Universidad Central “Marta Abreu” de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica

TRABAJO DE DIPLOMA

“Sistema de Registro Automático de Usuarios para la red UCLV”

Autor: Marisabel Rodríguez Torres

Tutor: MSc. José Omar Padrón Ramos

Santa Clara

2012

"Año 54 de la Revolución"

Universidad Central “Marta Abreu” de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica

TRABAJO DE DIPLOMA

“Sistema de Registro Automático de Usuarios para la red UCLV”

Autor: Marisabel Rodríguez Torres

E-mail: marisabelr@uclv.edu.cu

Tutor: MSc. José Omar Padrón Ramos

Profesor Asistente Dpto. de Automática,

Facultad de Ing. Eléctrica, UCLV.

E-mail: jpadron@uclv.edu.cu

Santa Clara

2012

"Año 54 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 Telecomunicaciones y Electrónica, 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 Tutor

Firma del Jefe de Departamento donde se defiende el trabajo

Firma del Responsable de Información Científico-Técnica

PENSAMIENTO

Detrás de cada línea de llegada hay una de partida, detrás de cada logro hay otro desafío.

Madre Teresa de Calcuta

DEDICATORIA

A mi familia por todo su amor, comprensión y apoyo, gracias a ustedes hoy estoy aquí.

A mi padre que es mi inspiración y mi ejemplo.

AGRADECIMIENTOS

A mis padres y hermano por ayudarme a hacer realidad este sueño.

A José Omar por brindarme su apoyo, sabiduría y sobre todo su amistad.

A toda mi familia abuelos, tíos y primos que han sabido estar siempre que los he necesitado.

A mi amiga Dayi que me ha comprendido y apoyado durante estos cinco años, por estar juntas en los buenos y malos momentos.

A Yani, Meyli, Leo, Ale, Adonis, Yaimara por compartir juntos todos esos días de estudio, por su amistad.

A Javier por ayudarme y apoyarme en la tesis.

A mis profesores por contribuir a mi formación y preparación profesional.

A mis viejos amigos.

A los que aquí no menciono pero que ocupan un lugar importante en mi vida porque me han apoyado y de alguna manera han contribuido a mi formación intelectual, profesional y humana.

Y a ti.

RESUMEN

Existen varias herramientas de software para controlar el ingreso a una red de área local, para permitir la protección ante posibles ataques y también realizar un seguimiento a la red cuando se cree que alguna de las máquinas ha sido comprometida. Estas herramientas son costosas, por las cuales hay que pagar licencias, y están sobredimensionados de acuerdo a los requerimientos que se necesitan en la red universitaria.

El "Sistema Automático de Registro de Usuarios" es un mecanismo eficiente e independiente de la voluntad de usuarios y técnicos para registrar el uso de los medios computacionales en la Universidad Central "Marta Abreu" de las Villas. El software registra los parámetros del usuario que haga uso de las computadoras donde se encuentre instalado y los almacene en una base de datos a la cual se conectará de forma remota para crear los registros históricos.

SARU comprende una serie de tres programas, una aplicación cliente, una base de datos centralizada y un programa de análisis y visualización de datos. El cliente, instalado como servicio en las computadoras, obtiene la hora de entrada al sistema, el nombre de usuario, el IP de la máquina y el nombre de la PC, almacenando estos parámetros en la base de datos remota.

Este sistema evita la brecha de seguridad originada por el no cumplimiento de las responsabilidades de los usuarios y el técnico de un laboratorio, además permite controlar el uso de los medios computacionales y hacer estudios estadísticos del mismo.

TABLA DE CONTENIDOS

INTRODUCCIÓN

La dirección de informatización de la Universidad Central “Marta Abreu” de Las Villas establece un código de ética para lograr que los estudiantes utilicen los medios computacionales eficientemente. En el caso del empleo de los laboratorios de computación para estudiantes, se establece un protocolo que exige una documentación, donde el técnico del local debe plasmar, para cada usuario, la hora de entrada, la hora de salida, el nombre de la computadora en la que trabajó y la firma del estudiante. El protocolo es obligatorio en toda el área universitaria pero no se cumple de forma sistemática, en lo cual influyen varios factores como: el nivel de responsabilidad del técnico, la disponibilidad del modelo en papel, lápices o lapiceros, la demora al realizar las anotaciones contra el tiempo de uso de la computadora, los horarios de clases. Estos factores, unidos al hecho del no cumplimiento sistemático, brindan una brecha de seguridad importante en la red universitaria, ya que un usuario con conocimientos avanzados puede burlar los registros del uso de la computadora y su presencia no puede ser probada en el momento de cometer alguna fechoría, como ha ocurrido muchas veces.

Se han creado muchos métodos para controlar el uso que se da a los medios computacionales y controlar el acceso a la red. Existen varias herramientas de software para controlar el ingreso a una red de área local, para permitir la protección ante posibles ataques y también realizar un seguimiento a la red cuando se cree que alguna de las máquinas ha sido comprometida. De esta manera se hace más fácil controlarlas y administrarlas. Existen varias herramientas de software muy eficientes entre las que se encuentran Tcp-wrappers, Netlog, Nstat, Aarhu, Aarhu, SATAN, ISS, Courtney, Gabriel, Nocol.

Existen también algunos programas que tienen entre sus objetivos acciones similares, por ejemplo aquellos cuyo propósito es administrar remotamente una red de computadoras como el DameWare NTUtilities, el NetSupport Manager, el Hyena, el Remote Desktop. También existen otros programas a nivel internacional que están más enfocados a

supervisar la actividad de los usuarios de una red, algunos son el iMonitorPC, el Spector 360, el ObserveIT y el Novell Compliance Management Platform.

El sistema operativo Windows, en sus diferentes versiones, también posee algunos mecanismos para controlar el estado y la actividad de los usuarios, como el registro de eventos en cada sesión de usuario y el administrador remoto. Específicamente en la Universidad Central “Marta Abreu” de las Villas estos servicios a pesar que funcionan plenamente en cada computadora, adolecen de la interactividad, o sea para obtener la actividad de un usuario en específico hay que descargar el registro de eventos o conectarse remoto a la computadora, las cuales son formas muy ineficaces y que atentan contra la utilidad del equipamiento y entorpecen las labores docentes. De los programas que se mencionaron en el párrafo anterior, todos son costosos, por los cuales hay que pagar licencias, y están sobredimensionados de acuerdo a los requerimientos que se necesitan en la red universitaria.

La parte más importante en la seguridad de la red son los usuarios de un sistema, a ellos no se les puede olvidar ni menospreciar. Siempre hay que tener en cuenta que la seguridad comienza y termina con personas. Obtener de los usuarios la concientización de los conceptos, usos y costumbres referentes a la seguridad, requiere tiempo y esfuerzo. Que los usuarios se concienticen de la necesidad y, más que nada, de las ganancias que se obtienen implementando planes de seguridad, exige trabajar directamente con ellos, de tal manera que se apoderen de los beneficios de tener un buen plan de seguridad. De esta forma, ante cualquier problema, es muy fácil determinar dónde se produjo o de dónde proviene.

Ante esta situación, se evidencia una problemática real presente en la universidad, la cual se puede definir de la siguiente manera: no existe un mecanismo eficiente e independiente de la voluntad de usuarios y técnicos, para registrar el uso de los medios computacionales, para controlar el uso de las sesiones de usuario y para analizar el uso que se le da a los laboratorios en la Universidad Central “Marta Abreu” de las Villas.

Ante esta problemática existen varias soluciones, una de ellas se brinda en el presente trabajo y para su implementación se define el siguiente objetivo general:

Objetivo General

- Crear un sistema de software distribuido que registre los parámetros del usuario que haga uso de todas y cada una de las computadoras de la red UCLV y los almacene en una base de datos a la cual se conectará de forma remota para crear los registros históricos.

Lograr un correcto orden en las acciones que lleve a lograr este objetivo es indispensable, para ello se definen los siguientes objetivos específicos:

Objetivos Específicos

- Definir algunos aspectos sobre seguridad informática y evaluar herramientas de software para la administración, control y gestión de las redes informáticas.
- Programar una aplicación cliente que se ejecutará como servicio en las computadoras, para obtener algunos de los parámetros de las sesiones de usuario que hagan uso de las mismas.
- Crear y configurar una base de datos en función del servidor al cual se conectará el cliente de cada computadora para almacenar de forma histórica los datos obtenidos.
- Programar una aplicación para configurar los parámetros que el cliente necesita para la conexión con el servidor.
- Evaluar los resultados obtenidos a partir de la prueba del software.

El software registrará los parámetros del usuario que haga uso de de todas y cada una de las computadoras de una red informática en la UCLV y los almacenará en una base de datos a la cual se conectará de forma remota para crear los registros históricos. El sistema estará comprendido de una serie de tres programas, una aplicación cliente, una base de datos centralizada y un programa de análisis y visualización de datos. El cliente, instalado como servicio en las computadoras, obtendrá la hora de entrada al sistema, el nombre de usuario, el IP de la máquina y el nombre de la PC, almacenando estos parámetros en la base de datos remota. En caso de existir problemas con la conexión de red, el software almacenaría todos los parámetros en un fichero local y en la próxima conexión activa, enviará todos los datos del fichero y posteriormente los del usuario que abrió la nueva sesión.

La propuesta de creación y aplicación de esta utilidad de software que pudiera llamarse “Sistema Automático de Registro de Usuarios” o SARU por sus siglas, evitará la brecha de seguridad originada por el no cumplimiento de las responsabilidades de los usuarios y el técnico de un laboratorio, además permitirá controlar el uso de los medios computacionales y hacer estudios estadísticos del mismo, comprobando la eficiencia real en el uso de las computadoras. De forma teórica puede validar la aplicación de muchos de los conocimientos aprendidos en algunas de las asignaturas de la carrera relacionadas con el perfil computacional como programación y telemática.

El presente trabajo está estructurado en: resumen, introducción, capítulo 1, capítulo 2, capítulo 3, conclusiones, recomendaciones, bibliografía.

En el primer capítulo se tratarán los sistemas de manejo y administración de usuarios para redes informáticas, la necesidad de que las redes sean seguras y de tener un control y registro de los usuarios de las redes informáticas así como investigación sobre la existencia de herramientas de software que permitan registrar automáticamente a los usuarios. En el segundo capítulo se describen las características propias del software con que se pretende trabajar, haciendo énfasis en sus requisitos funcionales y tratando más explícitamente las ventajas que se obtienen de la instalación del software. En el tercer capítulo se evaluará el desempeño del sistema de software SARU durante un tiempo de prueba así como un análisis de su aplicabilidad y usos futuros.

CAPÍTULO 1. Los sistemas de manejo y administración de usuarios para redes informáticas.

1.1. Introducción al capítulo

En este capítulo se tratarán los sistemas de manejo y administración de usuarios para redes informáticas, haciendo énfasis en conceptos como: redes informáticas, redes de área local y profundizando en algunos de los referentes más importantes del tema a nivel mundial. Otros aspectos que trata el capítulo es la necesidad de que las redes sean seguras, cuáles son las violaciones más frecuentes en las redes informáticas, cuáles son los software más utilizados para la administración de redes, qué herramientas existen para gestionar usuarios en una red (dígase chequear el estado de los usuarios, qué usuarios, que niveles de privilegio). También se aborda la necesidad de tener un control y registro de los usuarios de las redes informáticas y la investigación sobre la existencia de herramientas de software que permitan registrar automáticamente a los usuarios. Además de un análisis de las herramientas que se utilizarán en el trabajo (QT*Creator* y el gestor de base de datos MySQL, así como el lenguaje de programación UML).

1.2. Las redes de área local y el entorno de trabajo

Según Jordi Adell (1998) una red informática es un conjunto interconectado de ordenadores, que ofrece a sus usuarios diversos servicios relacionados con las comunicaciones y el acceso a la información. Los ordenadores conectados aumentan su funcionalidad ya que, en primer lugar permiten compartir recursos y periféricos especializados y costosos como impresoras y escáneres, en segundo lugar, facilitan el acceso a enormes cantidades de información almacenada remotamente, en tercer lugar promueven la comunicación entre las personas y los grupos utilizando una amplia variedad de medios (texto, imágenes, audio, video). Finalmente, en cuarto lugar, son una excelente herramienta para difundir rápida y eficientemente información entre sus usuarios.

Para poder formar una red según lo planteado por Gilberto Díaz (2009) se requieren los siguientes elementos: hardware, software y protocolos. Los elementos físicos (hardware) se

clasifican en dos grandes grupos: dispositivos de usuario final (*hosts*) y dispositivos de red. Los dispositivos de usuario final incluyen las computadoras, impresoras, escáneres y demás elementos que brindan servicios directamente al usuario y los segundos son todos aquellos que conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación. Las redes de computadoras pueden clasificarse de múltiples maneras, según su direccionalidad, arquitectura, etc. Según su direccionalidad las redes pueden clasificarse como *simplex* o unidireccionales, un nodo transmite y el otro recibe; *half-dúplex* o bidireccionales, sólo un nodo transmite a la vez y *full-dúplex*, ambos nodos pueden transmitir datos al mismo tiempo. Por otra parte la estructura de las redes está definida según su arquitectura**.** Lo primero que caracteriza una red de área local es la manera en que se conectan las estaciones; es decir, la forma que adopta el medio compartido entre las mismas. Básicamente existen tres topologías posibles:

- Topología en estrella: La topología en estrella consiste en conectar cada ordenador a un punto central, que puede ser tan sencillo como una simple unión física de los cables. Cuando un ordenador pone una trama en la red, ésta aparece de inmediato en las entradas del resto de ordenadores. Aunque se han definido estándares para este tipo de redes, en la actualidad ya casi no existen, puesto que no aportan ninguna ventaja sobre el resto y sí muchos inconvenientes (Peterson and Davie 2003).

- Topología en bus: La topología en bus consiste en un cable al que se unen todas las estaciones de la red. Todos los ordenadores están pendientes de si hay actividad en el cable. En el momento en que un ordenador pone una trama, todos los ordenadores la reciben y chequean si son el destinatario de la misma. Si es así, se la quedan, en caso contrario, la descartan (Peterson and Davie 2003).

- Topología en anillo: La topología en anillo consiste en conectar cada ordenador a dos más, de manera que se forme un anillo. Cuando un ordenador quiere enviar una trama a otro, ésta debe pasar por todos los ordenadores que haya entre ellos: la circulación por el anillo es unidireccional (Peterson and Davie 2003).

Como ha planteado Antonio Bueno (2010) según el tamaño las redes de computadoras se clasifican en: LAN[1]: de 10 metros a 1 kilómetro, suelen usar *broadcast* y su velocidad va de 10 a 100 MBps. MAN[2]: tamaño máximo 10 kilómetros. WAN[3]: tamaño entre 100 y 1000 kilómetros. INTERNET: más de 10000 kilómetros.

Federico Reina Toranzo y Juan Antonio Ruiz Rivas (2006) explican por su parte que las redes LAN son redes privadas localizadas en un edificio o campus. Su extensión es de algunos kilómetros. Muy usadas para la interconexión de computadores personales y estaciones de trabajo. Se caracterizan por: tamaño restringido, tecnología de transmisión por lo general *broadcast*, alta velocidad y topología en bus. Son redes con baja latencia y baja tasa de errores. Cuando se utiliza un medio compartido es necesario un mecanismo de arbitraje para resolver conflictos. Son siempre privadas.

Así mismo, una LAN puede estar conectada con otras LANs a cualquier distancia por medio de líneas telefónicas y ondas de radio. Pueden ser desde dos computadoras, hasta cientos de ellas. Todas se conectan entre sí por varios medios y topologías, a la(s) computadora(s) que se encarga de llevar el control de la red que es llamada "servidor" y a las computadoras que dependen del servidor, se les llama "nodos" o "estaciones de trabajo". Los nodos de una red pueden ser PC´s[4] que cuentan con su propio CPU, disco duro y software y tienen la capacidad de conectarse a la red en un momento dado; o pueden ser PC´s sin CPU o disco duro y son llamadas "terminales tontas", las cuales tienen que estar conectadas a la red para su funcionamiento. Las LANs son capaces de transmitir datos a velocidades muy rápidas pero las distancias son limitadas (Toranzo and Rivas 2006).

Una mejora importante ha sido la aparición de las redes de área local inalámbricas (*wireless* LAN), en las que el enlace entre estaciones no se lleva a cabo por medio de cables, sino por medio de enlaces radioeléctricos. Las ventajas de este tipo de enlaces, en cuanto a

[1] Local Area Network

[2] Metropolitan Area Network

[3] World Area Network

[4] Personal Computers

movilidad y facilidad de instalación, son evidentes. En una red es imprescindible identificar los ordenadores que forman parte de la misma. Cuando un ordenador genera una trama para otro, además de los datos que le quiere enviar, le pone el identificador del ordenador (u ordenadores) destino y el suyo, para que el dispositivo que recibe la trama pueda saber quién se la ha enviado. Para construir una red local, se precisan básicamente dos cosas: hardware (tarjetas, cables, conectores) y un software que sea consciente de que existen diferentes máquinas conectadas y ofrezca los servicios necesarios para que las aplicaciones puedan aprovecharlo. Lo más lógico es que este software se integre en el sistema operativo y ofrezca a las aplicaciones la visión de la red como un recurso propio más (Elliott 2002).

Según Javier Fernández Rivera (2000) gracias al rápido desarrollo de las telecomunicaciones, el mundo está avanzando hacia una única y gran comunidad global. Bajo este nuevo concepto de comunidad global podemos encontrar refugiadas nuevas interpretaciones o conceptualizaciones de procesos tradicionales, como la educación, trabajo, economía y hasta la forma de hacer amigos. El Internet es uno de los máximos protagonistas de esta revolución tecnológica digital, debido a su rápida aceptación y propagación, donde las redes de computadoras se han extendido a niveles jamás antes pensados, trayendo con ello un alto desarrollo tecnológico pero también algunos serios problemas, como los fraudes informáticos y las brechas de seguridad, entre otros. La propagación del conocimiento y la educación cada día se va beneficiando de este vertiginoso avance técnico, mediante el cual se hace posible llegar a más personas y en menos tiempo.

1.3. Algunos aspectos sobre la seguridad en las redes informáticas

Como han planteado Johann Marcelo Márquez Barja y Walter Baluja García (2004) las redes de computadoras se han convertido en el soporte de cualquier entidad o institución que pueda considerarse de punta. Éstas, además de la tecnología que involucran, brindan múltiples servicios con calidad, los cuales conllevan a más y mejores prestaciones, obteniéndose beneficios para la producción y el desarrollo. El amplio desarrollo de las nuevas tecnologías informáticas está ofreciendo un nuevo campo de acción para las

conductas antisociales y delictivas manifestadas en formas imposibles de imaginar, ofreciendo la posibilidad de cometer delitos tradicionales en formas no tradicionales. La mayor parte del mundo informático desconoce la magnitud del problema con el que se enfrenta y, generalmente no se invierte ni el capital humano ni económico necesario para prevenir daños y/o pérdidas de información. Paradójicamente, existe una demanda constante y muy importante de seguridad informática que está esperando a que alguien las atienda. Aún así esta demanda queda muy por debajo con relación a la cantidad de ataques y desastres en la seguridad que padecen los sistemas informáticos y las redes de computadoras.

La política de seguridad y su implementación deben ser lo menos obstructivas posibles. Si la política de seguridad es demasiado restrictiva, o está explicada inadecuadamente, es muy probable que sea violada o desactivada. Al margen de cualquier tipo de política que se implemente, algunos usuarios tienen la tendencia a violarla. En ocasiones las violaciones a la política son evidentes; otras veces estas infracciones no son detectadas. Los procedimientos de seguridad que se establecen deben reducir al mínimo la posibilidad de que no se detecte una infracción de seguridad (Barja and García 2004).

Cuando se detecta una violación a la política de seguridad (Hoet, Cozzi et al. 2007), debe determinarse si esta ocurrió debido a la negligencia de un individuo, a un accidente o error, por ignorancia a la política vigente o si deliberadamente la política fue pasada por alto. En este caso la violación quizás haya sido efectuada no solo por una persona, sino por un grupo que a sabiendas realiza un acto de violación directa a la política de seguridad. En cada una de estas circunstancias la ley debe contar con lineamientos acerca de las medidas que se deben tomar.

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones. La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización. La propia complejidad de la

red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. En medio de esta variedad, han ido aumentando las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas. Además de las técnicas y herramientas criptográficas, un componente muy importante para la protección de los sistemas consiste en la atención y vigilancia continua y sistemática por parte de los responsables de la red (Elliott 2002).

Resulta claro que proponer o identificar una política de seguridad requiere de un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

Para llevar a cabo el seguimiento de una correcta política de seguridad informática se debe realizar primeramente una evaluación del factor humano que intervienen, teniendo en cuenta que éste es el punto más vulnerable en toda la cadena de seguridad, de los mecanismos con que se cuentan para llevar a cabo los procesos necesarios (mecanismos técnicos, físicos ó lógicos), el ambiente en que se desempeña el sistema, las consecuencias que pueden traer aparejados los defectos en la seguridad (pérdidas físicas, pérdidas económicas, en la imagen de la organización, etc.), y cuáles son las amenazas posibles (Hoet, Cozzi et al. 2007).

Una vez evaluado todo lo anterior, se origina un programa de seguridad, que involucra los pasos a tomar para poder asegurar el umbral de seguridad que se desea. Luego, se pasa al plan de acción, que es cómo se va a llevar a cabo el programa de seguridad. Finalmente, se redactan los procedimientos y normas que permiten llegar a buen destino (Hoet, Cozzi et al. 2007).

Con el propósito de asegurar el cumplimiento de todo lo anterior, se realizan los controles y la vigilancia que aseguran el fiel cumplimiento de los tres puntos antes expuestos. Con el objeto de confirmar el buen funcionamiento de lo creado, se procede a simular eventos que atenten contra la seguridad del sistema. Como el proceso de seguridad es un proceso dinámico, es necesario realizar revisiones al programa de seguridad, al plan de acción y a los procedimientos y normas. Es claro que el establecimiento de políticas de seguridad es un proceso dinámico sobre el que hay que estar actuando permanentemente, de manera tal

que no quede desactualizado; que, cuando se le descubran debilidades, éstas sean subsanadas y, finalmente, que su práctica por los integrantes de la organización no caiga en desuso (Hoet, Cozzi et al. 2007).

Limitándose a la seguridad propiamente dicha, los riesgos pueden ser múltiples. El primer paso es conocerlos y el segundo es tomar decisiones al respecto; conocerlos y no tomar decisiones no tiene sentido.

Hoet, Cozzi y otros (2007), en su obra plantean que "*Hackers", "crakers",* entre otros, han hecho aparición en el vocabulario ordinario de los usuarios y de los administradores de las redes. El *hacker* que intenta acceder a los sistemas sobre todo para demostrar (a veces, para demostrarse a sí mismo/a) qué es capaz de hacer, al superar las barreras de protección que se hayan establecido. Por otra parte están los virus pero que afortunadamente, este riesgo es menor en la actualidad comparado con años atrás. Existe, de todas maneras, un riesgo constante porque de forma continua aparecen nuevas modalidades, que no son detectadas por los programas antivirus hasta que las nuevas versiones los contemplan. Un riesgo adicional es que los virus pueden llegar a afectar a los grandes sistemas, sobre todo a través de las redes, pero esto es realmente difícil por las características y la complejidad de los grandes equipos y debido a las características de diseño de sus sistemas operativos.

Existen también otros modos de ataques que podrían ocurrir más frecuentemente en las redes de información. El "*Denial of Service*" es un tipo de ataque cuya meta fundamental es la de negar el acceso del atacado a un recurso determinado o a sus propios recursos. Cabría tener en cuenta que, el uso ilegítimo de recursos puede también dar lugar a la negación de un servicio. Por ejemplo, un "*hacker*" puede utilizar un área del FTP anónimo como lugar para salvar archivos, consumiendo, de esta manera, espacio en el disco y generando tráfico en la red (Hoet, Cozzi et al. 2007).

Otra de las violaciones a las que puede ser vulnerable cualquier usuario son los servicios de correo. El e-mail *bombing* consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando el buzón del destinatario el *spamming*, que es una variante del e-mail *bombing*, se refiere a enviar el e-mail a centenares o millares de usuarios e, inclusive, a listas de interés. El *spamming* puede resultar aún más perjudicial si los destinatarios contestan el mail, haciendo que todos reciban la respuesta. Puede, además,

ocurrir inocentemente como resultado de enviar un mensaje a la lista y no darse cuenta de que la lista lo distribuye a millares de usuarios, o como resultado de mala configuración de un auto respondedor, por ejemplo el "*vacation*". El e-mail *bombing/spamming* se puede combinar con el e-mail *spoofing* – que altera la identidad de la cuenta que envía el *mail*, logrando que sea más difícil determinar quién está enviando realmente el *mail* (Toranzo and Rivas 2006).

Estos son algunos de entre los muchos ejemplos de prácticas ilícitas y violaciones informáticas que sistemáticamente se llevan a cabo, por lo que es necesario mantener un control de las redes de computadoras y de la práctica continua de las políticas de seguridad. En la actualidad se dispone de herramientas para limitar, impedir o frustrar conexiones indebidas a los recursos de la red. Para ello se pueden realizar auditorías de los recursos y llevar un registro de los accesos a cada uno de ellos. Si un usuario utilizara algún recurso al que no tiene derecho, se podría detectar o al menos registrar el evento. Las auditorías se pueden realizar sobre conexiones, accesos, utilización de dispositivos de impresión, uso de ficheros o aplicaciones concretas (Hoet, Cozzi et al. 2007).

1.4. Las herramientas de software para la administración de redes

Según Leonardo Hoet, Rodolfo Cozzi, Rodolfo Baader y Rodrigo Seguel (2007) se han creado muchos métodos para controlar el uso que se da a los medios computacionales y controlar el acceso a la red. Existen varias herramientas de software para controlar el ingreso a una red de área local, para permitir la protección ante posibles ataques y también realizar un seguimiento a la red cuando se cree que alguna de las máquinas ha sido comprometida. De esta manera se hace más fácil controlarlas y administrarlas. Estos autores describen algunos de estos métodos, entre los que se encuentran:

- **Tcp-wrappers**: es un software de domino público. Su función principal es proteger a los sistemas de conexiones no deseadas a determinados servicios de red, permitiendo a su vez ejecutar determinados comandos ante determinadas acciones de forma automática. Con este paquete podemos monitorear y filtrar peticiones entrantes a distintos servicios TCP-IP.

- **Netlog**: es un software de dominio público y una herramienta que genera trazas referentes a servicios basados en IP (TCP, UDP) e ICMP, así como tráfico en la red (los programas pueden ejecutarse en modo promiscuo) que pudiera ser "sospechoso" y que indicara un posible ataque a una máquina (por la naturaleza de ese tráfico). El paquete está formado por el siguiente conjunto de programas:
    - **tcplogger**: este programa escucha todos los servicios sobre TCP, dejando una traza de cada servicio en un archivo de trazas, indicando la hora, la máquina origen y el puerto de esa conexión.
    - **udplogger**: es semejante al anterior, pero para los servicios sobre UDP. Los archivos que generan estas dos herramientas pueden ser útiles también para detectar ataques de tipo SATAN o ISS, ya que en los archivos de trazas se aprecian intentos de conexión muy cortos en el tiempo a puertos (TCP o UDP) de forma consecutiva.
    - **icmplogger**: se encarga de trazar el tráfico de ICMP. Estos programas pueden guardar su información en ASCII o en formato binario.
    - **etherscan**: es una herramienta que monitorea la red buscando ciertos protocolos con actividad inusual, como puedan ser conexiones tftp, comandos en el puerto de sendmail (25 tcp) como vrfy, expn, algunos comandos de rpc como rpcinfo, peticiones al servidor de NIS (algunas herramientas utilizan este tipo de servidores para obtener el archivo de password, ej.: ypx), peticiones al demonio de mountd.
- **Nstat:** esta herramienta que originariamente fue diseñada para obtener estadísticas de uso de varios protocolos, se puede utilizar para detectar cambios en los patrones de uso de la red, que nos puedan hacer sospechar que algo raro está pasando en la misma**.**
- **Aarhus:** también es una herramienta de dominio público que permite auditar el tráfico IP que se produce en nuestra red, mostrándonos todas las conexiones del tipo indicado que descubre. Este programa escucha directamente la interfaz de

red de la máquina y su salida es mandada bien a un archivo de trazas o a otra máquina para allí ser leída.

- **Tcpdump**: es un software de dominio público que imprime las cabeceras de los paquetes que pasan por una interfaz de red. Este programa es posible ejecutarlo en modo promiscuo con lo que tendremos las cabeceras de los paquetes que viajan por la red. Tanto en la captura como en la visualización de la información, es posible aplicar filtros por protocolo (TCP, UDP, IP, ARP, RARP...), puertos (en este caso el puerto puede ser un número o un nombre especificado en el archivo/etc./services), direcciones fuente, direcciones destino, direcciones de red, así como realizar filtros con operadores (=, <, >, !=, and, not,...)

- **SATAN** (Security Administrator Tool for Analyzing Networks): es un software de dominio público que chequea máquinas conectadas en red y genera información sobre el tipo de máquina, qué servicios da cada máquina y avisa de algunos fallos de seguridad que tengan dichas máquinas

- **ISS** (Internet Security Scanner): es una herramienta de la cual existe versión de dominio público que chequea una serie de servicios para comprobar el nivel de seguridad que tiene esa máquina. ISS es capaz de chequear una dirección IP o un rango de direcciones IP.

- **Courtney**: es un software de dominio público que sirve para identificar la máquina origen que intenta realizar ataques mediante herramientas de tipo SATAN

- **Gabriel**: software que permite detectar "ataques" como los generados por SATAN. Identifica el posible ataque y de forma inmediata lo notifica al administrador o responsable de seguridad. La notificación se puede realizar de varias formas (e-mail, cu, archivo de trazas). Este programa existe, en este momento, para SunOs 4.1.x y Solaris, y está formado por un cliente y un servidor.

- **Nocol** (Network Operations Center On-Line): es un conjunto de programas de monitoreo de sistemas y redes. El software es un conjunto de agentes que recogen información y escriben la salida en un formato que se puede, luego, procesar. Cada dato procesado recibe el nombre de evento y cada evento tiene asociado una gravedad.

El sistema operativo Windows, en sus diferentes versiones, también posee algunos mecanismos para controlar el estado y la actividad de los usuarios, como el registro de eventos en cada sesión de usuario y el administrador remoto. El registro de Windows o registro del sistema es la base de datos que almacena las configuraciones y opciones del sistema operativo Microsoft Windows en sus versiones de 32 bits, 64 bits y Windows Mobile. Algunos lo definen como una base de datos jerárquica, pero esta definición no es muy exacta. El registro de Windows contiene información y configuraciones de todo el hardware, software, usuarios, y preferencias de la PC. Si un usuario hace cambios en las configuraciones del "Panel de control", en las asociaciones de ficheros, en las políticas del sistema o en el software instalado, los cambios se reflejan y almacenan en el registro. El registro mantiene esta información en forma de árbol, estableciendo un orden por el cual deben acceder el sistema operativo u otros programas, como las preferencias de usuario (perfiles), hojas de ajustes para directorios e iconos de programas, enumeración de hardware instalado y los puertos usados. El registro reemplaza los archivos de inicialización y configuración legados de Windows 3.x y MS-DOS (.ini), *autoexec.bat* y config.sys. El registro se almacena en varios ficheros que, dependiendo de la versión de Windows, se ubican en diferentes lugares dentro del sistema local, excepto ***NTuser*** (o archivo de usuario), que puede ser ubicado en otra máquina para permitir perfiles móviles. El registro de Windows tiende a crecer desmesuradamente cuando se instalan y desinstalan programas, con el paso del tiempo, etc., con lo que se produce un aumento en el tamaño del registro y posiblemente errores en entradas de aplicaciones obsoletas. Por ello, existen varias utilidades para optimizar el registro como TuneUp Utilities, CCleaner, que buscan y eliminan estas entradas erróneas y permiten compactar el registro completo. De esta manera, se reduce el tiempo de carga de la PC (Hoet, Cozzi et al. 2007).

Existen otros programas que tienen entre sus objetivos acciones similares a los mencionados anteriormente:

- **Remote Desktop Protocol** (RDP): es un protocolo propietario desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación entre un terminal (mostrando la información procesada que recibe del servidor) y un servidor Windows (recibiendo la información dada por el usuario en el terminal mediante el ratón ó el teclado). El modo de funcionamiento del protocolo es sencillo. La información gráfica que genera el servidor es convertida a un formato propio RDP y enviada a través de la red al terminal, que interpretará la información contenida en el paquete del protocolo para reconstruir la imagen a mostrar en la pantalla del terminal. Una vez iniciada la sesión desde un punto remoto el ordenador servidor mostrará la pantalla de bienvenida de Windows, no se verá lo que el usuario está realizando de forma remota. Tiene distintos tipos de aplicaciones: se utiliza frecuentemente para el acceso remoto en la administración de equipos, pero también es cada vez más utilizado en la gestión de servicios de terminal o clientes ligeros (*thin clients*).

- **Apple Remote Desktop**: es una buena manera de administrar los ordenadores Mac de una red. Con él se pueden distribuir programas, ofrecer ayuda en directo a usuarios finales, crear informes pormenorizados del uso de programas y equipos, así como automatizar tareas de administración rutinarias. Apple Remote Desktop también facilita la elaboración de informes sobre uso de aplicaciones, historial de navegación, inventarios y demás. Se pueden elaborar inventarios en los que figuren incluso equipos portátiles que no estén conectados a la red, y los resultados quedan guardados en la base de datos SQL incluida de serie para facilitar el acceso.

- **Hyena**: es una herramienta de administración de redes diseñada para simplificar y centralizar las tareas cotidianas de administración de redes. Proporciona nuevas habilidades para la gestión de los sistemas. Estas funcionalidades se consiguen gracias a una herramienta simple, centralizada y de fácil utilización.

Hyena le permite realizar una administración avanzada de: usuarios y grupos, programación de trabajos, discos y ficheros, servidores, eventos, impresoras y trabajos de impresión, informes. Está diseñado para simplificar y centralizar las tareas cotidianas de administración, proporcionando nuevas habilidades para la administración del sistema. Además es de fácil utilización.

- **ObserveIT**: brinda conformidad con la seguridad, generación y envío automático de informes detallados que rastrean cada acceso a sus servidores y bases de datos empresariales. Supervisión del acceso de agentes remotos, resolución de problemas instantáneamente, con su uso se puede descubrir la causa original de los cambios en la configuración de los sistemas utilizando la búsqueda detallada y la reproducción de vídeo de la sesión. Compatible con todas las formas de acceso tanto a consola como en remoto, con soporte para Citrix, Terminal Services, Escritorio Remoto, PC-Anywhere, VDI, VMware, VNC, NetOp, DameWare y muchos más. ObserveIT es totalmente transparente respecto al protocolo y la aplicación del cliente. Con un administrador de reglas muy flexible permite la inclusión o exclusión de políticas de grabación en función del usuario, grupos de usuarios, aplicaciones, archivos y tipos de archivos, o eventos específicos de teclado. Encuentra la sesión exacta que está buscando mediante búsquedas por texto libre en campos de metadatos como nombre del servidor, nombre de usuario, aplicaciones utilizadas, archivos accedidos, etc. Genera informes detallados (por ejemplo: "Mostrar todas las sesiones que hayan accedido al registro o a hojas de cálculo financieras en cualquier servidor en los últimos 10 días"). Permite la personalización de los filtros, la agrupación y la clasificación de los informes, exportación a XML/Excel y programación del envío automatizado de los informes (Castellano 2008).
- **Spector 360**: es el producto estrella de SpectorSoft. Registra los *websites* visitados, correos recibidos y enviados, chats y mensajería instantánea, texto ingresado, archivos enviados, documentos impresos y aplicaciones ejecutadas. Spector 360 incluso permite grabar un "video" de la actividad del usuario continuamente o bien en el caso de detectar actividad sospechosa.

Spector 360 está diseñada para organizaciones medianas y grandes con redes Windows o Macintosh (Hoet 2010).

- **NetSupport Manager**: es una solución de control remoto de PCs que permite la gestión remota de ordenadores y servidores a través de redes locales LAN e Internet. Combina el control remoto con herramientas para realizar el inventario tanto de software como de hardware de las máquinas remotas. También permite ejecutar y terminar aplicaciones de forma remota, gestionar los servicios de Windows y transferir ficheros a múltiples ordenadores de manera simultánea. NetSupport Manager es una de las aplicaciones más seguras del mercado ya que incluye opciones para proteger los datos y los accesos a ordenadores. También ofrece diversas herramientas de soporte como ayuda, entre ellas informes dinámicos de inventario de hardware y software, herramientas de gestión de sistemas y soporte de audio completo. Incluso ofrece la posibilidad de ver la pantalla de un operario en tiempo real a cualquier número de sistemas conectados como una herramienta de formación integrada. NetSupport Manager incluye compatibilidad total con los sistemas Vista y Windows 7 de 32 y 64 bits (Salvatore 2011).

1.5. Administración de usuarios

Como plantea Esteban Torres (2007) la persona encargada de las tareas de administración, gestión y seguridad de los equipos conectados a la red y de la red en su conjunto, tomada como una unidad global, es el administrador. Este conjunto abarca tanto a servidores como a estaciones clientes, el hardware y el software de la red, los servicios de red, las cuentas de usuarios y las relaciones de la red con el exterior.

El acceso a la red es el primer aspecto que debe tenerse en cuenta una vez instalado el software definido. Los servicios que ofrece una estación conectada a la red pueden ser utilizados por cualquier usuario que utilice esa estación de trabajo. El orden y la confidencialidad de cada puesto de trabajo o proyecto requieren un sistema que garantice que cada persona tenga acceso a sus datos y aplicaciones, evitando que otros usuarios

puedan ser perjudicados por el uso indebido del sistema o por la falta de una intención recta.

Cualquier administrador de sistema o de red tiene que tener en cuenta el posible asalto a la red por parte de personas que se dedican a este tipo de actividades, sabiendo que el ataque puede venir tanto de afuera como desde dentro de su organización. El modo de hacer distinciones entre los diferentes usuarios, implica la confección de cuentas de acceso personalizadas y un sistema de validación o autenticación que permite o impide el acceso de los usuarios a los recursos disponibles. El primer problema al que hay que hacer frente en el diseño de la estructura lógica de la red consiste en la asignación de nombres y direcciones de red a todos los ordenadores que vayan a convivir en ella. Tanto los nombres como las direcciones han de ser únicos en la red, pues identifican a los equipos (Torres 2007).

Las cuentas de usuario son el modo habitual de personalizar el acceso a la red. Así toda persona que utilice la red con regularidad debe tener una cuenta de acceso. Para que el control de este acceso sea suficientemente bueno, las cuentas deben ser personales, es decir, dos usuarios no deban compartir la misma cuenta. La cuenta proporciona el acceso a la red y lleva asociada todas las características y propiedades de los usuarios útiles en las labores de administración. Las cuentas de usuarios suelen tener parámetros semejantes a los que a continuación se describen, aunque cada sistema operativo de red tiene los suyos propios.

- Nombre de usuario: Es el nombre único atribuido a cada usuario y que utiliza para identificarse en la red.
- Contraseña: Es la cadena de caracteres que codifica una clave secreta de acceso a la red para cada usuario.
- Nombre completo del usuario: Es una cadena de caracteres con el nombre completo del usuario.
- Horario permitido de acceso a la red: Es un campo que describe las horas y los días en que el usuario tiene acceso a la red.
- Estaciones de inicio de sesión: Describe el nombre de los equipos desde los que el usuario puede presentarse en la red.

- Caducidad: Describe la fecha en que la cuenta expira. Es útil para cuentas de usuario que solo requieren acceso por períodos de tiempo concretos.
- Directorio particular: Es el lugar físico dentro del sistema de ficheros de la red en donde el usuario puede guardar sus datos.
- Archivo de inicio de sesión: Permiten configurar un conjunto de comandos que se ejecutaran automáticamente al inicio de la sesión de la red.
- Otros parámetros: Algunos sistemas operativos permiten configurar otros parámetros como son los perfiles de usuario, la cantidad de disco de que dispondrá cada usuario, disponibilidad de memoria central, tiempo de CPU, capacidad de entrada/salida, etc.

Además de las cuentas que pueden definir los administradores de la red, los sistemas operativos de red poseen unas cuentas por defecto con una funcionalidad específica, que normalmente no se pueden borrar, aunque sí modificar y desactivar. Una vez que se ha identificado a cada usuario con acceso a la red, se puede arbitrar sus derechos de acceso. Corresponde al administrador determinar el uso de cada recurso de la red o las operaciones que cada usuario puede realizar en cada estación de trabajo (Torres 2007).

1.6. Necesidad de fortalecer la seguridad mediante el control de usuarios

Explica José Pino Díaz (2009) que a fin de cuentas, los usuarios de un sistema son una parte a la que no hay que olvidar ni menospreciar. Siempre hay que tener en cuenta que la seguridad comienza y termina con personas. Obtener de los usuarios la concientización de los conceptos, usos y costumbres referentes a la seguridad, requiere tiempo y esfuerzo. Que los usuarios se concienticen de la necesidad y, más que nada, de las ganancias que se obtienen implementando planes de seguridad, exige trabajar directamente con ellos, de tal manera que se apoderen de los beneficios de tener un buen plan de seguridad. De esta forma, ante cualquier problema, es muy fácil determinar dónde se produjo o de dónde proviene.

La implementación de medidas de seguridad, es un proceso técnico administrativo. Como este proceso debe abarcar toda la organización, sin exclusión alguna, ha de estar

fuertemente apoyado por el sector gerencial, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria. Hay que tener muy en cuenta la complejidad que suma a la operatoria de la organización la implementación de estas medidas. Será necesario sopesar cuidadosamente la ganancia en seguridad respecto de los costos administrativos y técnicos que se generen (Díaz 2009).

1.7. Análisis

Todas las herramientas de administración de redes revisadas en la sección 1.4 son muy útiles en cuanto a la gestión integral del trabajo de una red informática, en conjunto todos estos programas se pueden dividir en dos categorías según sus características:

- *Sniffers* para analizar el tráfico de datos en la red.
- Administración remota.
    - Visualización de escritorios remotos.
    - Conocimiento de los principales parámetros de funcionamiento.
    - Conocimiento de los principales parámetros de las sesiones de usuario.

A pesar de sus extensas posibilidades en conjunto, ninguno de ellos ofrece posibilidad de:

- Obtener de forma automatizada y organizada el registro, en un sistema de base de datos, de los identificadores de las computadoras, los usuarios, la estampa de tiempo para diferentes eventos y los diferentes procesos que caracterizan una sesión de usuario.
- Forma de procesar estadísticamente estos datos, para obtener registros del uso de los componentes de la red, registros de la eficiencia en el uso, el tiempo de uso de las computadoras, entre otros parámetros importantes que permiten por ejemplo: evaluar el desempeño de la red, el cumplimiento del proceso docente educativo o la identificación de violaciones de seguridad y de los protocolos establecidos para el uso de los medios computacionales.

La solución a esta problemática se encuentra en la creación de un software que permita monitorear los parámetros de las sesiones de usuario, de forma automática y en conjunto para todas las computadoras que forman parte de una red local. Como valor agregado debe poseer una herramienta para el procesamiento de los datos almacenados.

1.8. Evaluación de las herramientas de software para el trabajo

Las principales herramientas que se utilizaron en el trabajo que aquí se describe fueron: el entorno de programación QTCreator y el gestor de base de datos MySQL, así como el entorno de diseño BOUML para diseñar y describir técnicamente los módulos de software.

QTCreator utiliza el *framework* Qt que vio la luz de forma pública por primera, vez según Oscar Andrés Vivas Albán (2010), en el año 1995. Fue desarrollado, como respuesta a la necesidad de disponer de un GUI[5] para una aplicación C++ multiplataforma orientado a objetos. La GUI es la parte gráfica de un programa que permite a un usuario interactuar con este. Debido a que constituye la primera toma de contacto de un sistema por parte del usuario, es necesario que sea agradable y con gran facilidad de uso para que éste se lleve una primera impresión positiva del software. La creación de GUIs siempre ha sido y sigue siendo un tema clave, que puede incluso llegar a tener un impacto mayor que otros factores a la hora de definir el éxito de un producto en el mercado. Interfaces innovadoras, interactivas y creativas, caracterizan a Qt.

En la última década, Qt ha pasado de ser un producto usado por unos pocos desarrolladores especializados, a un producto usado por miles de desarrolladores *open source* en todo el mundo, por lo que el futuro de esta tecnología es hoy día muy prometedor. Qt es una tecnología en auge que nos proporciona un juego de herramientas y elementos gráficos para la creación de interfaces y aplicaciones multiplataforma. Actualmente cuenta con un gran éxito y una gran implementación en diferentes ámbitos, que van desde las aplicaciones de escritorio hasta los sistemas electrónicos industriales y empotrados (Albán 2010).

[5] Interfaz gráfica de ususario.

Según David González Gutiérrez (2008/09) el paquete Qt integra herramientas de desarrollo y soporte tales como QtDesigner que es una herramienta de desarrollo que permite crear interfaces graficas de usuario, además proporciona un conjunto de componentes estándar y un mecanismo de conexión llamado *signal-slot*, con el que se conectan eventos de la interfaz con la lógica de programa que han de soportar. QtAssistant que es un componente de Qt que permite navegar por la documentación, en forma de páginas HTML[6], e implementa opciones de búsqueda y de extensión. QtLinguist, que propicia traducción rápida de programas, así como librerías de clases auxiliares a Qt y también incluye el compilador Gcc-MinGW, este último es una implementación del compilador Gcc para la plataforma Windows, que además incluye un conjunto de la API[7] de Win32, permitiendo un desarrollo de aplicaciones nativas para esa plataforma y pudiendo generar tanto ejecutables como librerías usando la API de Windows.

QtCreator es un excelente IDE[8] multiplataforma para desarrollar aplicaciones en C++ de manera sencilla y rápida. Como su nombre lo indica, está basado en la librería Qt y cuenta con las siguientes características principales (Gutiérrez 2008/09):

- Editor avanzado para C++.
- Diseñador de formularios (GUI) integrado.
- Herramientas para la administración y construcción de proyectos.
- Completado automático.
- Depurador visual.
- Además soporta los lenguajes: C#/.NET Languages (Mono), Python: PyQt y PySide, Ada, Pascal, Perl, PHP y Ruby.
- Ayuda sensible al contexto integrado.

[6] Hyper text markup language.

[7] Aplication program interface.

[8] Integrate development invironment.

MySQL según expone Oscar Pérez Mora (2010), es un sistema gestor de bases de datos (SGBD, DBMS[9] por sus siglas en inglés) muy conocido y ampliamente usado por su simplicidad y notable rendimiento. Aunque carece de algunas características avanzadas disponibles en otros SGBD del mercado, es una opción atractiva tanto para aplicaciones comerciales, como de entretenimiento precisamente por su facilidad de uso y tiempo reducido de puesta en marcha. Esto y su libre distribución en Internet bajo licencia GPL le otorgan como beneficios adicionales (no menos importantes) contar con un alto grado de estabilidad y un rápido desarrollo.

MySQ*L* es un SGBD que ha ganado popularidad por una serie de atractivas características:

• Está desarrollado en C/C++.

• Se distribuyen ejecutables para cerca de diecinueve plataformas diferentes.

• La API se encuentra disponible en C, C++, Eiffel , Java, Perl, PHP, Python, Ruby y TCL.

• Está optimizado para equipos de múltiples procesadores.

• Es muy destacable su velocidad de respuesta.

• Se puede utilizar como cliente-servidor o incrustado en aplicaciones.

• Cuenta con un rico conjunto de tipos de datos.

• Soporta múltiples métodos de almacenamiento de las tablas, con prestaciones y rendimiento diferentes para poder optimizar el SGBD a cada caso concreto.

• Su administración se basa en usuarios y privilegios.

• Se tiene constancia de casos en los que maneja cincuenta millones de registros, sesenta mil tablas y cinco millones de columnas.

• Sus opciones de conectividad abarcan TCP/IP, *sockets* UNIX y *sockets* NT, además de soportar completamente ODBC.

• Los mensajes de error pueden estar en español y hacer ordenaciones correctas con palabras acentuadas o con la letra ’ñ’.

• Es altamente confiable en cuanto a estabilidad se refiere.

Para todos aquellos que son adeptos a la filosofía de UNIX y del lenguaje C/C++, el uso de MySQL les será muy familiar, ya que su diseño y sus interfaces son acordes a esa filosofía: “crear herramientas que hagan una sola cosa y que la hagan bien”. MySQL tiene como

[9] Data base manage system.

principal objetivo ser una base de datos fiable y eficiente. Ninguna característica es implementada en MySQL si antes no se tiene la certeza que funcionará con la mejor velocidad de respuesta y, por supuesto, sin causar problemas de estabilidad. La influencia de C/C++ y UNIX se observa de igual manera en su sintaxis. Por ejemplo, la utilización de expresiones regulares, la diferenciación de funciones por los paréntesis, los valores lógicos como 0 y 1, la utilización del tabulador para completar sentencias, por mencionar algunos (Mora 2010).

UML es una especificación de notación orientada a objetos. Divide cada proyecto en un número de diagramas que representan las diferentes vistas del proyecto y estos a su vez representan la arquitectura del proyecto. Intenta solucionar el problema de propiedad de código que se da con los desarrolladores, al implementar un lenguaje de modelado común para todos los desarrollos se crea una documentación también común, que cualquier desarrollador con conocimientos de UML será capaz de entender, independientemente del lenguaje utilizado para el desarrollo. Es ahora un estándar, no existe otra especificación de diseño orientado a objetos, ya que es el resultado de las tres opciones existentes en el mercado. Su utilización es independiente del lenguaje de programación y de las características de los proyectos, ya que UML ha sido diseñado para modelar cualquier tipo de proyectos, tanto informáticos como de arquitectura, o de cualquier otro ramo. Presenta las siguientes características (Mora 2010):

- Mejores tiempos totales de desarrollo (de 50 % o más).
- Modelar sistemas (y no sólo de software) utilizando conceptos orientados a objetos.
- Establecer conceptos y artefactos ejecutables.
- Encaminar el desarrollo del escalamiento en sistemas complejos de misión crítica.
- Crear un lenguaje de modelado utilizado tanto por humanos como por máquinas.
- Mejor soporte a la planeación y al control de proyectos.
- Alta reutilización y minimización de costos.

1.9. Consideraciones finales del capítulo

El mundo está avanzando hacia una única y gran comunidad global bajo la cual se refugian nuevas interpretaciones o conceptualizaciones de procesos tradicionales, como la educación, trabajo, economía y hasta la forma de hacer amigos. La propagación del conocimiento y la educación cada día se va beneficiando de este vertiginoso desarrollo tecnológico, mediante el cual se hace posible llegar a más personas y en menos tiempo.

Las redes de computadoras se han convertido en el soporte de cualquier entidad o institución que pueda considerarse de punta, el amplio desarrollo de las nuevas tecnologías informáticas está ofreciendo un nuevo campo de acción para las conductas antisociales y delictivas manifestadas en formas antes imposibles de imaginar, ofreciendo la posibilidad de cometer delitos tradicionales en formas no tradicionales.

Existen muchos métodos y varias herramientas de software para controlar el uso que se da a los medios computacionales, para controlar el ingreso a una red de área local, permitir la protección ante posibles ataques y también realizar un seguimiento a la red.

Ante situaciones que comprometan la seguridad de las redes de computadoras se impone entonces la necesidad de ofrecer otro mecanismo que respalde la seguridad informática, en este caso un sistema de software que ofrecerá un mecanismo de control y gestión de la red.

CAPÍTULO 2. El Sistema SARU

2.1. Introducción al capítulo

En este capítulo se abordan temas referentes a las características propias del software creado como parte del trabajo, haciendo énfasis en sus requisitos funcionales y tratando más explícitamente las ventajas que se obtienen de la instalación del mismo. En el mismo ámbito se tratará la arquitectura del sistema, la descripción funcional del los módulos del software a través de diagramas de clase utilizando lenguaje de programación UML[10], y la interactividad y tolerancia ante los fallos que puedan suceder.

2.2. Requisitos funcionales del sistema

Las fallas de seguridad provenientes tanto del interior del sistema como del exterior, son un peligro que a diario pueden perjudicar el trabajo de cualquier persona o entidad. La propia complejidad de una red informática es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. Con el "Sistema Automático de Registro de Usuarios" o SARU por sus siglas lo que se pretende es crear una herramienta de software con la cual se pueda conocer en cualquier momento los parámetros de una o varias sesiones de usuario y poder obtener información de lo que se realiza o se ha realizado en cada una de las PC.

Cómo primer paso en la creación de este programa se establecieron un conjunto de requisitos funcionales a través de los cuales se pudo definir la arquitectura del sistema y la mejor funcionalidad de cada módulo.

- El programa se ejecutará como servicio en las computadoras.
- El programa obtendrá el nombre de usuario de la sesión que se inicie.

[10] Lenguaje de modelación unificado.

- El programa obtendrá la hora y fecha de entrada a la sesión de usuario.
- El programa obtendrá el número IP de la máquina donde se inicia la sesión de usuario.
- El programa obtendrá el nombre de la máquina donde se inicia la sesión de usuario.
- El programa enviará todos los parámetros a una base de datos de forma remota.
- En caso de existir problemas con la conexión a la red, el software almacenará todos los parámetros en un fichero local y en la próxima conexión activa, enviará todos los datos del fichero y posteriormente los del usuario que abrió la sesión a la base de datos.
- El programa posibilitará un procedimiento de seguridad para la detección de delitos informáticos y ofrecerá una herramienta que permita procesar el uso de los medios computacionales.

2.3. Definición de la arquitectura del sistema

En consonancia con los requisitos funcionales establecidos, para la solución de software planteada, se definió la arquitectura del sistema como **tres programas diferentes**, cada uno con un objetivo específico pero que contribuyen como un solo sistema a la solución general del trabajo. La figura 2.1 muestra cómo funcionaría el sistema de software SARU dividido en sus tres aplicaciones.

El primer programa instalado como cliente en las máquinas a las cuales el usuario tendrá acceso, se diseñó sin interfaz gráfica y se ejecuta de forma automática como un servicio, obteniendo con el inicio de cada sesión los parámetros característicos de cada usuario (nombre de usuario, fecha y hora de entrada, IP de la máquina, nombre de la PC), que luego serán almacenados en una base de datos.

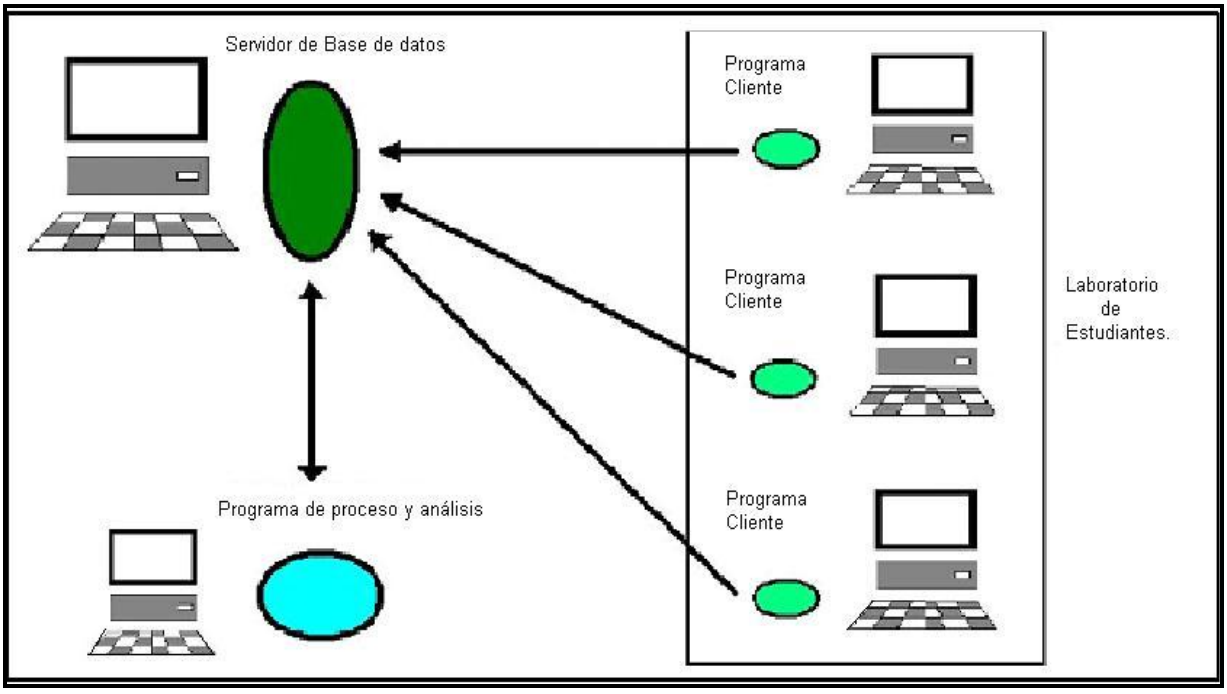

Figura 2.1 Esquema funcional de SARU.

La base de datos por su parte almacenará de manera organizada, automática y en forma de registros históricos los parámetros obtenidos, los datos se guardarán en una tabla, una columna para cada parámetro que caracteriza la sesión se usuario.

El último programa, diseñado con una interfaz gráfica de usuario, permite procesar y visualizar los datos registrados, este programa se comunicará con la base de datos para obtener la información a través de consultas SQL.

2.4. Descripción funcional de los módulos

El software SARU está constituido en realidad por tres programas, los cuales interactúan para funcionar como uno solo. A continuación se explican sus características y relaciones a través del lenguaje de programación UML posibilitando la comprensión del sistema de software, dividido en los módulos que lo integran.

2.4.1. Módulo cliente SARU

El primer programa de SARU, es el llamado “programa cliente” del cual se muestra su arquitectura en la figura 2.2. Aquí se puede observar el diagrama de clases de la aplicación.

La clase principal contiene dos objetos más, que permiten el funcionamiento del cliente. El primero de ellos es el objeto "**parametros**" y es del tipo de la clase **parametrosUsuario** la cual contiene las funciones necesarias para que el programa se ejecute sin dificultad. La función **detectarUsuario** detectará al usuario que se conecte a la PC, la función **detectarIP** detectará el IP de la máquina, la función **detectarTiempoEnt**, detectará el tiempo de entrada. El segundo de los objetos que tiene la clase principal es "**conexion**" que es del tipo **baseDatosCxn**. El objeto conexión le permitirá al cliente instalado en las máquinas a través de las funciones **conectar**, **insertar** y **desconectar**, conectarse a la base de datos, insertar los datos obtenidos por el objeto **parámetros** y desconectarse de la base de datos una vez que haya colocado allí la información.

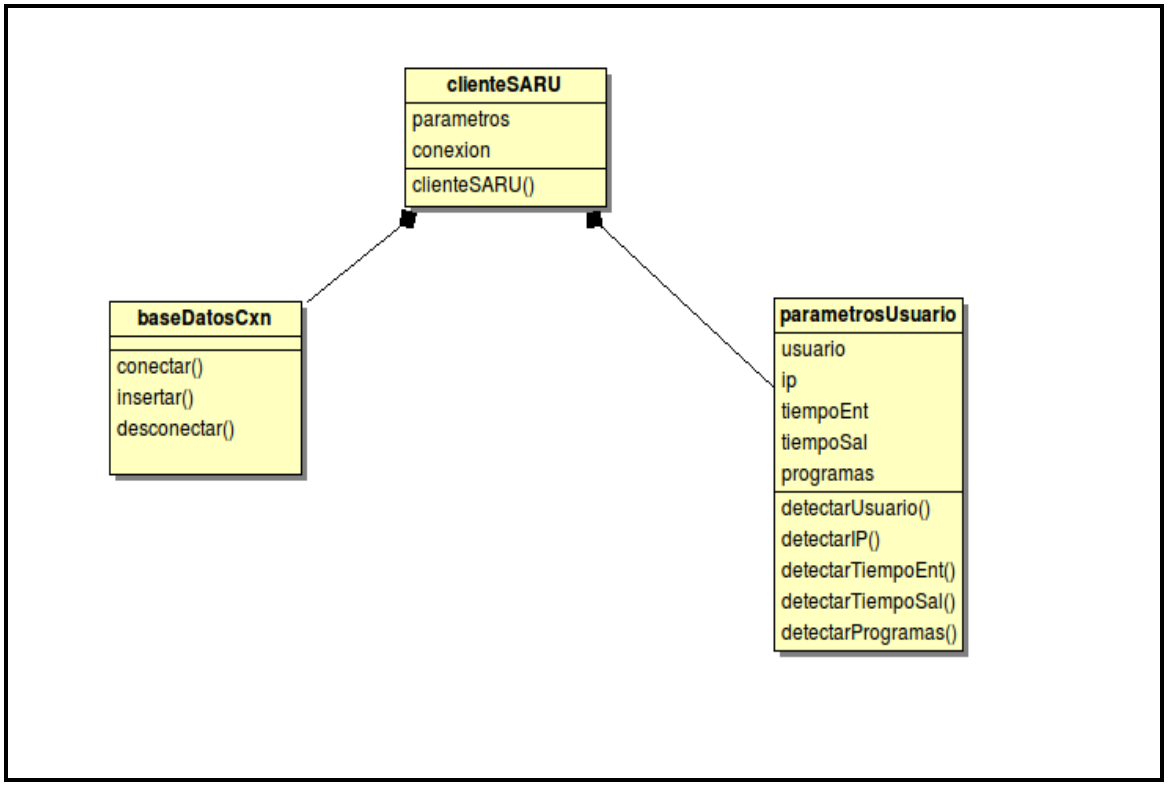

Figura 2.2 Diagrama de clases de la aplicación cliente.

2.4.2. El módulo de configuración

Existe un software adicional, que no está incluido entre los tres básicos del sistema pero que le permite al cliente SARU configurar su funcionamiento, este programa es el llamado "configurador de SARU" y permite comunicarle al cliente SARU a través de un fichero,

cuál es el IP del servidor de Bases de Datos, el nombre de la Base de Datos, y los parámetros de la conexión, así como el nombre del laboratorio donde se encuentra esta PC. En la figura 2.3 se puede observar el diagrama de clases de la aplicación configuración.

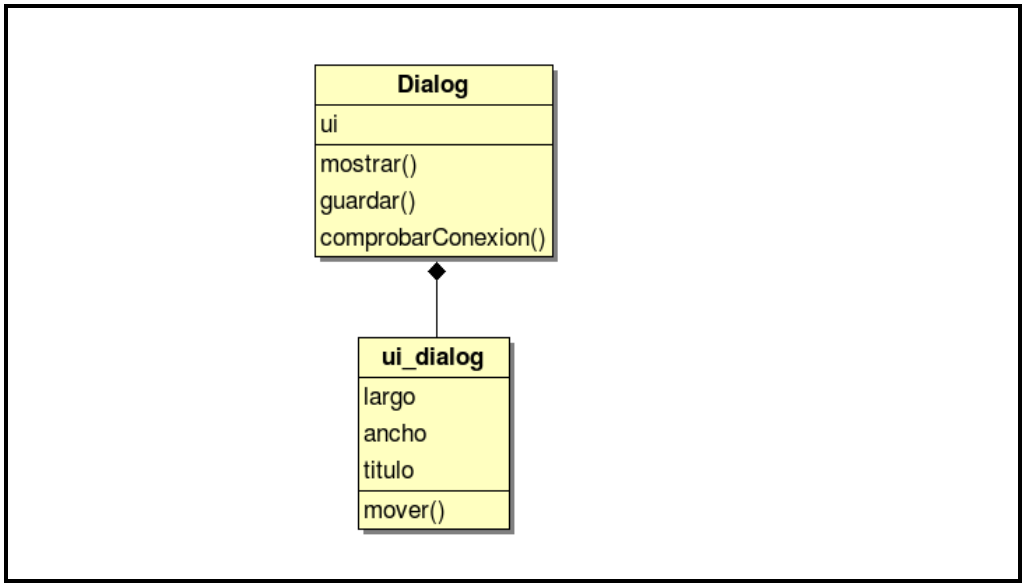

Figura 2.3 Diagrama de clases de la aplicación configuración.

La clase principal se llama **Dialog** la cual contiene un objeto llamado "**ui**" del tipo de clase **ui_dialog** que permite la visualización gráfica del configurador. Este objeto permite visualizar la interfaz de usuario del módulo configuración y facilita el trabajo del administrador. La clase **Dialog** contiene las funciones **mostrar, guardar y comprobarConexion**. El módulo muestra la última configuración efectuada si es que existe, luego almacena los parámetros de conexión necesarios para interactuar con la base de datos en el archivo de configuración para que los demás módulos del sistema SARU puedan obtener dichos parámetros y realizar la conexión, estos parámetros son el IP del servidor en el cual está la base de datos, el usuario, la contraseña, el nombre de la base de datos y de la tabla donde serán almacenados los registros históricos de cada sesión de usuario. Por último intenta conectarse utilizando los parámetros anteriores para chequear si son válidos.

2.4.3. Módulo base de datos

La base de datos se diseñó en un gestor MySQL, por las características propias de este programa, de fácil uso, buen desempeño, baja carga de memoria y procesador. El servidor se instaló en una computadora de la facultad y se creó una base de datos con el nombre "SARU" y dentro de esta se creó una tabla llamada "origen" con los siguientes campos:

Fecha, Hora, Usuario, IPMaquina, NombreMaquina.

(En la última versión serán en realidad dos tablas, la descrita anteriormente y otra que almacenará los programas ejecutados por el usuario)

Vea en la figura 2.4 una imagen de la tabla con valores adquiridos del software.

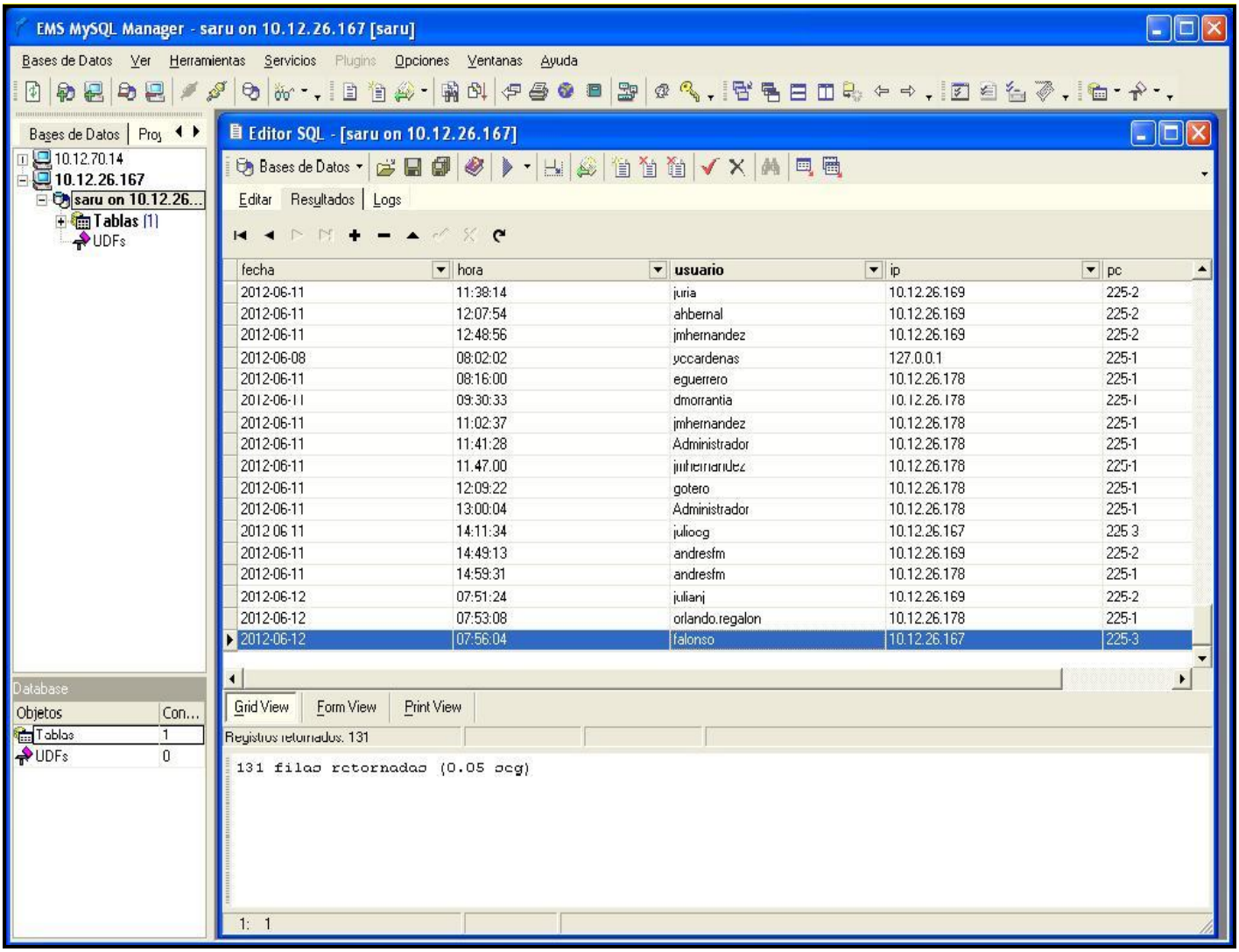

Figura 2.4 Editor SQL

2.4.4. Módulo el programa de procesamiento

El último módulo que comprende el sistema de software SARU es el programa de procesamiento, el mismo permite al administrador o la persona que lo requiera, visualizar todos los parámetros almacenados en la base de datos o las estadísticas que se puedan calcular. La arquitectura de este módulo se puede ver en la figura 2.5.

La clase fundamental contiene dos objetos que permiten su funcionamiento, esta clase se nombra **"principal**". El primer objeto se llama "**ui**" es del tipo de la clase **ui_principal** la cual contiene funciones que permiten al usuario poder ver la interfaz gráfica del programa y facilitar el trabajo del administrador. El segundo objeto se llama "**estadisticas**" y es del tipo de la clase **estadisticas** que contiene las funciones **traficoDiario**, **porcientoProgramas**, **ConsumoPromedio**, **horasDeUso**, **horaPico**, que permitirán controlar el uso de los medios computacionales y hacer estudios estadísticos del mismo, comprobando la eficiencia real del uso de las computadoras, pudiéndose obtener el tráfico diario, el por ciento de los programas más usados, consumo promedio de las PC y el horario pico del uso de los laboratorios.

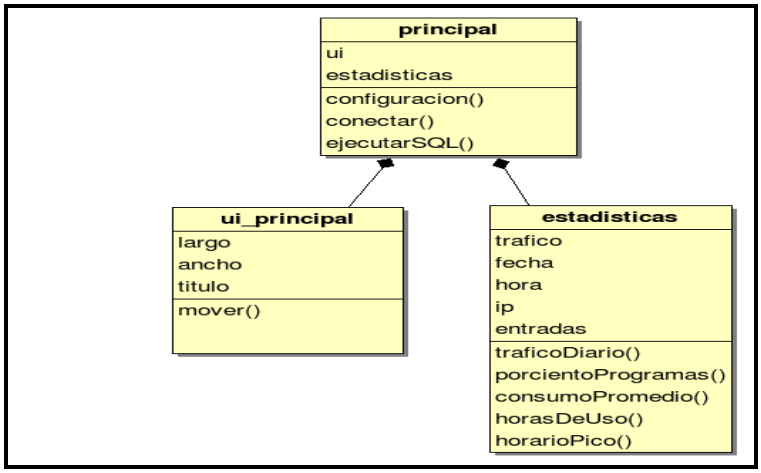

Figura 2.5 Diagrama de clases del módulo procesamiento.

La función **detectarProgramas** y el módulo de **estadisticas** se incluyen en el diseño del sistema de software SARU, pero no serán funcionales en este trabajo ya que el mismo sigue en desarrollo.

2.5. Programación y ambiente de desarrollo

El desarrollo del sistema SARU, como se mencionó en el capítulo 1, se realizó en el IDE de programación *QTCreator*, en su versión 2.0.1, utilizando todas las facilidades que brinda la plataforma QT, sobre todo para el tratamiento de cadenas de texto con la clase *QString*, lo cual siempre se dificulta en la programación en C++. Las interfaces gráficas de los módulos de configuración y de procesamiento, utilizando el *QTCreator* ahorraron mucho tiempo de desarrollo por las ventajas que tiene el diseñador, llamado *QTDesigner*. En la figura 2.6 se muestra una imagen del proceso de desarrollo del sistema SARU en el *QTCreator*.

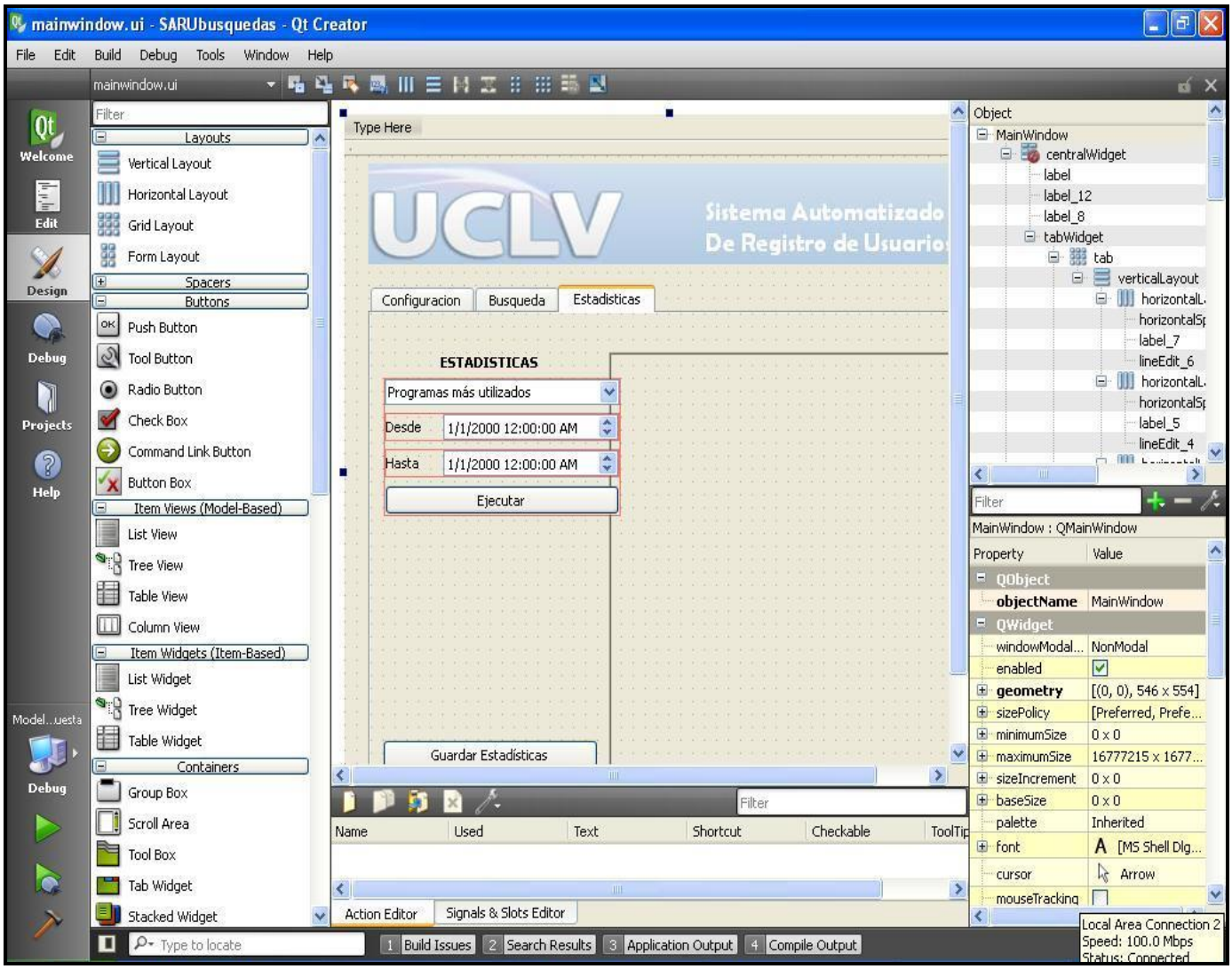

Figura 2.6 IDE de programación QTCreator

2.6. Interactividad y tolerancia a fallo

El sistema de software SARU está expuesto a que ocurran ciertos fallos que podrían afectar su eficiente desempeño a la hora de chequear a lo largo de cada sesión de usuario los parámetros que la caracterizan. Ante la posibilidad de que ocurran estos fallos se llevan a cabo algunas acciones que impiden que se burle esta herramienta de seguridad o que quede deshabilitada.

La pérdida del archivo de configuración es un fallo a partir del cual el software no funciona, pues sin él es imposible que el cliente instalado en las máquinas pueda conectarse con la base de datos y mandar cada uno de los parámetros característicos de cada sesión de usuario, quedando todos los datos guardados en el fichero temporal sin ser enviados a la base de datos, en este caso el software debe configurarse nuevamente. En caso de que se pierda la conexión a la red desde el inicio mismo de la sesión o una vez que el usuario haya comenzado a trabajar en la máquina, todos los parámetros característicos de esa sesión de usuario, así como todos los programas que se ejecuten serán guardados en archivos temporales, que una vez restablecida la conexión y en el comienzo de una nueva sesión de usuario, serán enviados de forma automática a los registros de la base de datos y luego se envían los del usuario que comenzó la nueva sesión. La figura 2.7 ejemplifica lo expuesto anteriormente. Si el usuario que está trabajando en la máquina intenta cometer alguna violación de seguridad informática y para eso trata de cerrar el programa que se ejecuta como un proceso en cada máquina mediante el "Administrador de Tareas" lo que sucederá es que a través de un código de protección que posee el programa, se llama a la función de la API de Windows que apaga la computadora.

En caso de que exista conexión a la red de área local pero el cliente no se conecta a la base de datos puede que hayan surgido algunas fallas, en ese caso se debe chequear si existen problemas en el servidor donde está instalada la base de datos, la configuración local, la instalación del *driver* ODBC[11] para la conexión con la base de datos o revisar los permisos para modificar la carpeta de los temporales para todos los usuarios, de no existir este

[11] Open Data Base Connectivity

permiso los parámetros de sesión no podrán ser almacenados de manera local en caso de pérdida de conexión con la base de datos.

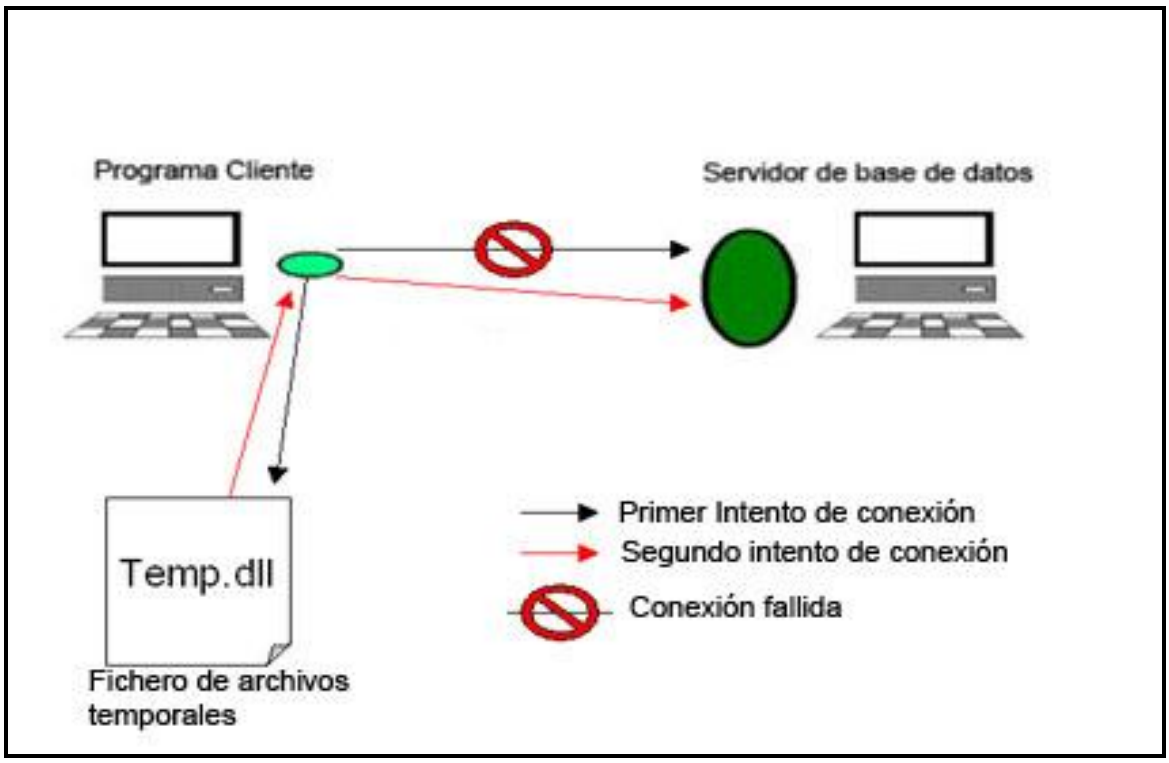

Figura 2.7 Esquema del sistema SARU sin conexión a la red.

Pueden existir problemas con la fecha y la hora local cuando la batería del BIOS de la máquina esté averiada, esto puede suceder en caso de no existir conexión con la base de datos, pues de lo contrario ese tipo de datos se toman del servidor donde está la base de datos mediante consultas SQL. Este problema aún no ha sido solucionado y queda como uno de los objetivos fundamentales para el posterior desarrollo del sistema de software SARU.

2.7. Consideraciones finales del capítulo

Mantener la seguridad informática es una prioridad para cualquier organismo o entidad en la actualidad. El sistema de software SARU es una herramienta conformada por varios

módulos que posibilita un mecanismo de seguridad informática para la obtención en tiempo real de los parámetros que caracterizan cada sesión de usuario, parámetros que son guardados de forma automática en una base de datos y a la cual se puede acceder de forma remota. De esta manera si existe alguna infracción de la seguridad informática en cualquiera de las PC donde se encuentra instalado el software se podrá conocer que usuario utilizó la máquina, sabiendo que máquina fue en la que se cometió la violación de seguridad, su IP, la fecha o la hora de la infracción.

CAPÍTULO 3. Pruebas reales del sistema, evaluación e impacto.

3.1. Introducción al capítulo

En el presente capítulo se describe la instalación del sistema SARU en uno de los laboratorios de la facultad y se evalúa el desempeño del mismo durante el tiempo en que el software estuvo a prueba. En el capítulo también se hizo un análisis de la aplicabilidad que posee el sistema de software SARU, así como sus posibles usos futuros, teniendo en cuenta que SARU es un software que se encuentra en pleno desarrollo y que se seguirá perfeccionando, hasta el momento se ofrece una herramienta que permite obtener los parámetros característicos de cada sesión de usuario en las PC donde se encuentre instalado. La obtención de datos estadísticos sobre el uso de los medios computacionales sabiendo qué programas ejecuta cada usuario a partir del módulo **estadísticas,** no será funcional para este trabajo, pero el mismo se propone como una herramienta que servirá de base para el desarrollo de este módulo.

3.2. Instalación y pruebas del sistema SARU en laboratorios de la facultad

El sistema de software SARU se instaló como prueba durante quince días en tres máquinas del laboratorio de estudiantes 225 de la Facultad de Ingeniería Eléctrica. El servidor de la base de datos radicó en el mismo laboratorio durante el tiempo de prueba.

Para que el software se ejecutara eficientemente fue necesario que en el inicio de cada sesión de usuario, el programa comenzara a funcionar automáticamente y para eso se instaló en cada máquina como un servicio. La figura 3.1 muestra el directorio donde se encuentran los dll[12] necesarios para que las aplicaciones realizadas con Qt puedan ejecutarse correctamente, este debe ser copiado en algún disco local de la máquina preferiblemente en C, dicho directorio contiene también los módulos y ejecutables que

[12] Dynamic link library

conforman el software, aunque los módulos de configuración y encuesta deben ser portables para el técnico y de esta manera no estar al alcance de los usuarios.

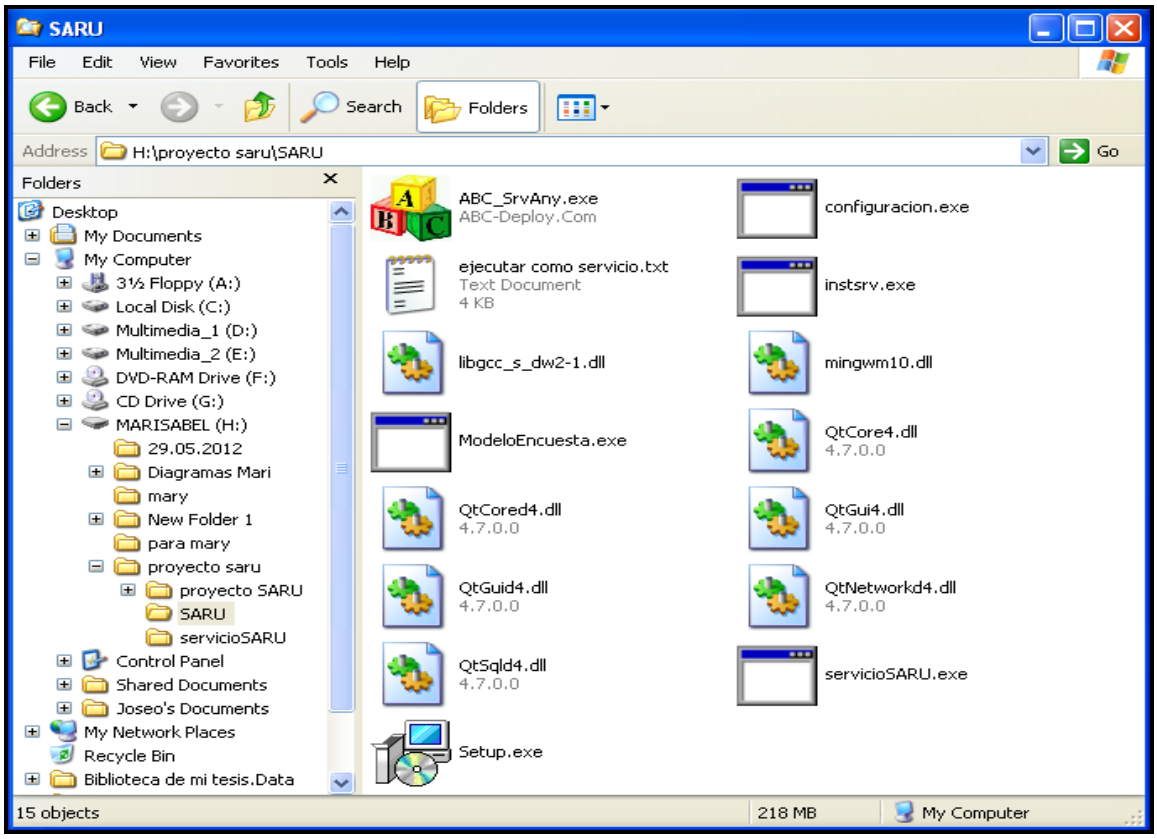

Figura 3.1 Carpeta SARU

Primeramente se ejecutó el módulo de configuración mostrado en la figura 3.2 y que exige los requerimientos necesarios para que cada PC pueda conectarse a la base de datos, sin este módulo SARU no encontrará la manera de conectarse al servidor de base de datos.

Luego se procedió a la instalación del *driver* ODBC para la conexión con a la base de datos. Se crearon los permisos para que el programa pudiera efectuar cambios desde la sesión de cualquier usuario en los ficheros temporales en los que se guardará la información pertinente a los registros históricos del usuario, de no existir estos permisos los parámetros de sesión no podrán ser almacenados de manera local en caso de pérdida de conexión con el servidor de la base de datos.

Figura 3.2 Módulo de Configuración.

La figura 3.3 muestra un ejemplo de cómo se almacenan los datos de forma local una vez perdida la conexión. Por último se procedió a la instalación del cliente como un servicio en cada una de las computadoras de forma simple, a través del editor de políticas del sistema ejecutando el comando (gpedit.msc) y especificando en "Configuración de equipo\Configuración de Windows\Secuencia de comandos (iniciar sesión)" y se agregó la dirección del ejecutable servicioSARU.exe. De esta forma se ejecuta de manera automática al inicio de cada sesión.

Para que los datos entregados por el sistema puedan persistir es necesario tener una base de datos instalada en un servidor remoto al que todos los clientes tributen los registros históricos obtenidos de cada sesión de usuario. Para esto fue necesario seguir los siguientes pasos, se instaló MySQL *server*, se creó un usuario que permite a las aplicaciones del sistema SARU conectarse a la base de datos y por último se confeccionó una tabla en la que se almacenaron los datos recopilados en diferentes columnas, la tabla cuenta con cinco columnas: **fecha**, **hora**, **IP**, **usuario** y **PC**.

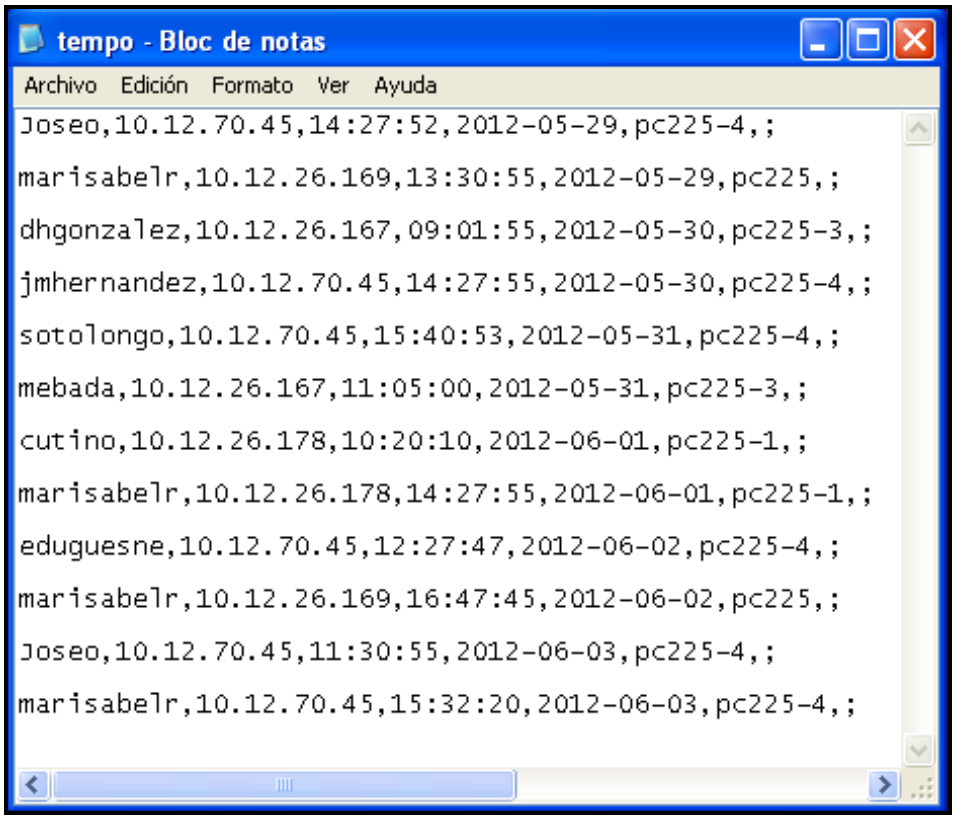

Figura 3.3 Fichero temporal

3.3. Evaluación de desempeño

Después de quince días de poner a prueba el sistema de software SARU en el laboratorio de estudiantes 225 de la Facultad de Ingeniería Eléctrica, se analizó una muestra de los resultados obtenidos. Hasta el momento, el software ofreció la información referente a la fecha, hora, usuario, IP y nombre de la PC, de cada sesión de usuario que se inició en cada computadora. Cada uno de estos parámetros se obtiene de forma separada según se desee. La figura 3.4 muestra los datos que brinda la opción **Buscar por usuarios**, esta posibilita saber todas las entradas de un usuario determinado en cualquier máquina, teniendo así un mayor control del tiempo que cada usuario utilizó en los laboratorios computacionales.

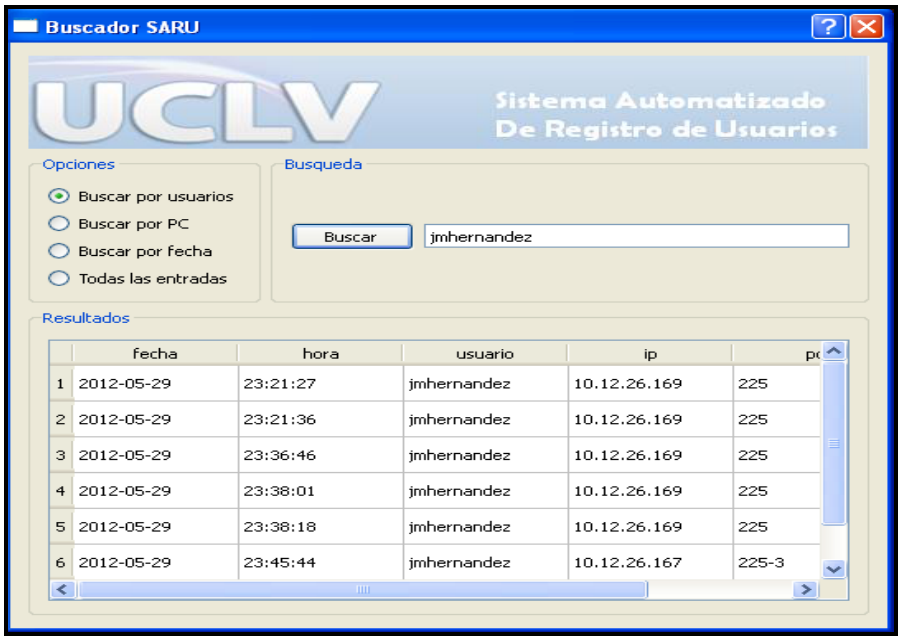

Figura 3.4 Buscador SARU.

La figura 3.5 muestra la opción **Buscar por PC**, una vez detectado cualquier delito informático si se conoce la máquina en la que se ejecutó la acción, se conocerán todos los usuarios que se registraron en esa PC específicamente.

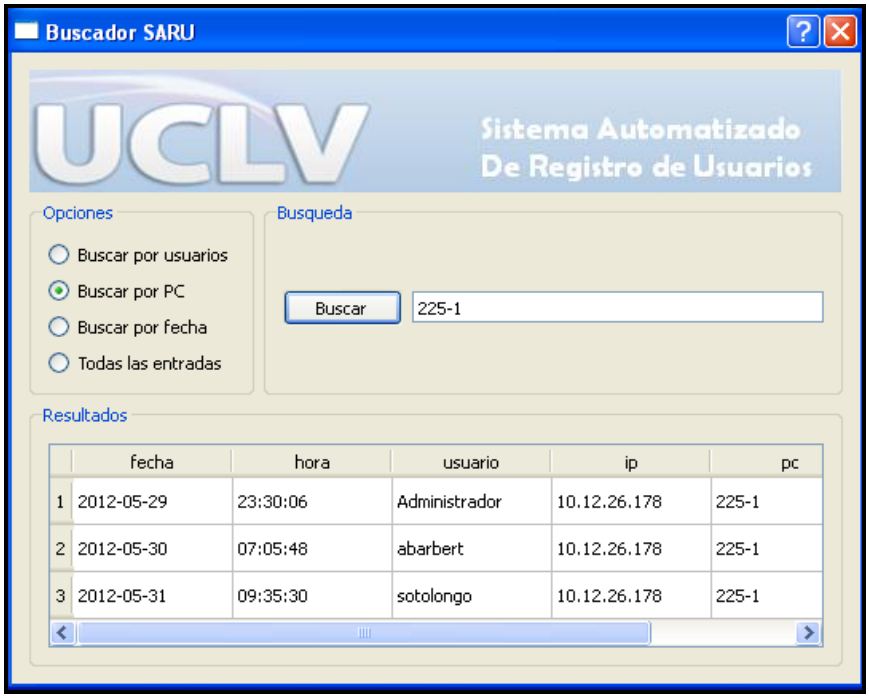

Figura 3.5 Buscador SARU.

La figura 3.6 muestra la opción **Buscar por fecha**, esta opción reduce el margen de búsqueda si sabemos el día en que se ejecutó cualquier violación de la seguridad informática, limitándose a un día se obtendrán todos los demás parámetros de cada sesión de usuario.

Figura 3.6 Buscador SARU.

La opción **Todas las entradas** mostrada en la figura 3.7 ofrece la posibilidad de revisar los datos registrados referentes a cada uno de los parámetros que conforman la tabla.

Figura 3.7 Buscador SARU.

El sistema de software SARU trabajó sin presentar ningún fallo técnico, incluso en ocasiones en las que existieron problemas de conexión a la red, los parámetros característicos de cada sesión de usuario como se mencionó en epígrafes anteriores fueron guardados en un fichero temporal y una vez restablecida la conexión a la red estos parámetros se enviaron a la base de datos y se muestran en el programa de visualización o **Buscador SARU**. Posibilitando una herramienta para supervisar las sesiones de los usuarios que utilizan las PC donde se encuentre instalado el software.

3.4. Aplicabilidad del sistema y posibles usos futuros

El acceso a la red es el primer aspecto que debe tenerse en cuenta una vez instalado cualquier software en una red de área local. El orden y la confidencialidad de cada puesto de trabajo o proyecto requieren un sistema que garantice que cada persona tenga acceso a

sus datos y aplicaciones, evitando que otros usuarios puedan ser perjudicados por el uso indebido del sistema o por la falta de una intención recta.

El sistema de software SARU particularmente ofrece obtener de forma automatizada y organizada el registro en un sistema de base de datos de los identificadores de las computadoras, los usuarios, la estampa de tiempo para diferentes eventos y los diferentes procesos que caracterizan una sesión de usuario. Constituye una herramienta de software que posibilita conocer en caso de que ocurra cualquier problema referente a la seguridad informática ciertos parámetros (nombre de usuario, IP de la máquina, PC, fecha y hora de inicio de sesión) que permitirán detectar de manera más organizada y segura el autor de esa acción o por lo menos reducirá el margen de búsqueda haciendo de esta herramienta un método eficiente de control y seguridad informática

La figura 3.8 muestra cómo puede ser usada la información que se registra en la base de datos, es un ejemplo sencillo de cómo saber la cantidad de veces que un usuario hizo uso de una determinada computadora.

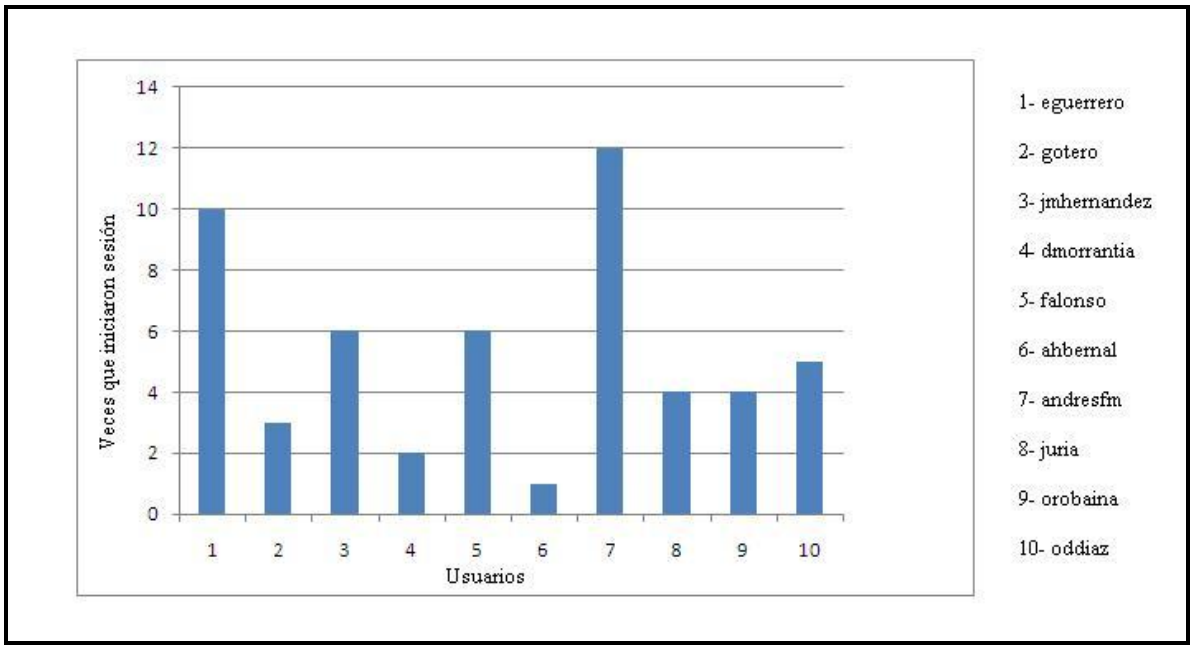

Figura 3.8 Uso de cada computadora por usuarios.

El sistema de software SARU está en pleno desarrollo, la implementación de algunas aplicaciones para su uso futuro como es el caso de obtener en tiempo real todos los programas que ejecute un usuario en su sesión están cimentados y solo faltan algunos detalles que posibilitarán poner lo antes posible en uso esta aplicación. De esta manera se podrá procesar estadísticamente la información almacenada en el servidor de base de datos, para obtener registros del uso de los componentes de la red, registros de la eficiencia en el uso, el tiempo de uso de las computadoras, entre otros parámetros importantes que permiten por ejemplo: evaluar el desempeño de la red, el cumplimiento del proceso docente educativo o la identificación de violaciones de seguridad y de los protocolos establecidos para el uso de los medios computacionales.

La figura 3.9 muestra un ejemplo de cómo esta herramienta de software podrá ser usada para estudios estadísticos, conociendo a partir de ella los programas más usados, entrada de usuarios por días, uso de programas por días, tiempo de uso de las computadoras; a través de gráficas.

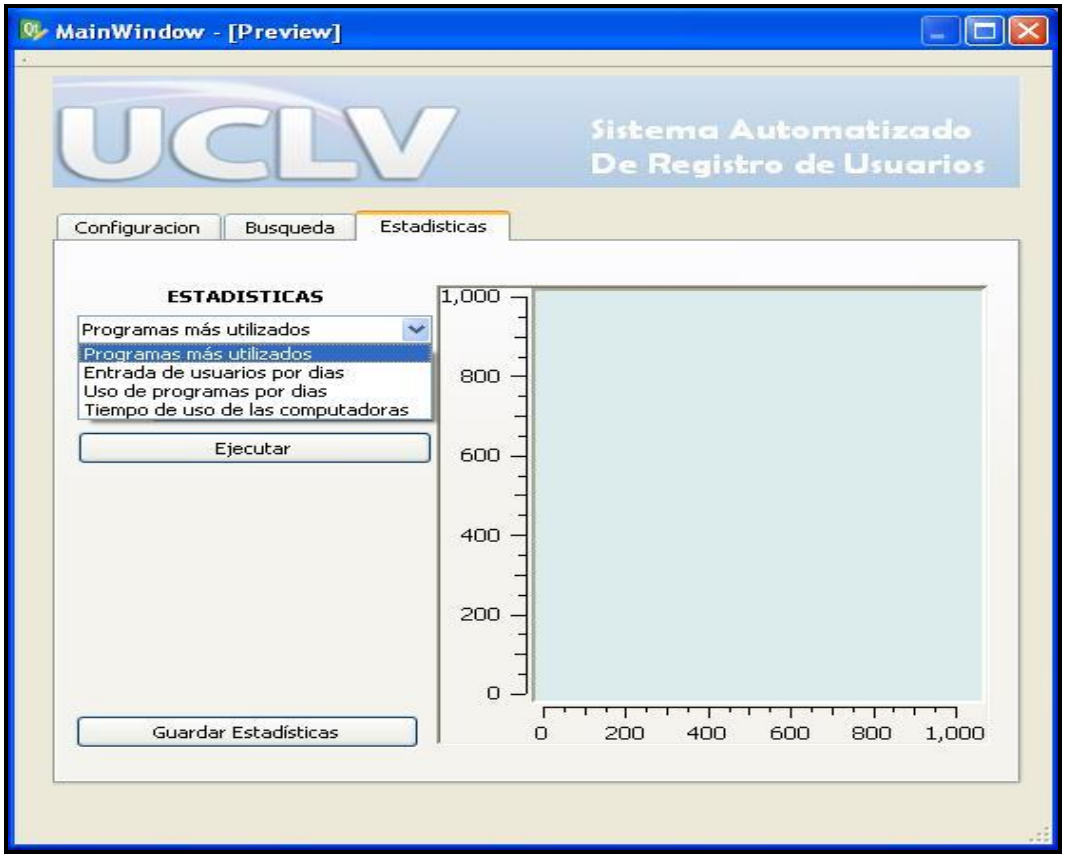

Figura 3.9 Estadísticas de SARU.

La figura 3.10 muestra más específicamente la manera de obtener una estadística en particular, con esta herramienta se podrá obtener los resultados queridos en un tiempo deseado y cada estadística se guardará independientemente una de otra.

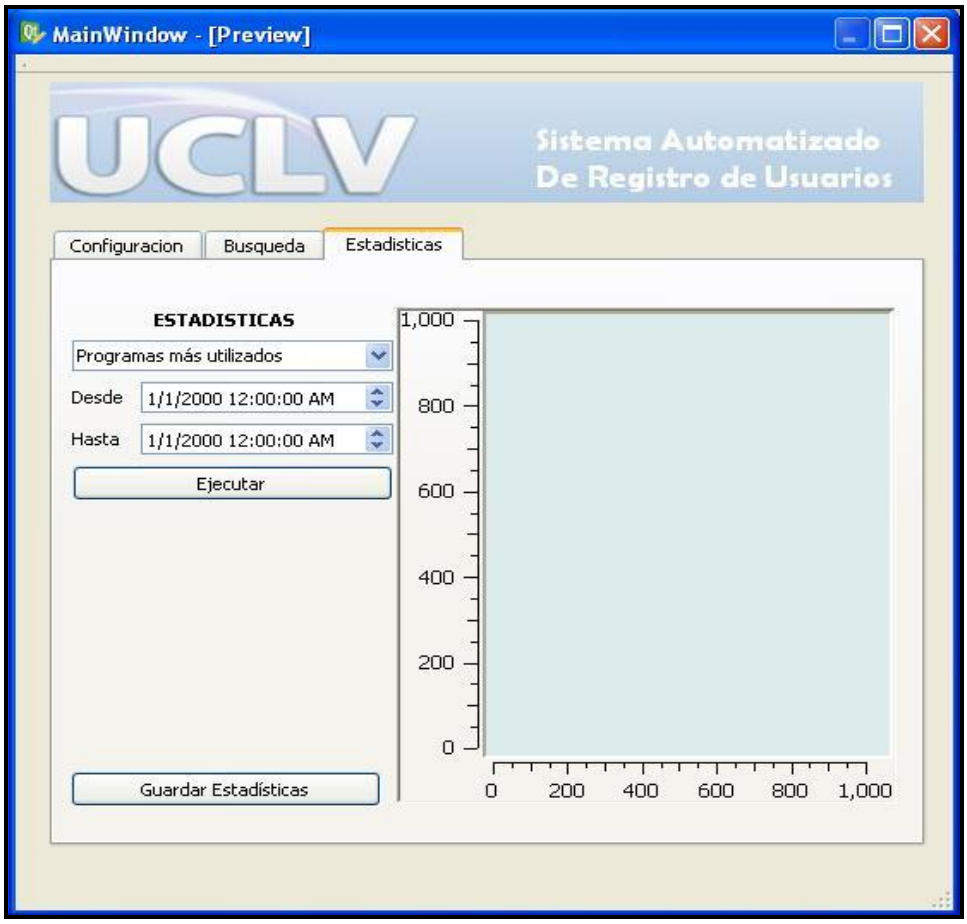

Figura 3.10 Estadísticas de SARU.

3.5. Consideraciones finales del capítulo

El sistema de software SARU está en pleno desarrollo y perfeccionamiento. Como se ha mencionado en epígrafes anteriores se ofrece una herramienta muy útil y con gran aplicabilidad, que podrá ser instalada de manera sencilla en los laboratorios computacionales de la Universidad Centra ¨Marta Abreu de las Villas¨ con la ayuda de técnicos y administradores de red. Contando así con un programa capaz de supervisar las

actividades de los usuarios en la red y detectar a los causantes de acciones que atenten contra la seguridad informática.

De esta manera, si se sigue implementando su desarrollo, SARU ofrecerá la posibilidad de realizar análisis estadísticos del uso de los laboratorios y medios computacionales, qué programas se ejecutan con más frecuencia, cuál es la hora pico del uso de los laboratorios así como el tiempo que estos se mantienen a disposición de los estudiantes entre otros parámetros.

El programa de manera general está diseñado para que se utilice de forma eficiente en todos los laboratorios de la universidad siempre y cuando se disponga del consentimiento de las personas responsables de la administración de los laboratorios y redes informáticas en cada facultad.

CONCLUSIONES

La exposición en el presente trabajo acerca de los aspectos de seguridad informática y el uso de las múltiples herramientas de software para administrar, controlar y gestionar las redes de computadoras, de la creación del sistema de software como un mecanismo de control que posibilitará mantener la integridad de las políticas de seguridad que se llevan a cabo en la Universidad Central Marta Abreu de las Villas y de las pruebas realizadas; permite llegar a las siguientes conclusiones:

1. Existen gran variedad de programas de supervisión y control del trabajo en las sesiones de usuario, todas muy útiles en cuanto a la gestión integral de una red informática, pero no existe una herramienta de software que gestione y aglutine de forma concentrada, en un solo servidor y cómo históricos, los datos principales de la actividad de los usuarios por cada computadora independiente.
2. El cliente SARU instalado como servicio en las máquinas funcionó de acuerdo a los requisitos funcionales establecidos, los usuarios no se percatan de su presencia y obtiene automáticamente el nombre de usuario, el IP de la máquina, el nombre de la PC, la fecha y la hora en el inicio de cada sesión de usuario.
3. La base de datos diseñada en el gestor MySQL, por las características propias de este programa, de fácil uso mantuvo un buen desempeño, propiciando todos los registros históricos de los parámetros que caracterizan a las sesiones de usuario de manera organizada, actualizándose con el inicio de cada nueva sesión.
4. El programa de proceso y visualización que obtiene la información almacenada en la base de datos a través de consultas SQL brinda la posibilidad de obtener en cualquier momento los registros referentes a los parámetros de cada sesión de usuario y además puede ser mejorado para brindar un cúmulo de posibilidades que ayudarían en gran medida el trabajo de la seguridad informática en la Universidad Central “Marta Abreu” de Las Villas.

5. A partir de las muestras almacenadas durante el tiempo en que el software estuvo a prueba se demostró que es una herramienta eficaz para el cumplimiento de las normas de registro en los laboratorios y además funciona como un mecanismo para la identificación de posibles violadores de la seguridad informática. Además permite procesar

estadísticamente la información almacenada en la base de datos posibilitando evaluar el desempeño de la red, registrar la eficiencia del tiempo de uso de las computadoras, registrar el uso de los componentes de la red, así como evaluar el cumplimiento del proceso docente educativo.

RECOMENDACIONES

Con el propósito de validar y perfeccionar el estudio realizado en este trabajo sobre el sistema de software SARU se propone considerar los siguientes aspectos, importantes para el futuro desarrollo de esta investigación:

1. Poner en práctica el sistema de software “SARU” en cada uno de los laboratorios computacionales de la facultad de Ingeniería Eléctrica de la Universidad Central Marta Abreu de las Villas, para mejorar los protocolos de seguridad informática.
2. Continuar desarrollando el software “SARU” e implementar la aplicación de obtener en tiempo real los programas que ejecute cada usuario, brindado una herramienta que permite hacer estudios estadísticos del uso de los medios computacionales de cada laboratorio.

REFERENCIAS BIBLIOGRÁFICAS

(2010). "Home (Remote RDP, Remote VNC, Remote Wave) ", 2012, from http://www.toremote.com/.

(2010). "La administración de sistemas aún más fácil.", 2012, from http://www.apple.com/es/remotedesktop/.

(2011). "Administra tus redes con Hyena." 2012, from http://recursosenweb.com/administra-tus-redes-con-hyena/.

Albán, O. A. V. (2010). "Introducción al Qt y al Qt creator."

Barja, J. M. M. and W. B. García (2004). "CURSO A DISTANCIA EN SEGURIDAD DE REDES DE COMPUTADORAS." Primer Congreso Virtual Latinoamericano de Educación a Distancia.

Bueno, A. (2010). "Unidad Didáctica: Redes Informáticas."

Castellano, R. (2008). "Seguridad informática." 2012, from http://www.seguridadar.com/?page_id=581.

Díaz, J. P. (2009). "Gestión y administración de proyectos."

Elliott, B. J. (2002). "Designing a structured cabling system to ISO 11801 2nd edition." Woodhead Publishing Limited.

Gutiérrez, D. G. (2008/09). "Tutorial de QtDesigner y QDevelop." Proyecto de Fin de Carrera.

Hoet, L., R. Cozzi, et al. (2007). "Manual de Sguridad en Redes." Coordinacion de Emergencia en Redes Infomáticas.

Hoet, R. (2010). "Spector 360 permite monitorear todo lo que un usuario hace en su PC y en Internet.", 2012, from http://es-la.facebook.com/note.php?note_id=182425685107610.

Mora, O. P. (2010). " Bases de Datos." Manual de Base de Datos.

Mora, O. P. (2010). "Manual Básico de MySQL."

Peterson, L. L. and B. S. Davie (2003). "Computer Networks a Systems Approach." Network Simulation Experiments Manual.

Salvatore, A. (2011). "NetSupport Manager, control remoto." 2012, from http://www.netsupportmanager.com/es/index.asp.

Toranzo, F. R. and J. A. R. Rivas (2006). "Redes de Area Local."

Torres, E. (2007). "Organización de la red." El sistema de acceso a la red

Gestión de los servicios. Administración y gestión de una red de área local.