PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

SERÉIS MIS TESTIGOS

ESCUELA DE SISTEMAS

TEMA:

ADMINISTRACIÓN Y SEGURIDAD DE LOS DISCOS DUROS UTILIZANDO HARDWARE Y SOFTWARE EN EL CENTRO DE INFORMATICA AULA No. 2 DE LA PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR SEDE AMBATO EN EL AÑO ACADEMICO 2008-2009

Disertación de Grado previo a la obtención del título de Ingeniería en Sistemas

AUTOR:

LUIS HERNAN URQUIZO TINTIN

DIRECTOR:

ING. MSc. PATRICIO MEDINA

Ambato – Ecuador

Junio 2009

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

ADMINISTRACIÓN Y SEGURIDAD DE LOS DISCOS DUROS UTILIZANDO HARDWARE Y SOFTWARE EN EL CENTRO DE INFORMATICA AULA No. 5 DE LA PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR SEDE AMBATO EN EL AÑO ACADEMICO 2008-2009

AUTOR:

LUIS HERNAN URQUIZO TINTIN

Ing. Msc. Patricio Medina **f)_____**

DIRECTOR DE DISERTACIÓN

CALIFICADOR **f)_____**

CALIFICADOR **f)_____**

Ing. Santiago Acurio **f)_____**

DIRECTOR DE LA ESCUELA DE SISTEMAS

Padre Dr. Cesar González Loor **f)_____**

PRORRECTOR DE LA PUCESA

DECLARACIÓN DE AUTENTICIDAD

Y RESPONSABILIDAD

Yo, Luis Hernán Urquizo Tintín, portador de la cedula de ciudadanía No. 180232566-0 declaro que los resultados obtenidos de la investigación que presento como informe final, previo a la obtención del título de Ingeniero en Sistemas son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de la redacción de este documento son y serán de mi sola responsabilidad legal y académica.

Luis Hernán Urquizo Tintín

CC: 180232566-0

AGRADECIMIENTO

Primeramente quiero darle gracias al eterno creador de todo lo existente como lo es “Dios”, a mi madre por sufrir los dolores que acecha tener un hijo y sin reproche alguno traerme al mundo y darme la vida y a mis hermanos que fueron un pilar fundamental para llegar a concluir mi carrera.

Un profundo y real agradecimiento a la Pontificia Universidad Católica del Ecuador Sede Ambato, por abrirme sus puertas y permitirme concluir mis estudios; así también a mis entrañables profesores, quienes a más de brindarme su conocimiento científico me dieron bases para ser un profesional a carta cabal.

Un especial agradecimiento al Ing. MSc. Patricio Medina, quien es a más de haber sido mi profesor, mi director de disertación es un verdadero y leal amigo, el cual con sus conocimientos y palabras de aliento me supo guiar y llevar a concluir el presente trabajo e incentivar en mi el amor al trabajo, la responsabilidad, respeto, honradez, solidaridad para ser una profesional integro.

DEDICATORIA

El presente trabajo va dedicado con todo mi cariño y amor a las personas que han estado y estarán siempre en mi corazón:

Mi adorable esposa, Guadalupe Ramos, que fue la persona que levanto en mi el deseo de concluir mi carrera, ya que sin su valioso apoyo no hubiera podido llegar al último de los peldaños en mi carrera educativa y el primer peldaño en mi vida profesional.

A mis tiernos hijos, Christian, David y Lizbeth, quienes fueron y son la razón de mi existencia, así como son la piedra angular a la dedicación y esfuerzo educativo y concluir mi añorado sueño, como es la culminación de una etapa más de mi vida.

RESUMEN

La presente investigación: Administración y Seguridad en los Discos Duros se aplico en el Laboratorio 5 de la Pontificia Universidad Católica del Ecuador Sede Ambato; el mismo está basado en la protección y seguridad inteligente mediante una recuperación instantánea de los datos del disco dura y del CMOS, mediante un Hardware llamado PCGuard y un software para la administración y monitoreo llamado NetManager. Empezamos con la instalación y configuración de la tarjeta, la cual va colocada en una ranura PCI del Mainboard, luego realizamos la instalación del software que permite controlar todas y cada una de las acciones de Administración y Recuperación de la información en cuestión de segundos sin consumir recursos, ni afectar el rendimiento del sistema. Gracias a estos elementos usados el Administrador del sistema puede realizar una restauración del sistema sin la necesidad de hacer los típicos pasos a saber: formateo del disco duro, instalación del sistema operativo y de más software necesarios para que los equipos funciones en optimas condiciones, todo este proceso se reduce a un simple orden desde el Servidor en el cual este instalado el NetManager sin generar pérdida de tiempo y recursos para la persona encargada del laboratorio.

ABSTRACT

The present investigation: Administration and Security in the hard disks you applies in the Laboratory 5 of the Catholic University of the Ecuador Sede Ambato; the same one is based on the protection and intelligent security by means of an instantaneous recovery of the data of the hard disk and of the CMOS, by means of a called Hardware PCGuard and a software for the administration and called control NetManager. We begin with the installation and configuration of the card, which goes placed in a groove PCI of the Mainboard, then we carry out the installation of the software that allows to control all and each one of the actions of Administration and Recovery of the information in question of seconds without consuming resources, neither to affect the yield of the system. Thanks to these used elements the Administrator of the system can carry out a restoration of the system without the necessity of making the typical steps that is: formated of the hard disk, installation of the operating system one and of necessary more software so that the teams functions under good conditions, this whole process decreases to a simple order from the Servant in the one which this installed the NetManager without generating loss of time and resources for the person in charge of the laboratory.

TABLA DE CONTENIDOS

CAPÍTULO I

CAPITULO II

CAPITULO III

CAPITULO IV

GRAFICOS ESTADISTICOS

FIGURAS O IMAGANES

CUADROS ESTADISTICOS

TABLAS

CAPÍTULO I

1. Planteamiento del Problema

La Pontificia Universidad Católica del Ecuador Sede Ambato en la actualidad no cuenta con una verdadera herramienta que pueda controlar sus equipos computacionales en cuanto se refiere al manejo que realizan sus usuarios (estudiantes).

Esta carencia a permanecido latente por algunos años, siendo así que la institución no tiene una estricta administración de sus equipos en el centro de informática de este centro educativo; de esta manera se vuelve indispensable el desarrollo de una auténtica configuración para administrar todos los manejos y procedimientos que realizan en el tiempo de uso de los equipos de los diferentes usuarios que lo ocupen para que la institución tenga calidad y buen servicio de sus equipos.

1.1. Delimitación del Problema

1.1.1. Tiempo

El tiempo aproximado de desarrollo del presente proyecto es de 6 meses estimando dos meses como margen de tolerancia por lo que considero real la finalización del proyecto para el mes de Mayo del 2009.

1.1.2. Espacio

Esta investigación se llevará acabo en la Pontificia Universidad Católica del Ecuador, Sede Ambato; la misma que se encuentra ubicado en el Sector Tropezón, Avenida Manuelita Sáenz S/N.

1.1.3. Lugar

Centro de Informática en la Aula # 2 de la Pontificia Universidad Católica del Ecuador, Sede Ambato

1.2. Importancia Justificación

Debido a los diferentes problemas que existe en cuanto a los controles que se debe tener en un centro de Informática, principalmente en una institución educativa por el mal uso de los equipos computacionales de parte de los diferentes usuarios (estudiantes), que lo hacen de una manera desconsiderada, por lo cual estos equipos en su mayoría de tiempo se tiene que estar evaluando y configurando en todo momento.

Por esta razón, Pontificia Universidad Católica del Ecuador Sede Ambato, pretende modernizar y purificar este problema existente. Ya que la investigación previamente realizada, ha revelado que actualmente en esta institución, existe una carencia en el control de los equipos del Centro de Informática.

En el mercado tecnológico y por Internet existen aplicaciones y Software que podría facilitar este trabajo, pero no se adaptan a las necesidades de la Universidad y debe estar configurando a cada momento y en cada equipo y esto presenta una demora de tiempo y trabajo hacerlo.

Por lo tanto, se justifica la necesidad de desarrollar una aplicación que permita administrar y controlar la configuración del equipo computacional de la Pontificia Universidad Católica del Ecuador Sede Ambato

1.3. Objetivos

1.3.1. General

Dotar de seguridad y una buena administración de los discos duros con hardware y software del Aula No. 2 del Centro de Computo de la Pontificia Universidad Católica del Ecuador Sede Ambato

1.3.2. Específicos

- Recolectar información sobre herramientas para la administración y control del software de los equipos.
- Determinar los medios idóneos para la administración y control del configurado en el equipo computacional
- Implementar una herramienta para la administración y control de configurado en los equipos.

1.4. Metodología de Investigación

Para desarrollar la presente investigación se utilizaran los siguientes métodos:

- **Investigativa**: Porque la principal función es la de investigar algunas aplicaciones para el conocimiento de estas aplicaciones que se necesita conocer, para el desarrollo del proyecto.

- **Descriptiva**: Identificar elementos y características especificas del problema a investigar, recolectando, analizando la información obtenida.

- **Histórica**: Porque se podrá evaluar los resultados obtenidos en el pasado y compararlos con lo que se obtendrá luego del desarrollo del sistema.

CAPITULO II

2. Marco Teórico.

Para realizar este sistema se tiene que conocer y saber todo lo referente a las distintas clases de seguridades existentes, además a que se refiere la seguridad informática:

2.1. ¿Qué es seguridad?

Podemos entender como seguridad una característica de cualquier sistema (informático o no) que nos indica que ese procedimiento está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica, particularizando para el caso de sistemas operativos o redes de computadoras, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera) más que de seguridad; por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros.

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos: confidencialidad, integridad y disponibilidad. La confidencialidad nos dice que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello, y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades; la integridad significa que los objetos sólo pueden ser modificados por elementos autorizados, y de una manera controlada, y la disponibilidad indica que los objetos

del sistema tienen que permanecer accesibles a elementos autorizados; Es el contrario de la negación de servicio.

Algunos estudios integran la seguridad dentro de una propiedad más general de los sistemas, la confiabilidad, entendida como el nivel de calidad del servicio ofrecido. Dependiendo del entorno en que un sistema trabaje, a sus responsables les interesará dar prioridad a un cierto aspecto de la seguridad.

Por ejemplo, en un sistema militar se antepondrá la confidencialidad de los datos almacenados o transmitidos sobre su disponibilidad: seguramente, es preferible que alguien borre información confidencial (que se podría recuperar después desde una cinta de backup) a que ese mismo atacante pueda leerla, o a que esa información esté disponible en un instante dado para los usuarios autorizados.

En seguridad informática en general, y especialmente en las relativas a seguridad, se intenta clasificar en grupos a los posibles elementos que pueden atacar nuestro sistema. A continuación se presenta una relación de los elementos que potencialmente pueden amenazar a la configuración del computador:

Personas

La mayoría de ataques a nuestro sistema van a provenir en última instancia de personas que, intencionada o inintencionadamente, pueden causarnos enormes pérdidas. Generalmente se tratará de piratas que intentan conseguir el máximo nivel de privilegio posible aprovechando alguno (o algunos) agujeros del software. Pero

con demasiada frecuencia se suele olvidar que los piratas "clásicos" no son los únicos que amenazan nuestros equipos.

Aquí se describen brevemente los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para nuestros sistemas. Generalmente se dividen en dos grandes grupos: los atacantes pasivos, aquellos que fisgonean por el sistema pero no lo modifican -o destruyen-, y los activos, aquellos que dañan el objetivo atacado, o lo modifican en su favor.

Personal

Las amenazas a la seguridad de un sistema proveniente del personal de la propia organización rara vez son tomadas en cuenta; se presupone un entorno de confianza donde a veces no existe, por lo que se pasa por alto el hecho de que casi cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática (secretariado, personal de seguridad, personal de limpieza y mantenimiento, etc.) puede comprometer la seguridad de los equipos. Aunque los ataques pueden ser intencionados lo normal es que más que de ataques se trate de accidentes causados por un error o por desconocimiento de las normas básicas de seguridad.

Curiosos

Los curiosos son los atacantes más habituales de sistemas. Aunque en la mayoría de situaciones se trata de ataques no destructivos, parece claro que no benefician en absoluto al entorno de fiabilidad que podamos generar en un determinado sistema.

A un curioso en realidad podemos considerarlo más como un ladrón de la información que como una amenaza de la misma; ya que este se nutre de conocimientos que adquiere al indagar en el sistema.

Virus

Un virus es una secuencia de código que se inserta en un fichero ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

Toda amenaza sea residente o casual en todos los casos su principal objetivo es el de hacer daño al sistema operativo así como a la información de la cual disponga o este a su alcance; que aparte de atacar al software también causa daños a nivel de hardware.

Terroristas

Por "terroristas" no debemos entender simplemente a los que se dedican a poner bombas o quemar autobuses; bajo esta definición se engloba a cualquier persona que ataca al sistema simplemente por causar algún tipo de daño en él.

Hemos hablado de los aspectos que engloba la seguridad informática, de los elementos a proteger, de los tipos de amenazas que contra ellos se presentan y del

origen de tales amenazas; para completar nuestra visión global de la seguridad, nos queda hablar de las formas de protección de nuestros sistemas.

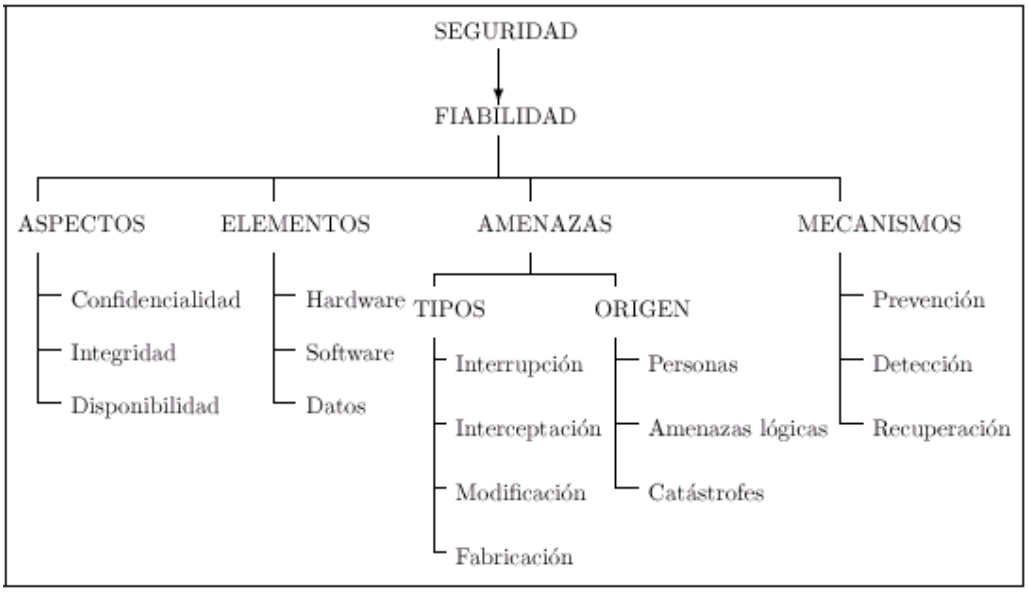


Figura No. 1: Mapa de Seguridad

Para proteger nuestro sistema se deben realizar análisis de las amenazas potenciales que puede sufrir nuestro sistema, las pérdidas que podrían generar, y la probabilidad de su ocurrencia; a partir de este análisis hemos de diseñar una política de seguridad que defina responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan.

Entonces podemos investigar algunos de los diferentes software, sistemas y seguridades que existen en la actualidad en el campo informático, pues para alcanzar el objetivo se debe evaluar las diferentes soluciones que están en el mercado; así tenemos por ejemplo:

2.2 Deep Freeze.

El Deep Freeze es ampliamente considerado como el líder en la industria del software del tipo "reinicie y restaure". El principal objetivo de Deep Freeze es que, mientras esté instalado, la computadora estará "congelada". Cualquier cambio que se le realice a una computadora "congelada" será eliminado al reiniciar la PC, es decir que el equipo volverá al estado en que se activó la protección.

Deep Freeze permite a los administradores proteger el sistema operativo y el software de una estación de trabajo sin restringir el acceso del usuario.

Cada vez que se reinicia el sistema, Deep Freeze restablece la computadora a su estado original, hasta el último byte.
Deep Freeze ofrece una protección total de la estación de trabajo frente a configuraciones incorrectas de software, virus, programas maliciosos (malware) y programas espías (spyware).

Los usuarios disfrutan de una experiencia informática libre de problemas y el personal de Tecnología de la Información (TI) se ve liberado de los tediosos problemas de software y soporte técnico.

Deep Freeze puede implementarse con facilidad y mantenerse en toda una empresa mediante una consola central.

Los coordinadores de tecnología ahora tienen el poder de proteger cientos o miles de computadoras a través de una LAN, una WAN o de Internet, una función invalorable para los administradores de varios sitios remotos.

Deep Freeze también ofrece periodos de mantenimiento programados que permiten trasladar las actualizaciones y los parches a las estaciones de trabajo en el momento más conveniente para su organización.

Puesto que el concepto “reiniciar para restaurar” de Deep Freeze no lentifica las computadoras ni incrementa el tiempo de reinicio, el software supera ampliamente las tecnologías de restauración basadas en imágenes, las cuales requieren tanto iniciación administrativa como tiempo de inactividad del sistema para poder repararlo.

Implementado globalmente en cincuenta países, Deep Freeze brinda protección infalible a más de seis millones de computadoras en todo el mundo

2.2.1 Características.

Entre las principales características tenemos:

- Consola de Administración
- Protección de uno o varios discos / particiones.
- Creación de hasta 15 Password permanentes
- Passwords de una sola vez (One time password - OTP)

- Más de 100 GB de espacio descongelado (Thawed: áreas del disco que no se protegen).
- Posibilidad de elegir particiones del disco descongeladas.
- Modo silencioso
- Reinicios o apagados programados.
- Tiempos de mantenimiento programados.
- Compatible con actualizaciones de Windows y Servidores.
- Ejecución de procesos Batch en tiempos de mantenimiento.
- Protección de password mediante cifrado.
- Encendido, reinicio y apagado de equipos manuales o programados.
- Bloqueo de dispositivos de entrada (teclado y mouse) desde la consola.
- Compatible con redes LAN y WAN
- CMOS protegida.
- MBR (Master Boot Record).
- Integración con Virtual Network Conection para visualización y control remoto de estaciones.
- Integración con Escritorio Remoto

2.2.2 Funcionamiento.

La protección funciona desde que el equipo inicia y antes de que empiece a cargar el sistema operativo, razón por la cual protege el equipo de cualquier virus, incluso los que atacan el MBR (Master Boot Record) que se refiere al sector de arranque y las particiones NTFS (New Technology File System) es un sistema de archivos para

definir el tamaño del cluster , incluso si el equipo se ha iniciado en Modo Seguro (es un estado de la computadora donde el sistema operativo en cuestión inicia solamente sus componentes base).

2.2.3 Implementación.

Antes de realizar la instalación se debe deshabilitar todo utilitario y todo software anti-virus que se ejecute en segundo plano, y se deben cerrar todas las aplicaciones abiertas. Estos programas pueden interferir con la instalación, lo que tendría como consecuencia que Deep Freeze no funcione correctamente.

Deep Freeze Enterprise ofrece una implementación centralizada y un control administrativo flexible. Por medio de Enterprise Console, instale, controle y administre las estaciones de trabajo protegidas por Deep Freeze.

Active y desactive la protección en forma selectiva o por grupo. Modifique en forma instantánea la configuración de una estación de trabajo. Reinicie, apague o active computadoras en forma remota. Vea el estado completo de cada estación de trabajo de su red.

Proteja cientos de miles de estaciones de trabajo a través de una LAN distribuida, de una WAN o de Internet.

Deep Freeze puede implementarse en estaciones de trabajo mediante una Attended Install (Instalación con supervisión), el Silent Install System (Sistema de instalación silenciosa), o como parte de un proceso de distribución de imágenes de disco.

Deep Freeze ha sido diseñado para funcionar con los principales productos de software de administración de escritorio y creación de imágenes. Use la Attended Install (Instalación con Supervisión) o bien el Silent Install System (Sistema de Instalación Silenciosa) para instalar Deep Freeze en una imagen maestra.

Después de crear la imagen, las estaciones de trabajo deben reiniciarse una vez más para que Deep Freeze pueda detectar correctamente los cambios en la configuración del disco. Si la imagen se instala en las estaciones de trabajo en modo no supervisado, deben tomarse medidas para asegurar que las estaciones de trabajo se reinicien y así permitan que se actualice la configuración.

Las funciones de seguridad de Deep Freeze incluyen la protección contra “ataques basados en diccionarios”. A tal fin, las estaciones de trabajo se reinician en forma automática después de 10 intentos fallidos.

Se deberán descongelar las estaciones de trabajo para que cualquier cambio permanente entre en efecto. La instalación de un software a menudo requiere uno o dos reinicios del equipo para completarse. Se recomienda utilizar la ficha “Control de reinicio” para permitir que la estación de trabajo se reinicie con Deep Freeze Descongelado hasta tanto se completen las instalaciones o los cambios.

2.2.4 Beneficios y ventajas

Entre sus principales y beneficios y ventajas que tiene este tipo de software que nos permite dar seguridad a nuestro computador, en lo referente a los discos duros del mismo son:

- Garantiza el 100% de disponibilidad en todas sus computadoras.
- Elimina el mantenimiento técnico rutinario a las computadoras.
- Economiza hasta en un 95% los costos de mantenimiento de sus equipos de cómputo.
- Certeza de que el software de los equipos funciona siempre bien.
- Aumenta el nivel de satisfacción del usuario.
- Maximiza la productividad al no tener conflictos por software.
- Incrementa la eficiencia informática del personal.
- Seguridad de su información.
- Pasara cualquier auditoria de software, nunca tendrá instalada piratería.
- Tranquilidad.
- Ahorro de tiempos y movimientos.
- Liderazgo y vanguardia tecnológica.
- Evita la pérdida de tiempo causada por conflictos de software.

Ventajas:

- Tecnología NO restrictiva.

- Los equipos protegidos con DEEP FREEZE no pueden tener daños permanentes por virus, con un simple reinicio restablece la configuración original.
- Usted tiene el control para hacer cambios permanentes a la configuración.
- La computadora funciona a la velocidad original y óptima.
- Permite instalar sus programas y actualizaciones de cualquier software con total seguridad.
- No desperdicia espacio en disco duro utilizando imágenes.
- No es detectable a la vista del usuario.
- Ocupa el 0.05% de espacio en un disco duro de 40 GB.
- Utiliza el 0.78125 % en una memoria RAM de 256 MB.
- No necesita usar puntos de restauración como Windows ME o XP.
- Permite ser configurado para ser clonado a otras máquinas.
- El costo del mantenimiento (Updates) a partir del segundo año cuesta el 20% de la licencia aproximadamente.
- Compatible con cualquier aplicación que corra bajo ambiente Windows.
- Incrementa en un 250% la vida útil del disco duro.
- Los equipos protegidos no fragmentan sus discos duros.
- Control de DEEP FREEZE por red local e Internet (según versión).

2.3 Norton Ghost

El Norton Ghost permite hacer copias de discos y particiones a unidades de almacenamiento (discos, cintas, grabadoras). Tiene soporte TCP y reconoce dispositivos LPT y USB.

Se puede ejecutar desde la línea de comandos o con un entorno gráfico. No tiene ninguna complicación, a menos que se quiera hacer cosas muy específicas (como excluir determinados directorios o archivos, cambiar la FAT, copiar varias particiones, etc.) para las que se necesiten comandos o parámetros especiales.

Pero esto último, para el 95 % de las operaciones no es necesario y en todo caso sólo se tiene que leer los apartados comandos y switches de la ayuda que son fáciles de entender.

2.3.1 Características.

- Realiza copias de seguridad de todo lo que tenga en su equipo: música digital, fotografías, documentos financieros, aplicaciones, configuraciones, sistema operativo, etc., en un solo paso.
- Recupera el sistema y los datos aun cuando no puede reiniciar el sistema operativo.
- Crea de forma automática un programa inicial de copia de seguridad basado en la configuración del equipo.

- Detecta automáticamente los dispositivos de almacenamiento, analiza el sistema y, durante la instalación, ofrece consejos sobre la mejor manera de realizar las copias de seguridad.
- Efectúa copias de seguridad incrementales que permiten ahorrar tiempo y espacio.
- Monitoriza y optimiza de manera automática el espacio del disco de la copia de seguridad.
- Efectúa copias de seguridad sobre la marcha, sin necesidad de volver a reiniciar el sistema.
- Realiza copias de seguridad de casi todos los medios, entre los que se incluyen unidades de CDR/RW y DVD+-R/RW, dispositivos USB y FireWire® (IEEE 1394), además de unidades Iomega®, Zip® y Jaz®.
- Desencadena la realización de copias de seguridad de los sucesos clave, como por ejemplo las instalaciones de un nuevo programa o los inicios de sesión de usuarios.
- Crea nuevas copias de seguridad con el botón “Backup Up Now” siempre que lo desee.
- Encripta las copias de seguridad para que resulten más seguras.
- Interfaz basada en tareas que simplifica la gestión y la monitorización.
- Permite visualizar de forma eficaz todas las copias de seguridad programadas, además del nivel de protección de seguridad asignado a cada una de las unidades del equipo.
- Encripta las copias de seguridad para que resulten más seguras.

- Instalación y configuración rápida y sencilla gracias al asistente de instalación en un solo paso.
- Con tan sólo pulsar un botón, inicia las copias de seguridad de las unidades externas.

2.3.2. Funcionamiento.

Entre sus principales funciones que realiza son las siguientes:

- Facilidad de uso mejorada

Una interfaz de usuario mejorada simplifica lo que necesita saber para hacer una copia correcta de respaldo, recuperar archivos, carpetas o su equipo completo.

Y para los expertos en Norton Ghost, la página “Avanzado” le da una vista sencilla de la mayoría de las funciones del producto.

- Compatible con Windows Vista ®

Norton Ghost ha sido diseñado y probado para ejecutarse en el nuevo sistema operativo Windows Vista ® y aún es compatible con las versiones anteriores de Windows.

- Configuración Fácil Mejorada

Ahora, configurar la primera copia de respaldo es aún más sencillo con la configuración “Fácil” mejorada, la cual aparece durante la instalación (a menos que decida omitirla) o automáticamente la primera vez que ejecute Norton Ghost. Especifique unas cuantas preferencias y puede comenzar a respaldar su equipo periódicamente.

- Copia de respaldo de archivos y carpetas

Limita la copia de respaldo para incluir un conjunto seleccionado de archivos o carpetas. Las copias de respaldo de archivos y carpetas son especialmente útiles si el espacio de almacenamiento para la copia de respaldo es limitado y hace cambios frecuentes a documentos importantes que desea respaldar.

- Copias de respaldo de una vez

La función de Copia de respaldo de una vez permite definir y ejecutar una copia de respaldo en cualquier momento sin guardar el trabajo de copia de respaldo para uso posterior.

- Editor de programación simplificado

Se puede editar fácilmente su programación de copias de respaldo existentes sin tener que hacer clic a través de varios diálogos o completar de nuevo las aplicaciones de respaldo.

- Administrar datos de copia de respaldo

Debido a que los puntos de recuperación y los datos de las copias de respaldo de archivos y carpetas requieren espacio de almacenamiento, Norton Ghost brinda la libertad de dónde y cómo manejar la cantidad de espacio en disco utilizada para almacenar datos de copias de respaldo.

Norton Ghost ofrece herramientas simples para manejar los datos de copias de respaldo e incluso poder administrarlos de forma automática.

- Estado de copia de respaldo y recuperación mejorado

La página de inicio ofrece el estado de protección de copia de respaldo en una vista sencilla. Pero también se puede utilizar el nuevo Calendario de Respaldos para ver respaldos pasados y próximos programados, para ver qué tan protegidos están los datos en realidad.

- Detección de destino de copia de respaldo automática

Norton Ghost detecta automáticamente cuando se conecta un nuevo dispositivo de almacenamiento a su equipo y puede indicarle cambiar el destino de copia de respaldo predeterminado a la nueva unidad de disco.

- Examinar archivos y carpetas perdidos o dañados.

La exploración mejorada de archivos y carpetas dentro de los puntos de recuperación facilita y agiliza la recuperación; la nueva función de respaldo de archivos y carpetas también permite buscar y recuperar archivos y carpetas rápidamente.

- Copias de respaldo desencadenadas por eventos

Además de las copias de respaldo programadas y manuales, Norton Ghost puede detectar ciertos acontecimientos y ejecutar una copia de respaldo automáticamente cuando ocurren, proporcionando un nivel adicional de protección para el equipo.

- Ajuste de rendimiento

Ajusta manualmente el efecto de ejecutar una copia de respaldo en el rendimiento de su equipo para adaptarse mejor a sus necesidades en el momento. Esta función es particularmente útil si se está trabajando en el equipo y no se desea que el proceso de respaldo lo retrase. Si se conocen los demográficos de su tráfico de red, ahora puede configurar el rendimiento de su red para evitar una sobrecarga de la red.

- Integración con Maxtor OneTouch

Si cuenta con una unidad de disco externa Maxtor OneTouch?, puede respaldar su equipo con sólo presionar un botón. No es necesario iniciar Norton Ghost.

- Disco de Recuperación de Symantec modificable

Cuando no pueda iniciar Windows, el Disco de Recuperación de Symantec recién mejorado (SRD) hace la recuperación más fácil que nunca.

- Si faltan controladores específicos en el Disco de Recuperación de Symantec, utilice la función Crear disco de recuperación para crear un Disco de Recuperación de Symantec modificado que incluya los controladores exactos necesarios para arrancar correctamente su equipo en el entorno de recuperación.

- La tecnología DeployAnywhere crea imágenes independientes del hardware.

- Crea imágenes básicas desde un sistema activo mediante la función de obtención de imágenes en caliente, sin dejar fuera de servicio el sistema.

- Compatibilidad con Microsoft Windows Vista ® y sistemas operativos de 64 bits.

- Única consola de administración centralizada para la administración de todas las tareas de migración.

- Filtros de inventario de Windows Vista ® incorporados para la identificación y detección de equipos listos para Windows Vista ®.

- Inventario de hardware y software para administrar de manera eficiente las imágenes y las implementaciones de software.

2.3.3 Ventajas Importantes.

- Mejora y aprovecha las mejores prácticas de Microsoft para la migración a Windows Vista ®.

- Simplifica la administración de imágenes al crear menos imágenes.

- El uso de la multidifusión acelera las implementaciones y reduce el tráfico general de red.

- Creación acelerada de imágenes en comparación con las herramientas de Sistema Operativo (SO) estándar con tecnología probada en el mercado.

- Ahorros significativos de costos y tiempo al crear imágenes para implementar, migrar y administrar sistemas.

2.4 LOCK MY PC

En algo que todas las personas estamos de acuerdo, es en que todos tenemos un espacio personal que celosamente cuidamos, y a ninguno de nosotros nos gustan aquellas personas que se entrometen en nuestro ordenador y revisan lo que tengan a la mano, “Lock My PC” será la herramienta que finalmente pondrá fin a estas miradas indeseadas.

El alejar a los mirones de nuestro ordenador será ahora tan fácil como presionar un botón del mouse, pues con “Lock My PC” podremos configurar fácilmente nuestro ordenador para bloquearlo al dar doble clic sobre el ícono del programa en la barra de tareas, o al presionar una combinación específica de teclas, adicionalmente, podrás configurar la aplicación para bloquear tu equipo después de cierto tiempo de inactividad, y también podrás marcar la opción de bloquear siempre el equipo al iniciar. Una vez bloqueado el equipo, lo único que los demás podrán ver será la pantalla de bloque, que puedes cambiar a tu gusto utilizando imágenes JPEG, BMP y GIF estáticos o animados. La única forma de desbloquear el equipo será introduciendo correctamente la contraseña guardada, la cual podremos decir al programa que debe ser cambiada cada xx días.

Al contrario de otras aplicaciones similares, “Lock My PC” también bloquea la combinación Ctrl + Alt + Supr del teclado, y si alguien reinicia incorrectamente el ordenador, este reiniciará bloqueado, lo que asegura una máxima confiabilidad contra intrusos.

2.4.1. Cuando utilizar Lock My PC

Cuando no estás sentado frente al mismo, si no te gusta que toquen tu PC, o temes que alguien mire documentos personales en tu disco duro, esta es la herramienta perfecta.

Con Lock My PC puedes evitar accesos no autorizados a tu ordenador. Con un simple clic en el menú del programa, Lock My PC pone la pantalla en negro, bloquea

el ratón y todas las combinaciones de teclas de Windows.

Para desbloquearlo, sólo tienes que introducir la contraseña correcta, y todo vuelve a la normalidad.

El programa tiene varias opciones de configuración: ejecutarlo con un clic en el icono o con una tecla rápida, eliminarlo de la lista de tareas activas para que el usuario no lo encuentre, etc.

Lock My PC tiene capacidad para seguir bloqueando el sistema incluso si alguien reinicia el PC. También puede generar un archivo log con información sobre los intentos fallidos de acceso.

Lock My PC™ es un fácil en el uso y la herramienta compacta para computadora rápida que cierra con llave cuando usted lo deja desatendido. Muestra una pantalla de la cerradura, desactiva Windows las teclas calientes y ratón. Usted puede cerrar con llave su PC con un “Hotkey” o de la bandeja del sistema. Para abrir a la computadora usted sólo debe entrar en contraseña correcta. Al contrario de otro software de cerradura de computadora similar que no puede cerrar con llave Ctrl+Alt+Del en una computadora Windows XP corriente, nuestra Cerradura Mi PC ejecuta el propio usuario para bloquear tales combinaciones importantes.

2.4.2. ¿Por qué usar Lock My PC?

Porque los usuarios o los cibernautas siempre están acechando en sus mensajes del e-

mail, programas, datos, archivos, etc., Lock My PC le permite cerrar con llave a su computadora con una contraseña mientras usted lo deja desatendido. Usted puede bloquear a la computadora, desde el menú o “Hotkey”, manualmente o cuando el computador no está siendo utilizado.

2.4.3. Rasgos y beneficios

- Rápida y segura la computadora está bloqueada por una combinación de teclas calientes, o con un clic.
- Bloque automático cuando la computadora está ociosa
- Bloqueo con Ctrl+Alt+Del.
- Modo de la instalación diferente – se puede personalizar o realizarlo en red.
- Seguridad de CD/DVD-ROM
- Apoyo del multiusuario
- Apagado automático cuando la computadora está bloqueada durante mucho tiempo.
- Opción de la contraseña ciega
- Modo de disimulo
- Compatibilidad con Windows XP x64.
- Ciclo de bloqueo para imágenes de pantalla.
- Protección para el protector de pantalla.
- Se puede ver películas bajo la pantalla con bloqueo.
- Protege con contraseña los programas para instalar y desinstalar.
- Permite emitir órdenes en línea.

En primer lugar, cuando su computadora es bloqueada por Windows, el usuario que tenga los privilegios Administrativos puede abrir a su computadora, esto obligará a cerrar la sesión. Si la opción de la pantalla Bienvenida se habilita en su computadora (las escenas predefinidas para la computadora del no-dominio), Win+L no bloquea la computadora en absoluto. Si se comparte con otros usuarios el login con su usernames pueden usar su computadora

TABLA COMPARATIVO EN SOFTWARE PARA RESTAURACIÓN DE SISTEMAS OPERATIVOS

	SOFTWARE		
CARACTERISTICAS	**DEEP FREEZE**	**NORTON GHOST**	**LOCK MY PC**
Protección total de virus, programas maliciosos y programas espías	x		
Funciona a la velocidad original y optima	x		x
Tiempos de mantenimiento programados	x	x	x
Posibilidad de elegir particiones del disco	x		
CMOS protegida	x		
Elimina el mantenimiento	x	x	

técnico rutinario a las computadoras			
Garantiza el 100% de disponibilidad en todas sus computadoras	x	x	x
Seguridad de su información	x	x	x
Encripta las copias de seguridad		x	
Examina archivos y carpetas perdidos o dañados.		x	
le permite definir y ejecutar una copia de respaldo		x	
No requiere Instalación			
Protección de fotos con clave			x
Es un archivo ejecutable			x

Tabla No. 1: Tabla comparativa de software de seguridad.

CAPITULO III

3. Desarrollo de la propuesta

La presente propuesta está basada en la protección y seguridad inteligente de la información mediante la recuperación instantánea de los datos del disco duro y del CMOS, para lo cual utilizaremos un Hardware desarrollado para este efecto llamado PCGuard y la utilización del Software NetManager el mismo que nos permitirá administrar y monitorear los equipos conectados a un servidor central.

Para el desarrollo de la investigación detallo los pasos y procedimientos para la instalación tanto del hardware y software utilizados para proteger cada uno de los equipos que se encuentran en el Laboratorio No. 5 de la Pontificia Universidad Católica del Ecuador Sede Ambato.

3.1. Saming Pc Guard.

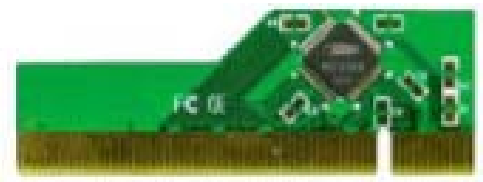


Figura No. 2: Tarjeta o Microchip “PCGuard”

PCGuard.- Es un microchip en forma de una tarjeta PCI -único en el mercado- que protege y asegura totalmente la información y configuración de su PC. Provee

simultáneamente una completa protección de la información guardada en el disco duro de la PC y del Sistema Operativo a través de funciones de grabación dinámica y recuperación instantánea.

PCGuard puede recuperar la información protegida, en segundos; sin ocupar espacio valioso en el disco duro o utilizar recursos del sistema. Usando PCProtek el sistema estará protegido contra toda clase de virus informáticos, hackers o intentos deliberados de destrucción de información guardada en el disco duro.

PCGuard es un HARDWARE de seguridad, ideal para ser utilizado en PCs que se encuentran dentro de una red LAN dentro de empresas, entidades de gobierno e institutos educativos por su extraordinaria capacidad de acelerar los procesos de mantenimiento y soporte técnico y protección de sistemas operativos.

3.1.1. Características Principales de PCGuard

Recupera información instantáneamente, incluso si se ha FORMATEADO el disco duro o se han reconfigurado particiones en el disco, protegiendo la información todo el tiempo.

Su operación es muy simple: no se necesitan conocimientos profundos en manejo de computadoras. Sólo se requiere REINICIAR la PC, presionar una tecla y toda la información será recuperada en segundos.

Nunca más perderá información vital, ni tiempo valioso reinstalando Sistemas Operativos.

La velocidad de protección y recuperación es impresionante: de 2 a 8 segundos para recuperar 40GB de información.

Es un drástico antivirus: recupera todo el sistema una vez infectado por cualquier virus, spyware, troyano o gusano.

Adopta una estructura inteligente de Doble Kernel [1]. Rápidamente protege y recupera el sistema operativo y los parámetros del CMOS [2].

Trabaja independientemente del Sistema Operativo y recupera información incluso si el Sistema Operativo se cae.

Compatible con MS Windows (95, 98, Me, NT, 2000, 2003, XP), y discos duros DMA 133/100/66, FAT16/FAT32/NTFS de hasta 320 GB. También soporta sistemas con doble Sistema Operativo y hasta 24 particiones de disco.

Sólo el Administrador del Sistema o persona autorizada puede modificar los parámetros de protección de PCGuard mediante el uso de una Contraseña o Password.

[1] Kernel: Parte fundamental de un sistema operativo. Permite la interacción entre el hardware y el resto del sistema.
[2] La CMOS guarda información fundamental de la configuración del sistema en un chip especial en la placa madre

Comparación con otros Productos

Comparación con otros Productos: Actividades	Antivirus	Antispyware	Antiadware	**PCGuard**
Tiempo que necesita para ser instalado	10 a 30 minutos	5 minutos	5 a 2 minutos	**1 a 2 minutos**
¿Necesita actualizaciones frecuentes?	1 por semana	1 por mes	1 por mes	NO
¿Cuanto tiempo necesita para trabajar?	30 a 45 minutos	10 a 30 minutos	5 a 20 minutos	**8 a 15 segundos**
¿Afecta el rendimiento de la computadora?	SI	SI	SI	**NO**
¿Ocupa espacio en el Disco Duro?	SI	SI	SI	**NO**
¿Tiene suscripción anual?	SI	NO	NO	**NO**
Virus	SI	NO	NO	**SI**
Spyware (espionaje)	SI	SI	NO	**SI**
Adware (publicidad)	NO	NO	SI	**SI**
Troyanos	NO	NO	NO	**SI**
Worms (gusanos)	NO	NO	NO	**SI**
Pop up installers	NO	NO	NO	**SI**

Ataques de Hackers	NO	NO	NO	**SI**
Instalaciones defectuosas	NO	NO	NO	**SI**
Errores de usuario	NO	NO	NO	**SI**
Vandalismo de usuario	NO	NO	NO	**SI**
Cambios de configuración no autorizados	NO	NO	NO	**SI**

Tabla No. 2: Comparación entre productos de seguridad.

3.2. Entidades que pueden acceder al Microchip PCGuard.

En organizaciones cualesquiera, donde existan computadoras utilizadas por personas con diferentes grados de conocimiento en computación, surgirán frecuentemente problemas técnicos e informáticos de diversa índole.

PCGuard soluciona definitivamente los siguientes problemas:

Información borrada o modificada, infecciones por virus o software espías, mala reconfiguración del sistema operativo. Un formateo accidental o intencional del disco duro, puede retrasar o interrumpir las actividades diarias de toda la Organización. Ataques maliciosos a las computadoras son muchas veces los causantes de que se paralicen las actividades en una organización, con pérdidas en algunos casos incalculables. Con el microchip de seguridad PCGuard, usted puede eliminar el daño que estos problemas pueden causar a su organización.

Para Empresas Privadas y Públicas

Es casi una constante dentro de las empresas privadas y públicas, el que los empleados instalen programas no autorizados, descarguen archivos infectados o cambien la configuración de las computadoras que usan.

Esta mala costumbre acarrea serios problemas para el área de sistemas o soporte técnico y pone en riesgo la seguridad de la información de la empresa.

El microchip de seguridad PCGuard soluciona este problema: permite -por medio de un Password-que los administradores y las personas autorizadas puedan proteger y recuperar toda la información de la PC en segundos.

Para Cabinas Internet

Es debido a los altos volúmenes de navegación sin control por Internet, que las computadoras terminan con archivos corruptos, o infectados con algún tipo de virus, troyanos, gusanos, etc.

El tiempo que se necesita para arreglar estos problemas, se traduce en perdidas de dinero debido a la inoperatividad de los sistemas durante la reparación.

Con la instalación del dispositivo de seguridad PCGuard, todos los problemas y modificaciones que sufren las computadoras pueden ser revertidos y completamente anulados EN SEGUNDOS con tan solo REINICIAR la computadora.

Para Ensambladores de Computadoras

Estudios estadísticos realizados entre vendedores y ensambladores de computadoras, demuestran que un 60% de las llamadas que reciben para Soporte Técnico o Servicio al cliente, están relacionadas con mal funcionamiento de programas (Software) en lugar de fallas de piezas electrónicas (Hardware).

Estos problemas generalmente son causados por negligencia o mal uso de la PC por parte del cliente o usuario final. Las pérdidas por soporte técnico en tiempo y dinero pueden ser muy altas.

Con el dispositivo de seguridad PCGuard, las computadoras siempre se recuperan de una caída del sistema.

Los clientes o usuarios solo deben REINICIAR su computadora para volver la PC a la normalidad, sin necesidad de llamar al área de Soporte.

Gracias a PCGuard, las llamadas por servicio técnico pueden ser sustancialmente reducidas.

3.3. Instalación de PCGuard en las computadoras del Laboratorio No. 5 de la Pontificia Universidad Católica del Ecuador Sede Ambato.

3.3.1. Procesos de la Instalación.

3.3.1.1. Instalación del software.

Como primer paso debemos empezar realizándolo la instalación del software o controladores del PCGuard, debido a que el sistema debe reconocer que se debe instalar un nuevo hardware, siguiendo los pasos como lo demuestra la figura No. 3; y al reiniciar el mismo se deberá colocar la tarjeta o microchip.

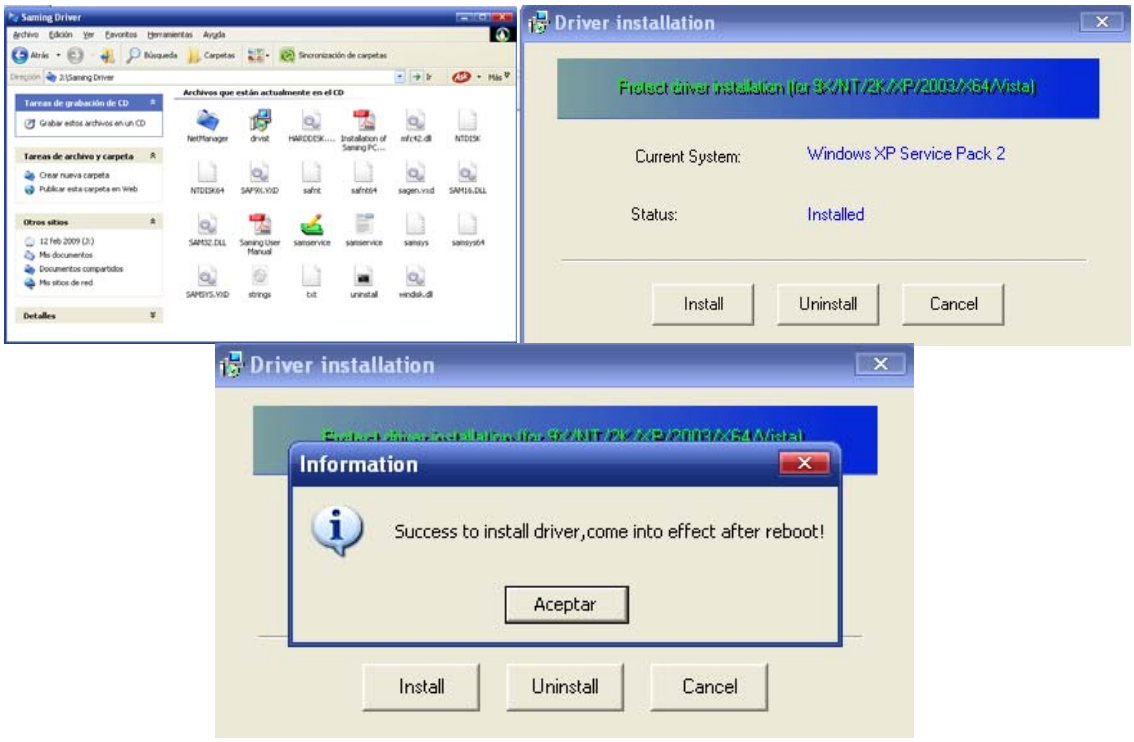


Figura No. 3: Archivos de instalación del Microchip “PCGuard”.

3.3.1.2. Instalación del Hardware PCGuard.

Para este paso debemos apagar el (los) equipo (s), y procedemos a colocar la tarjeta en la ranura PCI del Mainboard, como lo demuestra la figura No. 4.

Figura No. 4: Instalación de PCGuard

3.3.1.3. Configuración de Software y de la tarjeta PCguard.

Posterior a la instalación de la tarjeta debemos proceder a encender el computador, y durante el arranque del mismo debemos presionar la tecla “INICIO”, la misma que nos permitirá ingresar a las diferentes opciones con las cuales cuenta el microchip, de esta forma se configura dejándola lista para trabajar sin contratiempos ni inconvenientes.

Pasos para la instalación

a) Seleccionar “Instalar”, Figura 5. a)

b) Seleccionar la partición a la cual queremos dar protección, Unidad C:, Todo el disco duro ó simplemente seleccionamos las unidades y/o unidad que se desee. Figura 5 b).

c) Ahora se escoge el punto de recuperación de los datos, es decir si recuperamos directamente o con la utilización de un Password, presionando la tecla F9, con la auto recuperación desde el prompt, y, una recuperación automática. Figura 5 c).

d) Posterior a la selección del tipo de recuperación de la información debemos seleccionar la opción con la cual se la va a recuperar los datos, se puede sugerir que siempre se seleccione “Set Password”, para que el administrador sea el único que pueda o no aplicar la opción de recuperación. Figura 5 d).

e) Debemos se debe digitar la contraseña con la cual el administrador podrá recuperar la información. Figura 5 e).

f) Una vez concluido estos pasos simplemente empieza a guardarse la configuración de la partición seleccionada para el efecto de recuperación de datos, tardando como estimado 2 a 8 segundos de promedio en un disco duro de 40 GB. Figura 5 f).

g) Por último simplemente debemos reiniciar el equipo y ponernos a trabajar sin temor a los virus y/o mal manejo del software del computador.

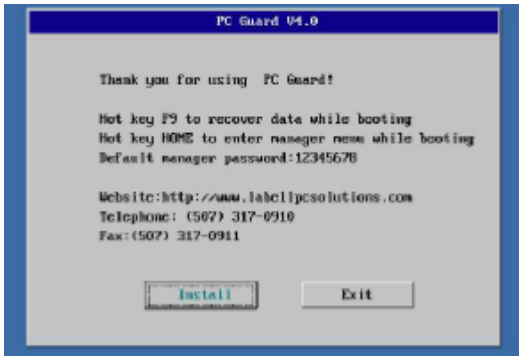


Figura No. 5 a). Acceso a la instalación.

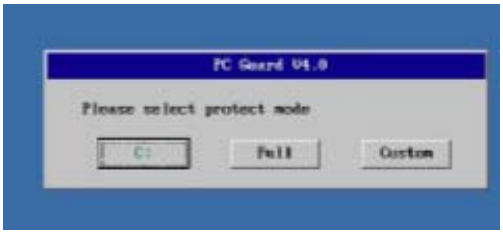


Figura No. 5 b) Selección de unidad de respaldo.

Figura No. 5 c) Tipo de acceso de respaldo.

Figura No. 5 d) Opción de gravado.

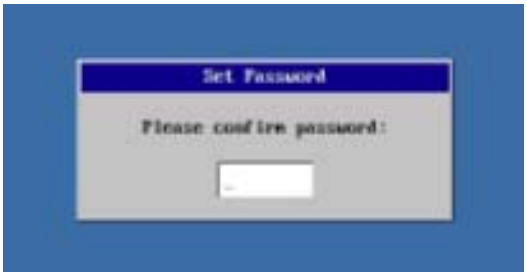


Figura No. 5 e) Digitación de clave de acceso.

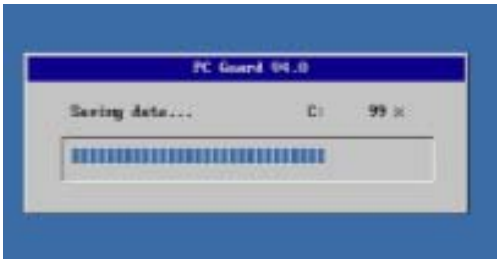


Figura No. 5 f) Gravado de información a respaldar.

3.4. Pruebas de funcionamiento del PCGuard.

Para la realización de las pruebas de funcionamiento del PCGuard en el Laboratorio No. 5 de la Pontificia Universidad Católica del Ecuador Sede Ambato, se ha procedido con la eliminación y restauración de la información, instalación de software, para finalmente realizar una prueba con la desinstalación de la tarjeta PCGuard del Mainboard, todas y cada una de ellas las detallamos a continuación.

3.4.1. Prueba A: Desinstalación y restauración de información.

3.4.1.1. Desinstalación de Microsoft Office.

Para la elaboración de esta prueba se ha desinstalado Microsoft Office (Figura 6), como un error común que en casos proceden los estudiantes o cualquier usuario de los laboratorios de la Pontificia Universidad Católica del Ecuador Sede Ambato, ya que no es el único software que se puede quitar del computador sin autorización del administrador del laboratorio.

Considerando estos antecedentes se verá como PCGuard restaura Microsoft Office (Figura 7), en cuestión de segundos sin tener la necesidad de volverlo a instalar y demorarse el tiempo que normalmente conlleva la misma.

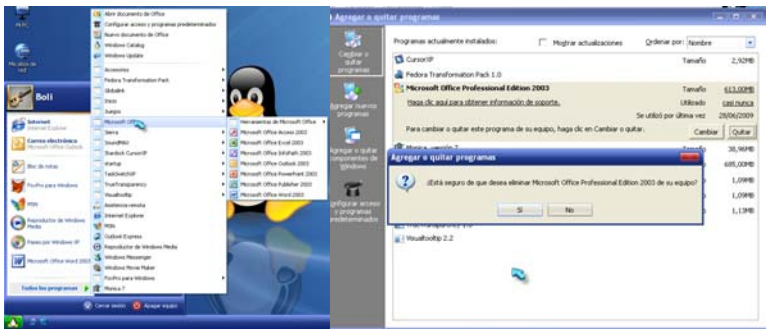


Figura No. 6: Desinstalación de Microsoft Office.

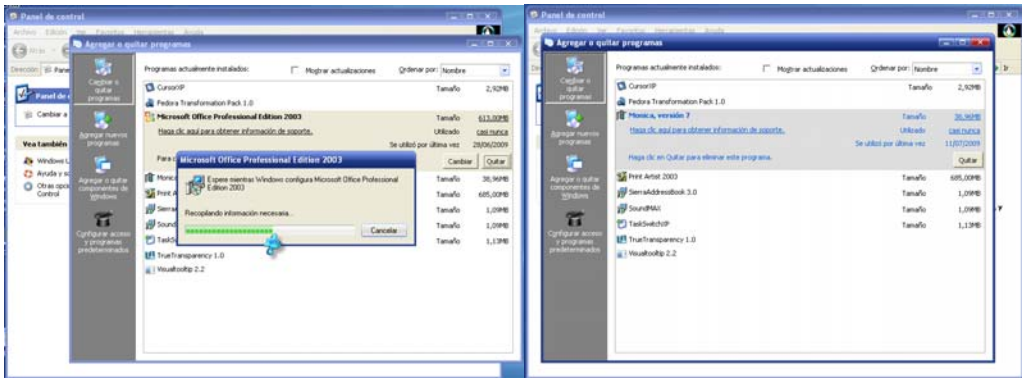


Figura No. 7: Microsoft Office, completamente desinstalado.

3.4.1.2. Restauración de Microsoft Office.

Como se comprueba a continuación, para restauración de Microsoft Office no es necesario volverlo a instalar, simplemente se debe utilizar el software de PCGuard, que con solo seleccionar la opción adecuada y digitar su contraseña de seguridad se verá como en cuestión de segundos Microsoft Office se encuentra nuevamente dentro de los programas que constaban en el computador. Para se procede a reiniciar el equipo y presionar la tecla F9 (Figura 8), con la cual accedemos a la opción de restaurar la información de a si ser el caso; luego de de ello automática e inmediatamente se enciende el computador y verificamos que Microsoft Office se encuentra nuevamente dentro de los programas (Figura 9).

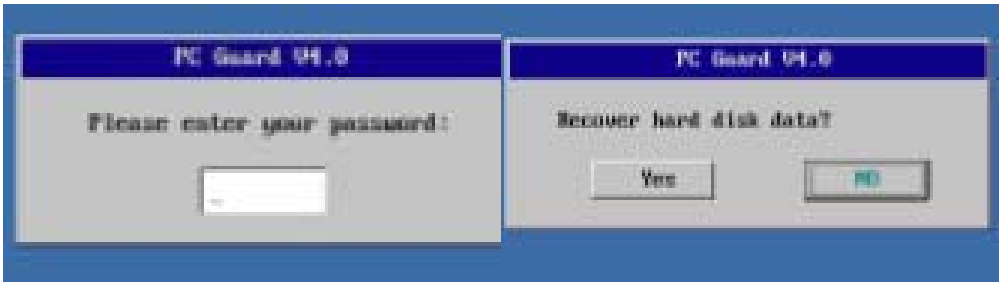


Figura No. 8: Ingreso a la opción de restauración de información.

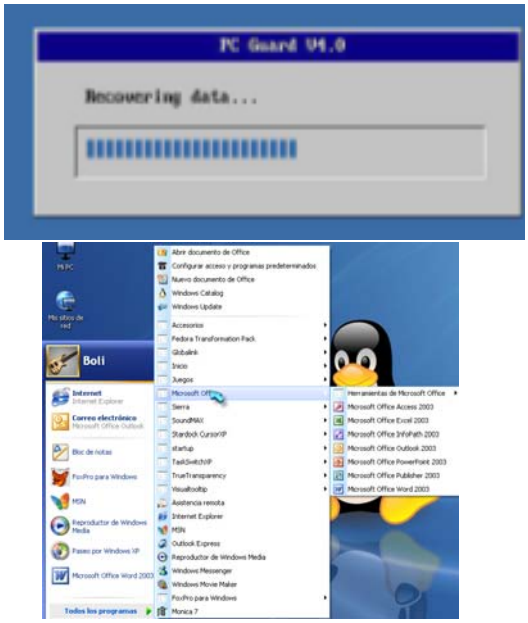


Figura No. 9: Restauración de la información eliminada por error.

3.4.2. Prueba B: Actualización de software del Laboratorio.

Dentro del campo educativo siempre existen diferentes necesidades ya sea por parte de los estudiantes o docentes que asisten al Laboratorio No. 5 de la Pontificia Universidad Católica del Ecuador Sede Ambato, se ha visto la necesidad de comprobar que si posterior a la fecha de guardado el software de su computador, se puede agregar otros programas a los ya anteriormente almacenados (Figura 10).

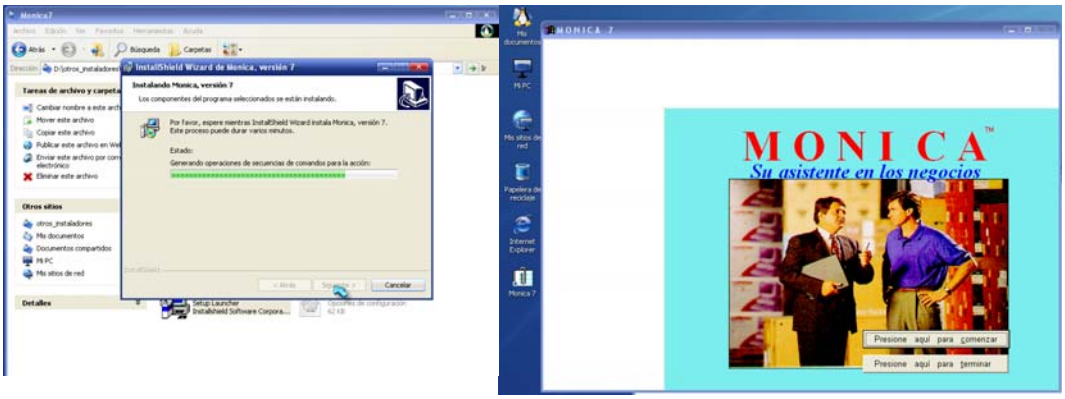


Figura No. 10: Software agregado al computador.

Ahora se procede a reiniciar el computador para agregar este Software instalado en la tarjeta PCGuard dentro de los datos que fueron ya almacenados en la misma, en la cual verificaremos luego de su restauración de la información, también quedará almacenado el otro programa o aplicación que se adiciono (Figura 11).

Para ello se debe reiniciar el computador y se debe presionar la tecla “INICIO” para acceder a las opciones de PCGuard y escogemos la opción “Save” para este caso (dependiendo la actividad que se desee realizar) Figura 12.

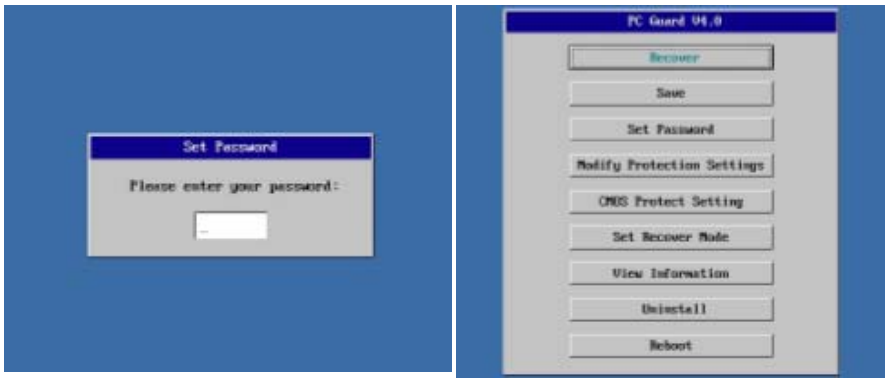


Figura No. 11: Almacenamiento de información con software adicionado al mismo.

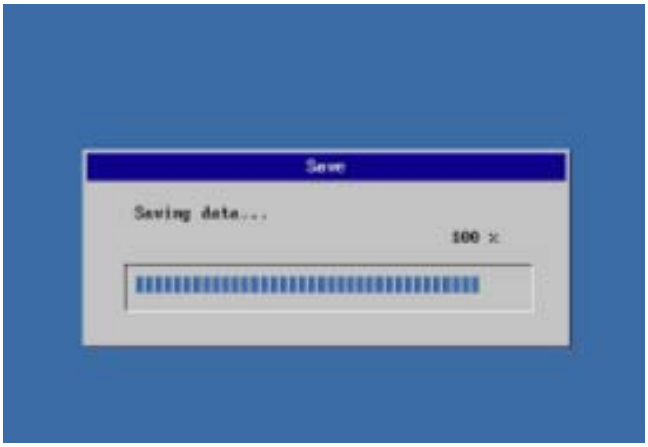


Figura No. 12: Almacenando la información.

3.4.3. Prueba C: Retiro manual de la tarjeta PCGuard.

Se verá como al retirar la tarjeta de PCGuard sin desinstala la misma ocurre incongruencias en el sistema operativo por lo cual se ve la importancia de la misma una vez procedido a su instalación y configuración.

Para ello se retirará manualmente el microchip y se procede a reiniciar el computador, verificando el error que ocurre (Figura 13), es por eso fundamental primero desinstalarla para que el sistema se configure y no se produzca errores de este tipo.

Se ve la obligación de no cometer estos errores, pues esto causaría daños como el no poder ingresar al sistema dándonos mayor trabajo debido a que se debe volver a instalar el sistema operativo y el demás software se utilice dentro del Laboratorio No. 5 de la Pontificia Universidad Católica del Ecuador Sede Ambato.

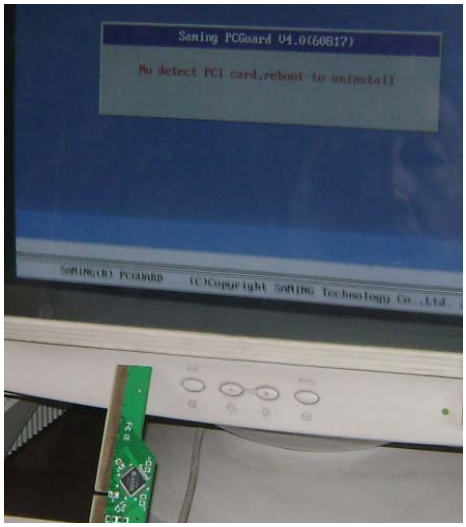


Figura No. 13: Error al retirar el microchip sin desinstalarlo.

3.4.4. Prueba D: Desinstalación de la tarjeta PCGuard.

Una vez demostrado la importancia y necesidad de la tarjeta PCGuard dentro del Laboratorio No. 5 de la Pontificia Universidad Católica del Ecuador se procede a realizar la prueba que es la desinstalación del microchip (Figura 14), restaurando la información y dejando al sistema como se lo encontró al inicio de las mismas, para posteriormente instalarla y configurarla nuevamente y que la persona encargada del laboratorio tenga respaldado los datos del sistema para su uso posterior de ser así el caso o necesidad, pues como en el laboratorio siempre ocurren eventos que no son programados en cuanto a los computadores será una herramienta que facilite el funcionamiento de el (los) computador (es) del laboratorio sin pérdida de tiempo. Para ello simplemente se debe reiniciar el computador, presionar la tecla “Inicio” y acceder a las opciones de PCGuard y seleccionar Uninstall, y optar por “Yes”, apagar el computador y proceder a retirar la tarjeta y el reinicio del computador.

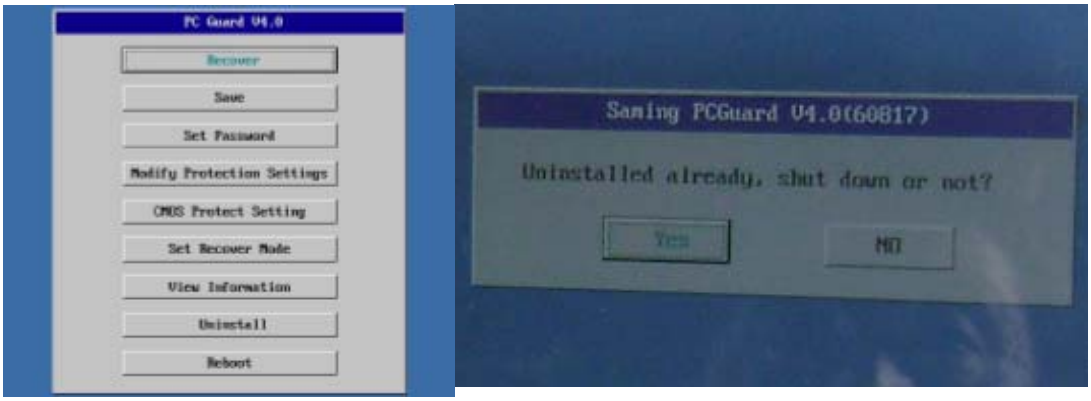


Figura No. 14: Desinstalación de PCGuard.

3.5. Administración del PCGuard mediante NET MANAGER desde el servidor.

Netmanager es un gestor de base de uso de las redes, tecnología para gestionar y llevar una verdadera administración y control de todos los clientes que se encuentren interconectados y relacionados con esta aplicación, para el manejo y vigilancia de las diferentes actividades que se desarrollan en un determinado sitio o lugar especifico.

3.5.1. Requisitos del Sistema.

El sistema para su instalación no tiene muchos requerimientos indispensables para la utilización de este software, los mismos que detallamos a continuación.

3.5.1.1. Requisito de Hardware:

Compatibilidad de plataforma de Intel, de un solo host de Internet / intranet.

3.5.1.2. Software de exigencia.

Como un software requerido para la instalación: Sistema operativo: Windows NT/2K (revisión de windows)

3.5.2. Instalación de Net Manager.

3.5.2.1. Instalación de NetManager “Cliente”

En primer lugar, usted debe descargar e instalar dos archivos de configuración que se encuentran en una carpeta llamada Netmanager que se localiza en un CD previamente grabado este dato, o también puede ubicarse en el escritorio de su computador.

Para abrir la carpeta, simplemente haga doble clic en ella. El siguiente grafico mostrará la posición del icono de Instalación.

Figura No. 15: Icono de instalación de Netmanager.

Haga doble clic en el icono referido, para mostrar el Interfaz de Instalación de NetManager como es mostrado en la figura.

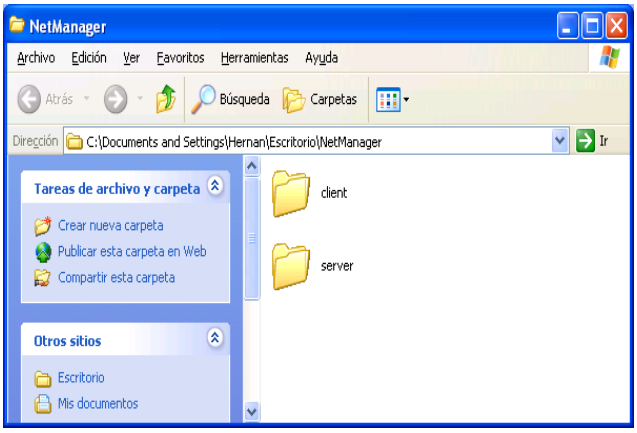


Figura No. 16: Carpeta de instalación.

Primeramente debemos instalar el archivo cliente en cada una de las computadoras que contiene el micro chip PcGuard, para lo cual damos doble clic en este registro y tendremos la siguiente figura 17:

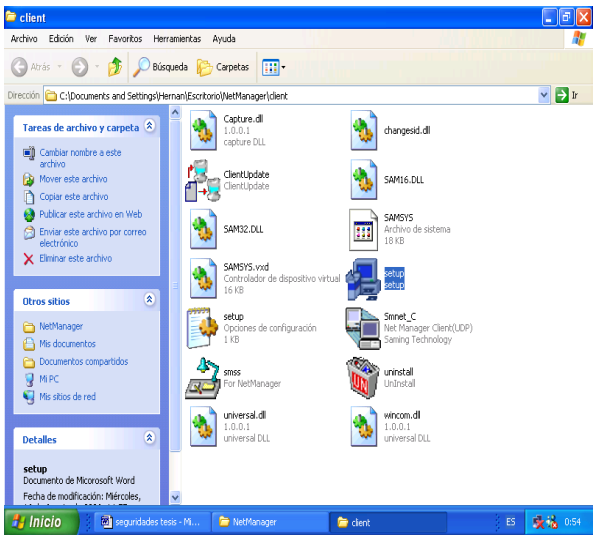


Figura No. 17: Icono “Setup” para la instalación.

Escogemos el icono Setup para su instalación, procedemos a seleccionar las diferentes opciones que durante la instalación se van presentando hasta llegar a concluir por completo con la instalación de Netmanager “Cliente” como muestra la figura No. 18.

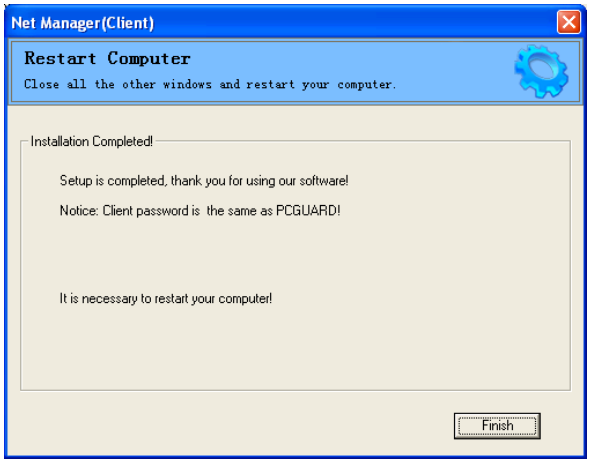


Figura No. 18: Finalización de la instalación

Este procedimiento detallado se debe realizar en cada una de las terminales del Laboratorio No. 5 de la Pontificia Universidad Católica del Ecuador Sede Ambato, para que el administrador del mismo pueda acceder a cada computador y pueda manipularlo y protegerlo con la utilización de PCGuard, mediante la utilización de NetManager.

3.5.2.2. Instalación de NetManager “Servidor”.

El siguiente paso es instalar el archivo servidor (Server), para este caso lo podemos hacer en un computador que puede o no tener el micro chip PcGuard, pues en esta

terminal será la que controle a todas las demás que se encuentren en el laboratorio con el hardware de seguridades en los discos duros de cada una de estas terminales.

Para lo cual damos doble clic en este archivo, en donde nos mostrará loa siguientes datos:

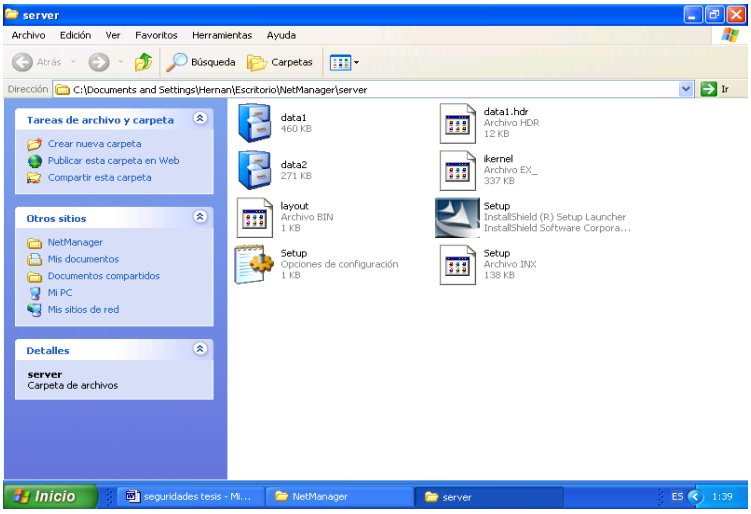


Figura No. 19: Instalación de Netmanager “Servidor”

Escogemos el archivo Setup para su configuración e instalación: Aceptamos todos los términos con el icono (Yes); A continuación nos pedirá información acerca el nombre del usuario y de la compañía, empresa con que se va a trabajar, seleccionando el destino que va a tener este registro.

Finalmente la instalación se ha completado del archivo Server (servidor) en el computador que se ha escogido como administrador, que va monitorear las demás terminales del laboratorio.

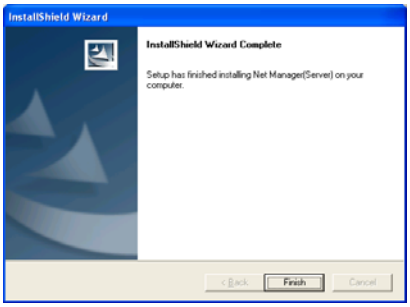


Figura No. 20: Finalización de la instalación de Netmanager “Servidor”

Con esta instalación y configuración para el monitoreo, administración y restauración desde un servidor, se pueden administrar todas las ventajas del microchip PCGUARD; entre los principales menús que contiene este software son las siguientes.

3.5.2.2. Menús del Servidor Netmanager

Monitoreo y restauración en el laboratorio.

Siempre el Net Manager usualmente estará el icono de este software en el escritorio del computador que esta como servidor de las demás terminales; y para ingresar siempre nos pedirá una clave que previamente ya fue preestablecida.

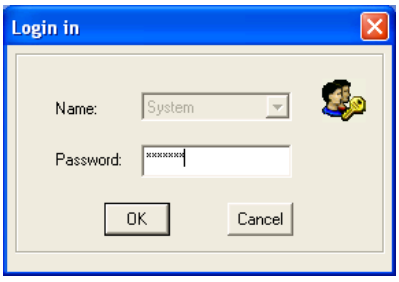


Figura No. 21: Ventana de acceso a NetManager.

Como podemos ver la figura No. 22; muestra los terminales que se encuentran instalados con la tarjeta PCGuard, a los cuales el administrador puede manipularlos sin la necesidad de estar sentados frente al mismo sino desde el servidor del laboratorio No. 5.

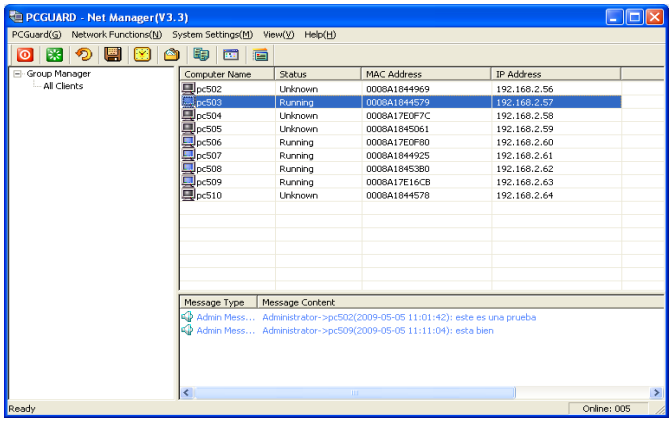


Figura No. 22: Monitoreo de los terminales del laboratorio.

PCGuard (Figura 23), se refiere exclusivamente al hardware PCGuard, en donde cada una de estos iconos nos permitirá a la configuración de una de las maquinas que se desea manipular, como podría ser recobrar datos, grabar, o desinstalar la tarjeta o micro chip de esta terminal señalada.

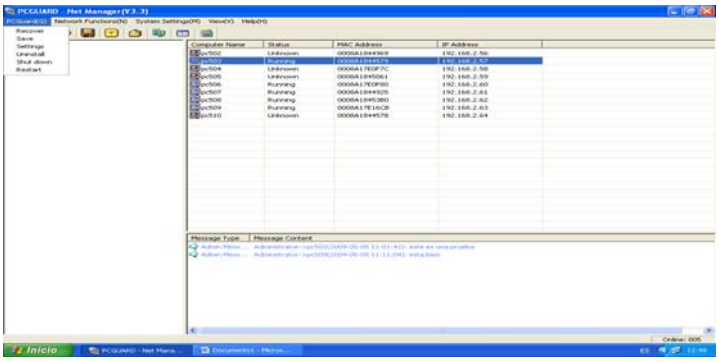


Figura No. 23: Acceso a cada uno de los terminales con PCGuard.

Network Funcional (Figura 24), permite trabajar con la red, demas monitores permitiendo enviar mensajes, transferir archivos; escenario para realizar una configuracion de la red que se esta administrando, asi tambien mirar la pantalla de cualquier terminal del laboratorio.

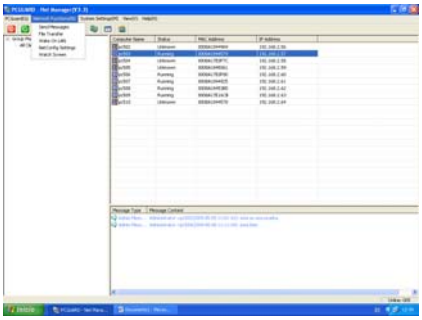


Figura No. 24: Monitoreo de los diferentes terminales.

Sistema Settings (Figura 25), describe un conjunto de actividades para el manejo del sistema, así podríamos resaltar tareas como un itinerario, horario en que todas las computadoras tengan una actividad específica en el tiempo definido ya sea para Recuperación o grabación de la información de los discos duros de cada una de ellas. Otro de los comandos nos ayuda a borrar al cliente que nos puede ocasionar problemas o dificultades en el trabajo de administración, así también a borrar los mensajes mandados por el servidor.

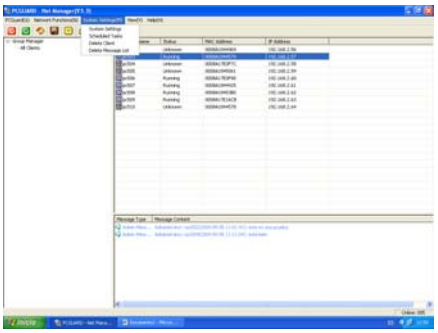


Figura 25: Configuración de los computadores del laboratorio.

View (Figura 26), ayuda a la visualización tanto de las terminales conectadas a la red, como al detalle general de cada una de estas con el fin de tener una clara y concisa referencia de las mismas.

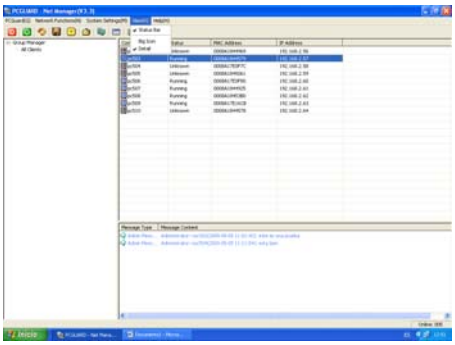


Figura No. 26: Visualización de terminales

3.6. Costos - Tiempos de Restauración

ACTIVIDADES	**Sin PCGuard**		**Con PCGuard**	
	Tiempo	Costo (cada/unidad)	Tiempo	Costo
Reinstalar el sistema Operativo	20-40 minutos/maquina	30 dolares	8 a 15 seg	0
Reinstalar el SW en los equipos	40 min o mas	40 dolares,según el software	0	0
Recuperación de daños	1 hora o mas/cada maquina	20 dolares en equipo	8 a 15 seg	0

Mantenimiento en los equipos	1 hora o mas/cada maquina	10 dolares en cada terminal	0	0
Proteccion de los equipos	2 a 3 horas	50 dolares o mas	0	0

Tabla No. 3: Relación de costos y tiempos de restauración

CAPÍTULO IV

4.1. CONCLUSIONES

- La inseguridad hoy en día en cuanto al software dañino para los sistemas operativos ha hecho que los usuarios empiecen a preocuparse por sus datos; adquiriendo diferentes tipos de seguridades para sus sistemas.

- La falta de prevención ante los virus informáticos hace que el administrador de sistemas se vean en la necesidad de adquirir nuevo software de control de virus como lo es Norton Antivirus, AVG, Panda, etc.

- La utilización de hardware PCGuard permite que el administrador de laboratorio disminuya su tiempo en la restauración del sistema de un determinado equipo.

- El uso de software de administración de red como Netmanager junto a PcGuard hacen un control efectivo en la recuperación y restauración del sistema.

- La instalación y configuración del Netmanager y PcGuard respectivamente reduce en un 99% los tiempos de restauración del sistema operativo de un equipo así como los costos de asistencia técnica.

- El PCGuard y Netmanager bien configurados y administrados correctamente es una herramienta con la que cuenta el administrador del laboratorio para posibles daños en el sistema operativo.

4.2. RECOMENDACIONES

- La persona encargada del laboratorio es la única que puede realizar la modificación o actualización de los parámetros de protección y restauración mediante la red.

- El administrador del laboratorio durante la configuración de Netmanager Cliente, deberá deshabilitar el Firewall en cada una de las terminales del laboratorio para poder instalarlo sin ningún inconveniente, debido al puerto que maneja este software.

- Nunca se debe retirar manualmente el microchip PCGuard sin antes haberlo desinstalado automáticamente, pues esto causa daños graves en el sistema operativo, dando como resultado negativo el no arranque del mismo, debiendo obligadamente el formateo del disco duro y del sistema operativo y demás programas.

- Siempre es recomendable que el laboratorista cuando respalde la información del sistema lo haga con una clave de seguridad tanto del hardware “PCGuard” y Software “NetManager” pues esto garantizará que sea la única persona que pueda manipular las seguridades de los discos duros del laboratorio.

- Cuando se actualice el software del laboratorio por parte del encargado del mismo, se debe proceder nuevamente a almacenar la información con la utilización del “NetManager” desde el servidor a todos los terminales, ya que ello permite tener la información actualizada para su restauración y/o recuperación de ser el caso.

BIBLIOGRAFÍA.

- Diccionario de Informática — Cultural SA. Madrid-España Edición 2002.
- Manual de Windows — Marco A. Tiznado Editorial: 1996.
- www.alerta-antivirus.es/seguridad/ — Fecha: 02/02/2009
- http://es.wikipedia.org/wiki/Deep_Freeze_(software)#Funcionamiento — Fecha: 02/02/2009
- http://www.tecnovamx.com/ DeepFreezeGral.html — Fecha: 10/03/2009
- http://deep-freeze.softonic.com/ — Fecha: 13/03/2009
- http://www.gcampus.com/pcguard.php — Fecha: 18/03/2009
- http://www.symantec.com/es/mx/business /ghost-solution-suite.shtm — Fecha: 06/04/2009
- http://www.labellpcsolutions.com/downloaddrivers /Pc%20Guard%20 Manual%20Spanish.pdf — Fecha: 07/04/2009

- http://www.labellpcsolutions.com/home.htmvirus Fecha: 19/04/2009

GLOSARIO DE TERMINOS

- **CMOS** Dispositivo que tiene almacenado la configuración básica del equipo y que no la pierde aunque se apague el computador, por estar alimentado generalmente por una fuente de alimentación autónoma.

- **HOTKEY** Tecla de activación. Nombre que recibe la tecla que al ser pulsada pone en marcha la ejecución de una función básica para el trabajo que está realizando el usuario.

- **LAN** Conjunto de ordenadores o computadoras que pueden compartir datos, aplicaciones y recursos (por ejemplo impresoras). Las computadoras de una red de área local (LAN, *Local Area Network*) están separadas por distancias de hasta unos pocos kilómetros, y se suelen usar en oficinas o campus universitarios.

- **Malware** Programas maliciosos, creados para hacer daños a los computadores a su alcance.

- **RAM** Memoria basada en semiconductores que puede ser leída y escrita por el microprocesador u otros dispositivos de hardware tantas veces como se quiera. Es una memoria de

almacenamiento temporal, donde el microprocesador coloca las aplicaciones que ejecuta el usuario y otra información necesaria para el control interno de tareas; su contenido desaparece cuando se apaga el ordenador o computadora, de ahí que los datos que se quieran conservar a largo plazo se tengan que almacenar en los discos. RAM es un acrónimo del inglés *Random Access Memory*.

- **FAT** Acrónimo de *File Allocation Table*, método de control de la ubicación física y del espacio libre de los archivos almacenados en disco empleado por ciertos sistemas operativos. Un archivo se almacena en un disco en segmentos de longitud fija llamados *clusters.*

- **TCP/IP** Acrónimo de *Transmission Control Protocol/Internet Protocol* (protocolo de control de transmisiones/protocolo de Internet), protocolos usados para el control de la transmisión en Internet. Permite que diferentes tipos de ordenadores o computadoras se comuniquen a través de redes heterogéneas

- **Spyware** Programas espías, creados por personas dedicadas a indagar en otros terminales que nos de su propiedad.

- **TI** Tecnología de la Información.

- **USB** Siglas de *Universal Serial Bus*, bus serie universal. Es una interfaz de hardware que permite conectar periféricos de baja velocidad, como el teclado, el ratón o *mouse*, la impresora o cámaras digitales, a los ordenadores o computadoras. Cada puerto USB es capaz de gestionar hasta 127 dispositivos, cuya conexión y desconexión se podrá realizar en caliente, es decir, sin necesidad de apagar la computadora.

ANEXO No. 1

Interpretación de datos.

La interpretación de datos se refiere al resultado de las encuestas aplicadas a los estudiantes de la Escuela de Sistemas de la Pontificia Universidad Católica del Ecuador sede Ambato, en la cual se pide su opinión personal acerca del problema planteado en esta investigación como es la Administración y Seguridad de los discos duros utilizando un Hardware y Software especializado.

Resultado de las encuestas aplicadas.

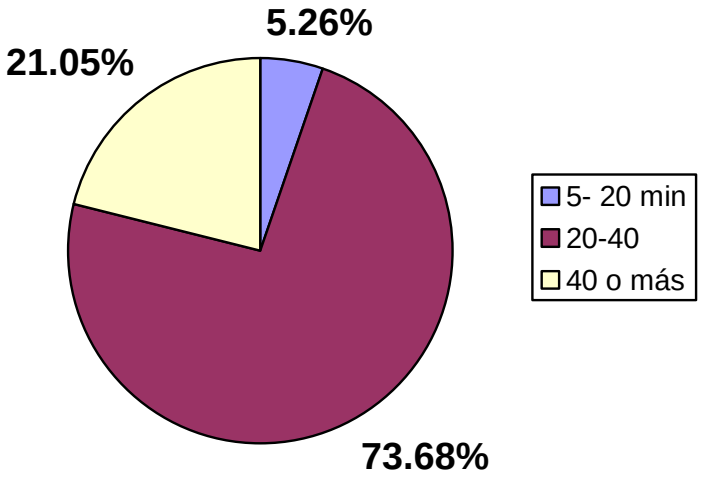
PREGUNTA 1

1. ¿Qué tiempo estima usted se demora en reinstalar el sistema operativo en un determinado computador?

Cuadro No. 1

ALTERNATIVA	CANT./Estudiantes	%
5-20 minutos	1	5.26
20-40 minutos	14	73.68
40 o más minutos	4	21.06
TOTAL	19	100

Gráfico No. 1



Fuente. Encuestas

Realizado por: Hernán Urquizo

ANALISIS

Como se puede observar en la gráfica, 1 encuestado que representa el 5.26% contesta que se demora de 5-20 minutos; 14 encuestados que representan el 73.68% contesta que se demora de 20-40 minutos y 4 encuestados que representan el 21.05% contesta que se demoran en instalar el sistema operativo más de 40 minutos.

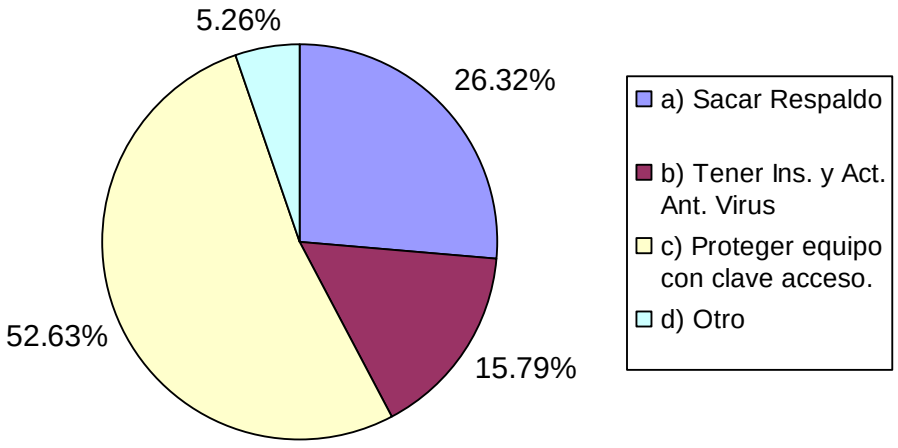
PREGUNTA 2.

2. ¿Cuál cree usted la mejor opción para proteger la configuración en el equipo que se encuentra en el laboratorio?

Cuadro No. 2

ALTERNATIVA	Cant./Estudiantes	%
a) Sacar Respaldo	5	26.31
b) Tener instalado y activado un antivirus	3	15.78
c) Proteger equipo con clave acceso.	10	52.63
d) Otro	1	5.26
TOTAL	19	100

Gráfico No. 2



Fuente. Encuestas

Realizado por: Hernán Urquizo

ANALISIS

Como se puede observar en la gráfica, 5 encuestados que representa el 26.32% contesta que se debe sacar respaldos; 3 encuestados que representan el 15.79% contesta que se debe tener instalado y actualizado un antivirus, 10 encuestados que representan el 52.63% contesta que se debe proteger su equipo con una clave de acceso, y 1 encuestado que representa el 5.26%, contesta que se debe tener otro tipo de protección de los equipos.

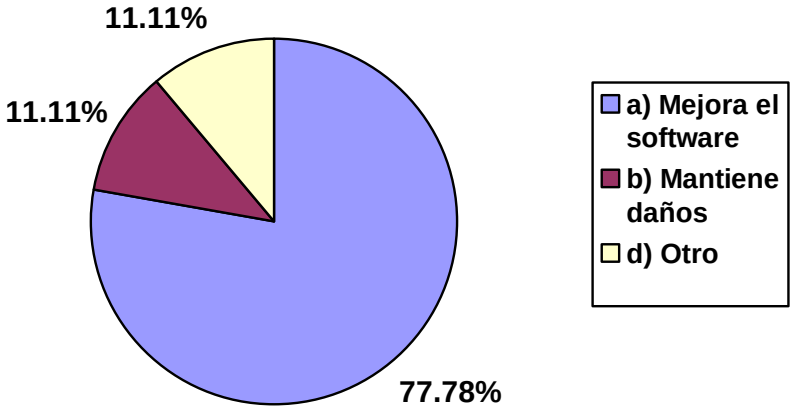
PREGUNTA 3.

3. Cree que al volver a reinstalar el software en los equipos, por daños causados por el usuario:

Cuadro No. 3

ALTERNATIVA	CANT./Estudiantes	%
a) Mejora el Software	17	89.47
b) Mantiene los daños	1	5.26
c) Otro	1	5.26
TOTAL	19	100

Gráfico No. 3



Fuente. Encuestas

Realizado por: Hernán Urquizo

ANALISIS

Como se puede observar en la gráfica, 7 encuestados que representa el 36.84% contesta que se mejora el software; 1 encuestado que representan el 5.26% contesta que se mantiene los daños, 10 encuestados que representan el 52.63% contesta que se disminuye los errores, y 1 encuestado que representa el 5.26%, contesta que es otro tipo de daños en los equipos.

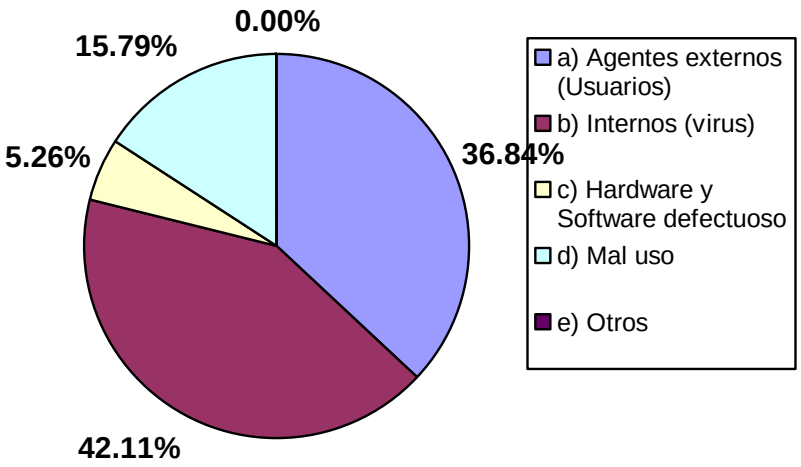
PREGUNTA 4.

4. ¿A qué agente podemos atribuirle daños en los equipos?

Cuadro No. 4

ALTERNATIVA	CANT./Estudiantes	%
a) Agentes externos (usuarios)	7	36.84
b) Internos (virus)	8	42.10
c) Hardware y Software defectuosos	1	5.26
d) Mal uso	3	15.78
e) Otros (electricidad)	0	0
TOTAL	19	100

Gráfico No. 4



Fuente. Encuestas

Realizado por: Hernán Urquizo

ANALISIS

Como se puede observar en la gráfica, 7 encuestados que representa el 36.84% contesta que se debe a los agentes externos (usuario), 8 encuestados que representan el 42.11% contesta que se debe los internos (virus), 1 encuestado que representan el 5.26% contesta que se debe al hardware y software defectuosos, y 3 encuestados que representa el 15.79%, contesta que se debe al mal uso en los equipos.

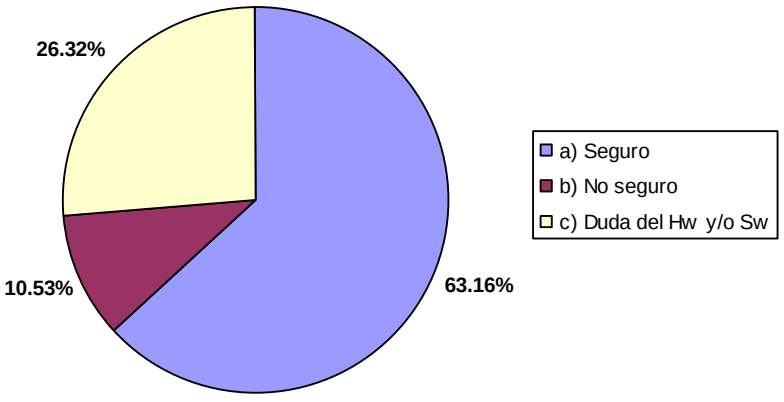
PREGUNTA 5.

5. ¿Se siente usted más seguro al saber que sus equipos tienen hardware y/o software que le ayude en la restauración de los mismos?

Cuadro No. 5

ALTERNATIVA	CANT./Estudiantes	%
a) Seguro	12	63.15
b) No seguro	2	10.52
c) Duda del Hardware y Software	5	26.31
TOTAL	19	100

Gráfico No. 5



Fuente. Encuestas

Realizado por: Hernán Urquizo

ANALISIS

Como se puede observar en la gráfica, 12 encuestados que representa el 63.16% contesta que es seguro que sus equipos tienen Hardware y/o Software que le ayude en la restauración de la información, 2 encuestados que representan el 10.52% contesta que no está seguro a esta ayuda de restauración, y 5 encuestados que representa el 26.31%, contesta que está en duda del Hardware y/o Software en los equipos.

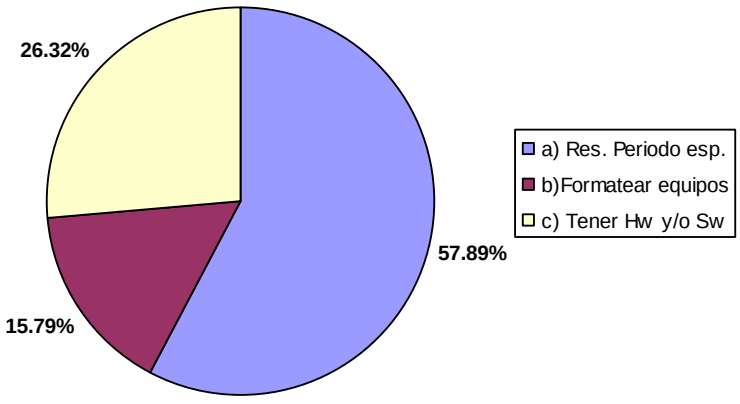
PREGUNTA 6.

6. Según su criterio ¿cuál sería la solución en cuanto a la restauración del Software instalado y configuración en sus equipos?

Cuadro No. 6

ALTERNATIVA	CANT./Estudiantes	%
a) Restaurar a un tiempo esperado	11	57.89
b) Formatear equipos	3	15.78
c) Tener Hardware y Software	5	26.31
TOTAL	19	100

Gráfico No. 6



Fuente. Encuestas

Realizado por: Hernán Urquizo

ANALISIS

Como se puede observar en la gráfica, 11 encuestados que representa el 57.89% contesta que se debe restaurar el funcionamiento de sus equipos a un determinado tiempo especifico, 3 encuestados que representan el 15.79% contesta que se debe formatear y volver a instalar el software en sus equipos, y 5 encuestados que representa el 26.31%, contesta que se debe tener Hardware y/o Software que le ayude a la recuperación de la información en los equipos.

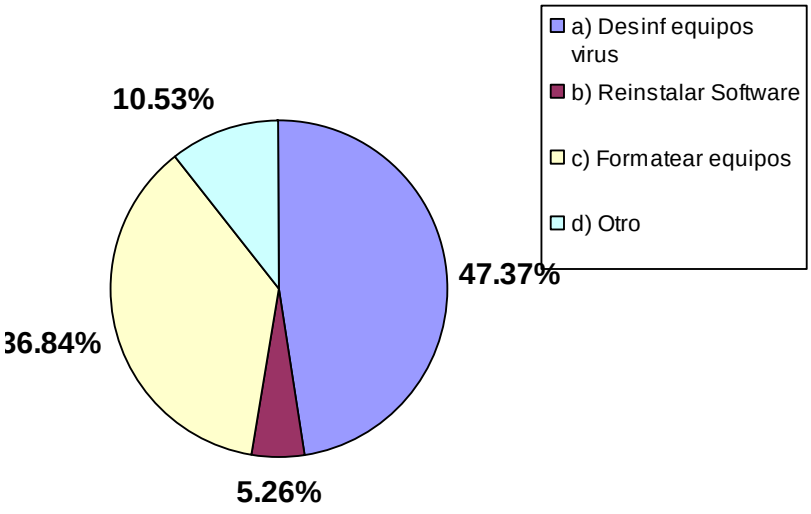
PREGUNTA 7.

7. ¿Cuál es el procedimiento cuando tiene un bajo rendimiento en sus equipos?

Cuadro No. 7

ALTERNATIVA	CANT./Estudiantes	%
a) Desinfectar los equipos	9	36.84
b) Reinstalar el Software	1	5.26
c) Formatear equipos	7	36.84
d) Otro	2	10.53
TOTAL	19	100

Gráfico No. 7



Fuente. Encuestas

Realizado por: Hernán Urquizo

ANALISIS

Como se puede observar en la gráfica, 9 encuestados que representa el 47.37% contesta que se debe desinfectar sus equipos de virus; 1 encuestado que representan el 5.26% contesta que se debe reinstalar el software en sus equipos, 7 encuestados que representan el 36.84% contesta que se debe formatear el equipo, y 2 encuestados que representa el 10.53%, contesta que es otro tipo de procedimiento en los equipos.

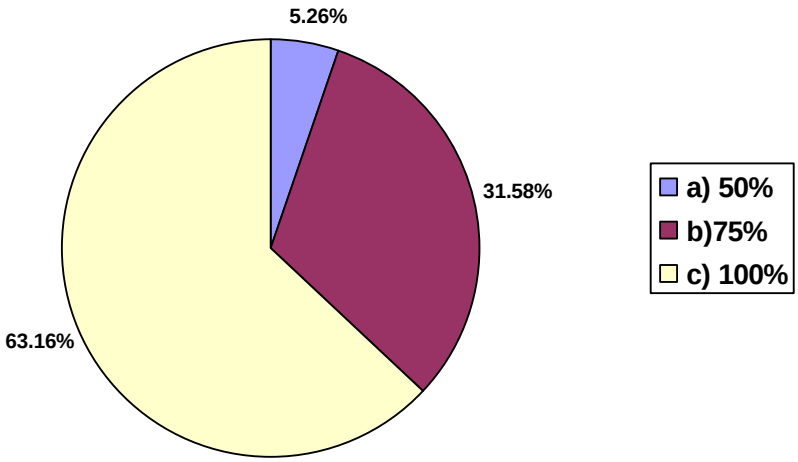
PREGUNTA 8.

8. ¿En qué porcentaje cree que mejorará la atención al usuario al brindarle un equipo siempre disponible y sin contratiempos?

Cuadro No. 8

ALTERNATIVA	CANT./Estudiantes	%
a) 50%	1	5.26
b) 75%	6	31.58
c) 100%	12	63.16
TOTAL	19	100

Gráfico No. 8



Fuente. Encuestas

Realizado por: Hernán Urquizo

ANÁLISIS

Como se puede observar en la gráfica, 1 encuestado que representa el 5.26% contesta que un 50% mejoraría la atención y tener siempre disponible los equipos, 6 encuestados que representan el 31.58% contesta que en un 75% mejorara nuestros equipos y sin contratiempos, y 12 encuestados que representa el 63.16%, contesta que nuestros equipos mejorara en un 100% la disponibilidad y sin problemas para la atención a los usuarios que manejen los equipos.

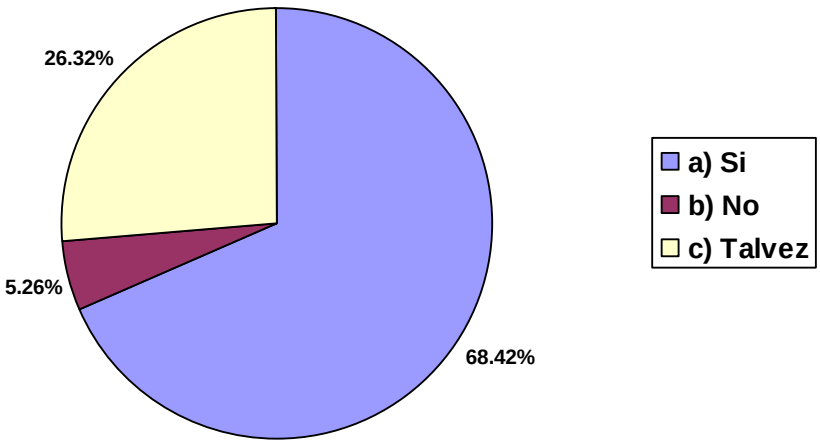
PREGUNTA 9.

9. Piensa que al tener instalado hardware y/o software de administración de seguridades se ahorraría tiempo al realizar el mantenimiento en los equipos.

Cuadro No. 9

ALTERNATIVA	CANT./Estudiantes	%
a) Si	13	68.42
b) No	1	5.26
c) Tal vez	5	26.32
TOTAL	19	100

Gráfico No. 9



Fuente. Encuestas

Realizado por: Hernán Urquizo

ANÁLISIS

Como se puede observar en la gráfica, 13 encuestados que representa el 68.42% contesta que si le ahorraría tiempo al tener instalado un hardware y/o software de administración en lo que seguridades en sus Disco duros de los equipos, 1 encuestado que representan el 5.26% contesta que no le ahorraría tiempo para el mantenimiento en los equipos, y 5 encuestados que representa el 26.32%, contesta que tal vez ahorraría tiempo al tener instalado este tipo de hardware y/o software en los equipos.

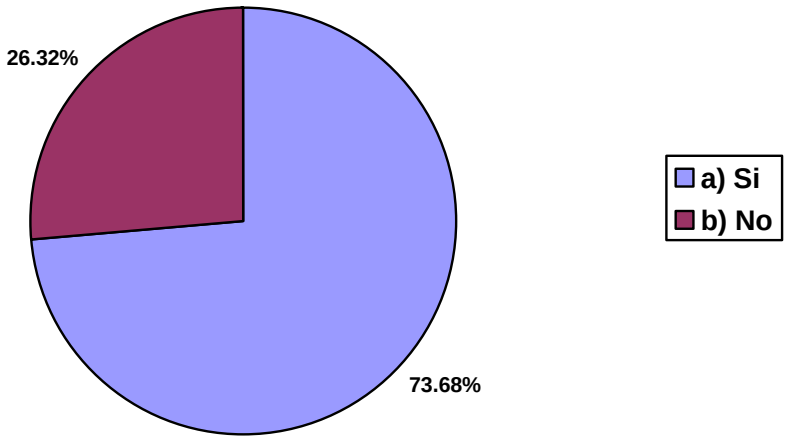
PREGUNTA 10.

10. Considera que se ahorraría tiempo al tener instalado hardware y/o software que permita recuperar la configuración que tiene su computador.

Cuadro No. 10

ALTERNATIVA	CANT./Estudiantes	%
a) Si	14	73.68
b) No	5	26.32
TOTAL	19	100

Gráfico No. 10



Fuente. Encuestas

Realizado por: Hernán Urquizo

ANALISIS

Como se puede observar en la gráfica, 14 encuestados que representa el 73.68% contesta que si le ahorraría tiempo al tener instalado un hardware y/o software que le permita recuperar la configuración que tiene su computador, 5 encuestados que representan el 26.32% contesta que no le ahorraría tiempo para la recuperación de la información que tiene sus equipos.

ANEXO No. 2

Manual del Usuario PCGuard

Pasos para la Instalación

En primer lugar, usted debe descargar e instalar a los controladores de PcGuard desde la página Web en: http://www.labellpcsolutions.com/formas/ descargar_pc_guard.htm; presione el Botón “Download” y usted lo encontrará disponible para todas las versiones de Windows incluyendo Windows Vista.

Descarga de Controladores

Usted debería seleccionar el Escritorio como su destino de archivo.

Al finalizar la descarga, su Escritorio tendrá un icono de PcGuard Drivers, que tiene que ser "descomprimido" con una utilidad llamada WinRAR (Fig A).

Si usted no tiene WinRAR instalado en su computadora, descárguelo desde aquí: http://www.rarlab.com/rar/wrar361.exe

FIG A

Para "descomprimir" este archivo, presionar el botón derecho de su ratón sobre el icono, y elegir la opción “Extract Here” del menú Cuando el proceso termina, la carpeta " Pc Guard Drivers” aparecerá en su Escritorio como se muestra en (Fig B).

FIG B

Para abrir la carpeta, simplemente haga doble click en ella.

El siguiente grafico (Fig C) mostrará la posición del icono de Instalación.

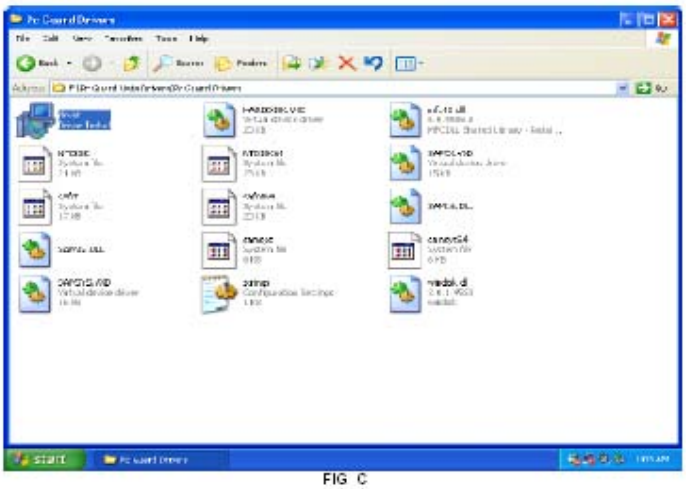


FIG C

Haga doble clic en el icono de Instalación, para mostrar el Interfaz de Instalación de Pc Guard drivers como es mostrado en (Fig D).

Instalación de Controladores

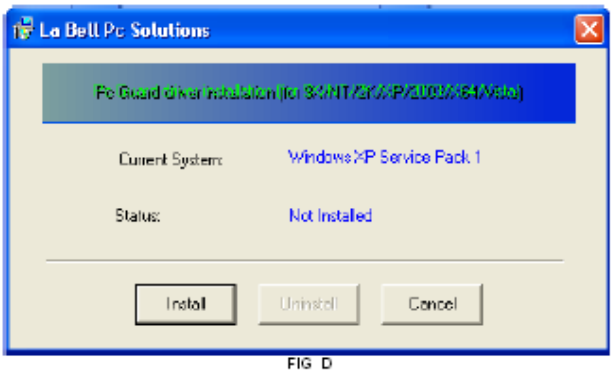


FIG D

Presione el botón Install y el mensaje en (Fig E) aparecerá.

FIG E

Ahora usted debe Apagar su computadora e instalar el microchip Pc Guard V4.0 en una ranura PCI vacía en la placa madre.

Instalación Física

El siguiente paso es remover una de las tapas de la computadora y ganar el acceso a los componentes internos. Localice una ranura PCI vacía en la placa madre, e instale Pc Guard, en ella, haciendo presión pero con cuidado. Asegúrese que Pc Guard este segura y firme en el lugar, como se muestra en (Fig F).

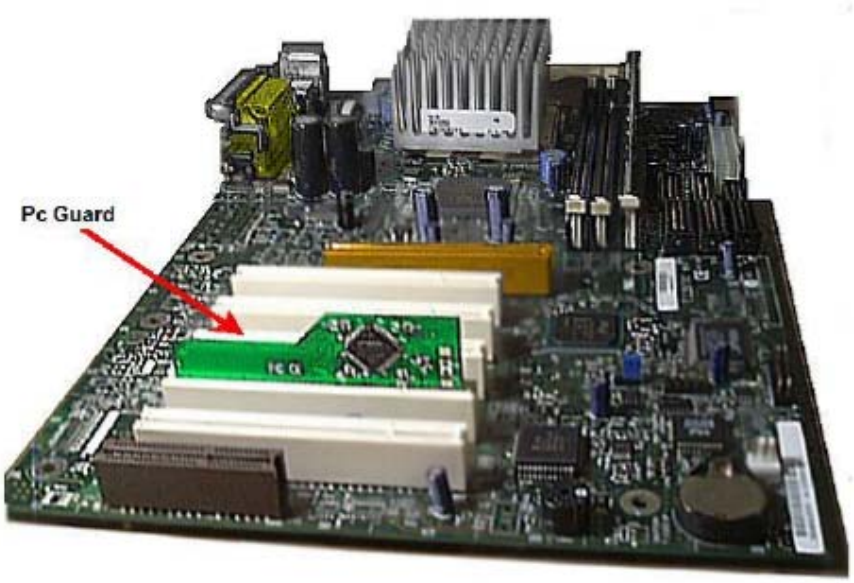


FIG F

Procure no dañar el microchip Pc Guard o la ranura PCI por aplicar demasiada.

Use precauciones antiestáticas manejando componentes electrónicos. Este tipo de corriente puede dañar permanentemente partes electrónicas.

En algunas computadoras, se debe de cambiar el orden de arranque en el BIOS para que la primera opción sea “Boot from LAN, o desde la Tarjeta de Red.

En modelos nuevos, usted no tiene que hacer esto.

Menú de Instalación de Pc Guard

Arranque la computadora. La pantalla de instalación de Pc Guard V4.0 aparecerá. Esta pantalla sólo aparece si Pc Guard no está instalado en su computadora.

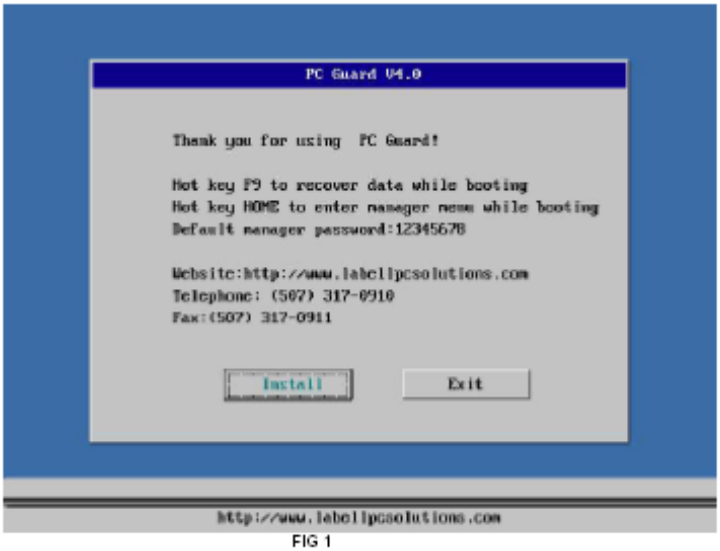


FIG 1

Pc Guard Viene con una Clave Preestablecida

Usando las teclas de Flecha, usted podrá cambiar las opciones.

Para Instalar Pc Guard V4.0 presione el Botón “INSTALL” y luego presione la tecla “Aceptar” en su teclado.

El grafico en (Fig 2), le ofrece las áreas que pueden ser protegidas con Pc Guard

FIG 2

Pc Guard protegerá su computadora dependiendo del área que usted escoja.

Las opciones son las siguientes:

[C :] La partición C: se protegerá. Si el Disco Duro no tiene más particiones todo el Disco Duro se protegerá.

[Full] Todo el Disco Duro se protege, incluyendo particiones y discos lógicos.

[Custom] Usted puede personalizar y decidir que particiones se protegerán Pc Guard puede proteger hasta 24 diferentes particiones.

Escoger la opción [Custom], hará aparecer la(Fig 3) . De lo contrario vaya a (Fig 5).

FIG 3

Siga las instrucciones, y realice su selección.

Cuando termine, tendrá que confirmar su selección en la (Fig 4).

FIG 4

Presionando NO, regresara a la figura (Fig 3).

Presionando YES, aparecerá la siguiente figura (Fig 5).

La Consola de Restauración (Fig 5) también aparecerá si selecciona [C:] o la opción [Full], del Menú de Áreas para ser protegidas (Fig 2).

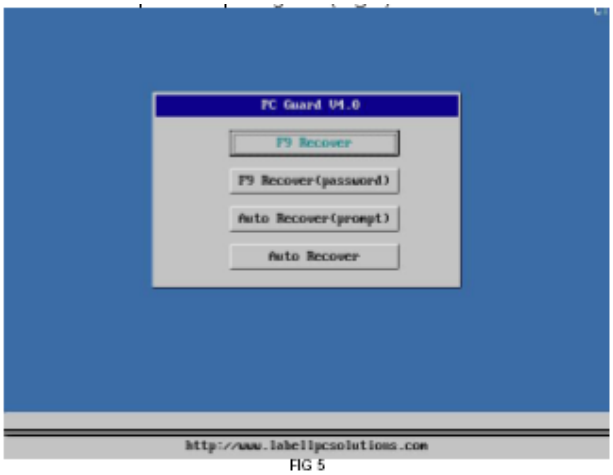


FIG 5

Consola de Restauración

En la Consola de Restauración usted decide como se restaurara su computadora.

[F9 Recover] (Manual. Para recuperar la última Configuración salvada por Pc Guard usted debe presionar varias veces a la Tecla F9 al iniciar su computadora).

[F9 Recover (password)] (Igual que la anterior, pero con esta opción usted debe ingresar su clave secreta para proceder).

[Auto Recover (prompt)] (Automático. Recupera la última configuración salvada cada vez que la computadora esta reinicializado y muestra el desarrollo del procedo de Recuperación.)

[Auto Recover] (Automático. Recupera la última configuración salvada cada vez que la computadora esta arrancada o reinicializado)

Al terminar esta etapa, aparecerá la siguiente Consola (Fig 6).

Consola de Tareas

FIG 6

Cada tarea es explicada a continuación:

[Save] – Guardar la configuración actual. (Fig 7)

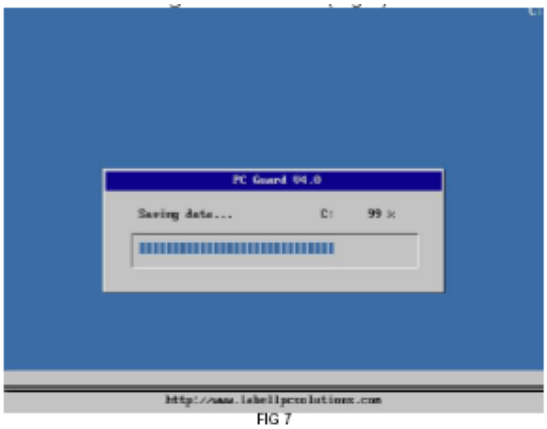


FIG 7

Pc Guard guardará la configuración actual de su computadora.

Al terminar el proceso, su sistema operativo se cargará.

[Set Password] – Establecer su clave secreta. (Fig 8) and (Fig 9)

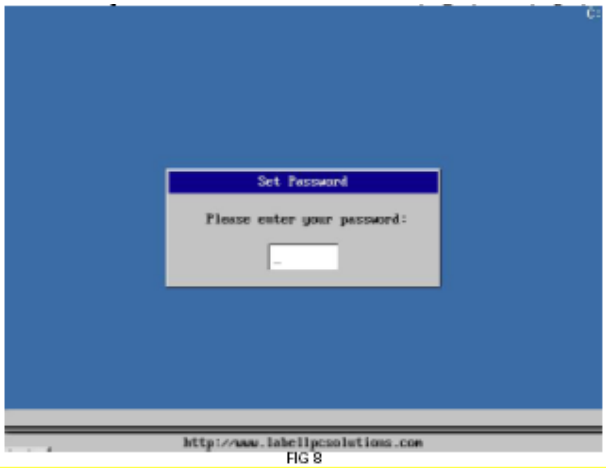


FIG 8

Por seguridad recomendamos cambiar la clave secreta preestablecida.

Aquí puede crear su clave secreta. Usted necesita la clave secreta para ordenar a Pc Guard que guarde cambios en su computadora.

Puede usar cualquier combinación de números, letras y símbolos especiales en su teclado, hasta un máximo de 8 caracteres de largo, al terminar presione la tecla “Aceptar” en su teclado.

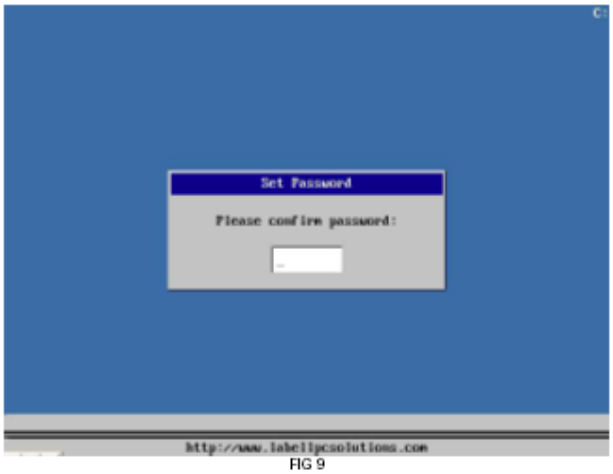


FIG 9

La (Fig 9) le pedirá que ingrese la clave secreta una vez más por motivos de seguridad. Otra vez, presione la tecla “Aceptar” en su teclado para confirmar su acción, al terminar, regresara a la Consola de Tareas (Fig 6).

[CMOS Protect Setting] – Protección del CMOS. (Fig 10)

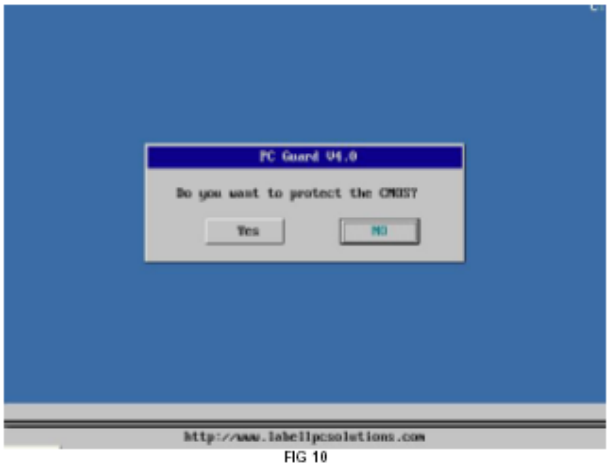


FIG 10

Esta opción le permite monitorear algún cambio en el área del CMOS, y recobrar los valores previamente guardados. (Disponible solamente si presiona YES).
Para terminar, presione la tecla “Aceptar”, y volverá a la Consola de Tareas (Fig 6).

[View Información] – PCGuard muestra el estado de protección actual de su Disco Duro y sus particiones. Aquí nada se puede cambiar.

Para regresar al menú anterior en (Fig 6), presione la tecla “ESC” en su teclado.

[Reboot] – Reiniciar su computadora. Todos los cambios hechos serán descartados. La última configuración salvada prevalecerá.

Administración del PCGuard.

Dando un toque varias veces a la tecla INICIO cuando su computadora arranca o reinicia, usted invocará a Pc Guard.

Pc Guard responderá a su llamado, y le pedirá la clave secreta (Fig 11)

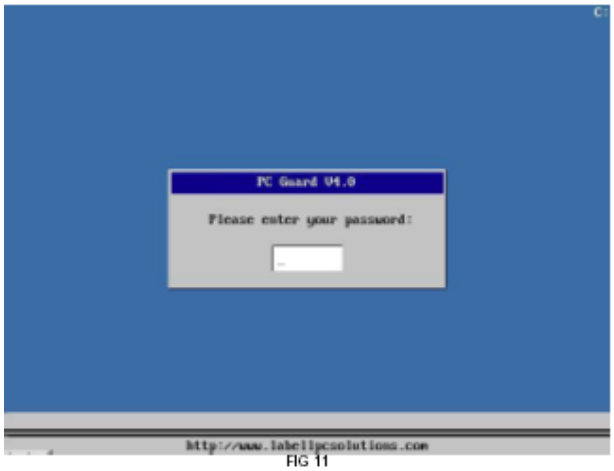


FIG 11

IMPORTANTE:

La clave secreta tiene que ser ingresada exactamente igual como se creó. (la letra „A. no es igual a la letra „a.). Recomendamos escribir y guardar su clave secreta en un lugar seguro. Ingrese la clave secreta y presione la tecla “Aceptar”.

El Menú de Administración de Pc Guard aparecerá (Fig 12).

Menú de Administración.

FIG 12

[Recover] – Restaura la última configuración guardada con Pc Guard. Usted debe de confirmar esta acción en la siguiente vista (Fig 13).

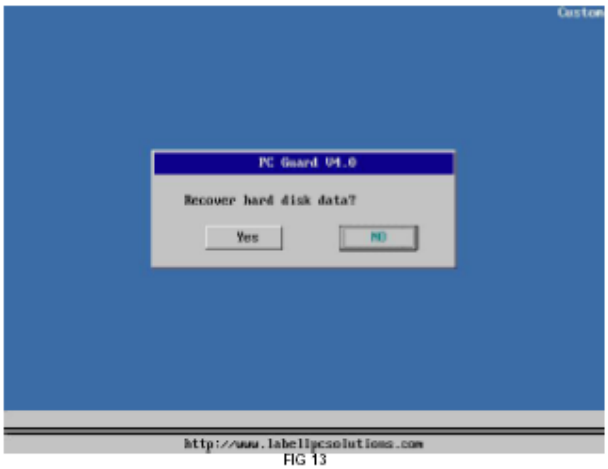


FIG 13

Presionando NO regresara al Menú de Administrador (Fig 12). Presionando YES comenzara la restauración (Fig 14).

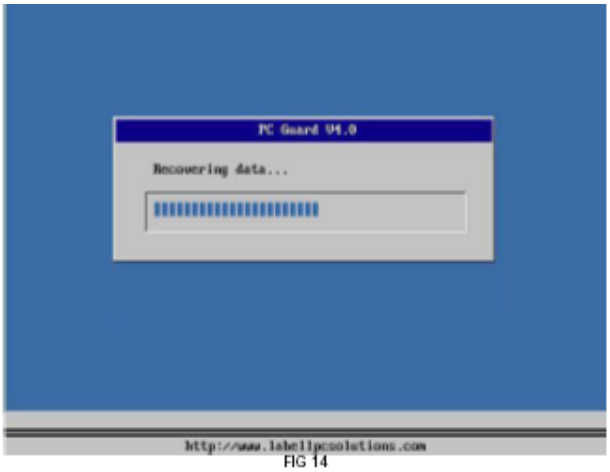


FIG 14

Terminado el proceso, su sistema operativo comienza a cargar.

Los últimos cambios en su computadora son desechados. La última configuración guardada con Pc Guard es la utilizada.

[Save] – Esta opción guarda la nueva configuración de su computadora.

El proceso es confirmado en la (Fig 15).

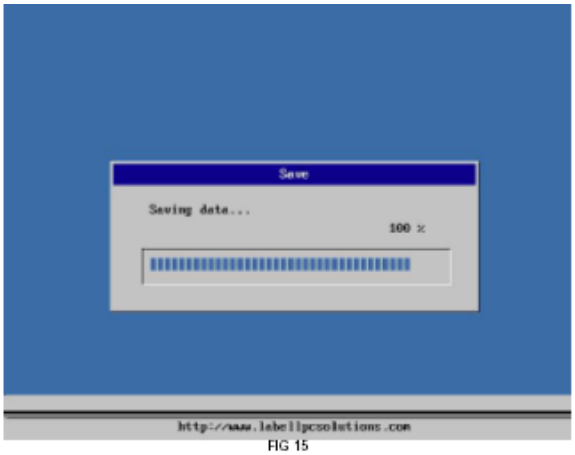


FIG 15

Esta tarea salva los nuevos cambios ocurridos en su computadora. Cuando la operación termina, el sistema operativo empieza a cargar. Los nuevos cambios se reflejan automáticamente.

[Set Password] – Establecer o cambiar la clave secreta.

La figura (Fig 16) muestra el siguiente dialogo.

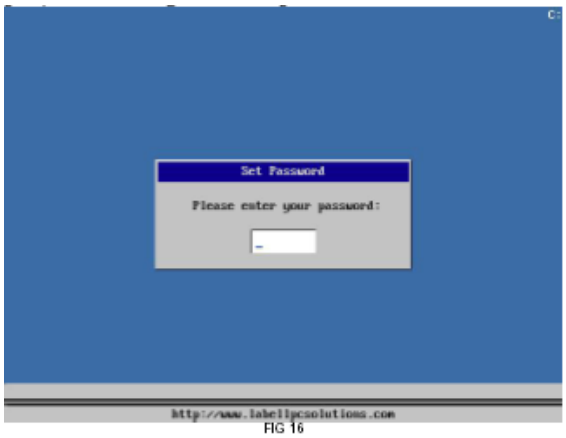


FIG 16

Ingrese la nueva clave secreta.

Puede usar cualquier combinación de números, letras y símbolos especiales en su teclado, hasta un máximo de 8 caracteres de largo.

Al terminar presione la tecla “Aceptar” en su teclado. Tiene que confirmar la nueva clave secreta como se muestra en la (Fig 17).

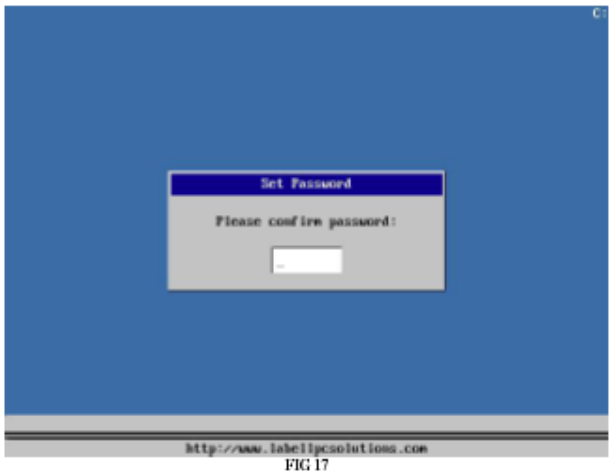


FIG 17

Por razones de seguridad recomendamos escribir y guardar su clave secreta en un lugar seguro. Presione la tecla “Aceptar” cuando termine. Inmediatamente, regresará al Menú de Administración (Fig 12).

[CMOS Protect Setting] – Pc Guard puede proteger el CMOS de su computador. Si usted escoge esta opción, el dialogo en figura (Fig 23) aparecerá.

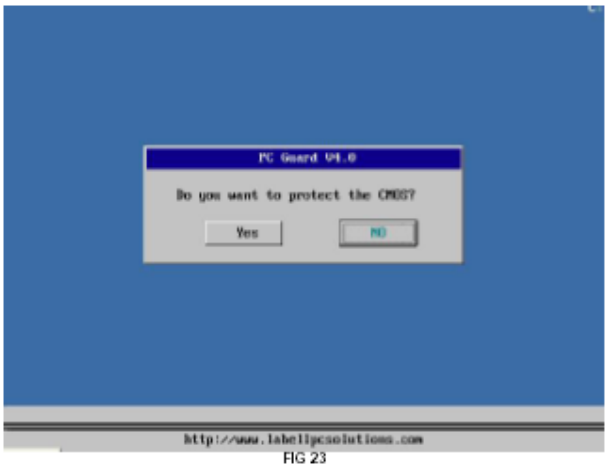


FIG 23

Presionando NO, regresara al Menú de Administración (Fig 12) sin haber hecho alteraciones. Presionando YES, regresara al Menú de Administración (Fig 12) pero habrá extendido la protección de Pc Guard al CMOS de su computadora.

[Set Recover Mode] – (Nuevo) esta opción le permite cambiar la forma en que Pc Guard protege su computadora desde el Menú de Administrador (Fig 24).

FIG 24

Para cambiarlo solo tiene que seleccionar una de las cuatro opciones. Pc Guard reconocerá su comando, y regresara al Menú de Administrador (Fig 12)

[View Información] – Esta opción le permite ver en un solo lugar las condiciones de protección de su computadora. Información como cuantas particiones tiene activas, cuales están protegidas y cuáles no, si el CMOS está protegido, y el Modo de Restauración actual de Pc Guard (Manual o Automático) (Fig 25).

FIG 25

Desde aquí usted no puede realizar ningún cambio. Para regresar al Menú de Administrador (Fig 12), presione la tecla de “ESC”.

[Uninstall] – esta opción des-instala Pc Guard de su computadora. Deberá remover físicamente Pc Guard de su computadora, de lo contrario, cada vez que la inicie o reinicie, el Menú de Instalación aparecerá. Otra forma de hacer desaparecer ese constante menú, es volver a instalar Pc Guard. Cuando usted selecciona esta opción, el siguiente dialogo aparece (Fig 26)

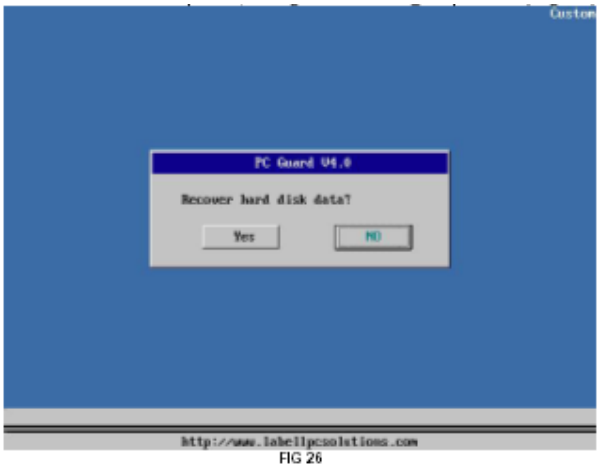


FIG 26

Presionando NO, lo regresara al Menú de Administrador (Fig 12). Presionando YES hará aparecer el siguiente dialogo (Fig 27).

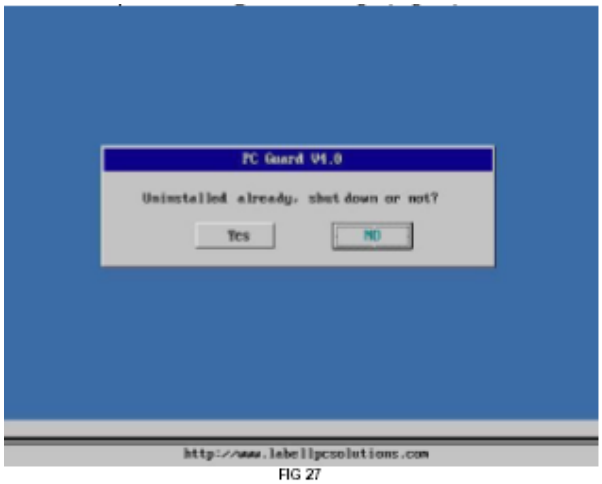


FIG 27

Presionando YES obliga a su computadora a apagarse, mientras que si presiona NO su computadora empezara a cargar su sistema operativo.

[Reboot] – Esta opción re-inicia su computadora

Proceso de Restauración.

Lo que usted vea a la hora de encender su computadora, dependerá de la forma de protección que escogió en la figura (Fig 5). Básicamente hay dos modalidades: Restauración Manual y Automática

Restauración Manual

(Necesita presionar la tecla F9 varias veces mientras su computadora enciende)

[F9 Recover] – La Restauración ocurre solo si usted presiona la tecla F9 cuando su computadora está iniciando o re-iniciando, de lo contrario, Pc Guard no dará indicios de su presencia en su computadora. Una vez presionada la tecla F9, el siguiente dialogo aparecerá (Fig 28).

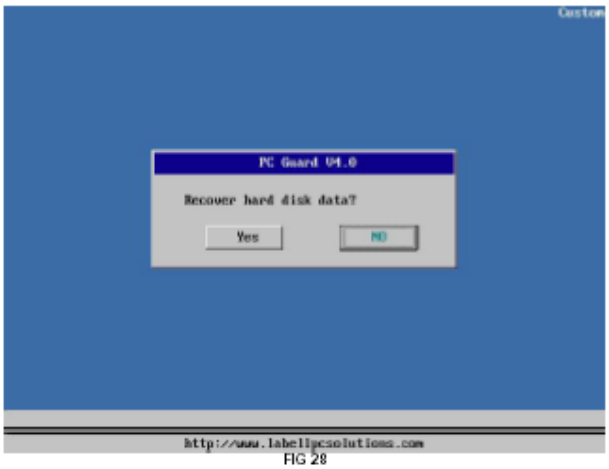


FIG 28

Presionando NO el proceso de Restauración se Cancela, y el sistema operativo continúa cargando. Presionando YES permite al proceso de Restauración que sea ejecutado (Fig 29).

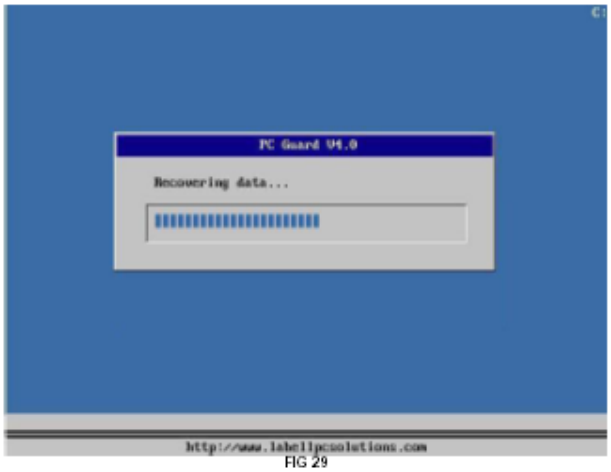


FIG 29

Una vez terminado el proceso de Restauración, el sistema operativo empieza a cargar. Los últimos cambios en su computadora son desechados. La última configuración salvada con Pc Guard es restablecida.

[F9 Recover (password)] – El procedimiento anterior se llevara a cabo después de ingresar la clave correcta mostrada en el siguiente dialogo (Fig 30).

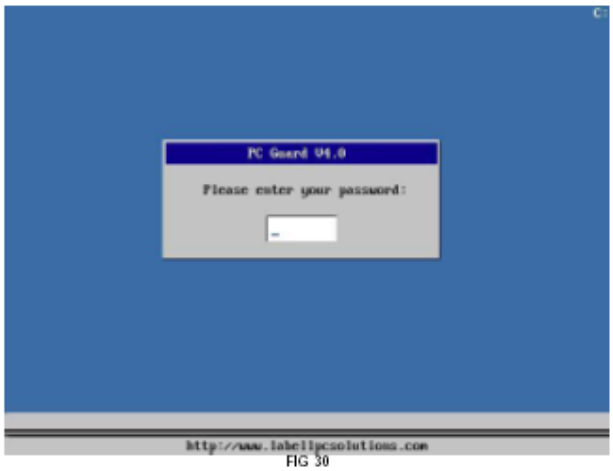


FIG 30

Una vez verificada la clave secreta, el procedimiento de Restauración es completado tal como se explicó anteriormente.

Restauración Automática.

[Auto Recover (Prompt)] – Restauración ocurre cada vez que su computadora inicia o reinicia. Un pequeño dialogo aparece momentáneamente para mostrar el proceso. No se necesita intervención de parte del usuario.

[Auto Recover] – Igual que el proceso anterior, con la diferencia de que no aparece ningún cuadro de dialogo.

Como Parte importante debemos remover exitosamente los controladores de Pc Guard de su computadora, usted debe primero desinstalar Pc Guard desde el Menú de Administrador, y escoger la opción [Uninstall] en figura (Fig 26) y (Fig 27). También se recomienda remover físicamente el microchip de Pc Guard.

Para desinstalar los controladores de Pc Guard, localice el icono de Instalación en el archivo de Pc Guard Drivers mostrado en (Fig 31).

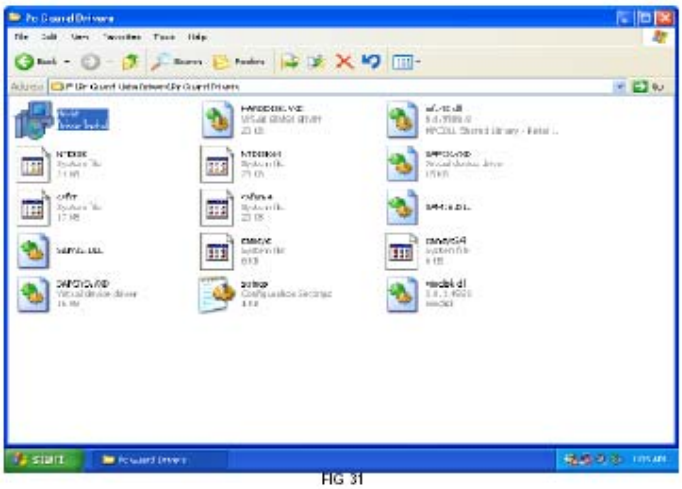


FIG 31

Haciendo doble click en el icono, el proceso de desinstalación comienza (Fig 32).

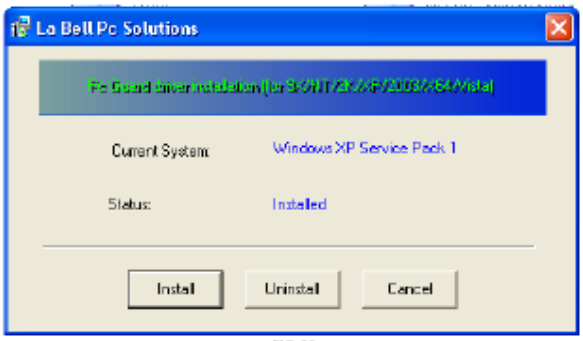


FIG 32

Presionando Uninstall usted recibirá un dialogo de confirmación (Fig 33).

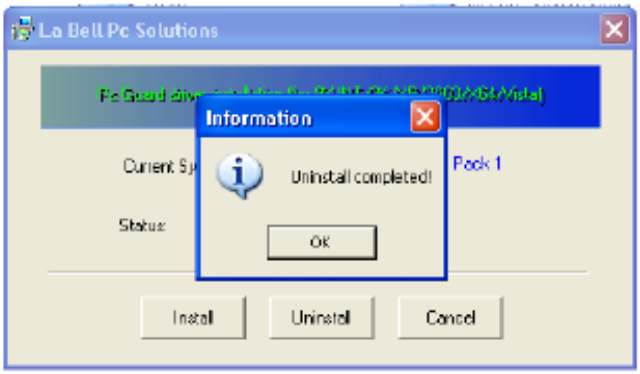


FIG 33

Presione OK para aceptar. Usted ha removido exitosamente Pc Guard de su computadora.