional ha adquirido gran auge, específicamente en el área de redes y seguridad y se puede decir que el monitoreo consiste en velar por el buen funcionamiento de un sistema, analizando su comportamiento ojala en tiempo real o lo más preciso posible. Desde esta perspectiva la automatización de este proceso cobra gran relevancia minimizando tiempos de espera, o entre revisiones, incluso la probabilidad de errores.

Un aspecto importante en el proceso de monitoreo y gestión de una red es mantener registros de esta, es decir, documentación y estadísticas, tanto de los dispositivos que conforman la red (estado, actividad, conectividad, etc.) como del uso mismo de la red. Además es importante incluir un sistema de reportes mediante el cual se pueda conocer información instantánea o histórica, además de un método de notificación de problemas para los usuarios.

Todo esto permite identificar problemas y realizar acciones preventivas, también permite visualizar el estado general de una red y sus servicios, es decir, si la red está sobre dimensionada o saturada, o bien conocer cuáles son los puntos de falla. La documentación y recopilación de información, es algo necesario en todo tipo de red y ayuda en la toma de decisiones en cuanto a compras, expansiones o reducciones basándose en estudios sobre la historia de la red y su utilización presente y futura.

1.2 Nivel Actual del Problema

Las empresas prestadoras de servicios están sujetas a cumplir con ciertos niveles de servicios tanto en el ámbito del desempeño, de la seguridad y de la disponibilidad, estos niveles se encuentran estandarizados o normados, siendo la disponibilidad un indicador principal.

En el contrato de prestación de servicios quedan estipulados los niveles de calidad y disponibilidad esperados y las multas asociadas a ellos.

A continuación se muestra como ejemplo un extracto de un contrato donde se estipulan los valores de las multas en caso de cortes de servicios.

Multas

Si el contratista no diere cumplimiento a cualquiera de las obligaciones contraídas en los plazos indicados en el contrato respectivo, el contratante aplicará multas en conformidad a la tabla que a continuación se transcribe:

- a) Disponibilidad: Cuando el servicio total, durante el período a facturar, tuviera una disponibilidad menor a la requerida, se le aplicará un porcentaje de multa sobre el valor bruto total del período, calculado en base a la siguiente tabla:

Porcentaje de multa	Disponibilidad del Servicio
0%	DR >= 99.5%
20%	99% <= DR < 99,5%
50%	90% <= DR < 99%
100%	DR < 90%

Donde DR = Disponibilidad Real medida durante el mes

- b) Caídas del servicio: Ante la caída del servicio contratado y la demora en la reposición del mismo sobrepase los plazos estipulados en el punto 4 de las Bases Técnicas, el contratista deberá pagar una multa del CINCO POR CIENTO (5%) del valor bruto mensual por cada hora de atraso.

En la actualidad la empresa posee una granja de más de 30 equipos, entre servidores y dispositivos de red.

Esto hace que se torne imprescindible tener un control constante sobre ellos, obtener fotografías o instantáneas del estado, además manejar información histórica y llevar un registro de incidencias

La empresa posee un sistema de monitoreo funcionando, y aunque cubre las necesidades esenciales, requiere ser mejorado, porque al ir creciendo la red y los servicios y estos a su vez van aumentando su complejidad, los requerimientos internos y de los clientes, también van en aumento y se van afinando necesitándose un sistema que cada vez sea más inteligente y confiable.

La actual herramienta utilizada posee algunas grandes falencias o desventajas que deben ser mejoradas:

- No continua desarrollándose bajo licencia GPL, de este producto ha derivado otro comercial, lo que implica el pago de la licencia del producto, más contratos anuales.
- No tiene manejo de eventos, esto quiere decir que no tiene la capacidad de responder, o tomar ciertas acciones correctivas previamente definidas frente a algunas fallas, por ejemplo intentar reiniciar automáticamente un servicio si este no responde.
- Realiza un chequeo secuencial de las máquinas y servicios. La desventaja de esta forma de chequeo, es que no hay un intervalo definido de monitoreo para cada servicio sino más bien un listado general de todas las máquinas y los servicios a ser monitoreados. Este punto es de vital importancia para los índices de disponibilidad, ya que al detectar una falla, si bien es cierto envía la notificación, si el problema era algo pasajero que no requería de intervención para solucionarse, sólo una vez termine de realizar la revisión del

listado y vuelva a iniciar la secuencia, se dará cuenta que el servicio se restableció, quedando un lapso de tiempo el servicio marcado como no disponible, cuando quizás el problema fue un corte de sólo segundos. El tiempo que toma revisar el listado no es constante, ya que va a depender de cómo responda cada test o prueba de servicio, por lo que un servicio puede estar siendo monitoreado en intervalos de 5 o 10 minutos generalmente.

- No se pueden establecer prioridades en los servicios. Unido al punto anterior, no es posible discriminar cuando un servicio requiere ser monitoreado cada 1 minuto, si es de alta prioridad, o quizás cada 20 minutos, si es una máquina o servicio de baja prioridad.
- Interfaz. Si bien es cierto la interfaz web es útil y puede presentar toda la información requerida, no tiene una interfaz simplificada para acceso desde celulares, lo que dificulta la lectura y visualización de los estados de los servicios desde la mayoría de los dispositivos móviles.

Ejemplo de una vista instantánea de los servicios vía web.

	conn	dns	ftp	http	pop3	postgres	smtp	sybase
Maquina1			-			-	-	
Maquina2		-	-	-		-		-
Maquina3		-	-		-	-	-	-
Maquina4		-	-		-		-	-
Maquina5		-	-	-	-	-		-
Maquina6		-	-		-	-	-	-
Maquina7		-	-		-	-	-	-
Maquina8		-	-		-		-	-
.....								
MaquinaN		-	-		-	-	-	-

El color verde indica que el servicio se encuentra funcionando en buenas condiciones, el color morado, indica que de ese servicio no hay información reciente, ya sea porque dejó de ser monitoreado, o por otro motivo, este color no genera notificaciones. Cuando un servicio no se encuentra disponible el color cambia a rojo enviando inmediatamente una notificación.

Ejemplo de un reporte de disponibilidad generado por la herramienta en un periodo de tiempo.

	conn	dns	ftp	http	pop3	postgres	smtp	sybase
Maquina1		99.91	-			-	-	
Maquina2		-	-	-		-		-
Maquina3		-	-		-	-	-	-
Maquina4		-	-		-		-	-
Maquina5	99,65	-	-	-	-	-	99,66	-
Maquina6		-	-	99,98	-	-	-	-
Maquina7	99,98	-	-	99,97	-	-	-	-
Maquina8		-	-		-		-	-
.....								
MaquinaN		-	-		-	-	-	-

Para el caso de este reporte, el único color que puede ser visualizado es el verde, que representa el 100% si hay un número distinto a este, aparece el número que corresponda.

Al pinchar en cada cuadro se puede obtener mayor detalle sobre el uptime, datos tales como fecha, hora y duración de las caídas como se aprecia en el siguiente ejemplo:

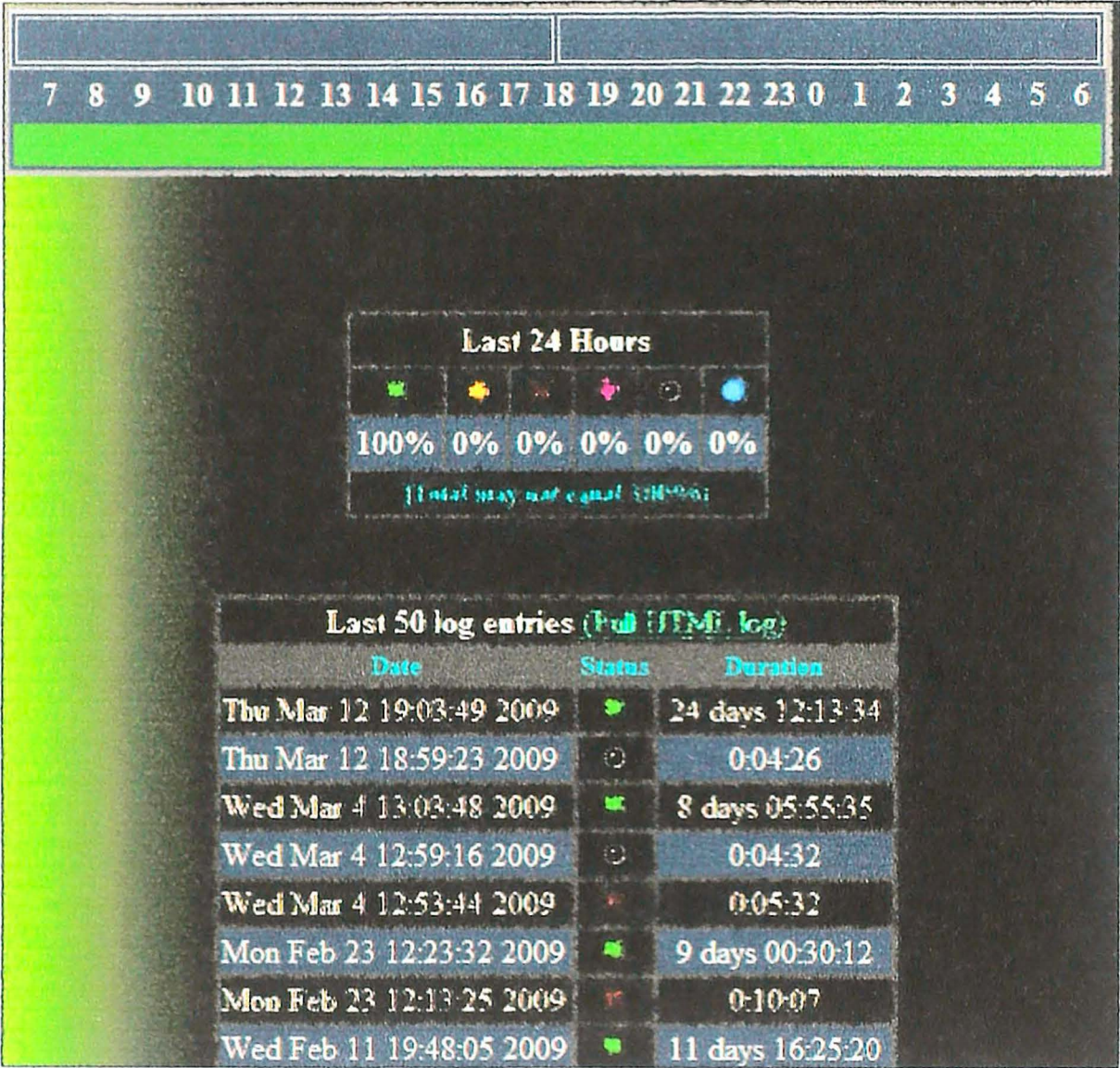


Figura 1.1 Registro detallado de incidentes

En la imagen se puede ver para cada evento o cambio de estado la respectiva fecha, y hora cuando se produce y la duración del estado.

Hay datos que han sido eliminados, por ejemplo aquellos que identifiquen en la realidad a la máquina o al servicio.

Al momento de presentar una propuesta de servicio se dejan establecidos ciertos tanto los niveles de servicio, como algunos tiempos de respuesta que el cliente debe esperar

por parte de la empresa, esto es, los tiempos de respuesta ante caídas o problemas en el servicio. Estos tiempos se definen como tiempos máximos esperados y van a depender de la gravedad o tipo de problema que se haya presentado con el servicio.

Un ejemplo de cómo se presenta este punto en una propuesta es el siguiente:

NIVELES DE SERVICIO

Datacare asegura un servicio 24x7. Datacare realiza monitoreos automáticos 24x7 a la conectividad de las máquinas y servicios, por lo que, en caso de fallas, cuenta con procedimientos de contingencia que permiten recuperar el servicio en el menor tiempo posible. Además, existe un teléfono de apoyo técnico y una cuenta de correo electrónico para reportar los incidentes y las soluciones de los mismos. Los tiempos asociados a la resolución de problemas tienen relación con las características del mismo. De lo anterior se obtienen los siguientes tiempos de solución:

- ✓ Indisponibilidad total del servicio, máximo 4 horas
- ✓ Eventos Intermedios, indisponibilidad parcial, máximo 2 horas
- ✓ Reconfiguraciones, menor a 8 horas
- ✓ Consultas e información, menor a 2 horas

Lo anterior considera tiempos máximos para solucionar cualquier tipo de incidente. En la mayoría de los casos, el tiempo es considerablemente menor al máximo. En caso de exceder este tiempo, Datacare se compromete a entregar una solución consistente en un servidor totalmente configurado con las características de los servidores pertenecientes a la presente propuesta, disponible para ser levantado inmediatamente en caso de que sea necesario, en reemplazo hasta que el servicio esté operativo. Lo mismo en lo que respecta a la conectividad.

Desde el punto de vista económico, las multas asociadas a cortes de servicios son altas ya que representan un perjuicio al cliente por no estar su servicio disponible. Las multas varían de un proyecto a otro, pero en promedio pueden alcanzar un monto cercano a 1UF por cada hora de corte por sobre el uptime contratado.

¿Qué es el uptime?

El uptime se define como el tiempo que un sistema o servicio se encuentra disponible para su uso normal. A pesar de ser una medida de tiempo, generalmente se expresa en términos de porcentajes.

Aparte de la cantidad de horas, un contrato de prestación de servicios tiene definido el horario en que ese uptime es primordial, por ejemplo, si el contrato dice:

- 24x7 equivale a “24 horas al día, 7 días a la semana”
- 24x5 equivale a “24 horas al día, 5 días a la semana”
- 12x5 equivale a “12 horas hábiles, 5 días a la semana”
- 8x5 equivale a “8 horas hábiles, 5 días a la semana”

El uptime se calcula para cada uno de los casos anteriores.

Para efectos de este trabajo, se considera que el servicio se presta 24x7.

Si se considera un mes de 30 días, se tiene una cantidad de 720 horas/mes que es el 100%.

De este dato se desprende la siguiente tabla con los niveles de uptime más utilizados y las horas que es permitido no esté disponible el servicio del cliente.

	Horas disponibles	Horas de corte permitido
99,7%	717,8 h/mes	2,2 h/mes
99,5%	716,4 h/mes	3,6 h/mes
99%	712,8 h/mes	7,2 h/mes
98,5%	709,2 h/mes	10,8 h/mes
98%	705,6 h/mes	14,4 h/mes
97,9%	704,9 h/mes	15,1 h/mes
97%	698,4 h/mes	21,6 h/mes

Tabla 1.1 Tiempos de uptime

Existe un mito dentro de las empresas u organizaciones de prestación de servicios, es el “Mito de los cinco nueves”. Este mito dice que es imposible ofrecer un uptime de cinco nueves. En el sitio <http://basicstate.com/htm/9999.htm> se muestra la siguiente tabla.

Uptime	year days	hh:mm:ss	month days	hh:mm:ss	day hh:mm:ss
99.9990	0	00:05:15	0	00:00:27	00:00:01
99.9900	0	00:52:34	0	00:04:28	00:00:09
99.9000	0	08:45:36	0	00:44:38	00:01:26
99.0000	3	15:36:00	0	07:26:24	00:14:24
98.0000	7	07:12:00	0	14:52:48	00:28:48
97.0000	10	22:48:00	0	22:19:12	00:43:12
96.0000	14	14:24:00	1	05:45:36	00:57:36
95.0000	18	06:00:00	1	13:12:00	01:12:00
94.0000	21	21:36:00	1	20:38:24	01:26:24
93.0000	25	13:12:00	2	04:04:48	01:40:48
92.0000	29	04:48:00	2	11:31:12	01:55:12
91.0000	32	20:24:00	2	18:57:36	02:09:36
90.0000	36	12:00:00	3	02:24:00	02:24:00

Tabla 1.2. Cálculo de uptime

Construir y mantener plataformas de alta disponibilidad es caro y complejo, tanto en lo económico como en los conocimientos técnicos que se requieren para ello.

1.2 Antecedentes de la empresa.

Datacare Ltda. es una empresa creada en el año 2004 e integrada por personas con 7 años de experiencia en el área de webhosting y afines, y que conformaban el área de Servicios Internet en el Instituto de Informática Educativa (IIE), de la Universidad de La Frontera en Temuco.

Encabeza la empresa un Gerente General y las actividades se organizan por áreas, las cuales están a cargo de la gestión de los distintos proyectos de la empresa.

La empresa Datacare Ltda., tiene como misión el potenciar a las organizaciones públicas o privadas, mediante el uso de tecnologías de Internet para apoyar y mejorar la gestión de sus negocios a través del mejor servicio del mercado, adaptable a las necesidades de cada cliente.

La empresa Datacare Ltda., busca cumplir su misión desarrollándose como una empresa de servicios de primer nivel basándose principalmente en los siguientes lineamientos:

- Asegurar el funcionamiento de los servicios proporcionados a los clientes, responsablemente, a través del uso de la mejor tecnología disponible.
- Mantener un trato directo y personalizado con los clientes para anticipar la identificación de nuevas necesidades, además de mantener informado a los clientes del estado y funcionamiento de sus servicios.
- Realizar permanentemente investigación y desarrollo de tecnologías de información y comunicaciones (TIC), para la mejora de los servicios.

1.2.1 Estructura Organizacional de Datacare Ltda.

La empresa se divide en tres grandes áreas las cuales se describen a continuación:

- **Gerencia General:** Encabezada por un Gerente General. Planifica, coordina y controla las distintas áreas y los proyectos de la empresa, lleva a cabo los lineamientos del plan estratégico de la empresa y es apoyado por un asistente administrativo. Otras tareas que desempeña es el tema de facturación y cobranza de los proyectos.
- **Área Operaciones:** Es encabezada por un Gerente de Operaciones y está cargo de realizar todas las tareas relacionadas con la implementación y operación de los servicios de redes, servidores y servicios. Manejo de configuraciones, también respaldos y estadísticas de los sistemas entre otros.
- **Área de Sistemas:** Es encabezada por un Gerente de Sistemas y está cargo de realizar todas las tareas relacionadas con el servicio de administración de bases de datos, mantención y administración de los sistemas entre otros.

En forma transversal a cada área existe una componente llamada "Calidad e Investigación" que es una tarea cuyo objetivo es la mejora de los procesos internos de la empresa y la investigación para la aplicación de nuevas tecnologías Internet que puedan abrir nuevas líneas de negocio de la empresa.

El presente trabajo se desarrolla en el área de Operaciones de la empresa.

La Figura 1.2 muestra el organigrama que representa la distribución de las áreas dentro de la empresa.

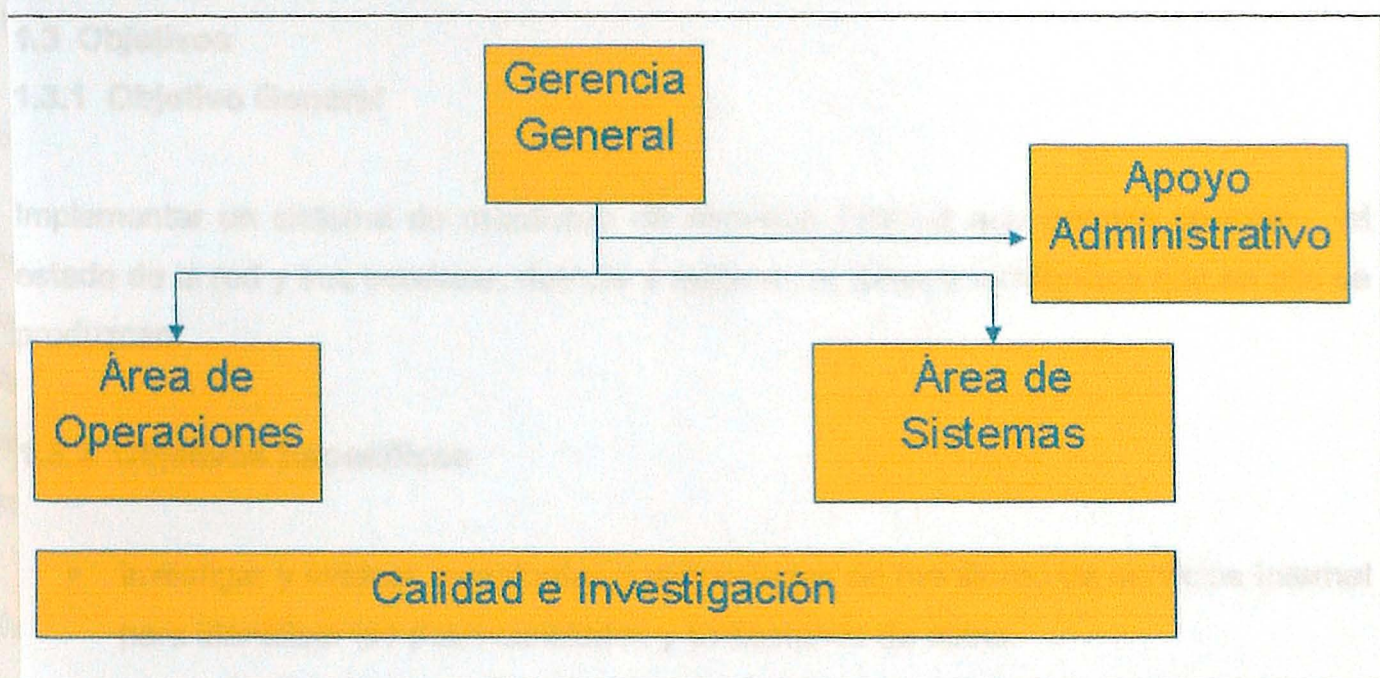


Figura 1.2 Organigrama de la Empresa

1.3 Objetivos

1.3.1 Objetivo General

Implementar un sistema de monitoreo de servicios Internet que permita conocer el estado de la red y sus servicios, detecte y registre las fallas o incidencias que en ella se produzcan.

1.3.2 Objetivos Específicos

- Investigar y evaluar tecnologías y aplicaciones de monitoreo de servicios Internet para identificar las potencialidades y limitaciones de estas.
- Implementar un sistema de monitoreo que se adecue a las necesidades de la empresa.
- Probar el sistema en un ambiente real de explotación de servicios Internet.

1.4 Limitaciones y Fronteras

El presente trabajo se desarrolla con los recursos disponibles del área de operaciones, tanto en recurso humano como en equipamiento. Por lo mismo, la implementación se hará sobre equipamiento ya existente. Es requerimiento de la empresa utilizar software de libre distribución. El sistema de monitoreo sólo es utilizado internamente en la empresa, no descartando en futuras versiones acceso a los clientes.

1.5 Conclusión del Capítulo

Este capítulo muestra el ámbito de trabajo del proyecto, se definen el objetivo general y los objetivos específicos que darán las líneas a seguir para conseguirlos.

2 FUNDAMENTOS TEÓRICOS

2.1 Conceptos Teóricos

Los avances en las tecnologías de la información han tenido un gran impacto en el mundo actual, tanto a nivel personal como a nivel empresarial. La información es un recurso valioso que puede ser utilizado de muchas maneras y que puede ser almacenado y transmitido de manera eficiente. En este capítulo se abordarán los conceptos teóricos que sustentan la gestión de la información y se explorarán las herramientas y técnicas que se utilizan para gestionar la información de manera efectiva.

Los conceptos teóricos que sustentan la gestión de la información son: la información, la comunicación, la gestión de la información, la tecnología de la información y la gestión de la tecnología de la información. Estos conceptos se relacionan entre sí y forman una base teórica para la gestión de la información.

CAPÍTULO II FUNDAMENTOS TEÓRICOS

Una vez que se han definido los conceptos teóricos, es necesario establecer los objetivos de la gestión de la información. Los objetivos de la gestión de la información son: la creación de la información, la organización de la información, la almacenamiento de la información, la recuperación de la información y la difusión de la información. Estos objetivos se relacionan entre sí y forman una base teórica para la gestión de la información.

A medida que las organizaciones van creciendo y ganando experiencia con la tecnología de la información, se van desarrollando las habilidades y técnicas necesarias para gestionar la información de manera efectiva. En este capítulo se abordarán los conceptos teóricos que sustentan la gestión de la información y se explorarán las herramientas y técnicas que se utilizan para gestionar la información de manera efectiva.

2 FUNDAMENTOS TEÓRICOS

2.1 Marco Teórico

Los avances en las Tecnologías de la Información han tenido durante la última década un enorme efecto sobre el mercado empresarial. La aparición de hardware cada vez más potente, software de gran calidad y redes muy rápidas, todos ellos conectados entre sí a escala mundial, ha permitido a las organizaciones desarrollar en mayor grado sus productos y servicios y comercializarlos en menor tiempo. Estos cambios han marcado la transición entre la era industrial y la era de la información, en la que todo está conectado y funciona de un modo más rápido y dinámico.

Las organizaciones tradicionalmente jerárquicas suelen tener dificultades para responder a los rápidos cambios del mercado, lo que obliga a adoptar estructuras más flexibles, dando paso a procesos horizontales, teniendo cada vez mayor capacidad de decisión los empleados. Es en este contexto que surgen los procesos de trabajo para Gestión de Servicios TI.

Una ventaja importante de las organizaciones orientadas a procesos es que estos pueden ser diseñados para facilitar una metodología con orientación al cliente, lo que mejora considerablemente la alineación entre las organizaciones TI (responsables de suministrar información) y los clientes (responsables de usar estos sistemas de información en sus negocios).

A medida que las organizaciones han avanzado y ganado experiencia con la metodología orientada a procesos de la Gestión de Servicios TI, se ha vuelto imperiosa la necesidad que sea coherente la gestión de estos procesos tanto dentro como fuera de estas.

La creciente importancia de la información para las empresas hace que éstas sometan la calidad de sus servicios de información a requisitos internos y externos cada vez más estrictos. Los estándares desempeñan un rol importante, mientras que los marcos de trabajo de “Mejores Prácticas” contribuyen al desarrollo de un sistema de gestión que satisfaga los requisitos exigidos. Una organización que no controle sus procesos no podrá conseguir buenos resultados en el Ciclo de Vida del Servicio ni en la gestión de estos. Lo mismo ocurre si no dispone de una buena organización interna.

Es por esto, entre otros motivos que se puede afirmar que se vive una evolución en el concepto de la Administración de las Tecnologías de Información. De considerar las TI desde el punto de vista puramente tecnológico, a considerarlas como habilitadoras del negocio, enfocándose en las necesidades y requerimientos del negocio mediante la integración de las TI con los procesos de negocio.

Esto se puede resumir en los siguientes conceptos:

- Los resultados financieros de una empresa son el resultado directo de sus procesos de negocio.
- Los procesos de negocio son dependientes y automatizados por los Servicios y Sistemas de TI
- La madurez y los controles de los procesos de TI impactan directamente sobre los Servicios de TI.
- Los profesionales de TI tienen un impacto directo sobre la consistencia de los procesos de TI.

Teniendo en cuenta estos conceptos se puede afirmar que:

- No existe una separación entre el proceso de negocio y la tecnología que lo soporta.
- Las organizaciones de TI deben entender qué Servicios proveen e implementar los procesos que soportan esos Servicios.

- El negocio y las regulaciones externas exigen a las organizaciones de TI que comprendan qué componentes de tecnología soportan a los Servicios de TI.
- La Gobernabilidad de TI y las estructuras de administración deben estar bien definidas para administrar tanto los Servicios como los procesos, de tal forma de eliminar los silos existentes de administración puramente tecnológica.

Para poder entender la concepción de una organización de TI basada en Servicios, es importante definir qué es un Servicio TI.

Servicio TI:

Una o más capacidades técnicas o profesionales de TI que habilitan un proceso de negocio. Un Servicio TI tiene las siguientes características:

- Cumple con una o más necesidades del cliente
- Soporta los objetivos de negocio del cliente
- Es percibido por el cliente como un todo coherente o un producto consumible.

Mediante esta definición un Servicio es una capacidad, no sólo una solución tecnológica o un dominio vertical como una aplicación de negocio o un servidor de aplicaciones.

Cuando se definen los Servicios de TI es necesario entender que existen básicamente dos tipos de Servicios TI. Estos se clasifican en Servicios “Técnicos” o “Profesionales”.

Un “Servicio Técnico” es definido como una capacidad tecnológica que el cliente consume o usa con el propósito de facilitar un proceso de negocio o una función. O un componente de Servicio que soporta a otro Servicio TI de cara al cliente. Los Servicios Técnicos podrían considerar tanto a los Servicios de Aplicaciones como a los Servicios de Infraestructura.

Ejemplos de Servicios Técnicos

Servicios generales de Infraestructura tales como:

- Mensajería/Email
- Servicios de Impresión
- Acceso a la Red o Internet

- Voice Communications
- Application Hosting
- Storage Management

- Servicios basados en Aplicaciones tales como:

- Sistemas de Administración Financiera
- Sistemas de Recursos Humanos

Un “Servicio Profesional” se define como las actividades de valor agregado que el personal de TI provee para soportar, mantener, monitorear o asegurar la entrega consistente y confiable de los Servicios Técnicos.

Ejemplos de Servicios Profesionales:

- Arquitectura de TI e Ingeniería
- Seguridad de TI
- Soporte de TI
- Servicios de Administración de Proyectos
- Consultoría de TI
- Desarrollo de Aplicaciones y Mejoramiento de Servicios

Es muy importante que la organización dedique un tiempo para definir los Servicios Profesionales, ya que en la gran mayoría de las organizaciones más del 60% del presupuesto anual de TI es gastado en estas actividades.

¿QUÉ ES ITIL?

ITIL es la sigla de una metodología desarrollada a fines de la década de los 80 por iniciativa del gobierno del Reino Unido, específicamente por la OGC u Oficina Gubernamental de Comercio Británica (Office of Government Commerce). Las siglas de ITIL significan (Information Technology Infrastructure Library) o Biblioteca de Infraestructura de Tecnologías de Información.

Esta metodología es la aproximación más aceptada globalmente para la gestión de servicios de Tecnologías de Información en todo el mundo, ya que es una recopilación de las mejores prácticas tanto del sector público como del sector privado. Estas mejores prácticas se desarrollan en base a la experiencia adquirida con el tiempo en determinada actividad, y son soportadas bajo esquemas organizacionales complejos, pero a su vez bien definidos, y que se apoyan en herramientas de evaluación e implementación.

ITIL como metodología propone el establecimiento de estándares que ayuden en el control, operación y administración de los recursos (ya sean propios o de los clientes). Plantea hacer una revisión y reestructuración de los procesos existentes en caso de que estos lo necesiten (si el nivel de eficiencia es bajo o que haya una forma mas eficiente de hacer las cosas), lo que lleva a una mejora continua.

Otra de las cosas que propone es que para cada actividad que se realice se debe hacer la documentación pertinente, ya que esta puede ser de gran utilidad para otros miembros del área, además de que quedan asentados todos los movimientos realizados, permitiendo que toda la gente esté al tanto de los cambios y no se tome a nadie por sorpresa.

En la documentación se pone la fecha en la que se hace el cambio, una breve descripción de los cambios que se hicieron, quien fue la persona que hizo el cambio, así como quien es el que autorizó el cambio, para que así se lleve todo un seguimiento de lo que pasa en el entorno. Esto es más que nada como método con el que se puede

establecer cierto control en el sistema de cambios, y así siempre va a haber un responsable y se van a decir los procedimientos y cambios efectuados.

En el siguiente diagrama se puede ver como hay segmentos del negocio aparentemente aislados, pero, en realidad todos toman parte importante en la obtención de las soluciones. Por ejemplo la prestación de servicios muchas veces no sería posible sin la gestión de infraestructura, asimismo las perspectivas del negocio no se darían sin la prestación de servicio y los servicios no serían posibles sin un soporte al servicio. Y el punto de interacción que se da entre estos segmentos del negocio es la búsqueda de soluciones, donde lo que se busca es que las perspectivas del negocio estén soportadas en base a la prestación de servicios; la prestación de servicios requiere que se le dé un soporte al servicio para que esté siempre disponible, la disponibilidad se puede lograr mediante la gestión de la infraestructura. Lo que lleva finalmente a, en lugar de tener al centro las soluciones se obtendrán clientes satisfechos.



Figura 2.1 Interacción de los procesos de negocios

CÓMO SE UTILIZA ITIL

ITIL postula que el servicio de soporte, la administración y la operación se realiza a través de cinco procesos:

- Manejo de Incidentes
- Manejo de Problemas
- Manejo de Configuraciones
- Manejo de Cambios
- Manejo de Entregas

1. Proceso de manejo de incidentes

Su objetivo primordial es reestablecer el servicio lo mas rápido posible para evitar que el cliente se vea afectado, la finalidad es minimizar los efectos de la operación. A este concepto se le llama disponibilidad.

En cada fase manejan cuatro puntos básicos, propiedad, monitoreo, registro y comunicación.

En el proceso de manejo de incidentes se da como primera etapa la detección del incidente (se presenta una anomalía o falla), una vez identificado se clasifica (si el problema es conocido o no), una vez solucionado se recurre a la documentación y registro del incidente y se evalúa.

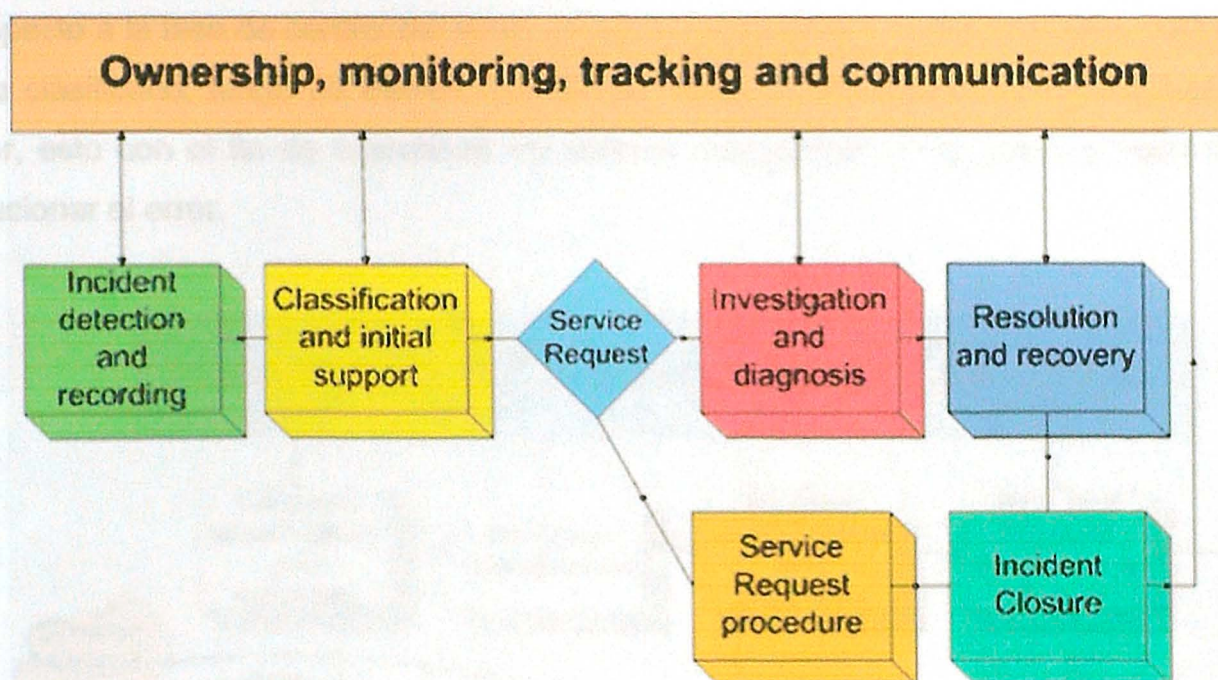


Figura 2.2 Fases del manejo de incidentes

2. Proceso de manejo de problemas

El objetivo de este proceso es prevenir y reducir al máximo los incidentes, esto lleva a una reducción en el nivel de incidencias. También ayuda a proporcionar soluciones rápidas y efectivas para asegurar el uso estructurado de recursos. Lo que se busca es tener pleno control del problema, esto se logra dándole un seguimiento y un monitoreo a la situación.

Este proceso se maneja en dos fases, la primera está relacionada con lo que es el control del problema y la segunda con el control del error.

El control del problema: identifica el problema en base a alguna sintomatología; se clasifica, al igual que en el proceso de manejo de incidentes, si es un problema conocido o no y se procede de acuerdo a ello.

Respecto a la fase de control del error, en esta se identifica y registra el error, esto sirve para clasificarlo, luego se evalúa el daño generado o que puede llegar a generar el error, esto con el fin de cuantificar los efectos que podría producirse en caso de no solucionar el error.

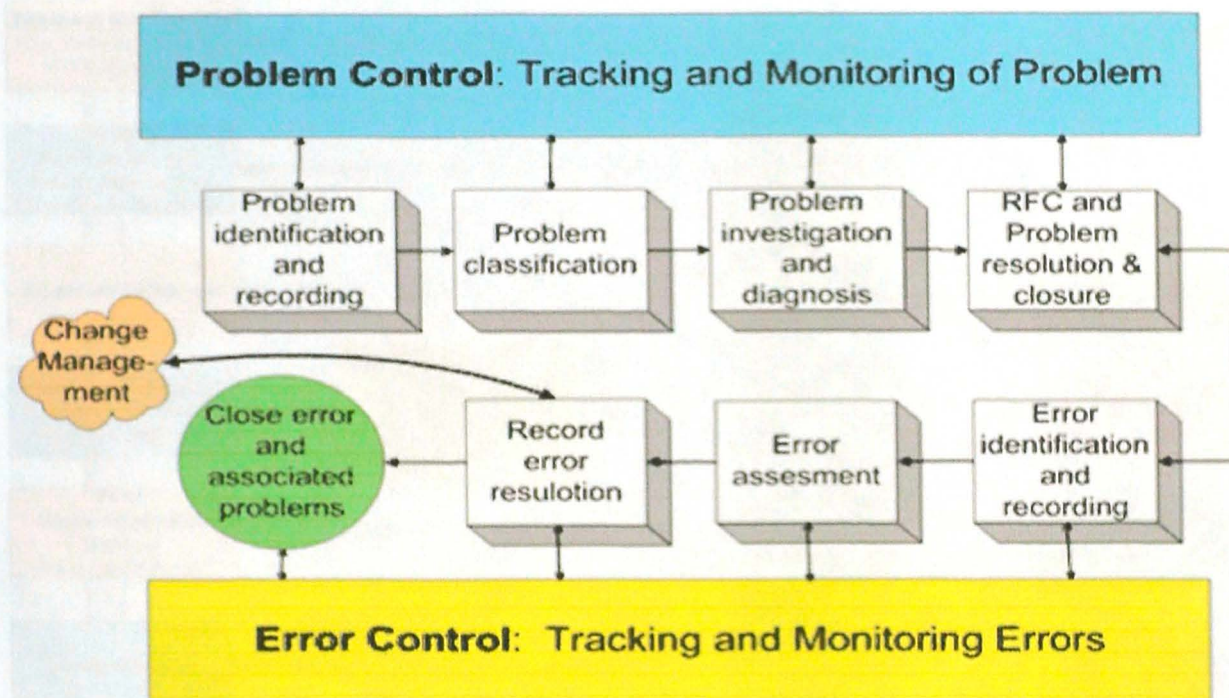


Figura 3. Fases del control de errores

3. Proceso de manejo de configuraciones

Su objetivo es proveer información real y actualizada de lo que se tiene configurado e instalado en cada sistema.

Este proceso es de los más complejos, ya que se mueve bajo cuatro vértices que son: administración de cambios, administración de liberaciones, administración de configuraciones y la administración de procesos diversos.

El nivel de complejidad de este modelo es alto, ya que influyen muchas variables y la mayoría son dinámicas, entonces al cambiar una o varias de ellas, afectan el sistema

en general. Aunque es lo más parecido a la realidad, debido a que el entorno es dinámico y las decisiones de unos afectan a otros.

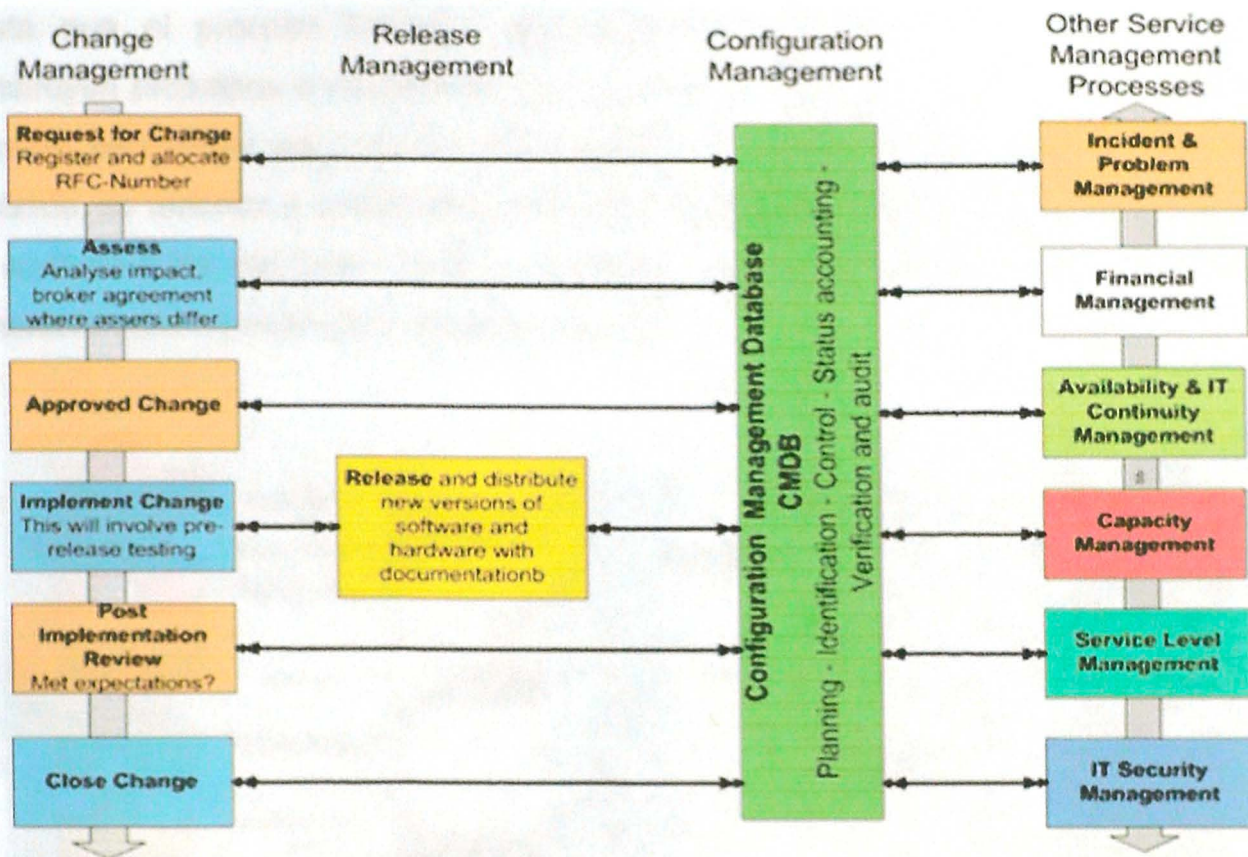


Figura 2.4 Proceso de manejo de configuraciones.

4. Proceso de control de cambios

El objetivo de este proceso es reducir los riesgos tanto técnicos, económicos y de tiempo al momento de la realización de cambios. El diagrama siguiente parece ser fácil de seguir, pero en realidad no lo es, ya que entre etapa y etapa se da una fase de monitoreo para ver que no hay un desvío de los objetivos.

Primero, hay un registro y clasificación del cambio que se tiene que hacer, se pasa a la fase de monitoreo y planeación, si el rendimiento es satisfactorio se da la aprobación del cambio, y en caso que el rendimiento sea malo se pasa a la fase de reingeniería hasta que el proceso funcione adecuadamente y se aprueben los cambio, se construyen prototipos o modelos en los que se van a hacer las pruebas, se hacen las pruebas pertinentes para ver las capacidades del sistema, una vez el proceso se ha probado, se autoriza e implementa. Después de la implementación, se revisa que esté de acuerdo a los objetivos iniciales y se ajusta a las necesidades, a esto también se le considera como revisión post implementación.

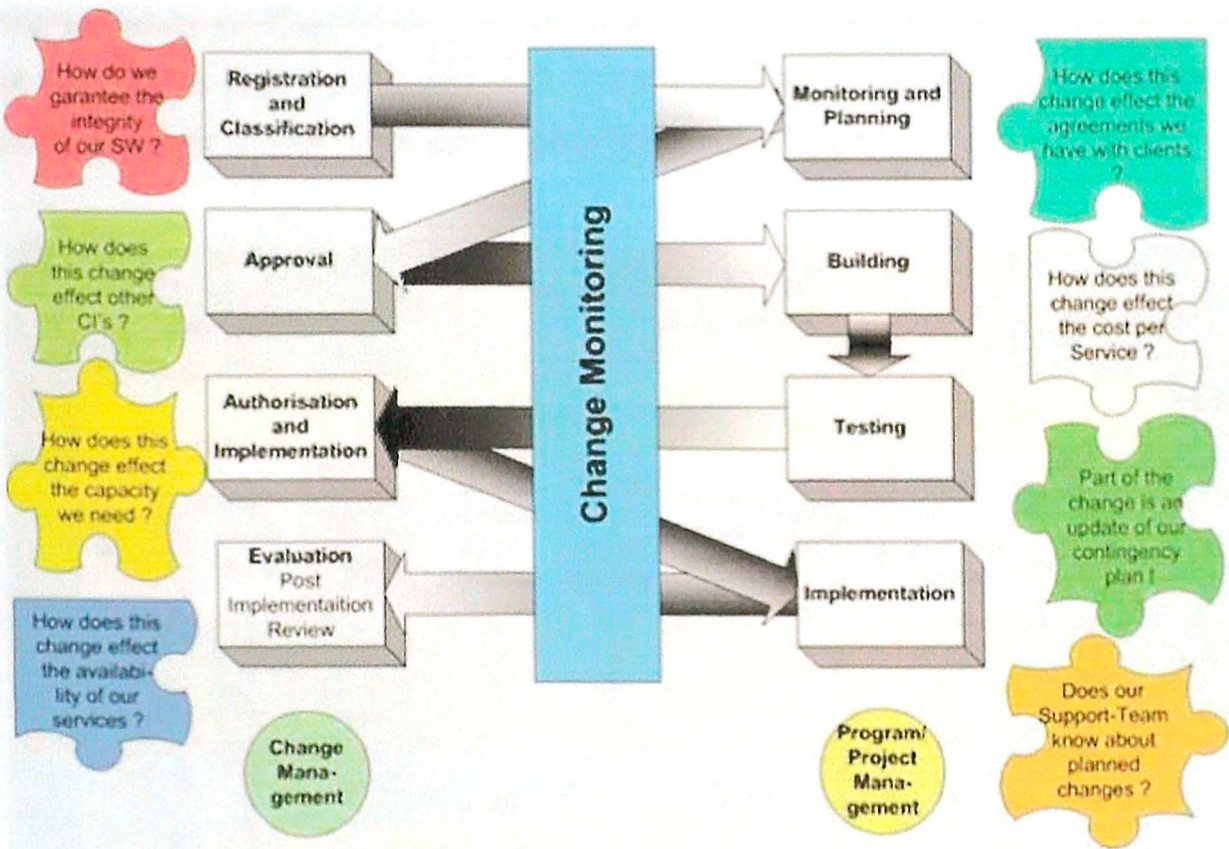


Figura 2.5 Proceso de manejo de cambios

5. Proceso de manejo de entregas

Su objetivo es planear y controlar la instalación de Software y Hardware bajo tres ambientes: ambiente de desarrollo, ambiente de pruebas controladas y ambiente real o de explotación. Este proceso tiene un diagrama que marca la transición de un ambiente a otro a medida que evoluciona el proyecto.

En el ambiente de desarrollo se debe gestionar la liberación de las políticas, de la planificación; el diseño lógico de la infraestructura y la adquisición de software y hardware están entre los ambientes de desarrollo y de pruebas controladas ya que en ambos deben ser probados. En el ambiente real o de explotación es donde se concreta cada fase anterior.

En el proceso de entrega del servicio el usuario ve concretados sus requerimientos, sin saber que detrás del servicio que está recibiendo hay un sin fin de actividades y de decisiones que se tuvieron que tomar para llegar a este punto.

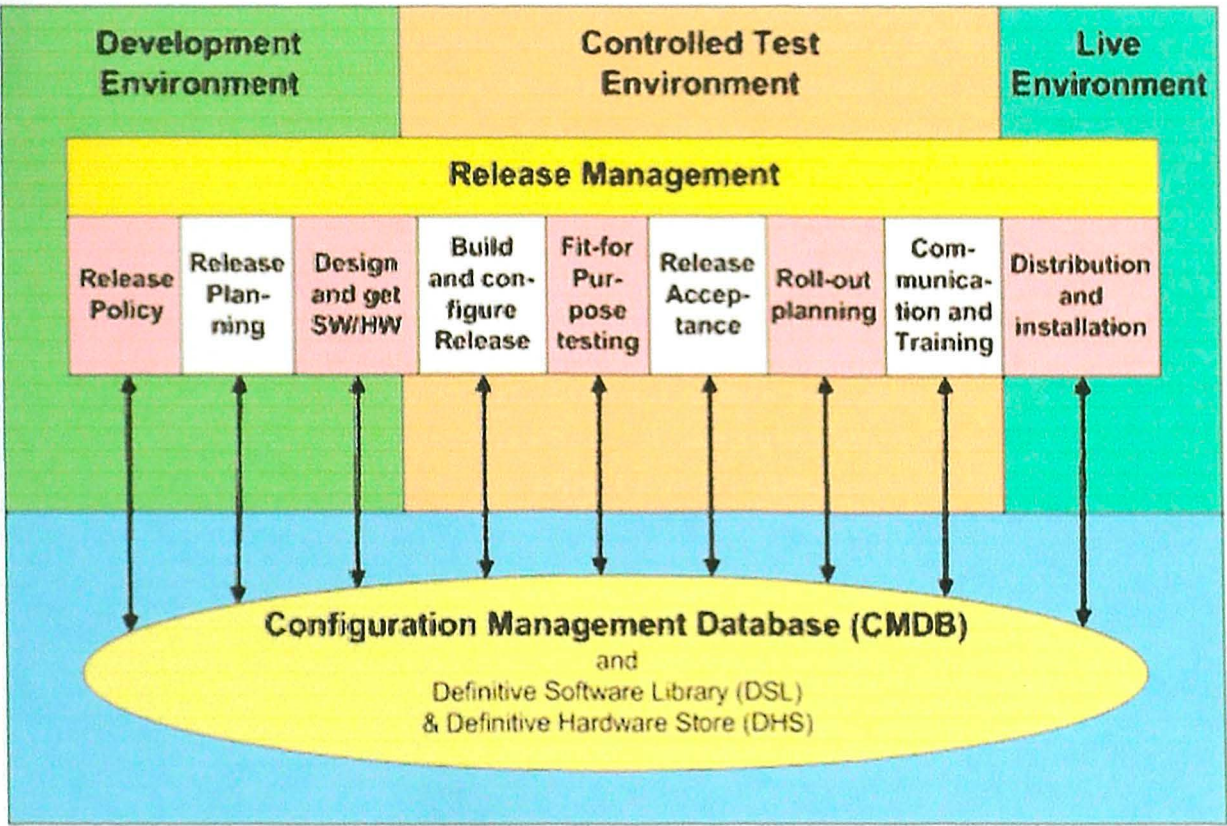


Figura 2.6 Proceso de manejo de liberaciones

A pesar de haber explicado resumidamente en que consiste la metodología ITIL, en este trabajo no será tomada en profundidad, sino más bien, es una fuente de referencia importante al momento de analizar qué, cómo o para qué implementar mejoras en la gestión de los servicios.

2.2 Conclusión del Capítulo

Se han dado a conocer conceptos relacionados a la gestión de servicios, que ayudarán a una mejor comprensión en los próximos capítulos.

CAPÍTULO III
DESARROLLO

3. DESARROLLO

3.1. Requerimientos de la aplicación

La aplicación se implementará sobre un sistema con las siguientes características o características:

- **Confidencialidad:** Esta aplicación debe ser de acceso restringido, de manera que solo personas que hayan pasado un proceso de selección y sean autorizadas por el sistema de acceso, puedan acceder a la información que se almacena en el sistema. La información debe ser de acceso restringido.
- **Seguridad:** Debe ser una aplicación segura, es decir, debe estar protegida por un sistema de seguridad que permita controlar el acceso a la información. Debe ser una aplicación segura, es decir, debe estar protegida por un sistema de seguridad.
- **Integridad:** La información que se almacena en el sistema debe ser de acceso restringido, es decir, debe estar protegida por un sistema de seguridad. La información debe ser de acceso restringido, es decir, debe estar protegida por un sistema de seguridad.
- **Disponibilidad:** La información que se almacena en el sistema debe ser de acceso restringido, es decir, debe estar protegida por un sistema de seguridad. La información debe ser de acceso restringido, es decir, debe estar protegida por un sistema de seguridad.
- **Seguridad:** La información que se almacena en el sistema debe ser de acceso restringido, es decir, debe estar protegida por un sistema de seguridad. La información debe ser de acceso restringido, es decir, debe estar protegida por un sistema de seguridad.

CAPÍTULO III DESARROLLO

3 DESARROLLO

3.1 Requerimientos de la aplicación

La solución a implementar debe contar con los siguientes requerimientos o características:

- **Confiabilidad:** Esto quiere decir que no debe presentar demasiados falsos positivos, los que se asume, siempre existirán, pero no pueden conducir a errores. En resumen disminuir la frecuencia de estos.
- **Robusta:** Debe ser una aplicación estable y con tolerancia a fallos, no puede presentar fallas o caídas permanentemente, debe soportar cortes de red, reinicios no programados de sistema.
- **Inteligente:** La aplicación debe estar dotada de cierta inteligencia, esto es, que sea capaz de tomar algunas acciones básicas ante ciertos eventos, esto es, reaccionar con acciones previamente definidas ante la alerta de un problema. Por ejemplo, intentar reiniciar el servidor web en caso este no responda.
- **Configuración:** Debe ser de fácil configuración, que permita en pasos simples agregar servicios o modificar los existentes.
- **Notificaciones:** Que sea capaz de encender alarmas o generar alertas (mail, sms, ejecución de comandos, etc) si detecta algún problema.
- **Reportes:** El sistema debe ser capaz de generar reportes de disponibilidad instantáneos e históricos. El mínimo dato a presentar debe ser el uptime (disponibilidad) o tiempo de caída por servicio.

- **Gráfica accesible:** Debe ser una herramienta visual que pueda ser consultada en cualquier momento y desde cualquier lugar, incluyendo el acceso desde dispositivos móviles.
- **Heterogeneidad:** La aplicación debe ser capaz de monitorear y/o ejecutar scripts en ambientes diversos, en cuanto a sistemas operativos (Linux, Unix y Windows), hardware y aplicaciones.
- **Tolerancia a fallos:** El sistema debe detectar fallas tanto en los servicios como en los accesos a ellos, esto es, alertar si se produce un corte en el acceso Internet a los servidores, ya que las máquinas y servicios siguen funcionando, pero no es posible acceder a ellos, lo que igualmente debe ser informado al cliente. Este punto también puede ser denominado monitoreo redundante.

A lo largo del tiempo se han desarrollado una variedad de herramientas de monitoreo, en distintos lenguajes, con distintos objetivos y características. Algunas son comerciales y otras freeware, por lo que no todas se ajustan a las necesidades de las organizaciones, incluso, a veces se debe usar una combinación de ellas. En el sitio de publicación de información Wikipedia se puede encontrar una comparación de varias herramientas, según algunos ítems generales. Este cuadro es sólo referencial, ya que puede ir variando en el tiempo, http://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems

3.2 Requerimientos de plataforma

La o las aplicaciones a instalar deben requerir las características mínimas de hardware para asegurar su portabilidad de una máquina a otra, asimismo con el sistema operativo, ya que puede ser necesario cambiar la instalación en caso de ocurrir un problema.

Características de hardware del actual servidor de monitoreo

- 1 Procesador Intel Pentium 4 3.0 GHz
- 1 Disco Duro SCSI de 76 GB
- 512 MB de RAM
- Una Interfaz de Red de 10/100 Mbps:

3.3 Alternativas de solución

3.3.1 Monitoreo externo

En el mercado existen variadas formas de enfrentar la necesidad de monitorear servicios, puede ser implementando una solución al interior de la organización, o bien contratando el servicio con una empresa externa. Tener mediciones externas le otorga un valor adicional, ya que los reportes son entregados por una entidad ajena a la empresa que brinda el servicio y esto se transforma en una garantía de información fidedigna para el cliente.

Una empresa dedicada al monitoreo de servicios Internet reconocida en el mercado es Atentus Servicios de Monitoreo S.A (www.atentus.com) cuyos productos son distintos sistemas de monitoreo ya sea de servicios o de enlaces, estos monitoreos son

realizados desde varios ISP (Proveedores de Servicios Internet). Esta es su principal ventaja, tener una mirada de los servicios y servidores desde la mayoría de las redes nacionales.

Los servicios o productos que ofrece Atentus se resumen en el siguiente cuadro:

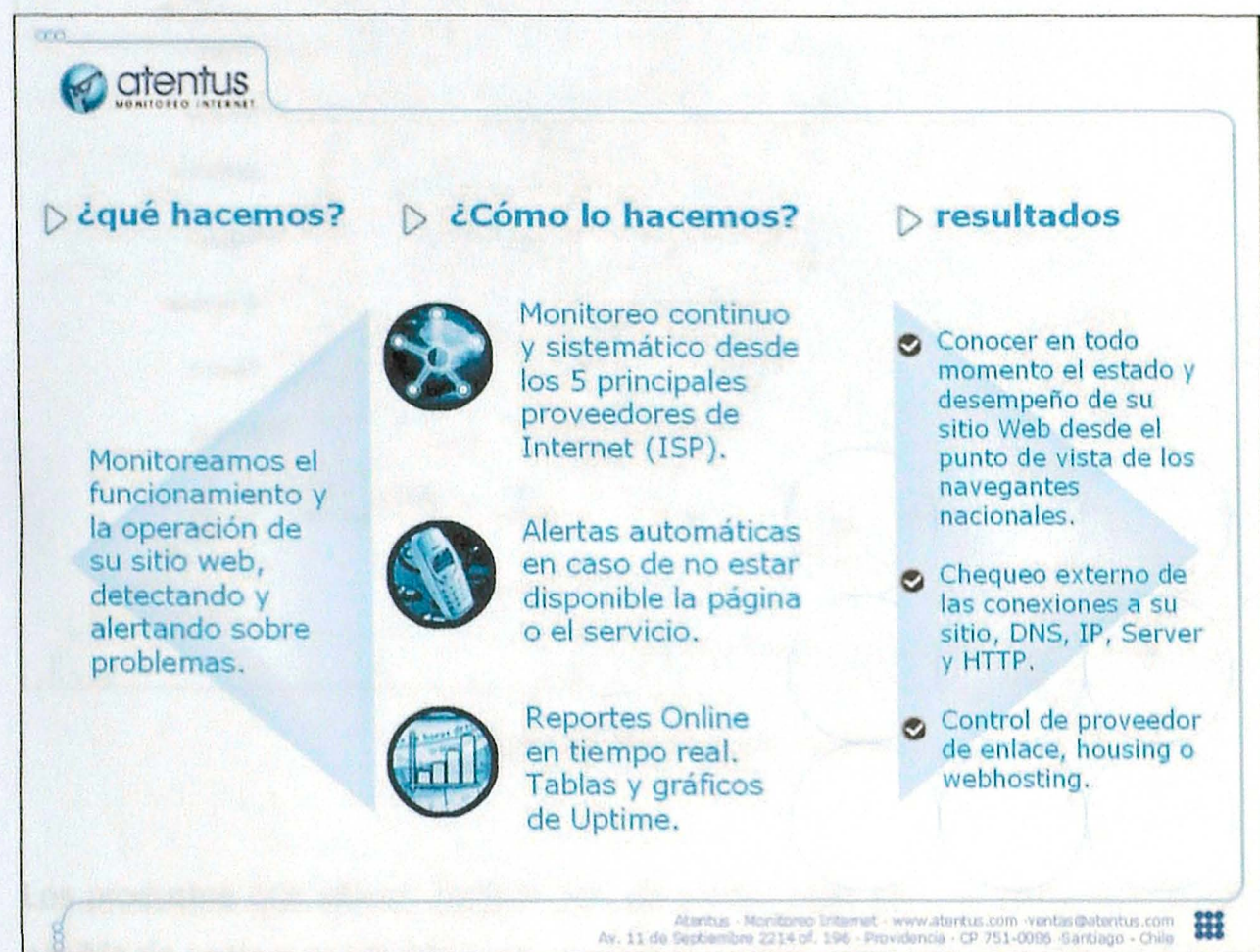


Figura 3.1 Presentación Atentus.com

A continuación se muestra como opera la red de monitoreo de Atentus.

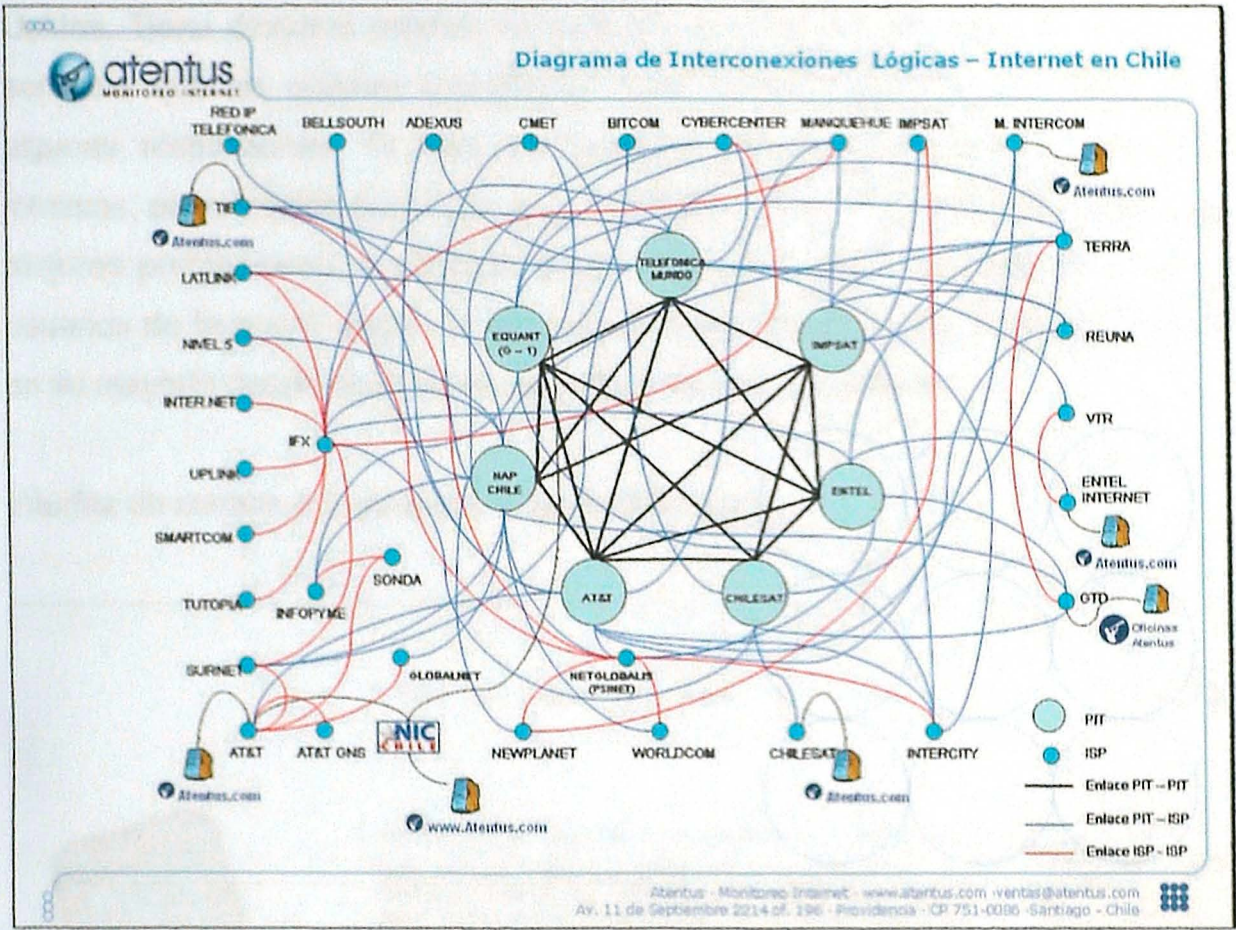


Figura 3.2 Red Operativa Atentus

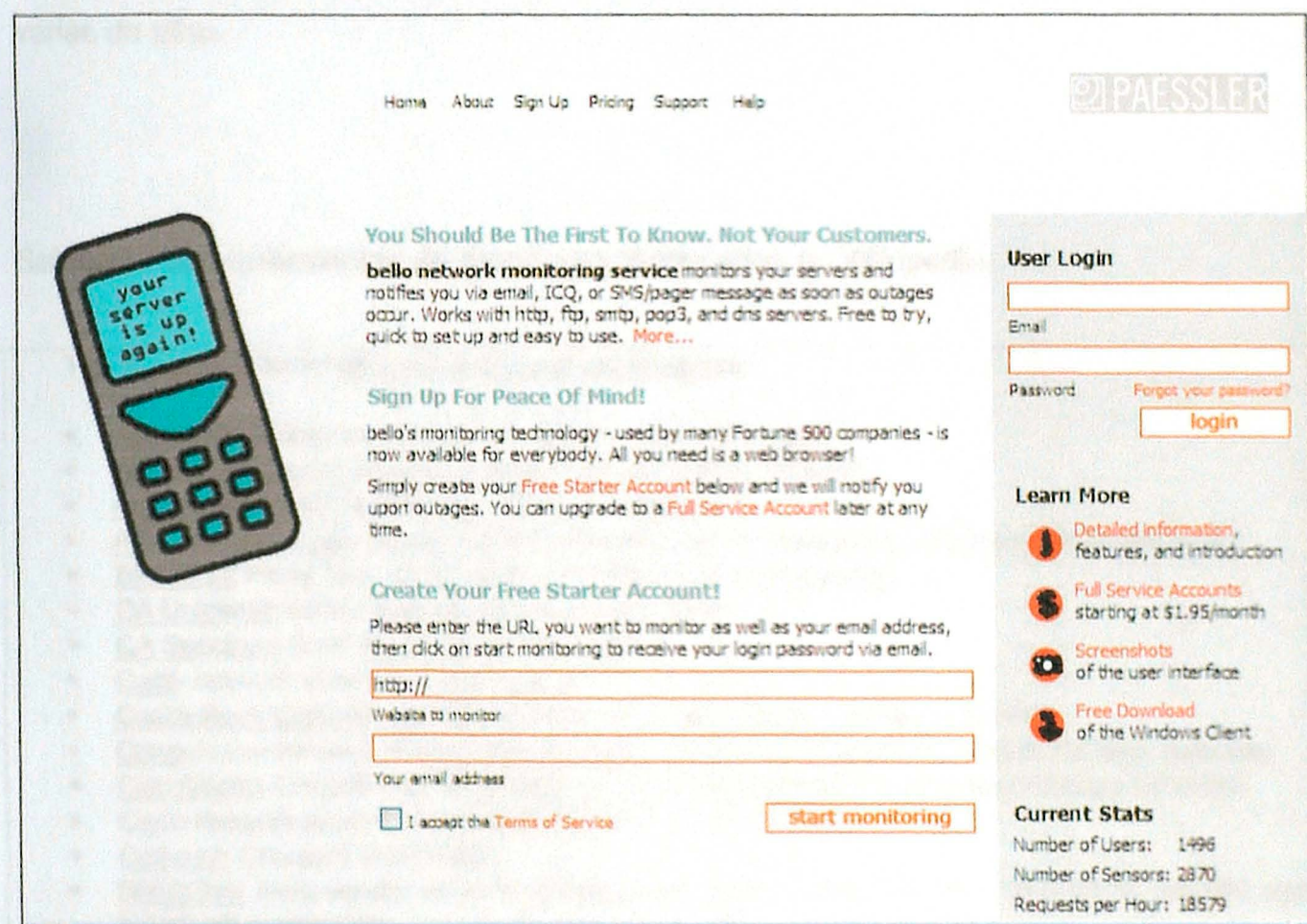
Los productos que ofrece Atentus son de primer nivel pero el costo que tienen no es posible de costear por la empresa, ya que por cada sitio o servicio que se inscriba para ser monitoreado se cancela una alta suma mensual. La cotización entregada es reservada por lo que no se puede publicar en este informe.

3.3.2 Monitoreo Externo Internacional

Otra opción es contratar un monitoreo internacional, esto es útil cuando los usuarios de los servicios que se prestan acceden desde estos enlaces. De este tipo de monitoreo se puede encontrar una amplia gama de empresas con distintas condiciones de servicio y

costos, en particular, se usó una que se llama Bello Monitoring (www.bello-monitors-the.net). Esta empresa presta servicios de monitoreo de sitios web desde Estados Unidos. Tiene distintos precios de acuerdo a la cantidad de sitios que se inscriban o servicios que se quieran monitorear, pero también tiene una versión gratuita con algunas restricciones. Si bien es cierto la versión gratuita tiene las prestaciones mínimas, es suficiente para usar este monitoreo como complemento a otro sistema con mejores prestaciones, y utilizarlo sólo como referencia. Además por el perfil de los usuarios de la mayor parte de los sistemas que administra la empresa, estos acceden en su mayoría desde enlaces nacionales y no internacionales.

Interfaz de acceso e inscripción a Bello Monitoring.



The screenshot displays the Bello Monitoring website interface. At the top, there is a navigation bar with links: Home, About, Sign Up, Pricing, Support, and Help. The PAESSLER logo is visible in the top right corner. On the left side, there is an illustration of a mobile phone with the text "your server is up again!" on its screen. The main content area is divided into several sections:

- You Should Be The First To Know. Not Your Customers.** This section describes the "bello network monitoring service" which monitors servers and notifies users via email, ICQ, or SMS/pager message as soon as outages occur. It works with http, ftp, smtp, pop3, and dns servers. A "More..." link is provided.
- Sign Up For Peace Of Mind!** This section states that bello's monitoring technology is used by many Fortune 500 companies and is now available for everybody. It mentions that users can create a "Free Starter Account" and upgrade to a "Full Service Account" later.
- Create Your Free Starter Account!** This section prompts users to enter the URL they want to monitor and their email address, then click on "start monitoring" to receive their login password via email. There is a checkbox for "I accept the Terms of Service".
- User Login** This section includes fields for Email and Password, a "Forgot your password?" link, and a "login" button.
- Learn More** This section lists four items: "Detailed information, features, and introduction", "Full Service Accounts starting at \$1.95/month", "Screenshots of the user interface", and "Free Download of the Windows Client".
- Current Stats** This section displays the following statistics: Number of Users: 1496, Number of Sensors: 2870, and Requests per Hour: 18579.

Figura 3.3 Interfaz de acceso

En Internet se pueden encontrar varios programas de monitoreo de redes, pero no todos cumplen con los requerimientos de este trabajo ya que pueden estar enfocados a suplir diversos objetivos o necesidades.

Por otra parte hay diversos programas que han nacido como buenas ideas o esperando convertirse en proyectos reconocidos, pero han quedado rezagados en el camino y no han continuado su desarrollo.

En Internet existen diversas comparativas de programas o soluciones de monitoreo. A modo de referencia, a continuación se presentan dos listados publicados en Internet, uno es de nombres de herramientas de monitoreo y la otra es una comparativa entre varias de ellas.

Selección de herramientas de monitoreo recopiladas en Wikipedia.

This is a partial **list of network management systems**.

- Alcatel 5620 Network Manager & Service Aware Manager
- Argus open-source network and systems monitoring software
- Attachmate NetIQ AppManager & SecurityManager
- AutoScan-Network - AutoScan-Network is a network discovering and managing application
- Blue Coat Proxy Servers for WAN Optimization and Web cache
- CA Unicenter Network and Systems Management
- CA Spectrum (formerly Aprisma Spectrum)
- Cacti- network statistics graphing tool.
- Castle Rock Computing SNMPC- Network monitoring and reporting system.
- Cisco Active Network Abstraction A network resource management platform for large networks
- CiscoWorks CiscoWorks Lan Management Solution Manages enterprise switching networks
- Cisco Network Analysis Module Analyzes live network traffic
- Comarch Comarch OSS Suite
- DataMiner multi-vendor network management platform for IPTV, HFC broadband, satellite and broadcast ecosystems
- ECI Telecom LightSoft Multidimensional Network Management System
- Ericsson OSSRC - Operations Support System, Radio and Core
- FireScope BSM - Web 2.0 Enabled Business Service Management, Network Monitoring and Management Software by FireScope, Inc.

- Fluke Networks Visual Performance Manager (VPM)
- Ganglia - an opensource distributed monitoring system for HPC clusters and grids
- Hewlett Packard OpenView framework
- Hewlett Packard HP OpenView TeMIP
- Hyperic Open source application, system and network monitoring software for web-based applications
- IBM AURORA Network Performance Profiling System
- IBM Tivoli NetView
- Intellipool Network Monitor
- IPHost Network Monitor Mail, web, database, and other servers monitoring tool
- LabTech Affordable network management and help desk system for MSPs, IT solution providers, and Corporate IT environments.
- Lucent VitalSuite Network and Service Management Software
- Lucent Navis Optical Management System (OMS)
- Microsoft Operations Manager (MOM)
- MOATIS Wide Area Management Services (managementasaservice.com)
- MRTG
- Nagios open source application
- NetBoss Service Assurance and Element Management
- NetDirector open source change and configuration management
- Netdisco Web-based network management tool targeted at large corporate and university networks.
- NetQoS
- NetFlow Monitor from CESNET
- Nokia Open EMS
- Nortel Enterprise Network and Service Management
- Nortel Enterprise Network Management System
- Nortel Enterprise Policy Manager
- Nortel Enterprise Switch Manager
- Nortel Proactive Voice Quality Management
- Network Administration Visualized (NAV) from Norwegian University of Science and Technology
- ODCNMS Open DataCenter Network Management System released under the GPL.
- Observer Free software network monitoring platform with BSD license.
- op5 Monitor - Open Source network monitoring
- OpenNMS Open-source network management platform released under the GPL.
- OPNET Technologies Sentinel software for network configuration auditing and change validation
- Opsware Opsware Network Automation System (NAS).
- PacketTrap - Network Management Software Provider.
- PathSolutions Switchmonitor Network Performance Monitoring System
- PRTG Traffic Grapher
- PolyMon - Open Source network monitoring running on Windows
- PrefixNE Network Management Software by Prefix IT Ltd.
- ProCurve Manager (PCM+) Comprehensive Management Software for products by ProCurve Networking by HP (base version free)
- Rackwise Data Center Manager - Management of physical datacenter infrastructure
- Raritan Computer's CommandCenter NOC
- ServersCheck Monitoring Software agentless & browser based systems monitoring software
- Siemens Integrated Network Management Services / System by Siemens
- SNM open source application
- Snort Open Source intrusion detection system

- SolarWinds Network Management Software Provider
- Spiceworks - Free Network Monitoring Software for Network Management
- StorageIM - Free Network Monitoring Software for Storage Resource Management
- TTI Telecom Service Assurance, Netrac Product Lines
- DNA (Dynamic Network Abstraction) by Sheer Networks (acquired by Cisco Systems)
- WhatsUp Gold Network monitoring solutions
- ZABBIX open source application and network monitoring solution. *nix, Apache, PHP, MySQL or PostgreSQL. GPL
- Zenoss commercial open source applications, server, and network management solution

Tabla 3.1 Recopilación herramientas en Wikipedia

Comparativa entre sistemas de monitoreo

Name	Packet Trap	doppler VUE	Nagios	Zabbix	Munin	Cacti	Zenoss	Argus	Hobbit Monitor	OpenN MS	SolarWinds Orion	GroundWork
Response Time	Fast	Fast	Fast	Fast	cron	?	Fast	Fast	Fast	Fast	Fast	Fast
Charts	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Logical Grouping	Unknown	Unknown	No	No	No	No	Yes	No	Unknown	No	Unknown	No
Trending	Yes	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Trend prediction	Unknown	No	No	No	Unknown	Unknown	Yes	Unknown	No	Unknown	No	Yes
Autodiscovery	Yes	Yes	No	Yes	No	Yes, using a plugin	Yes	No	No	Yes	Yes	Yes
Agent	Yes	No	Yes	Yes	Yes	No	SNMP, WMI, JMX, etc.	Yes	Yes	Yes, using NRPE	Yes	Not Req., supported
SNMP	Yes	Yes	Yes, using a plugin	Yes	Yes	Yes	Yes	Yes	Yes, using Devmon	Yes	Yes	Yes
SYSLOG	Yes	Unknown	No	No	No	No	Yes	No	Unknown	No	Yes	Yes
External scripts ^[1]	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Plugins ^[2]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes and supports BB extensions	Yes	Yes	Yes
Plugin creation ^[3]	Medium	.Net assemblies	Medium	Easy	Medium	Medium	Easy	Easy	Easy	?	Easy	Medium
Triggers/	Yes	Yes	Yes	Yes	Partial	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Alerts ⁽⁴⁾												
WebApp ⁽⁵⁾	Viewing and Reporting	Full control	Viewing only	Full control	Viewing only, very simple	Full control	Full control	Viewing Only	Viewing, acknowledging, limited configuration	Full control	Full control	Full control
Distributed Monitoring	Yes	No	Yes	Yes	Unknown	Unknown	Yes	Unknown	No	No	Yes	Yes
Data storage method	SQL	SQL	SQL	SQL	RRDtool	RRDtool and MySQL	RRDtool and MySQL	Berkely DB	Flat file and RRDtool	RRDtool and PostgreSQL	SQL	SQL
License			GPL	GPL		GPL	GPL					GPL

Tabla 4 Comparativa herramientas según Wiki

De acuerdo a los antecedentes recopilados, la comparativa de la tabla anterior, publicaciones en foros y literatura especializada en Internet y considerando los requerimientos antes planteados para este sistema, se decide implementar monitoreo local utilizando como herramienta principal Nagios. No es imprescindible tener monitoreo internacional ya que no representa a la mayoría de los usuarios de los sistemas administrados.

3.4 Implementación

De acuerdo a lo revisado en la literatura disponible, una de las aplicaciones más utilizadas es Nagios (www.nagios.org) de la cual además han nacido otras aplicaciones comerciales, es por esto que Nagios permite asegurar que está o estará en constante desarrollo, una comunidad creciente en caso de requerir ayuda para la solución de problemas, y que incorpora día a día nuevas aplicaciones como complementos para mejorar la experiencia con Nagios.

Por estas razones, y porque además cumple con los requerimientos antes expuestos es que la aplicación elegida a ser instalada es Nagios.

Al momento de realizar este trabajo la última versión estable disponible es la 3.0.6 en desarrollo se encuentra la versión 3.1.0. Se instala la versión 3.0.6.

Algunas razones por las que Nagios se ha convertido en un estándar en las organizaciones del rubro TI:

- **Proactivo:** Nagios provee la capacidad de alertar e incluso reaccionar sobre incidentes, antes que los usuarios se den por enterados.
- **Monitoreo detallado a la red completa**
 - Sistemas Operativos Windows, Unix/Linux
 - Dispositivos como Routers, Switchs, Firewalls, Impresoras
 - Servicios y Aplicaciones
- **Notificaciones**

Puede enviar notificaciones usando distintos medios como mail, sms, celular y a un grupo de usuarios.

Tiene la capacidad de escalar las notificaciones.
- **Resolución de problemas**

Da a conocer los problemas a través de la interfaz web

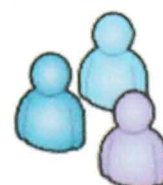
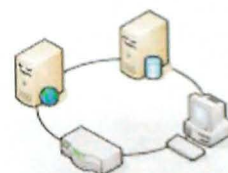
Puede reiniciar automáticamente aplicaciones o servicios si estos fallan
- **Planificación**

Puede programar bajadas de servicios o hosts anticipadamente.
- **Reportes**

Genera reportes de disponibilidad y un histórico de notificaciones.

Se puede mejorar la visualización de los reportes integrando otras herramientas (addons) a Nagios como Cacti y otros.
- **Interfaz multiusuario**

El acceso a la interfaz puede mediante usuarios que tendrán vistas restringidas, a cada usuario se le asigna un perfil de acuerdo a los privilegios asignados en la aplicación.



- Integración con aplicaciones existentes

Por ejemplo con aplicaciones de generación de tickets o helpdesk

- Arquitectura extensible

Actualmente hay alrededor de 200 addons y plugins disponibles en la comunidad Nagios para mejorar funcionalidades, y por ende la experiencia del usuario



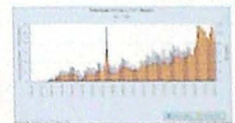
- Estable y confiable

- Desarrollo desde hace 10 años
- Puede llegar a monitorear 100.000 nodos
- Failover o protección ante fallas
- Ganador de varios premios y reconocimientos



- Comunidad

Comunidad de usuarios y listas de correos activas



- Código personalizable

Al ser un software de código abierto, al usuario se le otorga *libertad de acceder a el y hacer las modificaciones que estime necesarias.*

Liberado bajo licencia GPL

El año 2008 por segunda vez Nagios fue reconocido como "Software de Monitoreo del Año" en una encuesta realizada en línea a usuarios del sitio especializado LinuxQuestions.org con un 39.74% de las votaciones.

<http://www.linuxquestions.org/questions/2008-linuxquestions.org-members-choice-awards-83/monitoring-application-of-the-year-695651/>

Las instrucciones de instalación se encuentran en Anexo B “Instalación de Nagios”. Nagios usa varios archivos de configuración para los distintos elementos que lo componen. En la siguiente figura se puede ver como estos archivos están relacionados.

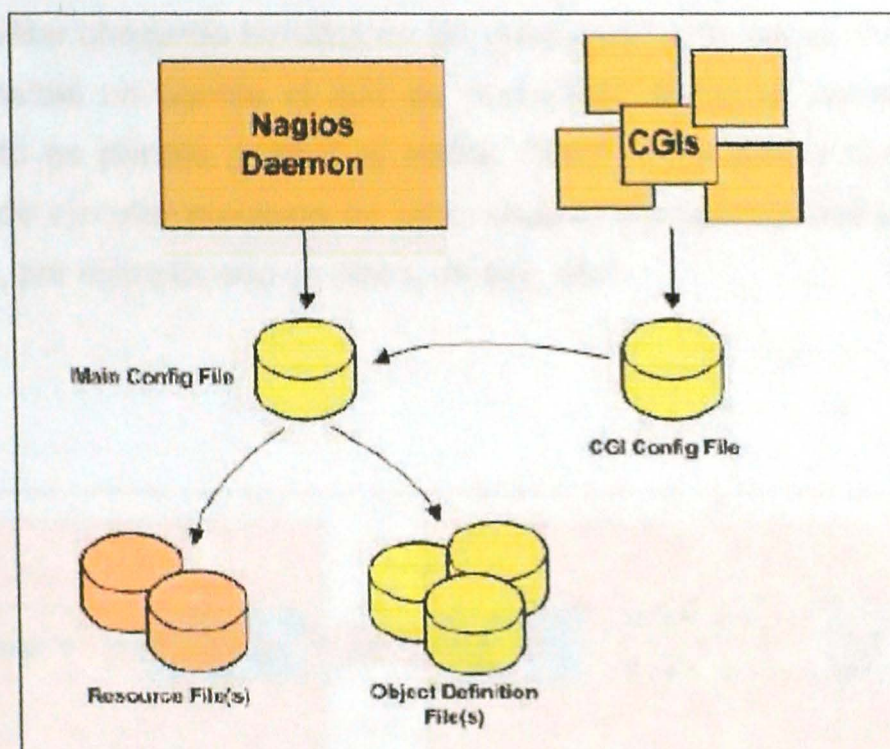


Figura 3.4 Archivos de configuración de Nagios

¿Qué funcionalidades se habilitarán de Nagios?

En primer lugar se habilitará la configuración básica, esto es, chequeo activo de servicios, los servidores y sus servicios serán revisados desde la máquina con Nagios usando TCP/IP. Cabe notar que el chequeo que se hace es interno, tanto la máquina que hace el chequeo (Host Nagios), como las máquinas analizadas (Hosts remotos) están en la misma red, por lo que no se detectará si hay un corte u otro problema fuera de la red (en enlaces o proveedores ISP fuera del datacenter).

Aparte de esta funcionalidad básica, es posible implementar otras funcionalidades activando ciertos Addons desarrollados para Nagios. Los addons son programas que se agregan como módulos a la instalación.

Algunos de estos addons se activarán en Nagios para lograr los resultados esperados.

Es posible habilitar chequeos remotos en las máquinas, esto quiere decir que en cada máquina se instala un agente el que es controlado desde el servidor principal de monitoreo. Esto es posible gracias al addon NRPE. Este addon le da a Nagios la funcionalidad de ejecutar procesos en otra máquina en forma transparente y como si fuesen locales, por ejemplo: uso de disco, de cpu, etc.

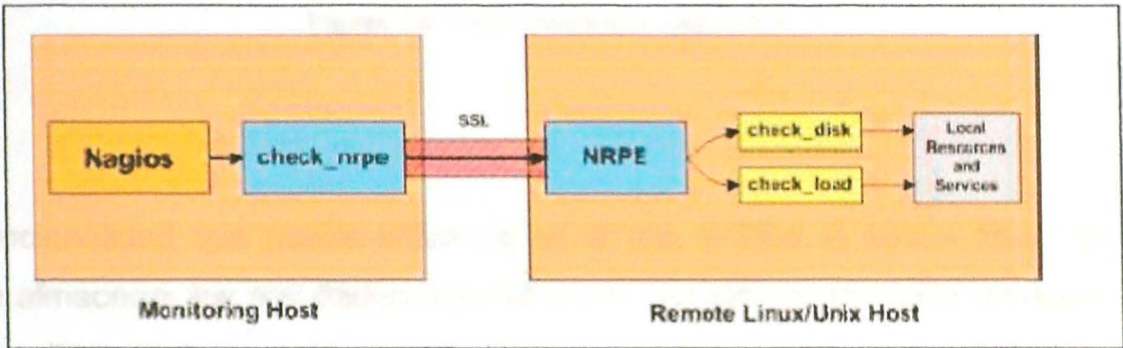


Figura 3.5 Funcionamiento Addon NRPE

La próxima etapa es habilitar Nagios con tolerancia a fallos, esto significa que la máquina instalada con Nagios seguirá revisando los servicios configurados, pero habrá una segunda máquina en una red externa a los servidores que estará monitoreando a la red de servidores, esto se puede implementar usando dos esquemas.

El primero es que esta segunda máquina con Nagios monitorea toda la red y servicios, osea, se duplica el monitoreo.

La segunda forma de implementar la tolerancia a fallos es que el Nagios adicional revise el funcionamiento y disponibilidad sólo de la máquina principal de Nagios.

Cualquiera de estas opciones logran el objetivo de detectar si hay cortes de enlaces, o si la máquina que hace el monitoreo deja de responder u otros problemas que se puedan presentar.

Para implementar esto se utiliza el addon NSCA cuya función es permitir a Nagios recibir chequeos pasivos desde otra máquina. NSCA también se usa para implementar esquemas distribuidos de monitoreo.

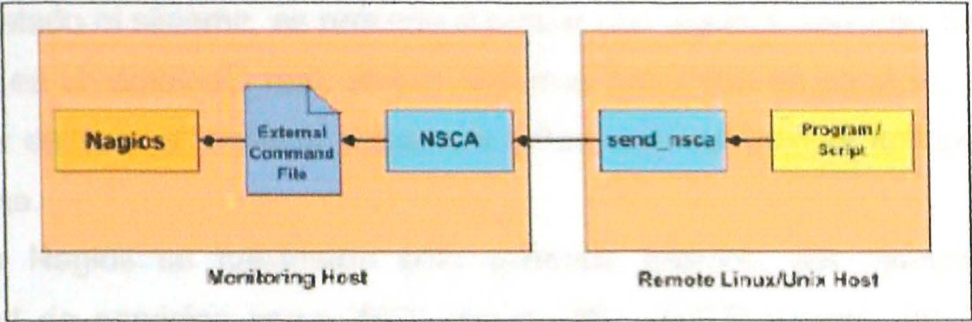


Figura 3.6 Funcionamiento Addon NSCA

Otra funcionalidad que puede utilizarse es la que provee el addon NDOUTils, el que permite almacenar los resultados obtenidos por Nagios en una base de datos MySQL, esto permite que varias instancias de Nagios puedan almacenar sus resultados en una única base de datos.

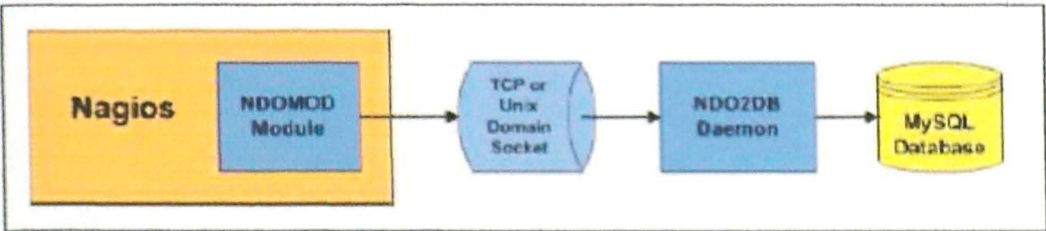


Figura 3.7 Funcionamiento Addon NDOUTils

La documentación completa de estos y otros addons se puede encontrar en el sitio de Nagios (www.nagios.org). Así también en el caso los plugins. Los plugins son pequeños programas o comandos para ejecutar ciertas acciones como por ejemplo, revisar un puerto TCP, ejecutar una consulta sobre una base de datos, revisar el espacio en disco, entre otras.

Una vez instalado el sistema, se procede a probar con algunos servicios para ver como se comporta en un ambiente real, ambos sistemas funcionan en paralelo, ya que no es factible dejar de usar el sistema actual sin antes conocer bien el funcionamiento del nuevo sistema.

Para probar Nagios se habilitaron sólo servicios básicos, por ejemplo, revisar la disponibilidad de servicios como WEB (puerto 80), SMTP (puerto 25), POP (puerto 110).

La instalación se irá mejorando e incorporando otros servicios o necesidades a chequear a medida se tenga mayor conocimiento de la herramienta, sus opciones y potencialidades.

3.5 Conclusión del Capítulo

La implementación del software Nagios se realizó con algunos contratiempos iniciales, como los mismos creadores del software explican en el manual, instalarlo por primera vez es un tanto complejo, la curva de aprendizaje es lenta inicialmente, pero una vez funcionando y familiarizado con la aplicación se torna más amigable manipularlo.

Además la gran cantidad de opciones del software, y utilitarios que se pueden instalar adicionalmente, hacen de Nagios un programa de constante aprendizaje y de interminables opciones a implementar.

4. DISCUSIÓN Y RESULTADOS

4.1. Resultados

La investigación en la educación física ha sido un campo de estudio que ha crecido rápidamente en los últimos años, debido a la importancia que se le ha dado al deporte y la actividad física en la vida cotidiana. Este capítulo presenta los resultados de la investigación, organizados en tres secciones: la primera se refiere a la metodología, la segunda a la descripción de los datos y la tercera a la interpretación de los resultados.

Como se puede ver en el cuadro 1, los resultados de la investigación muestran que la mayoría de los participantes en el estudio son hombres, lo que puede deberse a la mayor participación de este grupo en la actividad física.

Hasta el momento no se han encontrado estudios que hayan analizado la relación entre la actividad física y la salud en la población adulta, por lo que este estudio contribuye a la comprensión de este fenómeno.

La investigación en la educación física ha sido un campo de estudio que ha crecido rápidamente en los últimos años, debido a la importancia que se le ha dado al deporte y la actividad física en la vida cotidiana.

CAPÍTULO IV DISCUSIÓN Y RESULTADOS

4.2. Resultados de la Investigación

Según se puede ver en el cuadro 1, los resultados de la investigación muestran que la mayoría de los participantes en el estudio son hombres, lo que puede deberse a la mayor participación de este grupo en la actividad física.

El estudio ha demostrado que la actividad física tiene un impacto positivo en la salud de la población adulta, lo que puede deberse a la mayor participación de este grupo en la actividad física.

4. DISCUSIÓN Y RESULTADOS

4.1 Resultados

La habilitación de la aplicación Nagios ha sido un poco más lenta de lo esperado, el aprendizaje inicial un tanto costoso, pero que se ha ido agilizando con el paso del tiempo y la familiarización con los archivos de configuración, conceptos y definición de cada objeto.

Como aparece en la documentación, Nagios se autodefine como un software de difícil aprendizaje, y esta implementación no ha sido la excepción.

Hasta el momento se utiliza el programa sólo con tres equipos, en los que se hacen distintas pruebas, se configuran servicios, se prueban distintas opciones.

La idea es conocer las posibilidades que entrega la herramienta antes de agregar todas las máquinas y servicios.

La marcha blanca del sistema no ha estado exenta de problemas, se espera muy pronto dejar Nagios con todas las máquinas activas para que posteriormente se convierta en el único sistema de monitoreo en la empresa.

4.2 Estimación de Costos

Nagios al ser una herramienta de código libre y gratuita no genera costos para adquirirla e implementarla.

El hardware utilizado es parte de la plataforma que la empresa posee previamente para estos fines, no se considera comprar equipamiento, además no se requiere equipamiento de grandes características.

El recurso que sí puede ser considerado son las horas hombre utilizadas en este proyecto, estas horas pueden ser separadas en horas para implementación y horas para mantención o utilización del sistema.

El costo realmente importante es el potencial ahorro que se produce al tener un sistema de monitoreo eficiente, ya que las multas asociadas a downtime de los servicios que se aplican son altas.

No se puede evitar que se produzcan incidentes en los servicios, sean producto de intervención humana o no, pero sí se puede minimizar los tiempos que el servicio esté caído, ya que al tener un sistema eficiente, éste avisará oportunamente o bien podrá tomar acciones para corregir el problema.

4.3 Conclusión del Capítulo

Implementar un sistema eficiente de monitoreo de conectividad y servicios no necesariamente implica incurrir en altos costos, más bien es aprovechar adecuadamente los recursos existentes.

CAPÍTULO V

CONCLUSIONES Y TRABAJO FUTURO

5 CONCLUSIONES Y TRABAJO FUTURO

5.1 Conclusiones

Para implementar un sistema de monitoreo de servicios de alta disponibilidad no se requieren software comerciales o hardware especializado con un alto costo, lo que no los excluye, pero hoy en día con la oferta que entrega el mercado, se pueden encontrar buenos productos a bajo costo, o de costo cero.

El monitoreo de servicios es sólo una parte de la gestión de servicios, ya que no será eficiente un buen sistema de monitoreo si el servicio está mal implementado o no es administrado correctamente. La gestión de servicios parte desde una buena toma de requerimientos en adelante, en saber lo que realmente el cliente quiere o necesita.

Existen muchas herramientas que aparentemente hacen lo mismo, pero la decisión de cual utilizar va a depender del contexto en el que se requiera, ninguna aplicación es la panacea, ya que siempre puede existir la posibilidad de fallas, o pueden haber diferencias sutiles entre una y otra.

Tanto o más importante como la alerta sobre un incidente, es la capacidad de reacción que pueda tener el personal responsable y que cuente con los medios y conocimientos necesarios para resolverlos.

No es objetivo de este trabajo medir el performance de una red o de los servicios, sólo interesa la conectividad, saber si se encuentran operativos o no, tomando en cuenta los timeout asociados. Medir throughput, capacidad de respuesta utilizando benchmark si bien es cierto es parte de la gestión de servicios, pero en otra área que no corresponde a la monitorización de la operatividad de los servicios.

5.2 Trabajo Futuro

En un ámbito de constante cambio como son las TI no se puede pensar en el trabajo futuro como algo lejano, en particular en la gestión de servicios TI, los cambios se suceden día a día y se debe estar atento a ellos, y es más bien el estar dispuesto a asumir que cada día puede suceder o cambiar algo, tanto en los servidores y servidores de la empresa como en el mercado o comunidad virtual.

Siempre es posible mejorar lo que se ha hecho, y partiendo de esa base, es que no se debe perder de vista la mejora continua del sistema, revisión de tiempos de respuesta, servidores y servicios que están siendo monitoreados, que el sistema esté siempre al día, eliminar los servicios que ya no se utilicen e incorporar los nuevos.

Es por esto que se puede agrupar el trabajo futuro en dos grandes áreas, por una parte el trabajo en cuanto a la gestión de servicios en general, y por otro lado lo que queda pendiente en cuanto al sistema de monitoreo en sí.

En cuanto a la gestión de servicios, es necesario en un corto plazo abarcar las otras áreas que han quedado pendientes, esto es, mejorar la gestión en la implementación y demás etapas de los servicios.

Mantener actualizada la documentación y registro sobre los servicios de la empresa, ya que siempre es una falencia en el área de las TI tener una documentación pertinente y vigente, ya sea porque no se tiene la costumbre de ir registrando los sucesos o porque el costo de hacerlo es muy alto dado el dinamismo y nivel de cambios de esta área.

En cuanto al sistema de monitoreo específicamente, el primer requerimiento que surge es que, dado que para la empresa uno de los indicadores de calidad más importantes

es el uptime de los servicios, este sistema debe integrarse al Sistema de Gestión de Calidad.

Es importante no sólo monitorear los servicios, sino además los recursos de hardware de cada máquina, o al menos en las más críticas.

Habilitar nuevos plugins que permitan monitorear nuevos servicios o mejorar aquellos existentes que son complejos.

Este sistema de monitoreo puede ser mejorado apuntando hacia el lado de la seguridad informática, integrándolo con un sistema de detección de intrusos o antihacker.

Bibliografía Referenciada

- [1] Myth of the nines - Wikipedia, the free encyclopedia
<http://basicstate.com/htm/9999.htm>

- [2] ITIL® Home
<http://www.itsm-portal.com/>

- [3] Metodología ITIL
<http://www.monografias.com/trabajos31/metodologia-til/metodologia-til.shtml>

- [4] Comparison of network monitoring systems
http://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems

- [5] List of network management systems
http://en.wikipedia.org/w/index.php?title=List_of_Network_Management_Systems

- [6] Monitoring Application of the year
<http://www.linuxquestions.org/questions/2008-linuxquestions.org-members-choice-awards-83/monitoring-application-of-the-year-695651/>

Bibliografía Consultada

- [7] ITIL® Home
<http://www.itil-officialsite.com/>

- [8] Information Technology Infrastructure Library – Wikipedia
<http://en.wikipedia.org/wiki/ITIL>

- [9] Fundamentos de la Gestión TI - ITIL
http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL.php

- [10] Monitoring and Measurement in the Next Generation Technologies
<http://www.fp7-moment.eu/>

- [11] Web Site Monitoring by Dotcom-Monitor_com
<http://www.dotcom-monitor.com>

ANEXO A - Inicio de Datacare Ltda.

Debido a los altos requerimientos tecnológicos de la sociedad, el Instituto de Informática Educativa de la Universidad de la Frontera decide cambiar su dirección de trabajo para concentrarse exclusivamente a la investigación informática, de esta manera impulsa la externalización de sus procesos operativos dando lugar al nacimiento de nuevas empresas, entre ellas Datacare Ltda. en el año 2004.

Hoy, debido al historial y confiabilidad que ofrece Datacare, es posible encontrar entre sus clientes a organizaciones destacadas como lo es el Mineduc, RedEnlaces, IIE y CorpAraucania, entre otros.

El trabajo desarrollado por la empresa da pie a una variedad de funciones como lo es el trabajo con sitios Web de gran tamaño y alta disponibilidad, configuración y manejo de casillas electrónicas que incluyen direccionamiento, módulos de pago (Webpay), accesos FTP, administración de carpetas CGI-BIN, accesos SSI, accesos SSL, Webmail, Antispam, antivirus, autenticación vía IP, herramientas de trabajo colaborativo, como por ejemplo, Basic Support for Cooperative Work (BSCW), plataformas de sistemas operativos como Linux Red Hat Enterprise Server, Linux Red Hat, Linux Mandrake, Linux SUSE, Linux Debian, Linux Fedora, Microsoft Windows 2003 Server, Microsoft Windows 2000 Server, HP-UX, Sun Solaris, entre otros. Además de plataformas JSP, PHP, PL/SQL, C, Perl, Python.

Esta empresa, es una plataforma especializada en la prestación global de servicios para Internet, abarcando todos y cada uno de los servicios o productos que cualquier empresa, profesional o particular pueda necesitar para una efectiva presencia en la red. Los clientes son Empresas Particulares, Instituciones de Educación y Organizaciones de Gobierno que requieren servicios del nivel más alto a nivel nacional.

Los servicios que la empresa ofrece se listan a continuación:

- Hospedaje de aplicaciones (webhosting)
- Arriendo y alojamiento de servidores (housing)

- Mantención y operación de aplicaciones Web
- Servicios de software a través de Web (ASP)
- Servicios de Internet en general
- Asesorías en el diseño de redes y servicios de conectividad.

Razón Social:	Datacare Ltda.
Dirección:	Pablo Neruda #01765
Región:	Araucanía
Ciudad:	Temuco
Email:	datacare@datacare.cl
Teléfono/Fax:	231224
Nombre Representante Legal:	Sergio Troncoso U
Giro:	Asesorías y Servicios Tecnológicos.

Tabla A.1 Datos Datacare Ltda.

Su visión como Organización, es convertirse en la empresa líder en hosting para las organizaciones públicas y privadas, que deseen mejorar su presencia en la red.

Su misión como organización, es potenciar el desarrollo de las organizaciones mediante el uso de tecnologías de Internet para mejorar sus procesos de negocios y a su gestión general, a través de un alto nivel profesional.

Por lo anterior, sus objetivos son asegurar el funcionamiento de los servicios proporcionados a los clientes, responsablemente, a través del uso de la mejor tecnología disponible. Mantener un trato directo y personalizado con los clientes para anticipar la identificación de nuevas necesidades, además de mantener informado a los clientes del estado y funcionamiento de sus servicios. Realizar permanentemente investigación y desarrollo de tecnologías de información y comunicaciones (TIC), para la mejora de los servicios.

ANEXO B – Instalación de Nagios

Nagios

Artículo I. Fedora Quickstart

Introduction

This guide is intended to provide you with simple instructions on how to install Nagios from source (code) on Fedora and have it monitoring your local machine inside of 20 minutes. No advanced installation options are discussed here - just the basics that will work for 95% of users who want to get started.

These instructions were written based on a standard **Fedora Core 6** Linux distribution.

What You'll End Up With

If you follow these instructions, here's what you'll end up with:

- Nagios and the plugins will be installed underneath `/usr/local/nagios`
- Nagios will be configured to monitor a few aspects of your local system (CPU load, disk usage, etc.)
- The Nagios web interface will be accessible at `http://localhost/nagios/`

Prerequisites

During portions of the installation you'll need to have **root** access to your machine.

Make sure you've installed the following packages on your Fedora installation before continuing.

- Apache
- GCC compiler
- GD development libraries

You can use `yum` to install these packages by running the following commands (as root):

```
yum install httpd
yum install gcc
yum install glibc glibc-common
yum install gd gd-devel
```

1) Create Account Information

Become the root user.

```
su -l
```

Create a new *nagios* user account and give it a password.

```
/usr/sbin/useradd -m nagios  
passwd nagios
```

Create a new *nagcmd* group for allowing external commands to be submitted through the web interface. Add both the *nagios* user and the *apache* user to the group.

```
/usr/sbin/groupadd nagcmd  
/usr/sbin/usermod -a -G nagcmd nagios  
/usr/sbin/usermod -a -G nagcmd apache
```

2) Download Nagios and the Plugins

Create a directory for storing the downloads.

```
mkdir ~/downloads  
cd ~/downloads
```

Download the source code tarballs of both Nagios and the Nagios plugins (visit

<http://www.nagios.org/download/> for links to the latest versions). At the time of writing, the latest versions of Nagios and the Nagios plugins were 3.0.3 and 1.4.11, respectively.

```
wget http://osdn.dl.sourceforge.net/sourceforge/nagios/nagios-  
3.0.6.tar.gz  
wget http://osdn.dl.sourceforge.net/sourceforge/nagiosplug/nagios-  
plugins-1.4.11.tar.gz
```

3) Compile and Install Nagios

Extract the Nagios source code tarball.

```
cd ~/downloads  
tar xzf nagios-3.0.6.tar.gz  
cd nagios-3.0.6
```

Run the Nagios configure script, passing the name of the group you created earlier like so:

```
./configure --with-command-group=nagcmd
```


Compile the Nagios source code.

```
make all
```

Install binaries, init script, sample config files and set permissions on the external command directory.

```
make install
make install-init
make install-config
make install-commandmode
```

Don't start Nagios yet - there's still more that needs to be done...

4) Customize Configuration

Sample configuration files have now been installed in the `/usr/local/nagios/etc` directory. These sample files should work fine for getting started with Nagios. You'll need to make just one change before you proceed...

Edit the `/usr/local/nagios/etc/objects/contacts.cfg` config file with your favorite editor and change the email address associated with the `nagiosadmin` contact definition to the address you'd like to use for receiving alerts.

```
vi /usr/local/nagios/etc/objects/contacts.cfg
```

5) Configure the Web Interface

Install the Nagios web config file in the Apache conf.d directory.

```
make install-webconf
```

Create a `nagiosadmin` account for logging into the Nagios web interface. Remember the password you assign to this account - you'll need it later.

```
htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Restart Apache to make the new settings take effect.

```
service httpd restart
```



Note: Consider implementing the enhanced CGI security measures described [here](#) to ensure that your web authentication credentials are not compromised.

6) Compile and Install the Nagios Plugins

Extract the Nagios plugins source code tarball.

```
cd ~/downloads
tar xzf nagios-plugins-1.4.11.tar.gz
cd nagios-plugins-1.4.11
```

Compile and install the plugins.

```
./configure --with-nagios-user=nagios --with-nagios-group=nagios
make
make install
```

7) Start Nagios

Add Nagios to the list of system services and have it automatically start when the system boots.

```
chkconfig --add nagios
chkconfig nagios on
```

Verify the sample Nagios configuration files.

```
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

If there are no errors, start Nagios.

```
service nagios start
```

8) Modify SELinux Settings

Fedora ships with SELinux (Security Enhanced Linux) installed and in Enforcing mode by default. This can result in "Internal Server Error" messages when you attempt to access the Nagios CGIs.

See if SELinux is in Enforcing mode.

```
getenforce
```

Put SELinux into Permissive mode.

```
setenforce 0
```

To make this change permanent, you'll have to modify the settings in `/etc/selinux/config` and reboot.

Instead of disabling SELinux or setting it to permissive mode, you can use the following command to run the CGIs under SELinux enforcing/targeted mode:

```
chcon -R -t httpd_sys_content_t /usr/local/nagios/sbin/  
chcon -R -t httpd_sys_content_t /usr/local/nagios/share/
```

For information on running the Nagios CGIs under Enforcing mode with a targeted policy, visit the NagiosCommunity.org wiki at <http://www.nagioscommunity.org/wiki>.

9) Login to the Web Interface

You should now be able to access the Nagios web interface at the URL below. You'll be prompted for the username (*nagiosadmin*) and password you specified earlier.

<http://localhost/nagios/>

Click on the "Service Detail" navbar link to see details of what's being monitored on your local machine. It will take a few minutes for Nagios to check all the services associated with your machine, as the checks are spread out over time.

10) Other Modifications

Make sure your machine's firewall rules are configured to allow access to the web server if you want to access the Nagios interface remotely.

Configuring email notifications is out of the scope of this documentation. While Nagios is currently configured to send you email notifications, your system may not yet have a mail program properly installed or configured. Refer to your system documentation, search the web, or look to the [NagiosCommunity.org wiki](http://www.nagioscommunity.org/wiki) for specific instructions on configuring your system to send email messages to external addresses. More information on notifications can be found [here](#).

11) You're Done

Congratulations! You successfully installed Nagios. Your journey into monitoring is just beginning. You'll no doubt want to monitor more than just your local machine, so check out the following docs...

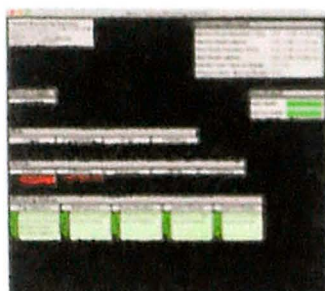
- [Monitoring Windows machines](#)
- [Monitoring Linux/Unix machines](#)
- [Monitoring Network servers](#)
- [Monitoring routers/switches](#)
- [Monitoring publicly available services \(HTTP, FTP, SSH, etc.\)](#)

ANEXO C – Screenshots de Nagios

Nagios® Screenshots



Main Splash Screen



Tactical Overview



Service Detail



Host Detail



Hostgroup Overview



Hostgroup Summary



Hostgroup Grid



Service Problems



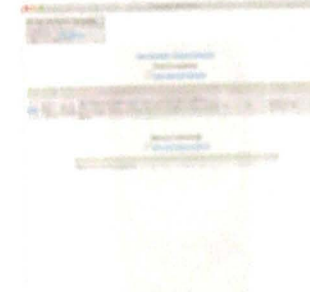
Circular Status Map



Balloon Status Map



Tree Status Map



Comments



Scheduled Downtime



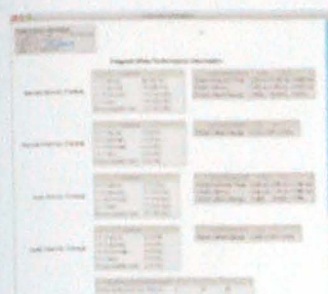
Scheduling Host Downtime



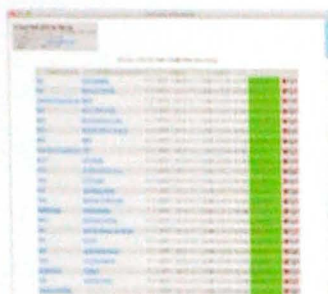
Scheduling Service Downtime



Nagios Process Info



Performance Info



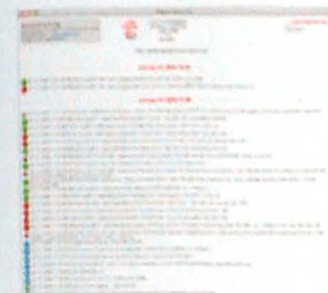
Scheduled Event Queue



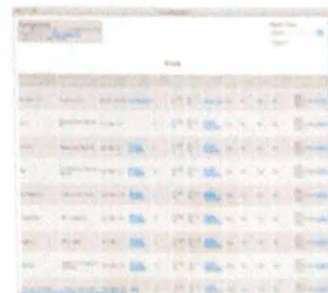
Alert History



Notification History



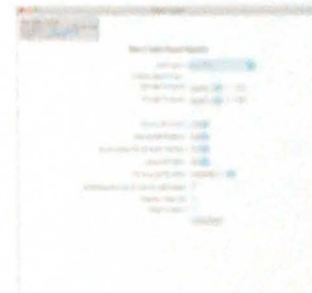
Event Log



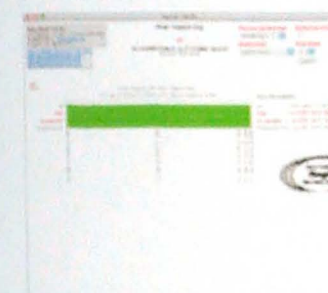
Configuration View



Alert Summary Menu



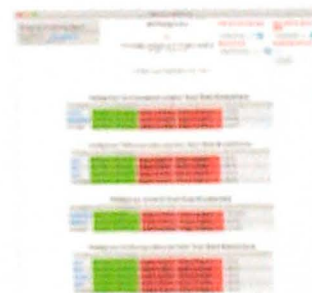
Trends Menu



Host State Trends



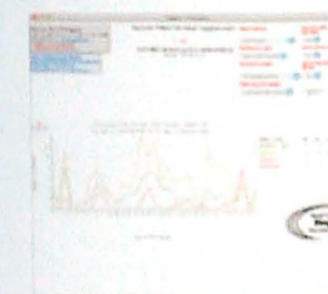
Service State Trends



Hostgroup Availability Report



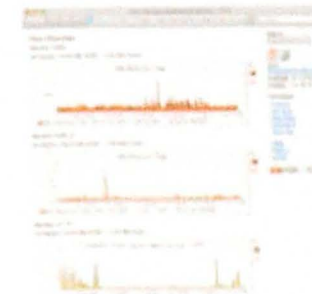
Service Availability Report



Service Alert Histogram



Host Alert Histogram



PNP Addon Graphs



WAP Interface