UNIVERSIDAD TECNICA DE AMBATO

FACULTAD DE INGENIERIA EN SISTEMAS

CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES E INFORMATICOS

TEMA:

"Estudio, Administración e Implementación de Políticas de Seguridad en la Red Informática del Hospital Millennium de la ciudad de Ambato."

Proyecto de Graduación modalidad Pasantía presentada como requisito previo a la obtención del Título de Ingeniero en Sistemas Computacionales e Informáticos.

AUTOR:

Franklin Geovanny Flores Saltos

TUTOR:

Ing. Clay Fernando Aldás Flores

Ambato – Ecuador

Diciembre/2007

APROBACION DEL TUTOR

En calidad de Tutor del Trabajo de Investigación sobre el tema:

"Estudio, Administración e Implementación de Políticas de Seguridad en la Red Informática del Hospital Millennium de la ciudad de Ambato.", de Franklin Geovanny Flores Saltos, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Universidad Técnica de Ambato, considero que dicho informe investigativo reúne los requisitos y méritos suficientes para ser sometidos a la evaluación de conformidad al Art. 68 del Reglamento de Pregrado de la Universidad Técnica de Ambato.

Ambato, Diciembre 2007

EL TUTOR

Ing. Clay Fernando Aldás Flores

GRACIAS

A mis padres, por su apoyo incondicional y por hacer de mi lo que soy.

A mis amigos (los que estuvieron y los que están), por hacer de lo que soy algo mejor.

A mis maestros, por los conocimientos que me impartieron y por enseñarme que con esfuerzo y dedicación es posible salir adelante.

A las personas que siempre me dieron ánimo a enfrentar y superar las adversidades.

CAPITULO I

EL PROBLEMA DE INVESTIGACION

1.1. TEMA DE INVESTIGACION

Estudio, Administración e Implementación de Políticas de Seguridad en la Red Informática del Hospital Millennium de la ciudad de Ambato.

1.2. PLANTEAMIENTO DEL PROBLEMA

1.2.1. CONTEXTUALIZACION

Con la explosión del uso masivo de Internet, tanto los ordenadores personales como las redes de ordenadores, pueden ser vulnerables a diversos tipos de ataques. Internet ha pasado a ser sin ningún tipo de dudas la mayor red pública de datos, a través de la cual se facilitan comunicaciones personales, educacionales y empresariales en todo el mundo. El volumen de tráfico de datos que se mueve en Internet crece exponencialmente de forma diaria. Día a día crece el número de comunicaciones vía correo electrónico, acceso a las redes corporativas de trabajadores o personas que se desplazan constantemente, transacciones comerciales, información educativa, noticias, etc.

Muchas organizaciones hoy en día, son amenazadas constantemente en sus activos, lo que puede representar miles o millones de dólares en pérdidas. Las vulnerabilidades en los sistemas de información pueden representar problemas graves, por ello es muy importante que las empresas contemporáneas comprendan los conceptos necesarios para combatir y defenderse de los posibles ataques a su información. Entre los posibles ataques a la que puede estar sujeta una red corporativa se encuentran los virus, troyanos y vándalos; los ataques de hackers, como podrían ser ataques de reconocimiento, de

acceso, de denegación de servicios y de interceptación de datos; una empresa debe estar protegida frente a los ataques desde dentro y fuera de la misma, donde en ocasiones los mismos empleados de forma inconciente, negligente o vengativa pueden causar daños irreparables.

Entre las principales consecuencias de estos ataques se encuentran la pérdida de datos de vital importancia, violación de la privacidad y caída de la red en forma temporal.

En la actualidad, la información es el bien de mayor valor para las empresas. El progreso de la Informática y de las redes de comunicación no sólo ha sido un beneficio para las mismas, debido a que tienen mayores niveles de sistematización, sino que generan un mayor nivel de prevención y responsabilidad frente a las amenazas sobre dicha información.

La seguridad informática tiene como propósito proteger la información organizacional, independiente del lugar en donde se encuentre, ya que ésta puede estar en diferentes medios como por ejemplo en papel impreso, en los discos duros o incluso en la memoria de las personas que la conocen. Por esto, la seguridad de la información es un asunto importante para todos, pues afecta directamente a los negocios de una empresa como a los individuos que hacen parte de ella.

Es por ello que hoy en día las empresas buscan la mejor forma de asegurar la organización y los recursos de la misma. En consecuencia surgen, tanto las empresas dedicadas a la seguridad informática y a los servicios de consultoría para el aseguramiento de los recursos tecnológicos y humanos que se ven involucrados en la organización, como los departamentos encargados de la seguridad de tecnología de información de las organizaciones.

En el caso del Hospital Millennium la seguridad de la red informática es un punto a ser tomado muy en cuenta ya que a través de ella circula información de gran importancia y confidencialidad, la misma debe estar protegida contra todo tipo de ataques. Parte de la

información son los Datos Médicos que son de gran importancia y de tratamiento muy delicado, ya que si se llegaran a cambiar de forma inconciente por alguna persona no autorizada podría traer graves consecuencias al paciente y afectaría la imagen y prestigio de la Institución.

1.2.2. ANALISIS CRITICO

La red informática del Hospital Millennium no se encuentra totalmente protegida contra los diferentes tipos de ataques a los que una red corporativa esta expuesta, ya que por la falta de tiempo no se han podido implementar todas las seguridades necesarias que una red corporativa requiere para que la información confidencial de la Institución esté segura y que se pueda de forma oportuna detectar y detener cualquier tipo de ataque que atente contra la Institución, la información que circula en la red o a cualquier dispositivo conectado a ella, en su mayoría los ataques pueden producir pérdida de tiempo o graves pérdidas económicas.

La gravedad de los ataques a los que se encuentra expuesta la red informática del Hospital, más aún cuando hoy en día no es necesario ser un experto para ser un intruso en una red gracias al gran número de herramientas de hacking que existen y pueden ser descargadas de Internet, hacen que una buena política de seguridad sea una parte indispensable para prevenir estos problemas. Como parte de las políticas de seguridad se debe implementar un antivirus corporativo que sea eficiente y proteja la red del ataque de virus, troyanos, gusanos, etc. Esto permitirá que las actividades del Hospital Millennium sean eficientes y ayuden a cumplir con las expectativas tanto de los socios como de los accionistas.

1.2.3. PROGNOSIS

Debido al gran número de amenazas a las que están expuestas las redes informáticas ninguna Institución o empresa esta en la capacidad de decir que cuenta con un sistema

100% seguro, sin embargo es necesario el tomar todas las medidas indispensables para brindar a la red informática el mayor nivel de seguridad posible.

En la red informática del Hospital Millennium falta mucho por hacer en cuanto a seguridad, el no contar con una seguridad adecuada significa que estamos dejando las puertas abiertas para ser atacados, produciendo de esta manera graves pérdidas económicas o de información a la Institución, esto puede llevar a brindar servicio ineficiente, lo que provocará pérdida de clientes.

Por lo mencionado se requieren implementar en el Hospital Millennium un sistema total de seguridad basado en identificación, privacidad, administración de las políticas y definición de un perímetro de seguridad, debido a que se maneja una cantidad grande de información sensible.

1.2.4. FORMULACION DEL PROBLEMA

¿Qué incidencia tiene la falta de seguridad adecuada de la red informática en el control y respaldo de la información confidencial del Hospital Millennium?

1.2.5. DELIMITACION DEL PROBLEMA

El presente trabajo investigativo se realizará en el Hospital Millennium durante el período comprendido de Abril - Agosto del 2007 con una población de 3 personas.

1.3. JUSTIFICACION

Es importante que las instituciones dedicadas a brindar un servicio de salud a la ciudadanía fortalezcan su capital y el crecimiento de su patrimonio para convertirse en instituciones de gran magnitud.

El tema de investigación propone principalmente dar solución a los posibles problemas de seguridad en la red informática del "Hospital Millennium", para que estos no dificulten el crecimiento y desarrollo económico del mismo. Este análisis esta orientado a complementar y fortalecer la seguridad de la red informática para que se pueda brindar la seguridad necesaria tanto a la información de los pacientes como de la Institución.

Los beneficios que alcanzará la Institución con este proyecto, es la fidelidad de los accionistas y clientes, lo que ayudará, para lograr incrementar las utilidades y a formar una buena imagen ante los clientes de la misma, por otra parte se pretende beneficiar en forma directa a las grandes aspiraciones de la Institución y principalmente proteger la información manipulada dentro del Hospital.

1.4. OBJETIVOS DE LA INVESTIGACION

1.4.1. OBJETIVO GENERAL

Dotar a la red informática del Hospital Millennium de las principales seguridades que permitan confidencialidad y seguridad de la información.

1.4.2. OBJETIVOS ESPECIFICOS

- Identificar las técnicas de seguridad informática actualmente usadas.
- Mejorar las actuales técnicas de seguridad informática.
- Implementar políticas de grupo requeridas para fortalecer la seguridad institucional.
- Implementar una adecuada sincronización y respaldo de usuarios y servidores.
- Evaluar y sugerir la implantación de un antivirus corporativo que contribuya a una eficiente seguridad informática.
- Planeación de la seguridad en la red y acceso a Internet.
- Implementación de un servidor corporativo para actualizaciones de software.

CAPITULO II

MARCO TEORICO

2.1. ANTECEDENTES INVESTIGATIVOS

Revisando archivos se determinó que existen trabajos relacionados con la presente investigación.

Algunos de los cuales se citan a continuación.

Freddy Darío Salazar Hidalgo. “Aseguramiento de la red del Centro de Informática de la Universidad Técnica de Ambato para protegerla de los ataques de denegación de servicios (DoS)”. Facultad de Ingeniería en Sistemas (FIS) de la Universidad Técnica de Ambato (UTA).

Santiago Nicolás Cortes Torres. “Estudio sobre soluciones y protección contra virus informáticos en sistemas Microsoft”. FIS – UTA.

Silvia Llerena. “Manejo de Seguridad en Redes Locales inalámbricas WLAN mediante la aplicación de redes privadas virtuales VPN”. FIS – UTA.

Franklin Danilo Ortega Castro. “Implantación de un sistema de Detección de intrusos en la Red Informática de la Universidad Técnica de Ambato”. FIS – UTA.

En conclusión este tipo de investigaciones están orientadas al mejoramiento y fortalecimiento de las redes corporativas y en consecuencia de la Institución, optimizando acceso a la información y garantizando el correcto respaldo y privacidad de la misma, ya que indican que al realizar un control más minucioso los datos serán confiables y las actividades diarias no se dificultarán inesperadamente.

Lo que será considerado para este trabajo y ayudará ha diseñar un sistemas de seguridad que se ajuste a las necesidades del Hospital Millennium.

2.2. FUNDAMENTACION LEGAL

El Hospital se constituyó como Compañía Anónima denominada “Hospital Millennium, HOSPIMILLENNIUM S.A.”, en la ciudad de Ambato el 1 de Agosto de 2003, con 81 Accionistas y regida por la ley de compañías.

Algunos de los estatutos del Hospital Millennium se citan a continuación.

ARTICULO PRIMERO.- Hospital Millennium, HOSPIMILLENNIUM S.A. es una compañía de nacionalidad Ecuatoriana, que se rige por las leyes vigentes en el Ecuador.
…

ARTICULO SEGUNDO.- OBJETO.- El objeto principal de la compañía es el de dedicarse a la prestación de servicios médicos, quirúrgicos y de reposo, a través de la instalación y explotación de establecimientos asistenciales y la atención de enfermos y/o internados. Ejercerá la dirección técnica y administrativa de dichos establecimientos, abarcando todas las especialidades, servicios y actividades que se relacionan directa o indirectamente con el área médica.
…

ARTICULO TERCERO.-DOMICILIO.- LA compañía tiene su domicilio principal en el cantón Ambato, provincia de Tungurahua, República del Ecuador.

…

Acuerdo Internacional

El 10 de Noviembre del 2005, se firmó el Contrato de Administración hospitalaria entre Hospital Millennium y American Hospital Management Company de Estados Unidos

de Norteamérica, empresa privada cuya oficina base se halla radicada en la ciudad de Boston y que cuenta con experiencia en la dirección de clínicas y hospitales de Centro, Sudamérica y el Caribe.

Licencias de Software

El Hospital Millennium cuenta con licencias de software en:

- Windows 2003 Server Standard R2 32bits y 64bits
- SQL Server 2005 Standard 32bits y 64bits
- Windows XP Profesional

2.3. CATEGORIZACIONES FUNDAMENTALES

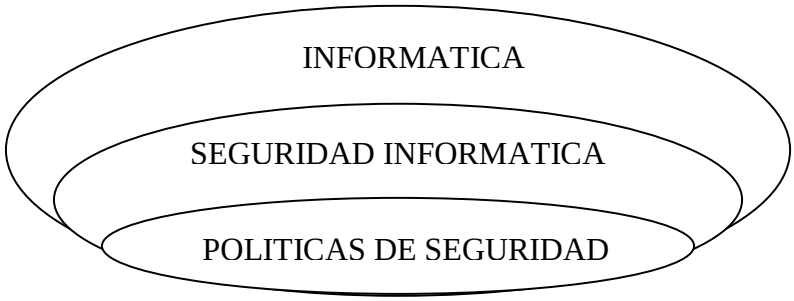


Figura 2.1 Categoría Fundamental 1

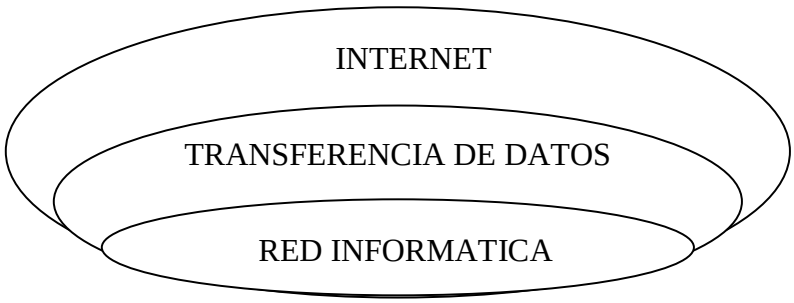


Figura 2.2 Categoría Fundamental 2

A continuación se expondrán las diferentes definiciones de las categorías que intervienen en la presente investigación.

INFORMATICA [01], “Ciencia del tratamiento racional, por medio de máquinas automáticas, de la información, considerada ésta como soporte de los conocimientos humanos y de las comunicaciones, en los campos técnico, económico y social.”

INFORMATICA [01], “Conjunto de Técnicas, métodos y máquinas aplicados al tratamiento lógico y automático de la información.”

INFORMATICA [01], “Actividad científica dirigida a la investigación de los medios (físicos e intelectuales) que permiten el tratamiento y elaboración automática de las informaciones necesarias para el desarrollo de las actividades humanas.”

Analizando las definiciones anteriores considero que Informática es la ciencia que estudia el tratamiento automático de la información.

SEGURIDAD INFORMATICA [02], “Es la definición y posterior implementación de protecciones, políticas y procedimientos, en búsqueda de la preservación de la integridad, disponibilidad y confidencialidad de la información, los recursos que la soportan (hardware, software, fireware, dispositivos de comunicación) y los individuos que la utilizan o conocen.”

SEGURIDAD INFORMATICA [02], “Es la administración de riesgos, definición, creación e implementación de políticas de seguridad, procedimientos, estándares, guías, clasificación de información, organización de la estructura de seguridad de la compañía, y la educación de los individuos de la organización.”

Analizando los conceptos de Seguridad Informática concluyo que es el estudio, creación y administración de políticas, métodos y procedimientos que permitan la

confidencialidad y seguridad de la información ya sea personal o de grandes corporaciones.

En la Seguridad Informática se deben considerar otros conceptos fundamentales como: integridad, confidencialidad, autenticidad, disponibilidad, no rechazo, los que se tratarán a continuación.

Integridad [03]. La información no puede ser modificada por quien no está autorizado.

Confidencialidad [03]. La información solo debe ser legible para los autorizados.

Disponibilidad [03]. La información debe estar disponible cuando se necesita.

Irrefutabilidad (No-Rechazo) [03]. Que no se pueda negar la autoría.

POLITICAS DE SEGURIDAD [03], “Son las que se encargan de asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación, estos mecanismos permiten saber que los operadores tiene sólo los permisos que se les dio.”

Analizando el concepto de Políticas de Seguridad puedo decir que son las que se encargan de establecer las medidas preventivas y correctivas en caso de sufrir un ataque informático.

INTERNET [04], es un sistema mundial de redes de computadoras, un conjunto integrado por las diferentes redes de cada país del mundo, por medio del cual un usuario en cualquier computadora puede, en caso de contar con los permisos apropiados, acceder información de otra computadora y poder tener inclusive comunicación directa con otros usuarios en otras computadoras.
Fue concebido por la agencia de nombre ARPA (Advanced Research Projects Agency) del gobierno de los Estados Unidos en el año de 1969 y se le conocía inicialmente como

ARPANET. El propósito original fue crear una red que permitiera a los investigadores en un Campus poder comunicarse a través de los sistemas de cómputo con investigadores en otras Universidades.

Hoy en día, el Internet es un medio de comunicación público, cooperativo y autosuficiente en términos económicos, accesible a cientos de millones de personas en el mundo entero. Técnicamente, lo que distingue al Internet es el uso del protocolo de comunicación TCP/IP (Transmission Control Protocol/Internet Protocol).

Para muchos usuarios del Internet, el correo electrónico (e-mail) ha reemplazado prácticamente al servicio postal para breves mensajes por escrito. El correo electrónico es la aplicación de mayor uso en la red. También se pueden realizar conversaciones "en vivo" con otros usuarios en otras localidades usando el IRC (Internet Relay Chat). Más recientemente, el software y hardware para telefonía en Internet permite conversaciones de voz en línea.

INTERNET [05], “Internet es una Red informática de transmisión de datos para la comunicación global que permite el intercambio de todo tipo de información (en formato digital) entre sus usuarios. El nombre proviene del acrónimo de las palabras inglesas International Network (red internacional).”

Analizando las definiciones de Internet considero que este es la Red de Redes ya que en la actualidad es el medio por el cual se realizan la mayor parte de transacciones comerciales, publicidad, etc. y permite además la comunicación en tiempo real de millones de personas de todo el mundo.

Entre otros términos igualmente importantes manejados en el ámbito de Internet tenemos los siguientes: web, página web, sitio web, portal, correo electrónico, buscador. Web [04], World Wide Web, o simplemente Web, es el universo de información accesible a través de Internet, una fuente inagotable del conocimiento humano.

Página Web [04], Una página de Internet o página Web es un documento electrónico que contiene información específica de un tema en particular y que es almacenado en algún sistema de cómputo que se encuentre conectado a la red mundial de información denominada Internet, de tal forma que este documento pueda ser consultado por cualesquier persona que se conecte a esta red mundial de comunicaciones y que cuente con los permisos apropiados para hacerlo.

Sitio Web [04], Es un conjunto de archivos electrónicos y páginas Web referentes a un tema en particular, que incluye una página inicial de bienvenida, generalmente denominada home page, con un nombre de dominio y dirección en Internet específicos.

Portal [04], es un término, sinónimo de puente, para referirse a un Sitio Web que sirve o pretende servir como un sitio principal de partida para las personas que se conectan al World Wide Web.

Correo Electrónico (email, electronic mail) [04], es el intercambio de mensajes almacenados en computadora por medio de las telecomunicaciones. El correo puede ser enviado tanto a individuos en lo particular como a listas de distribución.

Buscador o Motor de Búsqueda [04], Es un conjunto de programas coordinados que se encargan de visitar cada uno de los sitios que integran el Web, empleando los propios hipervínculos contenidos en las páginas Web para buscar y leer otros sitios, crear un enorme índice de todas las páginas que han sido leídas y registradas, llamado comúnmente catálogo, y mantener una copia actualizada de toda esta información, para luego presentar direcciones en Internet como resultado de las peticiones de búsqueda solicitadas por las personas que usan estos servicios de localización de páginas.

TRANSFERENCIA DE DATOS [06], Envío y/o recepción de datos a través de algún medio en una red o a través de un puerto. Para poder lograr una transferencia debe existir algún tipo de conexión (alambrada o inalámbrica) y un lenguaje en común

(protocolo) entre los dispositivos que se conectan. Las transferencias tienen un ancho de banda y una velocidad que suele medirse en bps o similares.

Analizando la definición anterior considero que la Transferencia de Datos es el envío y recepción ya sea de datos o información entre varias personas cos fines personales o institucionales a través de un lenguaje común.

RED INFORMATICA [04], En términos de tecnologías de información, una red es una serie de puntos o nodos interconectados por algún medio físico de comunicación. Las redes pueden interconectarse con otras redes y contener sub-redes.

La topología más común, o configuración general de redes, incluye el bus, la estrella, y las topologías token ring. Las redes se pueden clasificar también en términos de la separación física entre nodos, como redes de área local (LAN, local area network), redes de área metropolitana (MAN, metropolitan area network), y redes de área amplia (WAN, wide area network).

Una cierta clase de redes puede también ser clasificada por el tipo de tecnología de la transmisión de datos que se emplea. Por ejemplo, una red TCP/IP (Transport Control Protocol/Internet Protocol), o una red del tipo SNA (Systems Network Architecture); si transporta voz, datos, o ambas clases de señales; por quién puede utilizar la red (pública o privada); por la naturaleza de sus conexiones (conmutada, dedicada o no dedicada, o por conexión virtual); y por los tipos de conexiones físicas (por ejemplo, fibra óptica, cable coaxial, y par trenzado sin blindaje UTP). Las grandes redes de telefonía y las redes que usan su infraestructura (tal como el Internet) disponen de acuerdos para compartir e intercambiar recursos con otras compañías para formar redes mucho más grandes.
Analizando la definición anterior considero que una Red Informática es la que permite la comunicación entre dos o más computadoras, las redes se clasifican y administran de acuerdo a su tamaño, siendo la red más grande y más conocida a nivel mundial el Internet.

2.4. DETERMINACION DE VARIABLES

2.4.1. VARIABLE INDEPENDIENTE

Políticas de Seguridad.

2.4.2. VARIABLE DEPENDIENTE

Red Informática del “Hospital Millennium”.

2.5. HIPOTESIS

La implementación de Políticas de Seguridad, permitirá que la red informática del Hospital Millennium brinde la adecuada seguridad de la información y se pueda prevenir cualquier eventualidad que interrumpa las actividades diarias de la Institución.

CAPITULO III

METODOLOGIA

3.1. ENFOQUE

La presente investigación es predominante cualitativa, porque busca la comprensión de los problemas y es participativa e interna.

3.2. MODALIDAD DE INVESTIGACION

La elaboración de este trabajo y la ejecución de la investigación esta orientado hacia la investigación de Campo y Bibliográfica.

Investigación Bibliográfica se toma en cuenta porque el trabajo se ejecutará con datos obtenidos de fuentes de investigación científica disponibles como son: libros, periódicos, revistas, artículos, búsqueda en Internet, etc. Con el propósito de conocer y resolver el problema.

Investigación de Campo, se empleará con el propósito de verificar la hipótesis de trabajo, se acudirá a recopilar información primaria a través de entrevistas en la Institución, al jefe del departamento de sistemas, para de está manera conocer lo necesario para cumplir con los objetivos de la investigación.

3.3. NIVELES O TIPOS DE INVESTIGACION

Para la ejecución de la presente investigación se utilizará los siguientes tipos de investigación: exploratoria, descriptiva y explicativa.

Utilizaremos la exploratoria porque nos permitirá determinar el problema e identificar la incidencia dentro de la empresa, la descriptiva porque permitirá detallar las características primarias del objeto de estudio en lo que respecta a su origen y desarrollo, y la explicativa porque medirá el grado de relación de dos fenómenos, como son la variable dependiente en virtud de variaciones con la independiente.

3.4. POBLACION Y MUESTRA

En el problema objeto de investigación se identifica a la población motivo de estudio para el presente proyecto, que son los dos empleados pertenecientes al área de sistemas.

3.5. TECNICAS E INSTRUMENTOS DE INVESTIGACION

Para la ejecución de la presente investigación utilizaremos las siguientes técnicas e instrumentos:

Tipo de Información	Técnicas de Investigación	Instrumentos de Recolección de Información
▪ Información Secundaria	o Lectura Científica	~ Libros de Seguridad Informática ~ Tesis de grado ~ Internet
▪ Información Primaría	o Entrevista o Observación	~ Conversación ~ Trato con la Empresa

Tabla 3.1. Técnicas e Instrumentos de Investigación

CAPITULO IV

MARCO ADMINISTRATIVO

4.1. RECURSOS

4.1.1. INSTITUCIONALES

Hospital Millennium.

Biblioteca de la Facultad de Ingeniería en Sistemas, Universidad Técnica de Ambato.

4.1.2. HUMANOS

Investigador: Franklin Geovanny Flores Saltos

Coordinador Empresarial: Ing. Alex Luna, jefe del Departamento de Sistemas del Hospital Millennium.

Tutor: Ing. Clay Aldás, profesor de la Facultad de Ingeniería en Sistemas de la Universidad Técnica de Ambato.

4.1.3. MATERIALES

Equipo de cómputo

Libros

Suministros y materiales de oficina

Material Bibliográfico

Transporte

Flash Memory, CDS

4.1.4. FINANCIERO

Recursos Materiales

Nº	Denominación	C. Unitario	C. Total
1	Flash Memory (512 GB)	25.00	25.00
7	Empastado del informe	0.90	6.30
4	CDS. Grabables	0.75	3.00
3	Carpeta de Manila	0.25	0.75
	Transporte	0.18	100.00
	Alimentación	-	180.00
50	Copias de color negro	0.02	10.00
180	Impresiones	0.10	18.00
	Total		**343,05**

Tabla 4.1 Recursos Materiales

Recursos Físicos

Nº	Denominación	Tiempo	C. Unitario	C. Total
1	Centro de computo	60 horas	0.80	48.00
1	Cyber café	30 horas	1.00	30.00
	Total			**78.00**

Tabla 4.2 Recursos Físicos

Presupuesto Total

Denominación	Valor
Recursos materiales	343,05
Recursos físicos	78.00
Sub. Total	**421,05**
Imprevistos	80.00
Total	**501,05**

Tabla 4.3 Presupuesto Total

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Con el mejoramiento de las técnicas de seguridad informática, los datos sensibles o importantes de la Institución están protegidos contra algún posible intento de robo de información.

- La implementación de políticas de seguridad informática, facilitan la administración de red, así como reducen errores de los usuarios por mal manejo en los computadores.

- Con la realización de copias de seguridad periódicas de datos importantes, se asegura la recuperación total o en su mayoría de la información respaldada, en caso de producirse daño o pérdida de un computador.

- La implementación de Kaspersky Anti-Virus 6.0 permitió fortalecer la seguridad de la información sensible en la Institución, protegiéndola principalmente de virus informáticos.

- La sencillez de manejo del software Anti-Virus en los clientes, es posible gracias a las facilidades de configuración y control que brinda el módulo de administración del mismo.

- Con un correcto control de acceso y asignación de permisos a los datos, se garantiza que la información es manipulada y utilizada por las personas responsables de ésta.

- Con la implementación del Servidor Corporativos de Actualizaciones Windows Server Update Service 3.0, el software de los computadores miembros de la red informática, se mantendrán correctamente actualizados mejorando su rendimiento, seguridad y productividad en la organización

5.2. RECOMENDACIONES

- Estudiar el alcance y funcionalidad del Objeto de Política de Grupo, antes de habilitar o no sus opciones de configuración.

- Investigar que información debe ser manipulada por cada usuario, antes de asignar los permisos de acceso a cada archivo o directorio compartido en la red.

- Configurar el Windows Server Update Services, para que descargue sólo las actualizaciones de software que los computadores de la Institución requieren.

- Evaluar las capacidades de protección en tiempo real del software Anti-Virus, utilizando programas que simulen virus informáticos.

- Identificar la información importante y vital para la Institución, antes de realizar cualquier tarea de respaldo o copia de seguridad.

- Realizar las copias de seguridad de información cada cierto tiempo en cintas magnéticas para que el Servidor de Backups no se sobrecargue de datos.

- Elaborar un plan de contingencia que proteja la información importante de la Institución, en caso de presentarse algún tipo de desastre.

- Instruir a los usuarios del uso adecuado y recomendado que deben dar a los computadores, para de esta manera ayudar a complementar las políticas de seguridad informática de la Institución.

- Capacitar al personal para que puedan resolver problemas informáticos leves que se les presentan durante sus labores diarias, sin requerir la presencia del personal del área de sistemas.

5.3. BIBLIOGRAFIA

SALAZAR HIDALGO, Freddy Darío *Aseguramiento de la red del Centro de Informática de la Universidad Técnica de Ambato para protegerla de los ataques de denegación de servicios (DoS)* Facultad de Ingeniería en Sistemas (FIS) de la Universidad Técnica de Ambato (UTA).

CORTES TORRES, Santiago Nicolás *Estudio sobre soluciones y protección contra virus informáticos en sistemas Microsoft* FIS – UTA.

LLERENA, Silvia *Manejo de Seguridad en Redes Locales inalámbricas WLAN mediante la aplicación de redes privadas virtuales VPN* FIS – UTA.

ORTEGA CASTRO, Franklin Danilo *Implantación de un sistema de Detección de intrusos en la Red Informática de la Universidad Técnica de Ambato* FIS – UTA.

INFOMILLENNIUM, Boletín Informativo – Hospital Millennium, Ambato – Abril 2006, Nº 2.

REFERENCIAS WEB

[01] Programación, Ingeniero de Telecomunicaciones. 1º Curso. Disponible en: http://www.dei.inf.uc3m.es/docencia/p_s_ciclo/telecosTecnicas/teoria/tema1.pdf - 20-marzo-2007

[02] SÁNCHEZ ACEVEDO, Nicolás, SEGURA CASTAÑEDA, Juan Sebastián. Una Guía Metodológica para el Cálculo del Retorno de la Inversión en Seguridad

Informática: Un Caso de Estudio. Tutor: Jeimy Cano. Pontificia Universidad Javeriana, Departamento de Sistemas (Colombia). Año 2006. Disponible en: http://www.criptored.upm.es/paginas/ investigacion.htm - 20-marzo-2007

[03] Seguridad Informática. Disponible en: http://www.lenguajebinario.com.ar/foro/image-vp4427.html - 20-marzo-2007

[04] Principales definiciones de los términos más usados en Internet. Disponible en: http://www.informaticamilenium.com.mx/Paginas/espanol/sitioweb.htm#dinternet - 20-marzo-2007

[05] Definición de Internet. Disponible en: http://www.definicion.org/internet - 20-marzo-2007

[06] Definición de Transferencia. Disponible en: http://www.alegsa.com.ar/Dic/transferencia.php - 20-marzo-2007

[07] Microsoft Windows Server 2003. Disponible en: http://www.elrincondelprogramador.com/default.asp?pag=articulos%2Fleer.asp&id=60 – 5-septiembre-2007

[08] Políticas de seguridad Informática. Disponible en: http://www.segu-info.com.ar/tesis/index.htm – 5-septiembre-2007

[09] Guía de Microsoft Windows Server 2003. Disponible en: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/2e0186ba-1a09-42b5-81c8-3ecca4ddde5e.mspx?mfr=true – 5-septiembre-2007

[10] Windows Server Update Services. Disponible en: http://www.microsoft.com/latam/windowsserversystem/updateservices/compare/default.asp – 5-septiembre-2007

[11] Descripción de Linux. Disponible en:
http://fismat.umich.mx/~yenisei/guialinux.html - 10-septiembre-2007

[12] Tipping Point – Detalles de Producto. Disponible en:
http://www.3com.com/prod/es_ES_EMEA/detail.jsp?tab=features&sku=3CRTPX505-96 - 06-septiembre-2007

[13] Virtual Server 2005 R2. Disponible en:
http://www.webmasters.cl/foro/showthread.php?t=637 – 06-septiembre-2007

CAPITULO VI

PROPUESTA FINAL

6.1. ANALISIS

6.1.1. ANALISIS DE LA SEGURIDAD INFORMATICA ACTUAL

La red informática de la Institución se maneja de forma estructurada y con un número pequeño de computadores clientes con Sistema Operativo Windows XP y teniendo como controlador de dominio, un Servidor con Sistema Operativo Windows Server 2003.

Los computadores en su mayoría están protegidos por software Anti-Virus personales y diferentes, no administrados de forma centralizada, siendo vulnerables a virus o gusanos informáticos. Al no poder controlar la habilitación o deshabilitación de la protección en tiempo real del Anti-Virus, los usuarios tienen la posibilidad de controlar a su gusto la protección del computador, dejando vulnerable información importante, a ataques ya sea de algún tipo de virus o piratas informáticos. Las consecuencias de no proteger adecuadamente la información se presentan desde pequeñas interrupciones en las labores diarias de la Institución, hasta graves pérdidas económicas.

La mayor parte de computadores están controlados por claves de acceso al Bios y para el Sistema Operativo como usuario administrador del dominio o local; los usuarios de cada equipo manejan su propia clave de acceso con los permisos requeridos para sus labores diarias. Si un computador no está protegido con claves de acceso ya sea al Bios o al Sistema Operativo, algún usuario ajeno a la Institución o al área laboral podrá cambiar sin ninguna dificultad configuraciones necesarias en el equipo para su buen funcionamiento, este tipo de problemas interrumpen el desempeño de labores diarias.

Las actualizaciones de software que Windows XP las hace automáticamente, se las descarga cada equipo según la programación que tenga dicha tarea. La descarga independiente de actualizaciones por cada computador congestiona y reduce el ancho de banda que tiene la Institución para navegar en Internet.

Los usuarios pueden personalizar o configurar de acuerdo a sus gustos y preferencias los ambientes de trabajo de su computador, ya sea propiedades de pantalla, página de inicio de Internet Explorer, habilitar o deshabilitar a su conveniencia la red; ya que ningún objeto de política de grupo restringe la posibilidad de hacerlo. La imagen de una Institución debe también fortalecerse con cosas pequeñas como la utilización de ambientes de trabajo comunes, en todos los computadores de ésta; al no poder configurar su computador, los usuarios pueden sentirse inconformes o molestos, pero si se difunden las ventajas de la utilización o estandarización de configuraciones comunes en los equipos, se comprenderá de necesidad de las mismas.

Las copias de seguridad se las realiza sólo en ciertas áreas o usuarios específicos, de manera que toda la información importante no está realmente protegida en caso de algún daño o perdida de equipo, esto puede ocasionar perdidas significativas a la Institución, ya sean estas de información o económicas.

El acceso a Internet no está controlado y se lo puede hacer desde cualquier punto de red de la Institución con conexión habilitada, sin restricción alguna de navegación en la web. La navegación sin restricción puede ocasionar que usuarios no autorizados visiten páginas peligrosas o descarguen archivos nocivos, para los computadores o la información de la red interna. La utilización de Internet sin control reduce significativamente el ancho de banda, haciendo lentas tareas realmente importantes que muchos usuarios requieren hacer como parte de sus labores diarias.

6.1.2. PROPUESTA DEL NUEVO CONTROL DE SEGURIDAD INFORMATICA

Para que la información en una Institución esté bien protegida se requiere la implementación de políticas de seguridad que abarcan desde la correcta selección de hardware y software, hasta de pequeñas tareas globales o en cada computador.

En la actualidad se cuenta con diferentes Sistemas Operativos, que se los utiliza ya sea por las facilidades que presentan o de acuerdo a las actividades laborales de la empresa. Los más reconocidos actualmente son los Sistemas Servidores Windows y Linux.

[11] Linux es un sistema operativo, compatible Unix. Dos características muy peculiares lo diferencian del resto de los sistemas que se encuentran en el mercado, la primera, es que es libre, esto significa que no hay que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo, la segunda, es que el sistema viene acompañado del código fuente, es decir que se puede cambiarlo para adaptarlo a las necesidades de la Institución. El sistema lo forman el núcleo (kernel) más un gran número de programas / librerías que hacen posible su utilización. En los últimos tiempos, ciertas casas de software comercial han empezado a distribuir productos para Linux y la presencia del mismo en empresas aumenta rápidamente por la excelente relación calidad-precio que se consigue.

[07] Windows Server 2003 por su parte es un sistema operativo desarrollado por Microsoft, es más escalable y posee un mejor rendimiento que su predecesor Windows 2000 Server. Su sistema de archivos es NTFS, este permite encriptación, compresión de archivos, directorios y unidades completas. Permite montar dispositivos de almacenamiento sobre sistemas de archivos de otros dispositivos como Linux, Active Directory, etc. Cuenta con una guía preceptiva y de fácil uso para soluciones que permitan poner rápidamente la tecnología a trabajar. Ayuda a consolidar servidores aprovechando lo último en metodologías, software y hardware para optimizar la implementación del servidor.

El Sistema Operativo utilizado por Hospital Millennium es Windows Server 2003, por lo que las políticas de seguridad informática a implementarse se diseñaran entorno a éste. Con el crecimiento de la red informática de la Institución, es necesaria la implementación de nuevas políticas de seguridad que complementen, fortalezcan y garanticen la seguridad de la información importante, contribuyendo de esta forma al mejoramiento y progreso de la misma.

La información clínica que se manipulará por los diferentes usuarios de la red es de gran importancia y de tratamiento muy delicado, ya que si se llegaran a cambiar de forma inconciente o no, por alguna persona no autorizada podría traer graves consecuencias en diagnósticos médicos dados al paciente y afectaría la imagen y prestigio del Hospital.

Considerando lo anterior el proyecto propuesto abarca nuevas políticas de seguridad como:

- Estandarización y control del ambiente de trabajo en todos los computadores de la Institución mediante la creación de Objetos de Políticas de Grupo mediante la Consola de Administración para Políticas de Grupo de Microsoft.

- Adquisición de un Anti-Virus Corporativo que pueda ser administrado desde el área de sistemas y distribuido en todos los computadores, protegiendo de esta manera los equipos de ataques generados por virus informáticos. Previa la adquisición del Anti-Virus se realizará un estudio minucioso de las fortalezas y debilidades de los principales software Anti-Virus en la actualidad.

- Descarga y distribución de actualizaciones de software mediante Windows Server Update Service instalado en uno de los Servidores de la Institución. Windows Server Update Service es una herramienta de Windows que permite a los administradores implementar con rapidez y fiabilidad las actualizaciones críticas y de seguridad más recientes para sistemas operativos o software específicos.

- Asignación de permisos de acceso a los datos a todos los usuarios miembros del dominio de la red informática de Hospital Millennium, estos permisos serán otorgados a través de las propiedades de cada objeto compartido que lo requiera.

- Identificación de que usuarios o equipos requieren tener copias de seguridad de la información importante para la Institución, almacenadas en el Servidor de Backups para en caso de sufrir daños o perdidas de equipos se pueda restaurar total o en su mayoría los datos perdidos, estas copias de seguridad se las realizará utilizando las herramientas que los sistemas operativos Windows proporcionan a sus usuarios, en el caso del Hospital en los Sistemas Operativos Windows: XP y Server 2003.

- Control y supervisión del acceso a Internet en todos los computadores miembros de la red, otorgando niveles de acceso según sea lo requerido por el usuario. Para esta tarea se realizará un estudio minucioso de la estructura de la red y de los niveles de acceso que cada usuario tendrá, para de esta manera poder formar grupos de usuarios o segmentos de red que permitan realizar el control requerido.

6.1.3. ALCANCE

A través de la implantación de las nuevas políticas de seguridad se podrá realizar las operaciones de control que ayudarán a fortalecer la estructura informática del Hospital Millennium, HOSPIMILLENNIUM S.A., entre las operaciones más destacadas tenemos las descritas a continuación:

- Configuración y control de las estaciones de trabajo miembros del dominio.

- Control y monitoreo centralizado del software Anti-Virus distribuido en toda la red de la Institución.

- Actualización periódica de software tanto en las Estaciones de trabajo como en los Servidores.

- Control de Acceso a la información de la Institución por personal no autorizado para manipularla.

- Copias de Seguridad de la información sensible e importante para el Hospital Millennium.

- Control de acceso a Internet, otorgando niveles de permisos de navegación, según lo requiera el usuario de acuerdo a su área laboral.

6.1.4. ANALISIS DE RESTRICCIONES

Las principales restricciones que presentará el proyecto son las siguientes:

- Evitar que los usuarios administradores de su propio computador puedan cambiar ciertas configuraciones del sistema.

- Garantizar que los computadores no adquieran virus informáticos, ya que ningún software Anti-Virus es cien por ciento seguro y confiable.

- Evitar que los usuarios puedan revelar sus claves de acceso al sistema a otros usuarios y con esto ellos puedan ver o manipular información a la cual no están autorizados.

- Evitar que usuarios que tengan acceso a información importante puedan borrarla o manipularla de forma indebida

- En caso de pérdidas de información importante las copias de seguridad no garantizan que al restaurarlas devuelvan dicha información en su totalidad.

- La información de los usuarios y servidores, que se respaldará se lo hará sólo en el Servidor de Backups que posee la Institución.

- Evitar que los usuarios con acceso a Internet visiten páginas web indebidas o realicen tareas no permitidas, siempre y cuando su nivel de acceso a Internet se lo permita.

6.1.5. ESTUDIO DE FACTIBILIDAD

6.1.5.1. FACTIBILIDAD OPERATIVA

La implementación de las políticas de seguridad informática solucionarán inconvenientes que podrían presentarse a corto o largo plazo en la Institución, en relación al manejo o manipulación de la información sensible, por lo que se garantiza que el personal asumirá las nuevas reglas de manejo y acceso a los datos importantes, y hará un uso más eficiente de los recursos de red.

6.1.5.2. FACTIBILIDAD TECNICA

Las herramientas de software necesarias para la realización del proyecto se encuentran disponibles en su mayoría en la Institución y otras se podrán descargar gratuitamente del sitio oficial de Microsoft. El software que se utiliza en el Hospital Millennium, tiene su licencia respectiva, por ejemplo: Microsoft Windows Server 2003 R2 Edición Estándar, Microsoft SQL Server 2005, entre otros. Para el desarrollo del proyecto será necesaria la adquisición de las siguientes herramientas y dispositivos:

- Posterior al estudio y análisis de la eficiencia de los diferente software Anti-Virus, será requerida la adquisición del software seleccionado para poder proceder con la implementación de esté en la red informática de la Institución.

- La Institución ha previsto la adquisición de un Tipping Point (equipo de red para seguridad perimetral) para fortalecer su seguridad, este dispositivo permitirá la puesta en ejecución del estudio y diseño de los permisos de acceso a Internet y a la red interna que contempla el presente proyecto.

6.1.5.3. FACTIBILIDAD ECONOMICA

El costo que genera el diseño e implementación de las políticas de seguridad informática es bajo, ya que la mayor parte de herramientas están disponibles para el diseño y desarrollo del proyecto, siendo necesaria la compra únicamente del software Anti-Virus que sea seleccionado en el estudio. En función de ello y de los beneficios que aportará este proyecto a la seguridad de la red interna de la Institución, se lo considera económicamente factible. El costo aproximado del Software Anti-Virus es 40 dólares Americanos por computador.

6.2. DISEÑO

6.2.1. PROPUESTA

Se analizará la situación actual en cuanto a seguridades informáticas que la red de la Institución posee, determinando los puntos vulnerables y que deben ser mejorados para evitar pérdidas graves de información importante.

Se crearán nuevas políticas de seguridad informática que ayuden a fortalecer la estructura de red ya existente, protegiendo la información de los usuarios y ayudando a la Institución a mantener sus actividades diarias en normal funcionamiento.

Con la implementación de un Anti-Virus corporativo se podrá administrar y controlar la seguridad de los computadores evitando que virus informáticos dañen la información o inclusive el hardware del equipo, para complementar la protección de los datos se asignarán los permisos que cada usuario requiere para manipular la información

importante compartida en la red. Las seguridad de los datos es muy importante por esta razón se realizará copias de seguridad periódicas de toda la información sensible, de esta manera se tendrá un respaldo en casos de sufrir daños o perdidas de equipos.

Con la administración de un servidor Corporativo para Actualizaciones (Windows Server Update Services) se contribuirá para el mantenimiento de la red de computadoras, es decir que la capacidad para identificar actualizaciones e instalarlas en forma automática podrá ayudar a mantener la seguridad y productividad de los equipos de la Institución.

La implementación de objetos de políticas de grupo contribuirá a la seguridad de la red y disminuirá los errores de los usuarios, ya que permitirán configurar el ambiente de trabajo y denegar el acceso a ciertas partes del sistema operativo que puedan ocasionar errores, que deban ser resueltos por el personal del área de sistemas.

Con el control de acceso a Internet beneficiara importantemente la velocidad de las aplicaciones en red y transacciones en la web, ya que no se utilizará este servicio como un pasatiempo que distraiga a los empleados de sus labores diarias, si no que lo utilizarán para tareas laborales o de interés para la Institución.

6.2.2. HERRAMIENTAS

Las herramientas que se utilizarán para poner en marcha las diferentes fases del proyecto son las siguientes:

- Sistema Operativo Microsoft Windows Server 2003 R2 Edición Estándar, instalado como controlador de dominio en uno de los Servidores que posee la Institución.

  [07] Windows Server 2003 es un sistema operativo de propósitos múltiples capaz de manejar gran cantidad de funciones de servidor, de manera centralizada

o distribuida. Más seguro, fiable y con mayor disponibilidad que cualquiera de sus antecesores, mejorado y ampliado para aprovechar mejor los beneficios de la plataforma .NET.

Algunas de sus capacidades son:

- Servidor de archivos e impresión.
- Servidor web y aplicaciones web.
- Servidor de correo electrónico.
- Servidor de terminales.
- Servidor de acceso remoto y red privada virtual (VPN).
- Servidor de directorio, de Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), y de Windows Internet Naming Service (WINS).
- Servidor de transmisión de multimedia en tiempo real (Streaming).
- Servidor de infraestructura para aplicaciones de negocios en línea (tales como planificación de recursos de una empresa y software de administración de relaciones con el cliente).

[07] Windows Server 2003 proporciona una infraestructura integrada que ayuda a asegurar que la información de negocios este segura, y también proporciona fiabilidad, disponibilidad, y escalabilidad para que se pueda ofrecer la infraestructura de red que los usuarios solicitan. Además cuenta con herramientas flexibles que ayudan a ajustar su diseño e implementación a las necesidades organizativas y de red. Ayuda a administrar la red proactivamente al reforzar las políticas, tareas automatizadas y simplificación de actualizaciones.

- Microsoft Virtual Server 2005 R2. [13] Es una tecnología de virtualización específicamente creada para la plataforma de servidor Windows. Se trata de una pieza clave de cualquier estrategia de consolidación de servidores, ya que Virtual Server 2005 R2 aumenta el nivel de utilización del hardware y permite

al personal de IT (Tecnología de la Información) configurar y poner en servicio nuevos servidores o equipos clientes en un tiempo mínimo. Además simplifica la administración de tecnología y brinda a los clientes corporativos una mayor flexibilidad, automatización y control, permitiéndoles realizar pruebas de software en ambientes virtuales.

- Group Policy Management Console. [08] Es una herramienta o sistema de interfases programables para el manejo de Políticas de Grupo, así como las MMC (Consola de Administración Microsoft) que se construyen en estas interfases programables. Los componentes de Group Policy Management, por su parte, consolidan la administración de Políticas de Grupo a través de la empresa.

  [08] La Group Policy Management Console combina la funcionalidad de componentes múltiples en una sola interfaz de usuario (UI). La UI se estructura para emparejar la manera en que se utiliza y maneja Políticas de Grupo. Asimismo incorpora la funcionalidad relacionada con Políticas de Grupo de las siguientes herramientas en una sola MMC (Consola de Administración Microsoft):

  - Active Directory Users and Computers
  - Active Directory Sites and Services
  - Resultant Set of Policy (RSoP)

  [08] Group Policy Management también proporciona las siguientes capacidades extendidas que no estaban disponibles en herramientas anteriores de Políticas de Grupo. Con Group Policy Management se puede hacer:

  - Back up y restore de Objetos de Políticas de Grupo (GPOs).
  - Copiar e importar GPOs.
  - Usar filtros Windows Management Instrumentation (WMI).

- Generar reportes de GPO y RSoP.
- Buscar GPOs.

- Software Anti-Virus. Se utilizarán los tres principales Anti-Virus Corporativos catalogados como los mejores a nivel mundial por instituciones especializadas en el tema, y son los siguientes:
  - Kaspersky 6.0
  - BitDefender 8
  - F-Secure 6

  Características detalladas de los Anti-Virus mencionados, se detallan en el Anexo 1 (Informe de Evaluación de Anti-Virus)

- Windows Server Update Services. [10] Las principales capacidades de administración de actualizaciones que presenta esta herramienta de Microsoft se citan a continuación:

  - Control de distribución de actualizaciones centralizado: Usa un mecanismo de empuje donde los sistemas de los clientes contactan al servidor para aprobar las actualizaciones. Los administradores pueden configurar la frecuencia con la que los clientes contactan al servidor o ellos pueden utilizar una utilidad comando de línea o un script para disparar un chequeo para nuevas actualizaciones aprobadas.

  - Instalación de actualización y flexibilidad de planificación: Permite a los administradores especificar un plazo para cuando una actualización debería estar instalada en el sistema.

  - Reporte de status de instalación de actualizaciones: Provee reportes predefinidos y Standard de status de instalación. La información reportada está disponible a través de un API.

- Planificación de despliegue centralizado: Permite a los administradores identificar qué sistemas necesitan actualizaciones específicas. Los administradores pueden desplegar actualizaciones en el modo "detect-only" para permitir una mejor planificación.

- Administración de inventario: Descubre inventario de hardware básico incluido el nombre de host, versión del sistema operativo, lenguaje y dirección IP.

- Herramienta Copia de Seguridad de Windows. [09] La utilidad de Copia de seguridad ayuda a proteger los datos de pérdidas accidentales en el caso de que se produzca errores en el hardware o los medios de almacenamiento del sistema. Se puede utilizar la Copia de seguridad para crear un duplicado de los datos del disco duro y, a continuación, archivarlos en otros dispositivos de almacenamiento. El medio de almacenamiento de la copia de seguridad pueden ser una unidad lógica, como el disco duro u otro dispositivo de almacenamiento, como un disco extraíble, cintas magnéticas. Si los datos originales del disco duro se borran o se sobrescriben accidentalmente, o el acceso a estos es imposible debido a un error de funcionamiento del disco duro, se podrá restaurar los datos que estén en la copia archivada.

- Herramientas de configuración que facilite el dispositivo de Tipping Point que adquirirá la Institución. El Tipping Point es una plataforma hardware, especializada en la prevención de intrusión que consiste en tecnología avanzada del procesador de red. El dispositivo puede realizar millares de chequeos en cada flujo de paquetes simultáneamente.

  [12] El TippingPoint es un dispositivo en línea que se inserta fácil y transparente en la red. Mientras que los paquetes pasan con el IPS (Sistema de Prevención de intrusos), se examinan completamente para determinarse si son legítimos o malévolos.

[12] Los sistemas de la prevención de intrusos de Tipping Point proporcionan protección de uso, funcionamiento e infraestructura a velocidades gigabit con la inspección total del paquete. Las capacidades de protección de uso proporciona rápida, exacta y confiablemente protección contra ataques internos y externos en la red.

6.2.3. DIAGRAMA DE RED

La red informática de Hospital Millennium, HOSPIMILLENNIUM S.A. está estructurada con los grupos de computadores siguientes, cada uno con sus respectivos sub-grupos miembros:

Administración Hospital

- Gerencia
- Presidencia
- Área Financiera
- Dirección Medica
- Sistemas (Servidores y Estaciones de Trabajo)
- Seres Humanos
- Compras
- Ventas
- Marketing
- Cobranzas
- Bodega

Hospitalización

- Estaciones de Enfermería
- Farmacia
- Laboratorio
- Imágenes

- Emergencias
- Quirófanos
- Cajas y Admisiones
- Biblioteca

En las figuras siguientes se presenta la distribución de los computadores en la Institución:

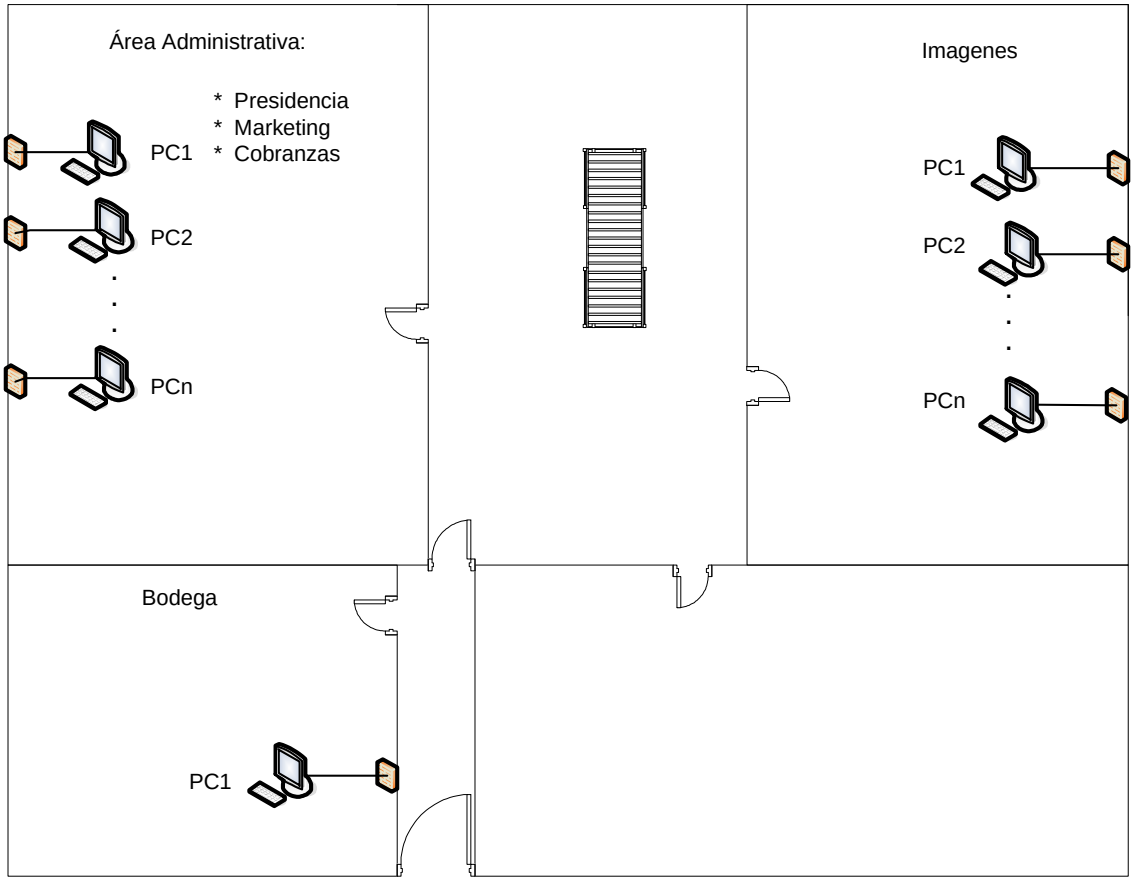


Figura 6.1. Diagrama de Red (Sub-Suelo)

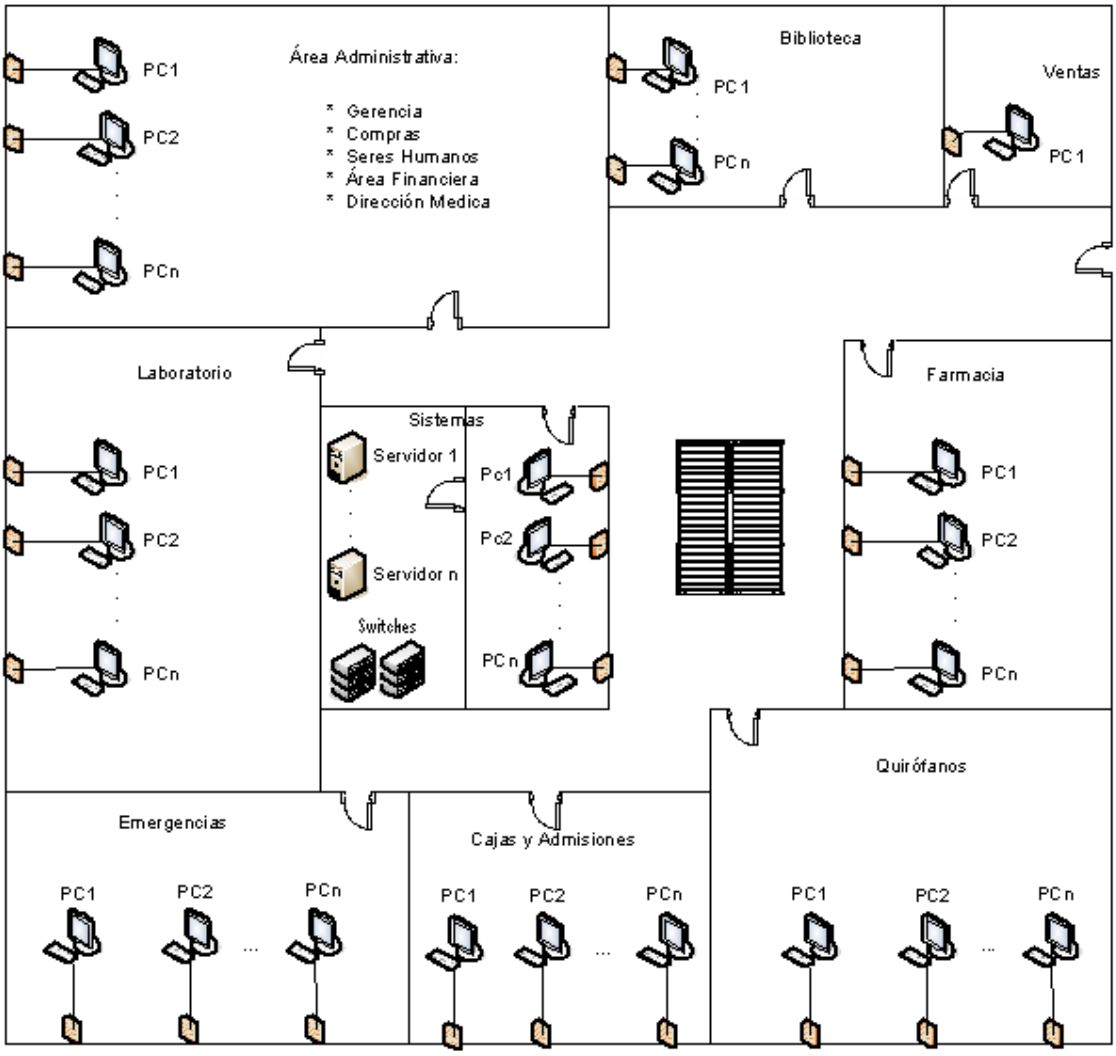


Figura 6.2. Diagrama de Red (Planta Baja)

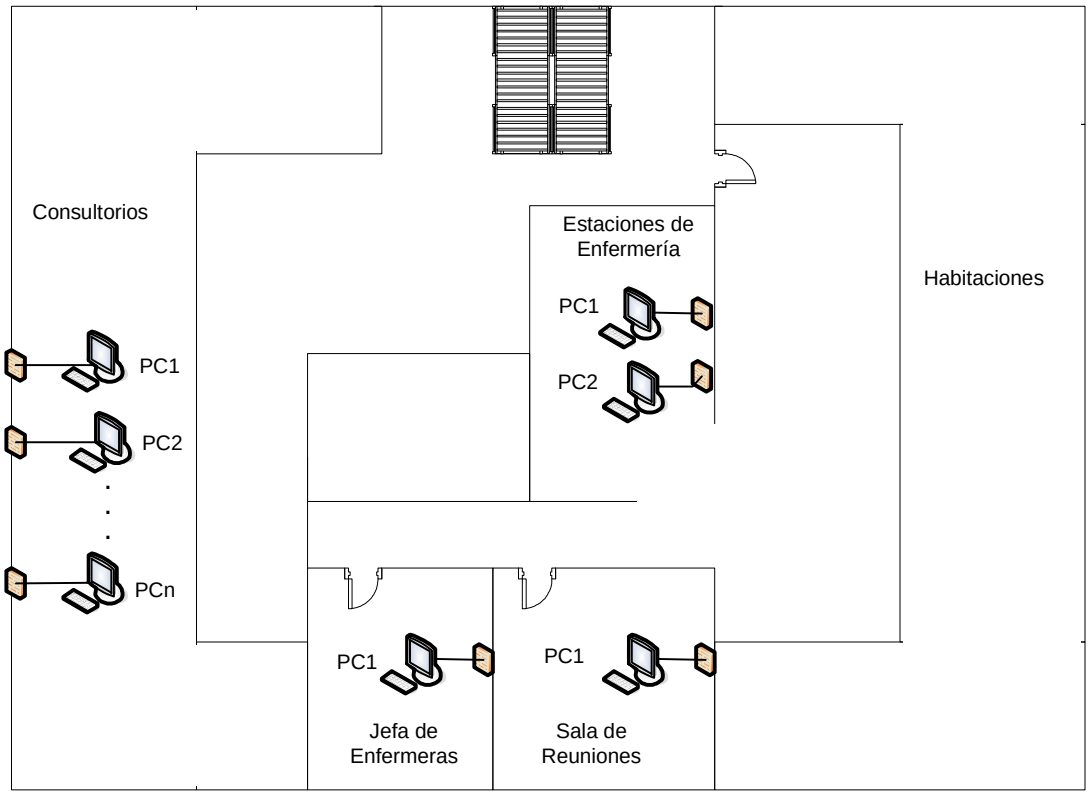


Figura 6.3. Diagrama de Red (Piso 1)

Para los Pisos 2 y 3 la distribución es similar al Piso 1, pero los computadores en la actualidad sólo están ubicados en los determinados consultorios.

6.3. IMPLEMENTACION

Para la implementación de las diferentes políticas de seguridad, fue necesario un estudio y análisis de cómo están estructurados los diferentes grupos de usuarios en el Active Directory del controlador de Dominio, y los permisos que cada usuario debería tener para acceder a los diferentes recursos de red e Internet.

Los grupos de usuarios están estructurados de acuerdo al área o departamento de trabajo. La mayor parte de información se almacena en el servidor por lo que debe ser accedida sólo por los usuarios que la necesitan, así mismo los computadores deben ser utilizados exclusivamente para las labores que cada puesto o cargo lo requieren.

IMPLEMENTACION DE DIRECTIVAS O POLÍTICAS DE GRUPO

Para la creación de Objetos de Políticas de Grupo (GPO) se consideraron entre otros, los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Adicional a esto se establecieron los grupos a los cuales se aplicarían los GPO, dividiendo en dos grupos principales a todos los usuarios y equipos miembros del dominio: Grupo Administradores y Grupo Hospital; aplicándose a estos los GPO necesarios para cumplir con los requerimientos previstos para dicho grupo.

La herramienta que se utilizó para la creación de los GPO fue Group Policy Management Console que se integra con las herramientas de administración proporcionadas por el Sistema Operativo del Servidor. Previa la creación de las GPO se realizó una revisión y estudio minucioso de las principales funciones o consecuencias que traería la habilitación o configuración de cada opción que posee un objeto de políticas en su interior. Los GPO se configuráron de acuerdo a las necesidades de cada grupo de usuarios o usuarios específicos, integrándose con la estructura del Active Directory en el Controlador de Dominio. La interface que brinda la Consola de Administración de Políticas de Grupo se muestra en la Figura 6.4.

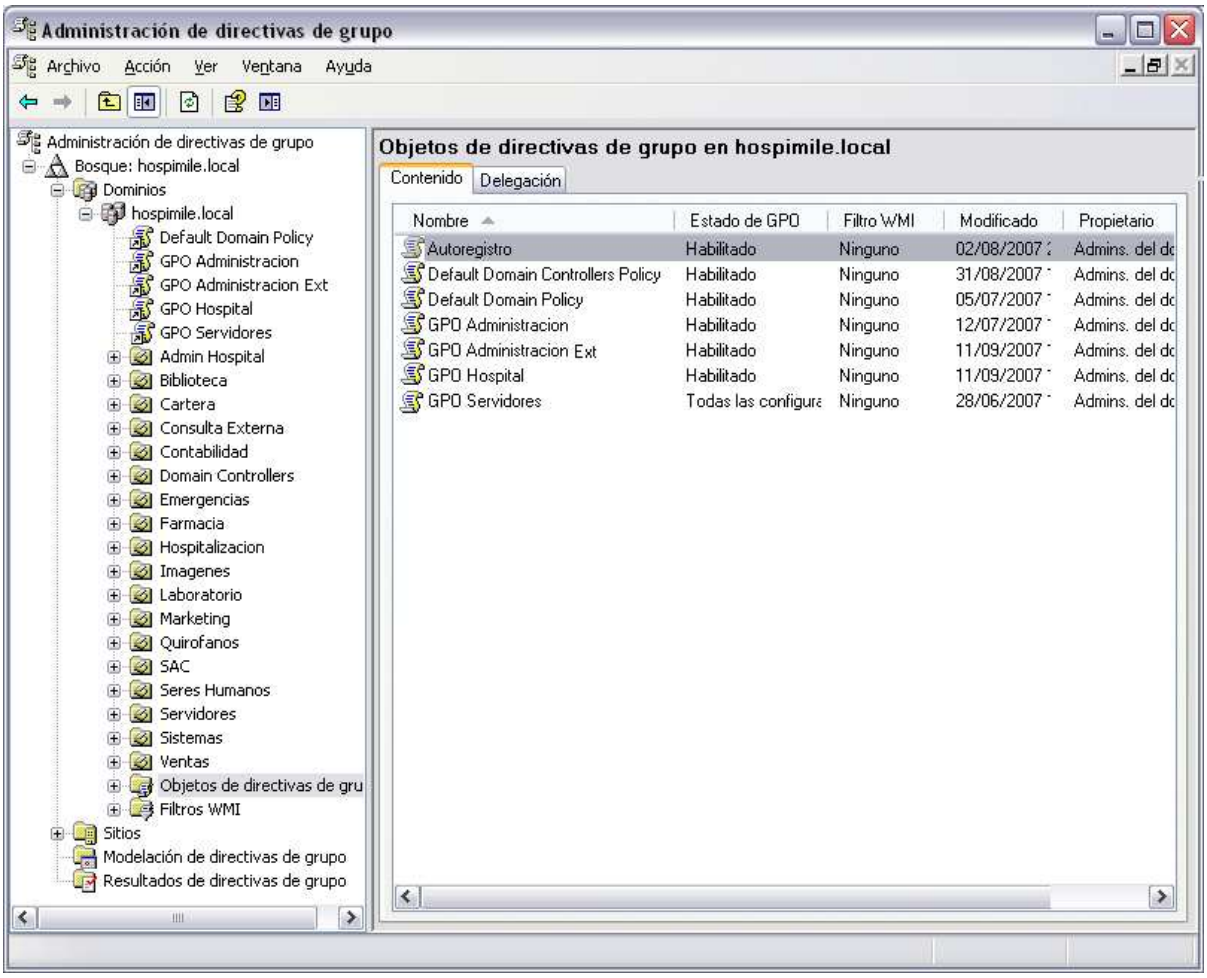


Figura 6.4. Consola de Administración de Políticas de Grupo

Mediante la implementación de los GPO se personalizó el ambiente de trabajo de todos los computadores en la Institución, dotando a cada usuario de los recursos necesarios para ejecutar sus labores diarias.

Las funciones principales de los GPO aplicados, es controlar el ambiente de configuración del Sistema Operativo impidiendo que cada usuario lo cambie, además ayudan a controlar la deshabilitación o cambio de las propiedad de la red en aquellos usuarios que son administradores de su equipo, controlan los periodos de actualización y restringen la posibilidad de deshabilitar ciertos servicios del sistema necesarios para el buen funcionamiento y seguridad del computador. Los objetos de políticas de grupo presentan el ambiente de trabajo que muestra la Figura 6.5.

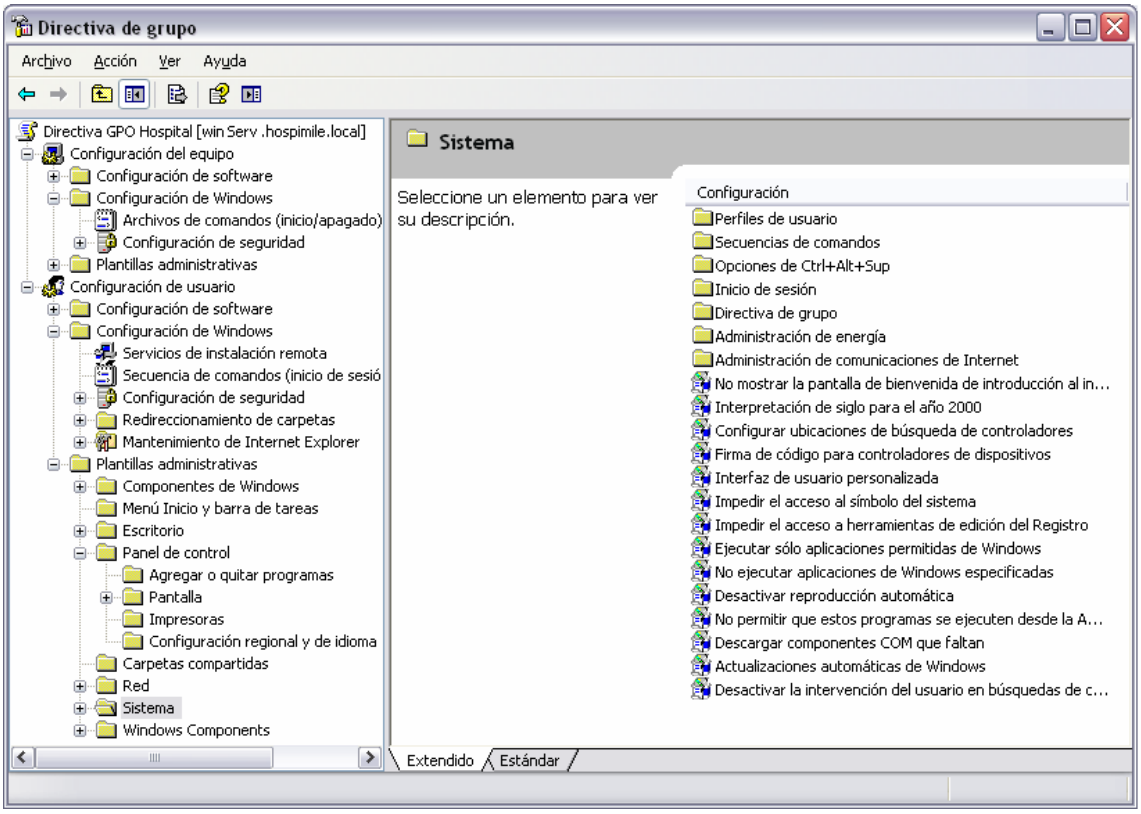


Figura 6.5. Consola de Configuración de Objetos de Políticas de Grupo

CONTROL DE ACCESO

Cuando se configuran permisos, se especifica el tipo de acceso de los grupos y usuarios. Por ejemplo, se puede permitir a un usuario leer el contenido de un archivo, dejar a otro realizar cambios en el archivo y evitar que los demás usuarios tengan acceso al mismo; la Figura 6.6 muestra el ambiente que presenta la asignación de permisos de acceso en forma general. Se puede establecer permisos similares en impresoras para que determinados usuarios puedan configurarlas y otros usuarios puedan imprimir sólo desde una o varias de ellas.

La mayor parte de permisos a nivel de archivos y directorios se las puede manipular desde las propiedades del mismo, en la ficha Seguridad. De forma predeterminada, en la familia de servidores Windows Server 2003, el propietario de los archivos y directorios

es el grupo Administradores. El propietario siempre puede cambiar los permisos de un objeto, incluso cuando a todos se les deniega el acceso al mismo.

Los permisos de acceso se configuraron realizando una pequeña investigación de que información podría ser manipulada por que usuario o grupo de usuarios, de acuerdo ha esta investigación se otorgo los permisos necesarios para que la información importante de la Institución se mantenga segura y manipulada sólo por el personal autorizado. Se puede dar permisos exclusivos o especiales a los usuarios, esto permite tener un control más estricto de acceso a la información, como se muestra en la Figura 6.7.

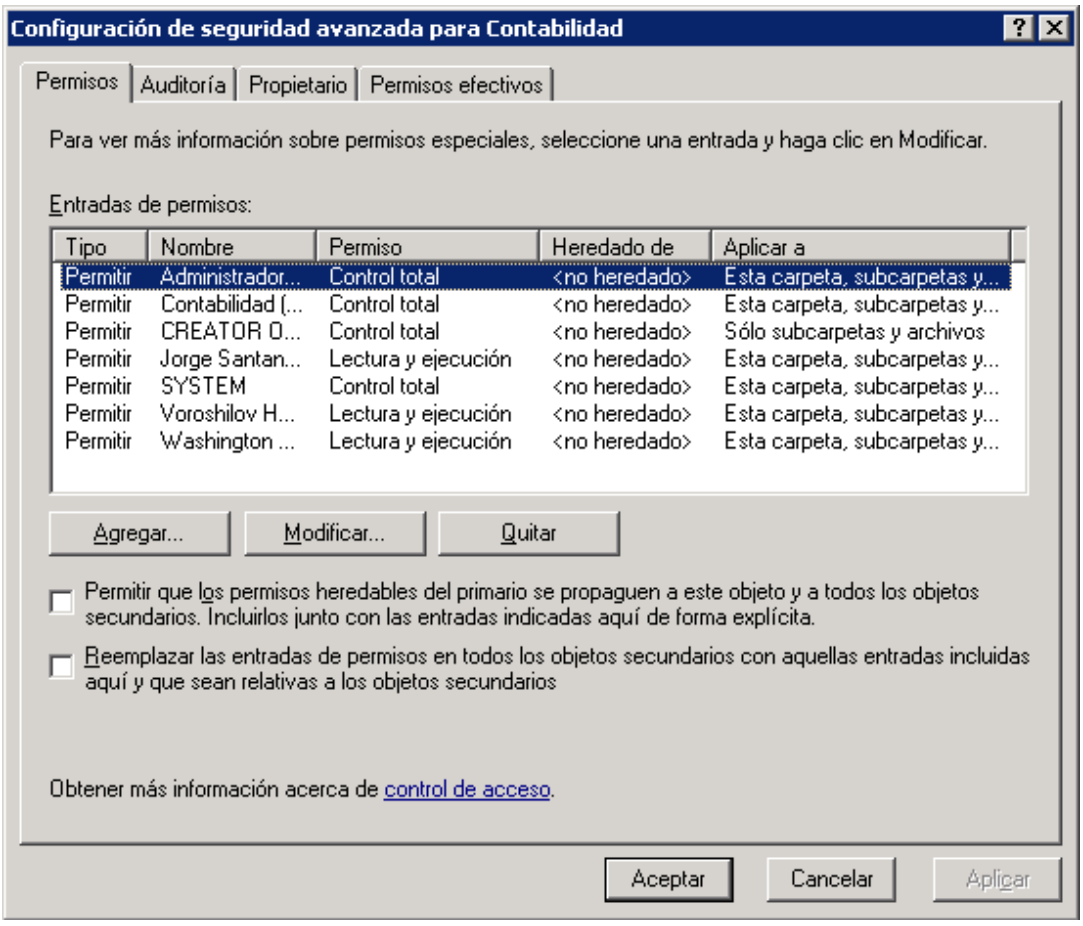


Figura 6.6. Configuración de Permisos de Acceso Generales en un Directorio

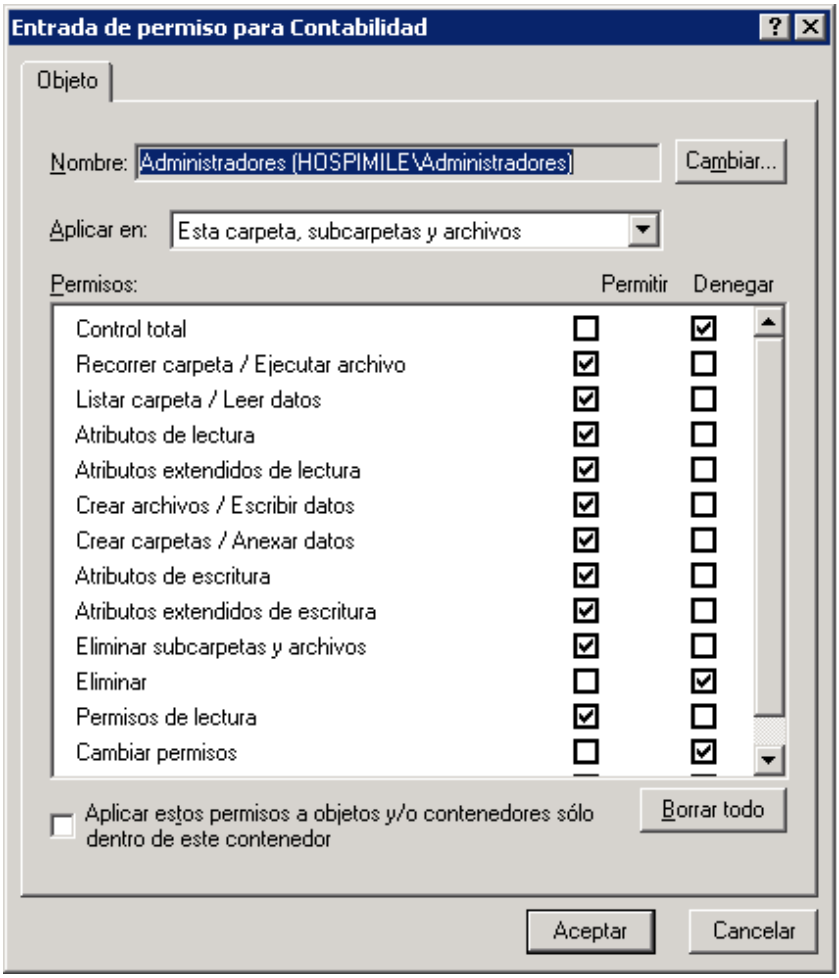


Figura 6.7. Configuración de Permisos de Acceso Especiales en un Directorio

Para complementar la seguridad de la red, control de acceso a los datos y asignación de permisos de navegar en Internet, la Institución adquirió un Tipping Point de 3COM (equipo de red para seguridad perimetral) que fue configurado por el técnico encargado de la implantación de dicho dispositivo, apoyándose en el informe de niveles de acceso tanto a la información como a Internet, el ambiente de configuración que brinda éste equipo se muestra en la Figura 6.8. Para que el dispositivo pueda ser configurado de acuerdo a las necesidades de la Institución, fue requerido complementar los niveles de acceso con una reestructuración lógica de toda la red interna del Hospital Millennium. Esta reestructuración contemplo principalmente la segmentación de la red, cada uno de estos segmentos tendría los accesos requeridos tanto para los datos como para Internet según el tipo de usuarios miembros del mismo.

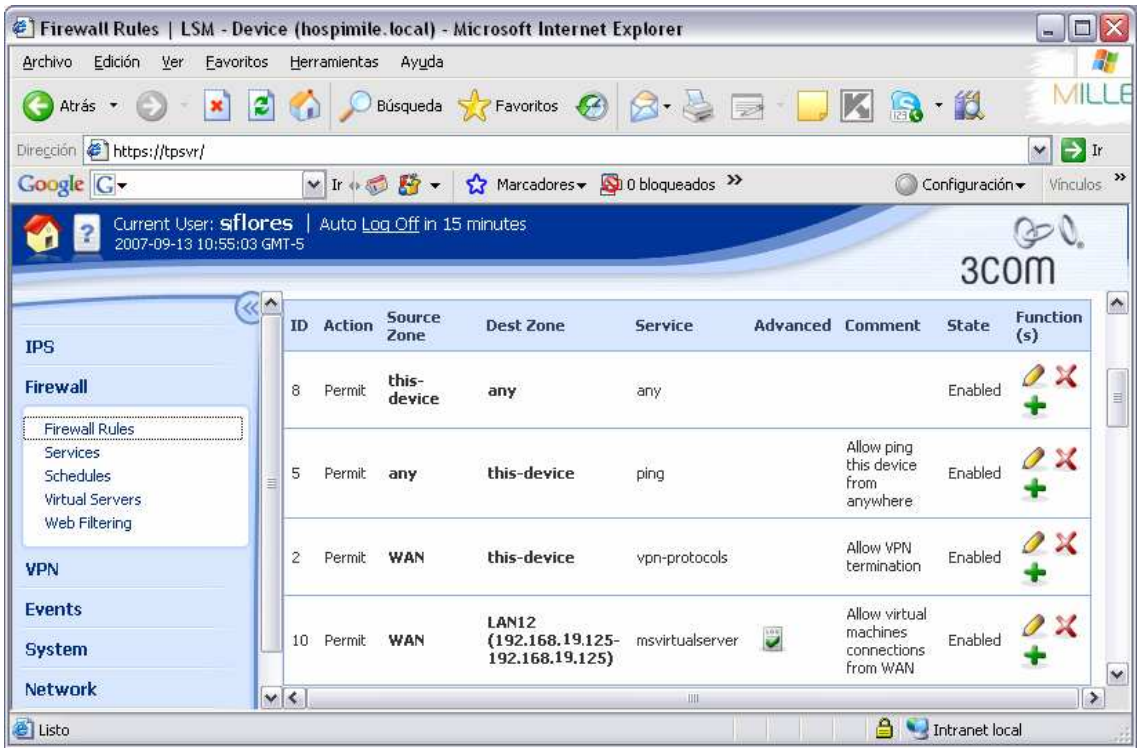


Figura 6.8. Tipping Point de 3Com - Ambiente de Configuración Web.

Los niveles de acceso se crearon de acuerdo al análisis de necesidades de utilización de Internet de cada usuario miembro del dominio, conformando grupos de usuarios que posteriormente pasaron a ser miembro de los segmentos de red, los niveles de acceso creados son:

- Acceso sin restricciones.
- Acceso controlado, esto implica control de descargas, chats, mensajería instantánea.
- Sólo navegación en la web.
- Sin acceso a Internet.

La segmentación de la red permitió apartar a los servidores de la vista de todos los computadores conectados a la red interna, dando la posibilidad de acceder a los servidores sólo aquellos grupos de usuarios que lo requieran. Esto complemento la

configuración de permisos de acceso más exclusivos que se realizo a nivel de archivos y directorios.

IMPLEMENTACION DEL SERVIDOR CORPORATIVO DE ACTUALIZACIONES

Para cumplir con este objetivo fue necesaria la instalación y configuración de Microsoft Windows Server Update Services (WSUS) 3.0, que es el encargado de descargar y distribuir las actualizaciones, proporciona además una solución completa para administrar actualizaciones en la red. La interfaz que presenta WSUS 3.0 para su configuración, consulta de estado de los equipos y reportes, se muestra en la Figura 6.9.

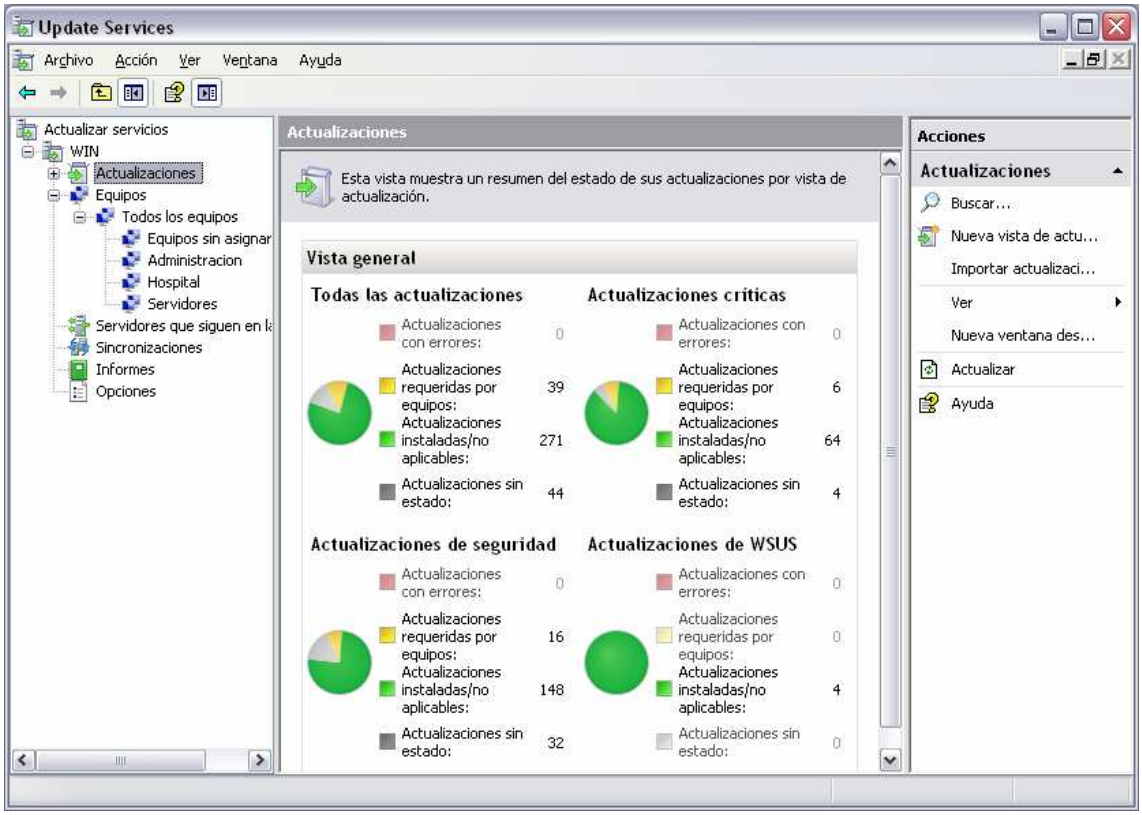


Figura 6.9. Consola de Administración de WSUS 3.0.

[10] Para poder instalar WSUS 3.0, el sistema de archivos del servidor tiene que cumplir los requisitos siguientes:

- Tanto la partición del sistema como la partición en la que se instala WSUS 3.0 deben estar formateadas con el sistema de archivos NTFS.
- Se recomienda un mínimo de 1 GB de espacio libre para la partición del sistema.
- Se recomienda 20 GB de espacio libre para el volumen donde WSUS almacena el contenido.
- Se recomienda un mínimo de 2 GB de espacio libre en el volumen donde el programa de instalación de WSUS instala Windows Internal Database.

El componente Actualizaciones Automáticas que posee Windows y estar conectado a la red son los únicos requisitos que deben cumplir los computadores clientes. Se puede usar Actualizaciones automáticas con WSUS 3.0 en equipos que ejecuten cualquiera de los sistemas operativos siguientes:

- Windows Vista.
- Windows Server con nombre de código “Longhorn”.
- Microsoft Windows Server 2003, todas las versiones y service packs.
- Microsoft Windows XP Professional, Service Pack 1 o Service Pack 2.
- Microsoft Windows 2000 Professional, Windows 2000 Server o Windows 2000 Advanced Server, todos estos con Service Pack 4.

[10] Para el funcionamiento correcto de WSUS se debe verificar que los siguientes permisos de disco estén otorgados a los usuarios especificados para los directorios especificados:

- El grupo de usuarios integrado o la cuenta de NT Authority\Network Service (en Windows Server 2003) debe tener permiso de lectura para la carpeta raíz de la unidad donde reside el directorio de contenido de WSUS. Si falta este permiso, las descargas de BITS no se realizarán correctamente.

- La cuenta de NT Authority\Network Service debe tener permisos de “Control total” para el directorio de contenido WSUS, generalmente: WSUS\WsusContent. Este permiso lo establece el programa de instalación del servidor WSUS cuando crea el directorio, pero determinado software de seguridad puede restablecer este permiso, sin este las descargas de BITS no se realizarán correctamente.
- La cuenta de NT Authority\Network Service debe tener permiso de “Control total” para las siguientes carpetas con el fin de mostrar correctamente el complemento de administración de WSUS:
    - %windir%\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files
    - %windir%\Temp

Antes de descargar las actualizaciones, deben especificarse qué actualizaciones se desean descargar, el idioma y la clasificación de las mismas.

La mejor manera de configurar las Actualizaciones automáticas en los equipos del entorno de red es con Active Directory, se puede usar un objeto de directiva de grupo (GPO) basado en dominios, en la que se señalará para los equipos clientes la dirección del servidor WSUS.

Las actualizaciones tienen que ser aprobadas antes de ser implementadas para cualquier equipo cliente. Los equipos se pondrán en contacto con el servidor WSUS de acuerdo a la periodicidad de actualización que se los haya configurado. Transcurrido este período, se podrá usar la característica de informes de WSUS para determinar si dichas actualizaciones se han implementado correctamente.

SELECCION E IMPLEMENTACION DE UN ANTIVIRUS CORPORATIVO

El software Anti-Virus debe ser bastante fácil de usar e instalar. Debe buscar e identificar con eficacia amenazas del virus, limpiar o aislar archivos infectados y

disponer de ayuda para que el usuario pueda estar bien informado de las actividades y capacidades del software.

[08] Para seleccionar un buen Anti-Virus se deben tomar en consideración algunas características como:

- Facilidad de empleo: el software antivirus debe ser simple de utilizar, sin importar la experiencia del usuario en computadores.
- Eficaz en identificar virus y gusanos: los mejores productos antivirus identifican archivos infectados rápidamente con exploración en tiempo real, buscando virus en archivos fuentes, email, mensajería instantánea, navegación web, etc.
- Informe de actividad: los programas Antivirus dan notificación inmediata de los virus encontrados por los exploradores en tiempo real y proporciona informes fáciles de resultados de exploración, incluyendo lo que encontró y qué hizo con los archivos infectados.
- Características del Software: un software antivirus con buenas características proporciona protección absoluta. Los mejores programas son los que ofrecen una variedad amplia de herramientas, de una exploración en tiempo real básica a una exploración más avanzadas, buenas heurísticas, etc.
- Facilidad de instalación y Configuración: los programas antivirus deben ser fáciles de instalar y permitir que con un par de clics se pueda iniciar con la exploración en busca de virus.
- Documentación de ayuda: el software antivirus debe contener varios medios de ayuda, como: ayuda vía email, chats en línea o asistencia telefónica. Debe también haber recursos en línea, tales como bases de conocimiento y foros disponibles para ayuda rápida y conveniente.

Tomando en consideración todas estas características se realizó la evaluación de varios software antivirus que brindarían las facilidades y prestaciones que la Institución requiere, y además considerando que estos ocupan los primeros lugares en el Ranking mundial. Mediante la evaluación y monitoreo del funcionamiento y desempeño de los

Anti-Virus se llego a la conclusión que Kaspersky Anti-Virus es el más adecuado, ya que brinda mayores facilidades de administración y control para una protección adecuada de servidores y las estaciones de trabajo. La evaluación de los antivirus abarco desde pruebas en entornos virtuales, hasta el análisis minucioso de sus características, tomando también en cuenta las opiniones dadas por expertos en foros especializados en el tema.

Con la adquisición e implementación de Kaspersky Anti-Virus, se consiguió centralizar la administración de los computadores en cuanto al servicio Anti-Virus y dar una protección de alta calidad a la información almacenada en todos los equipos de la Institución, ante cualquier amenaza de virus que podría presentarse. La distribución de software Anti-Virus en los computadores miembros de la red interna fue transparente y rápida ya que desde la consola de administración de Kaspersky Anti-Virus instalada en el área de sistemas se pudo repartir los paquetes de instalación automática en todos los clientes, esto se hizo luego de haber desinstalado los Anti-Virus personales que tenían ciertos computadores. La consola de administración y los paquetes de distribución se muestran en las figuras siguientes:

Figura 6.10. Consola de Administración de Kaspersky Anti-Virus

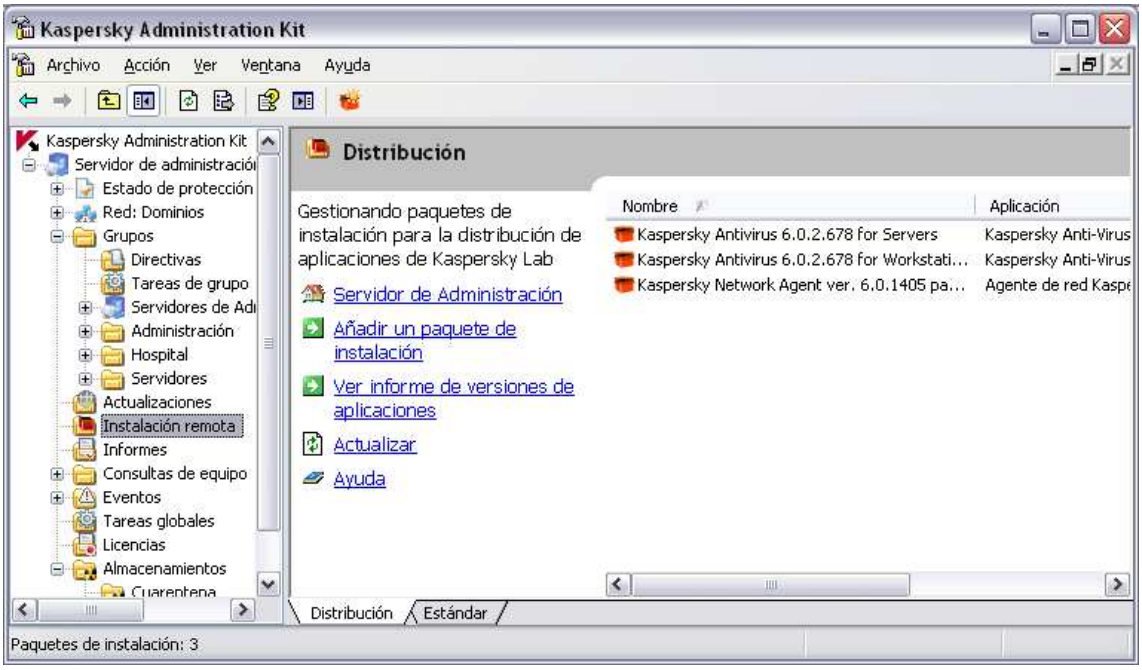


Figura 6.11. Visualización de paquetes de Instalación en la Consola de Administración de Kaspersky Anti-Virus

COPIAS DE SEGURIDAD DE LA INFORMACIÓN

Para realizar una copia de seguridad se debe contar con ciertos permisos y derechos de usuario en archivos y directorios. Para configurar un respaldo de información se recomienda que el usuario utilizado sea administrador u operador de copia de seguridad en el controlador de dominio, entonces se podrá realizar la copia de seguridad de cualquier archivo o directorio de forma local en cualquier equipo de la red que pertenezca a dicho dominio. Sin embargo, si el usuario no es administrador ni operador de copia de seguridad y desea realizar una copia de seguridad de los archivos, debe ser el propietario de los archivos y directorios cuya copia de seguridad desee llevar a cabo, o tiene que contar con uno o varios de los permisos siguientes para esos archivos y directorios: Lectura, Lectura y ejecución, Modificación o Control total.

Hay que asegurarse de que no haya ninguna restricción de cuota de disco que limite el acceso al disco duro. Tales restricciones imposibilitan realizar una copia de seguridad de los datos.

Se puede utilizar la utilidad Copia de Seguridad sólo de forma local; no se puede realizar una copia de seguridad de un equipo remoto, lo que se puede hacer es el almacenamiento del respaldo de seguridad en un computador remoto. Sólo se puede restaurar y realizar la copia de seguridad de los datos de Estado del sistema en un equipo local. No se puede restaurar ni realizar una copia de seguridad de datos de Estado del sistema en un equipo remoto, aunque sea administrador en dicho equipo.

Cuando se realiza una copia o restaure de los datos del Estado del sistema, se copiarán o restaurarán todos los datos del Estado del Sistema que sean relevantes para el equipo; no podrá optar por copiar o restaurar determinados elementos de estos datos. Esto se debe a las dependencias existentes entre los componentes del Estado del sistema. Sin embargo, se puede restaurar los datos del Estado del sistema a una ubicación alternativa.

Los datos de Estado del sistema contienen la mayoría de los elementos de la configuración de un sistema, pero puede que no incluyan toda la información necesaria para recuperar el sistema tras producirse un error. Por lo tanto, se recomienda hacer copia de seguridad de todos los volúmenes de inicio y sistema, incluido el Estado del sistema. Para restaurar datos de Estado del sistema en un controlador de dominio, se debe iniciar antes el equipo en el Modo de restauración de servicios de directorio.

Para realizar las copias de seguridad en la Institución se selecciono a los usuarios que lo requerían por la importancia de los datos que estos manejan, el respaldo de la información se configuró para que se realizase periódicamente y de forma incremental, permitiendo mantener segura la información importante, sobre todo los datos almacenados en los Servidores.

Algunos de los pasos importantes al configurar una copia de seguridad se muestran en las figuras siguientes:

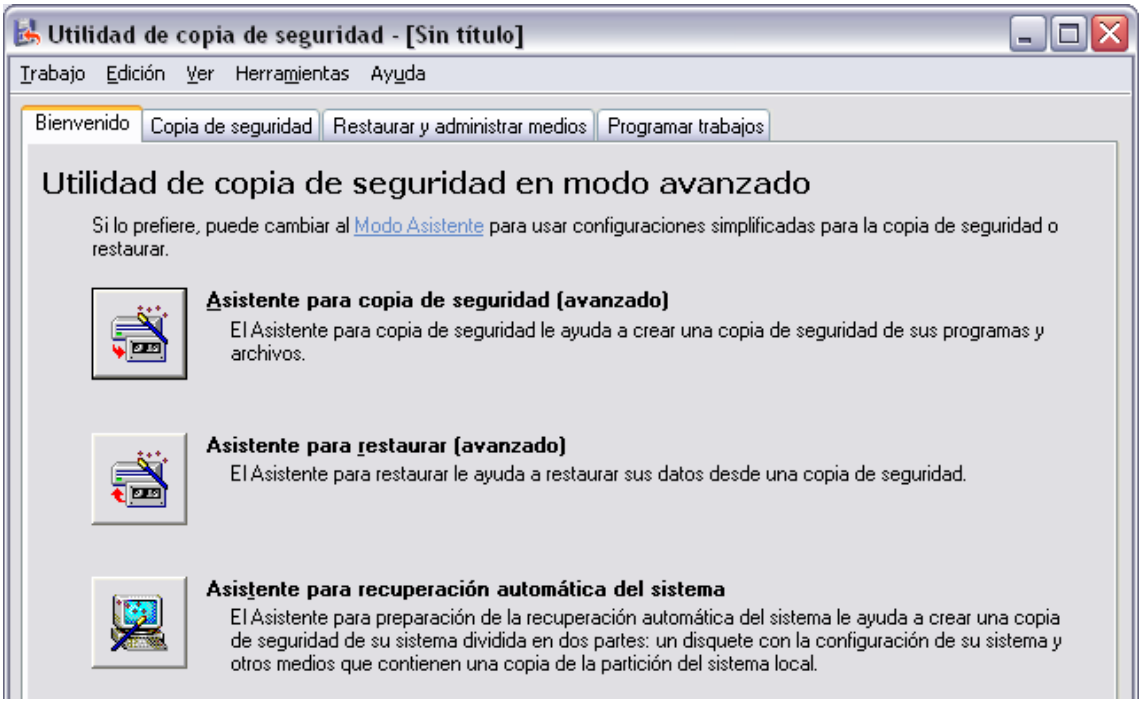


Figura 6.12. Utilidad de Copia de Seguridad - Presentación principal.

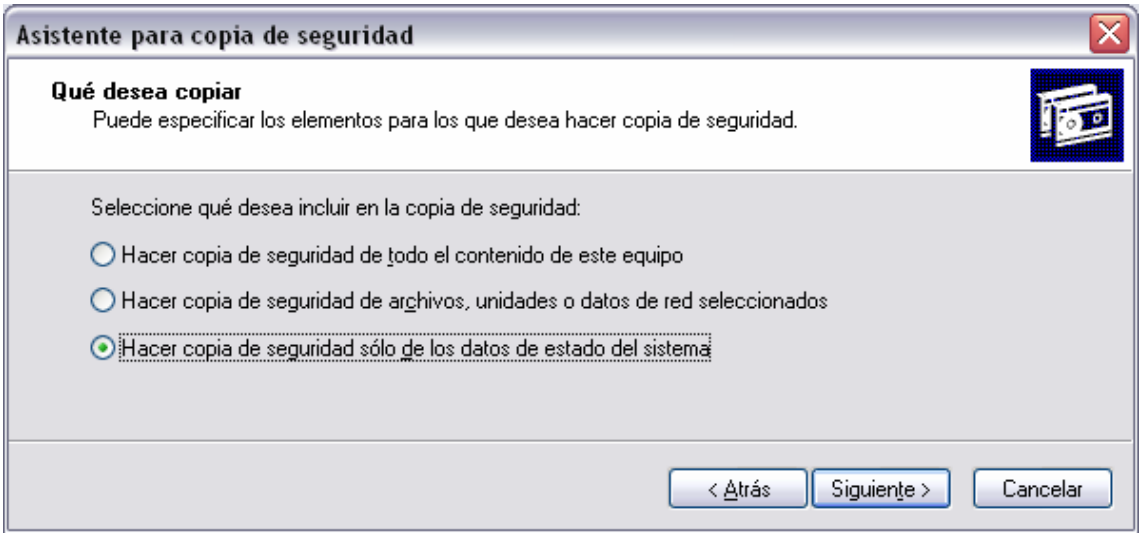


Figura 6.13. Utilidad de Copia de Seguridad – Selección de tipo de copia

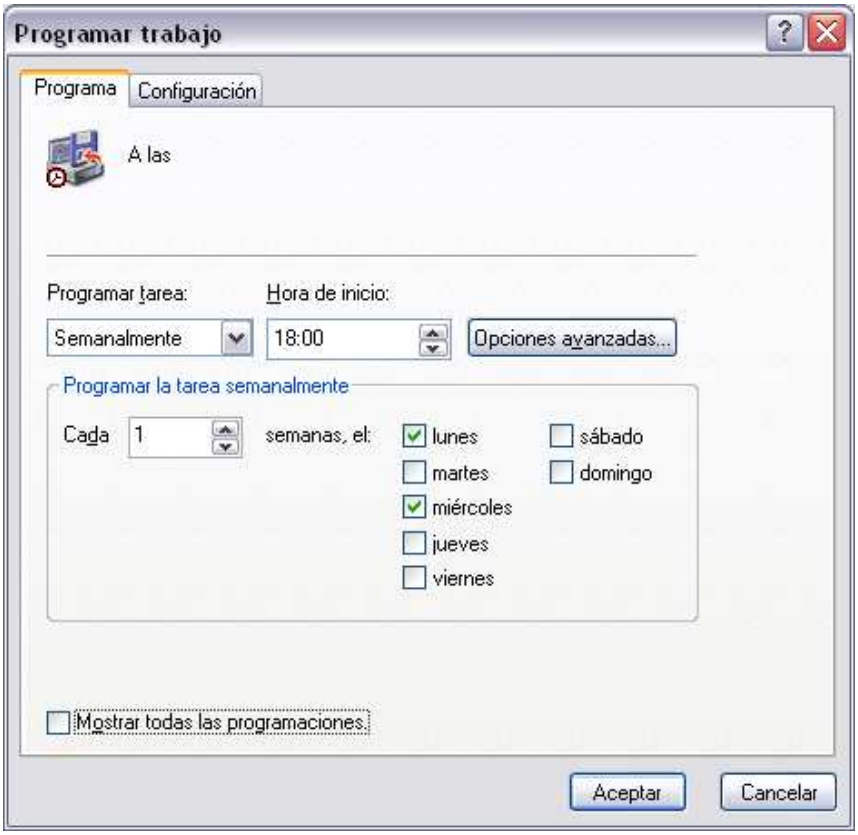


Figura 6.14. Utilidad de Copia de Seguridad – Programación de la tarea.

Una explicación más detallada de la implementación de los diferentes modulos que comprendio en presente proyecto de políticas de seguridad informática, se da en el Manual de Usuario ubicado en el Anexo 2.

6.4. PRUEBAS

Antes de realizar la implementación de los diferentes módulos que comprendió este proyecto se realizaron las siguientes pruebas.

DIRECTIVAS O POLÍTICAS DE GRUPO (GPO)

Para implementar las políticas o directivas de grupo se probó lo que cada una de las opciones de un objeto de política de grupo podría hacer en un computador, a partir de

esto se selecciono las necesarias y que se ajustaban a las necesidades de la Institución. Un ejemplo es la denegación de permisos de configuración que se muestra en la figura 6.14. Los GPO a implantarse pasaron un periodo de prueba en ciertos equipos seleccionados, en los que fue posible determinar si interferían con algún proceso o aplicación necesaria para las labores diarias, posteriormente fueron aprobadas por el Administrador de Sistemas de la Institución y se implementaron para todos los usuarios y equipos miembros de la red, fortaleciendo de esta forma la estructura informática del Hospital Millennium.

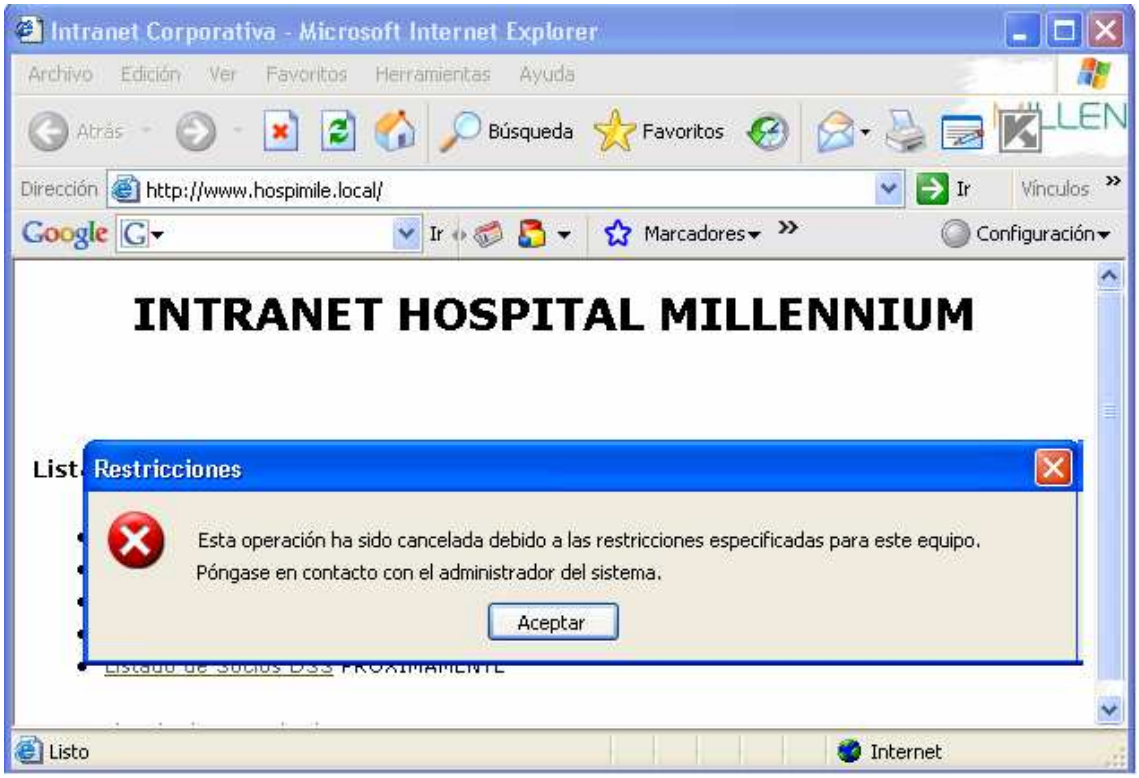
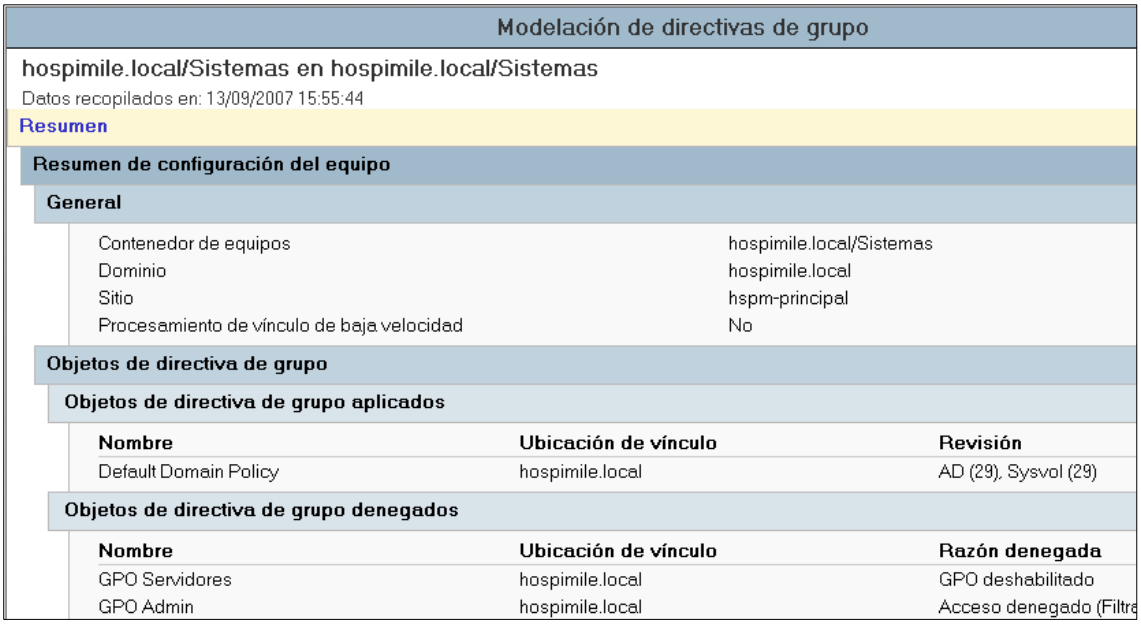


Figura 6.15. Denegación de Cambio de Propiedades de Internet Explorer.

Para ver el funcionamiento de un GPO la consola de administración permite realizar una modelación del GPO, como muestra la figura 6.15, esta funcionalidad de la consola de administración fue de gran ayuda para la realización de pruebas antes de la implementación.



Modelación de directivas de grupo

hospimile.local/Sistemas en hospimile.local/Sistemas

Datos recopilados en: 13/09/2007 15:55:44

Resumen

Resumen de configuración del equipo

General

Contenedor de equipos	hospimile.local/Sistemas
Dominio	hospimile.local
Sitio	hspm-principal
Procesamiento de vínculo de baja velocidad	No

Objetos de directiva de grupo

Objetos de directiva de grupo aplicados

Nombre	Ubicación de vínculo	Revisión
Default Domain Policy	hospimile.local	AD (29), Sysvol (29)

Objetos de directiva de grupo denegados

Nombre	Ubicación de vínculo	Razón denegada
GPO Servidores	hospimile.local	GPO deshabilitado
GPO Admin	hospimile.local	Acceso denegado (Filtr

Figura 6.16. Modelación de un GPO

CONTROL DE ACCESO

Para el control de acceso a los datos se realizó un pequeño estudio de las consecuencias al otorgar o negar uno u otro permiso, luego de esto se asignó a cada usuario los niveles de permisos que requería para acceder a su información. Un error de mala asignación de permisos que afecta al sistema clínico del Hospital se muestra en la figura 6.15.

Para el acceso a Internet luego de segmentar la red, se probo que todas las aplicaciones y servicios funcionarán correctamente y luego se configuró con el técnico que implantó el Tipping Point de 3Com (equipo de red para seguridad perimetral) las diferentes reglas y restricciones que cada segmento de red contendría, verificando que esto no ocasione conflictos con otras aplicaciones en las diferentes estaciones de trabajo.

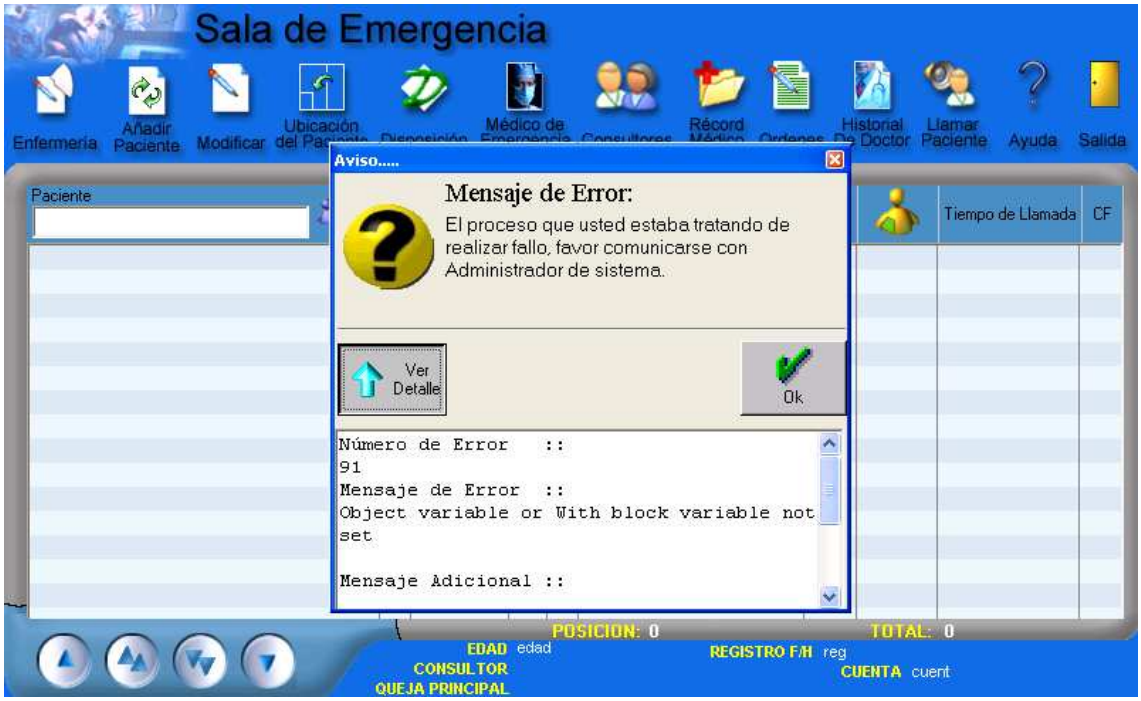


Figura 6.17. Error de mala asignación de permisos

SERVIDOR CORPORATIVO DE ACTUALIZACIONES

Para la implementación del servidor de actualizaciones se verificó que la distribución de las mismas en la red se hiciese correctamente, en algunos computadores que no se comunicaban con el Servidor Corporativo de Actualizaciones se tubo que borrar algunos registros del sistema y ejecutar ciertos comandos que restablecieron la utilidad Actualizaciones automáticas de los clientes y su correcta comunicación con el servidor de actualizaciones.

Los comandos para restablecer la comunicación con el servidor de actualizaciones son los siguientes:

- net stop wuauserv
- REG DELETE HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate /v AccountDomainSid /F
- REG DELETE HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate /v SusClientId /F

- REG DELETE HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate /v PingID /F
- net start wuauserv
- wuauclt.exe /detectnow
- wuauclt.exe /resetauthorization

ANTIVIRUS CORPORATIVO

El estudio y evaluación de los antivirus se la realizó en un entorno virtual monitoreando el comportamiento de cada uno de ellos, la facilidad de implantación y la transparencia con que estos actuaban en los clientes. Para determinar en parte la eficiencia de la protección en tiempo real se requirió realizar pruebas con archivos que simulaban virus informáticos, esto se lo hizo alojando en el disco duro local estos archivos y también llegando a ellos o intentando descargarlos durante la navegación por Internet; esto permitió determinar la efectividad de la protección y control de heurísticas que poseían los software antivirus.

Un ejemplo de protección en tiempo real de Kaspersky Anti-Virus, mientras se intenta descargar en el disco duro un virus desde Internet, se muestra en la figura 6.16.

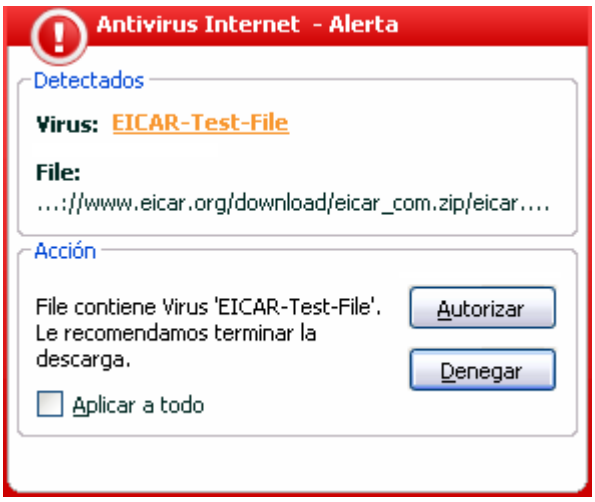


Figura 6.18. Mensaje de Alerta de Kaspersky Anti-virus

El Anti-virus que menos eficiencia mostró en la detención y eliminación de virus o programas malévolos en tiempo real fue F-Secure.

COPIAS DE SEGURIDAD DE LA INFORMACIÓN

Para comprobar que las copias de seguridad se realizaban correctamente se abrieron mediante el asistente para Copias de Seguridad los archivos generados por este y que están almacenados en el servidor de Backups.

Esto permitió determinar la efectividad con que trabajaba la utilidad encargada de realizar los respaldos de información. En la figura 6.17 se muestra como se visualizan los datos respaldados dentro de la utilidad copia de seguridad.

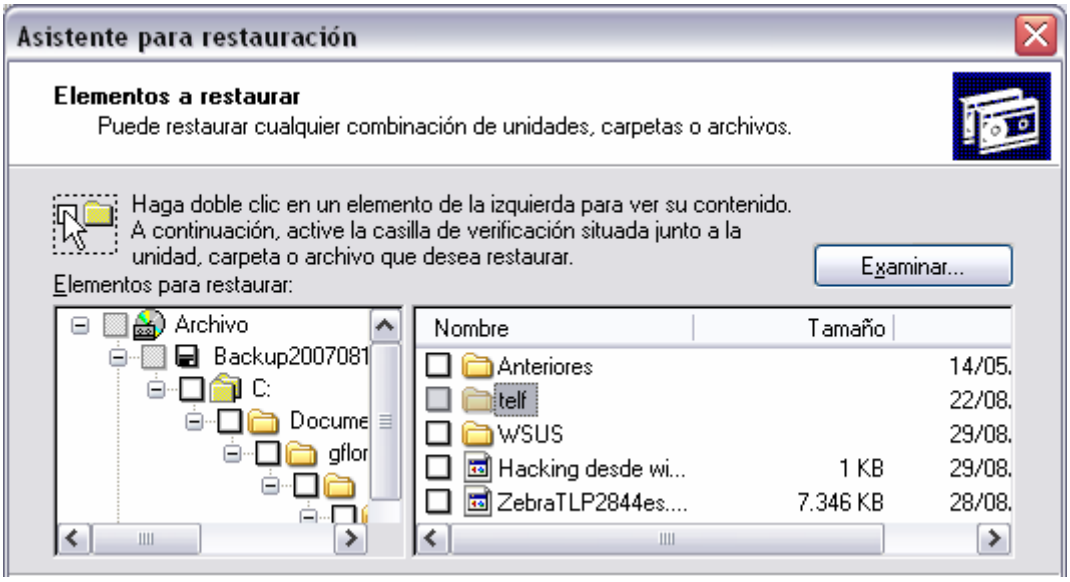


Figura 6.19. Asistente de restauración de copias de seguridad

INDICE DE FIGURAS Y TABLAS

FIGURAS **Pág.**

TABLAS **Pág.**

INDICE