IMPLEMENTACIÓN DE HERRAMIENTAS PARA EL MONITOREO DE LA RED Y PARA EL CONTROL DE INVENTARIOS. Y REALIZACIÓN DE LA ACTUALIZACIÓN DEL PLAN DE CONTINGENCIA DE LA ORGANIZACIÓN

MILTON ESCOBAR CEBALLOS

UNIVERSIDAD CATÓLICA POPULAR DEL RISARALDA
PROGRAMA DE INGENIERÍA DE SISTEMAS Y TELECOMUNICACIONES
PRACTICAS PROFESIONALES
PEREIRA
2010

IMPLEMENTACIÓN DE HERRAMIENTAS PARA EL MONITOREO DE LA RED Y PARA EL CONTROL DE INVENTARIOS. Y REALIZACIÓN DE LA ACTUALIZACIÓN DEL PLAN DE CONTINGENCIA DE LA ORGANIZACIÓN

MILTON ESCOBAR CEBALLOS

Informe de Práctica Profesional

TUTOR

Ehumir Salazar Rojas
Especialista en Telecomunicaciones

UNIVERSIDAD CATÓLICA POPULAR DEL RISARALDA
PROGRAMA DE INGENIERÍA DE SISTEMAS Y TELECOMUNICACIONES
PRACTICAS PROFESIONALES
PEREIRA
2010

CONTENIDO

Pág.

LISTA DE ILUSTRACIONES

Pág.

RESUMEN	ABSTRACT
La implementación de software libre dentro de las organizaciones, es una ventaja de tipo económico, ya que existen herramientas que permiten brindar servicios específicos, de alta calidad y un nivel de estabilidad bastante alto, las herramientas de monitoreo y de control de Inventario, que se utilizan en este proyecto, se encuentran licenciadas bajo el concepto de software libre y cada una cuenta con su respetiva documentación, en donde podemos encontrar las especificaciones y la guía de la instalación. Un plan de contingencia siempre debe estar actualizado y disponible para ser aplicado en el momento que sea necesario o en caso de emergencia, por lo tanto, una organización debe entender lo importante que es tener uno bien elaborado.	The implementation of free software within the organizations is an advantage of an economic, as There are tools to provide services specific, high quality and level of stability quite high, and monitoring tools Inventory control, which are used in this project, are licensed under the concept of software free and each one has its respects documentation where we can find the specifications and guidance Installation. A contingency plan should always be updated and available to be applied when necessary or in case of emergency, therefore, an organization must understand how important it is to have a well crafted.
DESCRIPTORES: Monitoreo, Control de Inventario, Plan de Contingencia, Nagios, Ocs Inventory, Centos 5.2	KEY WORDS: Monitoring, Inventary Control, Contingency Plan, Nagios, Ocs Inventory, Centos 5.2

INTRODUCCIÓN

Para muchas organizaciones el recurso más importante es la información, lo que implica que se haga necesaria la inversión de dinero para su protección y para un buen manejo de la misma, en muchos casos la información se maneja de forma digital y esto implica que se tengan Servidores, Bases de Datos, y aplicaciones para manejar dicha información. En la empresa Une Telefónica de Pereira se maneja la información de forma digital y se tienen implementados servidores para manejarla y a su vez brindarle una mayor confiabilidad y seguridad a los datos.

Partiendo de la necesidad de mantener con una alta disponibilidad la información, la organización sugirió la implementación de un sistema de monitoreo y a su vez una herramienta para el control de inventario y de esta forma poder evitar futuros problemas legales, dentro de la misma propuesta por parte de la empresa se planteo realizar una actualización a un plan de contingencia con el cual cuenta la organización, y por medio del que pretenden estar totalmente preparados para alguna eventualidad generada por cualquier tipo de emergencia.

Para la elaboración de dichas implementaciones, y actualizaciones se conto con la atenta colaboración de los administradores de la red, el administrador de bases de datos y el administrador de la seguridad de las redes informáticas de la empresa, los cuales facilitaron toda la información necesaria para el acceso a las plataformas de tecnología de la subgerencia de tecnologías de información de Une Telefónica de Pereira.

1. PRESENTACIÓN DE LA ORGANIZACIÓN O SITIO DE PRÁCTICA

1.1 HISTORIA

LOS PRIMEROS PASOS: Un grupo de visionarios Pereiranos viajó a Alemania en 1925 a la Feria de la Ciencia y se dio cuenta de que las plantas de teléfonos existentes en Bogotá, Cali y Medellín serían obsoletas en poco tiempo. Necesitaban para su operación de telefonistas e interconexión de cables en cada llamada. Decidieron que para Pereira había que comprar una planta automática. Corría el año de 1927 cuando se firmó el contrato directamente entre el Concejo Municipal que presidía Julio Castro y la empresa alemana Siemens. Un hito histórico para la ciudad y el continente, pues hasta ese momento, sólo Montevideo, la capital uruguaya, contaba con telefonía automatizada.

LLEGARON LOS ALEMANES: En ese mismo año (1927), llegaron a la Pereira de calles empedradas tiradas a cordel y por las que transitaban recuas de mulas con su abundante carga proveniente desde todas las direcciones, y construcciones de una o dos plantas, 3 técnicos alemanes de la Siemens: Alejandro Clark, Miguel Mauser y Enrique Hoppe.

El trío alemán inició sus labores utilizando personal colombiano, sin ninguna capacitación. Fue así como se formaron los tres más importantes personajes del servicio telefónico de aquella primera época: Luis Ángel Piedrahita, Juan de J. Franco y Florentino Arias.

EL MONTAJE: Se inició el montaje de la primera planta telefónica automática de Colombia, con la orientación y el control de todos los trabajos del ingeniero Alejandro Clark, seguido por Misael Mausser, responsable del montaje de planta y Enrique Hoppe como empalmador de cables. Los 3 eran maestros del personal colombiano, pero además en un cruce fraterno, aprendieron de éstos las bondades de la tierra del café.

LA FINANCIACIÓN: La financiación para una ciudad apenas en formación, de tan solo un poco más de 50 años de fundada, significó un gran esfuerzo de sus gentes y un empréstito del Banco Central Hipotecario en cuantía de un millón de pesos del cual se tomaron $120 mil pesos para el nuevo servicio de teléfonos. Mediante el acuerdo No.50 de septiembre 30 de 1927 el Concejo

Municipal de Pereira aprobó el contrato con Siemens y Halke...“ para dar servicio a mil líneas automáticas, con todo su equipo de comunicación que permita posteriormente su fácil aumento hasta 10.000 líneas sin que haya necesidad de modificación de ninguna clase".

PEREIRA EN 1929 YA TENIA TELEFONÍA AUTOMÁTICA: La población de Pereira para el año de 1929 era apenas de 55 mil habitantes de pie descalzo y actividades primarias de sustento diario, con los parques de La Libertad, El Lago y la Plaza de Bolívar como sus límites y las aguas aún limpias y abundantes del río Otún como su frontera. Para este contexto histórico la celebración de la inauguración de su planta telefónica era desconcertante, casi innecesaria, pero señalaba características propias de los pereiranos y que la historia se ha encargado de reconocerles: tenacidad y empuje . Buscar teléfonos automáticos en semejante latitud y condiciones no era más que la premonición de grandes obras del futuro y una confianza de que el teléfono formaría parte sustancial de una vida moderna muy cerca a los aleros de sus casas de tapia, pesebrera y grandes patios llenos de flores.

Los historiadores no se ponen de acuerdo si finalmente la cifra de los primeros abonados era de 500 o 700, pero lo cierto del caso es que sobraron líneas y así lo registra el Directorio de 1930 publicado por la tipografía Moderna.

El primer Gerente fue don Manuel Orozco Patiño. La primera campaña de mercadeo, fue la instalación de dos teléfonos de servicio público gratuitos en el más importante establecimiento de la época: el café Centro Social en la 18 con 8a. El objeto de la campaña era ganar suscriptores "El teléfono es un magnífico compañero. Entonces si todo el mundo tiene, usted porqué carece de él", rezaba la frase de combate de esa campaña.

HECHOS DE LA HISTORIA

- 1934 Se dio servicio a la región, hoy municipio, de Dosquebradas. Se estableció la larga distancia, por cable físico, con Santa Rosa de Cabal, Chinchiná y Manizales.

- 1935 Se extendió el servicio a la ciudad de Cartago

- 1937 Se hizo la conexión de larga distancia con la Compañía Central del Pacífico para comunicación con Cali e intermedias. En ese mismo año se extendió la larga distancia a Medellín.

- 1945 Terminada la II guerra mundial, se hace el primer ensanche.

- 1962 Ya se hacía el segundo ensanche en la planta telefónica y se copaba la capacidad total de 6 mil líneas.

- 1966 Ya se han hecho ensanches a 5 mil líneas más, lo que condujo a incrementar la numeración de 4 a 5 números, lo que además llevó a implementar una nueva central de mil líneas mediante el traslado de los correspondientes equipos a la sub central de Dosquebradas.

- 1972 Ensanche de 4 mil 300 líneas más.

- 1979 El temblor de noviembre de ese año obligó a desocupar las 5 plantas superiores del edificio donde estaba la Central principal para evitar su derrumbe total. La ciudadanía se movilizó para apuntalar muros, paredes y asegurar pisos, evitando así el derrumbe de la construcción, sepultando en escombros, 50 años de una obra que es orgullo de la conciencia cívica y futurista de los Pereiranos.

- 1986 Con la tecnología del futuro, Pereira empezó en ese año a instalar en Colombia las primeras centrales digitales EWSD con múltiplex de tiempo, empleando modulación por pulso (PCM). De nuevo Pereira marcó un hito en la historia.

- 1996 Con el proceso de instalación de las 80 mil líneas, se marca otro hito histórico de la Empresa y la ciudad. Se satisfizo la demanda insatisfecha de varios años. Cualquier pereirano podía ahora tener su propia línea telefónica

- En el año de 1996 mediante el acuerdo No. 30 expedido por el Concejo Municipal de Pereira en el que se facultaba al Alcalde Juan Manuel Arango Vélez, para la transformación de una de las organizaciones más importantes de la ciudad y la región en proceso de liquidación, Las Empresas Públicas de Pereira, como aparece en los documentos de la época:

- Hasta el año 2006 las Empresas Públicas de Medellín ha adquirido más del 56% de la participación accionaria de la compañía, e introdujo nuevos servicios no sólo de redes telefónicas e Internet, sino un nuevo canal de televisión gracias al servicio por suscripción. A pesar que sus acciones

corresponden en más de la mitad a la empresa antioqueña, la Empresa sigue teniendo autonomía en las decisiones para la prestación de los servicios en el Área Metropolitana del Centro Occidente, Santa Rosa de Cabal y Cartago; el 43% de las acciones pertenecen al Municipio de Pereira, y el otro 0.14% pertenece a los extrabajadores y jubilados.

- El estar a la vanguardia de la innovación en tecnología, en los procesos de gestión interna, en el cumplimiento de estándares internacionales de calidad y gestión social a Telefónica de Pereira, obtener en los últimos años certificaciones ISO 9001(certificado de calidad) y de adhirió al Pacto Mundial de la ONU. En el año 2003 UNE Telefónica de Pereira logró su certificación ISO 9001 conferida por la firma francesa BVQI.

- En el 2005 la Empresa se adhirió al Pacto Mundial de las Naciones Unidas, para el respeto no sólo de los derechos laborales, humanos, sino también medioambientales, y de lucha contra la corrupción. Hoy día, el documento continúa siendo objeto de sensibilización a los trabajadores, a través de los medios internos, con el fin de informar a sus clientes internos y externos el documento que los hizo integrantes a dicho Pacto de la ONU. El 25 de noviembre del mismo año, Telefónica logró su certificación en OHSAS 18001 contando como ente certificador a la misma de la firma francesa BVQI, con lo cual se convierte en la primera empresa de Servicios en Telecomunicaciones en Colombia certificada contra esta norma.

- En 2006 la Empresa inicia su proceso de verificación de requisitos para certificación en los sistemas de Gestión Ambiental con la norma 14000 y el de Responsabilidad Social (norma S.A. 8000) convirtiéndose en la primera empresa a nivel nacional en lograr certificar estos cuatros sistemas de gestión e implementar uno de forma Integral.

- A finales del año 2007 se empezó hacer el cambio de sede para el Edificio Inteligente, donde se encuentran hoy en día las instalaciones de UNE-Telefónica de Pereira y donde se están llevando proyectos de alta exigencia y mejoramiento como Proyecto Evolución, el cual se ejecutó con el acompañamiento de la firma consultora BM Consulting Group, buscando incrementar la productividad dentro de la Empresa.

Actualmente cuenta con una excelente oferta de productos de telecomunicaciones, empaquetamientos y calidad en la prestación de servicios; es una empresa 100% nacional, con un espectacular equipo de trabajo, hacemos la diferencia con talento humano

1.2 MISIÓN

Somos una empresa orientada al cliente prestando servicios integrales de telecomunicaciones.

1.3 VISIÓN

Seremos la Empresa de telecomunicaciones líder en la región por su excelencia en el servicio con compromiso social.

1.4 VALORES

- Integridad
- Excelencia
- Respeto
- Compromiso
- Responsabilidad Social

1.5 SERVICIOS QUE PRESTA

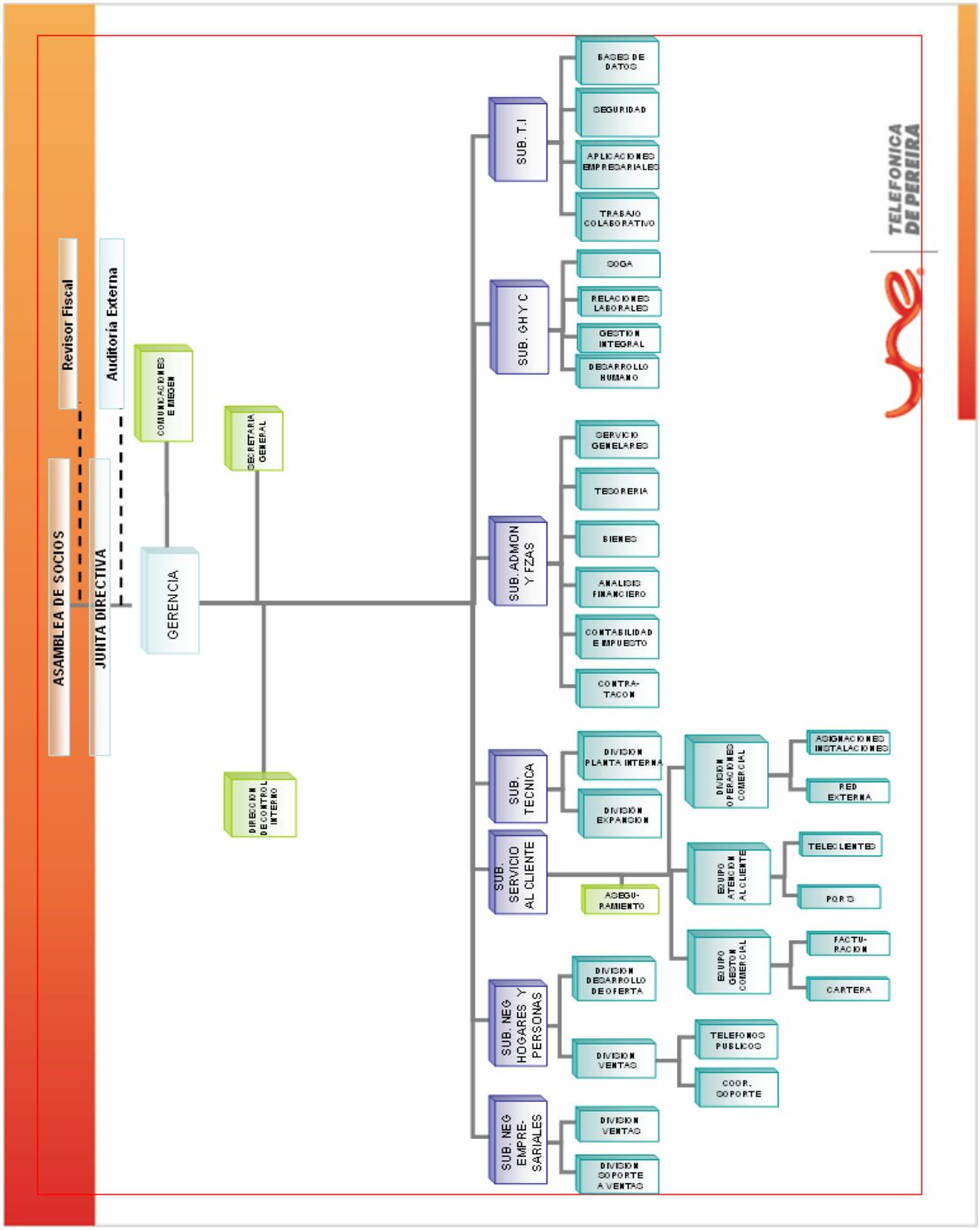
- Telefonía
- Televisión
- Banda ancha
- Internet dedicado
- Ultimas millas
- Transmisiones datos
- Iptv
- Voip
- IP centrex
- PBX
- Soluciones especiales
- Entre otros.

1.6 NÚMERO DE EMPLEADOS

Aproximadamente 800

1.7 ESTRUCTURA ORGÁNICA

Ilustración 1. Estructura Orgánica UNE Telefónica de Pereira



2. DEFINICIÓN DE LA LÍNEA DE INTERVENCIÓN

La práctica se llevara a cabo en el área de las Telecomunicaciones, ejerciendo tareas de implementación y documentación de la estructura de Red, de la empresa de Telecomunicaciones de Pereira.

3. DIAGNÓSTICO DEL ÁREA DE INTERVENCIÓN

Se utilizo el instrumento de observación directa e indirecta para la recolección de la información acerca de cómo se encuentra la infraestructura de TI, en la empresa UNE Telefónica de Pereira S.A.

De forma directa se pudo observar que se cuenta con infraestructura de red y ofimática bastante robustas, lo cual se encuentra en un correcto funcionamiento, también se cuenta con un plan de contingencia bien elaborado pero a la fecha desactualizado, se tuvo acceso a este documento para su análisis.

De forma indirecta, se pudo obtener información sobre algunos procesos que son importantes en la organización pero no se encuentran implementados, como los son el monitoreo de servidores de alto impacto para la compañía, y por último el plan de contingencia que requiere ser actualizado.

Por el número total de usuarios que a la fecha suman 800 aproximadamente se requiere del apoyo de soporte de red y ofimática debido a cambios en las diferentes plataformas implementadas este año, entre ellas el sistema de correo electrónico y una migración de la aplicación CORE de la empresa. Por lo anterior se brinda soporte y apoyo a estos procesos de manera directa y permanente.

4. EJE DE INTERVENCIÓN

La Empresa de Telecomunicaciones de Pereira, en el área de TI tiene la necesidad de suplir algunas deficiencias para las cuales ha planteado las siguientes prioridades:

- La implementación de una herramienta para el monitoreo de servidores, y de esta forma poder tener un mayor control sobre sus procesos y servicios.

- La implementación de una herramienta alterna que realice el constante inventario de hardware y software de los equipos de la organización.

- Realizar el estudio detallado y la actualización del Plan de Contingencia con el cual cuenta la empresa.

5. JUSTIFICACIÓN DEL EJE DE INTERVENCIÓN

La tecnología con el pasar de los días crece y mejora a un nivel acelerado, la información se convierte en un activo demasiado importante para una organización la cual debe de tenerla siempre protegida y a la vez disponible, los servidores son aquellos componentes que permiten administrar la información, para esto debe de existir planes de respaldo, una empresa no puede desperdiciar tiempo levantando sus servicios, porque necesita seguir produciendo a esto viene que se tenga un plan B a la hora de que pueda llegar a fallar algo en la misma, esto debe de estar documentado, adicional a esto si se cuenta con todo un sistema de monitoreo constante sobre los servidores se podría evitar tener que utilizar el plan B, y además poder realizar operaciones correctivas en los sistemas.

Para una organización es muy difícil estar continuamente verificando que software y que hardware tienen instalados sus empleados en su respectiva estación de trabajo, puesto que son muchas las estaciones a las que tendrían que realizarle el respectivo estudio, por lo tanto existen herramientas que se encargan de realizarlo automáticamente, realizar este tipo de control de inventario de cada máquina es muy importante, para evitar la instalación de software sin licencia, y de hardware no autorizado.

En la empresa de Telecomunicaciones de Pereira, no se tiene resuelto el problema del monitoreo de los servidores, se cuenta con un Plan de contingencia el cual esta desactualizado, estos problemas se buscan ser resueltos con esta práctica.

6. OBJETIVO GENERAL

Implementar herramientas para la monitorización de la red y para el control de inventarios. Y realizar la actualización del plan de Contingencia de la organización.

7. OBJETIVOS ESPECÍFICOS

- Ofrecer apoyo de soporte de red y ofimática
- Investigar sobre herramientas de monitoreo y control de inventario
- Elegir una herramienta para monitoreo e investigar acerca de la misma
- Implementar herramienta elegida para monitoreo
- Documentar la instalación de la herramienta elegida para monitoreo
- Elegir una herramienta para Control de Inventario e investigar acerca de la misma
- Implementar herramienta elegida para Control de Inventario
- Documentar la instalación de la herramienta elegida para Control de Inventario
- Realizar evaluación del estado actual del Plan de contingencia
- Realizar las actualizaciones correspondientes, para el Plan de Contingencia.

8. REFERENTES CONCEPTUALES

8.1 MONITOREO

La información es esencial para las decisiones que hacemos y las acciones que tomamos. La información oportuna y precisa permite:

- Aprender de las experiencias de otros.
- Identificar y capitalizar las oportunidades.
- Evitar situaciones de peligro o de riesgo.

El monitoreo y la evaluación significa recoger y usar información. Mientras que en la mayoría de los aspectos de nuestras vidas se reconoce la importancia de la información, en el contexto de proyectos y organizaciones no se reconoce la importancia de la información obtenida del monitoreo y evaluación. Con frecuencia, en el campo del desarrollo, el monitoreo es un requisito impuesto por los donantes en las instituciones. Como tal, los que reciben financiamiento son renuentes a realizar las actividades de monitoreo requeridas. El monitoreo también es visto como un fin en sí mismo, por lo que algunos gerentes de proyecto completan formularios y preparan informes sin que necesariamente utilicen la información para la evaluación interna y planificación del programa.

De manera similar, la evaluación se conduce con frecuencia para satisfacer requisitos externos o hacer un juicio sobre si un proyecto debe continuar recibiendo financiación. Con menos frecuencia, la evaluación es una herramienta para fortalecer un proyecto y empoderar a los participantes o clientes del proyecto.

La habilidad de adquirir y usar información relevante es tan importante para una red de defensa y promoción. Un componente de monitoreo y evaluación de impacto ayuda a la red a seguir la pista de sus éxitos, lograr credibilidad con los donantes, y motiva a los miembros a mantener el ritmo de trabajo. Si las actividades de defensa y promoción de una red provocan un cambio de política deseado, la red deseará demostrar una clara conexión entre sus objetivos y actividades y el resultado político conseguido.

El monitoreo es el proceso de recoger la información rutinariamente sobre todos los aspectos de una campaña de defensa y promoción y usarla en la administración y toma de decisiones de la red.

Un plan de monitoreo es una herramienta de administración básica y vital que provee a los miembros de la red y a otros interesados información que es esencial para el diseño, implementación, administración, y evaluación de las actividades de defensa y promoción. Para cumplir la función de monitoreo, el plan debe incluir sistemas para la recolección de datos e información sobre actividades claves, así como sistemas para sintetizar, analizar, y usar la información para tomar decisiones e iniciar acciones. La información del monitoreo puede ayudar a:

- Demostrar estrategias innovadoras y eficaces
- Generar apoyo financiero y político para las actividades de defensa y promoción
- Mejorar la imagen de la red.

La evaluación involucra un análisis objetivo y sistemático del desempeño de la red, su eficiencia e impacto con relación a sus objetivos. Su propósito final es

- Recoger lecciones de la experiencia para mejorar la calidad de una campaña de defensa y promoción
- Mejorar el diseño de campañas futuras y
- Demostrar los méritos de la red a los/las partidarios/as, políticos/as, donantes, miembros/as, etc.

La evaluación puede pensarse como una valoración en un período crítico, o un proceso para mirar impactos o logros.

8.1.1 Servidor: En informática, un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una

máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.

Este uso dual puede llevar a confusión. Por ejemplo, en el caso de un servidor web, este término podría referirse a la máquina que almacena y maneja los sitios web, y en este sentido es utilizada por las compañías que ofrecen hosting u hospedaje. Alternativamente, el servidor web podría referirse al software, como el servidor de http de Apache, que funciona en la máquina y maneja la entrega de los componentes de los páginas web como respuesta a peticiones de los navegadores de los clientes.

Los archivos para cada sitio de Internet se almacenan y se ejecutan en el servidor. Hay muchos servidores en Internet y muchos tipos de servidores, pero comparten la función común de proporcionar el acceso a los archivos y servicios.

Un servidor sirve información a los ordenadores que se conecten a él. Cuando los usuarios se conectan a un servidor pueden acceder a programas, archivos y otra información del servidor.

En la web, un servidor web es un ordenador que usa el protocolo http para enviar páginas web al ordenador de un usuario cuando el usuario las solicita.

Los servidores web, servidores de correo y servidores de bases de datos son a lo que tiene acceso la mayoría de la gente al usar Internet.

Algunos servidores manejan solamente correo o solamente archivos, mientras que otros hacen más de un trabajo, ya que un mismo ordenador puede tener diferentes programas de servidor funcionando al mismo tiempo.

Los servidores se conectan a la red mediante una interfaz que puede ser una red verdadera o mediante conexión vía línea telefónica o digital.

- Tipos de servidores

- Plataformas de Servidor (Server Platforms): Un término usado a menudo como sinónimo de sistema operativo, la plataforma es el hardware o software subyacentes para un sistema, es decir, el motor que dirige el servidor.

- Servidores de Aplicaciones (Application Servers): Designados a veces como un tipo de middleware (software que conecta dos aplicaciones), los servidores de aplicaciones ocupan una gran parte del territorio entre los servidores de bases de datos y el usuario, y a menudo los conectan.

- Servidores de Audio/Video (Audio/Video Servers): Los servidores de Audio/Video añaden capacidades multimedia a los sitios web permitiéndoles mostrar contenido multimedia en forma de flujo continuo (streaming) desde el servidor.

- Servidores de Chat (Chat Servers): Los servidores de chat permiten intercambiar información a una gran cantidad de usuarios ofreciendo la posibilidad de llevar a cabo discusiones en tiempo real.

- Servidores de Fax (Fax Servers): Un servidor de fax es una solución ideal para organizaciones que tratan de reducir el uso del teléfono pero necesitan enviar documentos por fax.

- Servidores FTP (FTP Servers): Uno de los servicios más antiguos de Internet, File Transfer Protocol permite mover uno o más archivos

- Servidores Groupware (Groupware Servers): Un servidor groupware es un software diseñado para permitir colaborar a los usuarios, sin importar la localización, vía Internet o vía Intranet corporativo y trabajar juntos en una atmósfera virtual.

- Servidores IRC (IRC Servers): Otra opción para usuarios que buscan la discusión en tiempo real, Internet Relay Chat consiste en varias redes de servidores separadas que permiten que los usuarios conecten el uno al otro vía una red IRC.

- Servidores de Listas (List Servers): Los servidores de listas ofrecen una manera mejor de manejar listas de correo electrónico, bien sean discusiones interactivas abiertas al público o listas unidireccionales de anuncios, boletines de noticias o publicidad.

- Servidores de Correo (Mail Servers): Casi tan ubicuos y cruciales como los servidores Web, los servidores de correo mueven y almacenan el correo electrónico a través de las redes corporativas (vía LANs y WANs) y a través de Internet.

- Servidores de Noticias (News Servers): Los servidores de noticias actúan como fuente de distribución y entrega para los millares de grupos de noticias públicos actualmente accesibles a través de la red de noticias USENET.

- Servidores Proxy (Proxy Servers): Los servidores proxy se sitúan entre un programa del cliente (típicamente un navegador) y un servidor externo (típicamente otro servidor web) para filtrar peticiones, mejorar el funcionamiento y compartir conexiones.

- Servidores Telnet (Telnet Servers): Un servidor telnet permite a los usuarios entrar en un ordenador huésped y realizar tareas como si estuviera trabajando directamente en ese ordenador.

- Servidores Web (Web Servers): Básicamente, un servidor web sirve contenido estático a un navegador, carga un archivo y lo sirve a través de la red al navegador de un usuario. Este intercambio es mediado por el navegador y el servidor que hablan el uno con el otro mediante HTTP. Se pueden utilizar varias tecnologías en el servidor para aumentar su potencia más allá de su capacidad de entregar páginas HTML; éstas incluyen scripts CGI, seguridad SSL y páginas activas del servidor (ASP).

8.1.2 Servicios de red. Es la fundación de un ambiente que computa networked. Los servicios de red están instalados generalmente en uno o más servidores para proporcionar recursos compartidos a cliente computadoras.

Los servicios de red se configuran en corporativo LAN' s para asegurar seguridad y la operación de uso fácil. Ayudan al LAN para funcionar suavemente y eficientemente. Servicios de red corporativos del uso de LANs tales como DNS (Domain Name System) para dar nombres a IP y Direcciones del MAC (la gente recuerda nombres como “nm.lan” mejor que ella recuerda números como “210.121.67.0 .18”), y DHCP para asegurarse de que cada uno en la red tenga un IP address válido.

DHCP facilita carga administrativa automatizando la asignación del IP de nodos en la red. La adición o quitar de nodos de la red no crea problemas con la recuperación del IP address; el servicio de DHCP dirige esto automáticamente. Los servidores de la autentificación son otro servicio de red, permiten que cada usuario tenga su propia cuenta, y todo que lo hacen por eso se registra bajo su nombre del usuario. Esto significa que no sólo es usuarios responsables cualquier cosa hacen mientras que en la red, pero también aumenta seguridad mientras que cualquier persona que desea tener acceso al LAN debe tener un nombre y una contraseña registrados del usuario.

Hacer la administración de la red sin tener cuentas del usuario para seguir la actividad del usuario (ilegal o de otra manera) o DHCP para automatizar la asignación del IP a los nodos, o el DNS para simplificar el acceso del IP address sería molesto de hecho. Permitiendo estos pocos servicios de red automatiza la administración compleja y desperdiciadora de tiempo a la red, y facilita así el tiempo muerto para los administradores de la red.

El email, imprimiendo y el archivo de la red que comparte servicios son también servicios de red. No se utilizan raramente en un ambiente del LAN, mientras que permiten que los usuarios tengan acceso a cualquier impresora conectada con la red, los archivos en el servidor u otros nodos conectados, y la transferencia de datos aerodinámica dentro de la red. Requieren a usuarios tener permisos de tener acceso a los recursos compartidos, y son simples configurar las derechas de la seguridad y de acceso para, con el servicio del directorio también un servicio de red.

Los servicios de red comunes incluyen:

- Servidores de la autentificación: sea servidores eso proporciona autentificación servicios a usuarios o otros sistemas. Los usuarios y otros servidores authentican a tal servidor, y reciben criptográfico boletos. Estos boletos entonces se intercambian el uno con el otro para verificar identidad.

La autentificación se utiliza como la base para autorización (determinándose si a privilegio será concedido a un usuario particular o proceso), aislamiento (guardando la información de el saberse a los no-participantes), y no-renegación (no pudiendo negar el hacer algo que era autorizado ser hecho basó en autentificación).

La autentificación principal algoritmos se utilizan contraseñas, Kerberos, y cifrado dominante público.

- Servicios del directorio: Antes de definir Que es un servicio del directorio uno debe entender cuál es el significado de un directorio. Fundamental, un directorio es como un diccionario; permite que uno mire para arriba un nombre y que recupere los artículos de la información asociados a ese nombre. Justo como una palabra en un diccionario puede tener definiciones múltiples, múltiplo que diversos pedazos de información se pueden asociar a un nombre dado. Y apenas como una palabra puede tener diversas partes del discurso, con diversas definiciones asociadas, un nombre en un directorio puede también tener muchos diversos tipos de datos

Desemejante de un diccionario típico, los nombres en un directorio se organizan en un árbol jerárquico, y cada nodo en el árbol representa un nombre válido que pueda tener su propio sistema de datos asociados. (De hecho, un diccionario es justo un caso degenerado de un directorio, donde está solamente un profunda la jerarquía llano.)

Los directorios pueden ser muy estrechos en alcance, apoyando solamente un sistema pequeño de tipos del nodo y de tipos de datos, o pueden ser muy amplios, apoyando un sistema arbitrario o extensible, en un diccionario, todos los nodos son palabras. En una guía de teléfonos, todos los nodos son nombres y los artículos de datos son principalmente números de teléfono justos. Ésos son dos ejemplos muy simples de directorios. En DNS todos los nodos son nombres del dominio o direcciones del Internet. El DNS utiliza un directorio levemente más

complejo, con nombres jerárquicos, pero el sistema de tipos usados en el DNS no es fácilmente extensible. En el directorio usado por un sistema operativo de la red, los nodos representan los recursos que son manejados por el OS, incluyendo usuarios, las computadoras, las impresoras y otros recursos compartidos, el etc.

Un servicio del directorio es simplemente el sistema de software que almacena y organiza la información en un directorio, y proporciona el acceso a esa información. Muchos diversos servicios del directorio se han utilizado desde el advenimiento del Internet.

- Protocolo dinámico de la configuración del anfitrión (DHCP): es un protocolo usado por los dispositivos networked (clientes) para obtener los varios parámetros necesarios para los clientes para funcionar en Internet Protocol Red (IP). Usando este protocolo, la carga de trabajo de la administración del sistema disminuye grandemente, y los dispositivos se pueden agregar a la red con configuraciones mínimas o ningunas manuales.

- DNS: Varia información de los asociados (DNS) con nombres del dominio; más importante, sirve como "libro de teléfono "para el Internet traduciendo la computadora human-readable hostnames, e.g. www.example.com, en Direcciones del IP, e.g. 208.77.188.166, que el equipo del establecimiento de una red necesita para entregar la información. También almacena la otra información tal como la lista de servidores del correo eso acepta email para un dominio dado. En el abastecimiento de un mundial palabra clave- el servicio basado del cambio de dirección, el Domain Name System es un componente esencial del contemporáneo Internet uso.

- E-mail: Correo electrónico, abrevió a menudo a E-mail, email, o simplemente correo, es a store-and-forward método de componer, de enviar, de recepción y de almacenar mensajes electrónicos encima de sistemas de comunicación. El término "E-mail" (como un sustantivo o verbo) aplica ambos a Internet sistema del E-mail basado en Simple Mail Transfer Protocol (Smtp) y a X.400 sistemas, y a Intranet sistemas no prohibiendo a usuarios dentro de una organización al E-mail. Intranets puede utilizar Protocolos del Internet o X.400 protocola para el soporte interno del servicio del E-mail workgroup colaboración. El E-mail es de uso frecuente entregar mensajes no solicitados a granel, o "Spam", solamente los programas del filtro existen que pueden suprimir automáticamente alguno o la mayor parte de éstos, dependiendo de la situación.

- Impresión: es un proceso para reproducir el texto y la imagen, típicamente con tinta encendido papel usar una presión de impresión. Se realiza a menudo como proceso industrial en grande, y es una parte esencial de publicar y de impresión de la transacción.

- Network File System: es cualquier computadora sistema de ficheros la cual ayuda compartiendo archivos, impresoras y otros recursos como almacenaje persistente sobre a red de ordenadores. Los primeros servidores de archivo fueron desarrollados en los años 70, y en 1985 Sun Microsystems creó el sistema de ficheros llamado “Network File System“(NFS) que se convirtió en el primer Network File System ampliamente utilizado. Otros sistemas de ficheros notables de la red son Sistema de ficheros de Andrew (AFS), Protocolo de la base de NetWare (NCP), y Bloque del mensaje del servidor (SMB) que también se conoce como sistema de ficheros común del Internet (CIFS).

8.2 CONTROL DE INVENTARIO

En la última década, el número de equipos que van formando parte del parque informático de una organización empresarial, centro tecnológico o campus universitario, ha ido aumentado a un ritmo acelerado. Esta nueva situación hace imprescindible la utilización de herramientas de gestión que permitan, entre otras funciones, inventariar los equipos y controlar el software instalado.

El origen del aumento sistemático de los parques informáticos de las empresas podemos encontrarlo principalmente en la cada vez más barata adquisición de elementos hardware y en la mayor puesta en marcha de prestaciones funcionales que toda organización quiere ofrecer a sus usuarios tanto internos como externos. Actualmente, ya no resulta extraño encontrarse con organizaciones empresariales que disponen de parques informáticos superiores a 200 equipos e incluso superando la cifra de 1000 equipos.

En el caso de un campus universitario, la media de equipos se eleva entre 2000 y 5000 equipos.

Igual que el número de equipos, también ha aumentado el número de usuarios, por lo que la gestión manual de un parque informático conlleva la dedicación de

unos recursos humanos y económicos muy valiosos y a menudo escasos. Este es uno de los principales motivos por el cual toda organización necesita de herramientas tecnológicas que le permitan supervisar su parque informático.

Las nuevas soluciones de control, consiguen centralizar todos los datos sobre sus infraestructuras (inventario de red), gestionar las incidencias que ocurran en el mismo (Service Desk), disponer de herramientas remotas para la formación de usuarios, dar soporte técnico y distribución de software.

Para llegar a cubrir todas estas áreas, "Control Total" se compone de los siguientes módulos funcionales:

- Inventario automático de red – Auditoria e inventario de redes
- Service Desk – Gestor de incidencias
- Gestión de lanzamientos – Distribución de Software
- SoporteWeb – Soporte Remoto
- DemoWeb – Comunicación Online
- Inventario automático de red – Auditoria e inventario automático de redes

Toda organización debe auditar qué elementos, tanto hardware como software, forman parte de su parque informático, es decir, disponer de un inventario de sus infraestructuras TI.

Son muchos los motivos por los cuales una organización necesita un inventario informático, pero los principales son el auditar y controlar el parque de ordenadores en cumplimiento con la LOPD (Ley Orgánica de Protección de Datos), prevenir futuras incidencias y usos indebidos de las infraestructuras, supervisar el uso de licencias adquiridas y programas no autorizados que puede ser instalados en los equipos de los usuarios, localizar fácilmente tanto equipos como aplicaciones, disponer de informes detallados y personalizados según las necesidades de la organización en un momento dado, obtener alertas de cambio de hardware y/o software que se produzca en cualquier equipo del parque así como también el historial correspondiente a esos cambios junto a el de incidencias que se hayan notificado desde ese equipo.

El proceso de recopilación de datos de todos los equipos de nuestro parque, por parte del módulo de Inventario automático de red, se realiza de manera automática sin intervención del personal técnico. No es necesaria instalación alguna ni de hardware ni de software en los equipos a inventariar, ni otorgar permisos especiales a los usuarios, como tampoco requerir su intervención. Toda la información recopilada siempre se encuentra actualizada y detallada al máximo.

El inventario informático que se recopila automáticamente, no sólo es información estática del hardware y software, también podemos conseguir el listado de dónde y cuándo inician sesión los usuarios, añadir cualquier tipo de dato que necesite nuestra organización en las fichas individuales de los equipos, comprobar qué equipos utilizan una determinada impresora, control de licencias de software e información adicional, de interés para los responsables de un parque informático.

8.2.1 Service Desk – Gestor de Incidencias. Las organizaciones dependen cada vez más de las Tecnologías de la Información para alcanzar sus objetivos corporativos. La misión del departamento de TI es ofrecer servicios fiables, de alta calidad y a un coste aceptable, por lo que debe incorporar de manera sistemática las mejores prácticas del mercado para la optimización continua de sus procesos.

El módulo de Service Desk de “Control Total”, facilita la gestión de incidencias, desde su registro inicial hasta su cierre, incorporando estándares internacionales de buenas prácticas como ITIL.

Gracias a este módulo se podrán obtener las siguientes características:

- Definir los Niveles de Servicio SLAs.

- Registrar la incidencia: quién informa del problema, síntomas, equipo involucrado, etc.

- Clasificar la incidencia y asignar el trabajo a realizar a un grupo de soporte o a un técnico.
- Investigar la causa de la incidencia y compararla con otras incidencias parecidas.

- Consultar la base de conocimiento.

- Documentar la solución, anexar ficheros con información relacionada y cerrar la incidencia.

- Comunicar automáticamente al usuario el estado de su solicitud a través del e-mail y/o portal de soporte

- Elaborar informes, que ayuden a conocer qué está sucediendo y a mejorar el proceso.

Una de las grandes ventajas que ofrece Service Desk, es su completa integración con el módulo de inventario automático de red. Gracias a esta unión, en el momento de registrar una incidencia o durante el proceso de su resolución, podemos consultar la ficha del equipo fuente de la incidencia, para conocer con exactitud y detalle el hardware y software que lo componen, de esta manera el técnico responsable de resolver la incidencia dispone de información básica que le facilitará la resolución.

La integración entre ambas aplicaciones, puede ser visualizada desde el lado del inventario, donde podemos encontrarnos con el historial de incidencias que un equipo haya notificado y todas las relacionadas con una concreta versión de un software de nuestro parque.

8.2.2 Gestión de lanzamientos - Distribución de Software. El proceso de instalación o desinstalación de un cierto componente de software en un gran número de equipos o en todos los que forman su parque informático, puede ser una tarea costosa, tanto en el número de horas dedicado como en el de recursos por parte del personal del departamento TI (Tecnologías de información).

Siguiendo las practicas de ITIL, “Control Total” ofrece el módulo de Gestión de Lanzamientos que permite desplegar e instalar automáticamente paquetes de software sobre los equipos seleccionados del parque, de manera completamente desatendida, y sin necesidad de configurar ningún componente adicional en los equipos sobre los que se va a realizar la instalación.

El módulo de Gestión de Lanzamientos añade más funcionalidad que instalar o desinstalar un componente de software, convirtiéndose una herramienta de gran versatilidad. Podemos llevar a cabo la ejecución de cualquier línea de comandos

en los equipos que seleccionemos, por lo que podemos realizar cualquier tipo de tarea que necesitemos, por ejemplo configuración de aplicaciones, paradas/ reinicio de servicios, copiar/borrar/buscar ficheros, etc.

Otras de las grandes características de este módulo, es su integración con el Inventario de red, formando entre ambas una herramienta imprescindible para la optimización del servicio de informática.

Con la herramienta de Inventario se decide en qué grupo o grupos de equipos se quiere hacer la distribución, cuyo progreso se sigue luego con Gestión de Lanzamientos para saber en cuáles se ha instalado, cuántos faltan por instalar y si ha habido alguna incidencia.

8.2.3 SoporteWeb – Soporte Remoto. Los usuarios de un parque informático en un momento dado necesitan de asistencia técnica por parte del personal de TI, ya sea para ayudarles a resolver una consulta técnica, en busca de asistencia para la resolución de una incidencia o formación.

El módulo de SoporteWeb aumenta las herramientas que el personal TI dispone para defi nir y dar con mayor rapidez con la solución de las incidencias. Soporte Web permite un acceso total a equipos remotos, visualización de escritorios entre equipos, grabación/ reproducción de sesiones interactivas, pizarra virtual y transferencia de ficheros.

Junto a toda la funcionalidad de una herramienta de asistencia remota, SoporteWeb lleva un gestor de colas de solicitudes para gestionar todas las solicitudes que los usuarios de nuestro parque hagan al departamento de soporte.

SoporteWeb es una aplicación en línea, por lo que no requiere de instalaciones de software en los equipos que interactúan y la herramienta puede ser utilizada desde cualquier PC conectado a la red local o Internet. Y la principal ventaja es que la posesión del control remoto de equipos se puede llevar a cabo sin la modificación de reglas de seguridad ni en cortafuegos o routers, ni directivas de seguridad.

8.2.4 DemoWeb – Comunicación Online. La función de DemoWeb, el último módulo de “Control Total, es poder reunir a varios asistentes para llevar a cabo una reunión virtual (reunión no presencial), ya sea para formación en línea, encuentros comerciales/técnicos o cualquier otro tipo de evento.

La aplicación en línea DemoWeb, permite la comunicación entre los asistentes mediante el uso de los navegadores de los equipos de los reunidos utilizando como pasarela la red local de la organización o Internet.

Entre las funcionalidades de DemoWeb permite destacar la visualización e interactividad de escritorios entre los asistentes, compartir aplicaciones entre ellos sin necesidad de que todos dispongan de ella en su propio equipo y grabación de las reuniones.

La aportación a un parque informático de todas las herramientas que incluye "Control Total" incrementa considerablemente las funcionalidades, tanto para lo que es la supervisión proactiva como para el control en tiempo real de todos los equipos que forman parte del parque. Junto a estas aplicaciones, "Control Total" facilita la realización de muchas de las tareas diarias que el responsable de sistemas ha de llevar a cabo e incrementa la interactividad con los usuarios.[1]

8.3 PLAN DE CONTINGENCIA

Se entiende por PLAN DE CONTINGENCIA los procedimientos alternativos al orden normal de una empresa, cuyo fin es permitir el normal funcionamiento de esta, aún cuando alguna de sus funciones se viese dañada por un accidente interno o externo.

Que una organización prepare sus planes de contingencia, no significa que reconozca la ineficacia de su empresa, sino que supone un avance a la hora de superar cualquier eventualidad que puedan acarrear perdidas o importantes pérdidas y llegado el caso no solo materiales sino personales.

Los Planes de Contingencia se deben hacer de cara a futuros acontecimientos para los que hace falta estar preparado. La función principal de un Plan de Contingencia es la continuidad de las operaciones de la empresa su elaboración la dividimos en cuatro etapas:

_____

[1] Sistemas de gestión pdf, www.forumt.net

- Evaluación.
- Planificación.
- Pruebas de viabilidad.
- Ejecución.

Las tres primeras hacen referencia al componente preventivo y la última a la ejecución del plan una vez ocurrido el siniestro.

La planificación aumenta la capacidad de organización en caso de siniestro sirviendo como punto de partida para las respuestas en caso de emergencia. [2]

8.3.1 Ciclo de vida. El plan de contingencias sigue el conocido ciclo de vida iterativo PDCA (plan-do-check-act, es decir, planificar-hacer-comprobar-actuar). Nace de un análisis de riesgo donde, entre otras amenazas, se identifican aquellas que afectan a la continuidad del negocio.

Sobre dicha base se seleccionan las contramedidas más adecuadas entre diferentes alternativas, siendo plasmadas en el plan de contingencias junto con los recursos necesarios para ponerlo en marcha.

El plan debe ser revisado periódicamente. Generalmente, la revisión será consecuencia de un nuevo análisis de riesgo. En cualquier caso, el plan de contingencias siempre es cuestionado cuando se materializa una amenaza, actuando de la siguiente manera:

- Si la amenaza estaba prevista y las contramedidas fueron eficaces: se corrigen solamente aspectos menores del plan para mejorar la eficiencia.

- Si la amenaza estaba prevista pero las contramedidas fueron ineficaces: debe analizarse la causa del fallo y proponer nuevas contramedidas.

_____

[2] Planes de contingencia, http://www.seguridad-la.com/artic/segcorp/7209.htm

- Si la amenaza no estaba prevista: debe promoverse un nuevo análisis de riesgos. Es posible que las contramedidas adoptadas fueran eficaces para una amenaza no prevista. No obstante, esto no es excusa para evitar el análisis de lo ocurrido.

Finalmente, se modifica el plan de contingencias de acuerdo a las revisiones aprobadas y, de nuevo, se inicia el ciclo de vida del plan.

8.3.2 Contenido. El plan de contingencias comprende tres sub-planes. Cada plan determina las contramedidas necesarias en cada momento del tiempo respecto a la materialización de cualquier amenaza:

- El plan de respaldo. Contempla las contramedidas preventivas antes de que se materialice una amenaza. Su finalidad es evitar dicha materialización.

- El plan de emergencia. Contempla las contramedidas necesarias durante la materialización de una amenaza, o inmediatamente después. Su finalidad es paliar los efectos adversos de la amenaza.

- El plan de recuperación. Contempla las medidas necesarias después de materializada y controlada la amenaza. Su finalidad es restaurar el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.

Por otra parte, el plan de contingencias no debe limitarse a estas medidas organizativas. También debe expresar claramente:

- Qué recursos materiales son necesarios.

- Qué personas están implicadas en el cumplimiento del plan.

- Cuáles son las responsabilidades concretas de esas personas y su rol dentro del plan.

- Qué protocolos de actuación deben seguir y cómo son.

Es mejor planificar cuando todavía no es necesario

Los responsables de la Planificación, deben evaluar constantemente los planes creados, del mismo modo deberán pensar en otras situaciones que se pudiesen producir. Un Plan de Contingencia estático se queda rápidamente obsoleto y alimenta una falsa sensación de seguridad, solo mediante la revisión y actualización periódicas de lo dispuesto en el Plan las medidas preparatorias adoptadas seguirán siendo apropiadas y pertinentes.
Toda planificación de contingencia debe establecer objetivos estratégicos así como un Plan de acción para alcanzar dichos objetivos.
A continuación veremos las diferencias fundamentales entre una Planificación de la Contingencia y la planificación de los objetivos:

La planificación de la contingencia implica trabajar con hipótesis y desarrollar los escenarios sobre los que se va a basar la planificación, la planificación de objetivos ya se conoce el punto de partida y se basará en la evaluación de las necesidades y recursos.

Un Plan de Contingencia debe ser exhaustivo pero sin entrar en demasiados detalles, debe ser de fácil lectura y cómodo de actualizar. Debemos tener en cuenta que un Plan de Contingencia, eminentemente, debe ser Operativo y debe expresar claramente lo que hay que hacer, por quien y cuando.

Toda Planificación debe tener en cuenta al personal que participar directamente en ella desde el personal que lo planifica hasta aquellos que operativamente participarían en el accidente. Debemos tener en cuenta los procedimientos para la revisión del Plan, quien lo actualizará y como, esa información, llegara a los afectados.

8.3.3 El Plan de Emergencia. Una Planificación de Contingencias debe ser también un Plan de Emergencia que contenga los siguientes elementos:

- Identificación del escenario
- Objetivos operativos
- Medidas que se deben adoptar

- Investigación
- Conclusiones

8.3.4 Objetivos Generales

Minimizar las perdidas

8.3.5 Objetivos Particulares

- Gestión y coordinación global, asignación de responsabilidades
- Activación del Plan de Emergencia
- Minimizar las perdidas

8.3.6 Contenido del Plan de Contingencia

- La naturaleza de la contingencia
- Las repercusiones operativas de la contingencia
- Las respuestas viables
- Las implicaciones financieras de las respuestas
- Cualquier efecto en otro proceso

Se deberán valorar los diferentes escenarios, esta actividad es la más intuitiva y sin embargo una de las más importantes ya que sienta las bases de toda la planificación posterior. Para establecer escenarios es necesario formular distintas hipótesis, aunque estas se basen en todos los conocimientos disponibles, nunca se debe eliminar el elemento de imprevisibilidad.

Debe ser un documento “vivo”, actualizándose, corrigiéndose, y mejorándose constantemente. No se trata de un documento que deba ser revisado exhaustivamente y fecha fija, sino de un documento que esté en permanente estado de cambio.

Los planes de contingencia deberán ser realistas y eficaces. Deberá existir un mecanismo para determinar qué plan de contingencia alternativo se instrumentará, tomando en consideración la eficiencia con respecto al costo. En situaciones de crisis, el rendimiento con respecto a otros objetivos es secundario.[2]

_____

[2] Planes de contingencia, http://www.seguridadla.com/artic/segcorp/7209.htm

9. DEFINICIÓN OPERACIONAL DE TÉRMINOS

- Software: En computación, el software -en sentido estricto- es todo programa o aplicación programada para realizar tareas específicas. El término "software" fue usado por primera vez por John W. Tukey en 1957.

Algunos autores prefieren ampliar la definición de software e incluir también en la definición todo lo que es producido en el desarrollo del mismo. La palabra "software" es un contraste de "hardware"; el software se ejecuta dentro del hardware.

- Hardware: hace referencia a cualquier componente físico tecnológico, que trabaja o interactúa de algún modo con la computadora. No sólo incluye elementos internos como el disco duro, CD-ROM, disquetera, sino que también hace referencia al cableado, circuitos, gabinete, etc. E incluso hace referencia a elementos externos como la impresora, el mouse, el teclado, el monitor y demás periféricos.

El hardware contrasta con el software, que es intangible y le da lógica al hardware (además de ejecutarse dentro de éste).

El hardware no es frecuentemente cambiado, en tanto el software puede ser creado, borrado y modificado sencillamente. (Excepto el firmware, que es un tipo de software que raramente es alterado).

- Sistema Operativo: Sistema tipo software que controla la computadora y administra los servicios y sus funciones como así también la ejecución de otros programas compatibles con éste.

Un sistema operativo permite interactuar con el hardware de computadoras, teléfonos celulares, PDAs, etc. y ejecutar programas compatibles en éstos.

Permite controlar las asignaciones de memoria, ordenar las solicitudes al sistema, controlar los dispositivos de entrada y salida, facilitar la conexión a redes y el manejo de archivos.

- Aplicación: Programa informático que permite a un usuario utilizar una computadora con un fin específico. Las aplicaciones son parte del software de una computadora, y suelen ejecutarse sobre el sistema operativo.
Una aplicación de software suele tener un único objetivo: navegar en la Web, revisar correo, explorar el disco duro, editar textos, jugar (un juego es un tipo de aplicación), etc. Una aplicación que posee múltiples programas se considera un paquete.

- Base de datos: Almacén de datos relacionados con diferentes modos de organización. Una base de datos representa algunos aspectos del mundo real, aquellos que le interesan al diseñador. Se diseña y almacena datos con un propósito específico. Con la palabra "datos" se hace referencia a hechos conocidos que pueden registrarse, como ser números telefónicos, direcciones, nombres, etc.

Las bases de datos almacenan datos, permitiendo manipularlos fácilmente y mostrarlos de diversas formas.

- Multimedia: Cualquier sistema que utiliza múltiples medios de comunicación al mismo tiempo para presentar información. Generalmente combinan textos, imágenes, sonidos, videos y animaciones.

- Streaming: (Transmisión al punto) Término que hace referencia al hecho de transmitir video o audio remotamente a través de una red (como Internet) en tiempo real sin necesidad de descargar el archivo completo.

Se hace Streaming, por ejemplo, cuando se transmite una radio, o un canal de televisión en vivo por Internet.

- Intranet: Red entre computadoras montada para el uso exclusivo dentro de una empresa u hogar. Se trata de una red privada que puede o no tener acceso a Internet, sirve para compartir recursos entre computadoras

- Red LAN: (Local Area Network - Red de Área Local). Interconexión de computadoras y periféricos para formar una red dentro de una empresa u hogar,

limitada generalmente a un edificio. Con esta se pueden intercambiar datos y compartir recursos entre las computadoras que conforman la red.

Una red puede contener: servidores, estaciones de trabajo, gateways, bridges (puentes), tarjetas de red, un medio (cableado o inalámbrico), concentradores de cableado, etc.

Existen varias soluciones de redes LAN: ethernet, token ring y arcnet.

- Red WAN: (Wide Area Network - Red de Área Extensa). WAN es una red de computadoras de gran tamaño, generalmente dispersa en un área metropolitana, a lo largo de un país o incluso a nivel planetario.

Este tipo de red contrasta con las PAN (personal area networks), las LAN (local area networks), las CAN (campus area networks) o las MAN (metropolitan area networks), que generalmente están limitadas a un cuarto, un edificio, un campus o un área metropolitana específica respectivamente, La más grande y conocida red WAN es internet.

- HTTP: Hypertext Transfer Protocol Secure (ó HTTPS) es una combinación del protocolo HTTP y protocolos criptográficos. Se emplea para lograr conexiones más seguras en la WWW, generalmente para transacciones de pagos o cada vez que se intercambie información sensible (por ejemplo, claves) en Internet.

De esta manera la información sensible, en el caso de ser interceptada por un ajeno, estará cifrada.

El nivel de protección que ofrece depende de la corrección de la implementación del navegador Web, del software y de los algoritmos criptográficos soportados. Además HTTPS es vulnerable cuando es aplicado a contenido estático públicamente disponible. El HTTPS fue creado por Netscape Communications en 1994 para su navegador Netscape Navigator.

- HTML: (Hyper Text Mark-up Language o Lenguaje de Marcas de Hipertexto). Lenguaje desarrollado por el CERN que sirve para modelar texto y agregarle funciones especiales (por Ej. hipervínculos). Es la base para la creación de páginas Web tradicionales.

El texto se modela a partir del uso de etiquetas o tags. También se pueden agregar scripts al código fuente HTML (generalmente JavaScript, PHP, etc.).

Por lo general los diseñadores utilizan herramientas gráficas WYSIWYG para la creación de páginas Web, las cuales generan el código fuente HTML automáticamente (ver Editores Web).

Junto con el código HTML se enlazan otros recursos como imágenes y sonidos, que se incluyen en archivos separados. Igualmente existe el MHTML que permite incorporar ciertos recursos dentro del archivo HTML.
Es un formato abierto que fue originalmente diseñado basado sobre las etiquetas SGML sin énfasis en las marcas rigurosas.

- SSL: (Secure Sockets Layer). Protocolo diseñado por la empresa Netscape para proveer comunicaciones encriptadas en Internet.

La empresa VeriSign es la encargada de emitir los certificados digitales RSA para su uso en transmisiones seguras por SSL, especialmente para la protección de sitios con acceso por HTTPS. Por ejemplo, páginas que utilizan tarjetas de créditos.

SSL da privacidad para datos y mensajes, además permite autentificar los datos enviados. Otro protocolo que se emplea para la transmisión de datos seguros en la WWW es el SHTTP, y puede complementarse con SSL. La principal diferencia con SSL radica en que SSL crea una conexión segura entre el cliente y el servidor Web, en esa conexión se pueden enviar cualquier cantidad de datos de forma segura. En tanto, SHTTP está diseñado para transmitir mensajes individuales de forma segura.

- DNS: (Domain Name System) Sistema de Nombres de Dominio. Conjunto de protocolos y servicios para la identificación/conversión de una dirección de Internet expresada en lenguaje natural por una dirección IP.

Una URL (dirección para acceder a una página Web) está compuesta por palabras separadas por puntos (Ej.: www.alegsa.com.ar), para acceder a la misma, sólo se debe recordar estas palabras. Esta dirección URL está asociada a un número (dirección IP) que identifica el servidor que se ha de contactar para verla (por Ej: 200.10.123.01). El servicio DNS se encarga de asociar una dirección URL a una dirección IP.

- IP Address: (Internet Protocol - Protocolo de Internet): Protocolo para la comunicación en una red a través de paquetes conmutados, es principalmente usado en Internet. Los datos se envían en bloques conocidos como paquetes (datagramas) de un determinado tamaño (MTU). El envío es no fiable (conocido también como best effort o mejor esfuerzo); se llama así porque el protocolo IP no garantiza si un paquete alcanza o no su destino correctamente. Un paquete puede llegar dañado, repetido, en otro orden o no llegar. Para la fiabilidad se utiliza el protocolo TCP de la capa de transporte.

Los paquetes poseen una cabecera con información sobre la máquina de origen y la de destino (sus direcciones IP), con esta información los enrutadores determinan por dónde enviar la información. Cada paquete de un mismo archivo puede enviarse por diferentes rutas dependiendo de la congestión del momento.

Actualmente se utiliza la versión IPv4, que luego será reemplazada por la IPv6, Suele utilizarse para abreviar dirección IP.

- Cifrado: (Cifrado, codificación o encriptación) es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros. Pueden ser contraseñas, números de tarjetas de crédito, conversaciones privadas, etc.

Para encriptar información se utilizan complejas fórmulas matemáticas y para desencriptar, se debe usar una clave como parámetro para esas fórmulas.

El texto plano que está encriptado o cifrado se llama criptograma.

Aclaración: encriptación Vs Cifrado: Se prefiere el uso de la palabra "cifrado" en lugar de "encriptación", debido a que esta última es una mala traducción del inglés encrypt.

- SMTP: (Simple Mail Transfer Protocol - Protocolo de Transferencia Simple de Correo). Protocolo estándar para enviar E-mails.

- Spam: Spam es todo aquel correo electrónico que contiene publicidad que no ha sido solicitada por el propietario de la cuenta de e-mail.

La actividad de los spammers -aquellos sujetos que se encargan de generar el Spam es considerada poco ética e incluso ilegal en muchos países.

Aquellas aplicaciones y herramientas encargadas de detectar o eliminar el Spam son llamados programas antispam.

El Spam puede clasificarse como un tipo de correo electrónico no deseado.

- SLA: Un acuerdo de nivel de servicio o Service Level Agreement, también conocido por las siglas ANS o SLA, es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. El ANS es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc. Básicamente el ANS define la relación entre ambas partes: proveedor y cliente. Un ANS identifica y define las necesidades del cliente a la vez que controla sus expectativas de servicio en relación a la capacidad del proveedor, proporciona un marco de entendimiento, simplifica asuntos complicados, reduce las áreas de conflicto y favorece el diálogo ante la disputa.

- Fichero: (Fichero, file o archivo) es un grupo de datos estructurados que son almacenados en algún medio y pueden ser usados por las aplicaciones.

La forma en que una computadora organiza, da nombre, almacena y manipula los archivos se denomina sistema de archivos y suele depender del sistema operativo y del medio de almacenamiento (disco duro, disco óptico, etc.).

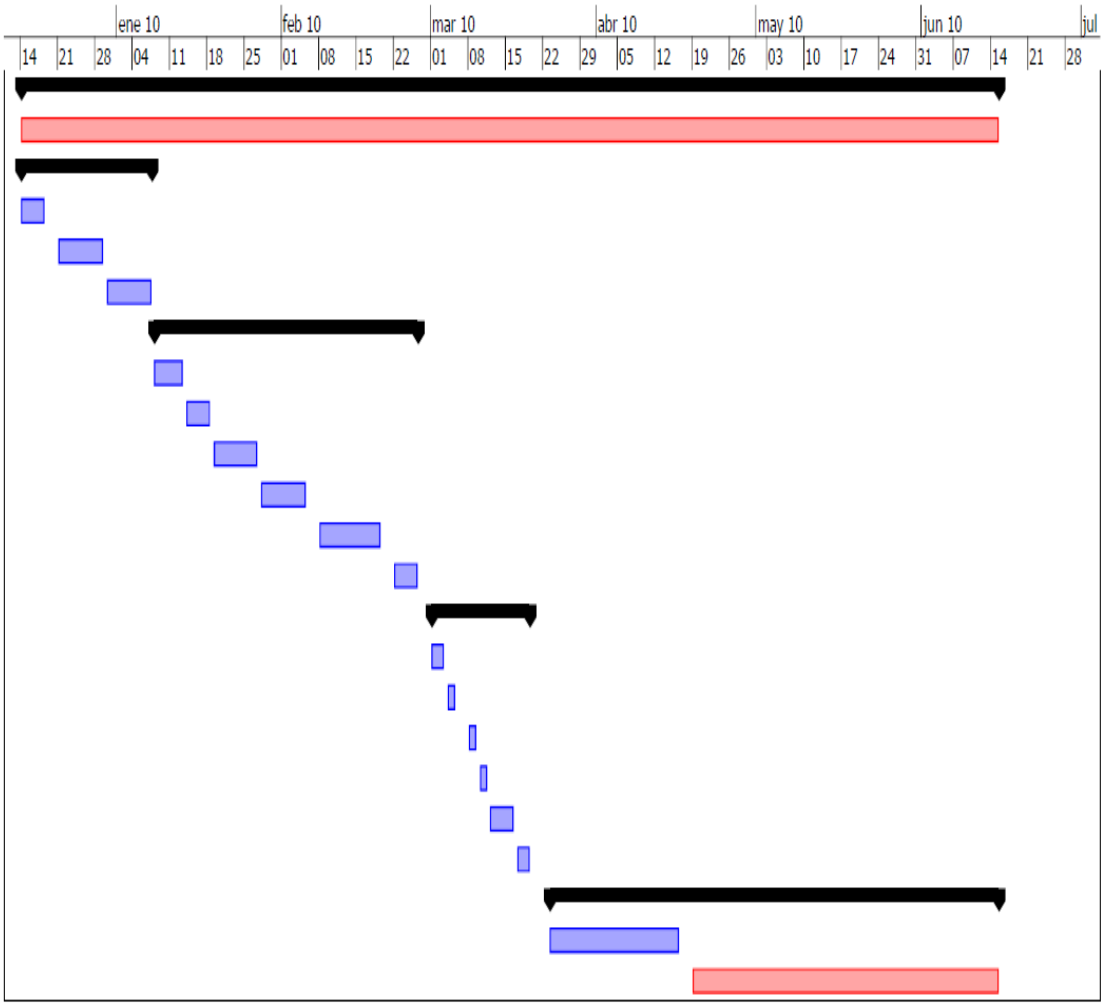
Parque Informático: Un parque informático se compone de todos aquellos recursos de tecnología con los que cuenta una organización.

10. CRONOGRAMA

	Nombre	Duración
1	**Practica Profesional**	**122 days**
2	Soporte	122 days
3	**Induccion e Introduccion a la Empresa**	**15 days**
4	Induccion a Telefonica de Pereira	5 days
5	Conociendo la arquitectura de red	5 days
6	Conociendo documentacion de procesos de ETP	5 days
7	**Implementacion herramienta para monitorizacion**	**35 days**
8	Investigar sobre herramientas de monitoreo	3 days
9	Elegir una herramienta e investigar todo acerca de la misma	3 days
10	Instalar herramienta elegida	7 days
11	Configurar herramienta elegida	7 days
12	Realizar instalaciones adicionales	10 days
13	Documentar la instalacion de la herramienta de monitoreo	5 days
14	**Implementacion herramienta para implementacion de inventario**	**15 days**
15	Investigar sobre herramientas para inventario	3 days
16	Elegir una herramienta e investigar acerca de la misma	2 days
17	Instalar herramienta elegida	2 days
18	Configurar herramienta elegida	2 days
19	Realizar instalaciones adicionales	3 days
20	Documentar la instalacion de la herramienta de inventario	3 days
21	**Actualizacion del Plan de contingencia**	**57 days**
22	Realizar evaluacion del estadto actual del Plan de Contingencia de ETP	17 days
23	Realizar las actualizaciones correspondientes	40 days

Practica Profesional 2010

.


ene 10
feb 10
mar 10
abr 10
may 10
jun 10
jul
14 21 28 04 11 18 25 01 08 15 22 01 08 15 22 29 05 12 19 26 03 10 17 24 31 07 14 21 28

11. HERRAMIENTA DE MONITOREO

11.1 JUSTIFICACIÓN

Luego de investigar acerca de diferentes herramientas de monitoreo, entre estas una recomendada por el ingeniero y jefe inmediato Fredy Ruano, se tomo la decisión de trabajar con Nagios la cual es una herramienta robusta y con un alto nivel de aceptación a nivel mundial, siendo esta una herramienta con licencia GNU, lo que quiere decir que es software libre, y no generaría un costo para la organización.

11.2 ESPECIFICACIONES NAGIOS

Versión: Nagios Core Version 3.x

URL: http://www.nagios.org
URL: http://nagioses.blogspot.com/

11.2.1 ¿Qué es nagios? Nagios es un sistema de monitorización de equipos y de servicios de red, creado para ayudar a los administradores a tener siempre el control de qué está pasando en la red y conocer los problemas que ocurren antes de que los usuarios de la misma los perciban.

Se trata de un software usado en todo el mundo que debe correr en sistemas Linux o Unix y que permite extender su funcionalidad con la utilización o creación de extensiones.

Nagios es un sistema de monitorización muy completo, con grandes posibilidades de ampliación y adaptación como demuestra su implantación en empresas,

universidades y organismos gubernamentales. Sin embargo, se trata de un sistema complejo que requiere una configuración e instalación elaborada que no lo hacen apropiado para ser usado en redes pequeñas.

Nagios es una solución robusta, escalable y económica para la monitorización de equipos y redes informáticas.

Algunas de las características con las que cuenta son:

- Monitorear servicios de red (SMTP, POP3, HTTP, PING, etc.)
- Monitorear recursos de los hosts (carga de procesador, uso de disco, etc.)
- Diseño simple de plugins para que podamos crear los nuestros a nuestras necesidades especificas.
- Habilidad de definir una jerarquía de hosts usando la opción parents.
- Notificaciones a contactos cuando un servicio o host tenga problemas y puedan resolverlo (email, pager o definido por el usuario).
- Rotación de log automática.
- Interfaz Web para observar la funcionalidad de los equipos monitoreados
- Etc.

11.2.2 Requisitos requerimientos del sistema. Cualquier equipo que este ejecutando Linux o una variante de Unix y con compilador C, y preferentemente que tenga:

- Un Web Server (Apache el ideal)
- Thomas Boutell's GD library esto para el statusmap y trends

11.3 LICENCIA

Nagios está bajo la GNU General Public License versión 2 publicada por la Free Software Foundation. Esto le da permiso legal de copiar, distribuir y/o modificar Nagios bajo ciertas condiciones. Lea el archivo 'LICENSE' en la distribución de Nagios o lea la versión en línea (http://www.nagios.org) para mayores detalles.

Nagios es proporcionado TAL CUAL sin NINGUNA GARANTÍA DE NINGÚN TIPO, INCLUYENDO GARANTÍA DE DISEÑO, COMERCIALIZACIÓN Y ADECUARSE PARA UN PROPÓSITO EN PARTICULAR.

11.4 RECONOCIMIENTOS

Muchas personas han contribuido a Nagios ya sea reportando 'bugs', sugerencias de mejora, escribiendo plugins, etc. Una lista de algunos contribuidores en el desarrollo de Nagios pueden ser localizados en http://www.nagios.org.

11.5 ÚLTIMA VERSIÓN

La última versión se encontrar en el Web Site de Nagios http://www.nagios.org.
Nagios y el logo de Nagios son marcas registradas de Ethan Galstad. Todas las demás marcas registradas, marcas de servicio, etc. son propiedad de sus respectivos dueños.

11.6 CARACTERÍSTICAS

Nagios, básicamente es un sistema que testea servicios y otros parámetros de una red, de muy diversas formas, y notifica todas las incidencias rápidamente a los administradores, es por tanto un sistema de alerta temprana.

- Interfaz Web: muestra la información en una interfaz Web desde la que el propio administrador puede establecer algunos parámetros, lo que permite observar este interfaz de forma remota vía cliente HTTP. Incluso desde dicha

interfaz Web, previa autenticación HTTP, permite también programar en el tiempo los chequeos a máquinas o servicios previamente configurados, las notificaciones, etc.

- Definición de jerarquías de servicios o de máquinas: Incorpora características muy interesantes como las dependencias de servicios o de equipos que permiten establecer jerarquías de servicios o de máquinas. De esta forma Nagios puede detectar si un servicio está inactivo o inaccesible; en el primer caso el equipo o servicio estaría down, mientras que en el segundo caso, el estado del servicio o equipo no se sabría porque la caída de uno superior impide su monitorización.

- Administración y definición de usuarios: otra característica que ofrece es la agrupación de contactos (personas a quién notificar) de manera que cuando una incidencia se produzca para equipos o servicios supervisados por esas personas, dicha notificación llegue a todas y cada una de ellas y no exclusivamente a una persona. Esto proporciona flexibilidad si por ejemplo la administración de la red se realiza en jornadas divididas por turnos. De esta forma se puede hacer que se notifique solo a la persona que se encuentra en su jornada laboral o que se notifique a un grupo de personas.

- Creación de nuevos comandos (plugins): Nagios también permite la creación sencilla e nuevos comandos (llamados plugins) para añadir nuevas funcionalidades al sistema, o bien combinar varios de los que se encuentran activos. En cierto modo Nagios puede ser tan flexible como se desee tanto en cuanto es software libre y por tanto el código fuente es abierto y modificable por cualquiera.

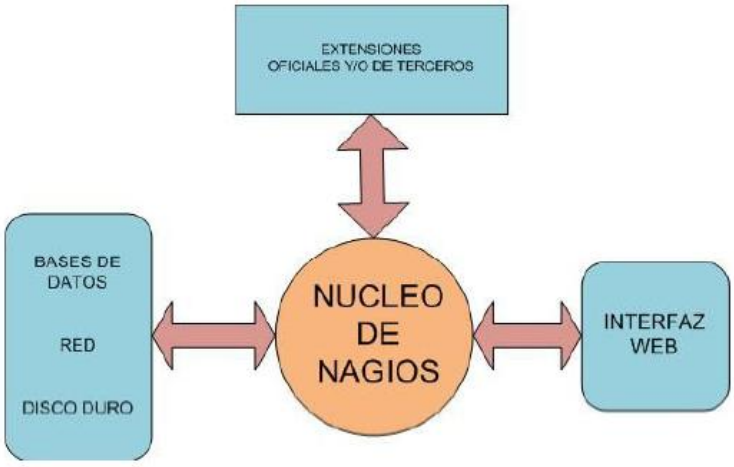
11.7 ESTRUCTURA

El núcleo de la aplicación, que forma la lógica de control de la aplicación, contiene el software necesario para realizar la monitorización de los servicios y equipos de la red que han sido definidos. Hace uso de diversos componentes que vienen con la aplicación, y puede hacer uso de otros componentes realizados por terceras personas.

Aunque permite la captura de paquetes SNMP para notificar sucesos, no es un sistema de monitorización y gestión basado en SNMP sino que realiza su labor basándose en una gran cantidad de pequeños módulos software que realizan chequeos de parte de la red.
Muestra los resultados de la monitorización y del uso de los diversos componentes en una interfaz Web a través de un conjunto de CGI's y páginas HTML que vienen incorporadas de serie. Y que permiten al administrador una completa visión de qué ocurre, dónde y en algunos casos, el por qué.

Por último, si se compila para ello, Nagios guardará los históricos en una base de datos para que al detener y reanudar el servicio de monitorización, todos los datos sigan como iban, sin cambios.

Ilustración 2. Estructura NAGIOS

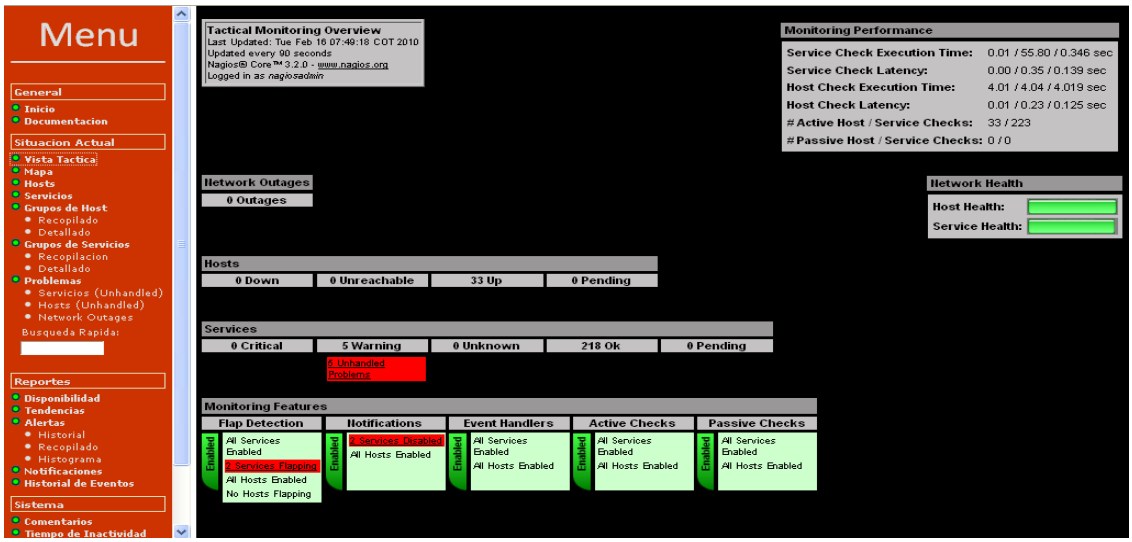


11.8 INTERFAZ WEB

La Web de administración de Nagios es altamente configurable.

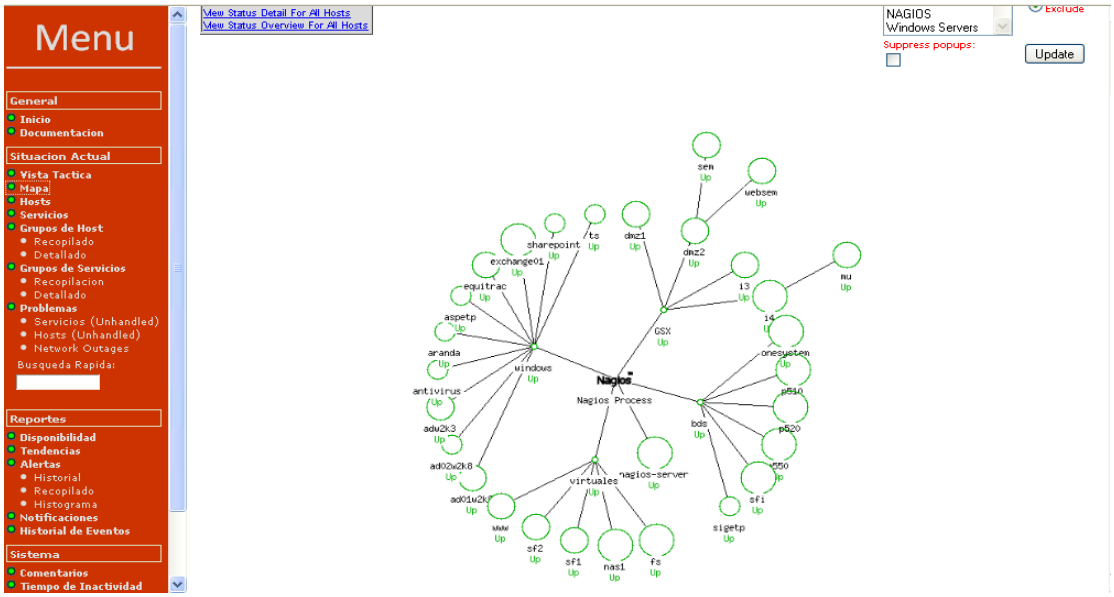
Vista Táctica (Tactical Overview): Muestra de forma rápida un resumen de todo el sistema que permita tomar decisiones rápidas apoyadas en una base real del estado del sistema.

Ilustración 3. Vista Táctica



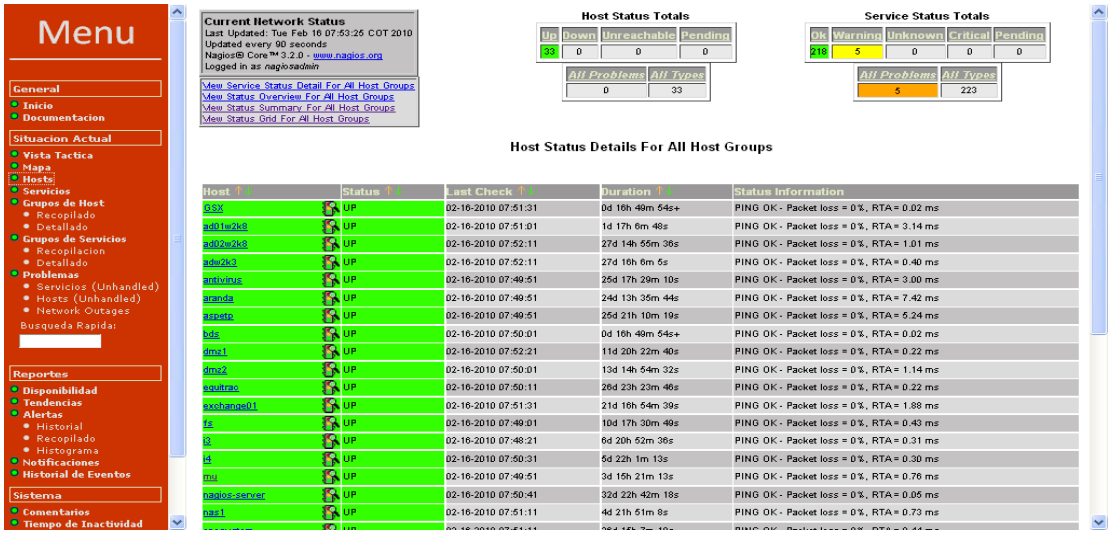
Mapa (Map): Esta opción permite ver un esquema gráfico de la red que monitoriza Nagios y el estado de cada elemento de la red.

Ilustración 4. Vista mapa



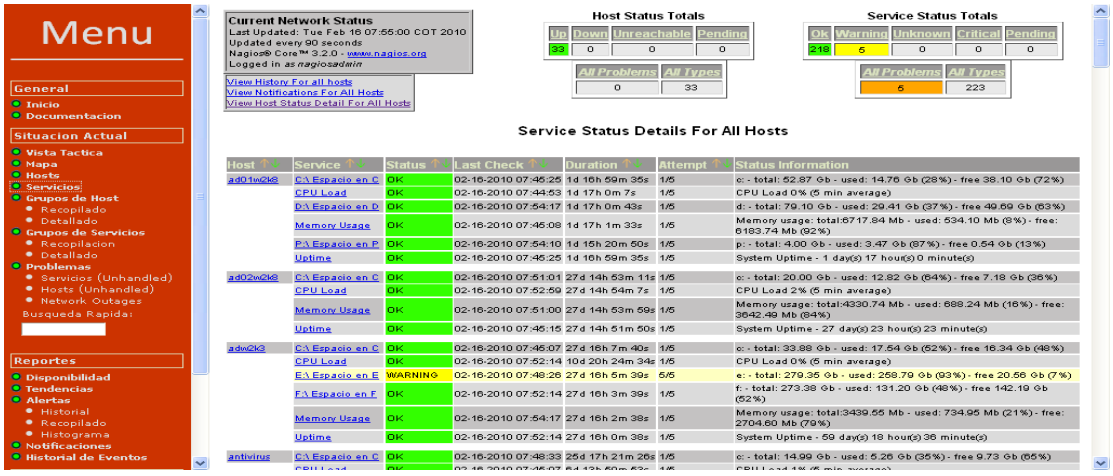
Hosts: Muestra si los equipos que están siendo monitorizados se encuentran activos, si se encuentran caídos o si el acceso a los mismos está dificultado por alguna cuestión.

Ilustración 5. Vista host



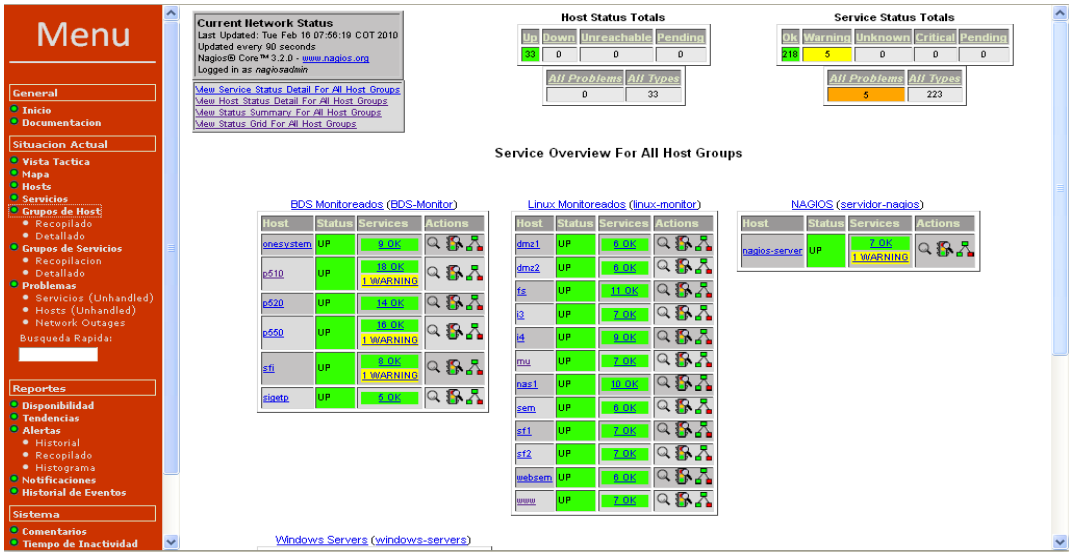
Servicios (Services): Muestra el estado de los servicios que se están monitorizando así como una descripción textual de si ha habido problemas, si no se tienen datos suficientes, etc.

Ilustración 6. Vista servicios



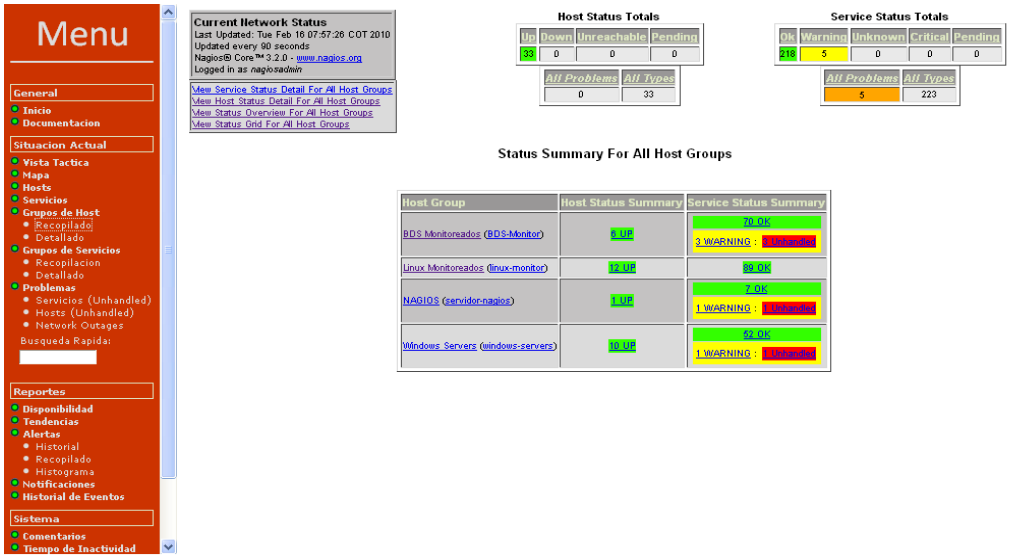
Grupos de Hosts (Hosts Groups): Muestra los diferentes tipos de grupos de hosts y sus correspondientes integrantes.

Ilustración 7. Vista grupo de host



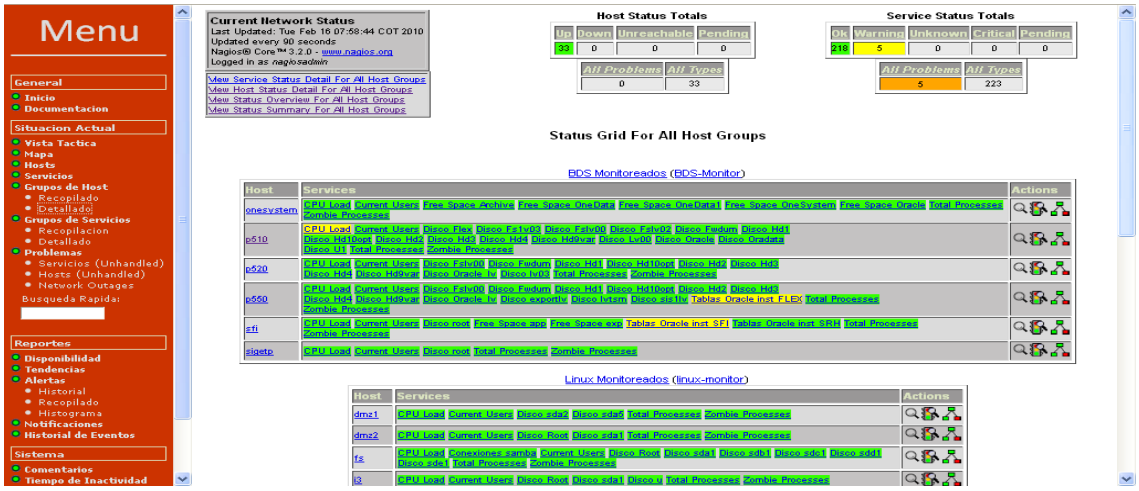
Recopilado: Muestra los grupos de hosts y el estado de sus servicios.

Ilustración 8. Vista recopilado



Detallado: Muestra todos los equipos de cada grupo y sus respectivos servicios Y estados

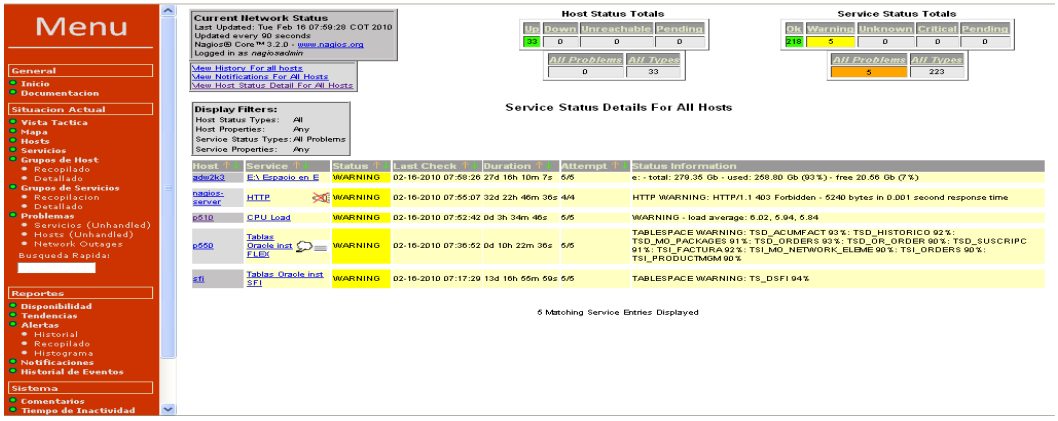
Ilustración 9. Vista detallado



Problemas (Problems): Esta opción muestra los hosts con sus respectivos servicios los cuales están teniendo problemas así como una descripción de dichos problemas.

Es especialmente útil para un administrador de red saber inmediatamente qué servicios están dejando de funcionar.

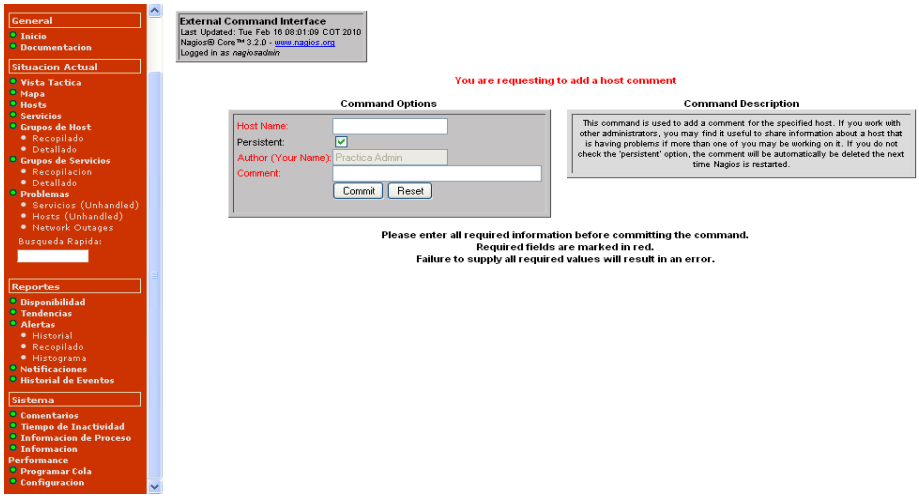
Ilustración 10. Vista problemas



Búsqueda Rápida (Quick Search): Búsqueda de hosts

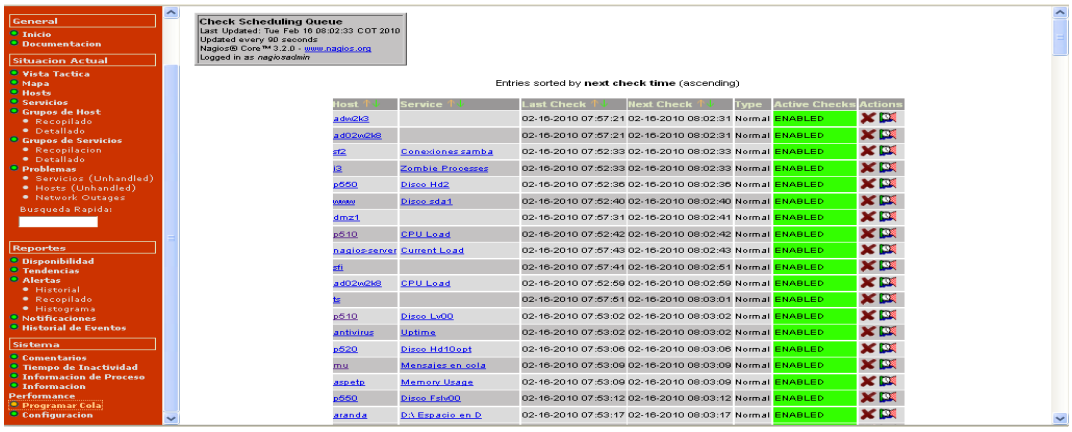
Creación de comentarios para equipos: Permite asociar un comentario a un equipo.

Ilustración 11. Búsqueda rápida



Cola de planificación: Esta opción muestra y permite cambiar la fecha y hora para la cual están planificadas la ejecución de los chequeos a servicios y equipos.

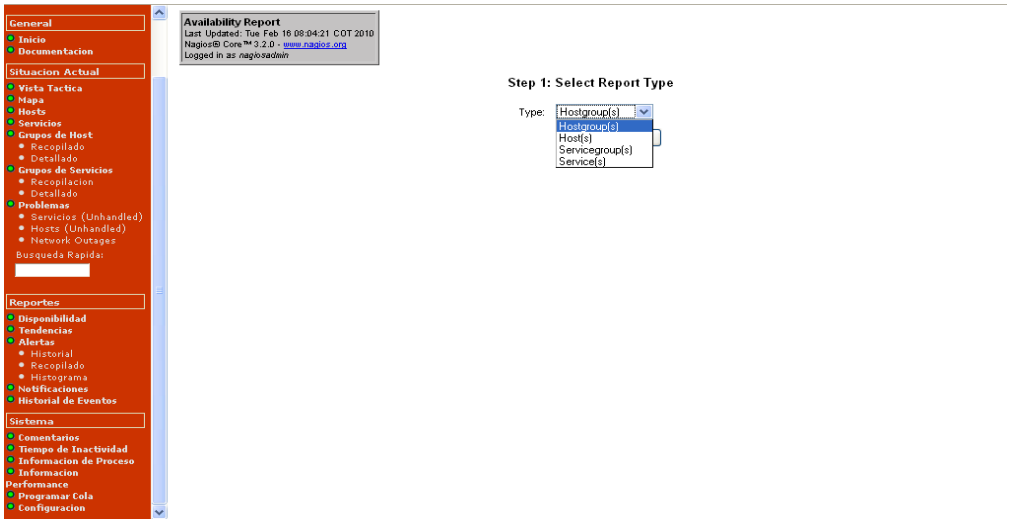
Ilustración 12. Cola de planificación



Configuración de informes: Común para casi cualquier informe. Permite elegir el rango de tiempo, la forma de presentación, el orden, etcétera, de los datos que aparecerán en el informe.

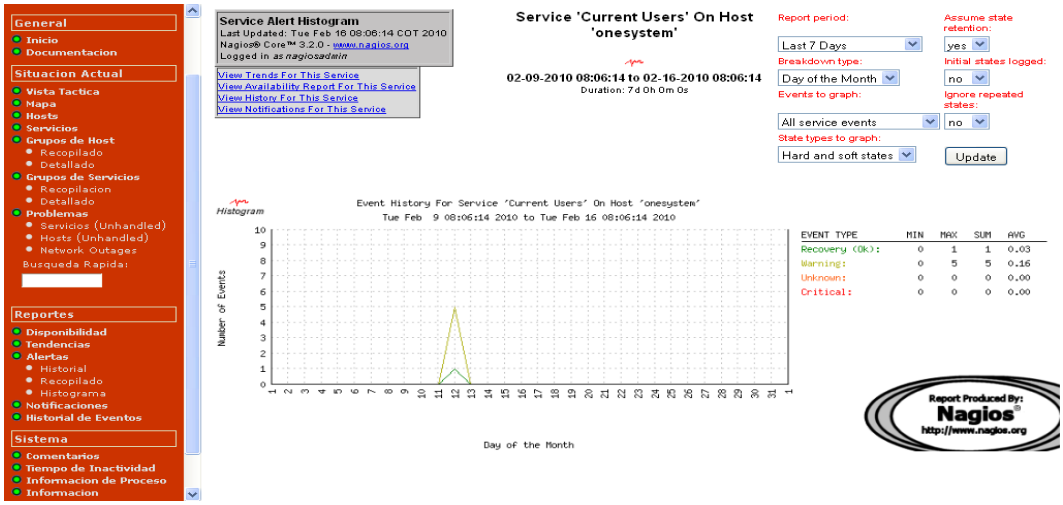
Informe de disponibilidad: Esta opción presenta en la ventana Web un listado con todos los equipos y los porcentajes de tiempo en los que cada uno ha estado activo e inactivo. Esto permite obtener unas estadísticas para ver si una máquina falla con frecuencia y tomar medidas al respecto.

Ilustración 13. Vista informe de disponibilidad



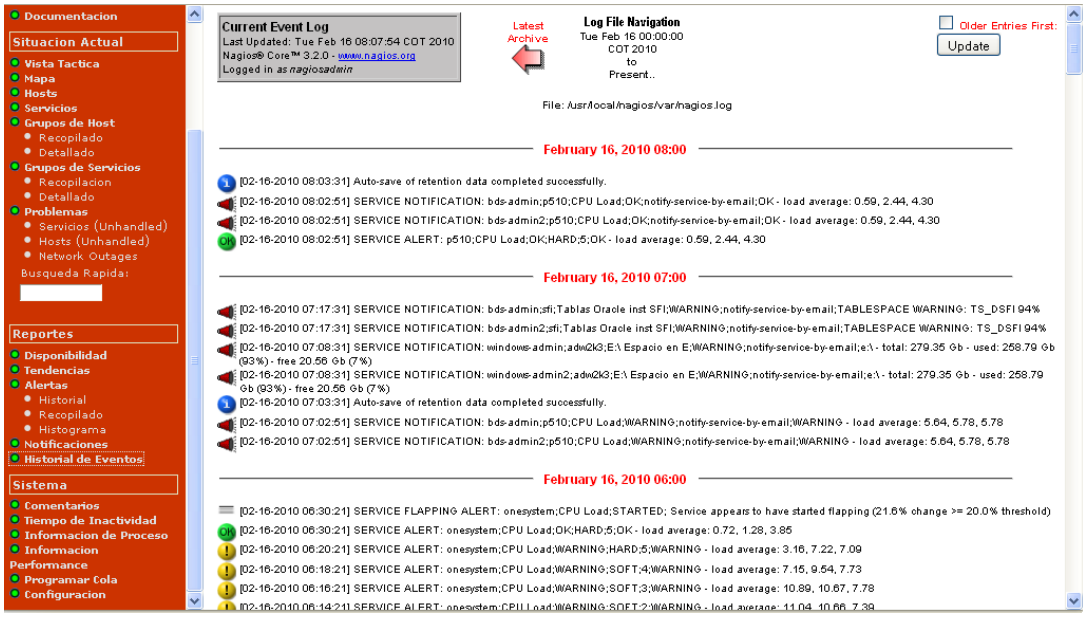
Histograma: Como cualquiera de los demás tipos de informe, el histograma muestra de forma gráfica distintos parámetros, a elegir, sobre los servicios y equipos monitorizados.

Ilustración 14. Vista histograma



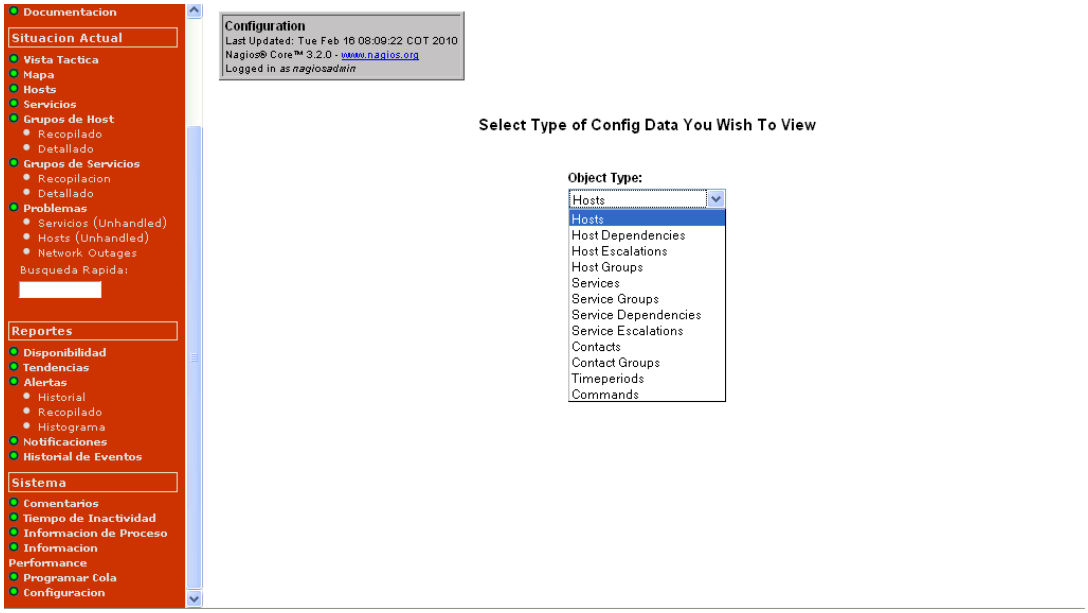
Histórico de eventos: Esta opción muestra el total de sucesos que han ocurrido en el sistema, desde la caída de un equipo hasta el envío a un contacto de una notificación vía correo electrónico.

Ilustración 15. Vista histórico de eventos



Configuración: Esta opción permite ver los datos de configuración del sistema desde host hasta comandos que utiliza el sistema

Ilustración 16. Vista configuración



11.9 INSTALACIÓN

La instalación de la aplicación NAGIOS fue realizada en CENTOS 5.2, Sistema en el cual ha mostrado un muy buen rendimiento, a continuación se vera como se realizo la instalación, partiendo desde el código fuente.

11.9.1 Siguiendo estas instrucciones, se logra obtener:

- Instalar Nagios y sus respectivos plugins bajo /usr/local/nagios.

- Nagios será configurado para que empiece a monitorear los sistemas. locales de los servidores escogidos (carga de CPU, uso en disco, etc.)

- Nagios será configurado para monitorear diferentes servicios en las maquinas Windows, Linux, Unix.

- La interfaz Web de Nagios será accesada en http://localhost/nagios/

11.9.2 Prerequisitos

Ingresar como root a la máquina de instalación.

Revisar con los siguientes comandos que tenga los siguientes paquetes instalados en la distribución de CENTOS antes de continuar.

- Apache

[root@monitor ~]# rpm -q httpd
httpd-2.2.3-11.el5_1.centos.3 ← Significa que el paquete se encuentra instalado

- Compilador GCC

  [root@monitor ~]# rpm -q gcc
  gcc-4.1.2-42.el5

- GD librerías de desarrollo

  [root@monitor ~]# rpm -q glibc glibc-common gd gd-devel
  glibc-2.5-24
  glibc-common-2.5-24
  gd-2.0.33-9.4.el5_1.1
  gd-devel-2.0.33-9.4.el5_1.1

En caso de que falte algún paquete deberá de ser instalado de la siguiente manera: por medio del repositorio (Se encuentra en el CD de CENTOS):

rpm -ivh nombrecompleto.rpm

También se pueden instalar paquetes por medio del comando YUM el cual requiere tener acceso a Internet desde la maquina, lo que quiere decir que debe de tener el Proxy configurado.

yum install nombre_del_paquete

Ahora procedemos a comenzar con la instalación de nagios.

Se deben realizar los siguientes pasos:

- Crear información de la cuenta: Ingresar como root a la maquina.

- Crear usuario nuevo nagios y proporcionarle una contraseña

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

- Crear un grupo nuevo nagcmd para permitir que comandos externos sean ingresados por medio de la interfaz Web. Agregar tanto el usuario nagios como el usuario apache al grupo.

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

- Descargar Nagios y Los Plugins: se deben descargar en una maquina Windows y subirlos por medio de FTP.

http://www.nagios.org/download/core/
http://www.nagios.org/download/plugins/

De las descargas anteriores se obtienen los siguientes archivos

- nagios-3.2.0.tar.gz y nagios-plugins-1.4.14.tar.gz

Se deben subir los archivos a /home/nagios, ahora se ingresa a ese directorio

```
# cd /home/nagios/
```

- Compilar e instalar Nagios: Extraer el código fuente del archivo comprimido de Nagios.

```
# gunzip nagios-3.2.0.tar.gz
# tar xvf nagios-3.2.0.tar
```

Ingresar a la carpeta que genera descomprimir dicho archivo.

```
# cd nagios-3.2.0
```

Ejecutar el script de configuración de Nagios, pasando el nombre del grupo que se creó anteriormente:

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

Compilar el código fuente de Nagios.

```
# make all
```

Instalar los binarios, el script de inicio, archivos de configuración de ejemplo y otorgar permisos en el directorio de comandos externos.

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

- Personalizar la configuración: Archivos de configuración de ejemplo han sido instalados en el directorio /usr/local/nagios/etc. Estos archivos de ejemplo deben de trabajar adecuadamente para empezar a utilizar Nagios. Se debe realizar un cambio más antes de proceder...

Editar el archivo de configuración /usr/local/nagios/etc/objects/contacts.cfg con un editor cualquiera y cambiar la dirección de correo que esta asociada con el contacto nagiosadmin con la dirección de correo donde recibiremos las alertas.

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

- Configurar la interfaz Web: Estando en el directorio /home/nagios/nagios-3.2.0 Instalar el archivo de configuración Web en el directorio conf.d de Apache.

make install-webconf

Crear la cuenta nagiosadmin para entrar a la interfaz Web de Nagios. No olvidar la contraseña que se asigno a esta cuenta - se necesitará después.

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

Reiniciar el servicio de Apache para que la nueva configuración tome efecto.

service httpd restart

- Compilar e instalar los Plugins de Nagios: ingresar al directorio /home/nagios

cd /home/nagios/

- Extraer los plugins de Nagios del archivo comprimido.

gunzip nagios-plugins-1.4.14.tar.gz
tar xvf nagios-plugins-1.4.14.tar

Ingresar a la carpeta que genera descomprimir dicho archivo.

cd nagios-plugins-1.4.14

Compilar e Instalar los plugins.

./configure --with-nagios-user=nagios --with-nagios-group=nagios

```
# make
# make install
```

- Iniciar Nagios: Agregar a Nagios a la lista de servicios del sistema para que así se ejecute automáticamente cada que el sistema se inicie.

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

- Revise los archivos de configuración de ejemplo de Nagios.

```
# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
Total Warnings: 0
Total Errors:   0
```

Si no hay errores, inicie Nagios.

```
# service nagios start
```

- Login a la interfaz WEB: Ahora es posible acceder a la interfaz Web de Nagios por medio de la siguiente dirección en la parte inferior. Será solicitado el usuario (nagiosadmin) y la contraseña especificada anteriormente.

http://localhost/nagios/

Dar clic en el MENÚ "Service Detail" para ver detalles de lo que esta siendo monitoreado en la máquina local. Tomara algunos minutos a Nagios para revisar todos los servicios asociados con su máquina, mientras las revisiones sean realizadas a su tiempo.

- Otras Modificaciones: Asegurarse de que las reglas de firewall en la máquina están configuradas para permitir el acceso al servidor Web, en caso de que se desea que la interfaz de Nagios sea accesada remotamente.

11.10 CONFIGURACIÓN DE CONTACTOS

Para la configuración de los contactos con los cuales se comunicara vía Email, el sistema Nagios se debe editar el archivo contacts.cfg

```
[root@monitor objects]# vi /usr/local/nagios/etc/objects/contacts.cfg
        define contact{
                contact_name            nagiosadmin             ; Short name of user
                use                     generic-contact         ; Inherit default values from
        generic-contact template (defined above)
                alias                   Practica Admin          ; Full name of user
                email                   practicarsi@etp.com.co  ; <<***** CHANGE THIS
        TO YOUR EMAIL ADDRESS ******
            }

        define contact{
                contact_name            bds-admin               ; Short name of user
                use                     generic-contact         ; Inherit default values from
        generic-contact template (defined above)
                alias                   Albeiro Rios            ; Full name of user

                email                   arios@etp.com.co        ; <<***** CHANGE THIS
        TO YOUR EMAIL ADDRESS ******
                }

        define contact{
                contact_name            bds-admin2              ; Short name of user
                use                     generic-contact         ; Inherit default values from
        generic-contact template (defined above)
                alias                   Jaime A. Gomez          ; Full name of user
                email                   jagomez@etp.com.co      ; <<***** CHANGE
        THIS TO YOUR EMAIL ADDRESS ******
                }
```

Y de esta forma se agregan los diferentes contactos que recibirán notificaciones de los servicios que les corresponden.

Se deben formar grupos de contacto para así agrupar los diferentes contactos que reciben notificación de un servicio o host especifico.

```
define contactgroup{
        contactgroup_name       admins
        alias                   Nagios Administrators
        members                 nagiosadmin
        }

define contactgroup{
        contactgroup_name       bdsadmins
        alias                   Administradores Aix
        members                 bds-admin, bds-admin2
        }
```

11.11 MONITOREANDO MAQUINAS WINDOWS

Se Puede monitorear servicios "privados" y atributos en máquinas con Windows, como por ejemplo:

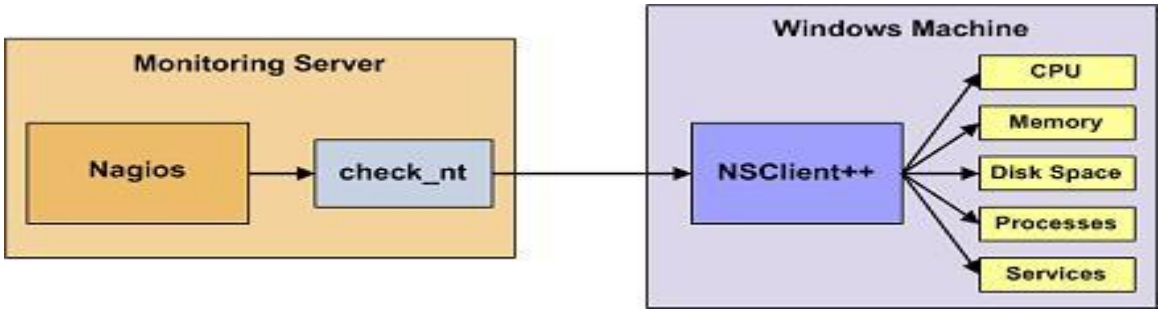
- Uso de Memoria
- Carga en CPU
- Uso en Disco Duro
- Estado en Servicios
- Procesos ejecutándose
- etc.

Nota: Estas instrucciones asumen que se instaló Nagios correctamente.

11.11.1 Descripción. El monitorear servicios privados o atributos de una máquina con Windows requiere que se instale un agente. Este agente actúa como un Proxy entre el plugin de Nagios que realiza el monitoreo y el servicio actual o atributo de la máquina Windows. Sin instalar un agente en Windows, Nagios no podría monitorear servicios privados o atributos de Windows.

Para este ejemplo, se instalara el complemento NSClient++ en la máquina con Windows y utilizaremos el plugin check_nt para comunicarnos con el complemento NSClient++. El plugin check_nt deberá ya estar instalado en el servidor de Nagios.

Ilustración 17. Descripción



Pasos

Existen algunos pasos que se deben seguir en orden para monitorear la nueva máquina Windows. Los cuales se describen a continuación:

- Realizar prerequisitos por primera vez
- Instalar un agente de monitoreo en la máquina Windows
- Crear nuevas definiciones de nuevo equipo (host) y nuevo servicio (service) para monitorear a la máquina Windows
- Reiniciar el servicio de Nagios

Ya se han hecho varias tareas de configuración durante la instalación para poder continuar con la instalación:

- Una definición del comando check_nt ha sido agregado al archivo commands.cfg ubicado en /usr/local/nagios/etc/objects/. Esto permite utilizar el plugin check_nt para monitorear servicios de Windows.
- Una plantilla de equipo de servidor Windows (llamada windows-server) ha sido creada en el archivo templates.cfg ubicado en /usr/local/nagios/etc/objects/. Esto

permite agregar nuevas definiciones de equipos con Windows de una manera simple.

Se pueden modificar estas definiciones u otras definiciones para satisfacer mejor las necesidades si así es necesario.

11.11.2 Pre-requisitos. La primera vez que se configura Nagios para monitorear una máquina Windows, se necesitara realizar un poco más de trabajo. Recuerde, que se necesita realizar esto para la primera máquina Windows que se va a monitorear.

En la maquina donde se instalo Nagios, se debe editar el archivo de configuración de Nagios principal (main).

vi /usr/local/nagios/etc/nagios.cfg
Se procede a quitar el carácter numeral (#) de la siguiente línea del archivo de configuración principal:

#cfg_file=/usr/local/nagios/etc/objects/windows.cfg
Guardar y salir,

¿Qué es lo que se hizo?

Se acabo de configurar a Nagios para que vea el archivo /usr/local/nagios/etc/objects/windows.cfg para así buscar definiciones adicionales de objetos. Ahí es donde debemos agregar definiciones de equipos y servicios Windows. Este archivo de configuración ya contiene algunos ejemplos de definiciones de equipos, grupos de equipos (hostgroups) y servicios. Para la primera máquina Windows, simplemente se modifica las definiciones de equipo y servicio en ese archivo, no hay necesidad de crear nuevos, solo copiar, pegar y modificar.

Ahora se debe de configurar la maquina Windows que se va a monitorear accediendo físicamente o por medio de un acceso remoto.

11.11.3 Instalar el agente Windows. Antes de monitorear servicios privados y atributos de las máquinas con Windows, es necesario instalar un agente a estas máquinas. Se recomienda utilizar el complemento NSClient++, que puede ser localizado en http://sourceforge.net/projects/nscplus. Las siguientes instrucciones lo llevaran a través de una instalación básica del complemento NSClient++, así como la configuración de Nagios para monitorear la máquina Windows.

- Descargar la última versión estable del complemento NSClient++ que sea compatible con su procesador (32-64 bits) desde http://sourceforge.net/projects/nscplus

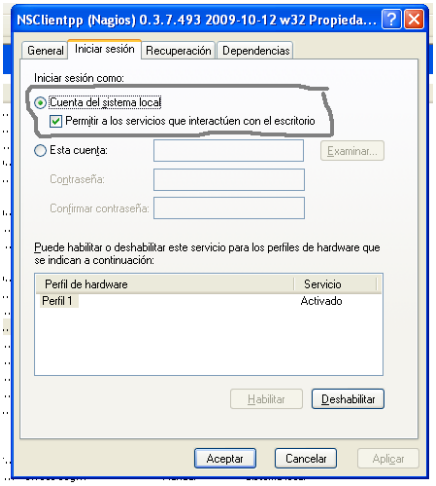
- Descomprimir los archivos de NSClient++ en un nuevo directorio C:\NSClient++

- Abrir un command prompt (CMD) y ubicarse en el directorio C:\NSClient++

- Registrar el servicio de NSClient++ con el siguiente comando: nsclient++ /install

- Instalar el "systray" de NSClient++ con el siguiente comando ('SysTray' es case-sensitive): nsclient++ SysTray
- Abrir el manejador de servicios (Panel de Control, Herramientas Administrativas, Servicios) y asegurarse de que el servicio NSClientpp es permitido para interactuar con el escritorio (ver el tab 'Log On' en el manejador de servicios). Si no esta permitido para interactuar con el escritorio, seleccione el cuadro para permitirlo.

Ilustración 18. Vista del servicio NsClientpp



- Editar el archivo NSC.INI (localizado en el directorio C:\NSClient++) y realizar los siguientes cambios:

    - Descomentar todos los módulos que aparecen listados en la sección [modules], excepto CheckWMI.dll y RemoteConfiguration.dll

    - Opcional, si requiere una contraseña para los clientes, cambie la opción 'password' en la sección [Settings].

    - Descomentar la opción 'allowed_hosts' en la sección [Settings]. Agregar la dirección IP del servidor de Nagios en esta línea o se deja en blanco para permitir a todos los equipos conectarse.

    - Verificar que la opción 'port' en la sección [NSClient] esta descomentada y asignada a '12489' (el puerto por default).

- En CMD en el directorio C:\NSClient++ iniciar el servicio de NSClient++ con el siguiente comando: nsclient++ /start

- Revisar en panel de control/herramientas administrativas/servicios si NSClientpp está corriendo en automático.

- Verificar que el FIREWALL contiene la regla para el programa nsclient++, si no es así se debe agregar. Dicho programa se encuentra alojado en C:\NSClient++\

Ahora se debe agregar el servidor Windows a la configuración de Nagios para su monitoreo.

11.11.4 Configurando Nagios. Conectarse a la maquina que tiene instalado Nagios, y ahora se procede a definir objetos en los archivos de configuración de Nagios en orden para monitorear la nueva máquina de Nagios.

Abra el archivo windows.cfg para editarlo.

- vi /usr/local/nagios/etc/objects/windows.cfg

Agregar una definición nueva de equipo para la máquina Windows que se desea monitorear. Si esta es la primera máquina Windows que se va a monitorear, debemos simplemente tener que modificar la definición de ejemplo del equipo en /usr/loca/nagios/etc/objects/windows.cfg. Se debe cambiar el host_name, alias, y address por lo valores apropiados para el equipo con Windows.

```
define host{
use windows-server  ;Esto se encuentra definido en templates.cfg
host_name winserver
alias My Windows Server
address 192.168.1.2
}
```

Ahora se puede agregar algunas definiciones de servicios (en el mismo archivo de configuración) en orden para decirle a Nagios que se van a monitorear varios aspectos de la máquina Windows. Si es la primera máquina Windows que va a monitorear, se debe simplemente modificar las definiciones de servicios de ejemplo en windows.cfg.

Nota: Remplazar "winserver" en las definiciones de ejemplo en la parte inferior con el nombre que se especifico en la directiva host_name en la definición de equipo que fue agregada.

Agregar la siguiente definición de servicio para monitorear la versión del complemento NSClient++ que se está ejecutando en el servidor Windows. Esto es útil cuando llega el tiempo de actualizar en los servidores Windows una nueva versión del complemento, y se podrá decir cuál de las máquinas Windows necesitan que se actualice a la última versión de NSClient++.

```
define service{
use generic-service
host_name winserver
service_description NSClient++ Version
check_command check_nt!CLIENTVERSION
}
```

Agregar la siguiente definición de servicio para monitorear el tiempo de actividad del servidor Windows.

```
define service{
use generic-service
host_name winserver
service_description Uptime
check_command check_nt!UPTIME
}
```

Agregar la siguiente definición de servicio para monitorear el uso de CPU en el servidor Windows y generar una alerta CRITICA si en 5 minutos la carga de CPU es de 90% o más o una alerta PRECAUCIÓN (WARNING) si en 5 minutos la carga es de 80% o más.

```
define service{
use generic-service
host_name winserver
service_description CPU Load
check_command check_nt!CPULOAD!-l 5,80,90
}
```

Agregar la siguiente definición de servicio para monitorear el uso de memoria del servidor Windows y generar una alerta CRITICA si el uso de memoria es de 90% o más y una alerta de PRECAUCIÓN (WARNING) si el uso de memoria es de 80% o más.

```
define service{
use generic-service
host_name winserver
service_description Memory Usage
check_command check_nt!MEMUSE!-w 80 -c 90
}
```

Agregarla siguiente definición de servicio para monitorear el uso en el disco C:\ del servidor Windows y generar una alerta CRITICA si el uso en disco es de 90% o más y una alerta de PRECAUCIÓN (WARNING) si el uso en disco es de 80% o más.

```
define service{
use generic-service
host_name winserver
service_description C:\ Drive Space
```

```
check_command check_nt!USEDDISKSPACE!-l c -w 80 -c 90
}
```

Agregar la siguiente definición de servicio para monitorear el estado del servicio W3SVC en una máquina Windows y generar una alerta CRITICA si el servicio es detenido.

```
define service{
use generic-service
host_name winserver
service_description W3SVC
check_command check_nt!SERVICESTATE!-d SHOWALL -l W3SVC
}
```

Agregar la siguiente definición de servicio para monitorear el proceso Explorer.exe de una máquina Windows y generar una alerta CRITICA si el proceso no se está ejecutando.

```
define service{
use generic-service
host_name winserver
service_description Explorer
check_command check_nt!PROCSTATE!-d SHOWALL -l Explorer.exe
}
```

Ya se han agregado algunos servicios básicos que deben ser monitoreados en la máquina Windows. Guardar y salir.

OPCIONAL: Protección con Contraseña

Si se ha especificado una contraseña en el archivo de configuración de NSClient++ para una máquina Windows, necesitamos modificar la definición del comando check_nt para incluir la contraseña. Abrimos el archivo commands.cfg para editarlo.

```
# vi /usr/local/nagios/etc/commands.cfg
```

Se cambia la definición del comando check_nt para incluir el argumento "-s <PASSWORD>" (donde PASSWORD es la contraseña que se especifico en la máquina Windows) así:

```
define command{
command_name check_nt
command_line $USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -s PASSWORD -v $ARG1$ $ARG2$
}
```

Guardar y salir del archivo.
Reiniciando Nagios

Verificar que las configuraciones están correctas

```
# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
Total Warnings: 0
Total Errors:   0
Restart Nagios:
# service nagios restart
```

Si el proceso de verificación produce algún error, se debe arreglar los archivos de configuración antes de continuar. Asegurarse de no reiniciar Nagios hasta que el proceso de verificación se complete sin errores.

PARA AGREGAR MÁS EQUIPOS WINDOWS

Se debe de agregar los equipos, definiendo cada host, en el mismo archivo, windows.cfg

```
define host{
use windows-server        ;Esto se encuentra definido en templates.cfg
host_name winserver1
alias My Windows Server 1
address 192.168.1.3
}
```

Y en cada servicio a monitorear basta con ponerle una coma y el nombre del host, ejemplo:

```
define service{
use generic-service
host_name winserver, winserver1
service_description CPU Load
check_command check_nt!CPULOAD!-l 5,80,90
}
```

Todos los equipos Windows definidos en este archivo windows.cfg quedan por default agregados al grupo siguiente grupo.

```
define hostgroup{
        hostgroup_name  windows-servers ; Nombre del grupo
        alias           Windows Servers         ; Descripción del grupo
}
```

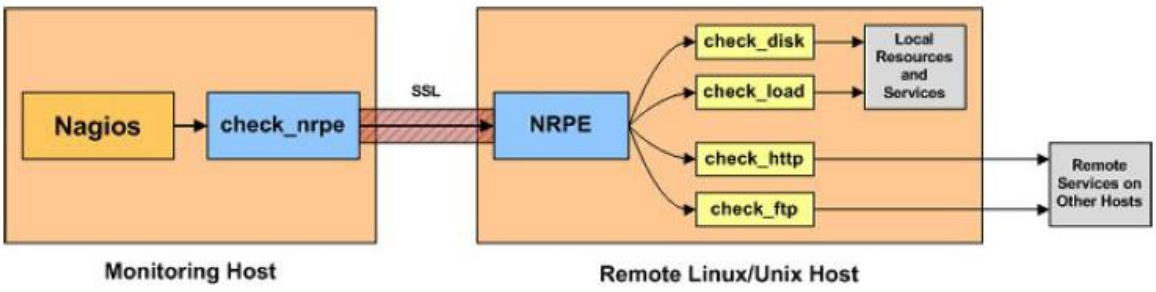
11.12 MONITOREANDO MAQUINAS LINUX

✓ NRPE: Este demonio permite ejecutar plugins en equipos remotos Linux/Unix. Esto puede ser útil si se necesita monitorear los recursos/atributos locales, entre los recursos que se pueden monitorear se encuentran:

- Carga de CPU
- Uso en Disco Duro
- Usuarios firmados
- Procesos Ejecutándose
- Etc.

Este demonio es instalado en la maquina que se va a monitorear el cual se encarga de comunicarse con el servidor de Nagios para entregarle la información solicitada.

Ilustración 19. Descripción del diseño



Este demonio consiste de dos partes o piezas.

- El check_nrpe plugin, el cual reside en el servidor de monitoreo de Nagios
- El demonio NRPE, el cual corre en la maquina Linux que se monitorea.

El demonio NRPE requiere la instalación previa de los plugins de Nagios, ya que sin estos el demonio no podría monitorear ningún servicio local.

11.12.1 Instalando NRPE con xinetd y openssl-devel

✓ Pasos a seguir en la maquina a monitorear (cliente)

Prerequisitos:
Tener instalado Xinetd (Recomendado), openssl-devel.

rpm -q xinetd openssl-devel
package xinetd is not installed ← Quiere decir que no se tiene el paquete instalado
openssl-devel-0.9.7a-43.2

Debido a que no se tiene el paquete instalado se debe realizar la instalación de cada uno, buscando el RPM del paquete que falta por ser instalado en el CD de instalación de la distribución en la que se está trabajando, o si se tiene acceso a

Internet desde la maquina en la que estamos instalando el demonio basta con dar el comando:

yum install xinetd

Cuando exista certeza de que se tienen xinetd y openssl-devel, correctamente instalados, se realiza lo siguiente.
Se crea un usuario nagios

useradd nagios
passwd nagios

Descargar nagios-plugins y el demonio NRPE en una maquina Windows y se sube a la maquina por ftp.

http://www.nagios.org/download/plugins
http://www.nagios.org/download/addons

Abrir la carpeta o directorio donde se encuentran estos dos archivos, en este caso /home/nagios/
Descomprimir e instalar plugins

gunzip nagios-plugins-1.4.14.tar.gz
tar xvf nagios-plugins-1.4.14.tar
Se ingresa al directorio generado por descomprimir el archivo nagios-plugins-1.4.14.tar.gz

cd nagios-plugins-1.4.14

Instalar plugins:
./configure --with-nagios-user=nagios --with-nagios-group=nagios
make
make install

Los permisos para el directorio de los plugins es necesario cambiarlos al usuario nagios

chown nagios.nagios /usr/local/nagios

chown -R nagios.nagios /usr/local/nagios/libexec

Descomprimir el Demonio NRPE que se encuentra en el directorio /home/nagios

gunzip nrpe-2.12.tar.gz
tar xvf nrpe-2.12.tar

Ingresar al directorio generado por descomprimir el archivo nrpe-2.12.tar.gz

cd nrpe-2.12

Instalar el demonio NRPE

./configure
General Options:

 NRPE port: 5666
 NRPE user: nagios
 NRPE group: nagios
 Nagios user: nagios
 Nagios group: nagios
make all
make install-plugin
make install-daemon
make install-daemon-config
make install-xinetd

Continuando con la configuración del NRPE, editar el archivo Xinetd NRPE:

Adicionar Servidor Monitor Nagios en la línea “only_from”

# vi /etc/xinetd.d/nrpe
only_from = 127.0.0.1 <nagios_ip_address>
Guardar y salir

Editar el archivo services:

Adicionar información acerca del servicio del demonio NRPE

```
# vi /etc/services
nrpe      5666/tcp    # NRPE
```

Guardar y salir

Configurar xinetd para que arranque cada que el sistema sea iniciado y reiniciamos el servicio de xinetd:

```
# chkconfig xinetd on
# service xinetd restart
```

Probar el demonio NRPE

Chequear si el demonio NRPE está corriendo y escuchando en el puerto 5666:

```
# netstat -at |grep nrpe
```
La salida debe de ser:
```
tcp    0    0 *:nrpe    *.*    LISTEN
```

Chequear si el demonio NRPE se encuentra funcionando:

```
# /usr/local/nagios/libexec/check_nrpe -H localhost
```
La salida debe de ser:
```
NRPE v2.12
```

NOTA: Se debe de verificar que no esté corriendo ningún firewall o que este configurado para poder tener una comunicación con el servidor de Nagios.

La sintaxis del comando check_nrpe es:

check_nrpe -H <host> [-n] [-u] [-p <puerto>] [-t <tiempo de expiracion>] [-c <comando>] [-a <lista de argumentos>]

Opciones:

-n = No use SSL
-u = Hace que el tiempo de respuesta retorne el estado UNKNOWN en vez de CRITICAL
<Host> = La dirección o el nombre del host que está ejecutando NRPE
[Puerto] = El puerto en el cual está escuchando el servicio (por defecto = 5666)
[Tiempo de expiración] = Numero de segundos antes de el tiempo de respuesta expire (por defecto=10)
[Comando] = El nombre del comando que el equipo remoto debería ejecutar. El nombre del comando que se coloca en esta opción debe estar listado en la lista de comandos del archivo nrpe.cfg
[Lista de argumentos] = Argumentos opcionales que deben ser pasados al comando. Múltiples argumentos deben ser separados por un espacio. Si esta opción es proveída, esta debe ser la última opción en la línea del comando.

Definir los servicios a monitorear vía NRPE en el archivo /usr/local/nagios/etc/nrpe.cfg:

- command[check_users]=/usr/local/nagios/libexec/check_users -w 5 -c 10

- command[check_load]=/usr/local/nagios/libexec/check_load -w 15,10,5 -c 30,25,20

- command[check_disk]=/usr/local/nagios/libexec/check_disk -w 20% -c 10% -p /
- command[check_zombie_procs]=/usr/local/nagios/libexec/check_procs -w 5 -c 10 -s Z

- command[check_total_procs]=/usr/local/nagios/libexec/check_procs -w 150 -c 200

- Guardar y salir

Los cambios que se realizan en el archivo /usr/local/nagios/etc/nrpe.cfg no necesitan reiniciar el servicio xinetd, basta solo con guardar los cambios del archivo.

✓ Pasos a seguir en maquina de NAGIOS (servidor)

Descargar el demonio NRPE en una maquina Windows y subirlo por ftp. http://www.nagios.org/download/addons

Ingresar en la carpeta donde se encuentran este archivo /home/nagios/

Descomprimir el Demonio NRPE

```
# gunzip nrpe-2.12.tar.gz
# tar xvf nrpe-2.12.tar
```

Ingresar al directorio generado por descomprimir el archivo nrpe-2.12.tar.gz

```
# cd nrpe-2.12
```

Compilar e Instalar el demonio NRPE

```
# ./configure
# make all
# make install-plugin
```

Realizar prueba de Conexión entre el demonio NRPE y el Servidor Nagios
Asegurarse de que el servidor de Nagios puede hablar con el demonio NRPE en el servidor remoto (cliente) que desea supervisar. sustituir "<IP de Remote Server>" con la dirección IP de los servidores remotos (clientes)

```
# /usr/local/nagios/libexec/check_nrpe -H <IP of Remote Server   (cliente)>
NRPE v2.12
```

Crear un comando para NRPE
Es necesario crear una definición de comando para que pueda existir la comunicación entre el equipo monitoreado y el servidor de Nagios

```
# vi /usr/local/nagios/etc/objects/commands.cfg
################################################################################
# NRPE CHECK COMMAND
#
# Command to use NRPE to check remote host systems
################################################################################
define command{
        command_name check_nrpe
        command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
}
```

Crear un templated para los equipos Linux en el fichero templates.cfg el cual se encuentra ubicado en /usr/local/nagios/etc/objects

vi /usr/local/nagios/etc/objects/templates.cfg

Ingresar una definición de host

```
define host{
        name                            linux-box-remote; Name of this template
        use                             generic-host; Inherit default values
        check_period            24x7
        check_interval          5
        retry_interval          1
        max_check_attempts      10
        check_command                   check-host-alive
        notification_period             24x7
        notification_interval 30
        notification_options            d,r
        contact_groups                  admin.  ; Le envía notificaciones vía email
        register                0       ;DONT REGISTER THIS - ITS A TEMPLATE
}
```

Crear un fichero en el cual se agregan los equipos LINUX y los servicios que se desean monitorear de cada uno.

```
# vi /usr/local/nagios/etc/objects/linux-box-remote.cfg
define host{
        use     linux-box-remote     ; Definifido en templates.cfg
        host_name Centos5    ; The name we're giving to this server
        alias    Centos5 ; A longer name for the server
        address   192.168.0.5   ; IP address of the server
}

define service{
        use             generic-service
        host_name       Centos5
        service_description CPU Load
        check_command       check_nrpe!check_load
}
```

```
define service{
        use             generic-service
        host_name       Centos5
        service_description Current Users
        check_command       check_nrpe!check_users
}

define service{
        use             generic-service
        host_name       Centos5
        service_description /dev/hda1 Free Space
        check_command       check_nrpe!check_hda1
}

define service{
        use             generic-service
        host_name       Centos5
        service_description Total Processes
        check_command       check_nrpe!check_total_procs
}

define service{
        use             generic-service
        host_name       Centos5
        service_description Zombie Processes
        check_command       check_nrpe!check_zombie_procs
}
```

Activar el archivo de configuración creado, linux-box-remote.cfg:

```
# vi /usr/local/nagios/etc/nagios.cfg
```
Adicionar:

```
# Definitions for monitoring remote Linux machine
cfg_file=/usr/local/nagios/etc/objects/linux-box-remote.cfg
```

Verificar la configuración de nagios que no exista ningún error:

```
# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
Total Warnings: 0
Total Errors:   0
```

Restart Nagios:

service nagios restart

Verificar entrando a la Interfaz Web
http://direccionservidornagios/nagios/

✓ Para agregar más equipos Linux

Se deben agregar los equipos, definiendo cada host, en el mismo archivo, linux-box-remote.cfg

```
define host{
        use             linux-box-remote     ; Inherit default values from a template
        host_name  equipol    ; The name we're giving to this server
        alias           Equipo Linux 1  ; A longer name for the server
        address       192.168.0.5   ; IP address of the server
}
```

Y en cada servicio a monitorear basta con ponerle una coma y el nombre del host, ejemplo:

```
define service{
        use                     generic-service
        host_name               Centos5, equipo1
        service_description   Total Processes
        check_command       check_nrpe!check_total_procs
}
```

11.12.2 Instalando NRPE con INETD y sin OPENSSL-DEVEL

✓ Pasos a seguir en maquina a monitorear (cliente)

Crear un usuario nagios

useradd nagios
passwd nagios

Descargar nagios-plugins y el demonio NRPE en una maquina Windows y se sube por ftp.

http://www.nagios.org/download/plugins
http://www.nagios.org/download/addons

Ubicarse en la carpeta donde se encuentran estos dos archivos /home/nagios/

Descomprimir e instalar plugins
gunzip nagios-plugins-1.4.14.tar.gz
tar xvf nagios-plugins-1.4.14.tar

Entrar al directorio generado por descomprimir el archivo nagios-plugins-1.4.14.tar.gz

#cd nagios-plugins-1.4.14

Instalar plugins:

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

Los permisos para el directorio de los plugins es necesario cambiarlos al usuario nagios

chown nagios.nagios /usr/local/nagios
chown -R nagios.nagios /usr/local/nagios/libexec

Descomprimir el Demonio NRPE que se encuentra en el directorio /home/nagios

gunzip nrpe-2.12.tar.gz
tar xvf nrpe-2.12.tar

Entrar al directorio generado por descomprimir el archivo nrpe-2.12.tar.gz

cd nrpe-2.12

Instalar el demonio NRPE

./configure --disable-ssl
General Options:

 NRPE port: 5666
 NRPE user: nagios
 NRPE group: nagios
 Nagios user: nagios
 Nagios group: nagios
make all
make install-plugin
make install-daemon
make install-daemon-config

Continuando con la configuración del NRPE, si el sistema utiliza inetd con tcpwrappers agregar la siguiente entrada en /etc/inetd.conf:

nrpe stream tcp nowait [nagios] /usr/sbin/tcpd /usr/local/nagios/bin/nrpe -c -n /u
sr/local/nagios/etc/nrpe.cfg -i

Si el sistema utiliza inetd SIN tcpwrappers agregar la siguiente entrada en /etc/inetd.conf:

nrpe stream tcp nowait [nagios] /usr/local/nagios/bin/nrpe -n -c /usr/local/nagios/etc/nrpe.cfg --inetd

Editar el archivo services:
Adicionar información acerca del servicio del demonio NRPE
vi /etc/services
nrpe 5666/tcp # NRPE
Guardar y salir

Ahora se debe de reiniciar el servicio INETD

ps -ax |grep inetd

Warning: bad syntax, perhaps a bogus '-'? See /usr/share/doc/procps-3.2.3/FAQ
29227 ? Ss 0:05 inetd -stayalive -pidfile /var/run/inetd.pid
15964 pts/0 R+ 0:00 grep INETD

Reiniciar el proceso para que asuma la nueva configuración, por lo que se tiene en cuenta el número del pid, 29227

kill -1 29227

Probar el demonio NRPE, y chequear si el demonio NRPE está corriendo y escuchando en el puerto 5666:

netstat -at |grep nrpe
La salida debe de ser:
tcp 0 0 *:nrpe *.* LISTEN

Chequear si el demonio NRPE se encuentra funcionando:

/usr/local/nagios/libexec/check_nrpe -H localhost
La salida debe de ser:
NRPE v2.12

NOTA: se debe verificar que no esté corriendo ningún firewall o que este configurado para poder tener una comunicación con el servidor de Nagios.

Definir los servicios a monitorear vía NRPE en el archivo /usr/local/nagios/etc/nrpe.cfg:

- command[check_users]=/usr/local/nagios/libexec/check_users -w 5 -c 10
- command[check_load]=/usr/local/nagios/libexec/check_load -w 15,10,5 -c 30,25,20
- command[check_disk]=/usr/local/nagios/libexec/check_disk -w 20% -c 10% -p /
- command[check_zombie_procs]=/usr/local/nagios/libexec/check_procs -w 5 -c 10 -s Z

- command[check_total_procs]=/usr/local/nagios/libexec/check_procs -w 150 -c 200

- Guardar y salir

✓ Pasos a seguir en la máquina de NAGIOS (Servidor)

Descargar el demonio NRPE en una maquina Windows y se sube por ftp.

http://www.nagios.org/download/addons

Ubicarse en la carpeta donde se encuentran este archivo en nuestro caso /home/nagios/

Descomprimir el demonio NRPE
gunzip nrpe-2.12.tar.gz
tar xvf nrpe-2.12.tar

Entrar al directorio generado por descomprimir el archivo nrpe-2.12.tar.gz

cd nrpe-2.12

Compilar e Instalar el demonio NRPE

./configure
make all
make install-plugin

Prueba de Conexión entre el demonio NRPE y el Servidor Nagios
Asegurarse de que el servidor Nagios puede hablar con el demonio NRPE en el servidor remoto (cliente) que desea supervisar. Sustituir "<IP de Remote Server>" con la dirección IP de los servidores remotos (clientes)

/usr/local/nagios/libexec/check_nrpe -H <IP of Remote Server (cliente)>
NRPE v2.12

La configuración del servidor nagios es igual a como se configura cuando se instala con xinetd y openssl-devel

11.13 CONFIGURACIONES UNE TELEFÓNICA DE PEREIRA

Interfaz Nagios Web: http://10.4.251.13/nagios
Servidor Nagios: 10.4.251.13
Sistema Operativo: CENTOS 5.2 Linux

- Para monitorear Servidores Windows se utilizo la instalación (MONITOREANDO MAQUINAS WINDOWS)

- Para monitorear Servidores LINUX se utilizo la instalación (INSTALANDO NRPE CON XINETD Y OPENSSL-DEVEL)

- Para monitorear Servidores AIX se utilizo la instalación (INSTALANDO NRPE CON INETD Y SIN OPENSSL-DEVEL)

11.14 CREACIÓN DE SCRIPTS (PLUGGINS) PARA NAGIOS

Los scripts para nagios se pueden crear en lenguaje shell, perl, etc. Se utilizo el lenguaje bash para crear scripts, el siguiente es un ejemplo de la creación e implementación de un script que da como resultado saber si la cola de mensajes está en estado OK, WARNING, CRITICAL, dependiendo de unos valores configurables.

- Ingresar al equipo que le deseamos monitorear la cola de mensajes, en este caso el servidor mu el cual tiene la dirección IP 172.16.1.28, conectarse a la maquina ingresar el usuario root, y la respectiva contraseña

    - Ingresar al directorio /usr/local/nagios/libexec en este directorio se encuentran todos los plugins que se encargan de hacer operaciones y dar una respuesta.
    # cd /usr/local/nagios/libexec

    - Crear un archivo nuevo llamado check_cola

vi check_cola

- Escribir el algoritmo programado en shell, el cual dará la respuesta de cuantos mensajes están en cola.

```
#Mensajes en Cola
w=$2
c=$4
npi=0
linea=`postqueue -p | tail -1`
if [ "$linea" == 'Mail queue is empty' ]
then
echo "Numero de mensajes en cola OK - cola vacia |;$w;$c;$npi"
exit 0
else
cola=`echo $linea | cut -d" " -f 5`
fi
# devolver la respuesta
if [ $cola -lt $w  ]
then
   echo "Numero de mensajes en cola OK - $cola en cola |;$w;$c;$npi"
   exit 0
fi
if [ $cola -lt $c ]
then
   echo "Numero de mensajes en cola WARNING - $cola en cola |;$w;$c;$npi"
   exit 1
fi
echo "Numero de mensajes en cola CRITICAL - $cola en cola |;$n;$w;$c;$npi"
exit 2
```

- Guardar y salir

- Dar todos los permisos al archivo, además le brindamos acceso al usuario nagios

```
# chown nagios.nagios  check_cola
# chmod 755 check_cola
```

- Configurar el nuevo script en el archivo de configuración de NRPE el cual se encuentra en /usr/local/nagios/etc

vi nrpe.cfg

- En la línea de comandos agregamos

command[check_cola]=/usr/local/nagios/libexec/check_cola -w 5 -c 10
Donde –w 5: es el numero de mensajes en cola que darían una alerta WARNING
Donde –c 10: es el numero de mensajes en cola que darían una alerta CRITICAL

- Ahora procedemos a realizar una prueba desde la maquina donde se encuentra instalado Nagios.

Enviar la siguiente línea de comando
/usr/local/nagios/libexec/check_nrpe -H 172.16.1.28 -c check_cola
Numero de mensajes en cola OK - cola vacia |;5;10;0

En este caso respondió que la cola está vacía, lo que quiere decir que el script está funcionando correctamente

- Ahora se procede llamando este nuevo script desde el servidor de nagios

- Ingresar al servidor de nagios (10.4.251.13) ingresar root, contraseña.

- Ubicarse en el directorio /usr/local/nagios/etc/objects/

cd /usr/local/nagios/etc/objects/

- Editar el archivo linux-box-remote.cfg, que fue creado previamente cuando se empezó a monitorear otros servicios de la maquina “mu” y agregar al final el nuevo servicio que monitoreara la cola de mensajes de el servidor “mu”.

vi linux-box-remote.cfg
Agregar:

```
define service{
        use                 linux-service ; definido en templates.cfg
        host_name       mu              ; nombre del equipo que contiene el script
        service_description Mensajes en cola     ; Descripcion
```

```
        check_command       check_nrpe!check_cola ; nombre del comando
        }
```
Guardar y Salir

- Verificar la configuración de nagios que no haya ningun error y se reinicia el servicio de Nagios:

```
# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
Total Warnings: 0
Total Errors:   0
Restart Nagios:
# service nagios restart
```

11.15 RESULTADOS OBTENIDOS

En el momento en que se realizo la investigación acerca de monitoreo se obtuvo que NAGIOS era la aplicación más completa para implementar dentro de la organización, debido a las características ya nombradas anteriormente y dentro de las cuales se puede enmarcar la alta disponibilidad, además partiendo de la experiencia obtenida por un grupo de personas que ya han implementado dicha herramienta, el alto nivel de documentación con la que cuenta la aplicación en Internet, se convirtió en una guía constante para la solución de los problemas presentados.

La herramienta utilizada para el monitoreo ha demostrado con el transcurso de los días después de la implementación, que cumple con los requerimientos que exige la empresa, entre los cuales se encuentra:

- La disponibilidad
- La seguridad
- Interface Web
- La implementación de Plugins, los cuales permiten la escalabilidad del monitoreo.
- Notificaciones vía Email.

- Monitoreo las 24 horas del día y durante toda la semana.

- Compatibilidad con los diferentes Sistemas Operativos, con los que la empresa cuenta.

- Aumentar la confiabilidad de los servicios que prestan, gracias a las notificaciones preventivas que brinda la herramienta.

- Graficas de monitoreo

- Flexible a la configuración.

Por lo tanto se puede notar que la herramienta es demasiado completa, y para la organización muy necesaria, ya que de esta forma se nota que suple las necesidades establecidas por la organización, dando como resultado la importancia de apoyar el software libre dentro de las organizaciones.

12. HERRAMIENTA DE CONTROL DE INVENTARIO

12.1 JUSTIFICACIÓN

El software libre es gratuito, seguro, aporta calidad, además brinda la libertad de utilizarse en las organizaciones, esto implica buen funcionamiento por menos gastos, estas son algunas de las razones por las cuales se eligió la herramienta de control de inventario “OCS INVENTORY”, adicional a esto, la ya nombrada herramienta, también cuenta con una gran documentación en la red, y un muy considerable número de usuarios que han tenido experiencia y resultados bastante buenos en sus instalaciones y funcionamiento de la misma, dicha herramienta se puede instalar en diferentes tipos de Sistemas Operativos, pero se selecciono la distribución de Linux “Centos” ya que esta posee características, de seguridad, rapidez, estabilidad, utiliza mejor los recursos, la probabilidad de bloqueo es demasiado baja, y una ventaja organizacional fue que ya se contaba con una distribución de Centos instalada, en la cual se encuentra implementado NAGIOS y esta dispone de memoria y capacidad de disco suficiente para la instalación de OCS INVENTORY, de esta manera optimizamos recursos y tiempo.

12.2 ESPECIFICACIONES OCS INVENTORY

12.2.1 OCS INVENTORY. Open Computer and Software Inventory Next Generation (OCS) es un software libre que permite a los usuarios administrar el inventario de sus activos de tecnologías de información. OCS-NG recopila información sobre el hardware y software de equipos que hay en la red que ejecutan el programa de cliente OCS ("agente OCS de inventario"). OCS puede utilizarse para visualizar el inventario a través de una interfaz Web. Además, OCS comprende la posibilidad de implementación de aplicaciones en los equipos de acuerdo a criterios de búsqueda. Además, tiene muchas opciones más como escanear la red por medio del IPDiscovery, o instalar aplicaciones remotamente creando Builds

12.2.2 Funcionamiento Interno. OCS se basa en los estándares vigentes. El diálogo entre los equipos clientes y el servidor se encuentra implementado en HTTP (Hypertext Transfer Protocol) y el formato de los datos se realiza en XML.

12.2.3 Servidor. El servidor de administración utiliza Apache, MySQL y Perl. OCS es multiplataforma y esto se da gracias a su simple diseño y el uso de mod_perl, el rendimiento del lado del servidor es muy bueno. Una máquina con pocos requerimientos podría realizar el inventario de miles de máquinas sin ningún tipo de problemas. El servidor, puede ser instalado en los siguientes sistemas operativos:

- GNU/Linux (Ubuntu, Debian, Suse, RedHat, Gentoo, Knoppix, Slackware, Mandriva, Fedora y Centos)

- Windows (XP, 2000, server 2003).

12.2.4 Agentes. Para recoger el máximo de la información posible, hay agentes que están instalados en equipos con los siguientes sistemas operativos:

- GNU/Linux (Ubuntu, Debian, Suse, RedHat, Gentoo, Knoppix, Slackware, Mandriva, Fedora y Centos).

- Windows (95, 98, NT4, 2000, XP, server 2003, Vista).

- Mac OS X (no official).

- Sun Solaris (no official).

- IBM AIX (no official).

12.2.5 Interfaz de Web. Una interfaz de Web opcional escrita en PHP ofrece servicios complementarios:

- Consulta del inventario

- Gestión de derechos de usuario

- Una interfaz de desglose servicio (o Helpdesk) para los técnicos

OCS + GLPI

GLPI es una aplicación Web de software libre distribuido bajo licencia GPL, que facilita la administración de recursos informáticos, el cual sus principales funcionalidades están articuladas sobre dos ejes.

El primer eje está relacionado con el inventario de todos los recursos informáticos, y el software existente (permite registrar y administrar el inventario de hardware, software y cualquier tipo de periféricos como impresoras, monitores, mouse, teclados, scanners, webcams, discos externos, tabletas gráficas, etc...), de una empresa o una red de computadora, cuyas características se almacenan en bases de datos de forma manual.

El otro eje está basado la administración y los historiales de las diferentes labores de mantenimiento y procedimientos relacionados, llevados a cabo sobre esos recursos informáticos (permite registrar información de inventario, de contactos, registrar solicitudes de servicio y asignar la atención de dichas solicitudes al personal de soporte correspondiente).

Una excelente idea es integrar GLPI y OCS, ya que juntando el HELP DESK de GLPI más la posibilidad de hacer un inventario de hardware y software totalmente actualizado y automático de OCS podemos hacer seguimiento de todo lo que se tenga inventariado y con ello conseguir estadísticas de falla, seguimiento del manejo del equipamiento de usuario, etc. Estas dos herramientas ya son capaces de trabajar en conjunto y además los equipos de desarrollo de ambos proyectos se han propuesto a corto plazo una fuerte integración de funcionalidades.

Extensión

El Inventario de OCS puede utilizarse para alimentar el Gerente de GLPI y así ofrece una potente solución de gestión de activos de TI.

12.2.6 Licencia. OCS Inventory es un software libre que se publica bajo la GNU GPLv2. Los desarrolladores son titulares directos de las regalías.

12.3 INSTALACIÓN

12.3.1 Instalación OCS Inventory (Servidor). Aplicación que se utiliza para realizar inventario de los equipos de la red mediante un agente que se instala en el cliente, los pasos a seguir son los siguientes:

- Primero se debe Instalar MySQL y Apache, en el caso de no tenerlo instalado.

yum install mysql-server mysql httpd

O por medio del repositorio
rpm –ivh mysql-server mysql httpd

- Editar el archivo de configuración de httpd y agregar lo siguiente

vi /etc/httpd/conf/httpd.conf
ServerName: ocs-inventory:80

Reiniciar el servicio de httpd (Apache)
service httpd start

Configurar para que inicie automáticamente cada que se reinicie el servidor
chkconfig httpd on

- Iniciar el servicio de mysql y configurar para permitir que se ejecute Cada vez que el servidor sea reiniciado,

service mysqld start
chkconfig mysqld on

- Cambiar la contraseña de mysql

mysql -u root mysql
mysql> UPDATE user SET password=PASSWORD('desired_password')
->WHERE User='root';
mysql>DELETE FROM user WHERE user = '';
>FLUSH PRIVILEGES;

mysql>DROP DATABASE test;
mysql>exit

- Instalar los siguientes package de PERL en el caso de que no se encuentren instalados.

Si no se encuentran estos repositorios entonces se deben instalar directamente desde Internet, lo cual implica tener configurado el Proxy en el caso de que exista el mismo.

yum install perl-Apache-DBI
yum install perl-SOAP-Lite

Buscar en los repositorios (DVD) subirlos por ftp e instalarlos

rpm -ivh perl-Compress-Zlib
rpm –ivh perl-HTML-Tagset
rpm –ivh perl-HTML-Parser
rpm –ivh perl-libwww-perl
rpm –ivh perl-XML-Parser
rpm –ivh perl-XML-Simple
rpm -ivh perl-DBI
rpm -ivh perl-DBD-MySQL
rpm -ivh perl-Net-IP

- Instalar los siguientes paquetes de PHP, los cuales configuran la consola de administración de OCS.

Revisar que paquetes no están instalados e instalarlos por medio del Repositorio

rpm –q php-mysql php-devel zlib-devel php-pear php-gd gcc
gcc-4.1.2-42.el5
zlib-devel-1.2.3-3

Los que no se encuentran instalados se deben de buscar en los repositorios los subimos por ftp y los instalamos

rpm -ivh php-pdo
rpm -ivh php-mysql
rpm -ivh php-devel
rpm -ivh php-pear
rpm -ivh php-gd

- Reiniciar el servicio de Apache para que los cambios tengan efecto.

service httpd restart

12.3.2 Instalar la aplicación OCS INVENTORY (Server)

- Descargar la última versión disponible en la Web Oficial, subir el archivo vía ftp o de cualquier otra forma.

- si esta en un archivo comprimido (tar.gz) descomprimir con los siguientes comandos:

gunzip OCSNG_UNIX_SERVER-1.3.1.tar.gz
tar xvf OCSNG_UNIX_SERVER-1.3.1.tar

- Ingresar a la carpeta creada con los datos descomprimidos

cd OCSNG_UNIX_SERVER-1.3.1

- Ejecutar el siguiente comando:

./setup.sh

- Aparecerán una serie de preguntas:
  - CAUTION: If upgrading Communication server from OCS Inventory NG 1.0 RC2 and previous, please remove any Apache configuration for Communication Server!
    Do you wish to continue ([y]/n)? presiona enter ya que la opción “Y” esta por defecto entre corchetes
    Your MySQL client seems to be part of MySQL version 5.0.

Your computer seems to be running MySQL 4.1 or higher, good ;-)

- Which host is running database server [localhost] ? colocar la dirección IP del servidor (loopback) 127.0.0.1 o servidor local

- On which port is running database server [3306] ? se deja el puerto de la base de datos por defecto que es (3306) presionar enter

- Where is Apache daemon binary [/usr/sbin/httpd] ? presionar enter

- Where is Apache main configuration file [/etc/httpd/httpd.conf] ? aquí se debe colocar la ruta correcta que es: /etc/httpd/conf/httpd.conf

- Which user account is running Apache web server [xxxx] ? presionar enter para dejar la cuenta de usuario por defecto

- Which user group is running Apache web server [xxx] ? presionar enter, para dejar la cuenta de usuario por defecto

- Where is PERL Intrepreter binary [/usr/bin/perl] ? presionar enter

- Do you wish to setup Communication server on this computer ([y]/n)? presionar enter

- Where is Apache Include configuration directory [//etc/httpd/conf.d/] ? cololar la ruta correcta: /etc/httpd/conf.d/

- Where to put Communication server log directory [/var/log/ocsinventory-NG] ? presionar enter

- Do you wish to setup Administration server (web administration console) on this computer ([y]/n) presionar enter

- Where is Apache root document directory [] ? se coloca la ruta: /var/www/

- Reiniciar los servicios de apache y mysql:

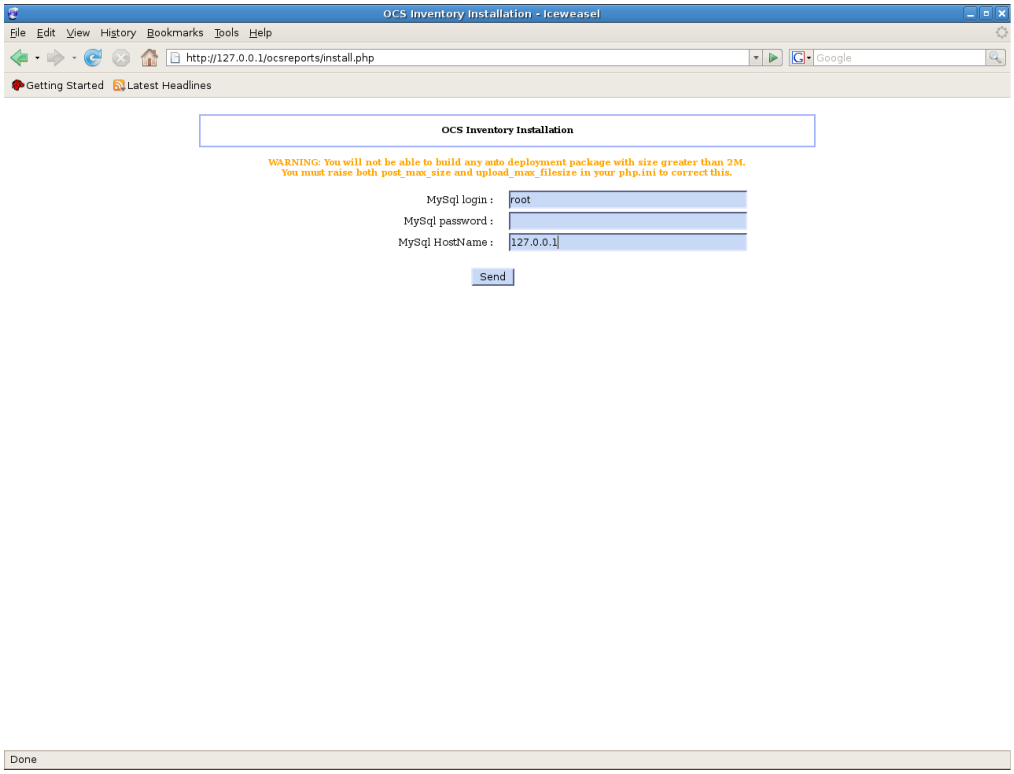
```
# service httpd restart
# service mysqld restart
```

- Abrir un navegador Web y colocar la siguiente dirección: http://(ipdelservidor)/ocsreports/install.php

- Aparecerá la siguiente pantalla: solicitando los datos:

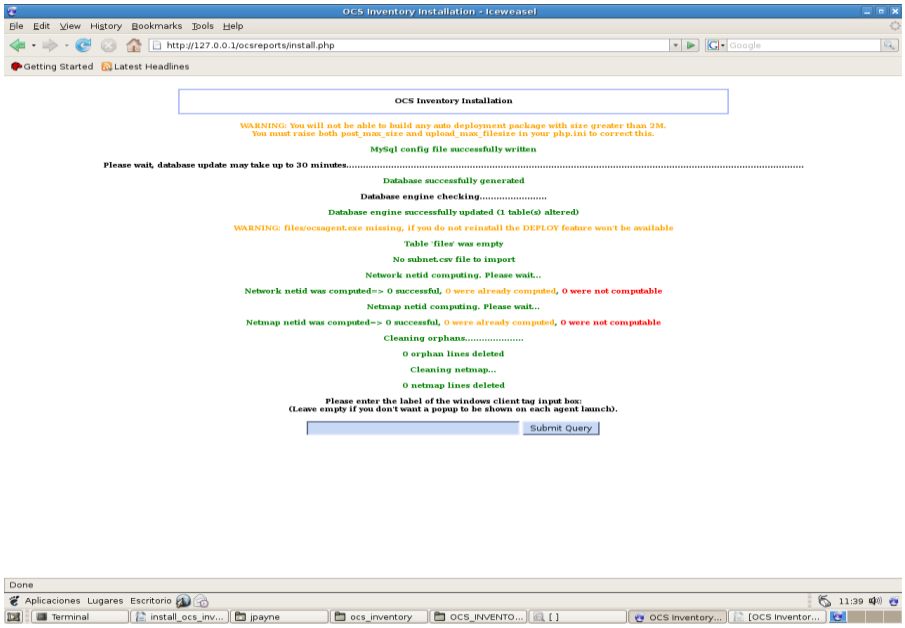
MySql login: root - Aquí se coloca root
MySql password: - por ahora se deja en blanco
MySql HostName: 127.0.0.1 - se coloca la dirección loopback
Presionar el botón send

Ilustración 20. Pantalla configuración.



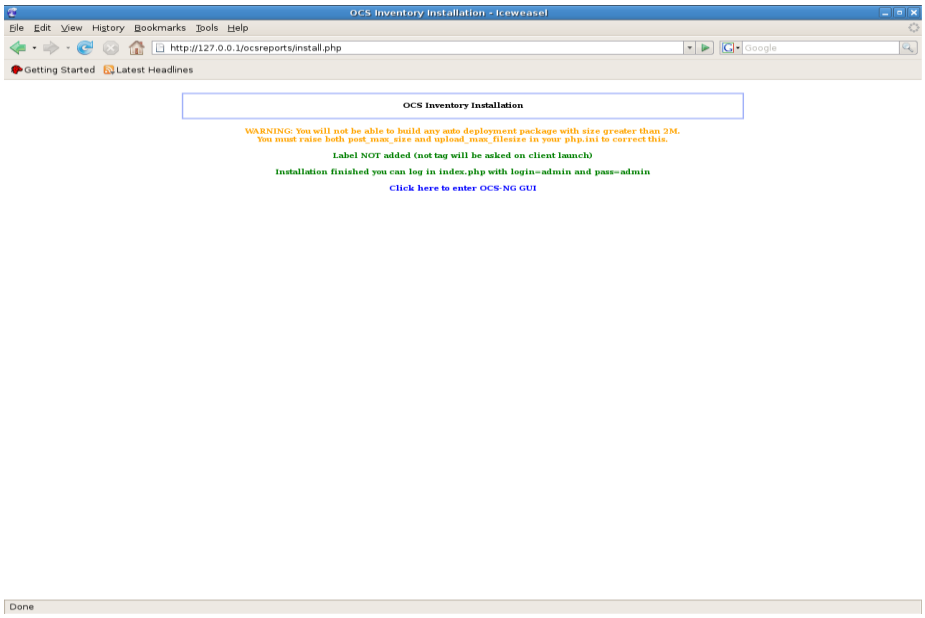
- Aparecerá la siguiente pantalla: en la cual se debe presionar el botón Submit Query

Ilustración 21. Pantalla datos configurados



- En la siguiente pantalla hacer clic en Click here to enter OCS-NG GUI

Ilustración 22. Pantalla adicional.



- Seleccionar el idioma, ahora proceder a introducir el usuario y la contraseña (usuario: admin, contraseña: admin) y hacer clic en el botón Aceptar

12.3.3 Instalar agente en Windows

- Se realiza un script .bat con la siguiente información:

```
@echo
echo Running system inventory, please wait
REM Call to OCS Inventory NG agent for deployment
if exist "%programfiles%\OCS Inventory Agent\OCSInventory.exe" goto exit
\\fsw2k8\publico\ocs-agente-windows\OcsAgentSetup.exe /S /SERVER: 10.4.251.13 /PNUM: 80 /NP
/TAG:"cualquiertexto" /DEBUG
:exit
cd "%programfiles%\OCS Inventory Agent"
OCSInventory.exe /server:10.4.251.13 /PNUM: 80 /debug /np /TAG:"Instalado correctamente"
echo Instalado Correctamente
```

Donde \\fsw2k8\publico\ocs-agente-windows\OcsAgentSetup.exe es un directorio compartido en la red donde se encuentra el instalador del agente.

- Ingresar en la maquina Windows, como administrador y lo ejecutamos, automáticamente se instalara y enviara su reporte a el servidor de OCS INVENTORY.

- También se puede subir dicho script en el directorio activo y se puede disparar la ejecución para todos los equipos Windows, de la empresa.

12.4 CONFIGURACIONES UNE TELEFÓNICA DE PEREIRA

- Dirección de la Web: http://10.4.251.13/ocsreports/

- Servidor Nagios: 10.4.251.13

- Sistema Operativo: CENTOS 5.2 Linux

12.5 RESULTADOS OBTENIDOS

Para la elección de la herramienta que realiza el control de inventario se partió de la necesidad de remplazar una herramienta utilizada por la organización, la cual adicional a realizar el control de inventario permite realizar, Control Remoto, Asistencia Remota, operaciones de solicitud de servicio, entre otras, por lo mencionado anteriormente se investigo sobre aplicaciones de software libre que permitieran realizar dichas tareas, dando como resultado una herramienta llamada OCS INVENTORY, la cual permite realizar control de inventario de toda la organización y además permite el manejo de solicitudes de servicio, pero no realiza, ni control remoto, ni asistencia remota, esto no pareció un problema para la organización.

Luego de la investigación y la recolección de información acerca de la herramienta, se procedió a la instalación, la cual se realizo completamente, pero para la organización no fue viable, ya que se hizo muy necesario tener control remoto y asistencia remota, gracias a esto se llego a la conclusión que iban a continuar utilizando la herramienta anterior, pero de igual forma dejar OCS INVENTORY implementado, para el momento en que sea necesario utilizarlo.

Gracias a lo a dicha conclusión podemos deducir que OCS INVENTORY es una herramienta utilizada y creada única y exclusivamente para la recolección de Inventario de software y hardware, y que no existe ninguna herramienta que este bajo la licencia de software libre realizada para Control de Inventario, Control Remoto y Asistencia Remota.

13. PLAN DE CONTINGENCIA

13.1 RESUMEN

Se realizo la actualización del documento de plan de contingencia con el cual cuenta la organización, y se adicionaron los equipos que no se encontraban documentados por ser relativamente nuevos con respecto al plan. En dicho documento se presentan los planes de manejo de riesgos a los cuales está permanentemente expuesta la Subgerencia de Tecnologías de Información. En los cuales se integran elementos como lo son, el Hardware y la Información, los cuales después de haber realizado una valoración de riesgos se encontraron como los elementos de mayor impacto.

13.2 INTRODUCCIÓN

Día a día se evidencia que la información representa una parte demasiado importante dentro de una organización, siendo necesaria en todo momento, por lo cual debe tener la total disponibilidad para ser modificada o consultada. Cierta cantidad de la información en las organizaciones se maneja de forma digital, es decir por medio de servidores, los cuales como su nombre lo indica brindan servicios que permiten de una forma mas eficiente manipular dicha información. En definición un servidor es “un tipo de software o hardware que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar los mismos”. Ahora bien, para lograr el objetivo mencionado anteriormente de tener disponibilidad de la información se deben tener en cuenta algunas técnicas, las cuales eviten la perdida, rompimiento de la privacidad y la veracidad de la misma; teniendo backups, también teniendo los servidores en cluster uno remplazando al otro en caso de caída de alguno, etc. Los servidores de la organización se encuentran implementados de manera física y de manera virtual.

Servidor Real (Físico): Es un servidor exclusivo, en el que se puede instalar aplicaciones, las cuales cuentan con los recursos totales de maquina

Servidor Virtual: Es una partición dentro de un servidor que habilita varias máquinas virtuales dentro de dicha máquina por medio de varias tecnologías.

Los servidores dedicados virtuales (SDV) usan una avanzada tecnología de virtualización, que le permite proveer acceso root y la capacidad de reiniciarlo cuando desee, igual que un servidor dedicado. Con la posibilidad de instalar sus propias aplicaciones y controlar completamente la configuración de su servidor, los SDV representan una alternativa económica y eficiente para aquellos que desean disfrutar los beneficios de un servidor dedicado pero aun no poseen el presupuesto para hacerlo.

Es necesario que existan dispositivos intermedios para la comunicación de equipos que comparten información, estos dispositivos se les llama elementos de networking, dichos elementos pueden ser Switches, Routers, Access Point, etc.

Los elementos anteriormente mencionados son electrónicos y esto influye en que debe existir una correcta fluidez de energía eléctrica para poder funcionar correctamente, de lo cual se genera una enorme necesidad de tener siempre electricidad disponible para la infraestructura de tecnología de la empresa, para suplir dicha necesidad se encuentran equipos llamados UPS.

13.3 PROCEDIMIENTO

La privacidad de los servicios y de los servidores que contienen información esencial de la empresa es prioritaria en la organización Une Telefonica de Pereira, esto por cuestiones de seguridad. Por lo tanto, solo se puede mencionar los pasos que se tuvieron en cuenta para realizar la actualización del documento de plan de contingencia, cumpliendo con esta exigencia en los siguientes puntos se mencionara que se hizo pero no se mencionaran datos exactos.

- Se realizo la actualización de la documentación de las diferentes tecnologías que se encuentran implementadas en la subgerencia de Tecnologías de Información de Une Telefonica de Pereira, para tener siempre disponible la información, en lo que influyen Switches, Servidores, UPS, PCs, partiendo de un plan de contingencia con el cual cuenta la organización.

- Se realizo la revisión y la actualización correspondiente a la documentación y plan de contingencia de cada uno de los servidores más importantes de la organización, adicional a esto se le creó su plan y documentación a los servidores que no contaban con dicha información.

- Se utilizo el siguiente formato para documentar los servidores.

CONFIGURACIÓN NOMBRE DEL SERVIDOR

I. DATOS GENERALES

UBICACIÓN FÍSICA:
MARCA:
MODELO:
SERIAL:
MEMORIA RAM:
PROCESADOR:
SISTEMA OPERATIVO:
DIRECCIÓN IP:
RESPONSABLE:
TIPO MAQUINA:

II. DESCRIPCIÓN:

II. SERVICIOS OFRECIDOS

-

III. INFORMACIÓN DISCOS

Discos Internos:

IV. FILESYSTEMS

Filesystem	Discos	Servicio	Sistema de Backup

V. PROCEDIMIENTOS ASOCIADOS

Fecha:	Realizado por:	Departamento: Subg. TI
Descripción:		
Solución:		

VI. PROCEDIMIENTOS DE BACKUP INTERNOS

NOMBRE	
DESCRIPCIÓN	
DESTINO	Hacia dónde va el backup
TIPO	Tar, tsm, ftp
AUTOMATIZACIÓN	cron, Schedule tsm, tarea prog.
COMANDO	Script usado (si aplica)
LOG	Que Log genera
Procedimiento de backup	
PROCEDIMIENTO DE RESTAURACIÓN	
Explicación de qué se puede restaurar con este backup	
Explicación de cómo se restaura.	

A cada servidor crítico se le aplico el formato, garantizando que cada uno cuente con un documento de configuración y respaldo.

- La organización cuenta con un espacio Web, donde se encuentra información básica acerca de cada uno de los servidores, en este espacio se creó un link para la documentación creada de cada uno de los ya mencionados servidores, para de esta forma tenerlos mejor referenciados y a su vez un mejor acceso a los soportes creados de configuración.

13.4 RESULTADOS OBTENIDOS

El documento de Plan de Contingencia con el cual contaba la empresa, y en el que se encontraba ilustrado una buena solución para la contingencia de los servidores y dispositivos de red de la organización, pero dicho documento se encontraba desactualizado con respecto a los nuevos servidores implementados en la organización, por lo tanto se procedió a documentar cada uno de los servidores críticos que existen a la fecha.

Se realizo la actualización del documento de Plan de Contingencia, actualizando y creando un documento por cada dispositivo, de lo anterior podemos deducir que se realizo la entrega de un documento actualizado con respecto a la continencia, la configuración y los sistemas de respaldo con que cuenta la empresa de los servidores actuales de la organización.

CONCLUSIONES

Se evidencia la necesidad de implementar sistemas de monitoreo en el área de TI, ya que permite tener acciones, Preventivas y Correctivas, que reducen el numero de errores que pueda presentar la infraestructura y así brindar la disponibilidad de los recursos de una forma oportuna.

Es necesario tener cierto nivel de control sobre los aplicativos y las herramientas que utiliza la organización, lo cual hace claro la necesidad de utilizar una herramienta que permita realizar el control del inventario de software y hardware de cada uno de los equipos de la organización, ya que la utilización no correcta de algunos aplicativos pueden poner en problemas jurídicos a la empresa.

La organización siempre ha tenido el conocimiento de lo necesario que es tener un Plan de Contingencia, ya que este permite tener planes y estrategias para aplicar en el momento de que exista algún error en los elementos que permiten tener un buen funcionamiento de todos los servicios prestados por el área de Tecnologías de Información de la empresa, por eso se hizo necesario y a su vez se evidencio la necesidad de realizar la actualización de dicho plan, gracias a esto se entendió sobre la importancia que tiene la documentación dentro del tema de respaldo de los servidores, ya que minimiza los tiempos de recuperación de los servicios que se prestan.

Durante el desarrollo del proyecto gracias a la experiencia obtenida se dedujo que el Monitoreo, el Control de Inventario y un buen Plan de Contingencia, son indispensables para un mejor funcionamiento del departamento de tecnologías de información de una organización.

El Software Libre, está al alcance de todos, nos brinda libertad de uso, ahorra gastos, aumenta la capacidad tecnológica y reduce la dependencia a proveedores, por lo tanto, la organización hace bien en implementar herramientas de software libre dentro del ámbito de las tecnologías, dichas herramientas son robustas, y de alta calidad, y esto trae consigo enormes beneficios para el área de TI.

Se brindo apoyo oportuno de soporte de red y ofimática dentro de la organización, de los cuales se puede nombrar, la migración de el servidor de correo electrónico,

instalación y actualización masiva de Donet, instalación de normas, configuración de equipos, entre otros trabajos asignados.

Se realizo investigación, la implementación y la documentación de la herramienta de Monitoreo.

Se realizo la investigación, la implementación y la documentación de la herramienta de Control de Inventario.

Se realizo la evaluación y se le aplicaron las actualizaciones necesarias al plan de contingencia con el cual cuenta la organización.

El cronograma propuesto fue cumplido con total éxito en cada uno de los puntos planteados, cumpliendo con esto los intervalos establecidos.

RECOMENDACIONES

Se recomienda realizar un backup constante al servidor de NAGIOS, para evitar futuras reinstalaciones y configuraciones del sistema de monitoreo y de control de inventario.

En caso de que se desee reinstalar alguna de las herramientas trabajadas en este documento se recomienda, realizarlo en el sistema operativo CENTOS 5.2, ya que gracias a la experiencia adquirida se puede asegurar que funcionan en óptimas condiciones.

Se recomienda crear la documentación respectiva a cada servidor que se implemente en la organización, para así tener siempre disponible un documento de configuración y respaldo, para utilizarlo en caso de emergencia y evitar futuras pérdidas.

BIBLIOGRAFÍA

Intranet, Une Telefónica de Pereira S.A.

INTEGRACIÓN DE SISTEMAS. Análisis y monitoreo de redes.
Disponible en: http://www.integracion-de-sistemas.com/analisis-y-monitoreo-de-redes/index.html

PROYECTO POLICITY. Manual de capacidad en defensa y promoción.
Disponible en:
http://www.policyproject.com/pubs/advocacy/Spanish/Policy%20Proj%20Sec%20III-8.pdf

WORLD LINGO. Servicio de red.
Disponible en: http://www.worldlingo.com//ma/enwiki/es/Network_service/1

MAYORAL, César. Planes de contingencia. Madrid / España

WIKIPEDIA. Plan de contingencias.
Disponible en: http://es.wikipedia.org/wiki/Plan_de_Contingencias

NAGIOS. The Industry Standard in IT Infrastructure
Disponible en: http://www.nagios.org/, Nagios - Monitoring

OCS, Next generation Inventary. Powerful inventory and package deployment system for Windows and Unix like Computers.
Disponible en: http://www.ocsinventory-ng.org/

SourcePYME. Migración a Software Libre. Instituto Tecnológico de Informática y la Universidad Politécnica: Valencia / España.

WordReference. Online language dictionaries: Vienna, Virginia, USA.
Disponible en: http://www.wordreference.com

BELT. Planes de contingencia.
Disponible en: http://www.seguridad-la.com/artic/segcorp/7209.htm

FORUM TECNOLOGICO. Sistemas de gestión.
Disponible En: www.forumt.net