



**UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE CIENCIAS
ESCUELA DE COMPUTACION**

**SISTEMA AUTOMATIZADO PARA LA GESTION DE
SOLICITUDES EN TECNOLOGIAS DE
INFORMACION**

TRABAJO ESPECIAL DE GRADO
presentado ante la ilustre
UNIVERSIDAD CENTRAL DE VENEZUELA
como parte de los requisitos para optar al el título de
LICENCIADO EN COMPUTACION

REALIZADO POR

Katherina Angélica Rodríguez Ossandón
Sergio Daniel Hernández Rodríguez

TUTOR ACADEMICO

Profesora Ana Morales

Caracas, Octubre 2008

RESUMEN

El acelerado avance en tecnologías de información ha traído como consecuencia el crecimiento exponencial de las redes de datos, aumentando considerablemente la cantidad de dispositivos de interconexión y de usuarios en las mismas, lo que ha originado que la tarea de mantenimiento, atención y soporte a usuarios en las organizaciones sea cada vez más compleja y costosa, aún contando con el conocimiento y las herramientas apropiadas. En este Trabajo Especial de Grado se presenta un Sistema automatizado, que permite llevar la gestión de solicitudes de servicio, gestión de inventario de plataforma tecnológica y de activos de red de una forma integrada, a fin de: Mejorar la productividad de los usuarios de la organización, controlar y monitorizar los procesos de servicio, optimizar el uso de los recursos disponibles, reducir el impacto de las incidencias sobre la organización, detectar las condiciones de la red organizativa de datos, detectar problemas de flujo y conectividad de datos por malos diseños de la red, entre otros.

Los resultados obtenidos al realizar las pruebas del Sistema muestran el impacto favorable sobre la organización, basado en la reducción de los tiempos de respuesta en la solución de las incidencias, en un 34,55%, el aumento en la productividad del personal del departamento de atención de usuarios y eficiencia en la gestión de activos.

Con este Trabajo Especial de Grado se deja ver la manera en que es posible integrar un conjunto de herramientas basadas en Software Libre, enfocadas en automatizar la gestión de solicitudes en tecnologías de información, permitiendo una adecuada gestión de incidencias e inventario de activos y dispositivos conectados a la red. Además, es novedoso, orientado al Web, seguro y robusto, gracias a que ofrece un diseño completamente modular, si la operación de un módulo falla el Sistema no deja de funcionar. Está pensado para ser escalable y fácil de adaptar, pese a ser una solución pensada para la empresa Ingedigit C.A., puede correr bajo cualquier ambiente, sin importar las dimensiones de la red, la cantidad de dispositivos conectados a ella y la dinámica de la organización.

INTRODUCCION

El avance en Tecnologías de Información ha traído como consecuencia el crecimiento exponencial de las redes de datos, aumentando considerablemente la cantidad de dispositivos de interconexión y de usuarios en las mismas, lo que ha originado que la tarea de mantenimiento y soporte a usuarios en las organizaciones sea cada vez más compleja y costosa, aún contando con el conocimiento y las herramientas apropiadas.

La mayoría de los organismos internacionales que se especializan en el tema de gestión de servicio, sugieren el uso de una aplicación automatizada para el proceso de registro, control, historial y estadísticas de las diferentes solicitudes de servicio, constituyendo ésta la manera más apropiada de llevar a cabo una buena Gestión en Tecnologías de Información, más aún, si la aplicación cuenta con el apoyo de una herramienta de inventario de hardware, software y activos de red.

La motivación para la realización de este Trabajo Especial de Grado, se fundamenta en brindar un Sistema basado en la integración de tres herramientas de Software Libre, para la empresa Ingedigit C.A, que permite cubrir las carencias en la Gestión en Tecnologías de Información y cuyo objetivo principal es proporcionar a los administradores de red y técnicos de soporte un conocimiento amplio al momento de atender cualquier solicitud de servicio.

En el capítulo uno se presenta una descripción del planteamiento del problema, donde se especifican: la justificación, objetivo general, objetivos específicos, metodología de desarrollo y alcance. A continuación, encontramos en el capítulo dos, el marco teórico, en el cual se encuentra basado este Trabajo, así como un estudio de factibilidad técnica que permitió seleccionar las herramientas mas apropiadas para la integración.

Dentro del capítulo tres se presenta la implementación que da solución a la problemática planteada, la descripción de los ambientes y pruebas realizadas se encuentran reflejadas en el capítulo cuatro. Todas las pruebas realizadas nos permiten concluir la efectividad y ventajas que ofrece el Sistema desarrollado, las cuales son detalladas en el capítulo cinco.

CAPÍTULO 1 EL PROBLEMA

1.1 Antecedentes

La empresa Ingedigit C.A, es una empresa encargada de suministrar soluciones integradas y servicios especializados, en las diferentes áreas de las Tecnologías de la Información y Telecomunicaciones.

La Empresa Ingedigit C.A., no contaba con un Sistema apropiado para la Gestión de Servicio dirigido a los usuarios, que permitiera llevar a cabo de manera eficiente, eficaz y efectivo, el proceso de registro, control, historial y estadísticas de las diferentes solicitudes de servicio que se generan diariamente en la Organización y que ofreciera la posibilidad de visualizar la información asociada a los componentes activos de red, hardware y software. Contar con toda esta información facilita y automatiza la resolución de incidencias, ya que el personal de soporte a usuario posee mayor conocimiento de la plataforma tecnológica existente al momento de solucionar los inconvenientes.

Parte del proceso de gestión era realizado diariamente de forma básica, mediante el uso de una aplicación propietaria llamada INFIRM, la cual únicamente proporciona el registro de las incidencias. El tipo de hardware, software y activos de red que posee la organización no se conocía en su totalidad, y la información que existía no estaba actualizada. INFIRM no permite llevar adecuadamente la gestión de servicio a usuarios, en virtud de que carece de los elementos fundamentales para ese propósito, tales como: reportes e indicadores sobre las incidencias, base de conocimiento para el registro y consulta de las soluciones a las incidencias, manejo de distintos perfiles de usuario, mecanismo para la apertura y notificación de incidencias vía correo electrónico, mecanismo de escalamiento automático y registro de hardware, software y componentes activos de red.

Cuando se presentaba una incidencia en la Organización la misma era registrada en el Sistema INFIRM de forma manual, pero se desconocían aspectos básicos para ofrecer solución a la misma, de la forma más expedita posible, tales como: dirección IP del dispositivo involucrado en la incidencia, subred a la que pertenece, paquetes de software que posee instalados y especificaciones de hardware básicas. Al momento de evaluar la solución más adecuada para la incidencia presentada, el personal de atención a usuarios no contaba con registros que permitieran consultar si la incidencia ha sido solventada en el pasado, por lo que, comenzaba la búsqueda de soluciones desde cero. Este factor es relevante, debido a que incrementa los tiempos de respuesta en resolver una incidencia, lo cual puede llevar a la misma a cambiar su nivel de severidad, convirtiéndose en un requerimiento crítico que afecta la productividad de la Organización.

El hecho de que la herramienta para la gestión de incidencias, manejada por la Organización sea propietaria, hace que su código fuente no sea verificable y extensible de acuerdo a las distintas necesidades que van surgiendo, puesto que

existe dependencia directa con los desarrolladores de la aplicación, quiénes son los únicos que tienen la posibilidad de agregar nuevas funcionalidades y llevar a cabo la corrección y depuración del código fuente. Para la Organización es muy importante minimizar los costos derivados del pago de licencias de software, por lo cual es un requerimiento, que todo Sistema que se implemente nuevo en la misma, sea basado en estándares abiertos.

1.2 Planteamiento del Problema

Actualmente la empresa Ingedigit C,A no cuenta con ninguna herramienta que permita llevar de forma adecuada la Gestión de Incidencias y la Gestión de Inventario dentro del Departamento de Atención a Usuarios, todas las solicitudes son atendidas vía telefónica por cualquier técnico o registradas en el Sistema INFIRM y para dar solución a las mismas éste debe trasladarse al lugar de la incidencia, evaluar las causas y plantear una solución. El nivel de conocimiento de los técnicos no se encuentra distribuido en diferentes niveles de soporte, es por esto, que en repetidas oportunidades el desconocimiento de algún técnico en el inconveniente evaluado, retrasa el tiempo en brindar respuesta a los usuarios, esto sin considerar si la incidencia fue presentada anteriormente y resulta por otro técnico de forma exitosa.

Es importante señalar que no existe un inventario de estaciones de trabajo y de dispositivos activos de red, por lo cual, al momento del técnico solucionar cualquier incidencia de red debe recolectar manualmente toda la información que involucre la misma: switch al que esta conectado el usuario, puertos activos, tipo de estación de trabajo entre otros. Muchos de los switches que se encuentran dentro de las instalaciones se encargan de prestar servicios bancarios, es por ello, de vital importancia contar con una herramienta para la administración de los dispositivos de red por parte del administrador, la cual brinde la información necesaria al momento de tratar una determinada incidencia.

En la Organización se hizo uso de la herramienta LAN MapShot (ver anexo H), para obtener información de los activos de red, los resultados obtenidos no fueron satisfactorios debido a que no se detectaron todos los dispositivos activos, solo la mitad de ellos, es por ello, la importancia de contar con una herramienta que permita gestionar la información de inventario con datos completos.

Las herramientas de software que puede utilizar cualquier usuario no se encuentran bajo ningún tipo de control, lo cual presenta una desventaja relevante, ya que la Organización queda totalmente expuesta a cualquier software dañino encontrado en la web, esto se ve reflejado en el número de casos reportados correspondientes a incidencias relacionadas con virus, troyanos y spyware.

La Organización esta conformada por cinco empresas, distribuidas en tres edificios, donde es necesario llevar un control sobre cada tipo de recurso existente dentro de la misma, con la finalidad de mantener el funcionamiento correcto de cada uno de los servicios prestados, de estaciones de trabajo y switches. Un Sistema de gestión automatizado brindará mayor información a los técnicos y

administradores al solucionar cualquier incidencia, gracias a que cuenta con información del hardware, software y de red del dispositivo involucrado en la incidencia. El Sistema propuesto permite distribuir a los técnicos en diferentes niveles de soporte, según el conocimiento de los mismos y escalar una solicitud si ésta no ha sido resuelta a un nivel de soporte superior, contado con una base de conocimientos que almacena las soluciones a los casos anteriormente reportados.

1.3 Justificación

Para la empresa Ingedigit C.A. el funcionamiento interno de la gestión de incidencias e inventario de hardware software y activos de red es de suma importancia, ya que permite mantener un control de los componentes, dispositivos y del desempeño del grupo soporte usuario, es por ello la necesidad de contar con una herramienta integrada que brinde un registro de información al día, consolidada, veraz e inmediata que facilite y automatice la gestión de servicio dirigido a los usuarios, que cuente con los elementos fundamentales como son: reportes e indicadores, base de conocimiento para el registro y consulta de las soluciones de las incidencias, que permita el escalamiento automático de las incidencias o solicitudes a través de los distintos departamentos y que contemple el manejo de prioridades. Adicionalmente, es de vital importancia, proveer un mecanismo para el registro y notificación de incidencias vía correo electrónico, lo cual es una ventaja notoria para la Organización debido a que el correo representa el medio de comunicación mas utilizado por los usuarios.

Al contar con información como: dirección IP del dispositivo involucrado en la incidencia, subred a la que pertenece, paquetes de software que posee instalados y especificaciones de hardware básicas al momento de atender la incidencia, el personal de atención a usuario, puede en muchos casos proporcionar atención inmediata a través de administración remota a los equipos para poder así, solucionar los conflictos sin la necesidad del traslado al lugar de la incidencia.

Además, al contar con esta información y de ser necesario el traslado del personal de soporte a usuario al lugar de la incidencia, éste ya tendría conocimiento de cuales causan la originaron, el estado actual de la incidencia y de cuál sería la forma correcta de implementar una solución, sin la necesidad de solicitar al usuario ningún tipo de información. Esto presenta una ventaja considerable debido a que los usuarios de la Organización desconocen los motivos que producen la incidencia que reportan.

La organización desea tener una visión detallada de la red, sus componentes e interacción entre ellos, para poder así precisar de forma expedita dónde se encuentran las fallas y cuáles son las causas que las originan, reduciendo considerablemente los costos en tiempo y recursos humanos dedicados al soporte y aumentando la satisfacción y el nivel de productividad de los usuarios de la empresa.

Es muy importante minimizar los costos de licencias por software, por tal motivo se propone una solución que además de adaptarse a los requerimientos, sea basada

en Software Libre, haciendo uso de estándares abiertos, lo que permite mayores niveles de seguridad e interoperatividad y facilita la adición de nuevas funcionalidades, la corrección y depuración del código fuente.

1.4 Objetivo General

Implementar un Sistema automatizado para la Gestión de Solicitudes en Tecnologías de Información, basado en la integración de tres herramientas de Software Libre, a nivel de interfaz, para garantizar la gestión y toma de decisiones eficiente del Departamento de atención a usuarios en la empresa Ingedigit C.A.

1.5 Objetivos Específicos

1. Analizar e identificar las herramientas apropiadas para el desarrollo del proyecto (Sistema integrado de Gestión de Incidencias y Sistemas de Inventario).
2. Integrar las herramientas seleccionadas en un Sistema Web amigable al usuario final donde se garantice la seguridad de los datos así como su integridad.
3. Implementar un módulo de software que permita al Sistema manejar la escalabilidad en cuanto a Gestión de Incidencias.
4. Implementar un módulo de software que permita al Sistema llevar control sobre los cambios ocurridos dentro del inventario.

1.6 Metodología de desarrollo

En este apartado se describe la metodología de desarrollo que se empleó en la integración de las herramientas propuestas.

En este sentido se presenta una visión de la metodología Rational Unified Process (RUP) y su enfoque en dos dimensiones.

Entre las mejores prácticas de desarrollo del software, que se implementaron para este proyecto, se encuentran [13]:

Desarrollo iterativo: permite una comprensión creciente del problema a través de refinamientos sucesivos para llegar a una solución efectiva.

Administración de requisitos: provee un enfoque sistemático para hallar, documentar, organizar y monitorear los requerimientos cambiantes de un Sistema.

Uso de arquitectura basada en componentes: provee un enfoque sistemático para definir una arquitectura usando componentes nuevos y preexistentes

Control de cambios: describe cómo controlar, rastrear y monitorear los cambios para permitir un desarrollo iterativo exitoso.

Modelado visual del software: permite capturar la estructura y comportamiento de arquitecturas y componentes, ver cómo los elementos se desarrollan entre sí, mantener consistencia entre diseño e implementación y promover una comunicación precisa.

Verificación de la calidad del software: durante todo el desarrollo estructura actividades para verificar la calidad del software antes de su puesta en producción.

1.7 Alcance

La solución propuesta para satisfacer los requerimientos de la empresa Ingedigit C.A tiene los siguientes alcances:

Integración a nivel de interfaz gráfica en una misma aplicación, para la gestión de incidencias e inventario.

Esta integración permitirá la autenticación de los usuarios una sola vez al Sistema, con visión según el tipo de usuario de los componentes ofrecidos por los tres Sistemas de licencia libre, sin la necesidad de acceder a ellos de forma separada, adicionalmente a las características y ventajas brindadas por los Sistemas integrados se implementará un módulo al Sistema Service Desk: Request Tracker, el cual se encargará de analizar diariamente las incidencias reportadas y de realizar el escalamiento automático de las mismas, cuando sus niveles de severidad se vean afectados por el tiempo que llevan sin resolverse.

Se manejaran tres escalas o niveles en prioridades de escalamiento: soporte nivel 1, soporte nivel 2 y soporte nivel 3 y cuatro niveles de severidad de incidencias: baja, media, alta y crítica.

Además se implementará un módulo a la herramienta de inventario OCS-Inventory para proporcionar y notificar a los técnicos y administradores de la organización los dispositivos que han cambiado su configuración de software y/o hardware, detectando de forma sencilla el uso ilícito de programas, saturaciones de dispositivos por instalación de software innecesario y hurto de componentes.

CAPÍTULO 2 MARCO TEÓRICO

2.1 Gestión de Incidencias

En este capítulo se presenta una descripción detallada de la Gestión de Incidencias, incluyendo definición, objetivos, beneficios, dificultades, así como las herramientas adecuadas para el control del proceso.

2.1.1. Definiciones

Incidencia: según la Biblioteca de Infraestructura de Tecnologías de Información [1], se define como cualquier alteración en los servicios de tecnologías de información.

Gestión de Incidencias: se define como el proceso que consiste en resolver cualquier evento que cause una interrupción en un servicio en Tecnologías de Información, de la forma rápida y eficaz [1].

La Gestión de Incidencias no sólo determina y analiza las causas de una incidencia, sino que además evalúa las mejores condiciones para restaurar el servicio afectado.

2.1.2. Objetivos de la Gestión de Incidencias

Los objetivos principales de la Gestión de Incidencias son [1]:

- Detectar cualquier alteración en los servicios en Tecnologías de Información.
- Registrar y clasificar éstas alteraciones.
- Asignar los recursos disponibles para restaurar el servicio afectado.

2.1.3. Beneficios de la Gestión de Incidencias

Los principales beneficios de una correcta Gestión de Incidencias incluyen [1]:

- Mejorar la productividad y satisfacción de los usuarios.
- Mayor control de los procesos y monitorización de los servicios.
- Optimización en el uso de los recursos disponibles.
- Reducción del impacto de las incidencias sobre la organización.
- Control y seguimiento del trabajo realizado.

2.1.4. Aspectos que abarca la Gestión de Incidencias

Los principales aspectos de una correcta Gestión de Incidencias incluyen [1]:

Registro de la incidencia, es realizado por el usuario que hace la solicitud o por el personal de atención a usuarios, donde se debe reflejar la descripción, naturaleza y equipos involucrados.

Clasificación de la incidencia, se realiza por el grupo de atención a usuarios, donde se determina la severidad de la incidencia de acuerdo a sus características.

Asignación del trabajo a realizar al grupo de atención a usuarios.

Investigación de la causa de la incidencia y su respectiva comparación con otras pasadas.

Documentación de la solución implementada, anexar archivos con información relacionada y cerrar la incidencia.

Comunicación automática al usuario sobre el estado de su solicitud a través del correo electrónico o un portal donde el usuario tiene acceso.

Elaboración de informes e indicadores de gestión que permitan precisar cómo se lleva a cabo la Gestión de Incidencias.

2.1.5. Dificultades para implementar la Gestión de Incidencias

Las principales dificultades a la hora de implementar la Gestión de Incidencias se resumen en:

- No se siguen los procedimientos previstos.
- Se resuelven las incidencias sin registrar su solución.
- No existe un mecanismo que permita el escalamiento de las incidencias a través del tiempo y tomando en cuenta su severidad.
- No están bien definidos los niveles de calidad de servicio ni los productos soportados. Lo que puede provocar que se procesen peticiones que no se incluían en los servicios previamente acordados.
- La ausencia de una herramienta completa y automatizada que permita facilitar el trabajo de atención en la gestión de incidencias.

2.1.6. Herramientas para la Gestión de Incidencias

Para llevar a cabo la Gestión de Incidencias existen herramientas conocidas con el nombre de Service Desk, cuyo objetivo es brindar apoyo a los departamentos relacionados con Tecnologías de Información, para atender las diferentes solicitudes de servicio que puedan presentarse, proporcionando al usuario una forma sencilla de reportar sus solicitudes, y a los técnicos una interfaz de comunicación con los usuarios [14].

En general, si esta labor diariamente no se sistematiza, se depende en gran medida de la capacidad de cada técnico y no se reutiliza todo el conocimiento, producto de la resolución de incidencias pasadas, es por ello, la importancia de una

herramienta apropiada que le permita a los técnicos dar solución de forma inmediata a los problemas presentados, haciendo uso de una base de conocimientos.

El uso de una herramienta de Gestión de Incidencias tiene tres objetivos básicos:

- Minimizar los períodos donde se encuentran fuera de servicio los Sistemas.
- Registrar la información relevante de todas las incidencias (Base de conocimiento).
- Brindar respuesta al usuario de la forma eficiente y en cortos períodos de tiempo.[14]

2.1.6.1. Características importantes de una herramienta Service Desk

Todo Service Desk debe cumplir con ciertas características que permitan llevar una Gestión de Incidencias de forma adecuada dentro de la organización, entre las cuales encontramos [1]:

- Permitir a los usuarios reportar cualquier tipo de incidencias.
- Asignación automática de casos, basada en las reglas predefinidas, tipo de problema o tipo de usuario.
- Brindar apoyo directo o redirigido a usuarios según la severidad de los casos.
- Manejar escalabilidad de casos según la severidad de los mismos.
- Manejar una base de conocimientos para almacenar la información sobre las soluciones a incidencias pasadas.
- Manejar diferentes tipos de indicadores: tiempo de respuesta, tiempo que lleva una solicitud abierta, tiempo en brindar solución a la solicitud, porcentajes de casos cerrados frente a casos abiertos, nivel de conocimiento de los técnicos, número de casos atendidos por técnico, otros.
- Proporcionar reportes detallados de los casos, así como la naturaleza, causa y solución de los mismos.

2.1.6.2. Parámetros importantes dentro una herramienta Service Desk

Todo Service Desk debe cumplir con parámetros esenciales que permitan llevar una Gestión de Incidencias de forma adecuada dentro de la organización, entre los cuales encontramos [1]:

Estados de las incidencias: permite configurar los diferentes estados que pueden experimentar las incidencias, de forma de brindar dicha información al administrador y al grupo de técnicos. Entre los estados más importantes que debe mantener todo Service Desk encontramos:

Abierto: representa las nuevas incidencias registradas en el Sistema, que se encuentran sin asignar a un responsable.

Asignado: representa aquellas incidencias que poseen un responsable.

Cerrado: representa aquellas incidencias culminadas de forma exitosa o no.

Clasificación de las incidencias: permite clasificar las incidencias, de forma de brindar al usuario y al técnico una distinción entre las mismas. Entre las clasificaciones más importantes que debe mantener todo Service Desk encontramos:

Hardware: representa las incidencias causadas por fallas relacionadas con el hardware del equipo.

Software: representa las incidencias causadas por fallas relacionadas con el software del equipo

Severidad de las incidencias: permite asignar a cada incidencia un nivel de severidad, de forma de indicar al grupo de técnicos cuáles son las que deben ser atendidas con urgencia. Entre los niveles de severidad más importantes que debe mantener todo Service Desk encontramos:

Crítica: representa todas aquellas incidencias que requieren atención inmediata, el tiempo de respuesta para estos casos debe ser aproximadamente de una (1) hora.

Alta: representa todas aquellas incidencias que requieren atención dentro de un tiempo estimado de dos (2) horas.

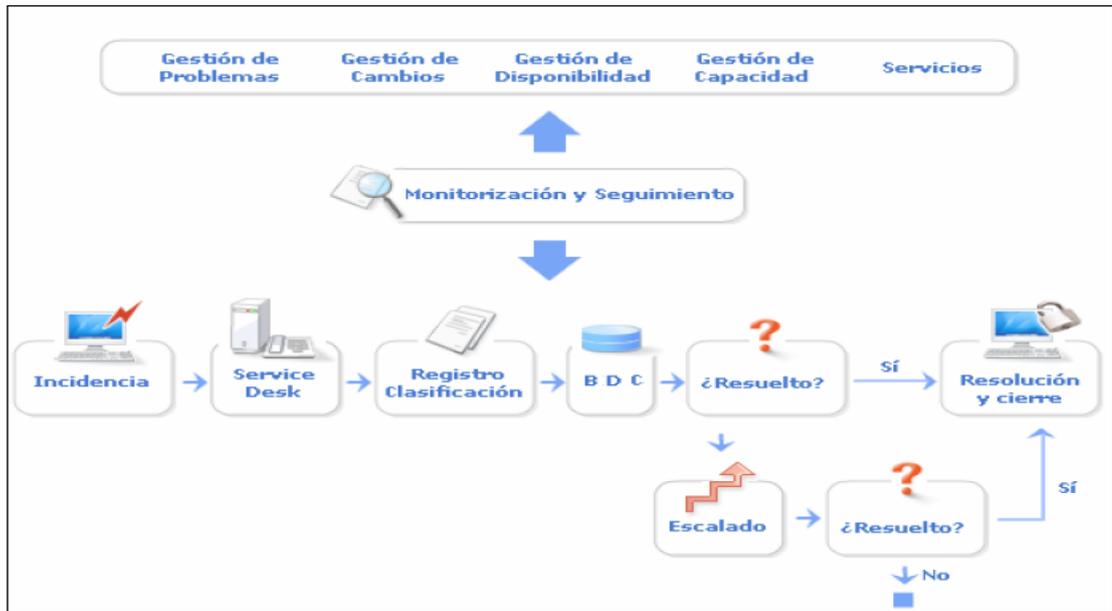
Intermedia: representa todas aquellas incidencias que requieren atención dentro de un tiempo estimado de cuatro (4) horas.

Baja: representa todas aquellas incidencias que requieren atención dentro de un tiempo estimado de ocho (8) horas.

Escalamiento: permite el escalamiento de las incidencias cuando su severidad cambia, bien sea, por el tiempo que lleva la incidencia sin ser atendida, por desconocimiento de una solución apropiada por parte del personal técnico, lo que supone que debe pasar a otro nivel, otros. El proceso de escalamiento se lleva a cabo entre los diferentes niveles, tomando en cuenta el conocimiento y la experiencia del personal técnico.

2.1.6.3. Flujo de trabajo de una herramienta Service Desk

Todo Service Desk debe seguir un flujo de trabajo determinado para permitir el funcionamiento correcto de la Gestión de Incidencias. En la figura 1 observamos el flujo de trabajo que debe implementar toda herramienta Service Desk.



* BDC= Base de Conocimiento

Figura 1: Flujo de una herramienta Service Desk

Fuente: Biblioteca de Infraestructura de Tecnologías de Información [1]. Año 1990.

2.1.6.3.1. Pasos del Flujo de Trabajo de una herramienta Service Desk

Comunicación de la incidencia: en éste paso debe llevarse a cabo la comunicación de la incidencia por parte del usuario al personal de soporte técnico, por medio de un operador telefónico o directamente por la aplicación. Este paso lo podemos observar en el gráfico cuando ocurre la incidencia.

Clasificación de la incidencia: en éste paso debe registrarse la incidencia en el Sistema y asignar la misma al grupo de técnicos, según su severidad y categoría.

Análisis y diagnóstico: en éste paso se consulta en la Base de Conocimiento (BDC) si existe una solución preestablecida en base a incidencias pasadas.

Se encuentra resuelta la incidencia: si se conoce el método de solución, se asignan los recursos necesarios, de lo contrario se debe escalar la incidencia a un nivel superior dentro de la organización.

Escalado: éste paso puede realizarse de forma funcional donde se lleva la incidencia a un nivel superior dentro del departamento de Tecnología de Información.

Resolución y cierre: en éste paso debe realizarse el registro de la solución a la incidencia en el Sistema y en la Base de conocimiento.

Monitorización y seguimiento: en éste paso debe generarse la emisión de informes, actualización de las bases de datos asociadas y monitorización de los niveles de servicio.

2.1.7 Metodología de desarrollo

Rational Unified Process

Rational Unified Process (RUP) es un proceso de desarrollo de software orientado a la implementación de un producto de calidad dentro de los tiempos y costos determinados. Se caracteriza por ser iterativo e incremental, estar centrado en la arquitectura, estar guiado por los casos de uso y dividir el proceso de desarrollo en fases (inicio, elaboración, construcción, transición), teniendo un subproducto del final en cada ciclo [15]. RUP proporciona un acercamiento disciplinado a la asignación de tareas y responsabilidades en una organización de desarrollo.

RUP integra las mejores prácticas de desarrollo de software a través de la definición de procesos, flujos de actividades, roles, documentos patrón y métricas.

Un aspecto característico de esta metodología, es su enfoque en dos dimensiones, cada una de las cuales describe aspectos específicos propios de RUP (ver Figura 2), estas dimensiones son [16]:

El eje horizontal representa el tiempo y muestra el aspecto dinámico del proceso. Se expresa en términos de ciclos, fases, iteraciones e hitos.

El eje vertical representa el aspecto estático del proceso. Se describe en términos de actividades, artefacto, trabajadores y workflows (disciplinas).

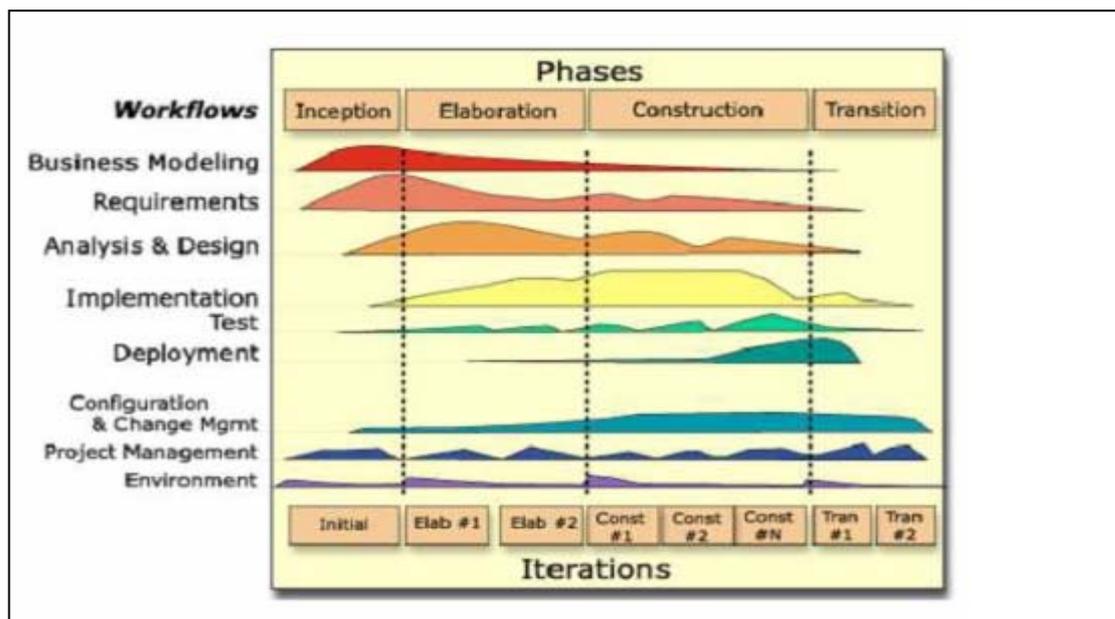


Figura 2: Modelo RUP.
Autor: P. Kruchten. Año 2005.

2.2 Gestión de Inventario de Hardware, Software y Activos de Red

En este capítulo se presenta una descripción detallada de la Gestión de Inventario de hardware, software y activos de red, que incluye definición, objetivos, beneficios, dificultades, así como las herramientas para el control del proceso.

El incremento en la complejidad de las redes y aplicaciones a causa de las nuevas demandas de los servicios en Tecnología de Información, ha cambiado sustancialmente la manera en que los Sistemas son gestionados. El enfoque se ha movido de una gestión orientada a los dispositivos a otra orientada al servicio.

Actualmente, pequeñas y grandes organizaciones necesitan una infraestructura tecnológica que soporte su negocio y que debe ser monitoreada e inventariada.

2.2.1 Definiciones

Inventario de plataforma tecnológica: proceso que permite conocer los recursos de tecnología de información de una organización [2].

La gestión de inventario tecnológico permite llevar un control sobre la plataforma que soporta las organizaciones de tecnologías, abarcando software, hardware y activos de red

Una buena gestión de inventario tecnológico proporciona los medios estadísticos sobre el flujo de información de la organización, permitiendo a los administradores de la red un conocimiento amplio y detallado de todos los recursos.

2.2.2 Objetivos de la Gestión de Inventarios: los objetivos principales de la Gestión de Inventario son [2]:

- Detectar las condiciones de la red organizativa.
- Detectar las herramientas dentro de la plataforma Tecnológica en la Organización.
- Conocer las aplicaciones utilizadas por cada usuario dentro de sus equipos de trabajo.
- Detectar problemas de flujo y conectividad de datos por malos diseños de la red.

2.2.3 Beneficios de la Gestión de Inventario: los principales beneficios de una correcta Gestión de Inventario incluyen [2]:

- Mejorar la productividad de la organización.
- Mayor control de los procesos y monitorización del servicio.
- Mayor control de plataforma tecnológica de la organización.
- Optimización de los recursos de red y equipos disponibles.
- Uso más eficiente de los recursos.
- Control centralizado de los diferentes servicios y equipos tecnológicos.

- Determinar la óptima secuencia de operaciones

2.2.4 Aspectos que abarca la Gestión de Inventario: entre los principales aspectos de una correcta Gestión de Inventario encontramos:

Descubrimiento de Red (Discovery): La gestión de red se hace cada vez más importante debido al crecimiento constante de las redes de computadoras. Una parte fundamental en la gestión de red, es sin lugar a dudas, el descubrimiento de la misma (*Discovery*), es decir, la topología subyacente de la red. Este conocimiento puede ser obtenido mediante diferentes métodos y puede ser usado desde diferentes perspectivas. Para el usuario la topología de una red debe resultar transparente.

El término topología de red es usado como el conjunto de nodos y los enlaces entre los mismos. Donde los nodos pueden ser dispositivos de red, hosts o cualquier componente activo en una red y los enlaces son las conexiones entre los mismos.

Una parte importante en el descubrimiento de red, es conocer todos los dispositivos que la conforman. Esto es una precondition absolutamente necesaria. Para lograr tener este conocimiento se explican en este apartado los distintos métodos y protocolos empleados para ese propósito.

Protocolo de descubrimiento Cisco (CDP, *Cisco Discovery Protocol*): El protocolo de descubrimiento Cisco es usado para obtener información de los dispositivos vecinos. [3]

CDP trabaja en la capa 2 del modelo de referencia de Interconexión de Sistemas Abiertos (OSI, *Open System Interconnection*).

Cada dispositivo configurado con CDP envía periódicamente mensajes a la dirección de multidifusión específica de Cisco (01:00:0C:CC:CC:CC). La data que se envía contiene información como la dirección de capa 3, capacidades y el nombre de la interfaz por la cual se envió el anuncio CDP.

Con esta información es posible iniciar el descubrimiento desde un dispositivo haciendo la lectura de la data CDP de su vecindario. Este proceso determina la topología de red. En un escenario donde todos los dispositivos soportan CDP, esto se realiza sin mayor dificultad.

La figura 3 muestra una red compuesta por dispositivos que soportan CDP.

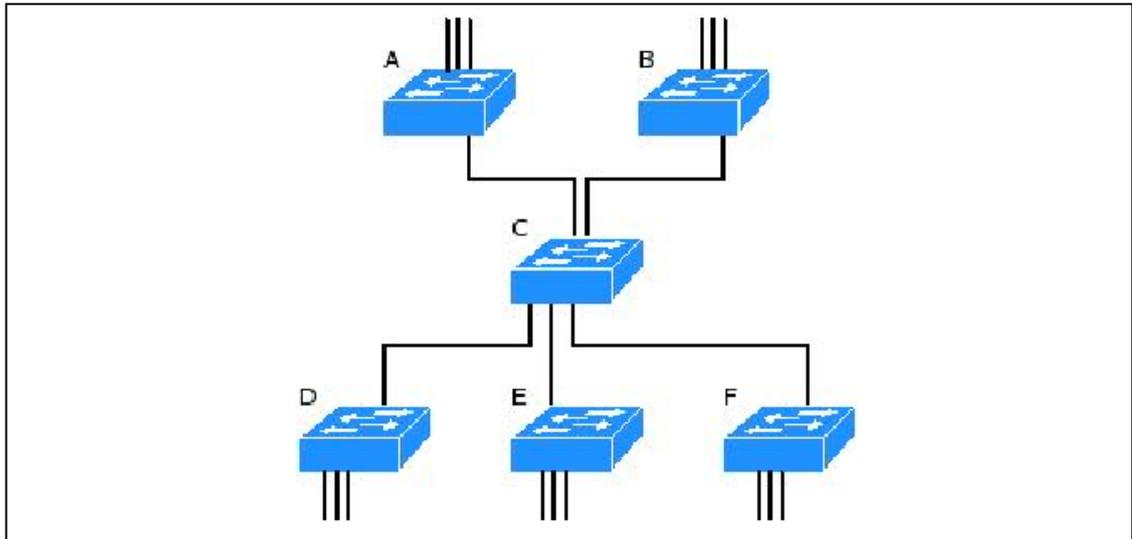


Figura 3: Ejemplo de una red con dispositivos que soportan CDP
Autor: Alexander Barthel. Año 2005.

Sin embargo existen dispositivos que no soportan este protocolo. Estos dispositivos pueden ser divididos en dos grupos. El primer grupo es aquel que tiene conocimiento de CDP y el segundo está formado por aquellos dispositivos que no conocen el protocolo. Los dispositivos que soportan CDP son capaces de enviar, recibir y almacenar data CDP. Mientras que los dispositivos que solo conocen la existencia de CDP no redireccionan los frames del protocolo. Los dispositivos que no tienen conocimiento por defecto redireccionan los frames al resto de los dispositivos. Si alguno de ellos soporta CDP, este recibirá y almacenará la data CDP, asumiendo que la información CDP pertenece al dispositivo que hizo la redirección. Esto causará una topología errónea [8].

La figura 4 muestra un escenario en el cual el dispositivo C no tiene conocimiento del protocolo.

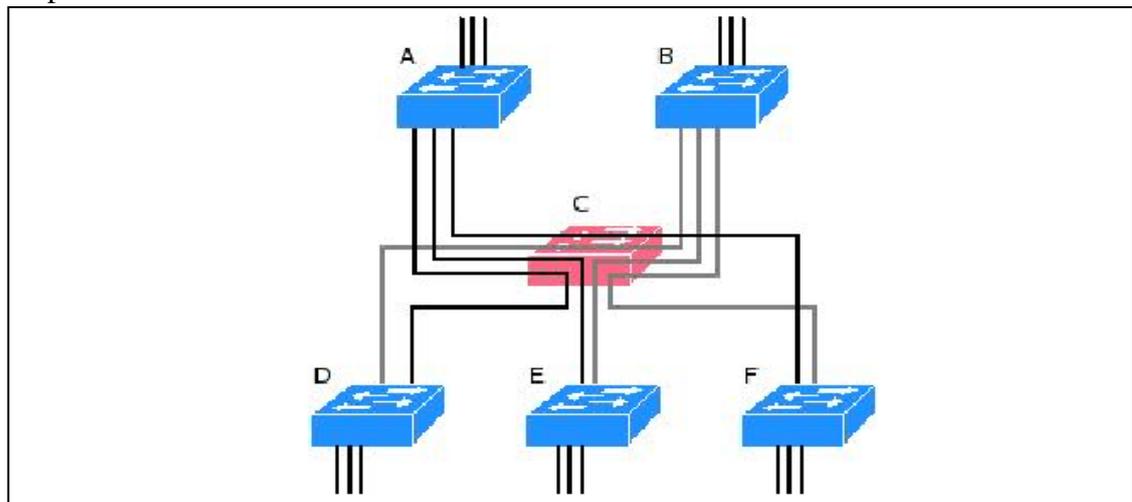


Figura 4: Ejemplo de una red donde el dispositivo “C” no soporta CDP
Autor: Alexander Barthel. Año 2005.

Los dispositivos que conocen CDP descartarían los frames CDP, este sería el comportamiento correcto. Sin embargo, el dispositivo C es una especie de frontera que separa los dispositivos que soportan CDP, en consecuencia C no es visto por el resto de los dispositivos, como se muestra en la figura 5.

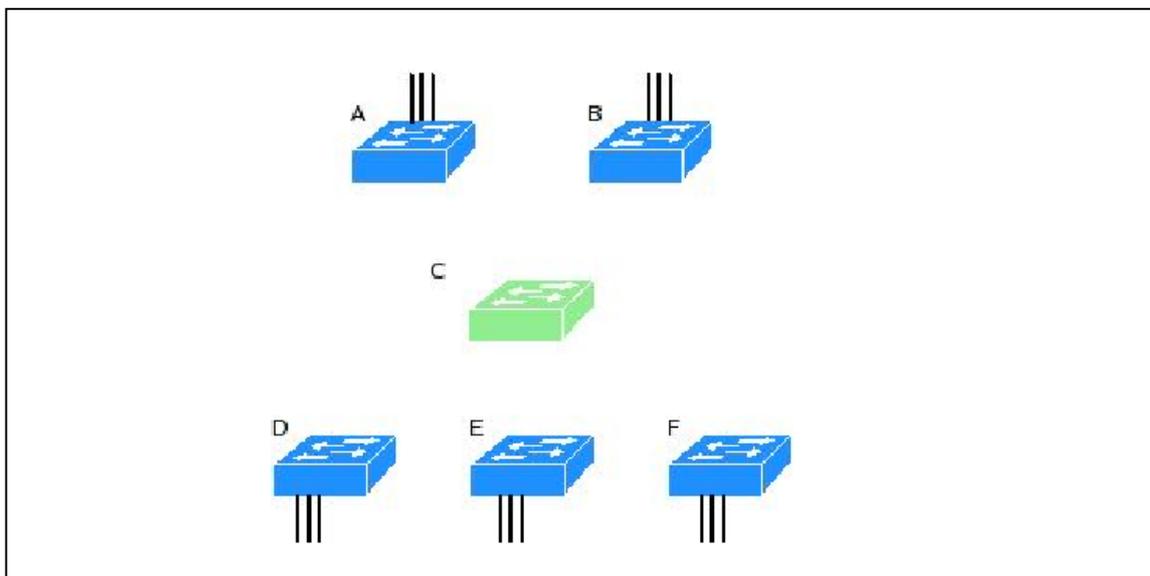


Figura 5: Ejemplo de una red donde el dispositivo “C” conoce la existencia del Protocolo CDP sin soportarlo.

Autor: Alexander Barthel. Año 2005.

Granularidad: La granularidad se define como el nivel de detalle con el que es realizado y representado un descubrimiento de red. Los niveles son diferenciados por la Organización Internacional de Estandarización (ISO, *International Organization for Standardization*) como capas de red. Estas capas son: capa-1, capa-2 o capa-3. Otra clasificación puede hacerse por regiones, de esta forma tenemos Redes de Área Local, Redes de Área Metropolitanas o Redes de Área Extensa. [8].

Cambios en la topología de red: Los cambios en la topología de las redes constituyen un verdadero desafío. Las redes no son estáticas, varían en el tiempo. Estos cambios pueden aparecer en todos los diferentes tipos de data. Por ejemplo, los nodos en una topología son agregados o eliminados. Esto se cumple también para los enlaces. Las representaciones y los procesos de recolección de datos deben ser diseñados para obedecer a estas limitaciones.

Una gestión adecuada debe permitir a los administradores visualizar los cambios ocurridos dentro de la topología de la red, con la finalidad de llevar un control adecuado de la misma, así como prevenir malos diseños que no contribuyan con el flujo de los datos.

Dependencia de los distintos fabricantes: Una red donde predominan componentes de un mismo fabricante resulta sencilla de inventariar. Sin embargo, la realidad es muy distinta, la mayoría de las redes son heterogéneas formadas por dispositivos de distintos fabricantes, en ellas la cooperación entre dispositivos para su gestión no está garantizada. Sin embargo, la experiencia muestra que hasta en las redes con dispositivos de la misma marca esa colaboración puede fallar. Es por ello la importancia de una gestión integrada basada en herramientas que permitan reconocer redes heterogéneas.

Descubrimiento de la topología de una red: La figura 5 ilustra el proceso de transferencia de datos de configuración y gestión desde ó hacia los dispositivos. Cada dispositivo de red se encuentra constituido por un agente, el cual posee los conocimientos de administración que son enviados al servidor de inventario.

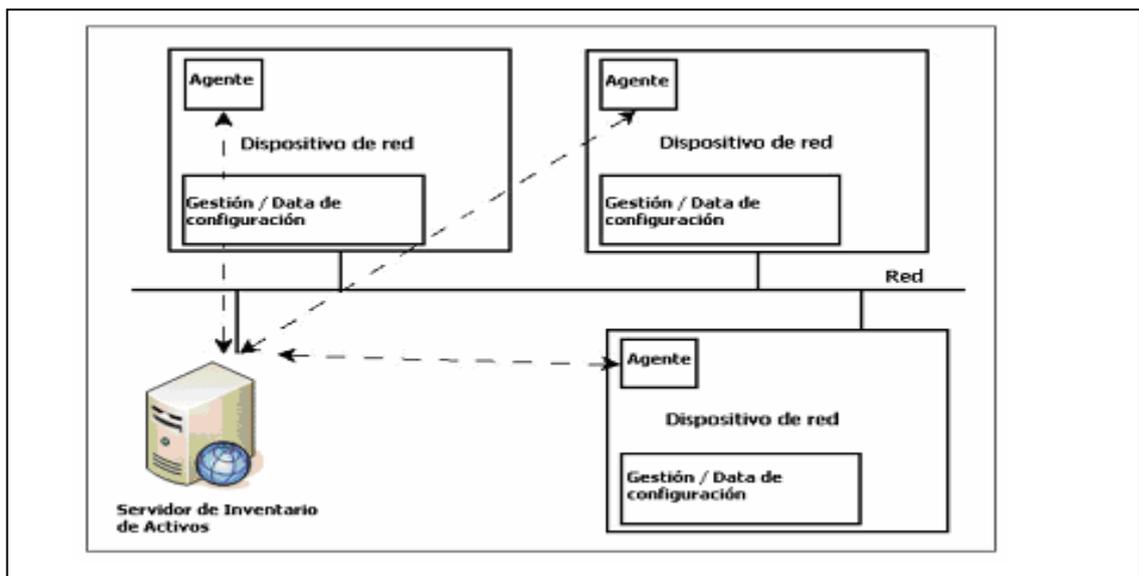


Figura 6: Arquitectura de gestión de red.
Modificado de [8].

Interfaz de línea de comandos: La interfaz de línea de comandos es una especie de consola implementada como parte del Sistema operativo en un dispositivo. Esta puede ser accedida a través de un puerto de consola que se encuentra en el dispositivo usando una sesión remota. Los puertos de consola son típicamente puertos seriales RS-232, los cuales pueden ser usados con un terminal. El hecho de usar un terminal conectado directamente al dispositivo de red tiene la desventaja de que se debe tener acceso físico al dispositivo.

Otra forma de usar la línea de comandos es vía una sesión remota, la cual es establecida a través de un puerto de comunicación de red. Para este propósito es necesario asignar una dirección IP (*Internet Protocol*) en la configuración del dispositivo.

Para comunicarse con cierto dispositivo, los protocolos de capa de aplicación como Telnet o Secure Console son usados para transmitir data a través del Protocolo de Control de Transmisión (TCP, *Transmission Control Protocol*).

La interfaz de línea de comandos depende del tipo de dispositivo y fabricante específico que la implementa. No existe un estándar común que especifique un conjunto de comandos o parámetros, ya que varían dependiendo de la versión del Sistema operativo aún en la misma clase de dispositivos.

Protocolo Simple de Administración de Red (SNMP, *Simple Network Management Protocol*): Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos de Internet utilizando un servicio no orientado a la conexión (UDP, *User Datagram Protocol*). SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento [4].

Las versiones de SNMP más utilizadas son dos: SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2). Ambas versiones tienen un número de características en común, pero SNMPv2 ofrece mejoras por medio de operaciones adicionales.

SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad, sin embargo no ha sido mayoritariamente aceptado en la industria.

Una red administrada a través de SNMP consiste de tres componentes claves [4]:

1. Dispositivos administrados
2. Agentes
3. Sistemas administradores de red.

Un dispositivo administrado: es un nodo de red que contiene un agente SNMP y reside en una red administrada. Estos recogen y almacenan información de administración, la cual es puesta a disposición de los Sistemas administradores usando SNMP [4]

Los dispositivos administrados, pueden ser routers, servidores de acceso, switches, bridges, hubs, computadores o impresoras. Los dispositivos administrados son también aquellos elementos que brindan información sobre su estado, como por ejemplo una central de alarma de incendio, un equipo de transmisión por fibra óptica.

Un agente: es un módulo de software de administración de red que reside en un dispositivo administrado. Un agente posee un conocimiento local de información de administración (memoria libre, número de paquetes IP recibidos, rutas, entre otros), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías [4].

Un Sistema administrador de red: ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados [4].

Comparación de los métodos de acceso

En la tabla 1 se muestra un cuadro comparativo entre los métodos de acceso línea de comandos y protocolo SNMP, se evalúan aspectos como protocolo de comunicación y aplicación soportado, autenticación, comandos y propósito.

Método de Acceso	Interfaz de línea de comando	SNMP
Protocolo de comunicación	TCP*/UDP	UDP*/TCP
Protocolo de aplicación	telnet/ssh	SNMP
Autenticación	Password	comunidad SNMP
Comandos	depende del dispositivo	SNMP
Tipos de dato	Implícitos	SNMP-MIBs
Propósito	Configuración	gestión y configuración

* Protocolo por defecto

Tabla 1: Comparación entre métodos de acceso línea de comandos y protocolo SNMP

Autor: S. Hernández y K. Rodríguez. Año 2008

Escaneo de subredes para la búsqueda de dispositivos: Sin conocer las direcciones de Capa-3 de los dispositivos que conforman una subred, no es posible establecer una comunicación mediante SNMP. Como se mencionó anteriormente es necesario conocer todos los dispositivos de una red. Una manera de encontrar cuáles de los dispositivos responden a SNMP es realizando un escaneo. Este método consiste en tratar de establecer una conexión SNMP con ciertas direcciones IP. Si se recibe una respuesta, la dirección IP verificada pertenece a un dispositivo que podría registrarse como disponible. De otra manera, si no se recibe ninguna respuesta se registra como no disponible.

Un inconveniente del método planteado se presenta, si las direcciones de los dispositivos son mezcladas aleatoriamente con direcciones de hosts. Esto origina un potencial riesgo de seguridad puesto que no puede determinarse si la dirección IP pertenece a un dispositivo de red o a un host. Cuando se envía una solicitud SNMP a una dirección, esta contiene la comunidad de lectura en texto plano (nota: SNMP versión 3 soporta mecanismo de encriptamiento). Si un host recibe ese mensaje SNMP fácilmente podría obtener la comunidad de lectura. Como la comunidad de lectura puede solamente ser empleada para la lectura de valores, este presenta un riesgo de seguridad bajo, asumiendo que la comunidad de lectura-escritura es distinta.

Los “timeouts” causados por los intentos SNMP a las direcciones que no están asignadas a ningún dispositivo, constituyen otro problema de este enfoque.

Escaneo de dispositivos por dirección de control de acceso al medio (MAC, *Media Access Control Address*): Este método intenta identificar dispositivos por su dirección MAC. La idea que está detrás, es que las direcciones MAC asignadas a los puertos de los dispositivos son consecutivas. No necesariamente todos los puertos tienen una dirección MAC distinta, si el dispositivo maneja una misma dirección para todos. Para este método se debe asumir que cada uno de los puertos tiene su propia dirección MAC y estas son asignadas consecutivamente.

Se debe satisfacer una condición: Para hacer posible la resolución de una dirección MAC a una dirección IP, debe existir una tabla del protocolo de resolución de direcciones (ARP, *Address Resolution Protocol*) donde buscar esa correspondencia. Una forma de obtener esa tabla sería leyendo la caché ARP de un dispositivo de Capa-3. El problema en este caso radica en que esta caché ARP debe estar actualizada y debe contener todas las direcciones necesarias. Para este propósito se podría utilizar un *ICMP echo request* usando una dirección IP de broadcast, determinando cuáles dispositivos responden a la solicitud.

Lista de dispositivos: Manteniendo una lista detallada de todos los dispositivos que conforman una red es un método simple. Sin embargo, el hecho de realizar este inventario de forma no automatizada tiene el inconveniente de que es muy costoso en tiempo y si no existe actualización de la data regularmente puede conducir a errores.

Comparación de los métodos para encontrar dispositivos: La mejor solución, que implica menos esfuerzo es CDP. Toda la información necesaria para conocer la topología se obtiene de los mismos dispositivos que soportan el protocolo.

El escaneo de un rango de direcciones IP se hace mediante un algoritmo simple. Si los *timeouts* y los mensajes SNMP enviados a los dispositivos están dentro de una cantidad razonable, este método es sencillo de implementar y trabaja en cualquier ambiente.

La búsqueda de dispositivos por dirección MAC reduce algunas de las fallas de escaneo del método anterior.

Una lista mantenida manualmente es una forma fácil de tener un registro de los dispositivos, sin embargo, podría estar desactualizada.

Un inventario software y hardware de la red automático permite conocer los recursos de Tecnologías de Información dentro de una organización, para brindar mayor control sobre los costos, adquisiciones, asistencia técnica y gestión de servicios, es por ello la importancia de contar con una base de datos la cual almacenará la información de hardware y software de los equipos de la red.

Entre la información más importante que debe manejar una herramienta para inventario de plataforma tecnológica encontramos:

- Direcciones IP's de los Equipos
- Direcciones MAC de los equipos
- Sistema Operativo
- Recursos de hardware (monitores, tarjetas entre otros)
- Software instalado dentro de los equipos.

2.2.5 Dificultades para implementar la Gestión de inventario

La mayor dificultad para realizar el proceso de Gestión de Inventario se presenta en el descubrimiento de la red, debido a que los fabricantes de hardware implementan sus propias soluciones para la administración de sus dispositivos. Actualmente no existe un estándar común para descubrir todos los dispositivos de una red. Se pensó que IEEE802.1AB sería un estándar común, pero éste no ha sido publicado hasta el momento en que se escribe este trabajo. Por ello surge la necesidad de una implementación general, verdaderamente efectiva que sea independiente del fabricante.

2.2.6 Herramientas para la Gestión de Inventario

El proceso de Gestión de Inventario de plataforma tecnológica, incluyendo activos de red dentro de una organización, requiere de herramientas que manejen los aspectos mencionados anteriormente: descubrimiento de red, protocolos involucrados, escaneo de subredes, topologías y granularidad [17].

Las herramientas podemos diferenciarlas en:

Automatizadas: permiten el reconocimiento automático de redes y dispositivos: routers, switches, hubs, hosts, entre otros, así como también, el software instalado en cada uno de los dispositivos escaneados. Entre éstas herramientas encontramos: Netdisco y Nedi, las cuales analizaremos en detalle en el próximo capítulo.

Manuales: permiten la gestión de los datos en base a cargas manuales al Sistema.

2.3 Estudio de factibilidad para la implementación de una herramienta automatizada de gestión.

Este capítulo describe una investigación realizada con el fin de precisar la factibilidad técnica de implementar un Sistema automatizado y completo para la gestión de solicitudes de Servicios en Tecnologías de Información, basado en la integración de las herramientas más apropiadas.

2.3.1 Factibilidad técnica de una herramienta Service Desk

Para el análisis de factibilidad en una herramienta Service Desk se evaluaron los siguientes elementos:

- Base de conocimiento.
- Manejo de prioridades y severidad de los casos.
- Escalamiento de casos.
- Reportes de gestión.
- Inventario automático.
- Usabilidad: según [5], se define como calidad del software que tiene múltiples componentes y que está asociado con:

- a) Facilidad de Aprendizaje
- b) Eficiencia en la ejecución
- c) Facilitar la Memorización
- d) Prevención y Tolerancia a los errores del usuario
- e) Satisfacción del Usuario.

Análisis de Soluciones Service Desk

La figura 2 muestra los perfiles de usuario requeridos para la una solución apropiada de Service Desk:

Perfil	Principales Funciones
Administrador	Control total sobre el Sistema
Técnico	Ejecuta la labor técnica y registra las soluciones en la base de conocimiento. Finaliza los casos.
Usuario	Crea nuevos casos y reporta su apreciación en cuanto a la eficiencia de los técnicos
Supervisor	Supervisa la reasignación de los tickets

Tabla 2: Perfiles de Usuarios
Autor: S. Hernández y K. Rodríguez. Año 2008

2.3.1.1 Análisis funcional y comparativo

El análisis funcional entre productos se realizó por medio de una revisión de software que comprendió los siguientes elementos:

Identificar los principales productos de software a estudiar, considerando los requerimientos de la organización.

Localizar productos en la plataforma de software abierto (Open Source).

Definir criterios de comparación y realizar análisis de los productos.

Obtener conclusiones y sugerencias de uso como consecuencia de la comparación realizada.

El análisis comparativo consistió en evaluar cada producto en términos de tres aspectos, de la forma siguiente:

Funcional: Consistió en comparar los productos desde un punto de vista funcional, buscando similitudes o diferencias en sus funciones básicas y algunas de nivel medio o avanzado. Se crearon tablas que reflejan las semejanzas o diferencias en las funciones de cada producto, pero en ningún momento estas tablas contienen una comparación completa, punto a punto, de todas las capacidades de los mismos, sino solamente una referencia para valorar sus características principales y crear un criterio claro de selección.

Compatibilidad: Consistió en comparar los productos en términos de la compatibilidad, especialmente en el formato de los archivos de reportes. Este análisis no es exhaustivo ni considera todas las capacidades de los diferentes formatos, sino sirve como referencia para identificar posibles incompatibilidades al trasladar un documento de una plataforma a otra.

Usabilidad: Se refiere a particularidades en el uso de las aplicaciones en una u otra plataforma. Los criterios usados para medir la usabilidad de los productos fueron:

a) Aprendizaje: Medir el tiempo en que un usuario novato ejecuta ciertas tareas (clasificarlas de acuerdo a las destrezas).

b) Eficiencia: Medir tiempo de ejecución de las tareas realizadas por expertos

c) Memorización: Medir el tiempo de ejecución de tareas típicas donde se dispone de usuarios casuales

d) Tolerancia y Prevención: Anticiparse a posibles escenarios que no conduzcan al éxito de la tarea y asistirlo para recuperarse de los errores

e) Satisfacción: Analizar la opinión de los usuarios después de utilizar el Sistema.

Para la medición de cada ítem se utilizó una escala tipo Likert de cinco puntos [9], donde uno (1) corresponde a “muy pobre”, dos (2) “pobre”, tres (3) “regular”, cuatro (4) “bueno” y cinco (5) corresponde a “muy bueno”. Se muestran los resultados en base a los criterios mencionados en este apartado (aprendizaje, eficiencia, dificultad de memorización, tolerancia, prevención y satisfacción).

Nota: La evaluación de las herramientas se hizo utilizando las últimas versiones disponibles y considerando que tuvieran un grado elevado de actividad de la comunidad de desarrollo de cada uno de las mismas.

2.3.1.2 Herramientas de software Analizadas

Precisar una solución de software libre que lograra satisfacer los requerimientos a la medida de la organización fue una tarea laboriosa. Entre los Service Desk analizados encontramos:

- GLPI
- Request Tracker
- OneOrZero

La tabla comparativa 3 muestra los aspectos funcionales con los que cumplen cada uno de los Service Desk estudiados:

Herramienta	Base de Conocimiento	Prioridades y Severidad	Escalamiento Automático	Reportes de Gestión
GLPI	Sí	No	No	Sí
Request Tracker	Sí	Sí	Sí	Sí
OneOrZero	Sí	Sí	No	Sí

Tabla 3: Aspectos funcionales de las herramientas Service Desk
Autor: S. Hernández y K. Rodríguez. Año 2008.

a) Aspectos de Usabilidad:

Las tablas comparativas 4,5 y 6 muestran los resultados bajo la escala de Likert, de un análisis comparativo de usabilidad en cada una de las herramientas Service Desk analizadas, se observan los resultados en base a los criterios de (aprendizaje, eficiencia, memorización, tolerancia, prevención y satisfacción).

Herramienta Service Desk GLPI:

Indicador	Nivel
Aprendizaje	1
Eficiencia	1
Memorización	1
Tolerancia y Prevención	1
Satisfacción	1

Tabla 4: Descripción de usabilidad en la herramienta GLPI
Autor: S. Hernández y K. Rodríguez. Año 2008

Herramienta Service Desk REQUEST TRACKER:

Indicador	Nivel
Aprendizaje	4
Eficiencia	5
Memorización	5
Tolerancia y Prevención	5
Satisfacción	4

Tabla 5: Descripción de usabilidad en la herramienta Request Tracker
Autor: S. Hernández y K. Rodríguez. Año 2008

Indicador	Nivel
Aprendizaje	4
Eficiencia	4
Memorización	4
Tolerancia y Prevención	4
Satisfacción	4

Tabla 6: Descripción de usabilidad en la herramienta OneOrZero
Autor: S. Hernández y K. Rodríguez. Año 2008

b) Aspectos Técnicos:

La tabla comparativa 7 ofrece un perfil técnico de cada una de las soluciones analizadas, con la finalidad de conocer las particularidades técnicas de las mismas al momento en que se necesite desempeñar labores de depuración al código.

Herramienta	Plataforma	Protocolo	Lenguaje fuente	Base de Datos	Sistema Operativo	Interfaz
GLPI	Libre	TCP/IP	PHP	MySQL	Linux/Unix	Web
Request Tracker	Libre	TCP/IP	Perl	Postgre	Linux/Unix	Web
OneOrZero	Libre	TCP/IP	PHP	MySQL	Linux/Unix	Web

Tabla 7: Descripción de las herramientas Service Desk analizadas
Autor: S. Hernández y K. Rodríguez. Año 2008

De las tablas comparativas se deduce que la herramienta más completa desde el punto de vista funcional es Request Tracker, la cual cumple con los puntajes más altos en usabilidad y cuenta con un manejador de Base de Datos poderoso y robusto como lo es PostgreSQL, y está diseñado usando el lenguaje de

programación Perl lo que le permite aprovechar la potencia del Sistema de operación donde se ejecuta.

2.3.1.3 Análisis de la arquitectura del Service Desk Request Tracker

Request Tracker es una herramienta que permite llevar el registro, control, historial y estadísticas de incidencias. Es orientada al web, está construida con el lenguaje de programación Perl y su backend está basado en PostgreSQL. La Interfaz web ha sido creada usando Mason, por lo que es fácil extender sus funcionalidades. Los reportes que genera pueden ser personalizados al igual que la interfaz gráfica. Todo esto hace que Request Tracker se adapte perfectamente a las necesidades de una Organización específica [6].

Esta herramienta puede ser empleada para varios propósitos: Registro de “Bugs” de software, Sistema de Gestión de Incidencia, Gestión de Proyectos, entre otros.

Cada incidencia es mostrada como una secuencia de transacciones, comenzando con el mensaje inicial de creación.

Las incidencias se asocian a colas, donde una cola determina el tipo de incidencia, su prioridad y quiénes son los encargados de atenderla.

El registro de incidencias en Request Tracker puede hacerse vía correo electrónico, interfaz web, o bien, línea de comandos en el caso de usuarios avanzados. Al momento de registrar la incidencia se debe indicar a cuál de las colas debe estar asociada. Las incidencias se conocen con el nombre de tickets. Los tickets son identificados por un número que lo identifica unívocamente en el Sistema.

Cada incidencia o ticket tiene una prioridad [6]. La prioridad es una forma de indicar la importancia de la incidencia. Cuando se crea una cola en el Sistema debe indicarse una prioridad inicial y una final. Cuando una incidencia alcanza la prioridad final entonces escala.

Las incidencias pueden tener un dueño, quien es el usuario responsable para resolverla. Solo se pueden asignar incidencias si no tienen dueño. En caso de que se necesite ser reasignada y no se es dueño de la misma, puede ser “robada” y de esta forma delegada a cualquiera de los usuarios del Sistema.

Una incidencia puede ser una tarea verdaderamente compleja y algunas veces puede ser necesario dividirla en tareas más pequeñas. Cuando esto sucede, la herramienta permite crear tickets para esas tareas más pequeñas y asociarlas con el ticket o incidencia original. Request Tracker provee una dependencia [6].

2.3.2 Factibilidad técnica para Inventario de plataforma Tecnológica

Para el análisis de factibilidad de la herramienta inventario de plataforma tecnológica se evaluaron los siguientes elementos:

- Reconocimiento de diferentes Sistemas operativos.
- Reconocimiento de toda clase de herramientas de software dentro de los equipos.
- Reconocimiento de hardware de diferentes fabricantes.
- Reconocimiento de direcciones IP's y direcciones MAC asociadas a los dispositivos.
- Reconocimiento de nombres de cuentas de usuarios.

2.3.2.1 Análisis funcional y comparativo

Estadísticas: Consistió en comparar las herramientas desde un punto de vista funcional, evaluando los elementos que debe manejar todo Sistema de inventario de plataforma. Se crearon tablas comparativas las cuales reflejan las ventajas sobre diversos componentes que poseen las herramientas analizadas.

2.3.2.2 Herramientas de software Analizadas

Para el manejo de inventario de la plataforma tecnológica se evaluaron las funcionalidades mencionadas anteriormente a las siguientes herramientas:

- INARED
- RDBMS
- OSAI
- CLAYOUS
- CITRIX
- EMC2
- OCSINVENTORY

Tabla comparativa de las herramientas analizadas:

La tabla comparativa 8 proporciona información sobre las herramientas evaluadas, en base a plataforma, tecnología, comunicación, lenguaje del código fuente, Sistema operativo soportado y país de origen.

HERRAMIENTA	Plataforma	Tecnología Principal	Comunicación	Lenguaje del Código Fuente Principal	Base de Datos	Sistema Operativo Servidor de Aplicación	Tipo Interface Administración	Sistemas Operativos Soportados de los Clientes Inventariados	País origen	COMENTARIOS
INARET	LIBRE	SOAP	TCP/IP	PHP/PERL/JAVA	MYSQL	Linux, Unix	WEB	Todos	VENEZUELA	DATA INVENTARIADA MUY COMPLETA. UTILIZA PHP PARA LA ADMINISTRACION, PERL PARA EL MAPEO DE REDES Y JAVA EN LOS AGENTES DE INVENTARIOS
RDBMS	LIBRE	.NET	NETBIOS	VISUAL BASIC	ACCESS	Windows 2000 Server, Windows 2003 Server y Linux	WINDOS GUI	Windows	MEXICO	CLIENTES WINDOWS REQUIEREN LIBRERIAS .NET
OSAI	LIBRE	PHP	TCP/IP	PHP	MYSQL	Linux, Unix	GUI	LINUX, UNIX, Windows 2000,XP,VISTA	HOLANDA	MUY COMPLETO PERO LIMITADO EN LOS SISTEMAS OPERATIVOS A INVENTARIAR
CLAYOUS	LIBRE	PHP	TCP/IP	PHP	MYSQL	Linux, Unix	GUI	Todos	USA	LIMITADO EN LA DATA QUE ES INVENTARIADA, SOLO INVENTARIA INFORMACION DE SISTEMA OPERATIVO
CITRIX	PROPIETARIA	JAVA	TCP/IP	JAVA Y BORLAND C	PROPIETARIA Y OPCION ORACLE Y MS SQL SERVER	Windows Server, Solaris, Unix, Linux	WINDOS GUI	Todos	USA	MUY COMPLETO PERO REQUIERE LICENCIA POR CLIENTE A INVENTARIAR
EMC2	PROPIETARIA	PROPIETARIA	PROTOCOLO PROPIETARIO	PROPIETARIA	PROPIETARIA Y OPCIONES VARIAS	Windows Server, Solaris, Mac Server, Unix, Linux	WINDOS GUI	Todos	USA	BUENA INTERCONEXION CON OTROS PAQUETES PROPIETARIOS PERO REQUIERE DE LICENCIA POR CLIENTE A INVENTARIAR
OCSInventory	LIBRE	HTTP	TCP/IP	PHP/PERL/JAVA	MYSQL	Linux, Unix	WEB	Todos	USA	CUMPLE LOS REQUERIMIENTOS

Tabla 8: Descripción de las herramientas de Inventario analizadas

Autor: S. Hernández y K. Rodríguez. Año 2008.

Se seleccionó el software OCS Inventory por cumplir con todos los requerimientos funcionales y por ser una herramienta completa para la gestión de inventario de plataforma tecnológica

2.3.2.3 Análisis arquitectura de inventario de OCS-Inventory.

OCS-Inventory es una herramienta diseñada para llevar a cabo el proceso de Gestión de Inventario de software y hardware. Esta implementado por completo en lenguaje PHP Hypertext Pre-processor (PHP), con base de datos MySQL.

Este Sistema utiliza un agente, que se encarga del inventario de los equipos cliente, y un servidor de administración, que centraliza los resultados de los inventarios, permitiendo visualizarlos así como también la creación de paquetes de despliegue [7].

Las comunicaciones entre los agentes y el servidor de administración se implementan por medio de los protocolos HTTP (Hypertext Transfer Protocol) y

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer). Todos los datos están en formato XML Zlib comprimido para reducir el tráfico de la red [7].

Lenguajes Soportados:

Portugués, Inglés, Francés, Alemán, Húngaro, Italiano, Polaco, Español, Ruso, Árabe

La gestión del servidor contiene cuatro componentes principales [7]:

El servidor de base de datos, que almacenan la información de los inventarios.

Servidor de Comunicación: se encargará de las comunicaciones HTTP entre servidor de base de datos y agentes.

Servidor de Despliegue: almacenará todos los paquetes de configuración de despliegue.

Administración de consola: permitirá a los administradores la consulta de la base de datos del servidor a través de un navegador.

En la siguiente figura se observa el diseño de la Arquitectura de OCS-Inventory, donde son resaltados todos los componentes principales de la misma y los protocolos de comunicación.

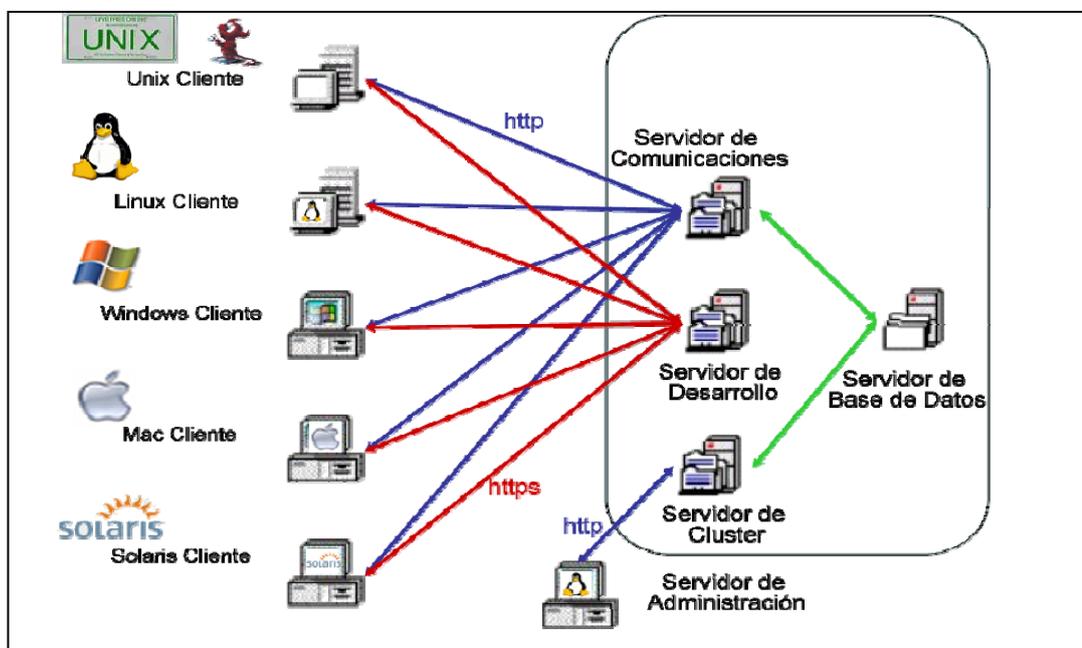


Figura 7: Arquitectura de la herramienta OCS-Inventory
Modificado de [7].

Proceso de Inventario: OCS-Inventory

El proceso de inventario realizado por el Sistema OCS-Inventory es automático donde todos los datos inventariados son almacenados en una base de datos centralizada, la cual recibe la data a través de los agentes de ejecución que residen en los dispositivos clientes [7].

Existen dentro del proceso de inventario, tres factores fundamentales:

Inventario: cada computador a inventariar requiere un agente que se ejecutará según la frecuencia que se especifique por el administrador. Este agente se encarga de recolectar toda la información asociada a los componentes de hardware y de software del equipo para enviarla al servidor haciendo uso del protocolo HTTP. La data de inventario es transmitida en formato XML y el inventario completo de un equipo no sobrepasa los 5 KB, evitando de esta forma sobrecarga en la red [7].

IP Discovery (Descubrimiento): el agente tiene la capacidad de realizar el procedimiento de “IP Discovery”, esto es, detectar todos los dispositivos de red activos que se encuentran en la misma subred del equipo donde se ejecuta. Esta información de descubrimiento es enviada al servidor haciendo uso también del protocolo HTTP [7].

Despliegue: el administrador puede crear sus propios scripts, archivos binarios, ejecutables, paquetes de instalación de software y actualizaciones de acuerdo con los requerimientos que se presenten y enviarlos a todos y cada uno de los equipos inventariados a través de la red haciendo uso del protocolo HTTPS [7].

Puertos	Tipo (serial, paralelo,...), nombre, descripción
Ranuras del Sistema	Nombre, descripción, designación (AGP1, PCI1, PCI2, ISA1,...)
Controladores	Fabricante, nombre, tipo (Floppy, IDE, SCSI, USB, PCMCIA, IEEE1394, Infrarojo...), tamaño en MB
Periféricos de almacenamiento	Fabricante, modelo, descripción, tipo (disco duro, CD-Rom, pendrive, cinta,...), tamaño en MB
Unidades lógicas / particiones	Identificador de la unidad lógica, tipo, Sistema de archivos (FAT,FAT32,NTFS,ext2/ext3, reiserFS,XFS...), tamaño en MB, espacio libre en MB
Dispositivos de sonido	Fabricante, nombre, descripción
Adaptadores de video	Nombre, chipset, memoria en MB, resolución
Monitores	Fabricante, descripción, tipo, número de serial
Módems	Nombre, modelo, descripción, tipo (interno, externo,...)
Adaptadores de red	Descripción, tipo (dial-up, ethernet, token ring, ATM, ...), velocidad en Mb/so Gb/s, dirección MAC, dirección IP, máscara de red, gateway, servidor DNS.
Impresoras	Nombre, controlador, puerto
Sistema operativo	Nombre, versión, compañía registrada, dueño, licencia
Software	nombre, descripción, versión
Registro del Sistema	Información sobre el registro (solo para Windows)

Tabla 9: Descripción de componentes inventarios a través de la herramienta OCS-Inventory

Autor: S. Hernández y K. Rodríguez. Año 2008

2.3.3 Factibilidad técnica para Inventario Activos de red

Para el análisis de factibilidad de la herramienta inventario de activos de red se evaluaron los siguientes elementos:

- Reconocimiento de redes heterogéneas.
- Reconocimiento de componentes de diferentes fabricantes.
- Reconocimiento en cambios de topologías de las redes.
- Manejo del protocolo SNMP (*Simple Network Management Protocol*)

2.3.3.1 Análisis funcional y comparativo

Para el análisis del módulo de inventario de activos de red se excluyó el aspecto asociado con la usabilidad, ya que este software no está diseñado para el usuario sin experticia y no resulta un elemento determinante en la elección de la solución. Lo más importante para este caso es que cumpla con la funcionalidad requerida que incluye elementos como: Soporte para el protocolo SNMP versión 1, 2 y 3, autodiscovery en red heterogénea de dispositivos de capa 2 y capa 3, detección de duplex mismatch y administración de dispositivos.

2.3.3.2 Herramientas de software Analizadas

Para el manejo de activos de red se evaluaron las funcionalidades mencionadas anteriormente a las siguientes herramientas:

- NETDISCO
- NEDI

La tabla comparativa 10 ofrece información detallada sobre las herramientas de inventario de red analizadas, con la finalidad de conocer las particularidades técnicas al momento en que se necesite desempeñar labores de depuración al código.

Herramienta	Soporte SNMP V1, V2 Y V3	Autodiscovery	Detección DUPLEX MISMATCH	Administración de dispositivos
Netdisco	Sí	Sí	Sí	Sí
Nedi	No	Sí	No	No

Tabla 10: Descripción de las herramientas de inventario de red analizadas

Autor: S. Hernández y K. Rodríguez. Año 2008.

Aspectos Técnicos: en la tabla 11 se observa un breve análisis de los componentes de los Sistemas de inventario de red analizados, donde se destaca la plataforma, tecnología, protocolo de comunicación, lenguaje del código fuente, base de datos manejada, Sistema operativo soportado e interfaz.

Herramienta	Plataforma	Tecnología	Protocolo	Lenguaje	Base de datos	Sistema Operativo	Interfaz
Netdisco	Libre	SNMP	TCP/IP	Perl	Postgre	Linux/Unix	Web
Nedi	Libre	Utilidades Unix	TCP/IP	C	MySQL	Linux/Unix	Cliente-Servidor

Tabla 11: Análisis de los componentes de las herramientas de inventario de red

analizadas. **Autor:** S. Hernández y K. Rodríguez. Año 2008

Se seleccionó luego de realizado este análisis la solución Netdisco para el manejo de inventario de activos de red, ya que además de ser una herramienta completa para la gestión de activos que cumple con los objetivos básicos de gestión proporciona los aspectos técnicos esenciales tales como soporte al protocolo SNMP v1,v2 y v3, autodiscovery para obtener información de la red y una base de datos robusta para el almacenamiento de los datos .

2.3.3.3 Análisis de la arquitectura de inventario de activos Netdisco

Netdisco es una aplicación de descubrimiento de red basada en información CDP. Está enteramente implementada en Perl. Las funciones de descubrimiento y gestión están controladas por un script de Perl. Es también posible operar esta aplicación a través de un front-end basado en web. Toda la data de topología recolectada es almacenada en una base de datos PostgreSQL. Esta base de datos es accedida a través del módulo netdisco.pm. La data SNMP se obtiene con ayuda de SNMP::Info. La visualización de la tipología es a través del componente GraphViz. La imagen de la red, y la información contenida en las páginas HTML son generadas por scripts que utilizan Mason para añadir data dinámicamente. Estas páginas son servidas por Apache [10].

En la figura 8 se puede observar la arquitectura de netdisco compuesta por una base de datos PostgreSQL, funciones de Ip discovery, y los requerimientos para soportar la herramienta como lo son servidor web apache y protocolo SNMP.

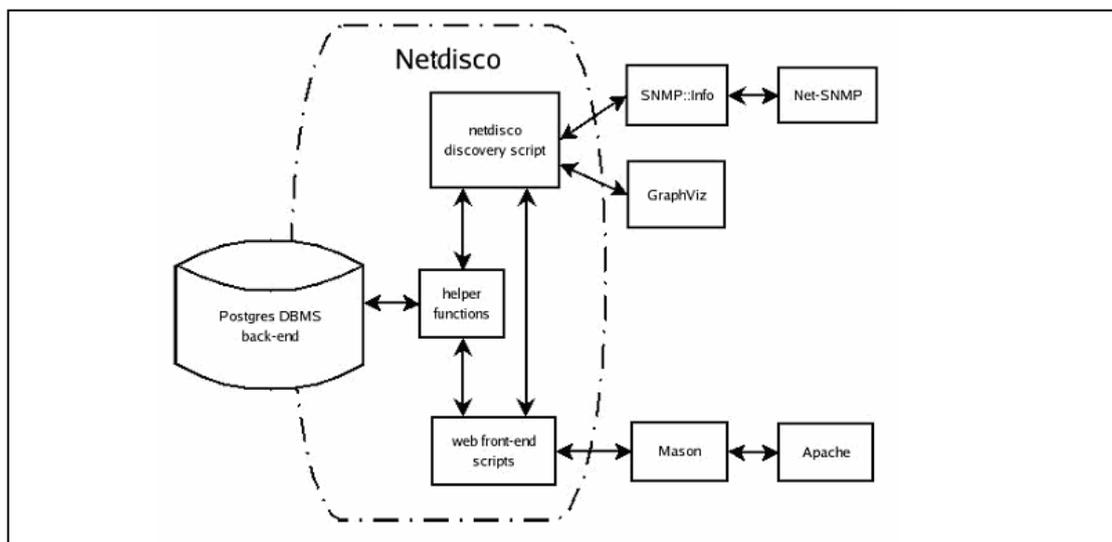


Figura 9: Arquitectura de la herramienta Netdisco

Autor: Alexander Barthel. Año 2005

Script de descubrimiento de red

El script en perl de netdisco es el componente central de la aplicación. Este contiene todas las funciones necesarias para operar. Por medio de operaciones de línea de comandos se puede tener una interacción completa con el aplicativo [10].

Las principales acciones son distintas operaciones de descubrimiento, como el descubrimiento de un simple dispositivo, un conjunto de dispositivos de la red o refrescar todos los dispositivos inventariados, coleccionar información ARP, llamada ARPnip; obtener las tablas de forwarding, llamadas MACsuck; creación de mapa; permitir depuración; control de usuarios; iniciar/detener el demonio de administración, el cual es usado por el front-end web.

Back-end de la base de datos

En la figura 10 se observa el diseño de la base de datos de la herramienta Netdisco a través de un diagrama Entidad-Relación. El back-end de Netdisco es construido con PostgreSQL. Los atributos indicados con “meta” son propiedades adicionales de una entidad, la cual es almacenada en las tablas correspondientes. Estos atributos no son necesarios para determinar la topología [18].

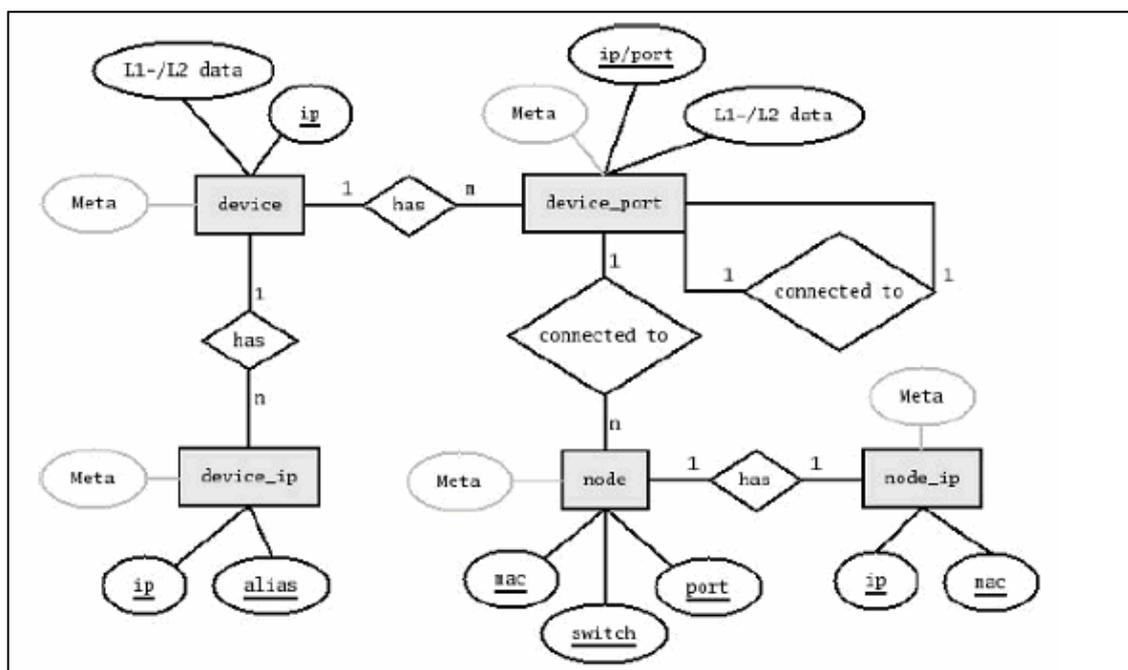


Figura 10: Diseño de la base de datos de Netdisco
Autor: Alexander Barthel. Año 2005.

A continuación se especifican las tablas y la data que almacena la base de datos de Netdisco.

Tabla	Información que mantiene
Device	Dispositivos específicos, parámetros SNMP usados para conectarse al dispositivo
Device_port	Data sobre los puertos de los dispositivos, incluyendo propiedades de capa 1 y 2 y dispositivos vecinos
Device_ip	Todos los alias IP de los dispositivos
Node	Dispositivos y puerto de los nodos que están conectados
Node_ip	Direcciones IP de los nodos, data ARP
Users	Usuarios de netdisco
Log	Información de registro
Device port_log	Logs del control de puertos que maneja la aplicación
admin.	Información del demonio de administración
Session	Información de sesión del front-end web
Oui	Asocia direcciones MAC a fabricantes

Tabla 12: Descripción de las tablas de la base de datos de Netdisco
Autor: Alexander Barthel. Año 2005.

CAPÍTULO 3 IMPLEMENTACIÓN DE LA SOLUCIÓN

En este capítulo se presenta de forma detallada la implementación de la solución para el Trabajo Especial de Grado, la cual consta de la integración de tres módulos de software.

3.1 Descripción del ambiente de desarrollo

Para la implementación de este trabajo especial de grado se acondicionó un ambiente de desarrollo con las siguientes herramientas:

- Sistema Operativo Linux Debian, versión 4, kernel 2.6.18-4-686
- Servicio de directorio LDAP, basado en Open LDAP.
- Servidor Web Apache versión 2
- Servidor de Base de Datos MySQL versión 5.0
- Lenguajes de Programación Perl.
- Framework de programación Mason.
- OCS-Inventory. Sistema de inventario de hardware y software.
- Request Traker. Sistema Service Desk.
- Netdisco. Sistema de inventario de activos de red.

3.2 Instalación y configuración de las herramientas de desarrollo

Para la implementación de la solución se instalaron en el ambiente de desarrollo las aplicaciones Netdisco, OCS-Inventory y Request Tracker.

A continuación se explica de forma detallada la instalación y configuración de cada una de estas herramientas de aplicación.

3.2.1 Instalación y configuración de OCS-Inventory:

Requisitos previos a la instalación: es necesario contar con la instalación previa de los siguientes requisitos de software. (Ver anexo A).

- Servidor de Base de Datos MySQL versión 5.0 con motor InnoDB activo, escuchando en el puerto 3306 con comunicación TCP/IP activada.
- Servidor Web Apache versión 2.0 o superior instalado, servidor de Comunicación y servidor de administración.
- Lenguaje de programación PHP versión 4.3.2 o superior, con soporte ZIP y GD.
- Lenguaje de programación Perl versión 5.6 o superior, instalado y configurado para el Servidor Apache.
- Módulo mod_perl versión 1.29 o superior instalado y configurado para el Servidor Apache de forma de usar el servidor de comunicación.
- Módulo Mod_php versión 4.3.2 o superior.
- Módulo Perl module XML::Simple versión 2.12 o superior.
- Módulo Perl module Compress::Zlib versión 1.33 o superior.

- Módulo Perl module DBI version 1.40 o superior.
- Módulo Perl module DBD::Mysql versión 2.9004 o superior.
- Módulo Perl module Apache::DBI versión 0.93 o superior.
- Módulo Perl module Net::IP versión 1.21 o superior.
- Módulo Perl module SOAP::Lite versión 0.66 o superior (no es obligatorio)
- Utilidad Make como GNU make.

Una vez instalados los módulos, librerías y paquetes de software necesarios para la instalación del servidor de inventario OCS-Inventory, se deben realizar los siguientes procedimientos:

1. Iniciar el servicio Web apache.
2. Descomprimir el archivo (tar.gz) que contiene comprimido el código del servidor, este paso generará una carpeta con el nombre OCSNG_LINUX_SERVER_1.01, donde se encuentran todos los archivos de instalación y configuración del servidor.
3. Ingresar a la carpeta OCSNG_LINUX_SERVER_1.01, para realizar la ejecución del script que contiene las sentencias de instalación llamado setup.sh. A continuación se configuran las rutas de instalación de los módulos de software previamente instalados, para indicar al servidor de OSC-Inventory donde buscare los archivos de configuración necesarios para dar inicio al Sistema.
4. Como último paso se inician los servicios apache y MySQL, se abre una sesión dentro del navegador Web con la siguiente dirección:

<http://127.0.0.1/ocsreports/install.php>

Aparecerá la pantalla inicial de OCS-Inventory, donde el usuario y password por defecto son “admin.”.

3.2.2 Instalación y configuración de Request Tracker:

Requisitos previos a la instalación: es necesario contar con la instalación previa de los siguientes requisitos de software (ver anexo B).

- Servidor de Base de Datos MySQL versión 4.1.0 o superior con motor InnoDB activo, escuchando en el puerto 3306 con comunicación TCP/IP activada.
- Servidor Web Apache versión 2.0 o superior instalado.

Una vez instalados los módulos de software necesarios para la instalación del servidor de Request Tracker, se deben realizar los siguientes procedimientos:

1. Instalar el servidor de aplicación Request Tracker.

2. Se debe editar el archivo de configuración RT_SiteConfig.pm, para configurar los siguientes parámetros:

- Nombre de la empresa.
- Nombre del usuario de la base de datos.
- Nombre del password de la base de datos.
- Nombre de la base de datos.
- Ruta de instalación de Request Tracker.
- Dirección IP del servidor.
- Dirección de correo del administrador.

3. Se debe editar el archivo de configuración de apache httpd.conf , para incluir el módulo `apache-modperl.conf` y reemplazar `DocumentRoot /var/www` por `DocumentRoot usr/share/request-tracker3.6/html/`

4. Se debe configurar el servidor de base de datos MySQL con el usuario `rtbd` con todos los privilegios y el password que se desee.

3.2.3 Instalación y configuración de Netdisco:

Para la instalación y configuración de la herramienta de activos Netdisco, se debe ejecutar el script `install.sh` desde la consola del administrador del sistema, éste script se encarga de instalar y configurar la herramienta y la base de datos necesaria para la ejecución de la misma, éste archivo lo encontramos en el anexo C. Luego de ejecutar el script, la herramienta estará instalada en el Sistema y se accede a través de la ruta `http://localhost/netdisco`.

3.3 Solución para el módulo de autenticación

Para dar solución a la integración de los Sistemas, el módulo de autenticación desarrollado permite al usuario autenticarse una sola vez al Sistema de gestión para tener acceso a todos los componentes del mismo. Este módulo cuenta con la integración a nivel de datos, a través del protocolo de acceso a directorio ligero (LDAP, *Lightweight Directory Access Protocol*), el cual almacena los datos de usuario login, password y rol de forma ordenada y centralizada [11].

El objetivo principal de este desarrollo se fundamenta en la definición de inicio de sesión única (SSO, *Single Sign-On*) [12].

En la siguiente figura podemos observar el diseño de arquitectura plantado para solucionar los requerimientos de autenticación por parte de los usuarios para acceder al Sistema integrado de gestión.

El primer paso se ve reflejado al momento que un usuario desee acceder al Sistema integrado, éste solicitará al usuario los datos de login, password y rol. Una vez introducidos estos datos, el Sistema evalúa la veracidad de los mismos en

el servicio de directorios LDAP. De ser correctos los datos introducidos se permitirá el acceso al usuario al Sistema de lo contrario de niega dicho acceso.

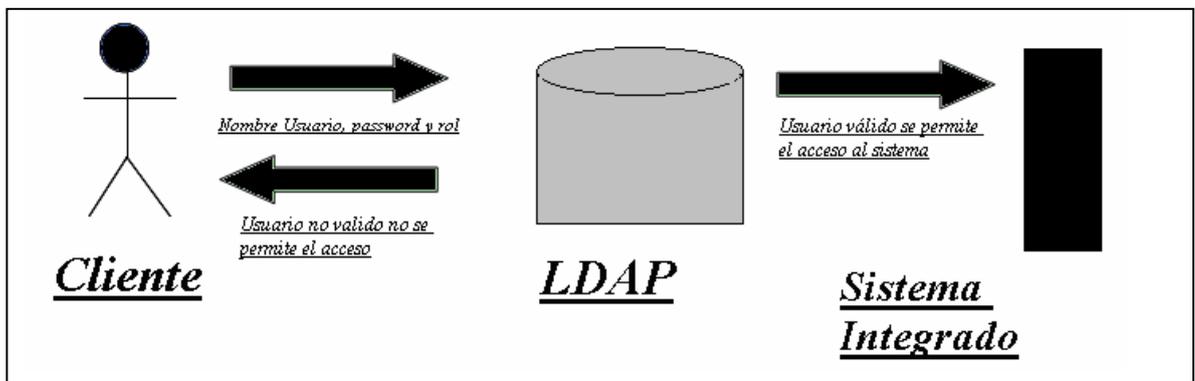


Figura 11: Proceso de autenticación al Sistema integrado.

Autor: S. Hernández y K. Rodríguez. Año 2008

Autenticación usando LDAP

Para la implementación del módulo Ldap se utilizaron los siguientes niveles:

1. **Simple Autenticación Usuario/Contraseña:** Esta es la estructura sobre el uso del almacenamiento de la clave en un algoritmo de hash, que básicamente está compuesto por una función no biyectiva, la cual hace que este se encuentre publicado, más no está a la luz pública de todos para ser usado. El problema sobre su almacenamiento y publicación, es que se debe definir un correcto criterio de uso, con respecto al algoritmo usado ya que debe ser seleccionado uno que no sea fácil de atacar.

2. **Usando certificación electrónica:** Aprovechando todas las virtudes del LDAP, es importante recalcar, dado que se define la publicación de claves públicas en la estructura, se puede utilizar una infraestructura de claves públicas para tener la autenticación y autorización de usuarios sobre recursos informáticos y datos.

A continuación se explica detalladamente cada componente de configuración dentro del servicio de directorio LDAP.

La base representa la raíz del directorio en nuestro caso es ingedigit.com, esto se realiza de la siguiente forma:

```
dc=ingedigit, dc=com
```

La base de búsqueda (*search base*) determina el punto del árbol a partir del cual hacer la búsqueda y el alcance (*scope*) determina la manera en que la búsqueda descende por el árbol.

El nombre distintivo (*distinguished name*) o DN es el identificador único para un objeto en el directorio, en nuestro caso será admin, representando al administrador.

```
uid=tecnico, ou=People, dc=ingedigit, dc=com
```

El nombre distintivo relativo (*relative distinguished name*) o RDN es la parte del DN que hace único al objeto en el contexto (subárbol).

```
uid=tecnico, ou=People
```

LDIF (*LDAP Interchange Format*): representa el formato para importar y exportar información de directorio entre servidores de directorios basados en LDAP, o para describir una serie de cambios que han de aplicarse al directorio, se usa en general el archivo de formato conocido como LDIF.

Instalación del servidor LDAP

En este trabajo se empleó el paquete OpenLDAP para Debian, que es la implementación de un servidor LDAP que se distribuye bajo licencia GNU (OpenSource). Está disponible en <http://www.openldap.org>. Sus componentes principales son:

- El demonio slapd
- El paquete que contiene las herramientas clientes ldap-utils
- El paquete para el backend Berkeley DB db4.2-util

Además, es compatible con LDAPv3, ofreciendo la habilidad de referir los clientes a otros servidores, publicar el esquema a través de consultas, internacionalización usando UTF-8 y soporte para SSL/TLS y SASL.

Configuración básica del servidor LDAP

La configuración básica del LDAP se encuentra contenida en el archivo slapd.conf ubicado en la ruta `/etc/ldap/`. Este archivo es de tipo texto tradicional Unix. A partir del comienzo del mismo se tiene la configuración global que afecta al demonio servidor slapd (ver anexo D).

Los esquemas estándar se encuentran en `/etc/ldap/schema`, siendo `core.schema` el mínimo requerido.

En este archivo se incluyen los esquemas necesarios de la siguiente forma:

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/inetorgperson.schema
schemacheck on.
```

El servicio slapd registra los eventos a través de syslogd facility LOCAL4.

El Nivel de bitácora del archivo de configuración indica cuánto registrar:

- Se usa -1 para registrar todo.
- Se usa 0 para registrar nada.

Cualquier otro número es la suma de bits filtro, por ejemplo: 296 es igual a

- 8bits para registrar el manejo de conexiones.
- 32 8bits para registrar el procesamiento de filtros de búsqueda.
- 256 8bits para registrar estadísticas de operación.

Se debe indicar un archivo para guardar el PID de slapd y otro guardar los argumentos de slapd. La configuración para bitácora y archivos de estado para este Sistema de gestión es la siguiente:

```
loglevel 0
pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
```

Los parámetros de configuración para criptografía son los siguientes:

```
TLSCipherSuite HIGH:MEDIUM:+SSLv2:RSA
TLSCACertificateFile /etc/ldap/cacert.pem
TLSCertificateFile /etc/ldap/slapd-cert.pem
TLSCertificateKeyFile /etc/ldap/slapd-key.pem
TLSVerifyClient 0
```

Cada backend define un tipo de almacenamiento y permite acceder a directorios específicos, en consecuencia debe haber al menos un backend definido.

El backend recomendado es bdb. Este es basado en archivos indexados Berkeley DB, usando el DN como índice.

La configuración correspondiente al backend en el archivo es como sigue:

```
backend bdb
cachesize 256
checkpoint 512 30
```

cachesize indica el número de entradas a mantener en el caché de memoria.

checkpoint define la frecuencia de checkpoints según cantidad de kilobytes escritos o minutos transcurridos.

Configuración de un directorio:

La configuración de un directorio requiere:

- Indicar el tipo de backend a utilizar.
- Indicar la ubicación del repositorio.
- Definir la base.
- Indicar el DN del “superusuario” (rootdn).

En el caso de este trabajo la configuración del directorio es la siguiente:

```
database bdb
directory "/var/lib/ldap"
suffix "dc=ingedigit,dc=com"
rootdn cn=admin,dc=ingedigit,dc=com
```

Al tratarse de una base de datos jerárquica la adecuada configuración de índices permite optimizar las consultas.

Los índices necesarios para obtener un buen rendimiento son:

eq (igualdad) para búsquedas exactas.

pres (presencia) para determinar si un objeto posee o no un atributo particular.

sub (substring) para hacer búsquedas sobre substrings de atributos

approx (aproximado) para hacer búsquedas con correspondencia fonética aproximada.

En el archivo de configuración se especificaron los siguientes índices:

```
index objectClass eq
index uid,uidNumber,gidNumber,memberUid eq
index cn,mail,sn,givenName eq,sub
```

Replicación del servidor Ldap

Con la finalidad de aumentar la seguridad, disponibilidad, fiabilidad y disminuir los tiempos de respuesta se implantó una réplica del servicio.

El servicio de directorio OpenLDAP ha sido diseñado para ser tolerante a fallas, incluye un mecanismo de replicación y distribución del directorio.

Se estableció un servidor maestro (*master server*) que contiene el directorio principal siendo el único susceptible de recibir modificaciones (agregados, modificaciones, eliminación). Luego se establecieron dos servidores réplica (*replica servers*) que replican las modificaciones efectuadas sobre el servidor maestro. De ahí en adelante cualquier cambio efectuado en el servidor maestro es automáticamente reflejado en los servidores réplica.

En organizaciones pequeñas con no más de diez equipos es posible operar solamente con el servidor maestro. En organizaciones más grandes es conveniente tener como mínimo un servidor réplica adicional. En organizaciones con cientos de estaciones de trabajo y varias subredes, como es el caso de Ingedigit C.A. suele ser práctico contar con dos servidores réplica para distribuir la carga de trabajo.

El esquema de replicación y su funcionamiento se muestra en la figura12

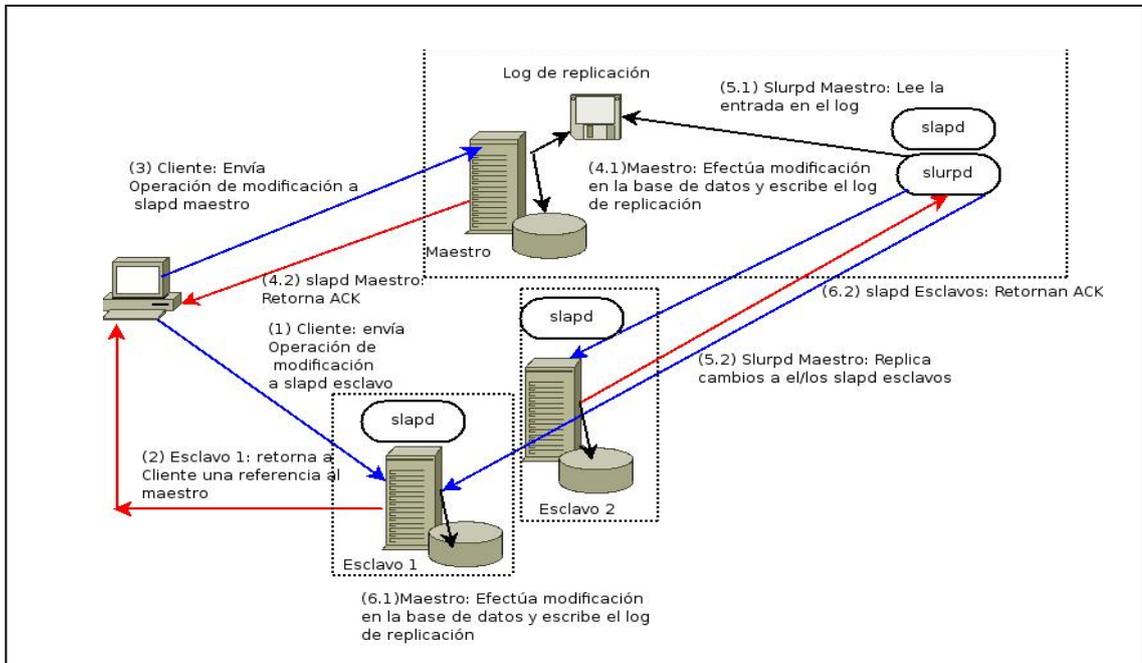


Figura 12: Esquema de replicación del servicio LDAP con un maestro y dos esclavos.

Autor: K. Rodríguez y S. Hernández

3.4 Solución para el Módulo de escalamiento

El módulo de escalamiento desarrollado está compuesto por dos sub-módulos: uno para el aumento automático de prioridad de las incidencias y otro para el escalamiento de incidencias entre colas de diferente nivel.

Request Tracker permite crear tantas colas como sean necesarias. Una cola puede definirse como un grupo de incidencias lógicamente relacionadas entre sí. Todas las incidencias en una cola pueden ser gestionadas por un grupo homogéneo de personas dentro de la organización. Cada cola determina un rango de prioridad para las incidencias que son creadas dentro de ella. Este rango se mueve entre una prioridad inicial y una prioridad final asociadas a la cola.

Cuando una incidencia entra a una cola del Sistema, lo hace con la prioridad inicial o base de esa cola, esta prioridad es incrementada de acuerdo a una matriz de decisión por el módulo para el aumento de prioridades. Una matriz de decisión permite definir el tiempo en el cual una incidencia debe ser atendida y lógicamente determina cuándo debe ser escalada a un nivel superior. La

construcción de la matriz de decisión responde a los requerimientos particulares de una organización y debe ser construida tomando en cuenta la naturaleza de la incidencia y su severidad.

El módulo se encuentra definido en el archivo `escalamiento.pl`, posicionado en la ruta `/usr/bin`. (Ver anexo E).

Inicialmente se inicializan todas las variables del Sistema y se crean las estructuras de datos para almacenar las incidencias.

Luego se determina por cada una de las colas cuáles son las incidencias activas y posteriormente se aumenta la prioridad de cada una de ellas. Esto se hace invocando la herramienta `crontool` con los parámetros convenientes dentro de la llamada al Sistema `system`.

La herramienta `crontool` es parte de Request Tracker y permite de manera práctica buscar un conjunto de incidencias y tomar una acción determinada sobre ellas.

Para el escalamiento de las incidencias entre colas se implementó un script que hace uso de un lenguaje particular, basado en SQL, que provee Request Tracker conocido como TicketSQL creado con el propósito de hacer consultas específicas en la base de datos de incidencias del Sistema y del utilitario de línea de comandos `rt`, que permite interactuar con el servidor de Request Tracker sobre `http` y ofrece una interfaz bastante práctica.

En tal sentido, por medio de un query TicketSQL se consulta por cada cola cuáles incidencias han alcanzado en un momento determinado su prioridad máxima, para de esta forma ser asignado a una cola de mayor prioridad.

Por cada cola se implementa un script de escalamiento. Este script tiene la siguiente forma:

```
rt ls "Priority > X and status='open'" | edit - set Queue = 'Z'
```

El comando anterior busca todas las incidencias que alcanzaron la prioridad máxima X definida en la cola y que están en estado abierto para luego escalarlas a la cola Z de siguiente prioridad.

La forma general del comando `rt` se detalla a continuación:

```
rt acción [opciones] [argumentos]
```

acción: son aplicadas sobre las incidencias, se tienen las siguientes acciones:

```
list ( Lista objetos dependiendo de una condición )
show ( Muestra el detalle de los objetos )
edit ( Edita el detalle de los objetos )
create ( Crea un nuevo objeto )
```

El intervalo de ejecución de los scripts varía según el nivel de soporte, ya que en un nivel de mayor prioridad la frecuencia de ejecución será menor en virtud de que las solicitudes en este nivel tienen mayor preferencia que las de los niveles inferiores.

3.4.1 Plantilla del idioma

RT provee una plantilla para 18 idiomas, entre ellos: chino (República Popular China) y chino (Taiwan), ruso, portugués, polaco, noruego, japonés, italiano, indonesio, húngaro, hebreo, alemán, francés, inglés, checo, finlandés, danés y español.

En este trabajo se mejoró la plantilla de idioma español en virtud de que algunas frases no tenían su correspondiente traducción o estaban incorrectas.

La plantilla de idioma español está definida en el archivo `es.po`, posicionado en la ruta `/usr/share/request-tracker3.6/lib/RT/I18N`.

Una plantilla de idioma en el Sistema RT es un archivo de texto plano con extensión `.po`, cuya estructura general se presenta a continuación:

```
#: Ruta del archivo donde se ubica la frase a traducir
msgid " Frase original que se va a traducir "
msgstr " Frase traducida "
```

A cada expresión que se desea traducir le corresponde un bloque como el anterior.

3. 5 Integración de módulos

Para realizar la integración entre los tres Sistemas, se desarrolló un módulo de software, cuya función es brindar abstracción de los datos sobre los distintos Sistemas de gestión (MySQL y PostgreSQL) de cada una de las herramientas utilizadas. (Ver anexo F)[20].

Este módulo desarrollado en el lenguaje de programación Perl y bajo el framework Mason se encuentra insertado dentro del código de la herramienta RT y permite extraer los datos del inventario de hardware y software de la herramienta OCS-Inventory y los datos de activos de red encontrados en la herramienta Netdisco.

Esta integración de datos es unida en una misma interfaz gráfica que brinda a los administradores y técnicos una visión detallada del equipo involucrado (configuración software, hardware, subred a la que pertenece, dispositivos de interconexión entre otros) en la incidencia reportada.

El archivo de R.T afectado con este módulo es `index.html` (Ver anexo G).

DBI es el acrónimo de *Database Interface*, y es un módulo que permite al programa abstraerse de la implementación específica del acceso a la base de datos, que puede ser distinta en cada base de datos, y le permite programar el

acceso a una base de datos de manera transparente. De esta forma se está facilitando la portabilidad de los diversos programas ya que no están unidos a ninguna base de datos.

Para el caso particular de este Trabajo Especial de Grado, este módulo resultó de gran utilidad ya que permitió realizar consultas de forma sencilla y transparente a Bases de Datos MySQL y PostgreSQL, la primera en el caso de inventario de Hardware y la segunda para el caso de inventario de componentes activos de la red de datos de la Organización.

Perl::DBI encaja entre los programas y las interfaces particulares de cada base de datos, los llamados DBD (de *Database Drivers*) que son los que implementan el acceso a la base de datos en sí.

DBI tiene una interfaz muy sencilla que permite al programador seleccionar la base de datos a utilizar y hacer consultas SQL, devolviendo los resultados en tablas o arreglos asociativos que pueden ser finalmente tratados en Perl. El acceso a una base de datos con Perl::DBI se limita a:

- La conexión de la base de datos, que se realiza con la función `connect` y en la que se indica la base de datos a utilizar, así como el usuario y contraseña para realizar la conexión.
- La preparación de una llamada SQL con la función `prepare`, que se utilizará para que el motor de la base de datos con la que se ha realizado la conexión compile la instrucción SQL y se prepare a ejecutarla.
- La ejecución de la llamada SQL ya preparada con la función `execute`.
- La recuperación de los datos resultados de la ejecución de la orden SQL con las funciones `fetchrow_array`, `fetchrow_arrayref` o `fetchrow_hashref`.
- La desconexión de la base de datos con la orden `disconnect`.

CAPITULO 4 AMBIENTES DE PRUEBAS

El objetivo del presente capítulo es exponer detalladamente el entorno donde se ejecutará el Sistema propuesto en este Trabajo Especial de Grado, tomando en consideración los aspectos fundamentales de hardware y software empleados para su implementación y de todos los componentes que interactúan con el Sistema. Se designaron dos ambientes de pruebas, los mismos se componen por configuraciones técnicas distintas y ubicación en diferentes edificios de la Organización, con la finalidad de evaluar aspectos de rendimiento de equipos.

Por cada uno de los ambientes de prueba se efectuó un levantamiento de información del estado actual de la red de datos, tomando en cuenta elementos como: capacidad de conectividad, diagramas de conexión y categoría de medios de transmisión. Se recolectaron los datos sobre el número de equipos conectados a la red, sus características de hardware y software y sobre el comportamiento promedio de la gestión de servicio en la Organización.

El propósito del levantamiento previo de información, es el de generar todos los indicadores necesarios que permitan determinar que tan confiables son los resultados que arroja el Sistema, permitiendo determinar su utilidad y si los resultados que se esperaban son realmente los que se obtienen

4.1 Ambiente 1: Grupo Ingedigit C.A. Edificio Lex, Piso PH.

El ambiente de prueba 1 se encuentra localizado en el edificio Lex piso PH del Grupo Ingedigit C.A.

Descripción del Hardware y Software. Las tablas 13 y 14 se detallan las especificaciones técnicas del primer ambiente de prueba donde se ejecutó la aplicación.

Hardware

Componente	Versión/Valor
CPU	Xeon dual Core
Memoria principal	4 GB
Memoria en disco	575 GB
Tarjeta de red (NIC)	10/100 Mbps

Tabla 13: Componentes de Hardware
Autor: K.Rodríguez y S.Hernández. Año 2008

Software

Componente	Versión/Valor
Sistema Operativo	Debian Etch 4.0
Kernel	2.6.18-4-686
Perl	5.8.8
SNMP::Info	0.9
Net-SNMP	5.2.3

PHP	5.2.0
Apache	2.2.3
PostgreSQL	8.1.11
MySQL	5.0.32
Netdisco	0.95
Ocs-Inventory	1.0.1.2
Request-Tracker	3.6

Tabla 14: Componentes de Software
Autor: K.Rodríguez y S.Hernández. Año 2008

Descripción de la red de datos. A continuación se detalla la información técnica de la red de datos donde se ejecutó la aplicación, obtenida a través de visitas a cada uno de los cuartos de cableado.

En primer lugar se construyó un diagrama físico general que contempla cada una de las edificaciones involucradas, la conectividad entre ellas y con el ISP. Luego, se construyeron diagramas físicos por cada edificación contemplando información relevante de cada uno de sus componentes activos. Finalmente, se elaboraron tablas para describir la capacidad de conectividad tanto en los cuartos de cableado como fuera de ellos y la categoría de los medios de transmisión.

Diagrama físico general. La Organización Ingedigit mantiene sus instalaciones distribuidas en tres edificios: Folgana, Venezuela y Lex. A continuación se presenta un diagrama físico general que muestra de forma gráfica la conectividad física de las edificaciones.

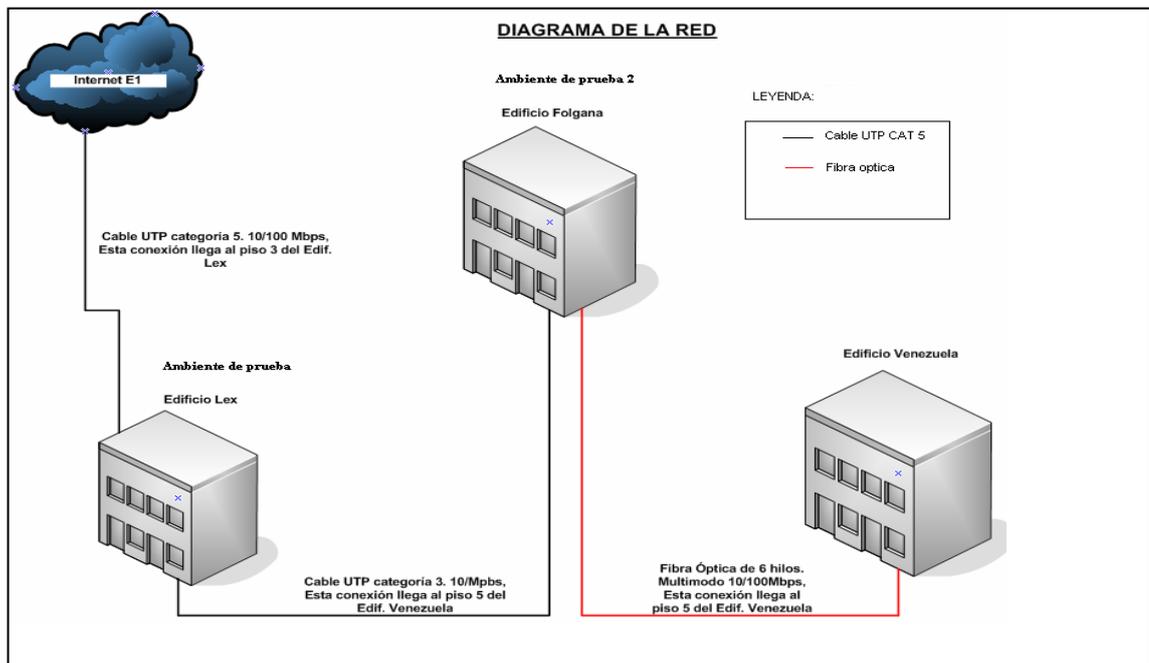


Figura 13: Diagrama de red. Ambiente 1
Autor: K.Rodríguez y S.Hernández. Año 2008

Diagramas físicos por edificio. Por cada uno de los edificios se elaboraron diagramas que permitieran visualizar la información relevante de cada uno de los componentes activos existentes (switches y concentradores), la conexión entre ellos indicando los puertos origen y destino, así como la categoría de los medios de transmisión.

A continuación se muestran cada uno de los diagramas:

Diagrama físico edificio Folgana

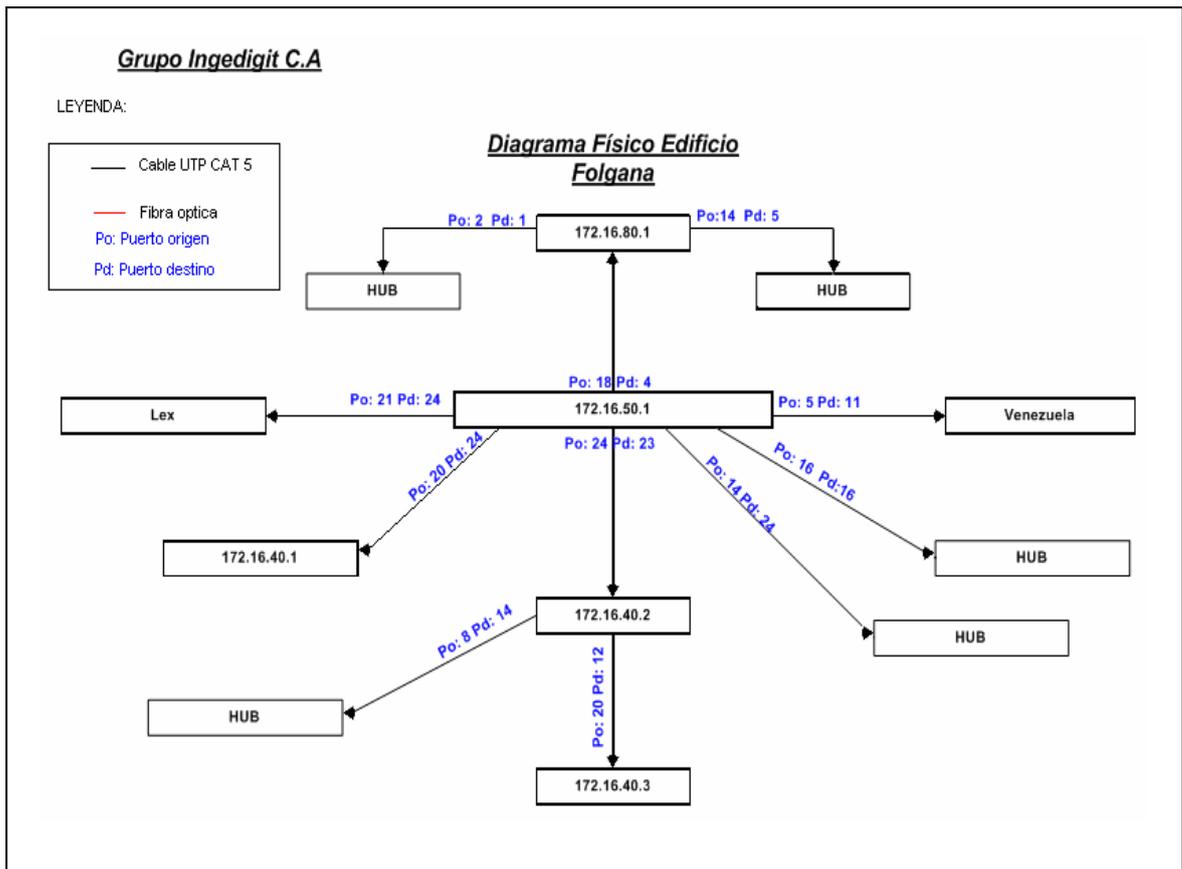


Figura 14:Diagrama edificio Folgana
Autor: K.Rodríguez y S.Hernández. Año 2008

Diagrama físico edificio Venezuela

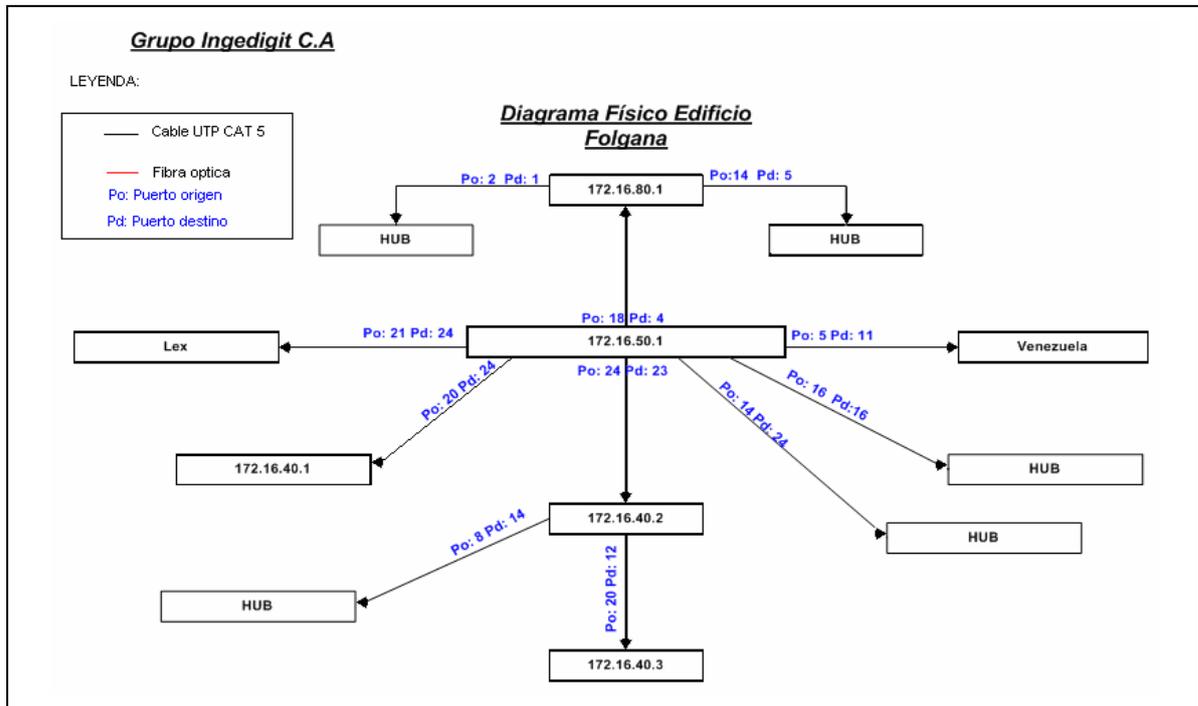


Figura 15:Diagrama edificio Venezuela
Autor: K.Rodríguez y S.Hernández. Año 2008.

Diagrama físico edificio lex

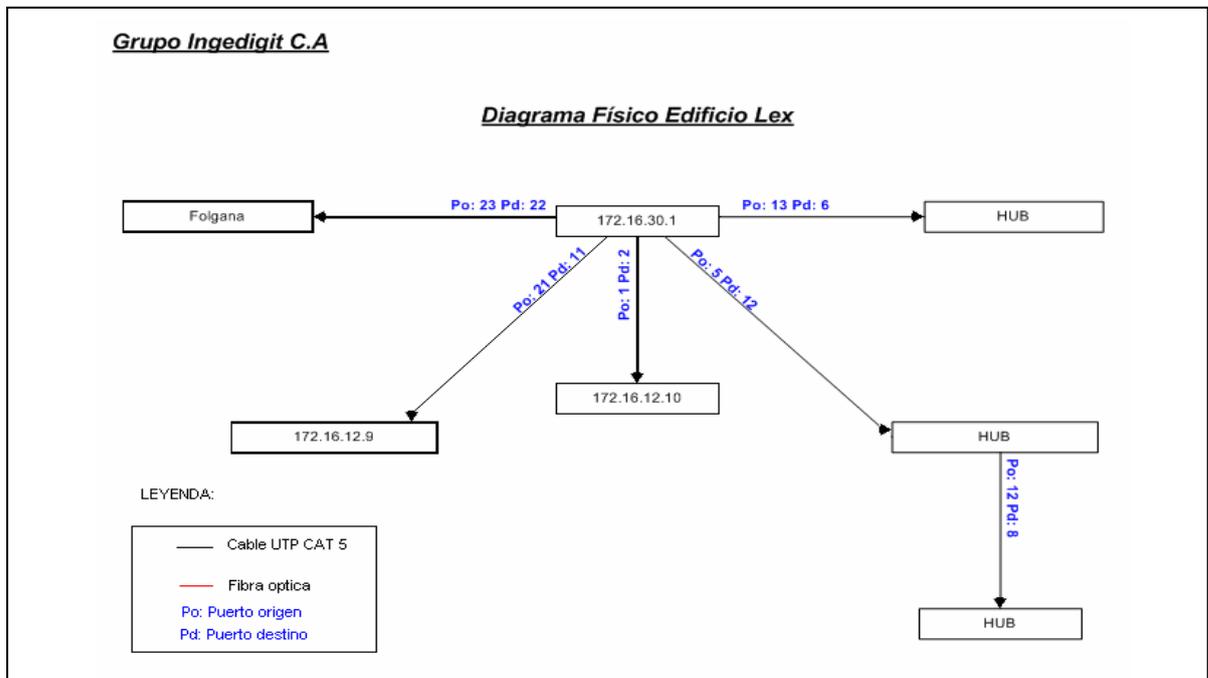


Figura 16:Diagrama edificio Lex
Autor: K.Rodríguez y S.Hernández. Año 2008

Con la finalidad de determinar que tan confiables es la información arrojada por las aplicaciones de inventario se llevó a cabo un levantamiento manual de información de la red, tomando en consideración el número y características de dispositivos activos.

4.1.2 Levantamiento manual de información de los componentes de red

Las tablas que se muestran a continuación describen la capacidad de conectividad tanto en los cuartos de cableado como fuera de ellos, la categoría de los medios de transmisión y las características de los componentes activos.

Cabe destacar que las tablas para describir los switches y concentradores difieren, puesto que en el primer caso se registra la dirección IP del dispositivo, mientras que en el segundo caso, por tratarse de dispositivos Capa-2 no se registra la dirección IP. En ambas tablas (switches y concentradores) se registra marca, modelo, total de puertos y total de puertos disponibles, tanto dentro del cuarto de cableado, como fuera de él.

4.1.2.1 Información de los dispositivos

Tabla de Switches del edificio Folgana

Ubicación	Piso 3	Equipo	Switches						
			IP	Marca	Modelo	Total puertos		Total disponibles	
						c.c.	otros	c.c.	otros
172.16.40.1	Nortel	Business Policy Switch 2000	24	-	0	-			
172.16.40.2	Nortel	Business Policy Switch 2000	24	-	0	-			
172.16.40.3	Nortel	BayStack 350	12	-	0	-			
Total			60	-	0	-			

Tabla 15:Switches Folgana piso 3
Autor: K.Rodríguez y S.Hernández. Año 2008

Ubicación	Piso 5	Equipo	Switches						
			IP	Marca	Modelo	Total puertos		Total disponibles	
						c.c.	otros	c.c.	otros
172.16.50.1	Nortel	Business Policy Switch 2000	24	-	0	-			
Total			24	-	0	-			

Tabla 16:Switches Folgana piso 5
Autor: K.Rodríguez y S.Hernández. Año 2008

Ubicación	Piso 8	Equipo	Switches			
IP	Marca	Modelo	Total puertos		Total puertos disponibles	
			c.c.	otros	c.c.	Otros
172.16.80.1	Nortel	Business Policy Switch 2000	24	-	0	-
Total			24	-	0	-

Tabla 17: Switches Folgana piso 8
Autor: K.Rodríguez y S.Hernández. Año 2008

Leyenda:

* c.c.: Cuarto de Cableado

* Otros: Disponibilidad fuera del cuarto de cableado

Tabla de concentradores del edificio Folgana.

Ubicación	Piso 3	Equipo	Concentradores			
Marca		Modelo	Total puertos		Total puertos disponibles	
			c.c.	Otros	c.c.	Otros
3Com		Superstack II	-	24	-	0
Total			-	24	-	0

Tabla 18: Concentradores Folgana piso 3
Autor: K.Rodríguez y S.Hernández. Año 2008

Ubicación	Piso 5	Equipo	Concentradores			
Marca		Modelo	Total puertos		Total puertos disponibles	
			c.c.	Otros	c.c.	Otros
3Com		Superstack II	-	26	-	11
Tiger Stack		Tiger Stack	-	16	-	1
Total			-	42	-	12

Tabla 19: Concentradores Folgana piso 5
Autor: K.Rodríguez y S.Hernández. Año 2008

Ubicación	Piso 8	Equipo	Concentradores			
Marca		Modelo	Total puertos		Total puertos disponibles	
			c.c.	Otros	c.c.	Otros
3Com		Superstack II	-	24	-	5
3Com		Superstack II	-	24	-	1
Total			-	48	-	6

Tabla 20 : Concentradores Folgana piso 8
Autor: K.Rodríguez y S.Hernández. Año 2008

Tabla de Switches del edificio Venezuela

Ubicación	Piso 5	Equipo	Switches			
			Total puertos		Total puertos disponibles	
			c.c.	otros	c.c.	otros
172.20.100.10	Nortel	BayStack 350	12	-	0	-
172.20.100.9	Nortel	Business Policy Switch 2000	24	-	0	-
172.16.10.244	Nortel	BayStack 325	-	24	-	13
172.16.12.191	Nortel	Ethernet Switch 470	24	-	1	-
172.20.100.8	Nortel	Business Policy Switch 2000	24	-	5	-
172.20.100.7	Nortel	Business Policy Switch 2000	24	-	4	-
172.20.100.12	Nortel	BayStack 460	24	-	0	-
172.20.100.11	Nortel	Business Policy Switch 2000	24	-	10	-
172.20.100.13	Nortel	BayStack 350	12	-	0	-
172.16.12.5	3Com	Entreprises	-	24	-	21
Total			168	48	20	34

Tabla 21:Switches Venezuela piso 5
Autor: K.Rodríguez y S.Hernández. Año 2008

Tabla de concentradores del edificio Venezuela

Ubicación	Piso 5	Equipo	Concentradores			
			Total puertos		Total puertos disponibles	
			c.c.	Otros	c.c.	Otros
3Com		Superstack	-	12	-	6
3Com		Superstack	-	12	-	0
Total			-	24	-	6

Tabla 22:Concentradores Venezuela piso 5
Autor: K.Rodríguez y S.Hernández. Año 2008

Tabla de Switches del edificio Lex

Ubicación	Piso 3	Equipo	Switches			
IP	Marca	Modelo	Total puertos		Total puertos disponibles	
			c.c.	Otros	c.c.	otros
172.16.30.1	Nortel	Business Policy Switch 2000	24	-	0	-
172.16.12.10	Nortel	Business Policy Switch 2000	24	-	0	-
Total			48	-	0	-

Tabla 23:Switches Lex piso 3
Autor: K.Rodríguez y S.Hernández. Año 2008

Ubicación	Piso PH	Equipo	Switches			
IP	Marca	Modelo	Total puertos		Total puertos disponibles	
			c.c.	Otros	c.c.	otros
172.16.12.9	Nortel	Business Policy Switch 2000	24	-	0	-
Total			24	-	0	-

Tabla 24:Switches Lex piso 6
Autor: K.Rodríguez y S.Hernández. Año 2008

Tabla de concentradores del edificio Lex

Ubicación	Piso 3	Equipo	Concentradores			
Marca		Modelo	Total puertos		Total puertos disponibles	
			c.c.	Otros	c.c.	Otros
3Com		Superstack	-	24	-	0
Total			-	24	-	0

Tabla 25:Concentradores Lex piso 3
Autor: K.Rodríguez y S.Hernández. Año 2008

Ubicación	Piso PH	Equipo	Concentradores			
Marca		Modelo	Total puertos		Total puertos disponibles	
			c.c.	Otros	c.c.	Otros
TP-LINK		SF1008D	-	8	-	4
HP		Advance stack hub	-	8	-	5
Total			-	16	-	9

Tabla 26:Concentradores Lex piso 6
Autor: K.Rodríguez y S.Hernández. Año 2008

Resultados entre los tres edificios

Total switches			20	
Total puertos		Total puertos disponibles		
c.c.	Otros	c.c.	Otros	
348	48	20	34	

Tabla 27:Total de Switches
Autor: K.Rodríguez y S.Hernández. Año 2008

Total concentradores			10	
Total puertos		Total puertos disponibles		
c.c.	Otros	c.c.	Otros	
-	158	-	33	

Tabla 28: Total de Concentradores
Autor: K.Rodríguez y S.Hernández. Año 2008

Categoría de los medios de comunicación: en la tabla se resume la categoría de medios de transmisión utilizada en cada uno de los edificios.

Edificio	Piso	Categoría de medio
Folgana	3	3
	5	5
	8	5
Venezuela	5	5
	6	5
LEX	3	5
	PH	5

Tabla 29:Categoría de los medios de transmisión
Autor: K.Rodríguez y S.Hernández. Año 2008

Conexión entre los edificios

Conexión entre Edificio Lex y Edificio Folgana: Cableado UTP categoría 3.

Conexión entre Edificio Folgana y Edificio Venezuela: Fibra óptica multimodo, funcionando a 100 Mbps.

4.1.2.2 Información de gestión

El siguiente análisis muestra un estudio sobre la gestión de incidencias dentro de la Organización Ingedigit, en un período de dos meses (Marzo, Abril), donde se evaluaron dos factores: tipo de incidencias ocurridas y tiempo de solución de las mismas por parte de los técnicos, esto con la finalidad de identificar las incidencias más frecuentes dentro de la Organización y evaluar los tiempos en que estas son resueltas. La frecuencia de las incidencias fue tomada como número de incidencias ocurridas en el período de los meses evaluados.

Es importante destacar que los tiempos en brindar solución a los usuarios por parte de los técnicos se ven afectado por el traslado de los mismos al lugar del problema, debido a la falta de información indispensable al momento dar solución a una solicitud.

4.1.2.2.1 Tipos de Incidencias ocurridas

En la tabla 30 se observa la frecuencia por cada tipo de incidencia ocurrida en la Organización. De un total de 99 incidencias presentadas en un período de dos meses, resaltan con mayor porcentaje las incidencias productos de fallas en

software con 79,79% de los casos, 16,16% para fallas de red, 4,04% para fallas en hardware y un 1,01% para casos anulados.

Incidencia	Frecuencia
Software	79
Red	16
Hardware	4
Anulado	1

Tabla 30: Frecuencia de Incidencias ocurridas
Autor: K. Rodríguez y S. Hernández

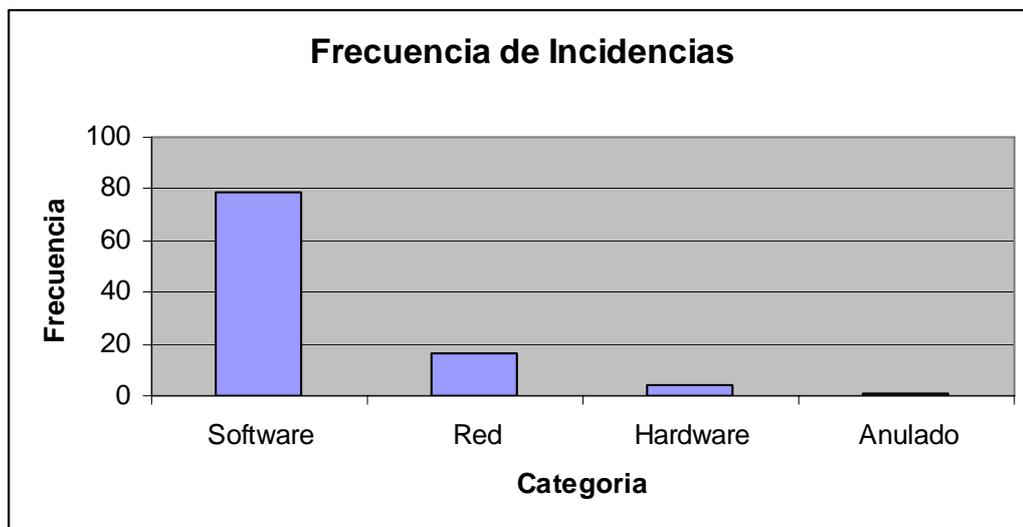


Figura 17: Gráfico Frecuencia de Incidencias
Autor K. Rodríguez y S. Hernández

En la tabla 31 y en la figura 18 se observan en detalle los tipos de fallas de software más frecuentes dentro de la Organización.

Incidencia	Frecuencia
Instalación / Desinstalación	8
Configuración / Actualización	10
Problemas con Sistema Operativo	13
Problemas con correo	7
Virus / Spyware / Troyano	30
Fallas generales	17
Configurar perfil	10
Problemas para imprimir	5

Tabla 31: Frecuencia de Incidencias de software
Autor: K. Rodríguez y S. Hernández

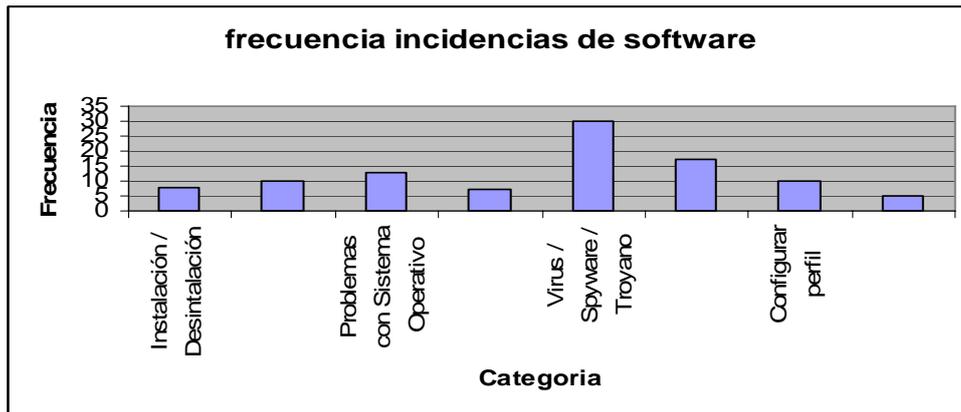


Figura 18: Frecuencia de Incidencias de software.
Autor K. Rodríguez y S. Hernández

En la tabla 32 y en la figura 19 se observan en detalle los tipos de fallas de red más frecuentes dentro de la Organización.

Incidencia	Frecuencia
Instalación / Desinstalación / configuración switches	7
Dirección IP duplicada	16
No se establece conexión	10
No se inicia session	8
Mal diseño de red	15
Fallas generales	15
Fallas conexión servidores	10
Saturación de puertos	19

Tabla 32: Frecuencia de Incidencias de red
Autor: K. Rodríguez y S. Hernández

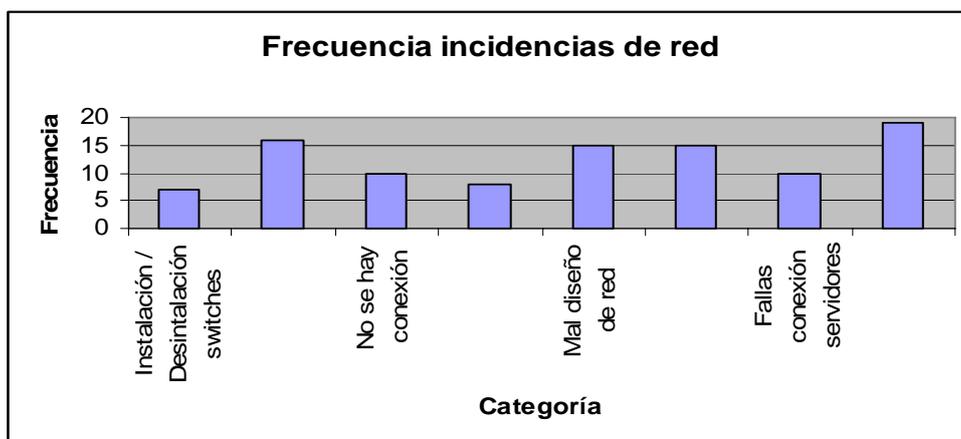


Figura 19: Frecuencia de Incidencias de red.
Autor K. Rodríguez y S. Hernández

En la tabla 33 y en la figura 20 se observan en detalle los tipos de fallas de hardware más frecuentes dentro de la Organización.

Incidencia	Frecuencia
Fallas monitor	3
Fallas disco duro	10
Fallas CPU	15
Fallas teclado/ Mouse	7
Fallas Tarjeta madre	11
Fallas Tarjeta sonido/ video	14
No enciende / apaga el equipo	30
Fallas Unidad CD / floppy	10

Tabla 33: Frecuencia de Incidencias de hardware
Autor: K. Rodríguez y S. Hernández

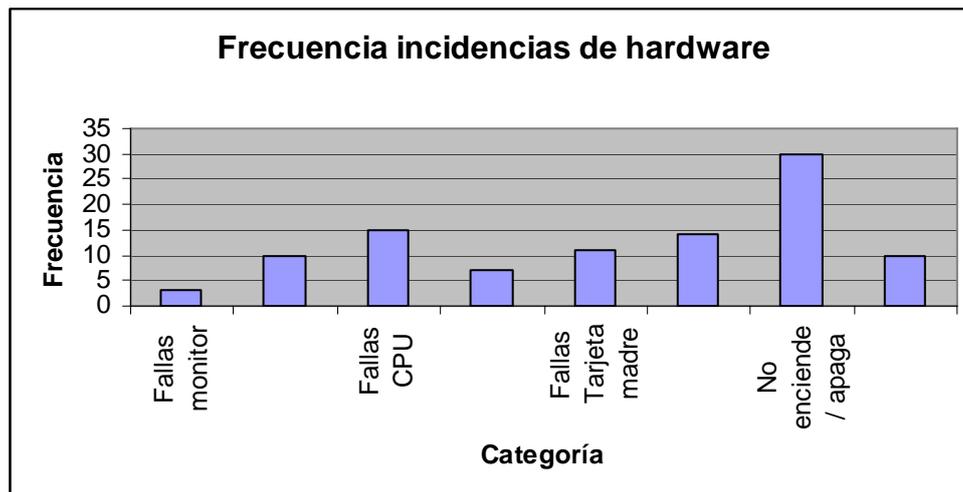


Figura 20: Frecuencia de Incidencias de hardware.
Autor K. Rodríguez y S. Hernández

4.1.2.2.2 Tiempo empleado por los técnicos en dar solución a una incidencia

A continuación se detalla un aproximado del tiempo empleado por los técnicos para solucionar cada una de las incidencias de software, hardware y red dentro de la Organización.

En la tabla 34 observamos un aproximado en tiempo que refleja cuanto demora un técnico en resolver cada una de las incidencias de software, este es uno de los factores más importante a minimizar con el desarrollo del Sistema de gestión automatizado presentado en este Trabajo Especial de Grado, debido a que la Organización desea brindar mejores tiempos de respuestas a los usuarios y permitir a los técnicos dar solución a los problemas de forma eficiente.

Incidencia	Tiempo estimado (horas)
Instalación / Desinstalación	1
Configuración / Actualización	1
Problemas con Sistema Operativo	8
Problemas con correo	4
Virus / Spyware / Troyano	8
Fallas generales	8
Configurar perfil	1
Problemas para imprimir	3

Tabla 34: Tiempo que tarda un técnico en solucionar una incidencia de software
Autor: K. Rodríguez y S. Hernández

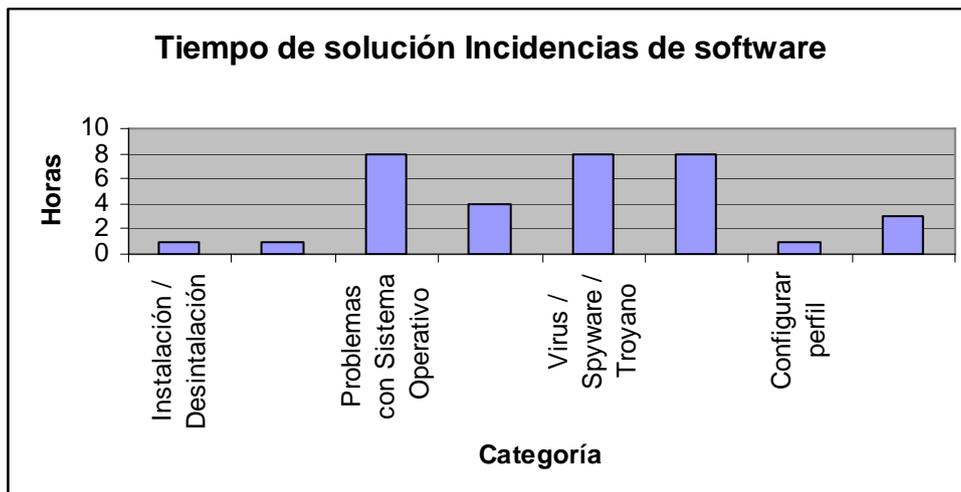


Figura 21: Tiempo que tarda un técnico en solucionar una incidencia de software
Autor: K. Rodríguez y S. Hernández

En la tabla 35 observamos un aproximado en tiempo que refleja cuanto demora un técnico en resolver cada una de las incidencias de red.

Incidencia	Tiempo estimado (Horas)
Instalación / Desinstalación / configuración switches	4
Dirección IP duplicada	8
No se establece conexión	4
No se inicia sesión	3
Mal diseño de red	8
Fallas generales	8
Fallas conexión servidores	8
Saturación de puertos	16

Tabla 35: Tiempo que tarda un técnico en solucionar una incidencia de red
Autor: K. Rodríguez y S. Hernández

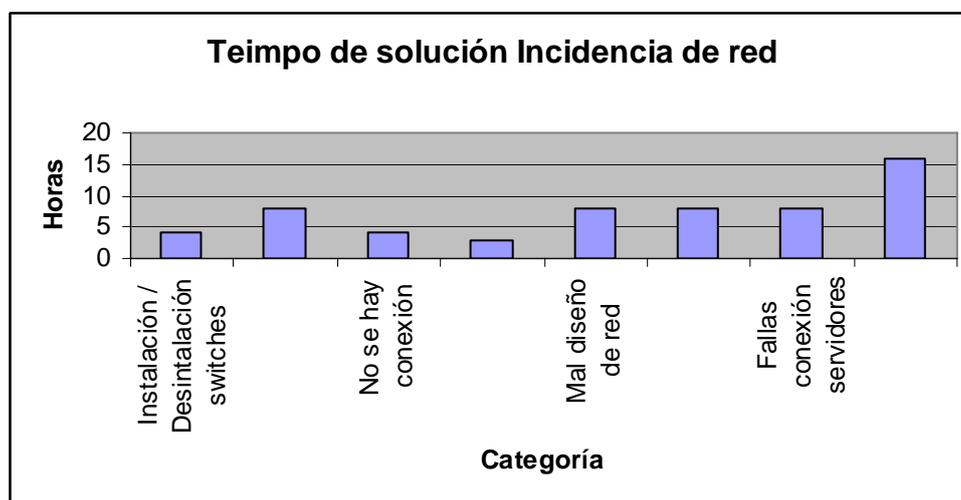


Figura 22: Tiempo que tarda un técnico en solucionar una incidencia de red
Autor: K. Rodríguez y S. Hernández

En la tabla 36 observamos un aproximado en tiempo que refleja cuanto demora un técnico en resolver cada una de las incidencias de hardware.

Incidencia	Tiempo estimado (horas)
Fallas monitor	3
Fallas disco duro	10
Fallas CPU	15
Fallas teclado/ Mouse	1
Fallas Tarjeta madre	4
Fallas Tarjeta sonido/ video	4
No enciende / apaga el equipo	5
Fallas Unidad CD / floppy	4

Tabla 36: Tiempo que tarda un técnico en solucionar una incidencia de hardware
Autor: K. Rodríguez y S. Hernández.

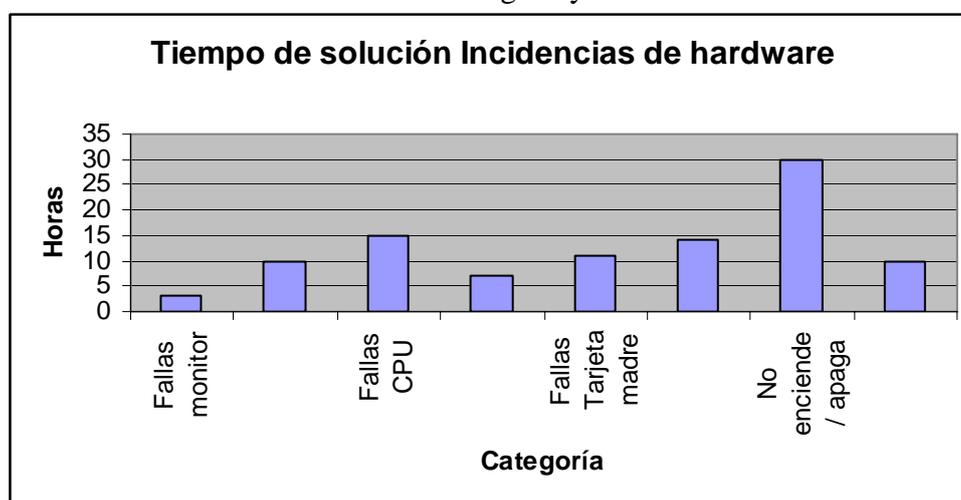


Figura 23: Tiempo que tarda un técnico en solucionar una incidencia de hardware
Autor K. Rodríguez y S. Hernández

Las incidencias más frecuentes dentro de la Organización son las relacionadas con software y red, donde los tiempos empleados en brindar solución varían en relación al conocimiento de los técnicos en cuanto a la información relacionada con la incidencia, es decir, en frecuentes oportunidades los técnicos desconocen por complemento los datos relevantes que se relacionan con la incidencia que desean resolver y deben iniciar la búsqueda de los mismos antes de plantear la solución, lo cual aumenta considerablemente los tiempos de respuesta.

Cuando se presentan incidencias relacionadas con inconvenientes en la red, los técnicos comienzan investigando el switch al que está conectado el usuario que reportó la incidencia, el puerto dentro de este dispositivo, y analizan los posibles escenarios de conexión entre los activos de la Organización, ya que desconocen la topología de red existente y la ubicación entre cada dispositivo activo. Es importante destacar este punto debido a que actualmente no se cuenta con esta

información, por lo que este levantamiento de información se realiza en cada oportunidad que se registra un problema de red.

Muchas de las incidencias dentro de la Organización podrían ser resueltas por los técnicos en intervalos de tiempo más cortos si se contaran con las herramientas de información apropiadas, evitando así el traslado de los mismos al lugar del problema.

El conocimiento y experiencia entre los técnicos es variante, éstos no se encuentran distribuidos en niveles de soporte que permitan abarcar diferentes áreas y aumentar los tiempos de solución de cada incidencia reportada, sino que cada vez que es presentada una incidencia, el técnico que se encuentre libre la puede tomar. Éste factor no resulta apropiado ya que en repetidas oportunidades se presentan incidencias que ya han sido resueltas con éxito, y el técnico que se le asignó desconoce como resolverla, es aquí la importancia que la Organización cuente con una base de conocimientos que permita a los técnicos consultar problemas resueltos anteriormente con todo el material que les facilite implementar la solución mas adecuada.

4.1.3 Resultados esperados

Los resultados esperados se clasificaron de acuerdo a los distintos módulos que conforman el Sistema propuesto.

A continuación se muestra una lista de las expectativas que se tenían al momento de implementar el Sistema:

Del módulo de Service Desk (Gestión de incidencias)

1. Disminuir el tiempo de resolución de las incidencias por parte de los técnicos.
2. Construir una completa Base de Conocimientos conformada por las soluciones de las incidencias frecuentes.
3. Obtener de forma automática al menos los tres tipos de indicadores que se llevan de forma manual en la Organización:
 - a. Incidencias resueltas por propietario de un nivel de soporte determinado
 - b. Incidencias resueltas en un determinado rango de fechas de un nivel de soporte determinado
 - c. Incidencias creadas en un rango determinado de fechas de un nivel de soporte determinado
4. Llevar un historial de acciones por cada uno de los usuarios del Sistema, indicando fecha, hora y acción realizada.
5. Ejecutar en forma automática y matricial el escalamiento de las incidencias en los niveles de soporte definidos.
6. Envío automático de mensajes de correo electrónico al grupo de técnicos registrados en el Sistema al momento de apertura y cierre de una incidencia.
7. Integración con un módulo de inventario.

Del módulo de inventario (Gestión de Inventario)

- 1) Detectar el número de componentes activos de red lo más aproximado posible obtenido en el levantamiento manual de información:
 - a) Número total de switches: 17
 - b) Número total de concentradores: 33

- 2) Por cada switch debe obtenerse al menos:
 - a) Direcciones Capa-2 o Capa-3 de los dispositivos que se encuentran conectados a él.
 - b) Velocidad a la cual se encuentran transmitiendo cada uno de los puertos.
 - c) Vlan asociada al puerto.
 - d) Última fecha de inventario.
 - e) Información del, modelo, Sistema operativo y ubicación.

- 3) Por cada concentrador debe obtenerse al menos:
 - a) Direcciones Capa-2 o Capa-3 de los dispositivos que se encuentran conectados a él.
 - b) Información de la modelo.

- 4) Detectar un número un número de estaciones de trabajo y servidores conectados a la red lo más aproximado posible al inventario manual con el que cuenta la Organización:
 - a) Número total de estaciones de trabajo: 298
 - b) Número total de servidores: 22

- 5) Registrar información técnica sobre los siguientes componentes de Hardware instalado:
 - a) Tarjeta de red
 - b) Disco duro
 - c) Memoria principal
 - d) Procesador
 - e) Monitor

- 6) Registrar información técnica sobre los siguientes componentes de Software instalado:
 - a) Sistema Operativo
 - b) Anti-virus
 - c) Suite de ofimática

7) Detectar cambios realizados en la configuración de Hardware/Software de los equipos.

4.1.4 Resultados encontrados con el Sistema automatizado de gestión

A continuación se encuentran los resultados obtenidos a través del Sistema automatizado de gestión dentro de la Organización Ingedigit en cuanto a reconocimiento de la red, configuraciones de equipos y gestión de incidencias presentadas en un período de dos meses.

Al Sistema estar conformado por la información de gestión de incidencias, inventario de hardware, software y activos de red ofrece a los administradores y técnicos contar con toda la información necesaria al momento de dar solución a un caso sin importar la categoría del mismo. Además permite llevar a cabo la mayoría de las implementaciones desde la oficina de Atención a Usuarios evitando así el traslado del personal al lugar del problema, lo cual brinda al usuario una atención rápida e inmediata a su solicitud y disminuye el tiempo empleado por los técnicos en dar solución al inconveniente.

4.1.4.1 Resultados de gestión

Los siguientes resultados ofrecen una visión sobre el comportamiento de la gestión de incidencias utilizando el Sistema automatizado de gestión desarrollado para este Trabajo Especial de Grado, resaltando las virtudes encontradas en cuanto a reducción de casos reportados, número de solicitudes abiertas y tiempos de respuesta para solucionar los inconvenientes. El análisis abarca los meses de Mayo y Junio del año 2008.

Para hacer uso de todas las virtudes implementadas dentro del Sistema Automatizado de Gestión se realizó la distribución del personal de atención a usuarios en tres niveles de soporte:

Nivel de soporte 1: conformado por los miembros del departamento de atención a usuarios.

Nivel de soporte 2: conformado por los miembros del departamento de producción y operaciones.

Nivel de soporte 3: conformado por los técnicos del departamento de tecnología.

Inicialmente las incidencias son asignadas al primer nivel de soporte durante un tiempo considerable, si éstas pasado éste tiempo no han sido resueltas ya sea por desconocimiento del técnico o por disponibilidad del mismo, escalarán automáticamente al nivel de soporte superior aumentado su severidad, con el objetivo de que sean atendidas lo más pronto posible.

4.1.4.1.1 Tipos de incidencias ocurridas

En los meses de Mayo y Junio se reportaron 74 incidencias dentro de la Organización abarcando hardware, software y red, las cuales han sido tratadas a través de los mecanismos proporcionados dentro del Sistema Automatizado de Gestión. En los dos meses anteriores (Marzo y Abril), sin herramienta de gestión se reportaron 99 incidencias, las cuales se almacenaron en una base de conocimientos para permitir probar el Sistema Automatizado de Gestión en los dos meses siguientes. Se produjo un 25,25% de mejora en la gestión de incidencias. Este porcentaje es un indicador para los administradores y técnicos de la Organización, el cual refleja las virtudes de contar con una herramienta que integra toda la información necesaria al momento de brindar solución a cada una de las incidencias ocurridas. La frecuencia de las incidencias fue tomada como número de incidencias ocurridas en el período de los meses evaluados.

En la tabla 37 se observa la frecuencia por cada tipo de incidencia ocurrida que ha sido tratada por el Sistema Automatizado de Gestión, donde resaltan con mayor porcentaje las incidencias productos de fallas en software con 84% de los casos, 10% para fallas de red, y un 6% para fallas en hardware.

Incidencia	Frecuencia
Software	84
Red	10
Hardware	6

Tabla 37: Frecuencia de Incidencias ocurridas
Autor: K. Rodríguez y S. Hernández

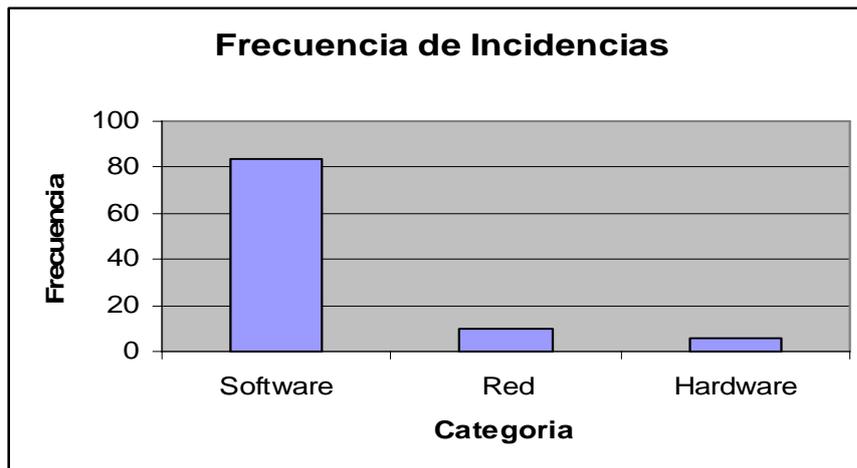


Figura 24: Frecuencia de Incidencias ocurridas
Autor: K.Rodríguez y S.Hernández. Año 2008

En la tabla 38 y en el gráfico 25 se observan en detalle los tipos de fallas de software y su frecuencia:

Incidencia	Frecuencia
Instalación / Desinstalación	13
Configuración / Actualización	15
Problemas con Sistema Operativo	7
Problemas con correo	7
Virus / Spyware / Troyano	23
Fallas generales	10
Configurar perfil	20
Problemas para imprimir	5

Tabla 38: Frecuencia de Incidencias de software
Autor: K. Rodríguez y S. Hernández

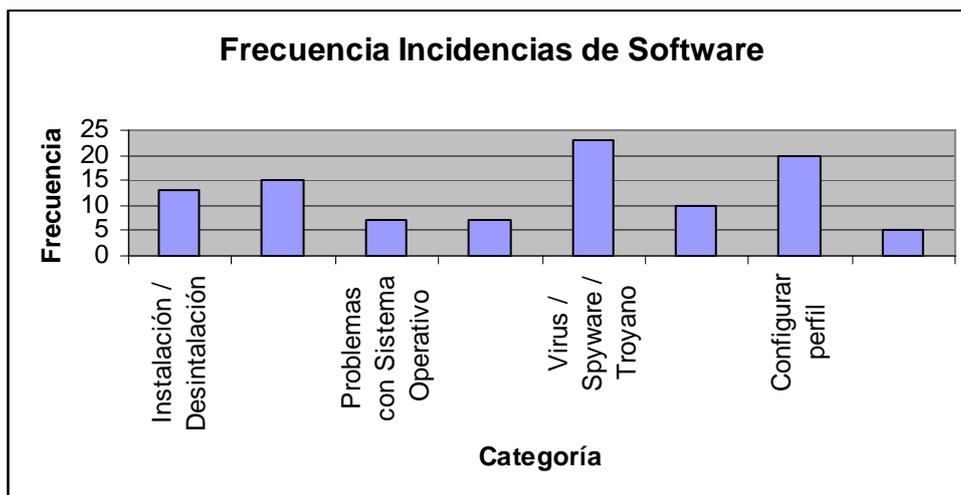


Figura 25: Frecuencia de Incidencias de software.
Autor K. Rodríguez y S. Hernández

En la tabla 39 y en el gráfico 26 se observan en detalle los tipos de fallas de red y su frecuencia:

Incidencia	Frecuencia
Instalación / Desinstalación switches	12
Configuración switches	20
No se hay conexión	9
No se inicia sesión	12
Mal diseño de red	13
Fallas generales	10
Fallas conexión servidores	13
Saturación de puertos	11

Tabla 39: Frecuencia de Incidencias de red
Autor: K. Rodríguez y S. Hernández

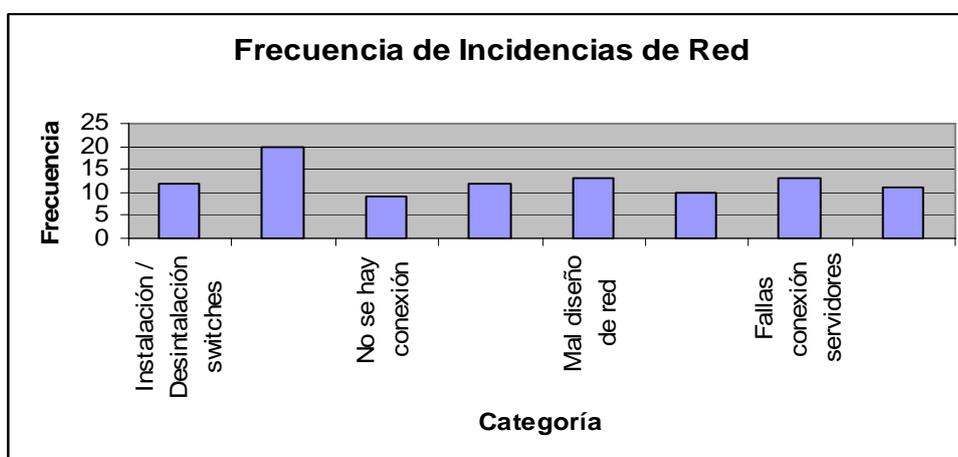


Figura 26: Frecuencia de Incidencias de red.
Autor: K. Rodríguez y S. Hernández

En la tabla 40 y en el gráfico 27 se observan en detalle los tipos de fallas de hardware y su frecuencia.

Incidencia	Frecuencia
Fallas monitor	2
Fallas disco duro	13
Fallas CPU	15
Fallas teclado/ Mouse	6
Fallas Tarjeta madre	15
Fallas Tarjeta sonido/ video	13
No enciende / apaga el equipo	23
Fallas Unidad CD / floppy	13

Tabla 40: Frecuencia de Incidencias de hardware
Autor: K. Rodríguez y S. Hernández

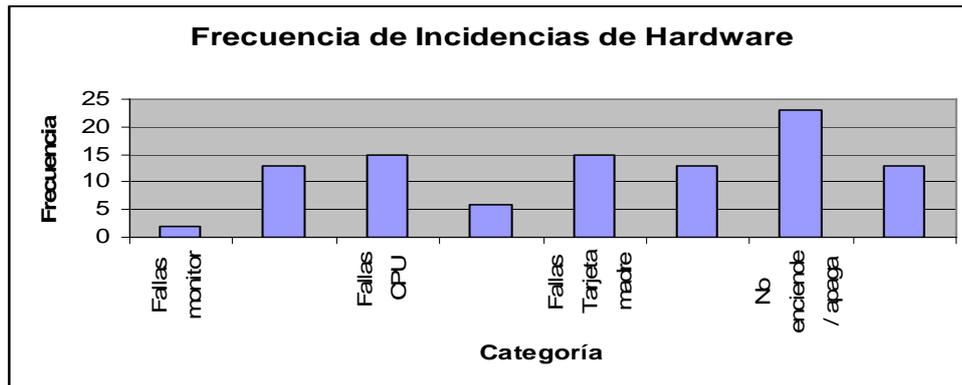


Figura 27: Frecuencia de Incidencias de hardware.
Autor K. Rodríguez y S. Hernández

4.1.4.1.2 Tiempo empleado por los técnicos en dar solución a una incidencia

A continuación se detalla un aproximado del tiempo empleado por los técnicos y la mejora con respecto a los meses anteriores para solucionar cada una de las incidencias de software, hardware y red dentro de la Organización, haciendo uso del Sistema Automatizado de Gestión conformado por una base de conocimientos y escalamiento de incidencias entre diferentes niveles de soporte. En la tabla 41 observamos un aproximado en tiempo que refleja cuanto demora un técnico en resolver cada una de las incidencias de software utilizando en Sistema de Gestión comparado a cuanto tardaba en solucionarlas sin este Sistema.

Incidencia	Tiempo estimado (horas) con Sistema de Gestión	Tiempo estimado (horas) sin Sistema de Gestión
Instalación desinstalación	0,75	1
Configuración Actualización	0,5	1
Problemas con Sistema Operativo	5	8
Problemas con correo	1	4
Virus / Spyware / Troyano	4	8
Fallas generales	6	8
Configurar perfil	1	1
Problemas para imprimir	2,25	3
Total horas	21,25	34

Tabla 41: Tiempo que tarda un técnico en solucionar una incidencia de software
Autor: K. Rodríguez y S. Hernández

Como se observa las instalaciones y desinstalaciones de paquetes, problemas de impresión, así como problemas con el correo mejoraron un 25% en los tiempos de solución al usuario, ya que aunque el técnico debe trasladarse obligatoriamente hasta la estación de trabajo del usuario, las solicitudes escalan entre los niveles de soporte del Sistema, para brindar mejores tiempos de repuesta. Se hace uso de toda la información y documentación encontrada en la base de datos de conocimiento construida en los meses anteriores para solucionar éstas incidencias.

Las configuraciones y actualizaciones de software, así como la detección de virus, spyware y troyanos mejoraron en tiempo un 50%, debido a que el Sistema Automatizado de Gestión permite verificar el software que poseen instalados cada uno de las estaciones clientes, detectando así paquetes maliciosos, posibles errores y actualizaciones que sean necesarias aplicar a éstos equipos.

Las incidencias relacionadas con problemas en Sistemas Operativos mejoraron en tiempo un 37,5% debido a que el Sistema Automatizado de Gestión permite detectar la versión de Sistema Operativo instalado, los parches y actualizaciones que posee la estación de trabajo afectada.

De esta forma el técnico puede conocer que Sistema y cuales actualizaciones deben instalarse nuevamente, puede también identificar cual fue la última actualización realizada a ese equipo y concluir si esta o cualquier otro software recientemente instalado dañó la configuración del Sistema Operativo.

Fallas en generales relacionadas con software mejoraron en tiempo un 25% gracias a toda la información que brinda el Sistema Automatizado de Gestión al técnico y el conocimiento que adquiere el mismo a través de la base de conocimiento, donde encuentra la documentación necesaria para dar solución rápida a inconvenientes frecuentes.

Las horas empleadas por los técnicos en resolver incidencias de software sin contar con el Sistema Automatizado de Gestión llegaron a 34 horas, mientras que contando con este Sistema desarrollado existe un aproximado de 21,25 horas, lo cual proporciona una mejora del 37,5 % en los tiempos de solucionarlas.

En la tabla 42 observamos un aproximado en tiempo que refleja cuanto demora un técnico en resolver cada una de las incidencias de red utilizando en Sistema Automatizado de Gestión comparado a cuanto tardaba en solucionarla sin éste Sistema.

Incidencia	Tiempo estimado (horas) con Sistema de Gestión	Tiempo estimado (horas) sin Sistema de Gestión
Instalación / Desinstalación configuración switches	3	4
IP duplicada	2	8
No se establece conexión	3.5	4
No se inicia sesión	2.5	3
Mal diseño de red	2	8
Fallas generales	4	8
Fallas conexión servidores	6	8
Saturación de puertos	8	16
Total horas	31	59

Tabla 42: Tiempo que tarda un técnico en solucionar una incidencia de red
Autor: K. Rodríguez y S. Hernández

Como se observa la instalación, desinstalación y configuración de switches mejoraron un 25% en los tiempos de solución, ya que, aunque el técnico debe trasladarse obligatoriamente hasta el cuarto de cableado, las solicitudes escalan entre los diferentes niveles de soporte establecidos en el Sistema, para brindar mejores tiempos de repuesta.

Cuando ocurren incidencias relacionadas con la duplicidad en direcciones IP, el Sistema Automatizado de Gestión proporciona al técnico las direcciones IPs asociadas a todos los dispositivos de la Organización, por ello, los tiempos en detectar este tipo de incidencias mejoraron en un 75%. Cuando no se contaba con ésta información el técnico debía consultar la dirección IP de todas las estaciones de trabajo y servidores existentes dentro de la Organización, por lo que los tiempos en solucionar estas incidencias resultaban bastante elevados, aproximadamente un día laboral. Si la duplicidad de direcciones IP se presentaba en servidores, los servicios quedaban completamente detenidos, retrasando así procedimientos importantes de la Organización.

Las fallas en conexión a los servidores mejoraron un 25% en tiempos y las relacionadas con el diseño de la red un 75%, debido a que el Sistema Automatizado de Gestión ofrece amplia información sobre el estado actual de la red, los switches, los puertos a los cuales se encuentran conectados los múltiples usuarios y la topología de red implementada, ésta información facilita la detección del inconveniente presentado.

Fallas en generales relacionadas con software mejoraron en tiempo un 50% gracias a toda la información que brinda el Sistema Automatizado de Gestión al técnico y el conocimiento que adquiere el mismo a través de la base de conocimiento, donde encuentra la documentación necesaria para dar solución rápida a inconvenientes frecuentes.

Las horas empleadas por los técnicos en resolver incidencias de red sin contar con el Sistema Automatizado de Gestión llegaron a 59 horas, mientras que contando con este Sistema desarrollado existe un aproximado de 31 horas, lo cual proporciona una mejora del 47,45 % en los tiempos de solución.

En la tabla 43 observamos un aproximado en tiempo que refleja cuantas horas demora un técnico en resolver cada una de las incidencias de hardware

Incidencia	Tiempo estimado (horas) con Sistema de Gestión	Tiempo estimado (horas) sin Sistema de Gestión
Fallas monitor	2,5	3
Fallas disco duro	7,5	10
Fallas CPU	11,25	15
Fallas teclado/ Mouse	0,75	1
Fallas Tarjeta madre	0,75	4
Fallas Tarjeta sonido/ video	3	4
No enciende / apaga el equipo	5	5
Fallas Unidad CD / floppy	3	4
Total horas	33,75	46

Tabla 43: Tiempo que tarda un técnico en solucionar una incidencia de hardware
Autor: K. Rodríguez y S. Hernández.

Como se observa las fallas en hardware mejoraron en tiempo un 25%, debido a que el Sistema Automatizado de Gestión sólo ofrece amplia información las características básicas del hardware encontrado en cada una de las estaciones de trabajo de los usuarios de la Organización, todo el tiempo empleado en cambios de dispositivos por parte de los técnicos se mantiene.

Las horas empleadas por los técnicos en resolver incidencias de hardware sin contar con el Sistema Automatizado de Gestión llegaron a 46 horas, mientras que contando con la información proporcionada con este Sistema desarrollado existe un aproximado de 33,75 horas, lo cual proporciona una mejora del 26,64 % en los tiempos de solucionarlas.

4.1.4.2 Resultados de Inventario

1. El número de componentes activos de red detectados se detalla a continuación:
 - a. Número total de switches: 17
 - b. Número total de concentradores: 33
2. Por cada switch se obtuvo la siguiente información:
3. Direcciones Capa-2 (MAC Address) de los dispositivos que se encuentran conectados a él.
4. Velocidad a la cual se encuentran transmitiendo cada uno de los puertos.
5. Vlan asociada al puerto.
6. Ultima fecha de inventario.
7. Información del modelo, Sistema operativo y ubicación.

La figura 28 presenta la vista del Sistema propuesto mostrando el listado de switches inventariados:

^ Lista de Switches

Switch	Descripcion	MAC	Sistema Operativo	Ultimo inventario
172.16.12.10	Business Policy Switch 2000 HW:10 FW:3.6.0.1 SW:v3.2.1.04 ISVN:3	00:04:dc:80:83:01	boss	2008-07-07 00:02:46
172.20.100.10	BayStack 350-12T HW:RevL FW:V1.47 SW:v3.1.0.22 ISVN:1	00:03:42:f7:5b:21	baystack	2008-07-07 00:02:55
172.16.40.1	Business Policy Switch 2000 HW:07 FW:2.5.0.3 SW:v3.2.1.04 ISVN:3	00:04:38:f7:fa:41	boss	2008-07-07 00:03:04
172.16.12.9	Business Policy Switch 2000 HW:11 FW:3.6.0.1 SW:v3.2.1.04 ISVN:3	00:09:97:a6:10:81	boss	2008-06-23 06:01:42
172.20.100.12	BayStack 460 - 24T - PWR HW:07 FW:3.0.0.5 SW:v3.0.6.08 ISVN:2	00:12:83:ff:61:41	boss	2008-07-07 00:01:26
172.16.30.1	Business Policy Switch 2000 HW:03 FW:3.6.0.1 SW:v2.5.2.04 ISVN:2	00:03:42:9b:d9:41	baystack	2008-07-07 00:01:35
172.20.100.11	Business Policy Switch 2000 HW:11 FW:3.6.0.1 SW:v2.5.2.04 ISVN:2	00:04:38:e9:a5:61	baystack	2008-07-07 00:01:44
172.16.50.1	Business Policy Switch 2000 HW:14 FW:3.6.0.1 SW:v2.5.2.04 ISVN:2	00:01:81:eb:2d:e1	baystack	2008-06-23 06:00:43
172.16.40.3	BayStack 350-12T HW:RevL FW:V1.47 SW:v3.1.0.22 ISVN:1	00:03:42:f7:6f:61	baystack	2008-06-23 06:00:55
172.16.80.1	Business Policy Switch 2000 HW:14 FW:3.6.0.1 SW:v2.5.2.04 ISVN:2	00:09:97:28:d7:41	baystack	2008-06-23 06:01:53
172.16.40.2	Business Policy Switch 2000 HW:03 FW:3.6.0.1 SW:v2.5.2.04 ISVN:2	00:03:42:e6:99:81	baystack	2008-07-07 00:00:01
172.20.100.13	BayStack 350-12T HW:RevL FW:V1.47 SW:v3.1.0.22 ISVN:1	00:03:42:f7:6a:01	baystack	2008-07-07 00:00:34
172.20.100.8	Business Policy Switch 2000 HW:14 FW:3.6.0.1 SW:v2.5.2.04 ISVN:2	00:04:dc:fff:b2:81	baystack	2008-07-07 00:00:44
172.16.10.244	BayStack 325-24T HW:02 FW:3.0.0.3 SW:v3.0.0.16	00:14:c7:f6:88:01	baystack	2008-07-07 00:01:17
172.20.100.9	Business Policy Switch 2000 HW:11 FW:3.6.0.1 SW:v3.1.8.12 ISVN:3	00:04:dc:81:6f:21	boss	2008-07-07 00:01:53
172.16.12.191	Ethernet Switch 470-24T-PWR HW:01 FW:3.6.0.6 SW:v3.6.2.04 BN:4 ISVN:2 (c) Nortel Networks	00:16:60:82:ff:61	boss	2008-07-07 00:03:14
172.20.100.7	Business Policy Switch 2000 HW:03 FW:3.6.0.1 SW:v3.1.8.12 ISVN:3	00:01:81:eb:88:21	boss	2008-07-07 00:03:23

Número total de Switches: 17

Figura 28: Listado de switches inventariados.

Origen: Sistema Automatizado de Gestión

Por cada uno de los switches se registra modelo, Sistema operativo, vlan asociada al puerto, estado del puerto, velocidad de transferencia, vlan y fecha del último inventario.

Service Desk. Resumen de casos

Editar

^ Informacion del dispositivo 172.20.100.10

Contacto	Ubicacion	MAC	Modelo	Sistema Operativo	Fecha ultimo discovery
Sergio Hernandez		00:03:42:f7:5b:21	350	baystack	2008-07-06 09:02:59

^ Lista de puertos del Switch 172.20.100.10

Puerto	Estado	Velocidad de transferencia	Vlan	Fecha del ultimo inventario
1.1	up	100 Mbps	1	2008-07-06 09:03:03.003091
1.10	down	100 Mbps	1	2008-07-06 09:03:03.004479
1.11	up	100 Mbps	1	2008-07-06 09:03:02.992006
1.12	up	100 Mbps	1	2008-07-06 09:03:02.998903
1.2	down	100 Mbps	1	2008-07-06 09:03:02.997473
1.3	up	100 Mbps	1	2008-07-06 09:03:02.99338
1.4	up	100 Mbps	1	2008-07-06 09:03:03.001712
1.5	up	10 Mbps	1	2008-07-06 09:03:03.006075
1.6	up	100 Mbps	1	2008-07-06 09:03:02.989225
1.7	down	100 Mbps	1	2008-07-06 09:03:02.99477
1.8	up	100 Mbps	1	2008-07-06 09:03:03.000336
1.9	up	100 Mbps	1	2008-07-06 09:03:02.996103

Tiempo de respuesta: 0.045324

UN SISTEMA AUTOMATIZADO PARA LA GESTION DE SOLICITUDES EN TECNOLOGIAS DE INFORMACION

Figura 29: Listado de información de los switches inventariados.

Origen: Sistema Automatizado de Gestión

La figura 30 muestra el mapa de la topología de red construido por el Sistema Automatizado de Gestión:

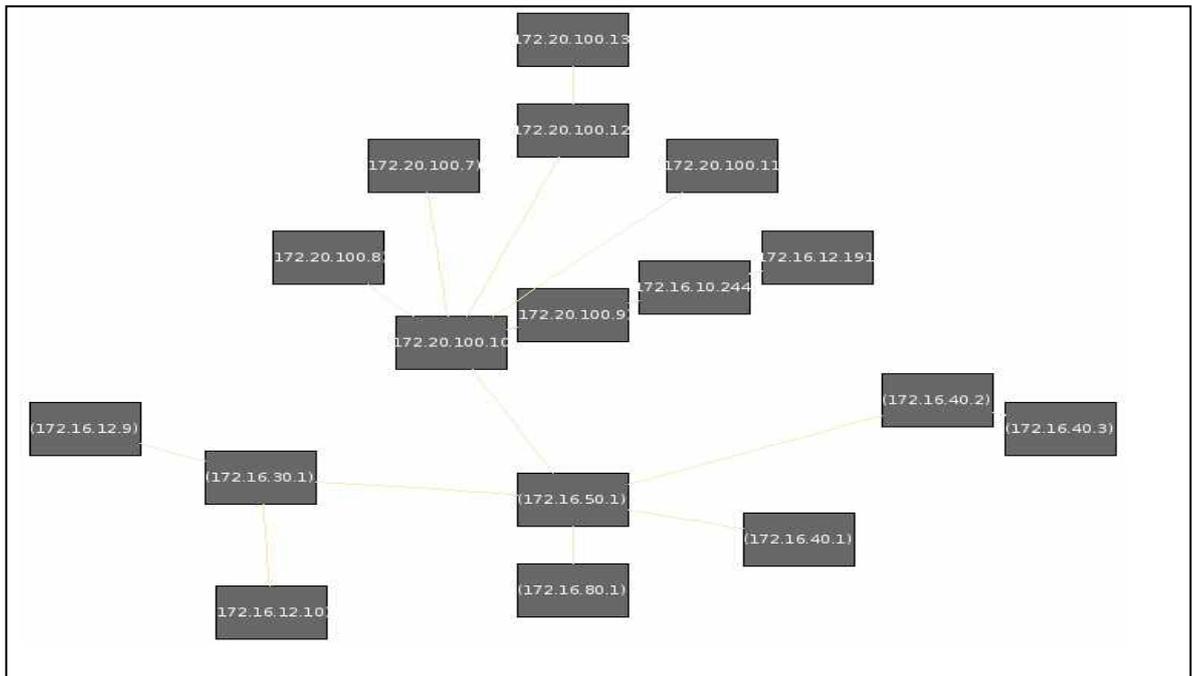


Figura 30: Topología de red Organización Ingedigit.

Origen: Sistema Automatizado de Gestión

Aquellos puertos de un switch que tienen conexión con un concentrador muestran más de una dirección Capa-2.

8. La información de Hardware proporcionada por el Sistema:

- Unidades de almacenamiento
- Monitor
- Tarjeta de red
- Memoria Principal
- Controladores
- Disco duro
- Procesador.

9. La información de Software proporcionada por el Sistema:

- Sistema Operativo
- Diferentes paquetes de software: por ejemplo suite ofimática
- Anti-Virus
- Versión y descripción del paquete de software instalado

Lista de Hosts

Host	Sistema Operativo	Usuario	Memoria(MB)	Procesador(MHz)
172.20.130.5	Linux		60	348
172.20.40.2	Microsoft Windows XP Professional	btineo	512	2934
172.16.18.39	Linux		3291	1995
172.16.18.33	Linux	geekbynature	471	3401
172.16.18.32	Linux	geekbynature/root	471	3400
172.16.18.33	Linux	desarrollo	471	3400
172.16.10.156	Microsoft Windows XP Professional	daniel	992	1792
172.16.10.34	Microsoft Windows 2000 Professional	fsoto	224	1792
172.16.18.33	Linux	katty	471	3400
172.20.100.87	Microsoft Windows Vista Home Premium	jefferson marcano	2048	1500
172.16.11.52	Microsoft Windows XP Professional	jdelaacruz	512	2992
172.16.10.230	Microsoft Windows 2000 Professional	mfreites	736	2400
172.16.10.230	Microsoft Windows 2000 Professional	mfreites	736	2400
172.16.10.207	Microsoft Windows XP Professional	ncisneros	448	1062
172.16.13.2	Microsoft Windows 2000 Professional	rnunes	736	1792
172.16.18.88	Microsoft Windows Server 2003 Standard Edition	conectividad	1024	2999
172.20.190.2	Microsoft Windows 2000 Professional	Administrador	192	348
172.20.190.3	Microsoft Windows XP Professional	arperez	512	1792
172.20.190.3	Microsoft Windows XP Professional	Administrador	512	1792
172.20.190.4	Microsoft Windows XP Professional	shernandez	256	334
172.20.190.4	Microsoft Windows XP Professional	Administrador	256	334
172.20.190.5	Microsoft Windows XP Professional	jpamphile	495	1399
172.20.190.6	Microsoft Windows XP Professional	ssarmiento	512	2399
172.20.190.6	Microsoft Windows XP Professional	Administrador	512	2399
172.20.50.1	Microsoft Windows XP Professional	lcalanche	447	2009
172.20.50.1	Microsoft Windows XP Professional	Administrador	447	2009
172.20.50.3	Microsoft Windows XP Professional	hkenny	1015	2660
223.1.1.128	Microsoft Windows XP Professional	mliscano	960	1999
223.1.1.128	Microsoft Windows XP Professional	Administrador	960	1999

Figura 31: Listado de información de las estaciones de trabajo inventariadas
Origen: Sistema Automatizado de Gestión

10. El Sistema de gestión detecta los cambios ocurridos en cuanto a: Software, Hardware, información Bios, memoria, controladores, monitores, almacenamiento, drivers, modems, tarjeta de red, tarjeta sonido, tarjeta videos, impresoras.

4.2 Ambiente 2: Grupo Ingedigit C.A. Edificio Folgana, Piso 5.

El ambiente de prueba 2 se encuentra localizado en el edificio Folgana piso 5 del Grupo Ingedigit C.A.

Descripción del Hardware y Software. Las tablas a continuación detallan las especificaciones técnicas del primer ambiente de pruebas donde se ejecutó la aplicación.

Hardware

Componente	Versión/Valor
CPU	Pentium D
Memoria principal	512 MB
Memoria en disco	80 GB
Tarjeta de red (NIC)	10/100 Mbps

Tabla 44:Componentes de Hardware ambiente 2

Autor: K.Rodríguez y S.Hernández. Año 2008

Software

Componente	Versión/Valor
Sistema Operativo	Debian Etch 4.0
Kernel	2.6.18-4-686
Perl	5.8.8
SNMP::Info	0.9
Net-SNMP	5.2.3
PHP	5.2.0
Apache	2.2.3
PostgreSQL	8.1.11
MySQL	5.0.32
Netdisco	0.95
Ocs-Inventory	1.0.1.2
Request-Tracker	3.6

Tabla 45 :Componentes de Software ambiente 2

Autor: K.Rodríguez y S.Hernández. Año 2008

Para la ejecución y prueba de éste ambiente se utilizará la misma red de datos empleada en el ambiente de prueba 1.

4.2.1 Resultados esperados

Los resultados esperados se clasificaron de acuerdo a los distintos módulos que conforman el Sistema propuesto y son los mismos establecidos para el ambiente de prueba 1.

4.2.2 Resultados encontrados con el Sistema automatizado de gestión

A continuación se encuentran los resultados obtenidos a través del Sistema automatizado de gestión dentro de la Organización Ingedigit en el ambiente de prueba 2, destacando reconocimiento de la red, configuraciones de equipos y gestión de incidencias presentadas en un período de un mes (Julio).

La frecuencia de las incidencias fue tomada como número de incidencias ocurridas en el mes evaluado.

4.2.2.1 Información de gestión

El siguiente análisis muestra un estudio sobre la gestión de incidencias dentro de la Organización Ingedigit, donde se evaluaron dos factores: tipo de incidencias ocurridas, tiempo de solución de las mismas por parte de los técnicos y escalamiento automático de solicitudes a través del módulo de service desk presente en el Sistema desarrollado.

Tipos de Incidencias ocurridas

En la tabla 46 se observa la frecuencia por cada tipo de incidencia ocurrida en la Organización, en el período de un mes, de un total de 93 incidencias resaltan con mayor porcentaje las incidencias productos de fallas en software con 70,96% de los casos, 22,58% para fallas de red y un 6,45% para fallas en hardware.

Incidencia	Frecuencia
Software	66
Red	21
Hardware	6

Tabla 46: Frecuencia de Incidencias ocurridas

Autor: K. Rodríguez y S. Hernández

En la figura 32 se observa una gráfica en barras que representa las incidencias ocurridas en la Organización en el mes de Julio y evaluadas en el ambiente de prueba 2

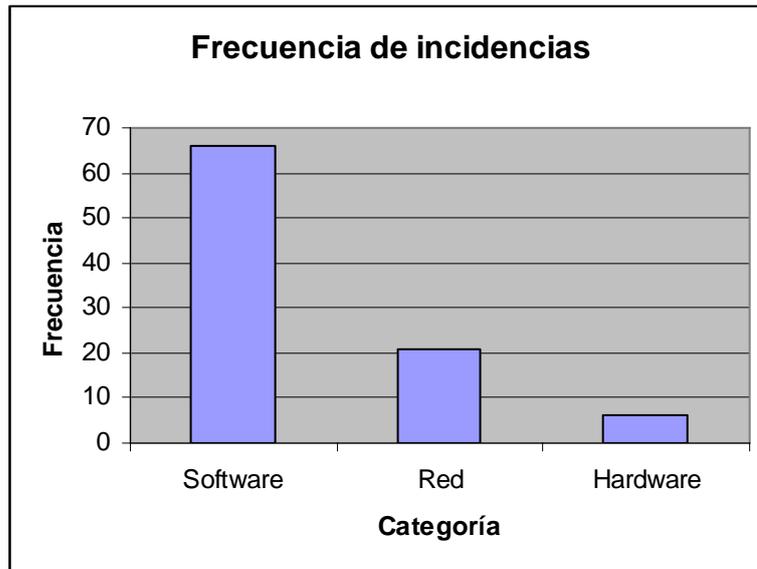


Figura 32: Frecuencia de Incidencias ambiente 2
Autor: K. Rodríguez y S. Hernández

En la tabla 47 y en la figura 33 se observan en detalle los tipos de fallas de software más frecuentes dentro de la Organización.

Incidencia	Frecuencia
Instalación / Desinstalación	4
Configuración / Actualización	16
Problemas con Sistema Operativo	12
Problemas con correo	4
Virus / Spyware / Troyano	39
Fallas generales	8
Configurar perfil	11
Problemas para imprimir	6

Tabla 47: Frecuencia de Incidencias de software
Autor: K. Rodríguez y S. Hernández

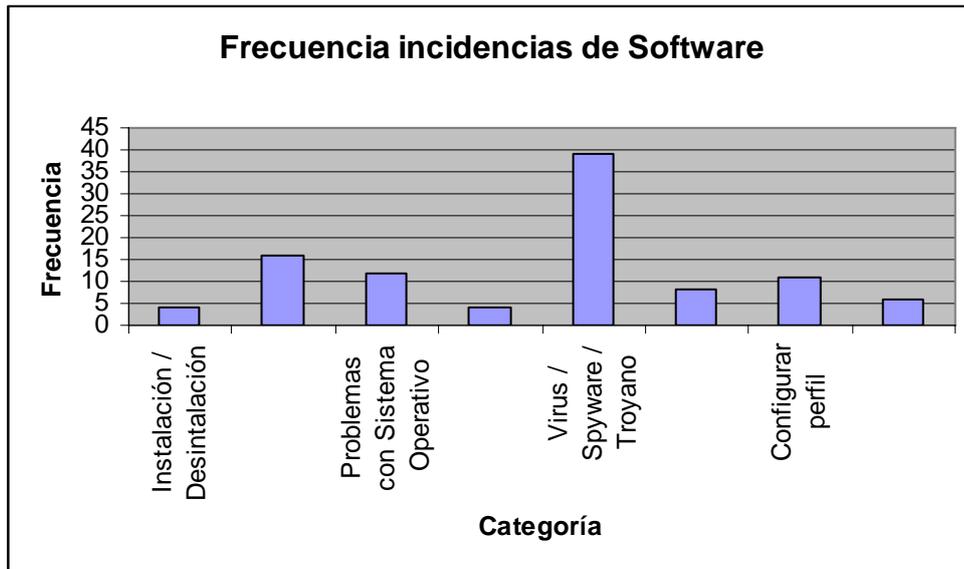


Figura 33: Frecuencia de Incidencias de software.
Autor K. Rodríguez y S. Hernández

En la tabla 48 y en la figura 34 se observan en detalle los tipos de fallas de red más frecuentes dentro de la Organización.

Incidencia	Frecuencia
Instalación / Desinstalación / configuración switches	7
Dirección IP duplicada	13
No se establece conexión	6
No se inicia sesión	7
Mal diseño de red	12
Fallas generales	11
Fallas conexión servidores	11
Saturación de puertos	33

Tabla 48: Frecuencia de Incidencias de red
Autor: K. Rodríguez y S. Hernández

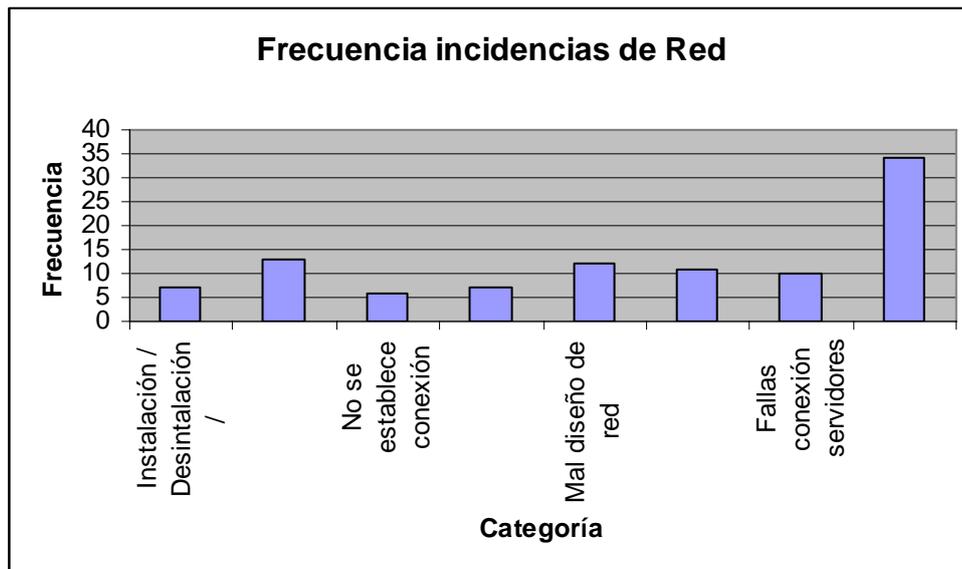


Figura 34: Frecuencia de Incidencias de red.
Autor K. Rodríguez y S. Hernández

En la tabla 49 y en la figura 35 se observan en detalle los tipos de fallas de hardware más frecuentes dentro de la Organización.

Incidencia	Frecuencia
Fallas monitor	2
Fallas disco duro	8
Fallas CPU	7
Fallas teclado/ Mouse	7
Fallas Tarjeta madre	19
Fallas Tarjeta sonido/ video	10
No enciende / apaga el equipo	39
Fallas Unidad CD / floppy	8

Tabla 49: Frecuencia de Incidencias de hardware
Autor: K. Rodríguez y S. Hernández

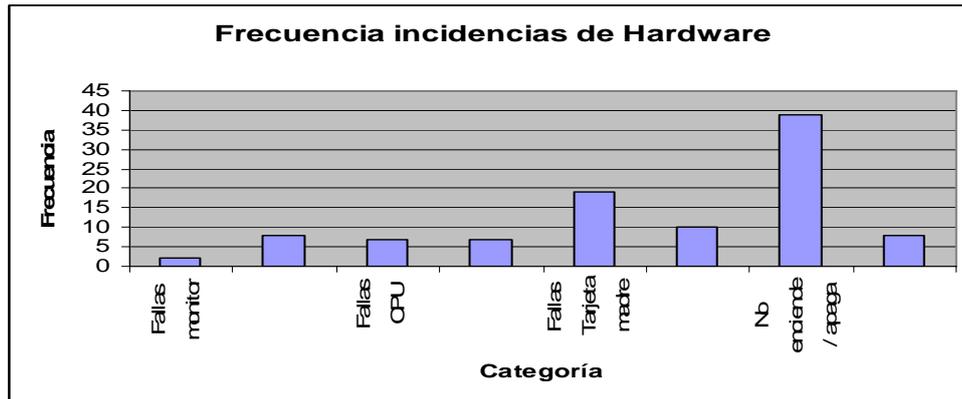


Figura 35: Frecuencia de Incidencias de hardware.
Autor K. Rodríguez y S. Hernández

4.2.2.2 Tiempo empleado por los técnicos en dar solución a una incidencia

A continuación se detalla un aproximado del tiempo empleado por los en solucionar cada una de las incidencias de software, hardware y red dentro de la Organización bajo el ambiente de prueba 2, haciendo uso del Sistema Automatizado de Gestión conformado por una base de conocimientos y escalamiento de incidencias entre diferentes niveles de soporte.

En la tabla 50 observamos un aproximado en tiempo que refleja cuanto demora un técnico en resolver cada una de las incidencias de software utilizando en Sistema de Gestión comparado a cuanto tardaba en solucionarla sin este Sistema.

Incidencia	Tiempo estimado (horas) con Sistema de Gestión	Tiempo estimado (horas) sin Sistema de Gestión
Instalación / desinstalación	0,75	1
Configuración / Actualización	0,75	1
Problemas con Sistema Operativo	6	8
Problemas con correo	3,5	4
Virus / Spyware / Troyano	3	8
Fallas generales	6	8
Configurar perfil	1	1
Problemas para imprimir	3	3
Total horas	23	34

Tabla 50: Tiempo que tarda un técnico en solucionar una incidencia de software
Autor: K. Rodríguez y S. Hernández

Como se observa las instalaciones, desinstalaciones, configuraciones, actualizaciones de paquetes y fallas en generales mejoraron un 25% en los tiempos de solución al usuario, ya que aunque el técnico debe trasladarse obligatoriamente hasta la estación de trabajo del usuario, las solicitudes pueden escalar entre los niveles de soporte del Sistema para brindar mejores tiempos de repuesta.

Las incidencias relacionadas con problemas en Sistemas Operativos mejoraron en tiempo un 25% debido a que el Sistema Automatizado de Gestión permite detectar la versión de Sistema Operativo instalado, los parches y actualizaciones que posee la estación de trabajo afectada.

De esta forma el técnico puede conocer que Sistema y cuales actualizaciones deben instalarse nuevamente, puede también identificar cual fue la última actualización realizada a ese equipo y concluir si esta o cualquier otro software recientemente instalado dañó la configuración del Sistema Operativo.

Las fallas con problemas de virus, troyanos y spyware mejoraron 62,5% ya que el Sistema automatizado de gestión permite a los técnicos conocer las últimas descargas de software existente en el equipo afectado para detectar aquellas que pudiesen ocasionar los problemas anteriormente señalados.

Adicionalmente los técnicos pueden verificar si el equipo requiere actualizaciones de seguridad o parches para estar protegido en la Web ya que el Sistema ofrece la información del software y parches instalados.

Las horas empleadas por los técnicos en resolver incidencias de software sin contar con el Sistema Automatizado de Gestión llegaron a 34 horas, mientras que contando con este Sistema desarrollado existe un aproximado de 23 horas, lo cual proporciona una mejora del 32,36 % en los tiempos de solucionarlas.

En la tabla 51 observamos un aproximado en tiempo que refleja cuanto demora un técnico en resolver cada una de las incidencias de red utilizando en Sistema Automatizado de Gestión comparado a cuanto tardaba en solucionarla sin éste Sistema.

Incidencia	Tiempo estimado (horas) con Sistema de Gestión	Tiempo estimado (horas) sin Sistema de Gestión
Instalación / Desinstalación configuración switches	3,5	4
IP duplicada	2	8
No se establece conexión	4	4
No se inicia sesión	2.5	3
Mal diseño de red	5	8
Fallas generales	6	8
Fallas conexión servidores	5	8
Saturación de puertos	9	16
Total horas	37	59

Tabla 51: Tiempo que tarda un técnico en solucionar una incidencia de red
Autor: K. Rodríguez y S. Hernández

Como se observa la instalación, desinstalación y configuración de switches mejoraron un 12,5% en los tiempos de solución, ya que, aunque el técnico debe trasladarse obligatoriamente hasta el cuarto de cableado, las solicitudes pueden escalar entre los diferentes niveles de soporte establecidos en el Sistema, para brindar mejores tiempos de repuesta.

Cuando ocurren incidencias relacionadas con la duplicidad en direcciones IP, el Sistema Automatizado de Gestión proporciona al técnico las direcciones IPs asociadas a todos los dispositivos de la Organización, por ello, los tiempos en detectar este tipo de incidencias mejoraron en un 75%. Cuando no se contaba con ésta información el técnico debía consultar la dirección IP de todas las estaciones de trabajo y servidores existentes dentro de la Organización, por lo que los tiempos en solucionar estas incidencias resultaban bastante elevados, aproximadamente un día laboral. Si la duplicidad de direcciones IP se presentaba en servidores, los servicios quedaban completamente detenidos, retrasando así procedimientos importantes de la Organización.

Las fallas en conexión a los servidores y las relacionadas con el diseño de la red mejoraron un 37,5% en tiempos, debido a que el Sistema Automatizado de Gestión ofrece amplia información sobre el estado actual de la red, los switches, los puertos a los cuales se encuentran conectados los múltiples usuarios y la topología de red implementada, ésta información facilita la detección del inconveniente presentado.

Fallas en generales relacionadas con software y las relacionadas no establecer conexión mejoraron en tiempo un 25% gracias a toda la información que brinda el Sistema Automatizado de Gestión al técnico y el conocimiento que adquiere el mismo a través de la base de conocimiento, donde encuentra la documentación necesaria para dar solución rápida a inconvenientes frecuentes.

Las horas empleadas por los técnicos en resolver incidencias de red sin contar con el Sistema Automatizado de Gestión llegaron a 59 horas, mientras que contando con este Sistema desarrollado existe un aproximado de 37 horas, lo cual proporciona una mejora del 37,28% en los tiempos de solucionarlas.

En la tabla 52 observamos un aproximado en tiempo que refleja cuantas horas demora un técnico en resolver cada una de las incidencias de hardware

Incidencia	Tiempo estimado (horas) con Sistema de Gestión	Tiempo estimado (horas) sin Sistema de Gestión
Fallas monitor	3	3
Fallas disco duro	8	10
Fallas CPU	11	15
Fallas teclado/ Mouse	0,75	1
Fallas Tarjeta madre	0,25	4
Fallas Tarjeta sonido/ video	3	4
No enciende / apaga el equipo	5	5
Fallas Unidad CD / floppy	3	4
Total horas	33,75	46

Tabla 52: Tiempo que tarda un técnico en solucionar una incidencia de hardware
Autor: K. Rodríguez y S. Hernández.

Como se observa las fallas en hardware mejoraron en tiempo un aproximado entre 15 y 25%, debido a que el Sistema Automatizado de Gestión sólo ofrece amplia información las características básicas del hardware encontrado en cada una de las estaciones de trabajo de los usuarios de la Organización, todo el tiempo empleado en cambios de dispositivos por parte de los técnicos se mantiene.

Las horas empleadas por los técnicos en resolver incidencias de hardware sin contar con el Sistema Automatizado de Gestión llegaron a 46 horas, mientras que contando con la información proporcionada con este Sistema desarrollado existe un aproximado de 34 horas, lo cual proporciona una mejora del 26,086 % en los tiempos de solucionarlas.

Con respecto a los resultado obtenidos en cuanto a inventario el Sistema arrojó los mismos resultados encontrados en la ejecución mediante el ambiente de prueba 1, ya que se contaba con la misma topología de red, mismo cableado y dispositivos activos.

CAPÍTULO 5 CONCLUSIONES

El diseño e implementación de una herramienta para automatizar la gestión de solicitudes en tecnologías de información es un reto complejo, dado a los niveles de exigencia cada vez mayores en el mercado actual.

Con este trabajo especial de grado se muestra la manera en que es posible integrar un conjunto de herramientas basadas en Software Libre enfocadas en automatizar la gestión de solicitudes en tecnologías de información, permitiendo una adecuada gestión de incidencias e inventario de activos y dispositivos conectados a la red. Además facilita el manejo y minimiza la complejidad a los usuarios, es novedosa, orientada al Web, segura y robusta, gracias a que ofrece un diseño completamente modular, si la operación de un módulo falla la herramienta no deja de funcionar. Está pensada para ser escalable y fácil de adaptar, pese a ser una solución pensada para la empresa Ingedigit C.A., puede correr bajo cualquier red sin importar las dimensiones de la red ni la cantidad de dispositivos conectados a ella.

La lógica se encuentra bien diferenciada del modelo de datos lo que hace sencillo la modificación del código fuente y la adición de nuevas funcionalidades.

Es portable, ya que se empleó el lenguaje de programación Perl cuya máquina virtual funciona en muchas más plataformas que la actual máquina virtual de Java.

La lógica que se sigue en el Sistema para las solicitudes pasa normalmente por tres procesos principales, que permiten identificar, analizar y satisfacer las necesidades del usuario, estos procesos son:

1. Captura
2. Escalamiento
3. Seguimiento y solución de las incidencias

Otros procesos que se siguen, sirven de apoyo a los procesos principales y son definidos de acuerdo a las necesidades del servicio que se brinda, estos son:

1. Administración de activos.
2. Capacitación.
3. Administración de los cambios.

Se distinguen también áreas funcionales que están conformadas por herramientas y conceptos tecnológicos que permiten la realización de las necesidades del servicio que brinda el Sistema. Estas áreas son:

1. Herramientas generadoras de reportes.
2. Base de conocimiento
3. Integración.

La utilización de este Sistema permite principalmente:

1. Mejora en la calidad del servicio
2. Mejora en los tiempos de respuesta al usuario
3. Incremento de productividad en los departamentos asociados a la atención al usuario.
4. Mejora en la satisfacción de los usuarios.
5. Incremento en el retorno de inversión.
6. Reducción en el costo de calidad.
7. Mejora en la planificación del mantenimiento.

5.1 Resumen de Resultados encontrados

En resumen señalamos las mejoras en cuanto a la gestión de incidencias encontradas en la Organización, utilizando el Sistema desarrollado en los dos ambientes de pruebas:

Incidencia	Mejora en ambiente 1	Mejora en ambiente 2
Software	37,50%	32,36%
Hardware	26,64%	26,086%
Red	47,45%	37,28%

Tabla 53: Mejoras en porcentajes encontradas con el Sistema automatizado de gestión

Autor: K. Rodríguez y S. Hernández

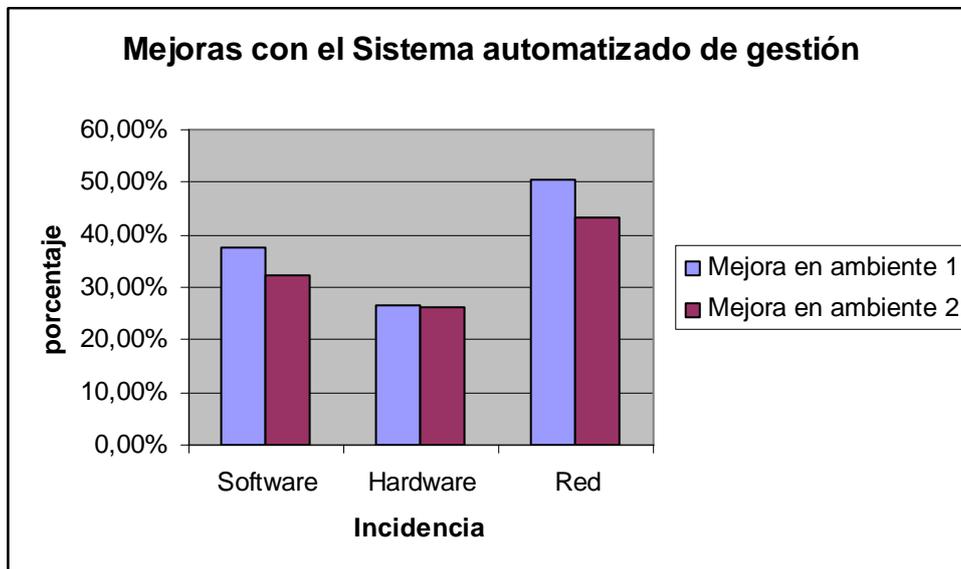


Figura 36: Mejoras con el Sistema automatizado de gestión.

Autor: K.Rodríguez, S.Hernández

Las incidencias más comunes en la Organización Ingedigit C.A son las relacionadas con software y red, debido a que no existía un control sobre las mismas, es decir, los activos de red se encuentran dispersos y sin ningún tipo de inventario que pudiera informar a los administradores y técnicos como se maneja

el flujo de datos y además no se sabía la configuración básica de las estaciones de trabajo de cada uno de los usuarios al momento de presentarse un inconveniente. Como observamos utilizando el Sistema desarrollado existe una mejora entre 32,36% y 37,50% en brindar solución a las incidencias relacionadas con software y un 47,45% a 37,28% en solucionar las de red, éstos valores presentan una ventaja importante en la Organización, que minimiza en gran medida el tiempo empleado en solucionar las mismas.

Las incidencias de hardware presentaron una mejora similar en ambos ambientes entre 26,086% y 26,64%, debido a que el factor principal que minimiza los tiempos en solucionarlas es el escalamiento automático de las solicitudes dentro del Sistema. Entre ambos ambientes de pruebas el sistema ofrece una mejora en la gestión de solicitudes en gestión de tecnologías de información de 34,55 %. En los tiempos de solución a las incidencias.

Es importante destacar que los porcentajes de mejora difieren en los ambientes no por estar ejecutándose en plataformas diferentes sino por el número de incidencias registradas y atendidas en esos meses de prueba.

La información de inventario en cuanto a hardware, software y activos de red proporcionada por Sistema, posee toda la esperada por la Organización y además cuenta con datos adicionales que permiten aumentar el conocimiento de los técnicos al resolver una incidencia.

Entre la información brindada por el Sistema encontramos:

1. Inventario de estaciones de trabajos.
2. Software.
3. Hardware
4. Activos y topología de la red.

Un factor importante es el escalamiento automático de solicitudes entre los diferentes niveles de soporte establecidos, para no permitir el retraso en atender alguna solicitud. Este módulo permitió disminuir el tiempo de una incidencia dentro del Sistema y aumentar la rapidez en que es proporcionada solución al usuario.

La base de conocimientos construida con el uso del Sistema proporciona la información necesaria a referencias y a soluciones pasadas, permitiendo al técnico consultar ésta información antes de dar solución a una incidencia que desconoce.

El reporte de los cambios ocurridos en la configuración de los equipos, es un factor que permite controlar todos los activos encontrados dentro de la organización.

Por medio de los resultados obtenidos en la implementación del Sistema automatizado de gestión en los dos ambientes de prueba, podemos concluir que éste Sistema brinda gran cantidad de conocimientos a los técnicos y

administradores de la red para el momento de dar solución al conjunto de incidencias presentadas, minimiza los tiempos y aumenta la productividad del departamento de atención a usuarios.

Es importante señalar que aunque el técnico tenga que trasladarse hasta el lugar de la incidencia en muchos casos para poder solucionarla, éste cuenta con el conocimiento de la configuración básica de equipo afectado, lo cual equivale a una información valiosa y difícil de obtener si no se cuenta con mecanismos apropiados.

Mientras mas informado se encuentre un técnico sobre el problema presentado más rápido podrá solventar el mismo, minimizando así los tiempos de respuesta a los usuarios y aumentando la satisfacción de los mismo.

5.2 Trabajos futuros y limitaciones

A pesar de que el Sistema ofrece funciones importantes dentro de la administración de redes, se tiene algunas líneas de trabajo a futuro con el objeto de fortalecer las características orientadas a la administración de redes, entre ellas:

1. Crear un módulo que permita el control de los servicios ofrecidos por los servidores.
2. Crear un módulo para el procesamiento automatizado de alertas vía el protocolo SNMP.
3. Crear un módulo para el análisis de Logs de cada uno de los activos, estaciones de trabajo y servidores conectados a la red. Que permita la notificación automática a los administradores.
4. Crear un módulo para el nivel adicional de administración que requieren las VLANs.
5. Crear un módulo que permita el monitoreo de tráfico en la red.
6. Creación de un nuevo módulo que permita administrar las Bases de datos desde la interfaz Web del Sistema.
7. Incrementar las clases SNMP::Info para incrementar la cantidad de dispositivos de red soportados.
8. Implementar una función que permita almacenar el historial de cambios que se realicen sobre la topología de la red.
9. Implementar una función que permita graficar los concentradores presentes en la red.
10. Implementar una función de búsqueda que indique la posición de un cierto nodo en el gráfico de la red.

11. Implementar un gráfico de red que permita la navegación a través de sus nodos.
12. Una de las limitaciones del Sistema es que no muestra de forma explícita la presencia de concentradores, al observar que existe más de una dirección MAC en un puerto se sabe que allí se encuentra conectado un concentrador.
13. Otra limitación la encontramos con la marca del dispositivo activo la cual no se obtiene, este punto podría ser tomado en cuenta para un desarrollo a futuro.

Para implementar las nuevas características de visualización del gráfico de red se sugiere emplear patrones de diseño orientados a objeto, los cuales permitirían asignar la información deseada a los nuevos métodos de visualización.

5.3 Dificultades encontradas en la implementación del Sistema

Las principales dificultades que se encontraron para la implementación del Sistema se deben al ambiente tecnológico heterogéneo que predomina en las redes, esto es, gran cantidad de dispositivos de distintos fabricantes para el caso de los activos de red, gran cantidad de tipos y versiones de Sistemas operativos, componentes de hardware y software y múltiples servicios de distinta naturaleza ejecutándose tanto en servidores como en estaciones de trabajo.

La situación anterior obligó a pasar por un largo período de búsqueda y análisis de las herramientas necesarias lograr una visión global de la plataforma tecnológica y un Sistema automatizado de gestión de solicitudes.

Sumado a lo anterior, se encontró una marcada resistencia al cambio de Sistema por parte de los usuarios (incluyendo los especializados y no especializados) que fue superada gracias a la implementación de una campaña de entrenamiento para el uso del nuevo Sistema y comunicación de las ventajas

ANEXO A PROCEDIMIENTO DE INSTALACION DE OCS-INVENTORY

Para la instalación de módulos, librerías y paquetes de software para OCS-Inventory se realizan los siguientes procedimientos

```
apt-get install libxml-simple-perl
apt-get install libcompress-zlib-perl
apt-get install libdbi-perl
apt-get install libdbd-mysql-perl
apt-get install libapache-dbi-perl
apt-get install libnet-ip-perl
apt-get install libsoap-lite-perl
apt-get install apache2
apt-get install php5
apt-get install perl
apt-get install mysql-server-5.0
apt-get install libphp-pclzip
apt-get install php5-gd
apt-get install libapache2-mod-perl2
apt-get install php5-mysql
```

Para la instalación del servidor se realiza los siguientes procedimientos:

```
# /etc/init.d/apache2 restart
# tar -xzf OCSNG_LINUX_SERVER_1.01.tar.gz
# cd OCSNG_LINUX_SERVER_1.01
# sh setup.sh ó ./setup.sh
```

Se configuran los siguientes parámetros:

Do you wish to continue ([y]/n)? presionar enter ya que la opción "Y" esta por defecto entre corchetes.

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] ? puerto de la base de datos por defecto (3306) presionar enter.

Where is Apache daemon binary [/usr/sbin/apache2] ? presionar enter

Where is Apache main configuration file [//etc/apache2/apache2.conf] ? se debe colocar la ruta correcta que es: /etc/apache2/apache.conf

Which user account is running Apache web server [www-data] ? 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/apache2/conf.d/]
```

```
? colocar la ruta correcta: /etc/apache2/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/
```

Configuración del archivo principal del servidor Web apache: se edita el archivo /etc/apache2/apache2.conf con el siguiente comando #nano

```
/etc/apache2/apache2.conf y sobre la línea: ServerRoot "/etc/apache2"
```

```
escribir ServerName 127.0.0.1
```

```
# /etc/init.d/apache2 restart
```

```
# /etc/init.d/mysql restart
```

ANEXO B PROCEDIMIENTO DE INSTALACION DE REQUEST TRACKER

Para realizar la instalación de los módulos de software necesarios se realizan los siguientes procedimientos

```
apt-get install apache2
apt-get install mysql-server-5.0
apt-get install request-tracker3.6
```

vi /etc/request-tracker3.6/RT_SiteConfig.pm, para configurar los siguientes parámetros:

- Set(\$rtname, 'empresa C.A ').
- Set(\$DatabaseUser , 'rtuser').
- Set(\$DatabasePassword , 'password').
- Set(\$DatabaseName , 'rtdb').
- Set(\$WebPath , "/rt").
- Set(\$WebBaseURL , "http://192.168.0.1").
- Set(\$CorrespondAddress , mail_de_soporte').

```
#vi /etc/apache/httpd.conf.
Include "/etc/request-tracker3/apache-modperl.conf"
```

```
mysql>GRANT ALL PRIVILEGES ON rtdb.* TO rtuser@localhost
IDENTIFIED BY 'password'.
```

```
mysql>FLUSH PRIVILEGES. mysql>quit
```

```
rt-setup-database --action init --dba rtuser --prompt-for-dba-
password.
```

ANEXO C
SCRIPT DE INSTALACIÓN DE NETDISCO
(archivo Install.sh)

```
apt-get install -y apache2 apache2-prefork-dev postgresql-8.1
postgresql-server-dev-8.1 postgresql-client-8.1 snmp snmpd
libbeecrypt6-dev libperl5.8 libperl-dev libsnmp-perl libapache-
mod-ssl libgraphviz-perl libdbi-perl libdbd-pg-perl libapache-
session-perl libexception-class-perl libnet-nbname-perl libheap-
perl libextutils-xsbuilder-perl libparams-validate-perl libclass-
container-perl libcompress-zlib-perl libapache-session-wrapper-
perl libgraph-perl libhtml-mason-perl gcc g++ make ncftp
libapache-dbi-perl

apt-get remove -y libapache2-mod-perl2
sleep 3

# start postgresql
/etc/init.d/postgresql-8.1 start
sleep 3

cp /etc/postgresql/8.1/main/pg_hba.conf
/etc/postgresql/8.1/main/pg_hba.conf.orig
echo "# TYPE DATABASE USER IP-ADDRESS IP-MASK METHOD" >
/etc/postgresql/8.1/main/pg_hba.conf
echo "local all all trust" >> /etc/postgresql/8.1/main/pg_hba.conf
echo "host all all 127.0.0.1 255.255.255.255 trust" >>
/etc/postgresql/8.1/main/pg_hba.conf
/etc/init.d/postgresql-8.1 restart
sleep 3

# Create user netdisco
/usr/sbin/useradd netdisco
/usr/sbin/groupadd netdisco
sleep 3

# netdisco
curdir=`pwd`
wget $NETDISCO
cd /usr/local/
tar zxvf $curdir/netdisco-0.95_with_mibs.tar.gz
mv /usr/local/netdisco-0.95 /usr/local/netdisco
cd $curdir
sleep 3

stty -echo
echo -n "Enter Netdisco Database password: "
read netdisco_passwd
echo ""
stty echo
cat /usr/local/netdisco/netdisco.conf | sed
"s/dbpassword/$netdisco_passwd/g" > /tmp/netdisco.conf.$$
mv -f /tmp/netdisco.conf.$$ /usr/local/netdisco/netdisco.conf
cat /usr/local/netdisco/netdisco_apache.conf | sed
"s/PASSWORDHERE/$netdisco_passwd/g" > /tmp/netdisco_apache.conf.$$
mv -f /tmp/netdisco_apache.conf.$$
/usr/local/netdisco/netdisco_apache.conf
echo -n "Enter domain name: "
```

```

read domain_read
echo ""
cat /usr/local/netdisco/netdisco.conf | sed
"s/mycompany\.com/$domain_read/g" > /tmp/netdisco.conf.$$
mv -f /tmp/netdisco.conf.$$ /usr/local/netdisco/netdisco.conf
#echo -n "Enter SNMP read string: "
read snmp_read
echo ""
cat /usr/local/netdisco/netdisco.conf | sed
"s/public/$snmp_read/g" > /tmp/netdisco.conf.$$
mv -f /tmp/netdisco.conf.$$ /usr/local/netdisco/netdisco.conf
#echo -n "Enter SNMP write string: "
read snmp_write
echo ""
cat /usr/local/netdisco/netdisco.conf | sed
"s/private/$snmp_write/g" > /tmp/netdisco.conf.$$
mv -f /tmp/netdisco.conf.$$ /usr/local/netdisco/netdisco.conf
sleep 3

# Making Apache2 - Modperl2 changes
# Edit Apache Config
echo "Include /usr/local/netdisco/netdisco_apache.conf" >>
/etc/apache2/apache2.conf
echo "Include /usr/local/netdisco/netdisco_apache_dir.conf" >>
/etc/apache2/apache2.conf
#cat /usr/local/netdisco/netdisco_apache.conf | sed 's/#LoadModule
perl_module libexec\/apache2\mod_perl.so/LoadModule perl_module
\usr\lib\apache2\modules\mod_perl.so/' >
/tmp/netdisco_apache.conf.$$
mv -f /tmp/netdisco_apache.conf.$$
/usr/local/netdisco/netdisco_apache.conf
#cat /usr/local/netdisco/netdisco_apache.conf | sed 's/#LoadModule
apreq_module libexec\apache2\mod_apreq2.so/LoadModule
apreq_module \usr\lib\apache2\modules\mod_apreq2.so/' >
/tmp/netdisco_apache.conf.$$
mv -f /tmp/netdisco_apache.conf.$$
/usr/local/netdisco/netdisco_apache.conf
#cat /usr/local/netdisco/netdisco_apache.conf | sed
's/#PerlModule/PerlModule/' > /tmp/netdisco_apache.conf.$$
mv -f /tmp/netdisco_apache.conf.$$
/usr/local/netdisco/netdisco_apache.conf
#cat /usr/local/netdisco/html/autohandler | sed 's/$r->connection-
>user/$r->user/' > /tmp/autohandler.$$
mv -f /tmp/autohandler.$$ /usr/local/netdisco/html/autohandler
#cat /usr/local/netdisco/html/login.html | sed 's/$r->connection-
>user($db_user->{username});/$r->user($db_user->{username});/' >
/tmp/login.html.$$
mv -f /tmp/login.html.$$ /usr/local/netdisco/html/login.html
#cd $curdir
sleep 3

#create db
cd /usr/local/netdisco/sql
./pg --init
#
cd $curdir
sleep 3

```

```

perl -MCPAN -e 'install Bundle::CPAN'
perl -MCPAN -e 'install Apache::DBI'
perl -MCPAN -e 'force install Apache::Test'
perl -MCPAN -e 'install DB_File'
perl -MCPAN -e 'install Storable'
perl -MCPAN -e 'install HTML::Entities'
#wget $MASONX
tar zxvf MasonX-Request-WithApacheSession-0.30.tar.gz
cd ./MasonX-Request-WithApacheSession-0.30
perl Makefile.PL && make && make install
cd $curdir
#wget $APACHE2HANDLER
tar zxvf MasonX-Apache2Handler-0.05.tar.gz
cd ./MasonX-Apache2Handler-0.05
perl Makefile.PL && make && make install
cd $curdir
#wget $MODPERL
tar zxvf mod_perl-2.0.3.tar.gz
cd ./mod_perl-2.0.3
perl Makefile.PL MP_APXS=/usr/bin/apxs2 && make && make install
cd $curdir
#wget $LIBAPREQ2
tar zxvf libapreq2-2.06-dev.tar.gz
cd ./libapreq2-2.06-dev
perl Makefile.PL --with-apache2-apxs=/usr/bin/apxs2 && make &&
make install
# Compile and Install Apache2::Request
cd ./glue/perl
perl Makefile.PL && make && make install
#sleep 3

cd $curdir
wget $SNMPINFO
tar zxvf SNMP-Info-1.04.tar.gz
cd SNMP-Info-1.04
perl Makefile.PL
make install
cd $curdir
sleep 3

# oui database
cd /usr/local/netdisco/
#./netdisco -O
make oui
cd $curdir

# crontab
read center_dev
#cat /usr/local/netdisco/netdisco.crontab | sed
"s/center_network_device/$center_dev/g" > /tmp/netdisco.crontab.$$
mv -f /tmp/netdisco.crontab.$$
/usr/local/netdisco/netdisco.crontab
crontab -u netdisco /usr/local/netdisco/netdisco.crontab
sleep 3
# startup
#cd $curdir
#cat /usr/local/netdisco/bin/netdisco_daemon | sed "s/su -l/su -
/g" > /tmp/netdisco_daemon.$$

```

```
#mv -f /tmp/netdisco_daemon.$$
/usr/local/netdisco/bin/netdisco_daemon
chmod +x /usr/local/netdisco/bin/netdisco_daemon

#ln -s /usr/local/netdisco/bin/netdisco_daemon
/etc/init.d/netdisco
/usr/sbin/update-rc.d -f netdisco defaults

sleep 3

#mkdir -p /usr/local/netdisco/data/logs
sleep 3

#/etc/init.d/apache2 force-reload
sleep 3

#/usr/local/netdisco/netdisco -u admin

#chown -R netdisco:netdisco /usr/local/netdisco/
#chown -R www-data:www-data /usr/local/netdisco/mason/
#/usr/local/netdisco/netdisco -r $center_dev
#/usr/local/netdisco/netdisco -m
#/usr/local/netdisco/netdisco -g
#/etc/init.d/netdisco start
#ipaddress=`/sbin/ifconfig eth0 | grep "inet addr:" | cut -c21-36
| cut -d' ' -f1`
```

ANEXO D CONFIGURACIÓN LDAP

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/nis.schema
include /etc/openldap/schema/samba.schema

slappasswd
New password: (introducimos clave)
Re-enter new password: (introducimos clave)
{SSHA}fE+wFAPFPDxb2SMrTPh3+uBRuDkyropX.

database ldbm
suffix "dc=ingedigit,dc=com"
rootdn "cn=admin,dc=ingedigit,dc=com"

# rootpw clave
rootpw {SSHA}fE+wFAPFPDxb2SMrTPh3+uBRuDkyropX
directory /var/lib/ldap

# Indices to maintain
index objectClass eq
index cn pres,sub,eq
index sn pres,sub,eq
index uid pres,sub,eq
index displayName pres,sub,eq
index uidNumber eq
index gidNumber eq
index memberUID eq
index sambaSID eq
index sambaPrimaryGroupSID eq
index sambaDomainName eq
index default sub

access to dn="admin*,dc=ingedigit,dc=com"
attr=userPassword,SambalmPassword,SambantPassword
by dn="cn=admin,dc=ingedigit,dc=com" write
by dn="cn=proxyuser,dc=ingedigit,dc=com" read
by self write
by anonymous auth
by * auth

access to dn=".*,ou=People,dc=ingedigit,dc=com"
by * read

access to dn=".*,dc=ingedigit,dc=com"
by self write
by * read

#/etc/init.d/ldap restart

#ps axu|grep slapd
ldap 11101 0.0 0.4 30124 4700 ? S 01:40 0:00 /usr/sbin/slapd -
u ldap -h ldap:///
```

ANEXO E MÓDULO DE ESCALAMIENTO

```
#!/usr/bin/perl
use strict;
use warnings;

# Ubicacion de las librerias RT y scripts
use lib ("/usr/share/request-tracker3.6/lib",
"/site/rt3/local/lib");
my $crontool = "/usr/bin/rt-crontool";

package RT;
use RT::Interface::CLI qw(CleanEnv);

# Inicializar el ambiente
CleanEnv();

# Caragar la configuracion de RT
RT::LoadConfig();

# Inicializar RT
RT::Init();

my $queues = new RT::Queues($RT::SystemUser);
$queues->LimitToEnabled();

# Aumentar prioridad en todas las
while (my $queue = $queues->Next)
{
my $queuename = $queue->Name;
system("$crontool --search RT::Search::ActiveTicketsInQueue " .
"--search-arg \"$queuename\" " .
"--action RT::Action::EscalatePriority");}
```

ANEXO F

MÓDULO DE INTEGRACIÓN DE DATOS

```

% use DBI;
% my $dbh = DBI-
>connect('DBI:Pg:dbname=netdisco','netdisco','1234')
% or die "no se pudo abrir la base de datos" . DBI->errstr;

% my $sth = $dbh->prepare('SELECT * FROM device')
% or die "no se pudo ejecutar el query" . DBI->errstr;
% my @data;
% $sth->execute()
% or die "no se pudo realizar el query";
%#while(@data = $sth->fetchrow_array()){
%#}
%#$dbh->disconnect;
%#<%def .link>
%#<a href="/<% $site %>"><% $label %></a>
%#<%args>
%#$site
%#$label=>ucfirst($site)
%#</%args>
%#</%def>
%#Link a sitio de prueba:
%#<ul>
%#<li><& .link, site=>'switches.html' &</li>
%#</ul>
% my $color_fila;
% while(@data = $sth->fetchrow_array()){
% $nswitch = $nswitch + 1;
% if ($nswitch % 2 == 0) {
% $color_fila = "evenline";
% } else { $color_fila = "odddline"; }
<td>
<tr class=<% $color_fila %> >
<td> <a href="/switches.html?str=<% $data[0] %>"> <% $data[0] %>
</a></td> <td> <% $data[3] %> </td> <td> <% $data[10] %> </td>
<td> <% $data[20] %> </td> <td> <% $data[27] %> </td>
</tr>
</td>
%}

%$dbh->disconnect;
% $dbh = DBI->connect('DBI:mysql:ocsweb','root','54321')
%or die "no se pudo abrir la base de datos" . DBI->errstr;
% $sth = $dbh->prepare('SELECT * FROM hardware')
% or die "no se pudo ejecutar el query" . DBI->errstr;
%# @data;
%$sth->execute()
%or die "no se pudo realizar el query";
%# while(@data = $sth->fetchrow_array()){
%# }
%# $dbh->disconnect;
% while(@data = $sth->fetchrow_array()){
% $nhosts = $nhosts + 1;
% if ($nhosts % 2 == 0) {
% $color_fila = "evenline";
% } else { $color_fila = "odddline"; }
<tr class=<% $color_fila %>>
<td> <a href="/hosts?str=<% $data[13] %>"> <% $data[13] %>
</a></td> <td> <% $data[5] %> </td> <td> <% $data[19] %> </td>
<td> <% $data[11] %> </td> <td> <% $data[9] %> </td>
</tr>
</td>
%}
%$dbh->disconnect;

```

ANEXO G

ARCHIVOS DE CONFIGURACION (switches.html, hosts.html e index.html)

Sentencias SQL

El query SQL para listar la información de todos los switches inventariados por netdisco se muestra a continuación:

```
%my $sth = $dbh->prepare('SELECT * FROM device')
%
    or die "no se pudo ejecutar el query" . DBI->errstr;
```

El query SQL para listar la información de todos los switches inventariados por netdisco se muestra a continuación:

```
% $sth = $dbh->prepare('SELECT * FROM hardware')
%
    or die "no se pudo ejecutar el query" . DBI->errstr;
```

Archivo Switches.html

El query SQL para listar la información de contacto, ubicación, dirección MAC, modelo, Sistema Operativo y fecha del último discovery del switch se muestra a continuación:

```
% $sth = $dbh->prepare("SELECT * FROM device where ip='$dir'")
%
    or die "no se pudo ejecutar el query" . DBI->errstr;
```

El query SQL para listar los puertos del switch, junto a la información asociada a cada puerto, como estado, velocidad de transferencia, vlan asociada y fecha de último inventario, se muestra a continuación:

```
% $sth = $dbh->prepare("SELECT * FROM device_port where ip='$dir' ORDER
BY port")
%
    or die "no se pudo ejecutar el query" . DBI->errstr;
```

Archivo Hosts.html

El query SQL para listar la información del switch que está asociado a un host, indicando dirección IP, dirección MAC y puerto del switch en particular, se muestra a continuación:

```
% $sth = $dbh->prepare("SELECT * FROM node where mac='$mac'")
%
    or die "no se pudo ejecutar el query" . DBI->errstr;
```

El query SQL para listar la información del software instalado en un host particular, se muestra a continuación:

```
% $sth = $dbh->prepare("SELECT * FROM networks where hardware_id='$id'")
%
    or die "no se pudo ejecutar el query" . DBI->errstr;
```

Archivo index.html

```
<html><head>
<meta http-equiv="refresh" content="30;
url=http://bestpractical.com/rt/rt-broken-install.html">
<title>Service Desk</title></head>
<body bgcolor=blue />


<br /><br />

<%init>

%# Variables y su inicialización

my $nswitch = 0;
my $nhosts = 0;
my @results;
my $sth2;
my @row3;
my $id;
my $types;
my $tam_disco;
my $fabricante_bios;
my $ssn;
my $smodel;
my $quality;
my $sth3;
my $sth4;

if ($ARGS{'QuickCreate'}) {
    my $ticket = RT::Ticket->new($session{'CurrentUser'});
    my ($tid, $trans, $tmsg) = $ticket->Create(Queue =>
$ARGS{'Queue'},
                                Owner => $ARGS{'Owner'},
                                Requestor => $session{'CurrentUser'}->UserObj-
>EmailAddress,
                                Subject => $ARGS{'Subject'});
    push (@results, $tmsg);
}
if ( $ARGS{'q'} ) {
    RT::Interface::Web::Redirect($RT::WebURL."Search/Simple.html?q=".$
m->interp->apply_escapes($ARGS{q}));
}
if ($ARGS{'HomeRefreshInterval'}) {
    $session{'home_refresh_interval'} =
$ARGS{'HomeRefreshInterval'};
}
my $actions;
</%init>
% use DBI;
% my $dbh = DBI-
>connect('DBI:Pg:dbname=netdisco2','netdisco','1234')
%         or die "no se pudo abrir la base de datos" . DBI-
>errstr;

%my $sth = $dbh->prepare('SELECT * FROM device')
%         or die "no se pudo ejecutar el query" . DBI->errstr;

% my @data;

%         $sth->execute()
%         or die "no se pudo realizar el query";
```

```

%#                               while(@data = $sth-
>fetchrow_array()){

%#                               }

%#                               $dbh->disconnect;

%#Vista de Lista de Switches

<div class="quick-create" width="100%">
<div class="">
<div class="titlebox " id="">
<div class="titlebox-title">
<span class="left">Lista de Switches</span>
<span class="right"></span>
<span class="widget"><a href="#" onclick="return rollup('TitleBox-
-_index.html-----Lista de Switches---0');" onFocus="this.blur();
return false;" title="Toggle visibility">X</a></span>

</div>

<div class="titlebox-content " id="TitleBox--_index.html-----
Lista de Switches---0">

<table border="0" cellspacing="0" cellpadding="1" width="100%">

<th class="collection-as-table">Switch</th><th class="collection-
as-table">Descripcion</th><th class="collection-as-
table">MAC</th><th class="collection-as-table">Sistema
Operativo</th><th class="collection-as-table">Ultimo
inventario</th>

<tr></tr>
<tr></tr>
<tr></tr>

%#<%def .link>
%#<a href="/<% $site %>"><% $label %></a>
%#<%args>
%#$site
%#$label=>ucfirst($site)
%#</%args>
%#</%def>
%#Link a sitio de prueba:
%#<ul>
%#<li><& .link, site=>'switches.html' &></li>
%#</ul>
% my $ip;
% my $color_fila;

% while(@data = $sth->fetchrow_array()){

% $nswitch = $nswitch + 1;

% if ($nswitch % 2 == 0) {
% $color_fila = "evenline";
% } else { $color_fila = "odddline"; }

<td>
<tr class=<% $color_fila %> >
<td> <a href="/switches.html?str=<% $data[0] %>"> <% $data[0] %>
</a></td> <td> <% $data[3] %> </td> <td> <% $data[10] %> </td>
<td> <% $data[20] %> </td> <td> <% $data[27] %> </td>
</tr>
</td>

```

```

%}
</table>
<p> <b> N&uacutemero total de Switches: </b> <% $nswitch %> </p>
<hr class="clear" />
</div>
</div>

%$dbh->disconnect;

%# CAMBIO OCS

<br><br>
% $dbh = DBI->connect('DBI:mysql:ocsweb','root','54321')
%          or die "no se pudo abrir la base de datos" . DBI-
>errstr;

% $sth = $dbh->prepare('SELECT * FROM hardware')
%          or die "no se pudo ejecutar el query" . DBI->errstr;

%# @data;

%          $sth->execute()
%          or die "no se pudo realizar el query";

%# while(@data = $sth->fetchrow_array()){
%# }

%# $dbh->disconnect;

<div class="quick-create" width="100%">
<div class="">
<div class="titlebox " id="">
<div class="titlebox-title">
<span class="left">Lista de Hosts</span>
<span class="right"></span>

<span class="widget"><a href="#" onclick="return rollup('TitleBox-
_index.html-----Lista de Hosts---0');" onfocus="this.blur();
return false;" title="Toggle visibility">X</a></span>

</div>

%#Vista de Lista de Hosts

<div class="titlebox-content " id="TitleBox--_index.html-----
Lista de Hosts---0">

<table border="0" cellspacing="0" cellpadding="1" width="100%">

<th class="collection-as-table">Host</th><th class="collection-as-
table">Nombre equipo</th><th class="collection-as-
table">Usuario</th><th class="collection-as-table">Sistema
Operativo</th><th class="collection-as-table">Memoria (MB) </th><th
class="collection-as-table">Procesador (MHz) </th><th
class="collection-as-table">Disco (GB) </th><th class="collection-
as-table">Fabricante</th><th class="collection-as-
table">Modelo</th><th class="collection-as-table">Calidad</th>

<tr></tr>

```

```

<tr></tr>
<tr></tr>

% while(@data = $sth->fetchrow_array()){

% $nhosts = $nhosts + 1;

% if ($nhosts % 2 == 0) {
% $color_fila = "evenline";
%} else { $color_fila = "odddline"; }

% $ip= $data[13];

% $sth2 = $dbh->prepare("select * from hardware where
ipaddr='$ip'")
%         or die "no se pudo ejecutar el query" . DBI->errstr;

%         $sth2->execute()
%         or die "no se pudo realizar el query";

% @row3 = $sth2->fetchrow_array();

% $id = $row3[0];

% $types="hard drive";

% $sth3 = $dbh->prepare("select * from drives where
hardware_id='$id' and Type ='$types'")
%         or die "no se pudo ejecutar el query" . DBI->errstr;

%         $sth3->execute()
%         or die "no se pudo realizar el query";

% @row3 = $sth3->fetchrow_array();

% $tam_disco = $row3[5]/1000;

% $sth4 = $dbh->prepare("select * from bios where
hardware_id='$id'")
%         or die "no se pudo ejecutar el query" . DBI->errstr;

%         $sth4->execute()
%         or die "no se pudo realizar el query";

% @row3 = $sth4->fetchrow_array();

% $fabricante_bios = $row3[5];
% $smodel = $row3[2];
% $ssn = $row3[3];
% $quality = (($data[11]/2048) + ($data[9]/3321) +
($tam_disco/148));

<td>
<tr class=<% $color_fila %>>
<td> <a href="/hosts?str=<% $ip %>"> <% $data[13] %> </a> </td>
<td> <% $data[2] %> </td><td> <% $data[19] %> </td> <td> <%
$data[5] %> </td> <td> <% $data[11] %> </td> <td> <% $data[9] %>
</td> <td> <% $tam_disco %> </td><td> <% $fabricante_bios %> </td>
<td> <% $smodel %> </td>
%if ($quality > 1.5 ) {
<td><% $quality %></td>
%}
%if ($quality < 1.5 ) {
<td><font color="red"> <% $quality %> </font></td>
%}

```

```

</tr>
</td>
%}

</table>

<p><b> N\u00e9mero total de hosts: </b> <% $nhosts %> </p>
<hr class="clear" />
</div>
</div>
</div>

%#Vista de Registro de eventos

<div class="quick-create" width="100%">
<div class="">
<div class="titlebox " id="">
<div class="titlebox-title">
<span class="left">Registro de eventos</span>
<span class="right"></span>

<span class="widget"><a href="#" onclick="return rollup('TitleBox-
_index.html-----Registro---0');" onfocus="this.blur(); return
false;" title="Toggle visibility">X</a></span>

</div>

<div class="titlebox-content " id="TitleBox--_index.html-----
Registro---0">

<table border="0" cellspacing="0" cellpadding="1" width="100%">

<th class="collection-as-table">Registro</th><th
class="collection-as-table">Descripcion</th>
<tr></tr>
<tr></tr>
<tr></tr>
<td> <a href="/cambios.html"> Inventario de Hardware y Software
</a></td> <td> Registra todos los cambios de hardware y software
</td>
<tr></tr>
<td> <a href="/red.html"> Red </a></td><td> Registra todos los
cambios de dispositivos de red </td>

</table>
</div>
</div>
</div>

%#Vista de Mapa de Res

<div class="quick-create" width="100%">
<div class="">
<div class="titlebox " id="">
<div class="titlebox-title">
<span class="left">Mapa de Red</span>
<span class="right"></span>

<span class="widget"><a href="#" onclick="return rollup('TitleBox-
_index.html-----Mapa de Red---0');" onfocus="this.blur(); return
false;" title="Toggle visibility">X</a></span>

</div>

<div class="titlebox-content " id="TitleBox--_index.html-----Mapa
de Red---0">

```

```
<table border="0" cellspacing="0" cellpadding="1" width="100%">

<div id="mapa">
  <a
href="http://es.wikipedia.org/wiki/Arquitectura_de_red"><center><i
mg src="<%$RT::WebImagesURL%>/netmap.jpg" alt="<%loc("Mapa de
Red")%>" width="1024" height="768" /></a>
</div>

</table>
</div>
</div>
</div>
</div>

%$dbh->disconnect;

%# --></body></html>
```

ANEXO H

Diagrama obtenido con la Herramienta LAN MapShot

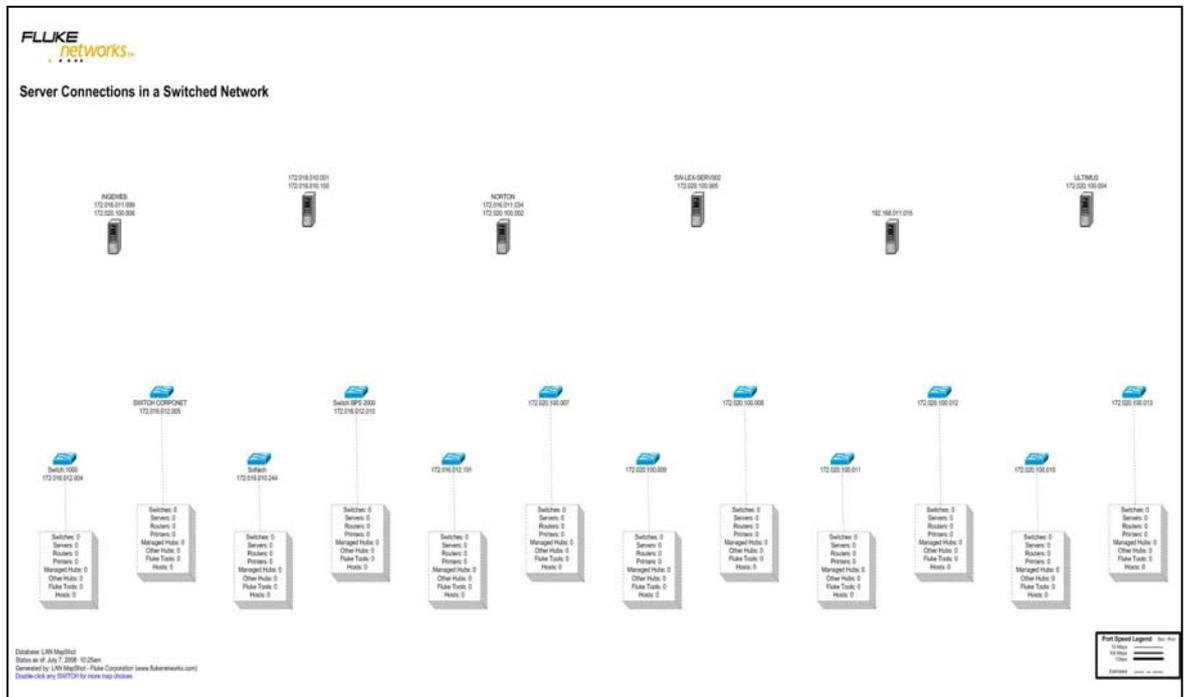


Figura 37: Diagrama obtenido con la Herramienta LAN MapShot.
Autor: K.Rodríguez, S.Hernández

ANEXO I

PANTALLAS DEL SISTEMA AUTOMATIZADO DE GESTIÓN



Figura 38: Pantalla inicial del sistema
Fuente: Sistema Automatizado de Gestión.

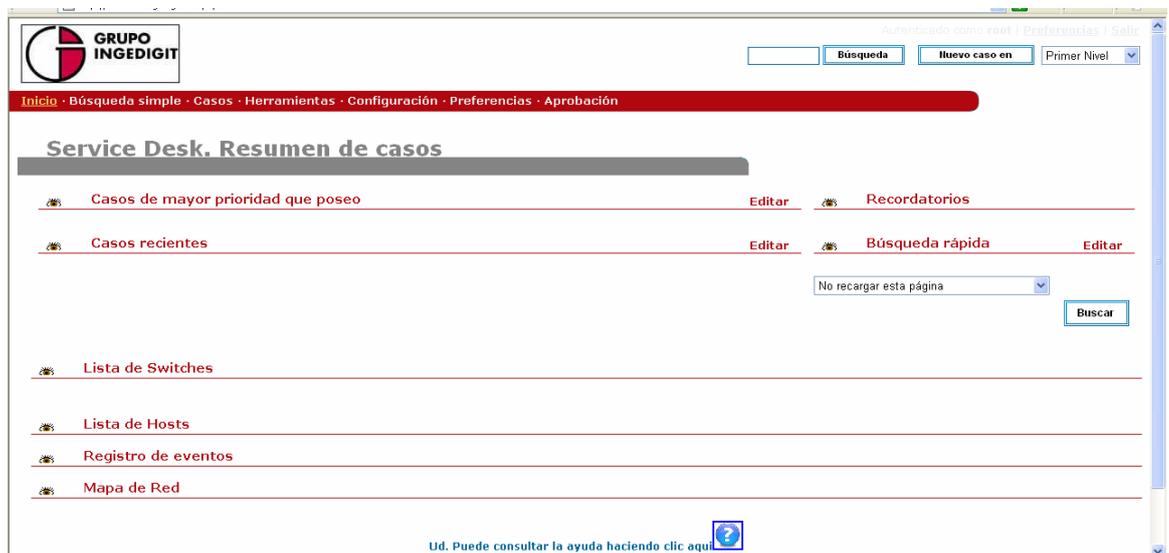


Figura 39: Pantalla principal del sistema
Fuente: Sistema Automatizado de Gestión.

[Editar](#)

#	Cola	Estado	Asunto	Creado	Tomar	Técnico asignado
17	Primer Nivel	nuevo	E-Mail 2	Hace 7 meses	root@localhost	Nobody
44	Primer Nivel	nuevo	Fallas en el monitor	Hace 3 meses	ecarrasco@ingedigit.com	Nobody
45	Primer Nivel	nuevo	No puedo iniciar la sesión	Hace 2 meses	ecarrasco@ingedigit.com	Nobody
46	Primer Nivel	nuevo	Fallas de conexión	Hace 2 meses	maria.rodriguez@ingedigit.com	Nobody
47	Primer Nivel	nuevo	Fallas de conexion	Hace 6 semanas	oswaldo.badillo@ingedigit.com	Nobody
48	Primer Nivel	nuevo	Problemas de autentificacion con active directory	Hace 5 semanas	karenrespo@ingedigit.com	Nobody
49	Primer Nivel	nuevo	Falla tarjeta linksys en Debian	Hace 3 semanas	oscar.nieto@ingedigit.com	Nobody
50	Primer Nivel	nuevo	Instalacion de Sistema Administrativo SIGAD	Hace 3 semanas	oscar.nieto@ingedigit.com	Nobody
51	Primer Nivel	nuevo	Instalacion de Sistema Administrativo SIGAD	Hace 3 semanas	oscar.nieto@ingedigit.com	Nobody

Figura 40: Lista de Casos recientes
Fuente: Sistema Automatizado de Gestión.

Lista de Switches

Switch	Descripcion	MAC	Sistema Operativo	Ultimo inventario
172.20.100.8	Business Policy Switch 2000 HW:14 FW:3.6.0.1 SW:v2.5.2.04 ISVN:2	00:04:dc:ff:b2:81	baystack	2008-06-06 08:01:07
172.20.100.12	BayStack 460 - 24T - PWR HW:07 FW:3.0.0.5 SW:v3.0.6.08 ISVN:2	00:12:83:ff:61:41	boss	2008-06-06 08:02:08
172.16.30.1	Business Policy Switch 2000 HW:11 FW:3.6.0.1 SW:v2.5.2.04 ISVN:2	00:03:42:9b:d9:41	baystack	2008-06-06 08:02:29
172.20.100.11	Business Policy Switch 2000 HW:11 FW:3.6.0.1 SW:v2.5.2.04 ISVN:2	00:04:38:e9:a5:61	baystack	2008-06-06 08:00:14
172.20.100.9	Business Policy Switch 2000 HW:11 FW:3.6.0.1 SW:v3.1.8.12 ISVN:3	00:04:dc:81:6f:21	boss	2008-06-06 08:00:24
172.16.50.1	Business Policy Switch 2000 HW:14 FW:3.6.0.1 SW:v2.5.2.04 ISVN:2	00:01:81:eb:2d:e1	baystack	2008-06-06 08:00:35
172.16.80.1	Business Policy Switch 2000 HW:14 FW:3.6.0.1 SW:v2.5.2.04 ISVN:2	00:09:97:28:d7:41	baystack	2008-06-06 08:01:28
172.16.12.10	Business Policy Switch 2000 HW:10 FW:3.6.0.1 SW:v3.2.1.04 ISVN:3	00:04:dc:80:83:01	boss	2008-06-06 08:01:48
172.16.40.1	Business Policy Switch 2000 HW:07 FW:2.5.0.3 SW:v3.2.1.04 ISVN:3	00:04:38:f7:fa:41	boss	2008-06-06 08:02:19
172.16.12.191	Ethernet Switch 470-24T-PWR HW:01 FW:3.6.0.6 SW:v3.6.2.04 BN:4 ISVN:2 (c) Nortel Networks	00:16:60:82:ff:61	boss	2008-06-06 08:02:40
172.20.100.7	Business Policy Switch 2000 HW:03 FW:3.6.0.1 SW:v3.1.8.12 ISVN:3	00:01:81:eb:88:21	boss	2008-06-06 08:02:49
172.20.100.10	BayStack 350-12T HW:RevL FW:V1.47 SW:v3.1.0.22 ISVN:1	00:03:42:f7:5b:21	baystack	2008-06-06 08:01:57
172.16.12.9	Business Policy Switch 2000 HW:11 FW:3.6.0.1 SW:v3.2.1.04 ISVN:3	00:09:97:a6:10:81	boss	2008-06-06 08:01:18
172.16.10.244	BayStack 325-24T HW:02 FW:3.0.0.3 SW:v3.0.0.16	00:14:c7:f6:88:01	baystack	2008-06-06 08:01:38
172.16.40.2	Business Policy Switch 2000 HW:03 FW:3.6.0.1 SW:v2.5.2.04 ISVN:2	00:03:42:e6:99:81	baystack	2008-06-06 08:00:03
172.16.40.3	BayStack 350-12T HW:RevL FW:V1.47 SW:v3.1.0.22 ISVN:1	00:03:42:f7:6f:61	baystack	2008-06-06 08:00:46
172.20.100.13	BayStack 350-12T HW:RevL FW:V1.47 SW:v3.1.0.22 ISVN:1	00:03:42:f7:6a:01	baystack	2008-06-06 08:00:56

Número total de Switches: 17

Figura 41: Lista de Switches
Fuente: Sistema Automatizado de Gestión.

Lista de Hosts

Host	Nombre equipo	Usuario	Sistema Operativo	Memoria (MB)	Procesador (MHz)	Disco (GB)	Fabricante	Modelo	Calidad
172.20.130.5	aragorn		Linux	60	348	0	Compaq	Deskpro EP/SB Series	0.134084589543812
172.20.40.2	BTINEO	btineo	Microsoft Windows XP Professional	512	2934	72.582	Intel Corp.		1.62388775360727
172.16.18.39	debian	geekbynature	Linux	3291	1995	0	Dell Inc.	PowerEdge 2900	2.20765626764341
172.16.18.33	debian	geekbynature	Linux	471	3401	0	Dell Inc.	OptiPlex 320	1.25406959853019
172.16.18.32	debian1	geekbynature/root	Linux	471	3400	0	Dell Inc.	OptiPlex 320	1.25376848440793
172.16.18.33	desarrollo	desarrollo	Linux	471	3400	0	Dell Inc.	OptiPlex 320	1.25376848440793
172.16.10.156	FEGLOFF	daniel	Microsoft Windows XP Professional	992	1792	76.316	American Megatrends Inc.	M935CG	1.53962015572483
172.16.10.34	FSOTO	fsoto	Microsoft Windows 2000 Professional	224	1792	30.718	American Megatrends Inc.	M935CG	0.856525561130236
172.16.18.33	ingedigitt	katty	Linux	471	3400	0	Dell Inc.	OptiPlex 320	1.25376848440793
172.20.100.87	JEFFERSON	jefferson marcano	Microsoft Windows Vista Home Premium	2048	1500	183.9	Hewlett-Packard	HP Pavilion dv6500 Notebook PC	2.69423875094607
172.16.11.52	JOSEDELACRUZ	jdelaacruz	Microsoft Windows XP Professional	512	2992	76.308	Phoenix Technologies, LTD		1.66652804837358
172.16.10.230	MFREITES	mfreites	Microsoft Windows 2000 Professional	736	2400	10.997	American Megatrends Inc.	M935D	1.15635294745965
172.16.10.230	MFREITES	mfreites	Microsoft Windows 2000 Professional	736	2400	10.997	American Megatrends Inc.	M935D	1.15635294745965
172.16.10.207	NCISNEROS	ncisneros	Microsoft Windows XP Professional	448	1062	38.154	Phoenix Technologies, LTD	KM266A-8237	0.796330495129276

Figura 42: Lista de Hosts
Fuente: Sistema Automatizado de Gestión.

Registro de eventos

Registro	Descripcion
Inventario de Hardware y Software Red	Registra todos los cambios de hardware y software Registra todos los cambios de dispositivos de red

Figura 43: Registro de eventos del sistema
Fuente: Sistema Automatizado de Gestión.

GRUPO INGEDIGIT

Autenticado como root | Preferencias | Salir

Búsqueda Nuevo caso en Primer Nivel

Inicio · Búsqueda simple · Casos · Herramientas · Configuración · Preferencias · Aprobación

Búsqueda de casos

Para buscar un caso puede indicar el identificador del caso, nombre del nivel al que pertenece el caso, "dirección email del solicitante o propietario del caso. Puede también buscar palabras que se encuentren en los cuerpos y adjuntos de casos.

Si necesita puede buscar por cualquier palabra en el histórico completo de casos escribiendo: " **fulltext:palabra** .

Búsqueda

Ud. Puede consultar la ayuda haciendo clic aquí

Ud. Puede conocer mas acerca de los creadores de esta herramienta haciendo clic aquí

Figura 44: Pantalla de Búsqueda simple de Casos del sistema
Fuente: Sistema Automatizado de Gestión.

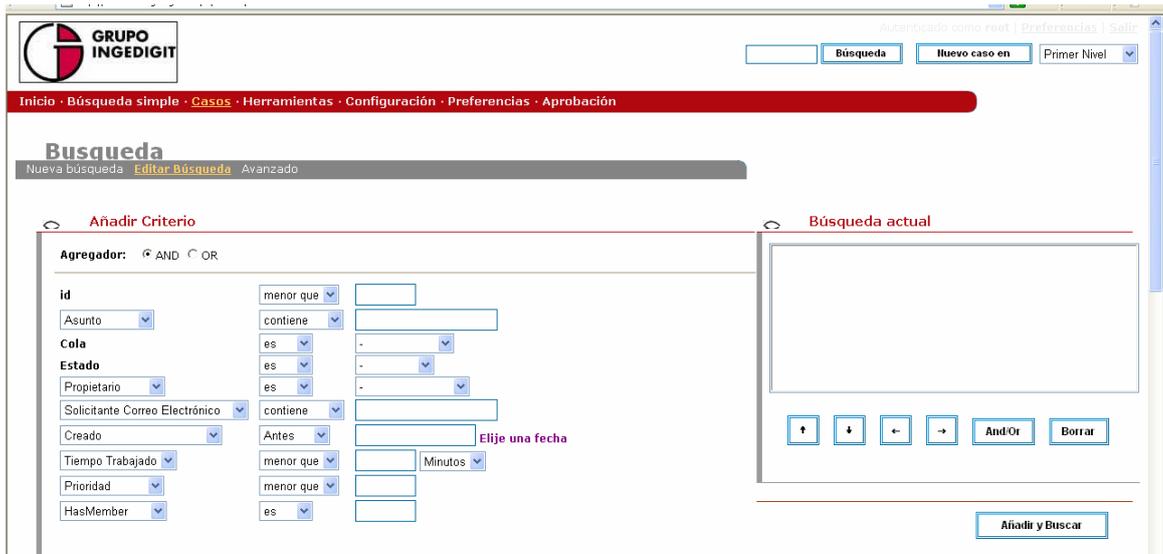


Figura 45: Pantalla de Edición de Búsqueda de Casos del sistema
Fuente: Sistema Automatizado de Gestión.



Figura 46: Pantalla de Herramientas del sistema (informes)
Fuente: Sistema Automatizado de Gestión.

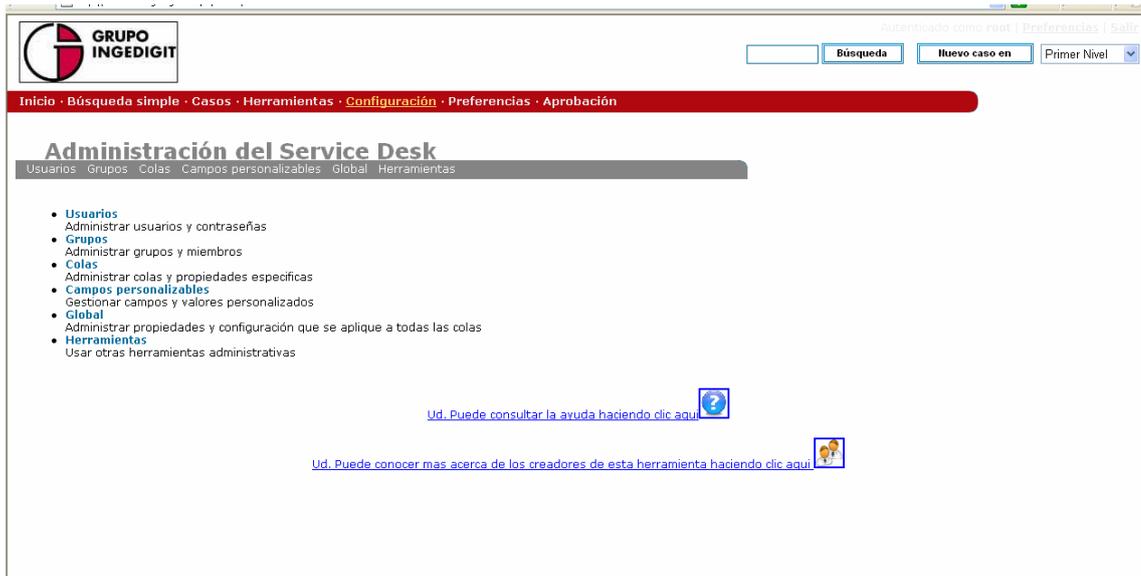


Figura 47: Pantalla de Administración del sistema
Fuente: Sistema Automatizado de Gestión.

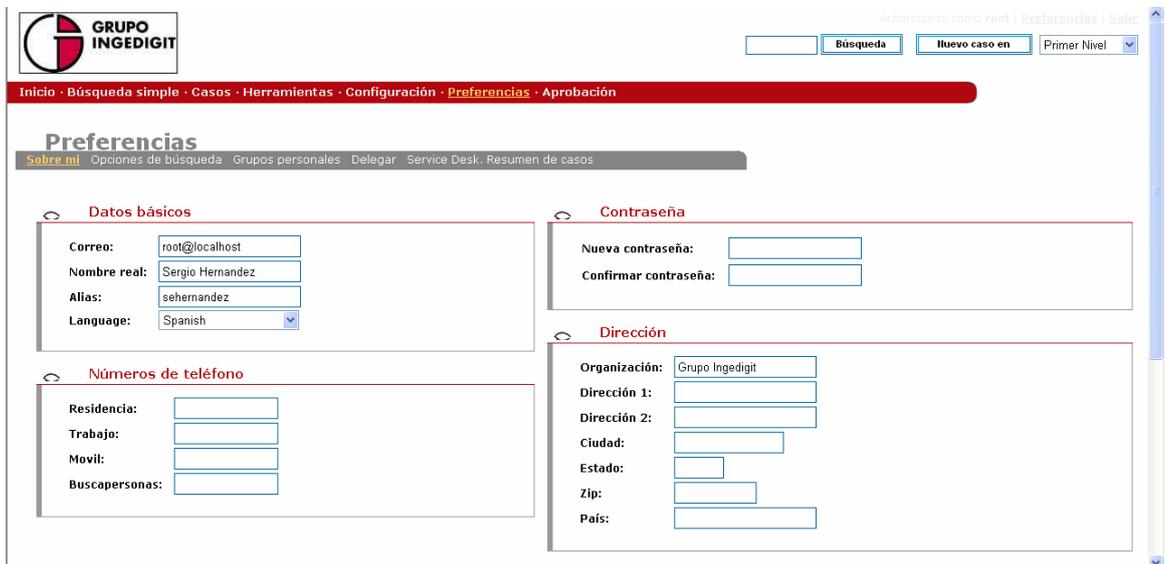


Figura 48: Pantalla de Preferencias de usuario del sistema
Fuente: Sistema Automatizado de Gestión.

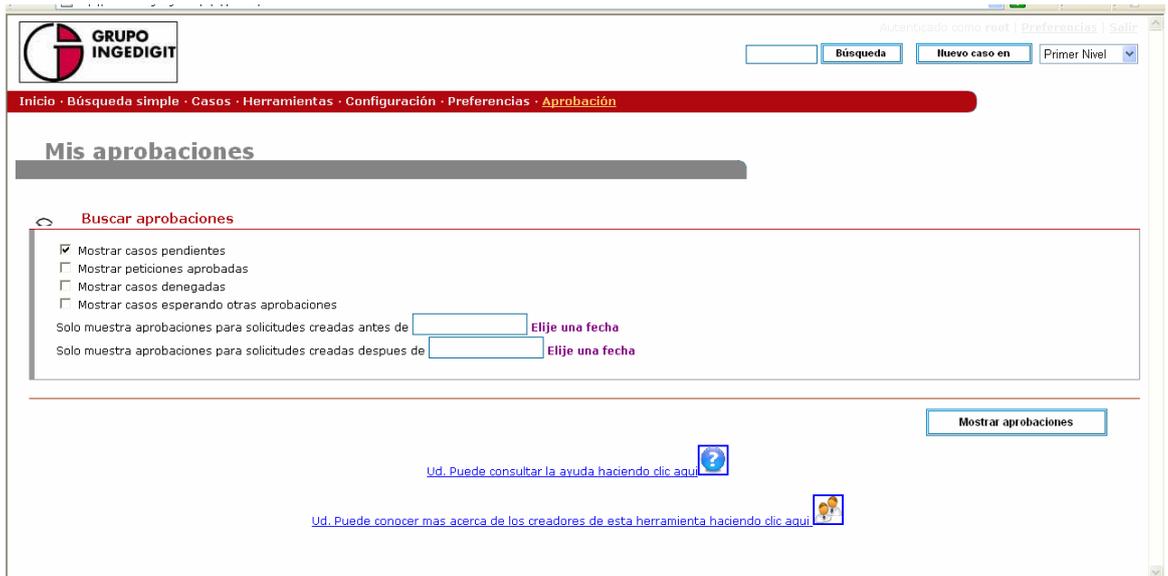


Figura 49: Pantalla de Aprobaciones de casos del sistema
Fuente: Sistema Automatizado de Gestión.

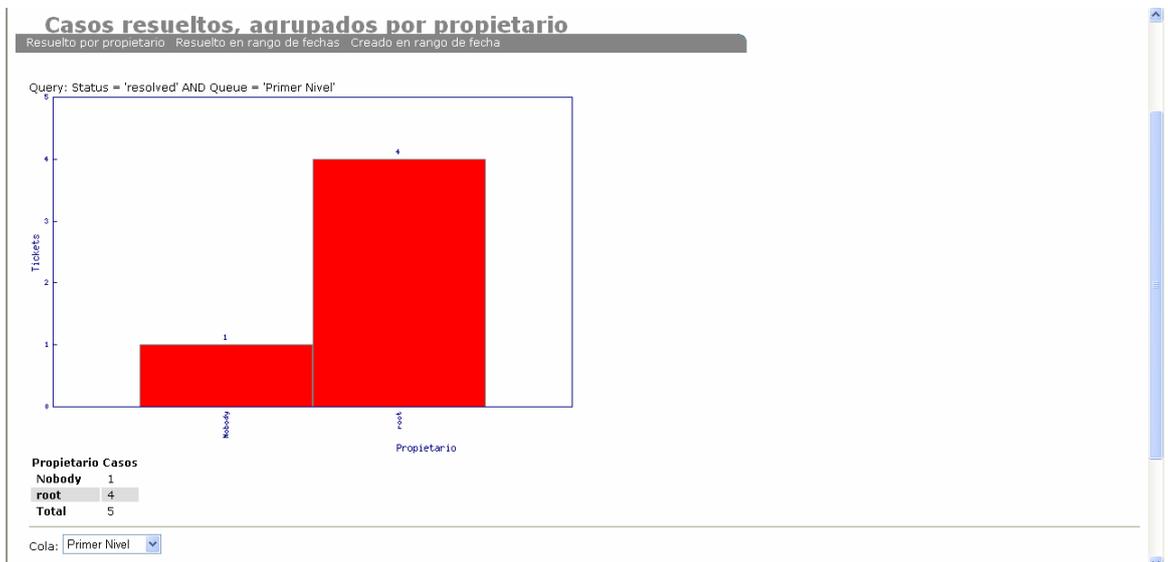


Figura 50: Reporte de casos resueltos agrupados por propietario
Fuente: Sistema Automatizado de Gestión.

REFERENCIAS BIBLIOGRÁFICAS

- [1] Information Technology Infrastructure Library. Año 1990. Disponible en http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/introduccion_objetivos_gestion_de_incidentes/introduccion_objetivos_gestion_de_incidentes.php. Consultado Diciembre 2007
- [2] Fernando Torres Lez, Angel Martínez Sánchez, Pedro Poza. “Inventario tecnológico” .Año 2000.
- [3] Gestión básica de redes Cisco: Disponible en <http://www.cisco.com>. Consultado Noviembre 2007
- [4] RFC 1157: Simple Network Management Protocol (SNMP). Consultado Octubre 2007.
- [5] J.Preece.“Interaction Design Beyond Human-Computer Interaction”. Año 2000.
- [6] J. Vincent, R. Spier, D. Rolsky, D. Chamberlain, R. Foley. “RT Essentials”. O'Reilly. Año 2005
- [7] Gestión Inventario: Disponible en <http://www.ocsinventory-ng.org/>. Consultado Diciembre 2007.
- [8] Alexander Barthel. “Análisis, implementation and Enhancement of Vendor dependent and independent Layer-2 Network Topology Discovery”. Año 2005
- [9] Torgerson, W. “Theory and Methods of Scaling”. New York- Wiley. Año 1965.
- [10] Gestión de activos: Disponible en <http://www.netdisco.org>. Consultado Diciembre 2007.
- [11] RFC 1777-es: Protocolo Ligero de Acceso a Directorio (LDAP). Consultado Enero 2008.
- [12] Miquel Trilla. “Single Sign-On”. Año 2005.
- [13] P. Kruchten, “Rational Unified Process-An Introduction”, Adison-Wesley. Año 2001
- [14] López Solís, Rosa Idolina, “Modelo para medir la madurez de los procesos y funciones del Help Desk”, Tesis de Maestría en Ciencias en Tecnología Informática del ITESM, Monterrey, N.L., México, Diciembre 2003. Disponible en: <http://biblioteca.itesm.mx>

- [15] Ana Griman. Guía de laboratorio. Racional Unified Process. 2002.
- [16] Ana Griman, Luis Eduardo Mendoza. Notas de clase sobre metodología IDEFIX. 2005.
- [17] Bass Len, Clements Paul y Kazman Rick. “Software Architecture in Practice”. Addison-Wesley. E.E.U.U. 1998.
- [18] Elmarsi, Ramez y Navathe, Shamkant. “Fundamentals of Database Systems”. Addison-Wesley. E.E.U.U. 2002.
- [19] Ian Gilfillan. “MYSQL”, Editorial ANAYA MULTIMEDIA. 2003.
- [20] Kim W. y Seo J. 2000. “ Classifying schematic and data heterogeneity in multidatabases system”. COMPUTER. 1998.
- [21] Vaswani. “MYSQL: The Complete References”. McGraw-Hill. 1ra. Edición. 2004.