Universidad Central “Marta Abreu” de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Automática y Sistemas Computacionales

TRABAJO DE DIPLOMA

Sistema de Seguridad y Control Automatizado para Microcomputadoras en Red (SISCAM-R).

Autor: Eduardo Morera Darraido.

Tutor: Ing, Dannis Rivero Cañizares.

Santa Clara

2009

"Año del 50 Aniversario del Triunfo de la Revolución"

Universidad Central “Marta Abreu” de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Automática y Sistemas Computacionales

TRABAJO DE DIPLOMA

Sistema de Seguridad y Control Automatizado para Microcomputadoras en Red (SISCAM-R).

Autor: Eduardo Morera Darraido.

morera@uclv.edu.cu

Tutor: Ing, Dannis Rivero Cañizares.

Dpto. Informatización, CDICT, dannis@uclv.edu.cu

Santa Clara

2009

"Año del 50 Aniversario del Triunfo de la Revolución"

Hago constar que el presente trabajo de diploma fue realizado en la Universidad Central "Marta Abreu" de Las Villas como parte de la culminación de estudios de la especialidad de Ingeniería en Automática, autorizando a que el mismo sea utilizado por la Institución, para los fines que estime conveniente, tanto de forma parcial como total y que además no podrá ser presentado en eventos, ni publicados sin autorización de la Universidad.

Firma del Autor

Los abajo firmantes certificamos que el presente trabajo ha sido realizado según acuerdo de la dirección de nuestro centro y el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

Firma del Autor

Firma del Jefe de Departamento donde se defiende el trabajo

Firma del Responsable de Información Científico-Técnica

PENSAMIENTO

La duda es el principio de la sabiduría.

Anónimo

DEDICATORIA

Este trabajo es para mis padres, hermano, abuelos, y muy en especial a mi abuela Doris que no se pierde ni un segundo de mi vida.

AGRADECIMIENTOS

-A mi familia que ha estado conmigo en todo momento y ha confiado en que yo podía lograrlo.

-A mi tutor y amigo Dannis por la paciencia que ha tenido conmigo y por ser realista en las metas trazadas.

-A mi inseparable amiga Ndandou que estuvimos juntos en tantos momentos difíciles y nos ayudamos el uno al otro para salir adelante.

-A mis amigos Félix, Reinier, Miguel, Rolando y Yohani por darme ánimo y hacerme reír en los momentos difíciles.

-A Yeiniel por las horas que dedicó a perfeccionar mi trabajo y la disposición que tuvo siempre a la hora de ofrecer su ayuda incondicional.

-A Carlos, Orelvis, Marlen, Adrián y Julio César por el apoyo en el desarrollo del software.

-A mis profesores que me enseñaron a ser un profesional.

-A los trabajadores del CDICT por considerarme uno más de ellos.

-A todas aquellas personas que me rodean y me quieren.

TAREA TÉCNICA

Para la realización del presente trabajo de diploma se realizaron las siguientes actividades:

1. Realizar un estudio del estado de arte en el tema de control de medios de hardware y software en computadoras personales. Analizar y comparar los distintos software conocidos que brindan un inventario de los medios de software y hardware en las computadoras personales para poder determinar los elementos que nos pudieran facilitar la creación de un nuevo sistema.
2. Diseñar la estructura del sistema y elaborar los distintos diagramas de casos de uso y de estado.
3. Implementar la herramienta de encuesta de hardware y software diseñada.
4. Implementar la interfaz gráfica de interacción con los distintos actores del sistema.
5. Efectuar pruebas en el terreno del sistema implementado.
6. Elaborar el informe final.

Firma del Autor

Firma del Tutor

RESUMEN

El Sistema de Seguridad y Control Automatizado para Microcomputadoras en Red (SISCAM-R) es un sistema que propone el control de los medios de hardware y software de microcomputadoras ubicadas en pequeños dominios. Este es un sistema que controla automáticamente cualquier anomalía que se presente en los medios de hardware o software de una computadora personal ya sea por algún cambio de dispositivo o por su rotura, así como por la instalación de un nuevo software o desinstalación de uno existente.

En el sistema diseñado el control se establece a través de reportes emitidos en períodos de tiempos previamente establecidos donde se efectúa una comparación de las encuestas realizadas a cada computadora personal y los registros de los medios que debe disponer cada una de ellas.

Con el desarrollo de este sistema se pretende minimizar en gran medida el robo o cambio no autorizado de medios de hardware pertenecientes a las microcomputadoras del CDICT; además de otros centros que necesiten emplearlo; así como una planificación de los ciclos de mantenimiento a las estructuras de software y hardware de los distintos medios de cómputo.

El SISCAM-R se encuentra en fase de prueba para poder generalizar su funcionamiento en el CDICT y otras áreas de la UCLV que lo deseen.

INDICE

INTRODUCCIÓN

Con el aumento del número de computadoras disponibles en la Universidad y por ende la cantidad de laboratorios y locales con estos medios se hace mucho más complejo el control físico y de la utilización de estos dispositivos. Esta diversidad de medios y locales, unido al descontrol por parte de algunas autoridades, ha motivado que se hayan cometido robos de computadoras y la adulteración de componentes del hardware en otras.

A fin de evitar estos hechos se han perfeccionado los mecanismos de control y la reglamentación vigente para el control de las computadoras personales en cada área. Por ello se estableció que se recogiera en una planilla las características técnicas de cada una de las computadoras de que dispone cada entidad de la Universidad, este control se debe actualizar cada vez que se efectué alguna modificación en el medio y es responsabilidad de la administración de cada área su ejecución. Esta medida aunque significa un avance en cuanto a los controles establecidos carece de sistematicidad y objetividad toda vez que se puede efectuar una alteración en las características técnicas de alguna computadora personal y no ser detectada por los usuarios de la misma puesto que desconocen las características técnicas del medio o simplemente no es de su responsabilidad velar por este tipo de control. Por ello disponer de un medio automatizado de control permanente de la integridad física de las computadoras personales de un área es de vital importancia.

En el presente trabajo se realizó un análisis de los sistemas existentes con el objetivo de tratar el problema actual, una vez terminados estos análisis se determinó que había que crear un nuevo sistema con funcionalidades acordes al problema específico que se presenta en estas instituciones debido a que los anteriores no cuentan con todas las herramientas necesarias para el uso que se propone.

Para identificar y dar solución en un período de tiempo pequeño a las violaciones se necesita un sistema centralizado capaz de realizar encuestas a cada una de las computadoras de modo automático por tanto se propone la creación del Sistema de Seguridad y Control Automatizado para Microcomputadoras en Red (SISCAM-R) que tiene como función principal el control de los medios de *hardware* y *software* de las computadoras ubicadas en el Centro de Documentación e Información Científico Técnica (CDICT) de nuestra universidad, además debe ser adaptable a cualquier otra dependencia que requiera de su utilización.

El sistema a crear debe poseer arquitectura cliente – servidor, es decir de manera centralizada, en un servidor o computadora con los requerimientos necesarios para que funcione el servicio correctamente. El sistema debe basar su funcionamiento en un pedido de reporte a cada una de las computadoras conectadas a la red LAN del centro en cuestión. Cada PC de manera individual debe responder a la petición hecha por el sistema enviando un reporte que contiene la información relacionada con los principales dispositivos de hardware y todos los software instalados, así como las fechas de modificación o cambio de ambos. Los reportes obtenidos se almacenan en una base de datos en el servidor donde se comparan con un modelo de referencia para cada grupo de computadoras ubicadas por la función que realiza y por tipo. Se pueden obtener 3 casos diferentes de reportes. El primero es el reporte que no se puede realizar porque la máquina esta apagada o desconectada de la red, en este caso se guarda un reporte con un mensaje que indique que no se pudo realizar la tarea por alguna de las causas anteriores. El segundo caso es el reporte sin incidencias o sea un reporte que después de comparar con la referencia esta correcto, en este caso se almacena en la base de datos con un mensaje indicando que todo esta en orden. El tercero de los casos es el más crítico de todos y es cuando el reporte comparado presenta diferencias o violaciones, entonces se envía una alarma visual al personal establecido para que tome una decisión al respecto y además se almacena en la base de datos como una incidencia.

Adicionalmente el sistema debe contar con un cronograma de mantenimientos que es elaborado por el personal con autoridad para establecer estas tareas. Con esta función todos los usuarios que utilicen estas computadoras conocerán cuando se verán afectados los servicios por mantenimiento o reparación y podrán planificarse con tiempo para evitar la

menor cantidad de afectaciones posibles. El sistema esta planificado para que funcione sobre plataforma Windows. El SISCAM-R debe tener una interfaz visual donde el usuario puede autentificarse utilizando login y contraseña y accede a los servicios establecidos según su nivel de jerarquía.

Objetivo General:

Desarrollar el Sistema de Seguridad y Control Automatizado de Microcomputadoras en Red (SISCAM-R) que disponga de un control de cada estructura de hardware y software instalados en cada una de las computadoras del centro, así como disponer de un cronograma de mantenimiento e incidencias de cada una de ellas.

Objetivos Específicos:

1. Analizar los antecedentes de este tipo de software. Estudiar algunos software de gestión remota a fin de agilizar el proceso de creación basándolo en soluciones existentes.
2. Diseñar el software que se desea producir y sus funcionalidades usando los métodos propuestos en la Ingeniería de Software.
3. Implementar el Sistema de Seguridad y Control Automatizado y realizar pruebas piloto que validen su utilidad y eficiencia.

Para dar cumplimiento a estos objetivos se utilizaron como técnicas en la recolección de la información el análisis documental y la consulta a expertos.

Con el diseño, desarrollo e implementación del SISCAM-R se pretende alcanzar los siguientes resultados:

1- Centralizar el control de medios de hardware y software de las computadoras conectadas a la red informática del CDICT.

2- Minimizar en gran medida las violaciones o anomalías presentadas con respecto a estos medios.

3- Mantener informados a los usuarios del CDICT sobre la fecha en que se programan los mantenimientos o reparaciones para evitar la menor afectación posible.

Organización del Informe:

Este trabajo está estructurado en 3 capítulos. En el primer capítulo se hace una revisión bibliográfica del tema a tratar y se exponen las características de cada uno de los sistemas a los que tenemos acceso y que realizan funciones similares al que se propone. Se demuestra la necesidad de implementar un nuevo software que se adapte a los requerimientos necesarios. En el segundo capítulo se aborda todo lo relacionado con el nuevo sistema sus características, estructura, funcionalidades y diseño. Para el tercer capítulo se reservan los resultados del sistema en la fase de prueba, el análisis económico y algunos elementos que justifiquen los resultados positivos del SISCAM-R.

CAPÍTULO 1. Sistemas de Diagnóstico e Información.

1.1 Introducción

Dada la problemática de robo y violaciones a los medios de hardware y software de los distintos centros universitarios, así como los sistemas de control establecidos al efecto, se tuvo que investigar acerca de software capaces de eliminar estas desventajosas situaciones y permitir un mejor control de los medios.

En el análisis del caso se abordan varios sistemas de diagnóstico e información que presentan diferentes formas de obtención de la información sobre los medios en cuestión. En el desarrollo del capítulo se analizan y comparan las diferentes estructuras de estos sistemas, tipo de reporte, extensiones que poseen, interfaz gráfica, nivel de información obtenida sobre los dispositivos y programas instalados, etc.

1.2 Comando DxDiag de Windows.

El modo más simple de conocer los principales medios de hardware y software que usa cualquier PC con Windows 98 y Sistemas Operativos superiores es utilizando el comando DxDiag. Para utilizar el comando se realizan las siguientes operaciones:

Inicio \ Ejecutar \ dxdiag para Windows en español

Start \ Run\ dxdiag para Windows en inglés

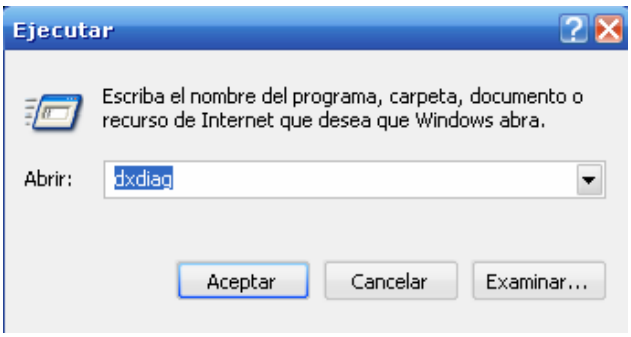

Figura 1. 1. Ejecutar / Run

Una vez realizados los pasos descritos anteriormente estamos en presencia de la manera más simple de obtener la información del hardware y software de las computadoras modernas.

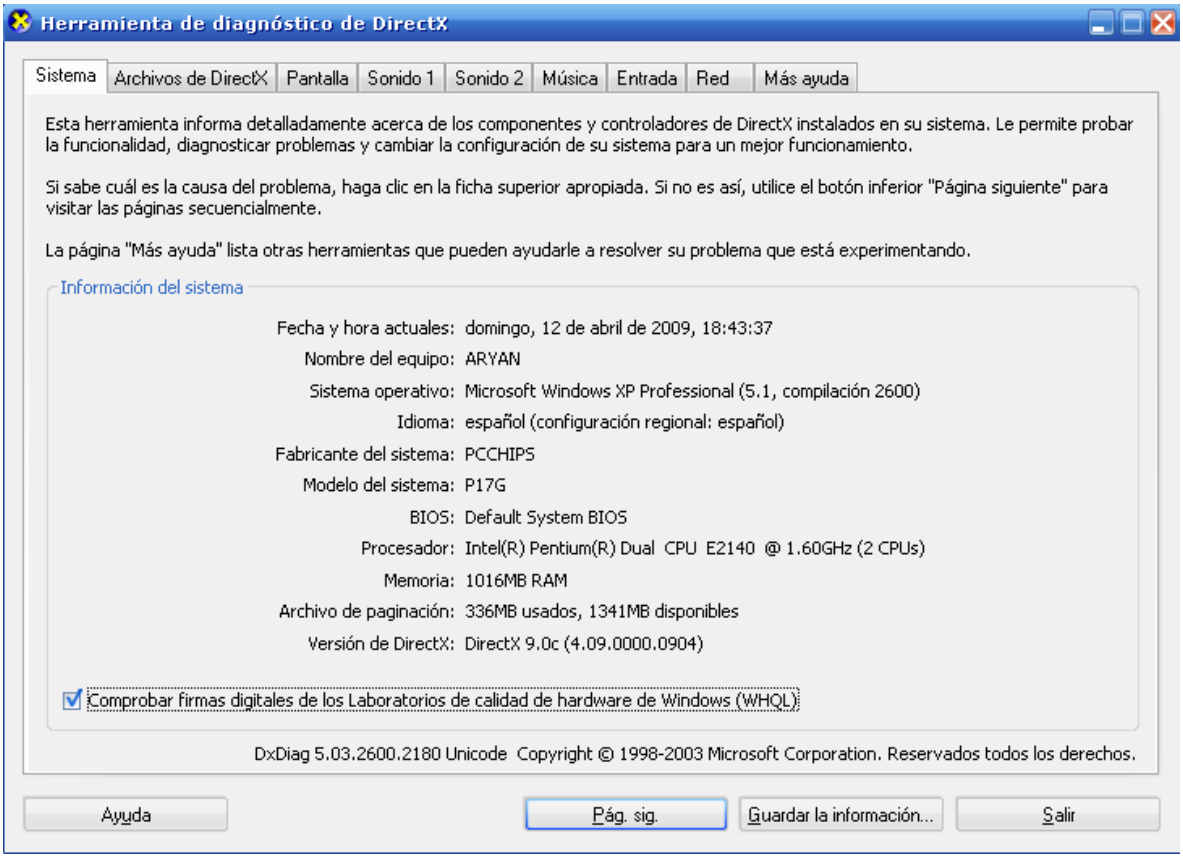

Figura 1. 2. Herramienta de Diagnostico de Direct X

Se muestra la pantalla más general que brinda el comando, de la que se obtienen las características esenciales que se desean conocer. Esta funcionalidad cuenta además con otras pestañas donde se encuentran informaciones sobre el funcionamiento de software y configuraciones para mejorar el rendimiento de nuestra computadora. También se encuentran

más detalles sobre hardware y ayudas para realizar los cambios correctamente. Esta herramienta básica permite además realizar un reporte en modo texto que constituye un elemento primordial en este trabajo. Una vez conocida la información se necesita almacenarla para tener constancia de los medios y en caso de anomalías comparar lo que se tenía anteriormente y lo que se tiene ahora y en base a esto tomar decisiones para resolver el problema presentado. (Corporation, 2007).

1.3 Sistemas de Diagnóstico e Información Anteriores.

Fue necesario avanzar en el modo de conocer la información y diagnóstico de hardware y software. A nivel mundial se dieron a la tarea de desarrollar herramientas mucho más complejas para lograr el fin perseguido. Algunas empresas o corporaciones como es natural privatizaron sus productos, otras las pusieron a disposición de la comunidad informática. Lo cierto es que en Cuba ya sea por cualquiera de estas vías o por otras no mencionadas se dispone de manera general de algunas de estas herramientas.

1.3.1 AIDA32.

La primera de estas herramientas de diagnóstico es el AIDA 32 o como se le conoce comúnmente AIDA.

Generación de Informes con Aida32

Aida32 es un programa de auditoría muy completo. Permite obtener información de un equipo muy variada: dispositivos de hardware conectados a la placa base(motherboard), sistema operativo, parámetros del servidor, características del monitor, dispositivos de almacenamiento, información de las DirectX(conjunto de componentes [DirectDraw, Direct3D, DirectSound, DirectPlay y DirectInput] creado por la compañía Microsoft para la obtención del mayor rendimiento por parte de los dispositivos gráficos, ejemplo las tarjetas gráficas.), programas instalados, información de la red, parámetros varios de configuración y una comparativa de la memoria. (Lancharro, 2003)

Toda esta información se puede mostrar en diversos informes. Aida32 permite generar informes con toda o parte de la información y mostrarlos de diferente forma. Los formatos de salida son los siguientes:

Texto simple: Txt.

HTML: HyperText Markup Language (*Lenguaje de Marcas de Hipertexto*).

MHTML: [Mime HTML] Multipurpose Internet Mail Extension HyperText Markup Language (Protocolo de Transferencia de Hipertexto Multiuso de la Extensión del Correo del Internet).

XML: Extensible Markup Language (Lenguaje de Marcas Extensible).

CSV: Comma-Separated Values.

MIF: MapInfo Data Interchange file.

INI: Ésta es una extensión de archivo para denotar ficheros de configuración utilizados por aplicaciones de los sistemas operativos Windows.

ADO: **ActiveX Data Objects** (Es uno de los mecanismos que usan los programas de computadoras para comunicarse con las bases de datos, darles órdenes y obtener resultados de ellas.

Especialmente interesante es el formato ADO. Eligiendo y configurando en las preferencias esa opción se pueden insertar los resultados del informe en una base de datos. Si en un futuro se quieren ampliar los informes del programa con estadísticas que no están se puede hacer estudiando la información que hay en la base de datos. Entre las bases de datos con las que trabaja está Access, Oracle, SQL Server y MySQL, cuyas estructuras vienen incluidas con Aida32. (Cotarelo, 2004)

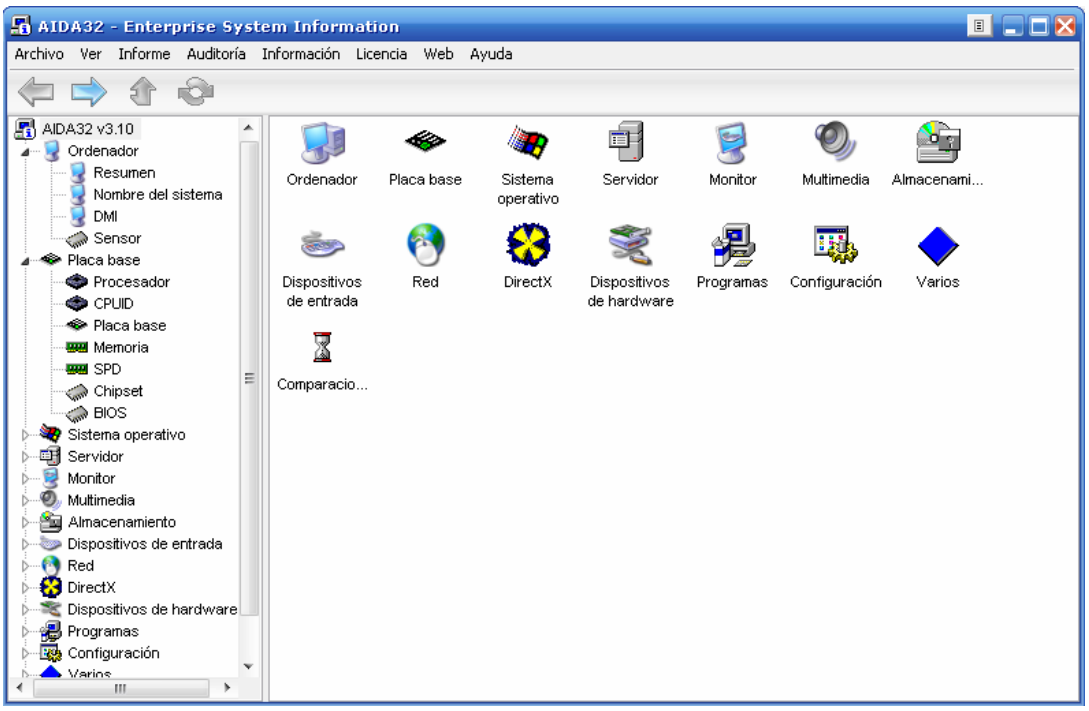

Figura 1. 3. Herramienta de Diagnóstico e Información AIDA32

1.3.2 SiSoftware SANDRA.

La segunda de las herramientas es el SiSoftware-Sandra (nombre completo del software) o simplemente Sandra como se conoce comúnmente. Este programa combina, a partes iguales, el análisis exhaustivo del sistema operativo con las herramientas más útiles para el mantenimiento del ordenador y el software de los dispositivos asociados.

Las cualidades de SiSoftware Sandra se dejan ver desde que se ejecuta el programa, su interfaz gráfica, elaborada y dividida en categorías, así como la gran cantidad de asistentes que incorpora, hacen de este programa una de las mejores opciones para el diagnóstico e información.

La detección de dispositivos asociados es fiable, aunque un tanto lenta en algunas ocasiones. Si el dispositivo de hardware más reciente, no es localizado con exactitud, siempre se puede recurrir a la actualización automática del programa y sus bases de datos.

Una de sus mejores cualidades es la cantidad de pruebas de rendimiento que incorpora, lo que permite comparar los resultados de este sistema con otros de características parecidas. Además,

también ayuda a resolver pequeños problemas de rendimiento que se puedan presentar. (TOOGLE, 2009)

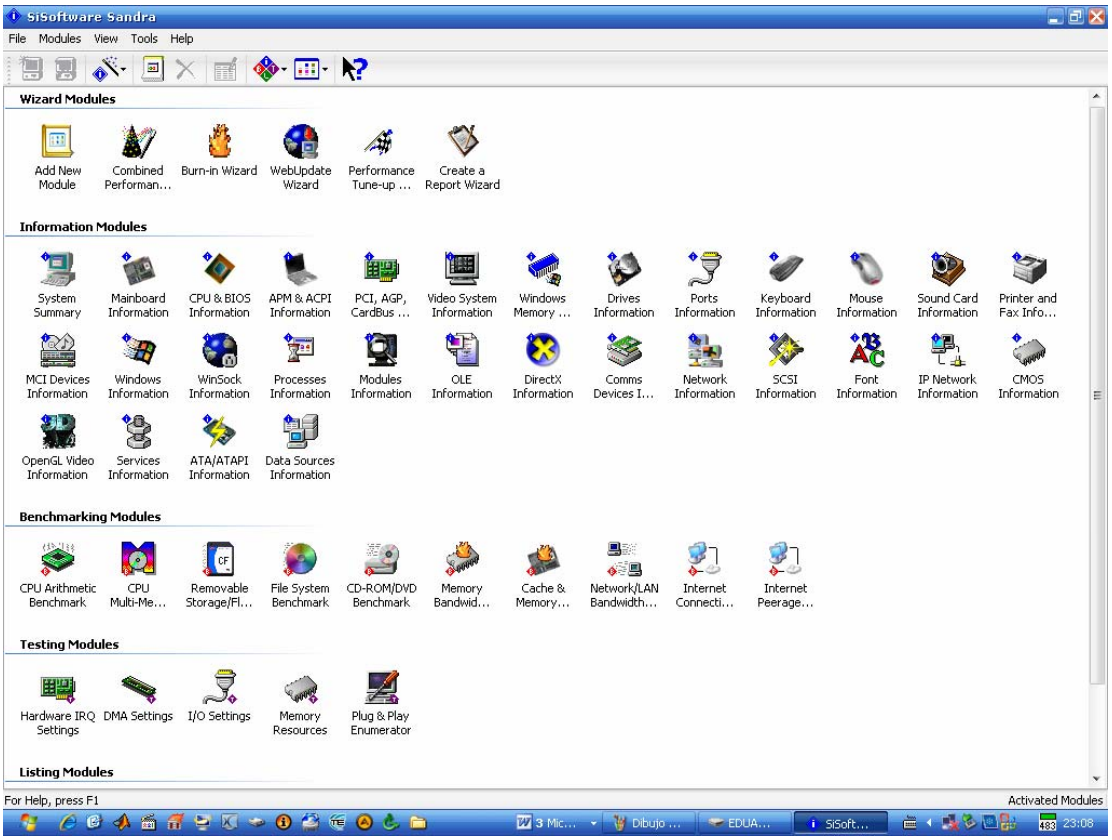

Figura 1. 4. Herramienta de Diagnóstico e Información SiSoftware SANDRA

1.3.3 EVEREST ULTIMATE EDITION

Everest Ultimate Edition tiene como antecedente a los programas de dominio público *ASMDemo for DOS*, *AIDA16* y por último *AIDA32* (compatible con Windows), creado por el húngaro *Tamás Miklós* en el año 1995. EVEREST Ultimate Edition es un sistema líder de la industria de diagnóstico y en la evaluación comparativa como solución para los usuarios de PC, basado en tecnología EVEREST. (Corporate, 2009)

El Everest Ultimate Edition brinda información sobre los siguientes elementos de una computadora personal:

Periféricos. Dispositivos de Hardware conectados al PC.

Procesador (marca, creador, modelo.)

Sistema Operativo.

Memoria.

Procesos activos.

Configuración de red local.

Temperatura.

Gestión de energía.

Tipo de placa base.

Monitor.

Servidores.

Multimedia.

Y otros dispositivos.

El EVEREST es muy popular en la actualidad pues a diferencia de sus antecesores tiene características que permiten una notable mejoría tales como:

Trabajo por pestañas.

La interfaz del programa se encuentra divida en dos pestañas diferentes. Por un lado “Favoritos” y por otro “Menú”. Dentro de cada una de ellas se localizan diferentes opciones. En la de “Menú” se puede visualizar toda la información acerca de los análisis. Y en “Favoritos” se agregan diferentes opciones a las que se recurran con cierta periodicidad.

Sencilla metodología de trabajo.

La metodología de trabajo que ofrece la aplicación es muy sencilla. El análisis se realiza de manera automática cuando se inicia la utilidad. Una vez que se ingresa al programa, todos los datos se encuentran a disposición del usuario.

Informes detallados.

Todos los informes que ofrece la herramienta están claramente detallados. Dependiendo del tipo de consultas y los datos que requieran serán los resultados que se podrán observar. El software cuenta con un asistente de informes.

Barra de ayuda.

Dentro del programa, el usuario se encontrará con una barra que le da la posibilidad de ingresar a diferentes clases de ayuda. En la misma en encuentran opciones que permiten contactarse con soporte en línea, y encontrar información del programa.

Visualización de Datos.

A la hora de ver datos, el usuario podrá hacerlo de una manera totalmente sencilla y cómoda, ya que el programa ofrece una visualización similar a la que se puede disfrutar en el explorador de Windows.

Sistema de comparaciones.

Everest Ultimate Edition cuenta con un sistema de comparaciones que otorgan la posibilidad de contrastar diferentes aspectos de funcionamiento, lo que acarrea como resultado la obtención de mejores resultados en todos los aspectos.

Detalle de configuraciones.

En esta opción se pueden localizar todas las configuraciones que se utilizan en el ordenador. A diferencia de otras aplicaciones, en ésta se puede observar detalladamente algunos datos importantes en caso de desear su modificación.

Las pruebas que realiza el EVEREST se hacen específicamente en los sectores de: memoria, discos duros, unidades de almacenamiento, seguridad, dispositivos de hardware, red local y DirectX. Los resultados de las mismas, se podrán observar claramente organizados en una estructura de árbol.

También es posible generar logs e informes a partir de la información que interese, exportando un documento *.txt o *.HTML. Además el programa incluye enlaces Web para expandir los datos obtenidos y, en algunos casos, descargar los últimos controladores requeridos.

En la actualidad, Everest Ultimate Edition continúa estando a la vanguardia de los programas dedicados a la medición, reconocimiento y optimización de ordenadores, siendo un líder de su categoría y esto lo demuestra el gran número de usuarios que lo emplean para el reconocimiento de dispositivos de hardware y software. (Corporate, 2009)

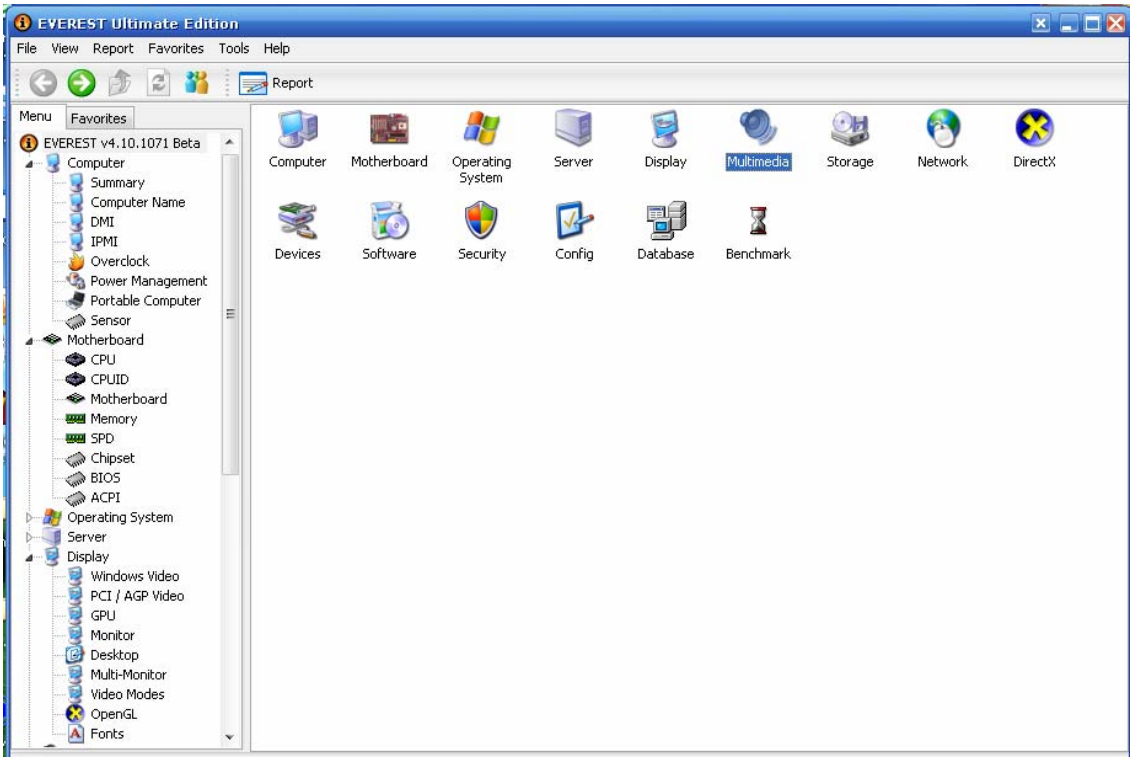

Figura 1. 5. Herramienta de Diagnóstico e Información Everest Ultimate Edition

Figura 1. 6. Datos del Everest que se muestran fuera de la ventana estándar.

Condiciones que debe reunir una computadora para el empleo del Everest Ultimate Edition

Requerimientos Mínimos

Procesador: 1.3 GHz.

Memoria RAM: 128 MB.

Tarjeta Gráfica: 64 MB RAM.

Espacio Libre en el Ordenador: 10 MB.

Sistema operativo: Windows 90/ME/2000/XP/Vista/7.

Requerimientos Recomendados

Procesador: 2.4 GHz o superior.

Memoria RAM: 512 MB o superior.

Tarjeta Gráfica: 128 MB RAM o superior.

Espacio Libre en el Ordenador: 115 MB o superior.

Sistema operativo: Windows 98/ME/2000/XP/Vista/7.

Tabla de Versiones del software(Corporate, 2009).

Versión	***Fecha de Lanzamiento***	***Aporte destacado***
Everest Ultimate Edition 3.5	19 de octubre de 2006	Soporte para tecnología de 2 y 4 procesadores de Intel Core 2.

Everest Ultimate Edition 4.0	5 de abril de 2007	Aplicación para barra lateral de Windows Vista, soporte para OpenGL.
Everest Ultimate Edition 4.2	10 de octubre de 2007	Soporta PCI Express 2.0. Nuevo método de medición.
Everest Ultimate Edition 4.5	20 de marzo de 2008	Soporta hasta 6 microprocesadores.
Everest Ultimate Edition 4.6	6 de septiembre de 2008	Soporte mejorado para OpenGL 3 y procesadores Intel Centrino y AMD Xeon. .
Everest Ultimate Edition 5.0	5 de febrero de 2009.	Soporta OpenGL 3.0, Windows 7 y nuevo módulo de alertas.

1.3.4 DAMEWARE

El Dameware es otra de las herramientas que permite tener reportes de las computadoras conectadas a la red además de otras funcionalidades de control tales como visualización de las PC conectadas en ese momento, acceso remoto y control de IP. (International, 2009).

Esta herramienta solo se menciona porque sus funcionalidades están orientadas al control de las computadoras estándares y servidores en la red. Es utilizada generalmente por administradores para diagnósticos en dominios.

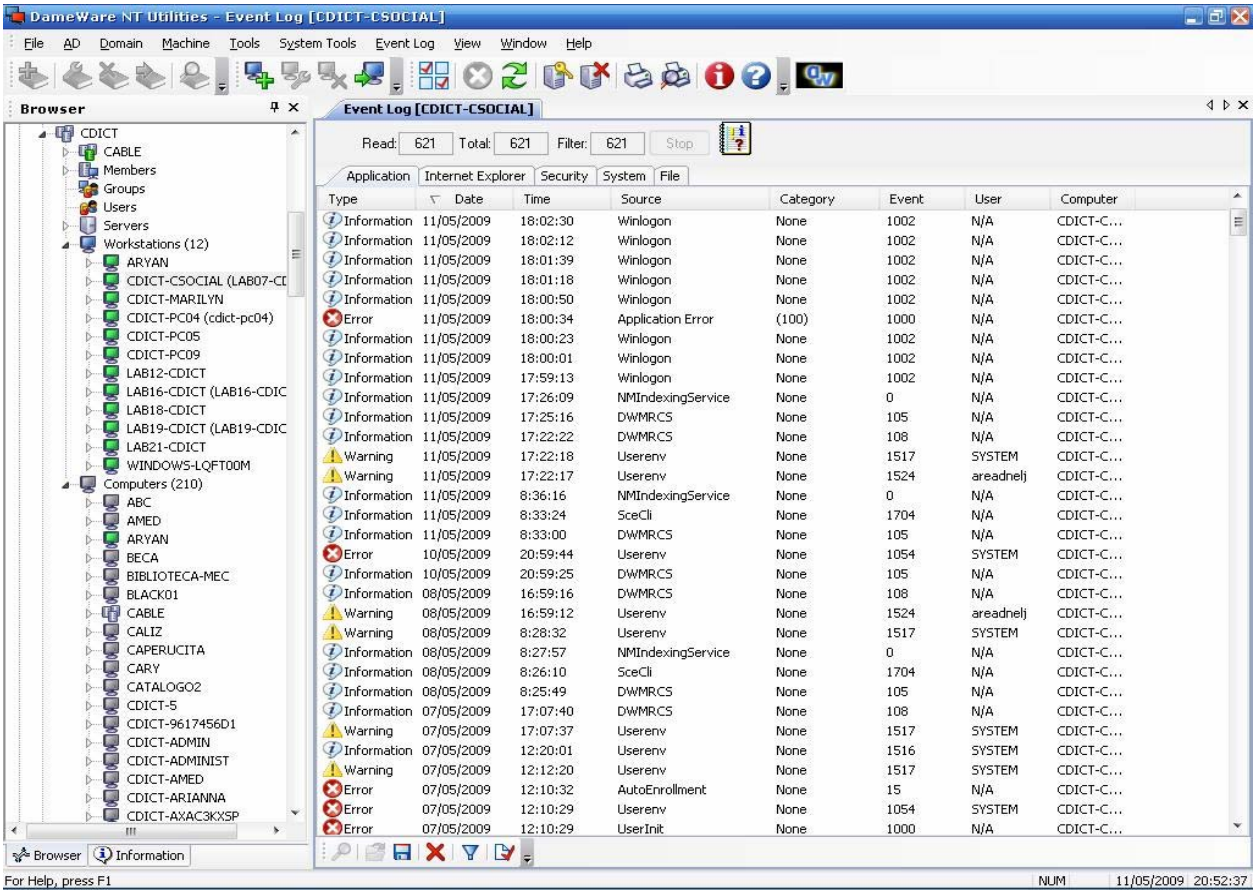

Figura 1. 7. Herramienta de Información y Control Dameware.

1.3.5 Dr. Hardware

Este software ha ganado popularidad en los últimos tiempos y cada vez más usuarios lo utilizan ya que posee mucho más actualizadas las funciones para nombrar los componentes de las computadoras y los tipos de software que estas tengan. Por otra parte ya con esta herramienta se permite hacer un test a los componentes de la PC y en breve período de tiempo se obtienen las

características reales del equipo y las compara con otras que almacena por defecto. También se puede realizar los reportes ya conocidos. El Dr. Hardware puede ejecutarse en los sistemas operativos Windows 95, 98, Me, NT4, 2000, 2003, XP y Vista tanto en 32 como en 64 bit. (Gebhard, 2009)

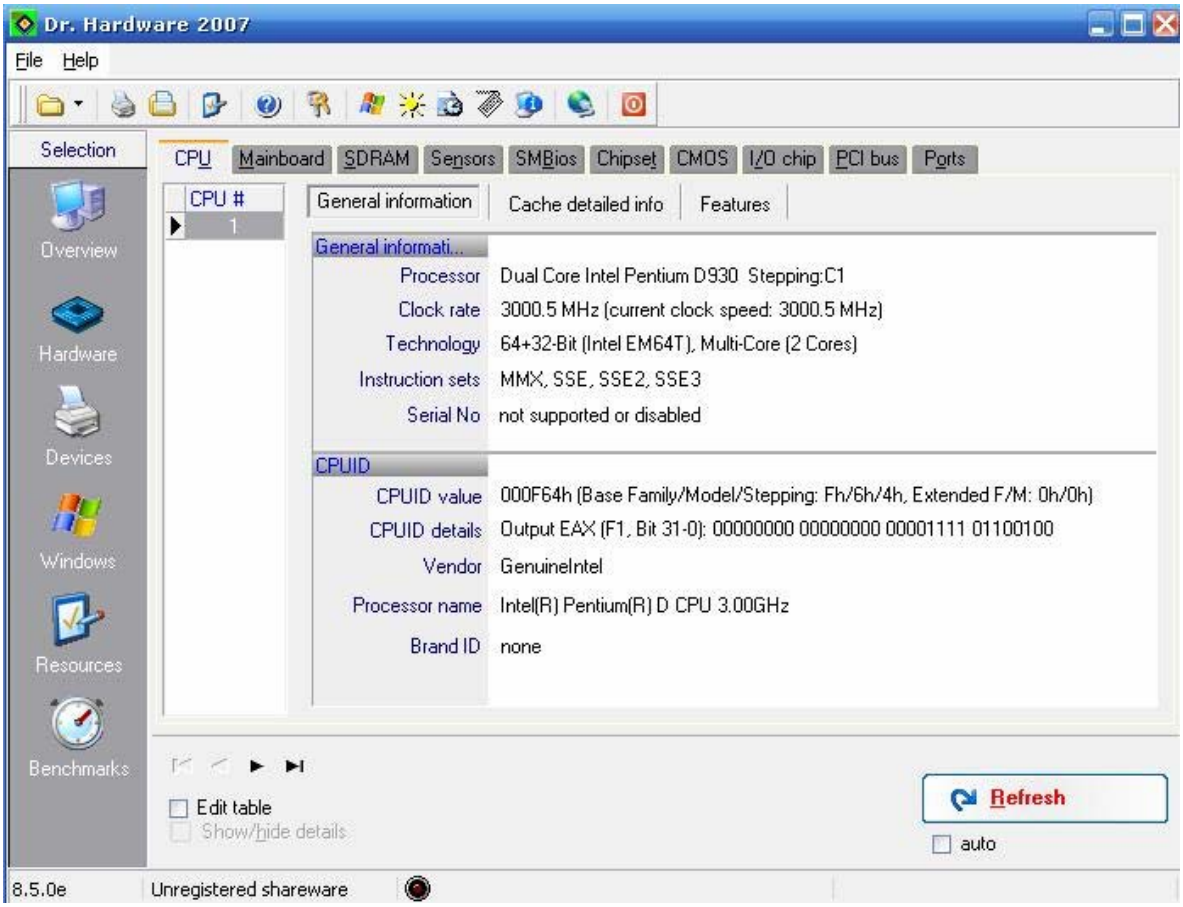

Figura 1. 8. Herramienta de Diagnóstico e Información Dr. Hardware 2007.

1.3.6 Sistema de Inventario Periódico de Hardware (SIPH)

Este sistema fue desarrollado en el 2008 en el CDICT con el apoyo de estudiantes del grupo CHASQUI y fue el primer paso para lograr controlar los dispositivos de hardware. El SIPH estuvo en un período de pruebas y se decidió no utilizarlo definitivamente y tomar los elementos que este posee para establecer las bases del nuevo sistema SISCAM-R. (Vera, Morera, Hernández, López, 2009)

Estructura del SIPH:

1- Obtención de las propiedades de hardware del (SIPH)

2- Generación del archivo

3- Salvar el inventario

4- La Aplicación Web

5- Tecnologías utilizadas

6- Interfaz Gráfica

1-Obtención de las propiedades de hardware del (SIPH)

Monitor: Fabricante y tamaño en pulgadas de la pantalla.

Procesador: Tipo y velocidad.

Discos duros: Cantidad presente y capacidad en Gigabytes de cada uno.

CD-ROM: Cantidad presente y tipo de cada uno.

Memoria RAM: Cantidad presente y capacidad de cada una en Megabytes.

2-Generación del archivo

Los resultados del inventario se guardan en un archivo con formato XML.

3-Salvar el inventario

Se establece el camino en que se desea guardar el reporte, se crea una carpeta cuyo nombre será la fecha del día presente y dentro de esta se guarda el fichero XML cuyo nombre será el nombre completo de la máquina en la red.

Ejemplo, \\10.12.36.101\reportes

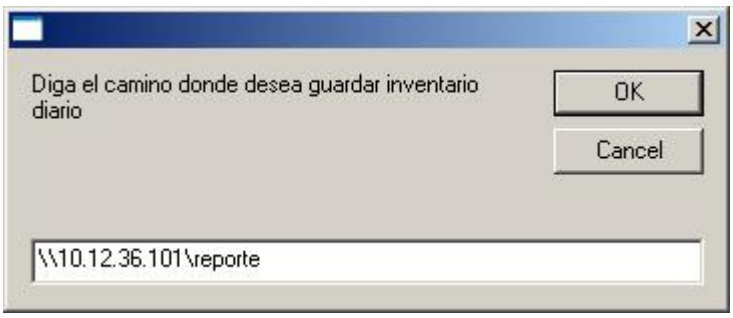

Figura 1. 9. Reportes del SIPH.

Luego en esta carpeta compartida se creará la carpeta, por ejemplo, 12-08-2009 y dentro de esta carpeta se crea el archivo:

LAB16-CDICT.CDICT.uclv.edu.cu.xml

Y así se obtienen los datos que se necesitan de la máquina en cuestión guardada en la carpeta.

4- La Aplicación Web

El Sistema de Inventario Periódico de Hardware, es una aplicación Web, la cual necesita para su correcto funcionamiento un servidor Web apache, con PHP instalado, así como el sistema de gestión de bases de datos MySQL para el manejo de la base de datos.

La estructura de la base de datos usada por el sistema es la siguiente:

Tabla PC: En esta tabla se almacenan las distintas computadoras de la red. Se colocó un *Id (idetificador)* para cada PC como llave primaria para evitar contradicciones cuando se cambie el nombre o el IP de una máquina. En el campo *name* se guarda el nombre de la máquina, en el campo IP el IP, en el campo *is_functional* se guarda si la máquina esta funcionando para contemplarla o no en el reporte y en el campo *xml_descript_path* se guarda el camino donde esta guardado el archivo XML que contiene el inventario.

	Campo	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado	Extra
☐	pc_id	int(11)			No		auto_increment
☐	pc_name	varchar(255)	utf8_unicode_ci		No		
☐	pc_ip	varchar(15)	utf8_unicode_ci		No		
☐	pc_is_functional	tinyint(1)			No		
☐	pc_xml_descrip_path	varchar(255)	utf8_unicode_ci		No		

Figura 1. 10. Tabla PC.

Tabla Report: En esta tabla se guardan los reportes. En el campo *id* se guarda el ID del reporte, en el campo *pc_id* se guarda el IP de la máquina que generó el reporte, en el campo *date* se guarda la fecha de cuando se generó el reporte y en el campo *xml_descript_path* se guarda el camino donde esta guardado el archivo XML que contiene el inventario.

El sitio mantiene un control de los reportes de la siguiente forma:

	Campo	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado	Extra
☐	rep_id	int(11)			No		auto_increment
☐	pc_id	int(11)			No		
☐	rep_date	varchar(255)	utf8_unicode_ci		No		
☐	rep_xml_descrip_path	varchar(1000)	utf8_unicode_ci		Sí	*NULL*	

Figura 1. 11. Tabla Report.

En el interior de una carpeta nombrada DATA se almacenan otras diferentes y cada una con el estándar de las máquinas de manera individual *(std*), el inventario diario de cada máquina *(daily*) en carpetas por día y los reportes por día (report) si es que la máquina tuvo una ocurrencia de reporte.

El sitio se encarga de generar los reportes analizando el estándar de cada máquina y los inventarios diarios asociados, si existe el inventario diario se verifica que la máquina esté funcional y si es así busca las diferencias para crear un reporte y agregarlo a la base de datos. Si no se encontró el inventario diario de la máquina igualmente se crea un reporte indicando que no se realizó el inventario diario de la máquina en cuestión.

5- Tecnologías utilizadas

Para el proceso de encuesta a la base de datos, se creó una capa de datos usando PHP, basada en Data Access Component *(DAC)*, la cual logra un grado de abstracción, que permite encuestar la base de datos de una forma de más fácil comprensión, además muestra facilidades para realizar transacciones con la posibilidad de deshacerlas posteriormente si se hace necesario, y para manipular resultados paginados, lo cual facilita el trabajo cuando las consultas a las base de datos devuelven estructuras relativamente grandes.

6-Interfaz Gráfica

Se usó para la puesta a punto de la interfaz gráfica, el software certificado Macromedia Dreamweaver para el desarrollo de las plantillas *(.html)*, las cuales son utilizadas por los scripts para generar el contenido de la página en tiempo de ejecución. Este proceso se realiza por medio de una clase *Template*, la cual permite registrar variables específicas en las diferentes plantillas de forma sencilla y rápida. (Vera, Morera, Hernández, López, 2009)

Figura 1. 12. Interfaz Gráfica del SIPH.

1.4 Ventajas y Limitaciones de los distintos sistemas analizados

Ventajas

a) Con el comando DxDiag no es necesario disponer de ningún software adicional para conocer las principales características de cada PC.

b) Con el AIDA, SANDRA y EVEREST se puede obtener un volumen de información grande acerca de hardware y software instalados en cada PC.

c) El AIDA permite realizar auditorias a PC en red de manera automática.

d) El EVEREST utiliza métodos para el reconocimiento de hardware y software muy efectivos.

e) Dameware es una poderosa herramienta de control e información que también permite realizar reportes sobre dispositivos de hardware y software.

f) Dr.Hardware se propone como la herramienta de diagnóstico e información con los datos más actualizados y con la novedad de poder realizar test a los dispositivos en breve período de tiempo. Posee además la capacidad de realizar reportes.

g) El Sistema de Inventario Periódico de Hardware (SIPH) es el sistema más parecido al que se necesita actualmente. A diferencia de los anteriores este puede almacenar el reporte en una carpeta determinada y delimitar los dispositivos de hardware por grupos funcionales.

Limitaciones

a) Todos necesitan tener instalados el software de diagnóstico e información en la computadora (cliente) a encuestar para poder realizar los reportes.

b) La mayoría realiza reportes automáticamente considerando aspectos establecidos por un administrador del sistema o un usuario determinado.

c) Ninguno toma decisiones en caso de ausencia o cambio sin autorización de hardware o software.

d) Ninguno ofrece una planificación de las tareas a realizar en un tiempo establecido por administradores y usuarios.

e) La mayoría tienen propietarios y licencias que pagar.

Una vez analizados los sistemas anteriores en cuanto al nivel de información sobre dispositivos de hardware, interfaces gráficas, formatos de reportes, tipos de extensiones, información actualizada y encuestas programadas, se concluye que ninguno de ellos se ajusta a los requerimientos necesarios por lo que se decide crear un nuevo sistema que cumpla con estos. Se debe resaltar que no se hizo énfasis en la comunicación que emplean estos sistemas dado que se pretende usar otra filosofía de trabajo donde los clientes realicen el menor número de operaciones y así evitar sobrecargarlo para no comprometer el correcto funcionamiento del sistema a emplearse por tener un cliente fuera de servicio.

CAPÍTULO 2. Sistema de Seguridad y Control Automatizado para Microcomputadoras en Red (SISCAM-R)

2.1 Introducción

El Sistema de Seguridad y Control Automatizado de Microcomputadoras en Red (SISCAM-R) surge por la necesidad de reunir en un solo sistema, de manera automática, el control de los medios de hardware y software de las computadoras del Centro de Documentación e Información Científico Técnica (CDICT) y de esta forma perfeccionar los mecanismos de control establecidos al efecto.

En este capítulo se abordarán aspectos que describen la estructura completa del sistema, una descripción general de su composición, modelado de las estructuras en UML, herramientas que se utilizaron para el desarrollo, esquemas para la comprensión y posterior desarrollo del código del software, infraestructura, aspecto visual, arquitecturas utilizadas y por último la implementación de la infraestructura. Con el desarrollo de estos elementos se crea el sistema que se necesita para solucionar la problemática fundamental de este trabajo.

2.2 Descripción general

El SISCAM-R es un sistema que esta orientado a las dos estructuras de una computadora:

Hardware:

Permite conocer las principales características de los dispositivos de una PC, motherboard, HDD, RAM, monitor, teclado, mouse, tarjeta de red, lectores \ quemadores CD-DVD.

Software:

Permite conocer los software que están instalados en cada una de las PC, fecha de instalación o modificación de los mismos.

Además se le agregan dos funciones que resultan novedosas en el sistema.

Cronograma:

Permite conocer la fecha dispuesta para mantenimientos y reparaciones de software y hardware en cada grupo de computadoras.

Monitoreo y Reporte:

Permite realizar avisos ante cualquier actividad o violación que se realice con los medios anteriores.

2.3 Modelado del SISCAM-R

En la modelación de este sistema se utilizó el Lenguaje Unificado de Modelado (UML) del inglés ***U****nified* ***M****odeling* ***L****anguage*. El proceso unificado es un proceso de desarrollo de software o sea es el conjunto de actividades necesarias para transformar los requisitos de un usuario en un software, sin embargo el proceso unificado es más que un simple proceso; es un marco de trabajo genérico que puede especializarse para una gran variedad de sistemas, para diferentes áreas de aplicación, tipos de organizaciones, diferentes niveles de aptitud y tamaños de proyectos. El proceso unificado esta formado por componentes interconectados a través de interfaces bien definidas. Con esta herramienta se persigue definir y documentar las funciones del sistema ya que UML se ha convertido en un estándar a nivel mundial por estar dirigido por casos de uso, estar centrado en la arquitectura y ser iterativo e incremental.

El modelo esta basado en las relaciones entre actores y casos de uso, elementos que facilitan la implementación de las funcionalidades del SISCAM –R por lo que garantiza un fácil desarrollo del software. (RUMBAUGH, 2000)

2.3.1 Herramienta Utilizada

Como herramienta para el desarrollo de este sistema se utilizó el ***VISUAL PARADIGM for UML Enterprise Edition,*** **versión 6.0 (2007).**

Esta herramienta presenta ventajas que facilitan considerablemente el desarrollo de cualquier aplicación tales como:

- Un lenguaje gráfico que permite entender rápidamente lo que se quiere y por tanto reduce el tiempo de desarrollo de la aplicación.
- Posee una amplia simbología que permiten definir funcionalidades de manera muy particular incluso cuando la función a realizar sea muy semejante a otra.
- Una vez desarrollado el esquema de las funciones de la aplicación el Visual Paradigm es capaz de generar el código básico en varios lenguajes de programación.
- Los propietarios del software continúan desarrollando aplicaciones para su mejoramiento.

Aunque existen otras herramientas para acometer este trabajo se decidió usar esta herramienta por las anteriores razones ya que nos permite realizar este propósito en menor tiempo y con una calidad superior.

2.3.2 Diagramas de casos de uso del sistema.

En la Fig. 2.1 se muestran los actores y diagramas de casos de uso del SISCAM-R de manera general así como las interacciones o relaciones entre cada uno de ellos. Los casos particulares se abordaran en epígrafes posteriores.

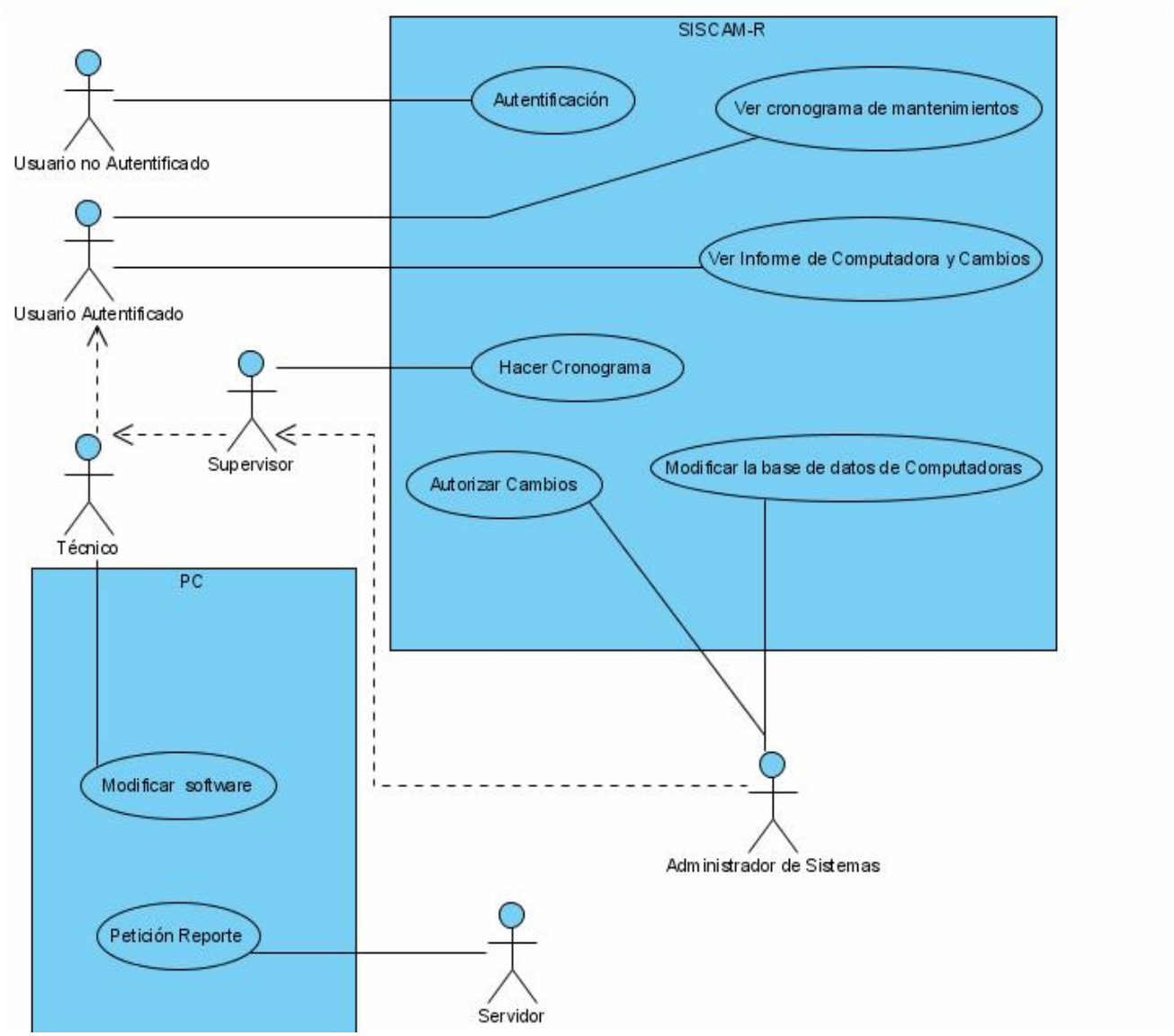

Figura 2. 1. Casos de Uso Generales del Sistema

2.3.3 Actores

El sistema cuenta con seis actores, uno es un medio de hardware y cinco son personas que interactúan de manera directa con el SISCAM-R. A continuación se describen cada uno de ellos con sus respectivas funciones.

Usuario no autentificado:

-Se encuentra en espera de autentificarse.

Usuario autentificado:

- Tiene acceso a ver dispositivos de software y hardware además de los cambios en caso de que se hayan realizado.
- Tiene acceso a ver el cronograma de mantenimiento de software y hardware.

Técnico:

- Hereda los permisos del actor anterior.
- Tiene como responsabilidad la instalación, reparación o eliminación de los software de las computadoras siguiendo el cronograma establecido por el supervisor.

Supervisor:

- Hereda los permisos del actor anterior.
- Tiene como responsabilidad la elaboración del cronograma de mantenimiento de software y hardware.

Administrador de Sistema:

- Hereda los permisos del actor anterior.
- Autoriza los cambios de hardware o software.
- Puede modificar la base de datos de las computadoras.

PC Servidor:

- Hace peticiones de reportes a cada una de las PC conectadas a la red dentro del dominio CDICT.

2.3.4 Casos de uso generales

Autentificación:

La *autentificación* en un caso de uso general que contiene a la *autorización*

Para autentificarse se colocan las credenciales en el lugar destinado para este fin y se ingresa, entonces el sistema compara las credenciales para comprobar que el usuario es válido y

posteriormente pasa a la *autorización* que es donde se define el tipo de usuario y se le otorgan los permisos correspondientes para interactuar con el sistema.

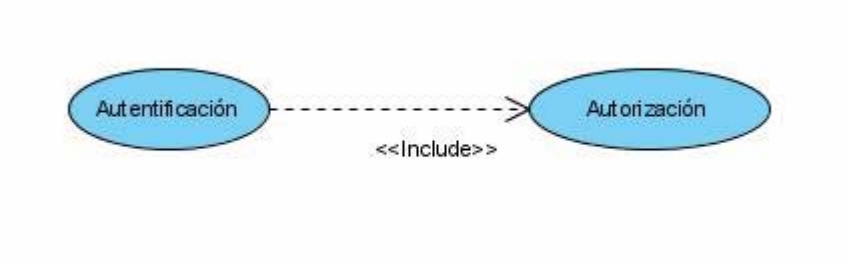

Figura 2. 2. Casos de Uso de la Autentificación.

El usuario autentificado solicita ver el cronograma de mantenimientos y además puede seleccionar la forma en que lo quiere ver ya sea general (incluye todas las computadoras del lugar) o por computadoras (solo muestra el cronograma asignado a una computadora en específico).

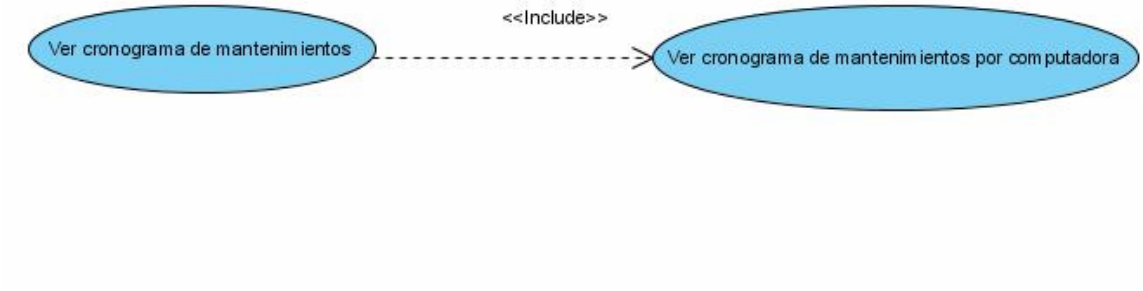

Figura 2. 3. Casos de Uso del Cronograma.

Informe de Computadoras y Cambios:

Los informes y cambios de las computadoras se pueden seleccionar de 2 formas sea general (incluye todas las computadoras del lugar) o por computadoras (solo muestra el cronograma asignado a una computadora en específico).

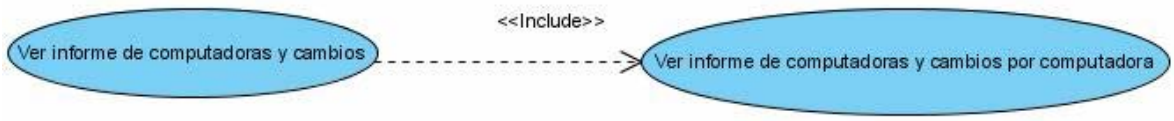

Figura 2. 4. Casos de Uso de Informes y Cambios

Modificar Base de Datos:

La base de datos del sistema se modifica por bloques donde cada uno corresponde a una de las computadoras que conforma la red que abarca el SISCAM-R.

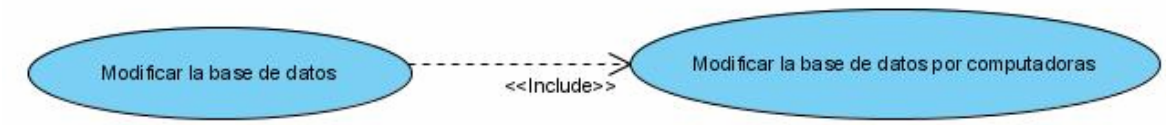

Figura 2. 5. Casos de Uso Modificación de la Base de Datos

2.3.5 Diagrama de Clases

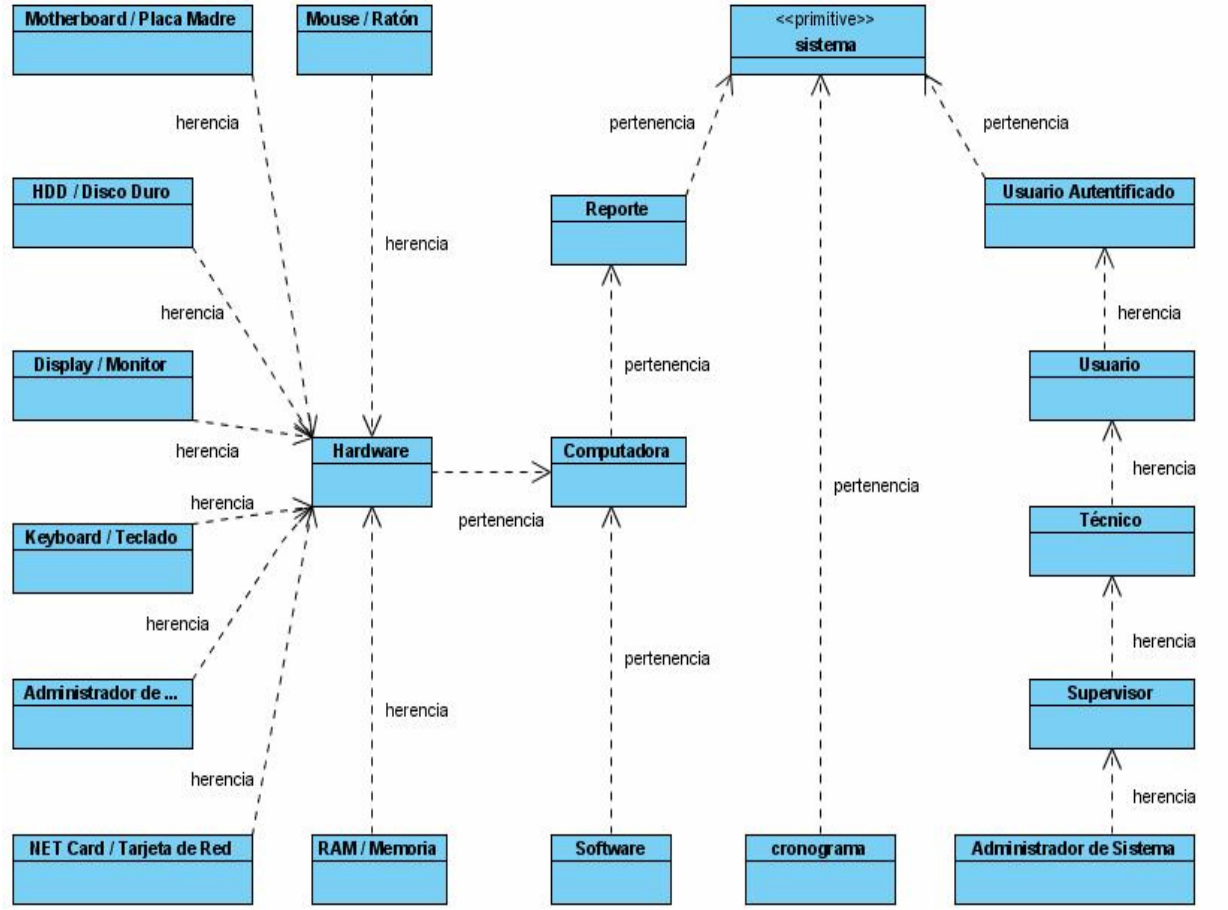

Figura 2. 6. Clases del SISCAM-R

2.4 Infraestructura y aspectos generales de la aplicación

Para el desarrollo de la infraestructura del sistema se analizó cada caso (interfaz visual, reportes, cronograma, base de datos, dispositivos de hardware, software, etc.) de modo muy particular y detallado tratando de obtener el mayor provecho de cada estructura y hacerla de fácil uso tanto para administradores como para usuarios estándares. Además la política de trabajo siempre estuvo encaminada a resolver el problema del control de los medios de hardware y software de nuestra universidad siguiendo los lineamientos planteados en REGLAMENTO DE SEGURIDAD PARA LAS TECNOLOGÍAS DE LA INFORMACIÓN (ver Anexo 1).

A continuación se explican las estructuras, herramientas y estrategias que se utilizaron en el desarrollo del sistema.

2.4.1 Interfaz de usuario y aspecto visual.

Para el diseño gráfico de logotipos e imágenes se utilizó el paquete Macromedia Dreamweaver 8.

Cuando se accede al sitio aparecen estructuras tales como logotipos de presentación del sistema y del centro propietario y un corto mensaje de bienvenida a los usuarios que realizan la visita. En la parte izquierda se encuentra el módulo de autentificación para poder acceder a las demás informaciones y funcionalidades del sitio.

Figura 2.7 Sitio Web del SISCAM-R (Inicio)

Una vez realizada la autentificación se puede acceder a la información contenida en las restantes pestañas según el nivel de privilegios del usuario autentificado, dicho de otra manera según el nivel de privilegios del usuario autentificado es el tipo de información que se presenta en las restantes pestañas.

Figura 2.8 Sitio Web del SISCAM-R (Informaciones)

2.4.2 Estructuras utilizadas

La primera de las estructuras es el sitio Web, desarrollado en PHP, que usa como principal protocolo para la comunicación HTTP. El sitio permite autentificarnos para otorgar los diferentes privilegios con que se puede operar el sistema, se presenta además la información y por último el acceso a la base de datos donde se puede obtener o escribir los datos necesarios para el funcionamiento del SISCAM-R.

El segundo elemento que conforma al sistema es la base de datos. Esta se encuentra estructurada por entidades y cada entidad tiene atributos según la función específica que realiza.

¿Cómo se justifica cada identidad empleada en la base de datos?

La entidad principal es el *reporte* que es lo que entrega el sistema y existe uno para cada *computadora* la que a su vez tiene *hardware* y *software* pero además cada medio de *hardware* es de un tipo diferente y por eso se definen *display, hdd, keyboard, motherboard, tred, RAM, mouse*. Además con el sistema interactúan usuarios (*user*) y cada uno de ellos realiza un rol determinado *user_role* y *role*.

¿Qué elementos forman a cada una de las identidades?

reporte: repid(reporte), repdate(fecha), represult(resultado) , uid(usuario), pcid(computadora)

computadora: pcid(computadora), pcmac(mac), pcip(ip) , pcname(nombre)

hardware: hid(hardware), pcid(pc), htype(tipo)

software: softid(software), pcid(computadora), softname(nombre), softversion(version)

display:displayid(monitor), dname(nombre), dmodel(modelol, dtype(tipo), hid(hardware)

hdd: hddid(disco duro), hdtype(tipo), hdmark(marca), hdcapacity(capacidad), hid(hardware)

keyboard: keybid(teclado), kname(nombre), ktype(tipo), hid(hardware)

motherboard: mbid(placa madre), mbname(nombre), mbcpu(procesador), mbchipset(chipset), mbBIOStype(tipo de BIOS), hid(hardware)

tred: tredid(tarjeta de red), rname(nombre), rtype(tipo), hid(hardware)

RAM: ramid(memoria de acceso aleatorio), ramname(nombre),

ramtype(tipo), ramsze(capacidad), hid(hardware)

mouse: mouseid(ratón), mname(nombre), mtype(tipo), hid(hardware)

user_role: uid(usuario), rid(rol)

user: uid(usuario), uname(nombre), umail(correo electrónico)

role: rid(rol), rname(nombre).

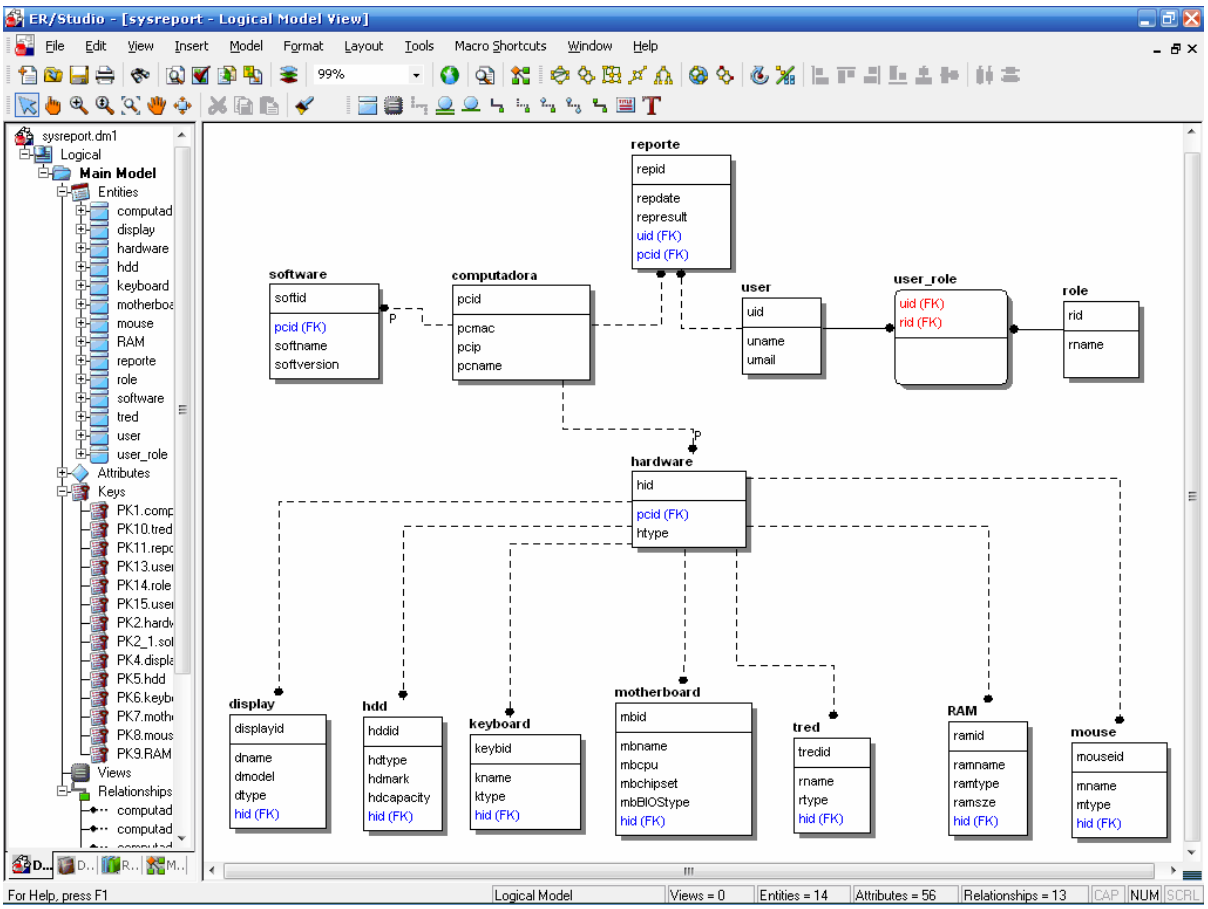

Figura 2.9 Diagrama lógico de la base de datos

Para comprobar el funcionamiento de la base de datos se utilizó el software xampp-win32 1.6.6 para simular las condiciones de un servidor con MySQL.

La tercera de las estructuras es el sistema que se encarga de realizar las encuestas a cada una de las computadoras del CDICT para después elaborar el reporte que almacena en la base de datos. Esta estructura funciona como un servicio que se instala en cada una de las computadoras de la red del CDICT según vaya encuestando, una vez que vaya terminando el servicio deja de ejecutarse y se repite el ciclo tantas veces como se haya programado el control de los medios informáticos.

La cuarta estructura se refiere al cronograma que es el módulo donde se programan los mantenimientos y reparaciones a los medios de hardware y software. Para esto se tiene una ventana donde se encuentran las opciones *Cronograma por PC* o *Cronograma General* donde el usuario selecciona la opción que desee. En el primer caso solo aparece el cronograma individual

de la computadora seleccionada y en el 2do caso aparecen todas las planificaciones del sistema completo.

2.4.3 Implementación de la infraestructura

Se propuso que el SISCAM-R se ejecute en un servidor con *S.O. WINDOWS* (las estructuras se implementaron para Windows) con *MySQL 4.0* por ser software libre, multiplataforma y además tiene un prestigio reconocido a nivel mundial. El servidor además debe tener al menos 512MB de RAM y 1.0GB de procesador dado que el sistema debe encuestar a cada una de las PC del CDICT en un tiempo determinado por administradores y que a veces puede ser pequeño por tanto necesita tener estas características para realizar las operaciones correctas. El período de tiempo entre un ciclo completo de encuesta y el siguiente puede ser tan pequeño como el administrador decida, puede darse el caso que se establezca que cada treinta minutos se realice un ciclo de encuestamiento o quizás menos. (Schumacher, 2009)

La estructura encargada de realizar reportes fue desarrollada en Python por permitir la división del programa en módulos reutilizables desde otros programas y se utiliza además como lenguaje de programación interpretado, lo que ahorra un tiempo considerable en el desarrollo del programa, pues no es necesario compilar ni enlazar. El intérprete se puede utilizar de modo interactivo, lo que facilita experimentar con características del lenguaje, escribir programas desechables o probar funciones durante el desarrollo del mismo. Python posee una licencia de código abierto, denominada Python Software Foundation License, que es compatible con la licencia GPL a partir de la versión 2.1.1. (Van Rossum, 2005)(Duque,).

Para el desarrollo de los códigos en Python se empleó Eclipse. El entorno de desarrollo integrado (IDE) de Eclipse emplea módulos (en inglés plug-in) para proporcionar toda su funcionalidad al frente de la plataforma de cliente rico, a diferencia de otros entornos monolíticos donde las funcionalidades están todas incluidas, las necesite el usuario o no. Este mecanismo de módulos es una plataforma ligera para componentes de software. Adicionalmente le permite a Eclipse extenderse usando lenguajes de programación como son C/C++ y Python. (Foundation, 2009).

Para ejecutar el servicio SISCAM-R se utilizó el software ServiceInstaler desarrollado por estudiantes de la facultad de Matemática-Física-Computación (MFC).

La base de datos se realizó empleando el software EMBARCADERO ER/STUDIO V6.0.1 por ser compatible con MySQL 4.0, mejora la consistencia de los datos, traza los orígenes de los datos y mejora la integración y exactitud. ER/Studio provee una interfaz visual de fácil utilización para documentar, entender y publicar información acerca de las bases de datos existentes de tal forma que puedan ser mejor controladas para soportar los objetivos trazados. (Embarcadero, 2009).

De modo general se cuenta con sistema que es un software basado en tecnología libre que trae ventajas para los distintos niveles de la universidad por tanto:

- La Universidad Central “Marta Abreu” de Las Villas en su conjunto puede disponer del SISCAM-R para las funciones que estime conveniente.
- No se necesitan licencias o permisos para utilizarlo.
- Contribuye en gran medida a la seguridad y control de los medios de hardware y software.

A manera de conclusión del capítulo se puede decir que el sistema muestra un avance considerable en la resolución de estos problemas y reduce el margen de error de la metodología anterior.

CAPÍTULO 3. Aplicaciones y Resultados del SISCAM-R

3.1 Aplicaciones Generales

El SISCAM-R presenta estructuras que pueden modificarse para cada tipo de centro según las especificaciones propias que ellos presenten. En cada caso se debe tener en cuenta el tipo de red y la cantidad de computadoras que existen para obtener los reportes, cuidando siempre el tamaño que pueda tomar la base de datos y las características del servidor que se destine para esto. Además se debe tener mucho cuidado a la hora de introducir los datos de cada computadora (referencia) que se utilizan para comparar con el reporte, de lo contrario es un reporte que se dejará de hacer hasta tanto no se corrija el error. De manera general se considera que una vez que el software sea estable puede utilizarse donde sea necesario.

3.1.1 Aplicaciones en el CDICT

A continuación se muestra un mapa que delimita las diferentes zonas que posee el CDICT en cuanto a la seguridad de los dispositivos de hardware y software. La Zona Cero dibujada en verde es donde no existe ninguna computadora. La Zona Alerta dibujada en Anaranjado es donde existen computadoras que pueden sufrir fallas de seguridad pero son locales que permanecen cerrados fuera de horario laboral y con poco personal en el horario de trabajo por tanto hay que prestar atención. La Zona Peligrosa dibujada en rojo es la más vulnerable a fallas en la seguridad, generalmente son zonas donde acuden o circulan gran cantidad de personal tanto en horario laboral como fuera de este. Es entonces esta última donde se debe prestar la mayor atención y se evidencia la necesidad urgente de utilizar el SISCAM-R como medio de control más eficaz.

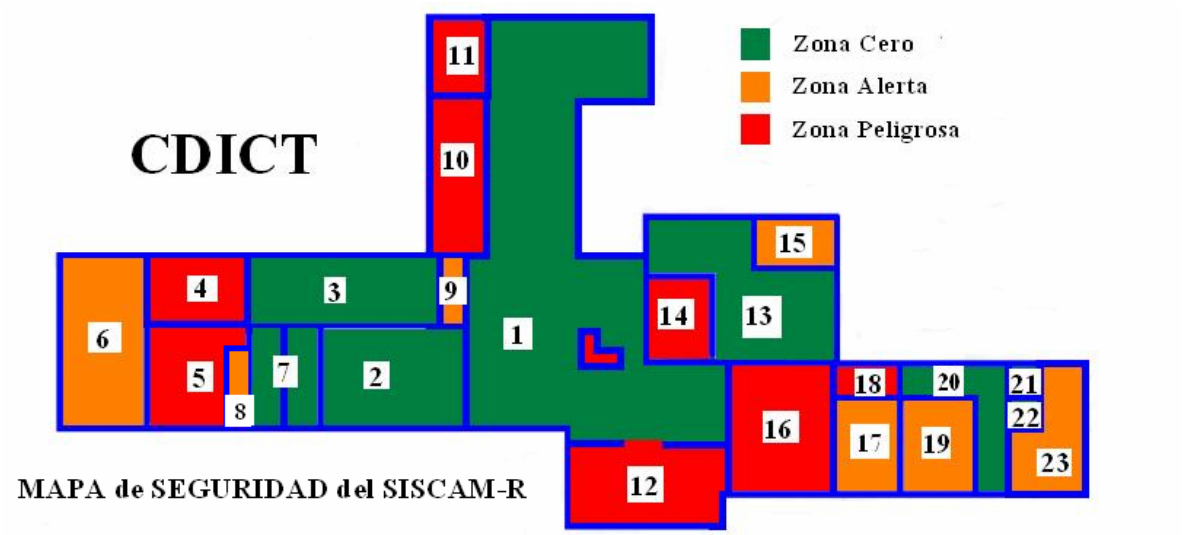

Figura 3. 1 Mapa del CDICT para la implementación del SISCAM-R

1-Salón de Estudio **(1)**	2-Galería	3-Pasillo
4-Local de Internet **(10)**	5-Laboratorio # 1 **(16)**	6-Editorial **(7)**
7-Baños	8-Dpto. Servidores **(7)**	9-Dpto. Seg. Informática **(2)**
10-Sala PSI-DER **(6)**	11-Sala HUM **(4)**	12-Sala Soc.-C.Empres. **(5)**
13-F.General	14-Recibidor **(2)**	15-Coronado **(1)**
16-Laboratorio# # 2 **(20)**	17-Dirección **(1)**	18-Secretaría-Admin. **(2)**
19-Salón de Reuniones **(1)**	20-Pasillo trasero	21-Pantry
22-Baño	23-Dpto. Serv. Esp. **(9)**	**TOTAL: (94)**

Nota: El número encerrado en paréntesis al final de cada Dpto. es la cantidad de computadoras que posee.

3.1.2 Resultados del SISCAM-R en la fase de pruebas.

La base de datos en fase de pruebas utilizando el xampp-win32 para lograr el ambiente de MySQL. En la siguiente figura se muestran todas las tablas del sistema de manera general

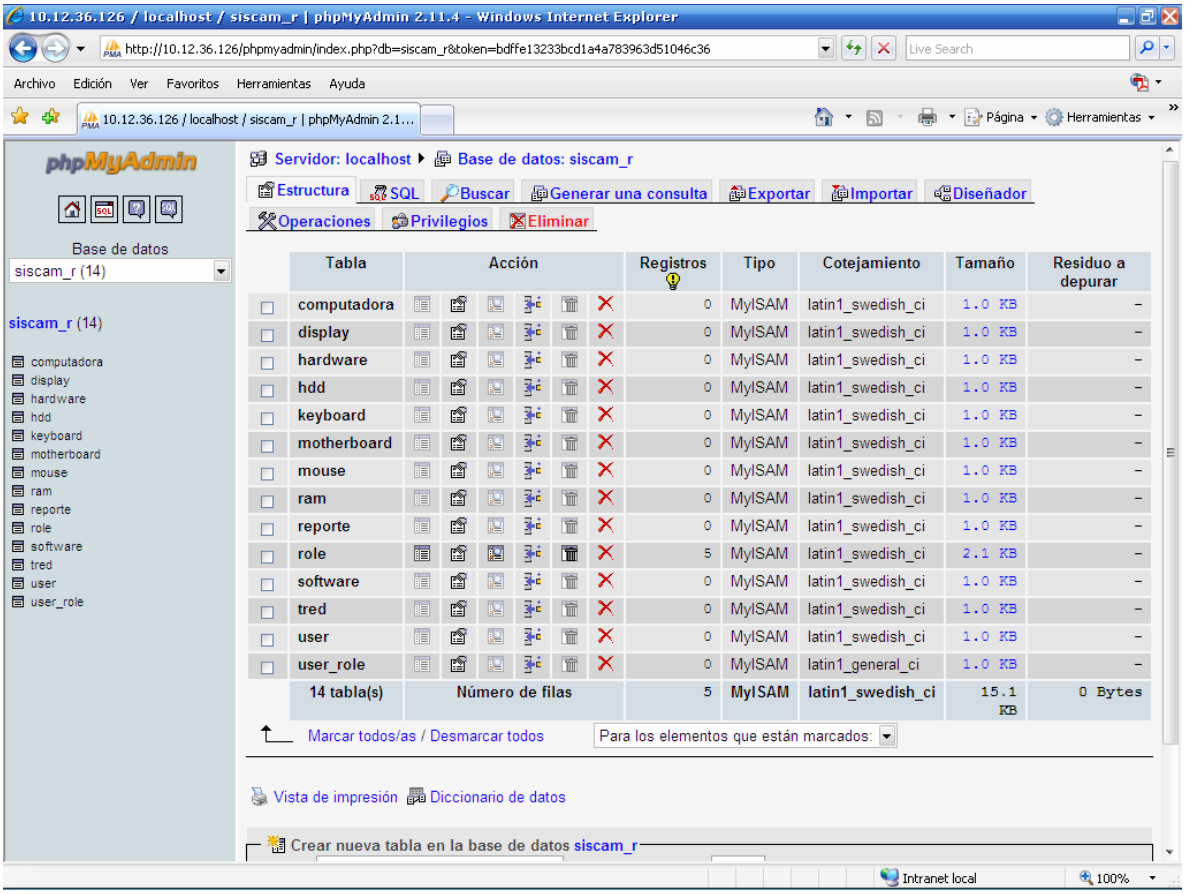

Figura 3. 2 Base de Datos General

En la siguiente figura se muestra la tabla rol con sus atributos particulares.

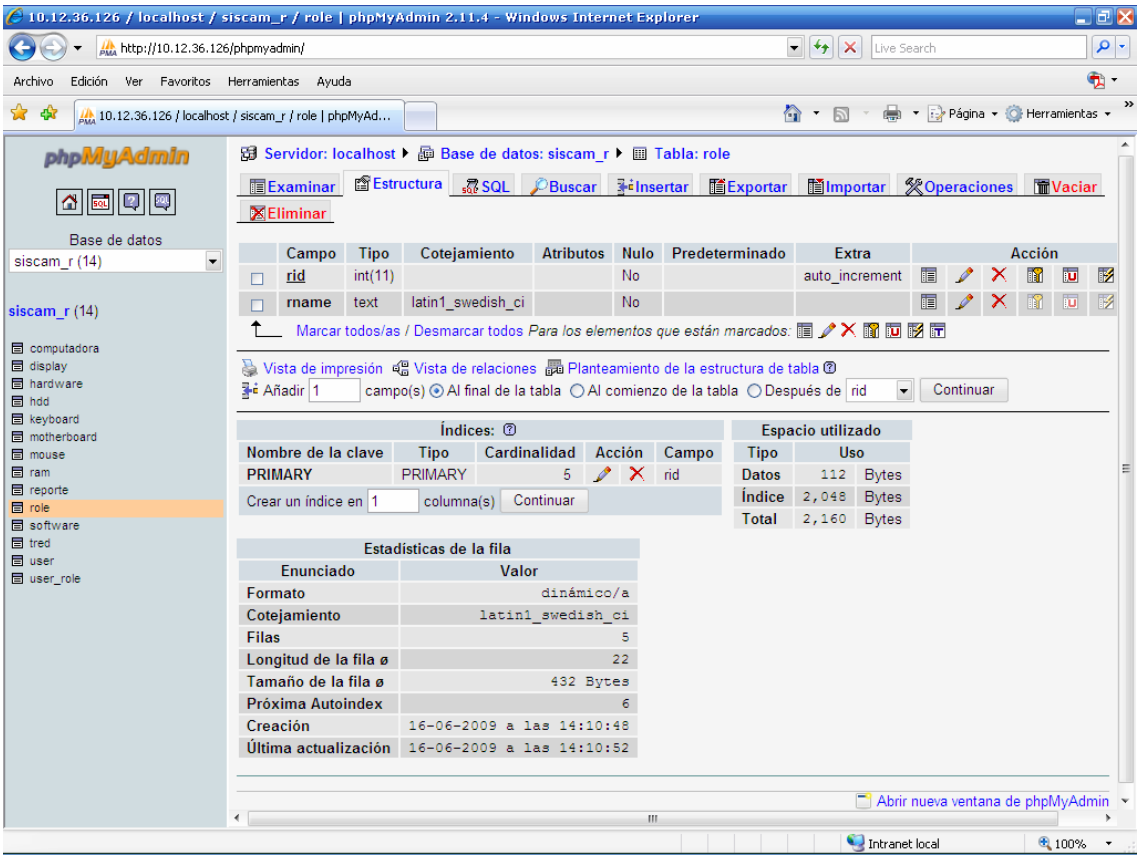

Figura 3.3 Base de datos (elementos particulares)

A continuación se presenta el sistema de encuestas ejecutándose en el software Eclipse for Python 1.31 para que se pueda observar los pasos que se realizan en cada máquina de lo contrario si se presentara en un ejecutable no veríamos nada porque es un servicio que se instala en la computadora encuestada de forma transparente al usuario o sea se ejecutaría sin percatarnos de ello.

Se tomó una muestra de al menos 13 computadoras para demostrar las funcionalidades de esta estructura. El rango de computadoras de 10.12.36.100 hasta 10.12.36.106, 10.12.36.111 y 10.12.36.112 se encontraban apagadas en el momento de la encuesta por lo que no devuelve ninguna información mientras que la 10.12.36.107,…...108,……109 y……110 se encontraban encendidas y muestran el reporte con los medios de hardware y software que posee incluyendo el usuario autentificado en ese momento. El reporte obtenido (logs) se guarda en un archivo de texto *.txt y se almacena luego en la base de datos.

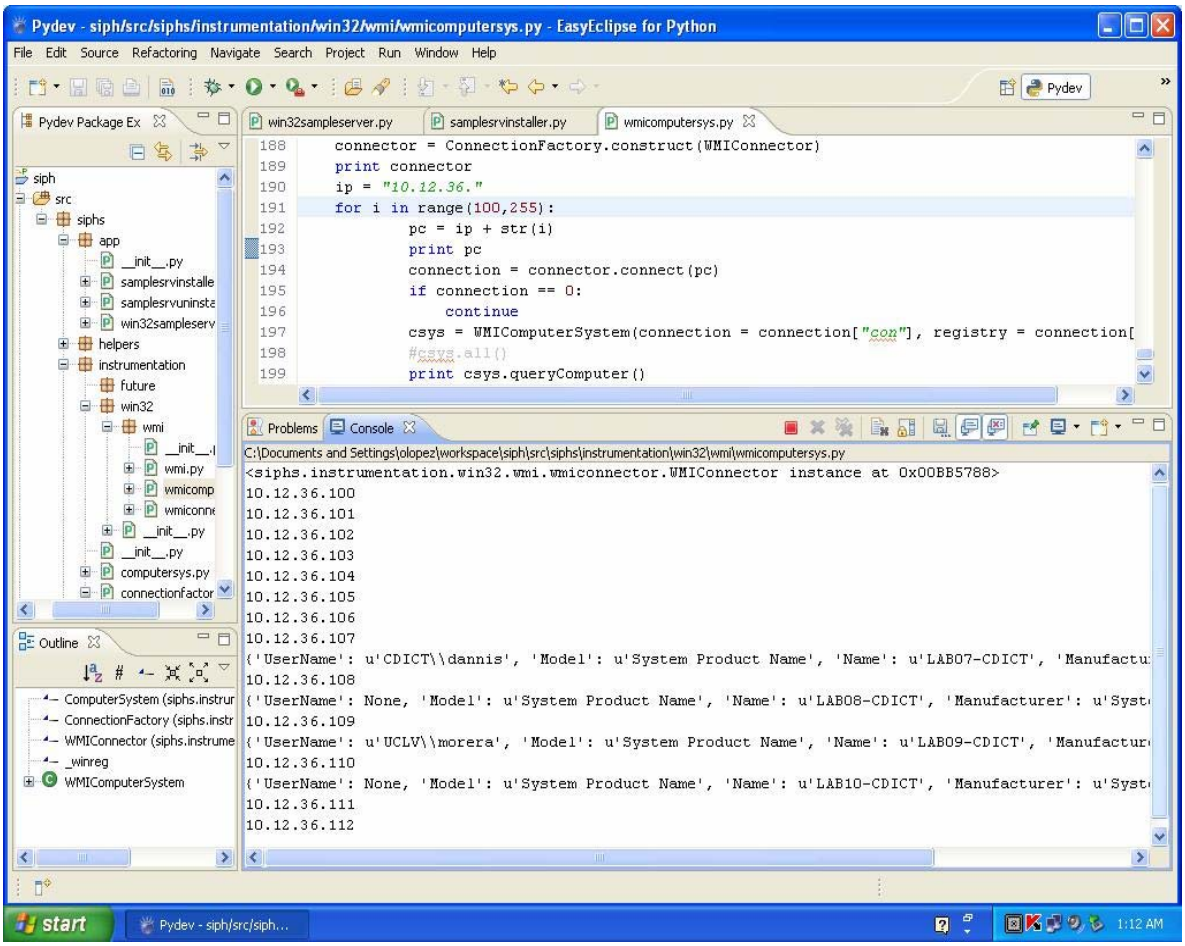

Figura 3. 4 Sistema de encuestas en ejecución

Tanto el reporte de hardware como el de software se comparan uno a uno con su referencia con vista a localizar el problema rápidamente. En el caso del cronograma se establece un área donde se publica la información para que sea accedida por el resto de los usuarios.

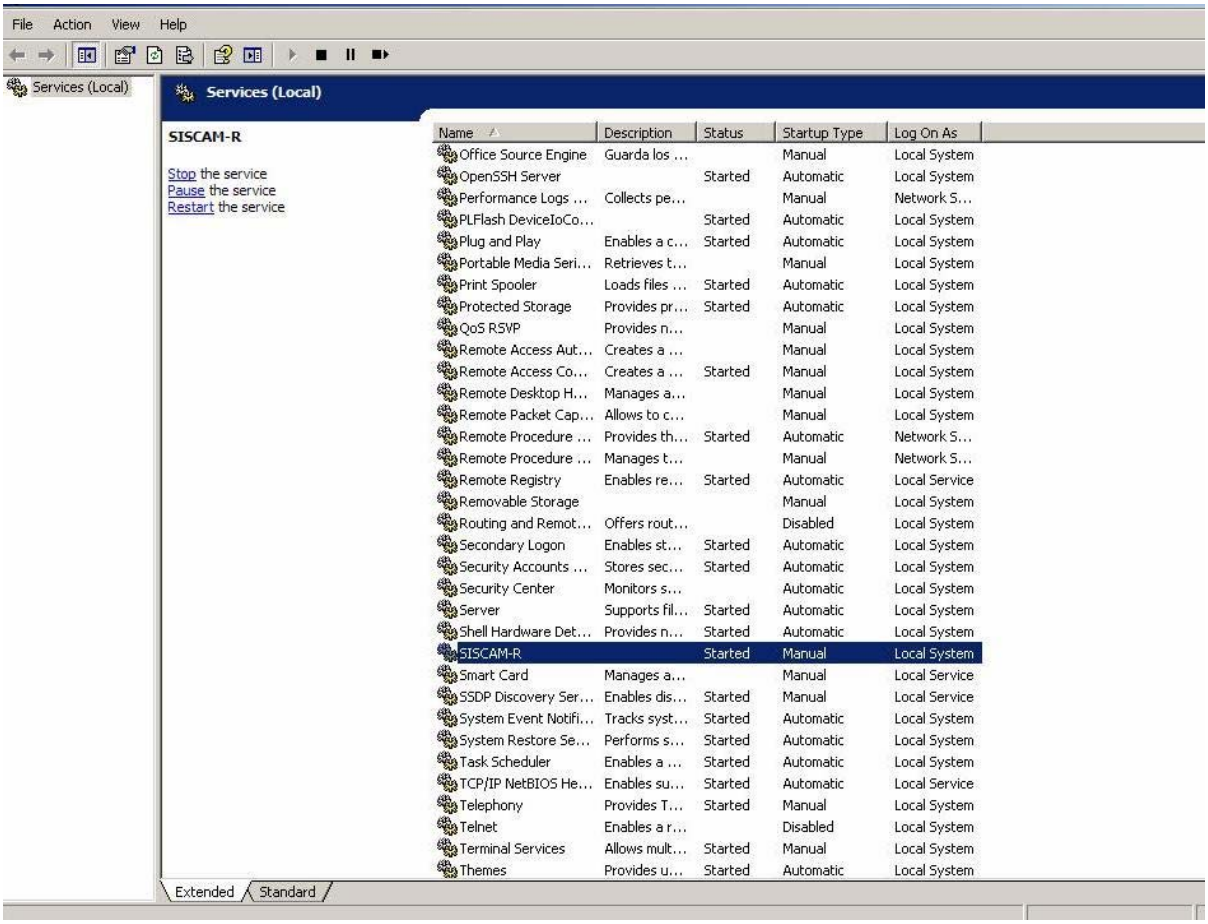

Figura 3. 5 Servicio SISCAM-R en ejecución.

3.2 Análisis económico

Para el desarrollo del presente trabajo se dispuso de las computadoras instaladas en el CDICT incluyendo el servidor donde se encuentra el sistema. Los software que se utilizaron en el desarrollo del SISCAM-R en su mayoría son libres, siendo una de las debilidades del sistema que en su utilización se emplearon algunos software propietarios que se emplean en el país sin autorización previa de los dueños en virtud del bloqueo económico que afecta a Cuba.

El personal que colaboró con la puesta en funcionamiento de nuestro software son trabajadores y estudiantes de esta institución.

Por otra parte el sistema desarrollado presenta un beneficio económico implícito toda vez que por su función de medio de control del hardware de las computadoras personales del área donde se este utilizando se evita el cambio o alteración de estos elementos sin la autorización correspondiente, de esta forma se evita el robo o extravío de estos elementos.

CONCLUSIONES

1- Ninguno de los distintos software analizados, que brindan información de la estructura de hardware y software de las computadoras personales, se ajustan a los requerimientos del área.

2- El SISCAM-R es una eficaz herramienta que brinda, de manera automatizada, la información requerida de los medios de hardware y software de las computadoras personales del área conectadas a la red.

3- El sistema desarrollado dispone de una interfaz gráfica amigable y de fácil entendimiento por parte de los usuarios potenciales del mismo.

4- La utilización del SISCAM-R permite un eficaz control de los medios de computo del área evitando la perdida o extravio de los mismos y por ende el consiguiente gasto a la economía del país.

RECOMENDACIONES

1 Desarrollar el SISCAM-R de forma que sea un sistema multiplataforma y basado en tecnología de software libre.

2 Estudiar y desarrollar la opción que permita obtener reportes de las computadoras personales aun cuando se encuentran apagadas pero conectadas a las redes eléctrica e informática utilizando información contenida en los dispositivos que permanecen energizados, BIOS, Tarjeta de red, Fuente de alimentación, etc.

3 Mantener el sistema en fase de pruebas en un período de 2 a 3 meses hasta tanto se corrijan los posibles errores que puedan presentarse.

REFERENCIAS BIBLIOGRÁFICAS

COTARELO, D. T. 2004. *Auditoría de equipos informáticos (II)*. [Página Web]. Disponible en: http://observatorio.cnice.mec.es/modules.php?op=modload&name=News&file=article&sid=145 (Consultado: 15 de abril 2009).

DARRAIDO, E. M., LLANES, J. D. H., JIMÉNEZ, O. L. y VERA, C. C. 2008. *Sistema de Inventario Periódico de Hardware*. [Software]. Santa Clara: CHASQUI.

DUQUE, R. G. *Python para todos.*

ECLIPSE FOUNDATION. 2009. *ECLIPSE*. [Página Web]. Disponible en: http://www.eclipse.org

(Consultado: 8 de mayo 2009).

EMBARACADERO TECHNOLOGIES INC (2009) ER/Studio Modelado de datos empresarial.

EVEREST CORPORATE. 2009. *Everest Ultimate Edition*. [Página Web]. Disponible en: http://www.mp3.es/Es/Everest_Ultimate_Edition (Consultado: 7 abril 2009).

GEBHARD, P. 2009. *Dr. Hardware - Your PC Expert*. [Página Web]. Disponible en: http://www.dr-hardware.com/ (Consultado: 22 de abril 2009).

JACOBSON, I., BOOCH, G. y RUMBAUGH, J. 2000. *El Proceso Unificado de Desarrollo de Software.* 1ra. Madrid:

LANCHARRO, F. J. 2003. *Analizadores de sistemas*. [Página Web]. Disponible en: http://www.terra.es/tecnologia/articulo/html/tec9805.htm (Consultado: 14 de abril 2009).

PYTHON SOFTWARE FOUNDATION. 2009a. *Lenguaje de programación Python*. [Página Web]. Disponible en: http://www.python.org/

(Consultado: 5 de mayo 2009).

PYTHON SOFTWARE FOUNDATION. 2009b. *Python Programming Language*. [Página Web]. Disponible en: http://www.python.org/

(Consultado: 5 de mayo 2009).

ROBIN SCHUMACHER. 2009. *¿Por qué pasar a la versión de Microsoft SQL Server?* . [Página Web]. Disponible en: http://www.mysql.com/

(Consultado: 7de mayo 2009).

ROSUMM, G. V. y L.DRAKE, F. 2005. Guía de aprendizaje de Python. [Revista electrónica]. Disponible en (Consultado: 10 de marzo 2009).

SOFTONIC INTERNATIONAL. 2008. *Dameware*. [Página Web]. Disponible en: http://dameware-nt-utilities.softonic.com/ (Consultado: 14 de abril 2009).

TOGGLE. 2009. *Sisoftware Sandra*. [Página Web]. Disponible en: http://wiki.toggle.com/es/index.php?title=SiSoftware_Sandra_Lite&cat=Windows (Consultado: 15 de abril 2009).

VALVE CORPORATION. 2007. *DXDIAG*. [Página Web]. Disponible en: http://supportwiki.steampowered.com/es/DXDIAG (Consultado: 8 de abril 2009).

ANEXOS

Anexo 1

REGLAMENTO DE SEGURIDAD

PARA LAS TECNOLOGÍAS DE LA INFORMACIÓN

……

CAPITULO II

DEL SISTEMA DE SEGURIDAD INFORMATICA.

…….

ARTÍCULO 9: Los jefes a las diferentes instancias en los órganos, organismos y entidades responden por la protección de los bienes informáticos que le han sido asignados y tienen las siguientes obligaciones:

a) Identificar los requerimientos de seguridad de los bienes informáticos bajo su responsabilidad y de las aplicaciones en desarrollo, determinar el nivel de acceso de los usuarios a los mismos y la vigencia de estos accesos.
b) Participar en el diseño del Sistema de Seguridad y en la elaboración, evaluación y actualización del Plan de Seguridad Informática en la parte que concierne a su esfera de acción y garantizar su cumplimiento.

c) Aplicar las medidas y procedimientos establecidos en su área de responsabilidad.
d) Especificar al personal subordinado las medidas y procedimientos establecidos y controlar su cumplimiento.
e) Participar en la elaboración de los procedimientos de recuperación ante incidentes de seguridad y en sus pruebas periódicas.
f) Imponer o proponer sanciones ante violaciones del Sistema de Seguridad, en correspondencia con su naturaleza y con los daños ocasionados.

ARTÍCULO 10: El responsable de la actividad informática en cada entidad tiene las siguientes obligaciones:

a) Participar en el diseño del Sistema de Seguridad y en la elaboración, evaluación y actualización del Plan de Seguridad Informática, supervisar su aplicación y disciplina de cumplimiento.
b) Establecer y mantener los controles en correspondencia con el grado de protección requerido por el Sistema de Seguridad Informática diseñado.
c) Garantizar la disponibilidad de los bienes informáticos.
d) Asesorar a las distintas instancias sobre los aspectos técnicos vinculados con la seguridad de las tecnologías de la información.
e) Establecer los controles necesarios para impedir la instalación de cualquier tipo de hardware o software sin la autorización de la Dirección de la Entidad.
f) Participar en la elaboración de los procedimientos de recuperación ante incidentes de seguridad y en sus pruebas periódicas.
g) Informar a los usuarios de las regulaciones establecidas.

ARTÍCULO 11: Los usuarios de las tecnologías de la información asumen en primera instancia la responsabilidad de las consecuencias que se deriven de la utilización impropia de las mismas.

ARTÍCULO 12: Los usuarios de las tecnologías de información en órganos, organismos y entidades tienen las siguientes obligaciones:

a) Adquirir la preparación necesaria y los conocimientos de Seguridad Informática imprescindibles para el desempeño de su trabajo.

b) Contar con la autorización expresa del jefe facultado, para obtener acceso a cualquiera de los bienes informáticos.
c) Utilizar las tecnologías de información solo en interés de la entidad.
d) No transgredir ninguna de las medidas de seguridad establecidas.
e) Proteger las tecnologías o la terminal de red que le ha sido asignada y colaborar en la protección de cualquier otra, para evitar que sea robada o dañada, usada la información que contiene o utilizado de manera impropia el sistema al que esté conectada.
f) No instalar ni utilizar en las tecnologías equipamientos o programas ni modificar la configuración de las mismas, sin la correspondiente autorización del jefe facultado.
g) Cumplir las reglas establecidas para el empleo de las contraseñas.
h) Informar al dirigente facultado de cualquier anomalía de seguridad detectada.

CAPITULO III

EMPLEO CONVENIENTE Y SEGURO DE LAS TECNOLOGÍAS DE LA INFORMACION

Sección Primera

Clasificación y control de bienes informáticos

ARTÍCULO 13: Los bienes informáticos de una entidad deben ser utilizados en las funciones propias del trabajo en correspondencia con su objeto social.

ARTÍCULO 14: Todos los bienes informáticos de una entidad deberán estar identificados y controlados, para lo cual se conformará y mantendrá actualizado un inventario de éstos incluyendo sus componentes y las especificaciones técnicas de aquellos que pudieran ser suplantados.

ARTÍCULO 15: Cada uno de los bienes informáticos de una entidad tienen que ser puestos bajo la custodia documentada legalmente de una persona, que actuando por delegación de la dirección de la entidad, es responsable de su protección.

ARTÍCULO 16: Los jefes de entidades instrumentarán los procedimientos que se requieran para garantizar la autorización y el control sobre el movimiento de los bienes informáticos, los cuales deberán ser considerados a esos efectos de igual forma que el resto de los medios de la entidad.

Sección Segunda

Del personal

…….

ARTÍCULO 21: El uso no autorizado de las tecnologías de información y sus servicios asociados constituye una violación de los derechos de la entidad que es sancionable. Es un deber y un derecho de la dirección de cada entidad la supervisión del empleo de las tecnologías de la información por parte de los usuarios.

ARTÍCULO 22: Los Jefes a cada nivel, garantizarán que el personal vinculado a las tecnologías de la información esté capacitado para la utilización de las mismas, así como que conozca sus deberes y derechos en relación con el Sistema de Seguridad Informática implementado, los cuales deberán firmar una declaración como constancia de su conocimiento y compromiso de cumplimiento, que se incluirá en el contrato de trabajo.

ARTÍCULO 23: El acceso a las facilidades de procesamiento y a los servicios que brindan las tecnologías por parte de personal que no forme parte de la plantilla será en todos los casos objeto de una estricta autorización y control por parte de la dirección de cada entidad y a partir de los riesgos que esto pueda introducir se establecerán los requerimientos específicos que correspondan para garantizar la seguridad.

ARTÍCULO 24: Los usuarios de las tecnologías de la información están en la obligación de informar de inmediato cualquier incidente de seguridad, debilidad o amenaza a sistemas o servicios y las direcciones correspondientes exigirán su cumplimiento.

ARTÍCULO 25: Constituye una violación grave de la seguridad la realización de acciones de comprobación de vulnerabilidades contra sistemas informáticos nacionales o extranjeros.

ARTÍCULO 26: Ninguna persona está autorizada a introducir, ejecutar, distribuir o conservar en los medios de cómputo programas que puedan ser utilizados para comprobar, monitorear o transgredir la seguridad, así como información contraria al interés social, la moral y las buenas costumbres, excepto aquellas aplicaciones destinadas a la comprobación del sistema instalado en la organización para uso por especialistas expresamente autorizados por la dirección de la misma. En ningún caso este tipo de programas o información se expondrá mediante las tecnologías para su libre acceso.

Sección Tercera

Seguridad Física y Ambiental

ARTÍCULO 27: La dirección de cada entidad determinará las tecnologías de información que por las funciones a que estén destinadas, la información que contengan y las condiciones de los locales en que se encuentren ubicadas, requieran la aplicación específica de medidas de protección física.

ARTÍCULO 28: Las tecnologías de la información se ubicarán en áreas que garanticen la aplicación de medidas alternativas que permitan la creación de una barrera de protección a estos medios e impidan su empleo para cometer acciones malintencionadas o delictivas.

ARTÍCULO 29: En los edificios e instalaciones de cada entidad se determinarán áreas o zonas controladas con requerimientos específicos, protegidas por un perímetro de seguridad definido en dependencia de la importancia de los bienes informáticos contenidos en ellas y su utilización, de acuerdo con los criterios y denominaciones siguientes:

a) **Áreas limitadas,** son aquellas donde se concentran bienes informáticos de valor medio cuya afectación puede determinar parcialmente los resultados de la gestión de la entidad o de terceros.

b) **Áreas restringidas,** son aquellas en que se concentran bienes informáticos de alto valor e importancia crítica cuya afectación pueda paralizar o afectar severamente la gestión de ramas o sectores de la economía o de la sociedad; territorios o entidades.

c) **Áreas estratégicas**, son aquellas en que se concentran bienes informáticos de alto valor e importancia crítica que inciden de forma determinante en la seguridad y la defensa nacional; la seguridad aeronáutica; biológica; industrial; la generación y distribución de energía eléctrica; las redes informáticas y de comunicaciones del país; las relaciones exteriores y de colaboración; la economía nacional; las investigaciones científicas y el desarrollo tecnológico; la alimentación de la población; la salud pública y el suministro de agua.

ARTÍCULO 30: Las áreas o zonas controladas estarán protegidas con medidas adecuadas para garantizar el acceso exclusivamente al personal autorizado.

ARTÍCULO 31: La selección y diseño de las áreas controladas tomará en cuenta la posibilidad de daño por fuego, inundación, explosión, perturbaciones del orden y otras formas de desastre natural o artificial.

ARTÍCULO 32: El equipamiento instalado en las áreas controladas estará protegido contra fallas de alimentación y otras anomalías eléctricas, incluyendo el uso de fuentes de alimentación alternativas para los procesos que deban continuar en caso de un fallo de electricidad prolongado y será ubicado y protegido de manera tal que se reduzcan los riesgos de amenazas ambientales y oportunidades de cualquier tipo de acceso no autorizado.

ARTÍCULO 33: En las Áreas Limitadas se aplicarán las medidas de protección física siguientes:

a) Se ubicarán en locales cuyas puertas y ventanas estén provistas de cierres seguros;
b) A los locales que tengan ventanas que se comuniquen con el exterior de la instalación, se le aplicarán medidas que garanticen su seguridad y que eviten la visibilidad hacia el interior del mismo;
c) Se prohíbe el acceso de personal no autorizado por la dirección de la entidad.
d) Se prohíbe la permanencia del personal fuera del horario laboral sin la debida justificación y autorización por escrito de la dirección de la entidad. Las autorizaciones referidas serán conservadas para su verificación en caso de necesidad.

ARTÍCULO 34: En las Áreas Restringidas, además de las medidas requeridas en las Áreas Limitadas, se aplicarán las siguientes:

a) Tienen que permanecer cerradas, incluso cuando existan personas laborando en ellas, y el acceso a las mismas debe ser controlado mediante los documentos de registro que para ello se establezcan;
b) El personal que acceda a estas áreas deberá cumplir requisitos especiales de idoneidad.
c) Los medios informáticos no podrán estar conectados de manera física o lógica a medios que se encuentren fuera del alcance de estas áreas ni a redes públicas de transmisión de datos;
d) Se aplicarán sistemas de detección y alarma que permitan una respuesta , efectiva ante accesos no autorizados cuando no se encuentre el personal que labora en las mismas;
e) Se implementarán mecanismos y procedimientos de supervisión de la actividad que se realiza en estas áreas;
f) Se prohíbe la introducción de soportes ópticos y magnéticos personales, excepto los que hayan sido autorizados de forma expresa por la dirección de la entidad.
g) Se prohíbe la introducción de cámaras fotográficas, de grabación de imágenes o cualquier tipo de almacenamiento digital ajeno a la misma.

ARTÍCULO 35: En las Áreas Estratégicas, además de las medidas requeridas en las Áreas Restringidas y Limitadas, se aplicarán las siguientes:

a) Todo el personal que labora en ellas o que por razones de servicio sea autorizado a permanecer en las mismas, deberá contar con una identificación personal visible que

distinga el área.

b) Se implementarán medios especiales de supervisión de la actividad que en ellas se realiza;
c) El acceso a estas áreas por personas ajenas a la misma solo se realizará de manera excepcional, restringida y bajo supervisión, mediante un permiso especial en cada caso emitido por la dirección de la entidad.

ARTÍCULO 36: Todas las tecnologías de información, independientemente de su importancia, se protegerán contra alteraciones o sustracciones, ya sea de éstas o sus componentes, así como de la información que contienen.

ARTÍCULO 37: En las redes de las entidades los cables de alimentación o de comunicaciones que transporten datos o apoyen los servicios de información se protegerán contra la intercepción o el daño. Los cables de alimentación deberán estar separados de los cables de comunicaciones para evitar la interferencia.

ARTÍCULO 38: Los jefes de entidades garantizarán que el equipamiento reciba el mantenimiento correcto de acuerdo con los intervalos de servicio y especificaciones recomendados por el fabricante para asegurar su disponibilidad e integridad continuas. En caso de necesidad de envío de equipamiento fuera de las instalaciones para que reciban mantenimiento, se realizará en correspondencia con los procedimientos que se establezcan previamente para ello, observando las regulaciones establecidas en el país en materia de protección a la información.

ARTÍCULO 39: El uso fuera de las instalaciones de una entidad de cualquier equipo para el procesamiento de información tiene que estar autorizado legalmente por la dirección de la misma mediante el documento correspondiente. La seguridad que se le garantice deberá ser equivalente a la que tiene en las instalaciones habituales el equipamiento usado para el mismo propósito, tomando en cuenta los riesgos de trabajar fuera de la instalación.

ARTÍCULO 40: El equipamiento que cause baja o sea destinado para otras funciones será objeto de un procedimiento adecuado para evitar que la información que contiene pueda resultar comprometida. Los dispositivos de almacenamiento que contengan información crítica para la entidad deberán destruirse físicamente o sobrescribirse mediante un proceso completo en lugar de borrarlos como usualmente se hace.

ARTÍCULO 41: Se prohíbe el movimiento sin autorización de los equipos, la información o el software y en caso de que se autorice será realizado mediante un documento oficial que demuestre su legalidad y el movimiento deberá registrarse a la salida y a la entrada al reintegrarse el medio a su origen. Se deberán realizar inspecciones sorpresivas para detectar las extracciones no autorizadas.

Sección Cuarta

Seguridad de Operaciones

ARTÍCULO 42: Al determinar las responsabilidades que se asignan al personal se tendrá en cuenta el principio de separación de funciones, considerando aquellas tareas que no deben ser realizadas por una misma persona, a fin de reducir oportunidades de modificación no autorizada o mal uso de los sistemas informáticos.

ARTÍCULO 43: La introducción en una entidad de nuevos sistemas informáticos, actualizaciones y nuevas versiones será aprobada previamente a partir de su correspondencia con el sistema de seguridad establecido y los resultados de las pruebas que se realicen para determinar si cumple los criterios de seguridad apropiados.

ARTÍCULO 44: Las acciones para cubrir las brechas de seguridad y la corrección de los errores del sistema deberán estar minuciosamente controladas en cada entidad. Los procedimientos deberán asegurar que:

a) solo el personal claramente identificado y autorizado tenga acceso a sistemas en funcionamiento y a los datos;

b) todas las acciones de emergencia tomadas sean documentadas detalladamente;
c) la acción de emergencia sea reportada a la dirección y realizada de manera ordenada;

…….

CAPITULO IV

GESTIÓN DE INCIDENTES DE SEGURIDAD

ARTÍCULO 86: Las entidades están obligadas a formular la estrategia a seguir ante cualquier incidente o violación de la seguridad que pueda producirse en correspondencia con la importancia de los bienes informáticos que posea y las posibles alternativas a emplear para garantizar los servicios. Dicha estrategia deberá ser consecuente con los objetivos básicos de la entidad y tomará en consideración:

a) Los riesgos que la entidad enfrenta en términos de su probabilidad y su impacto, incluyendo una identificación y asignación de prioridades a los procesos críticos.
b) El impacto probable de las interrupciones sobre la gestión de la entidad.
c) Comprobar y actualizar regularmente los planes y procesos establecidos.

ARTÍCULO 87: Una vez establecida la estrategia a seguir, las entidades dispondrán las medidas y procedimientos que correspondan con el fin de garantizar la continuidad, el restablecimiento y la recuperación de los procesos informáticos.

ARTÍCULO 88: Las medidas y procedimientos de recuperación serán definidas a partir de la identificación de los posibles eventos que puedan causar la interrupción o afectación de los procesos informáticos e incluirán las acciones de respuesta a realizar, la determinación de los responsables de su cumplimiento y los recursos necesarios en cada caso.

ARTÍCULO 89: Los procedimientos para la gestión de incidentes y violaciones de Seguridad Informática, especificarán los pasos a seguir para garantizar una correcta evaluación de lo que ha ocurrido, a quién, cómo y cuándo debe ser reportado, la respuesta

adecuada, así como los aspectos relacionados con su documentación, la preservación de las evidencias y las acciones a seguir una vez restablecida la situación inicial. Para ello considerarán lo siguiente:

a) el reporte inmediato de la acción a la autoridad correspondiente;
b) la comunicación con los afectados o los involucrados en la recuperación del incidente;
c) el análisis y la identificación de las causas de los incidentes;
d) el registro de todos los eventos vinculados con el incidente;
e) la recolección y preservación de las trazas de auditoría y otras evidencias;
f) la planificación y la implementación de medidas para prevenir la recurrencia, si fuera necesario;

ARTÍCULO 90: Ante cualquier incidente que afecte la Seguridad Informática de una entidad, se designará por la dirección de la misma una comisión presidida por un miembro del Consejo de Dirección e integrada por especialistas no comprometidos directamente con el incidente, que realizará las investigaciones necesarias con el fin de esclarecer lo ocurrido, determinar el impacto, precisar los responsables y proponer la conducta a seguir.

ARTÍCULO 91: La dirección de cada entidad garantizará que al producirse un incidente o violación de la seguridad informática la información sobre este acontecimiento se reporte inmediatamente a la Oficina de Seguridad para las Redes Informáticas y a la instancia superior de la entidad. Este reporte incluirá como mínimo:

a) En que consistió el incidente o violación.
b) Fecha y hora de comienzo del incidente y de su detección.
c) Implicaciones y daños para la entidad y para terceros.
d) Acciones iniciales tomadas.
e) Evaluación preliminar