UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

"ANÁLISIS DEL USO DE LAS REDES SOCIALES EN LOS ESTUDIANTES, MEDIANTE SOFTWARE KEYLOGGER EN LA INSTITUCIÓN ÁPECS"

Estudiante

María de Lourdes Carchi Atariguana

Tutor

Ing. Marco Lituma

Cuenca – Ecuador

Noviembre-2011

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE RESPONSABILIDAD

Ing. Marco Lituma Orellana
Director de Tesis

CERTIFICA:

Que el presente de investigación, “Análisis del uso de las Redes Sociales en los estudiantes, mediante software Keylogger en la institución Ápecs”, realizado por la Srta. María de Lourdes Carchi Atariguana, egresada de la Facultad de Sistemas Informáticos, se ajusta a los requerimientos técnico-metodológicos y legales establecidos por la Universidad Tecnológica Israel, por lo que se autoriza su presentación.

Cuenca, 7 de Noviembre de 2011

_____

Ing. Marco Lituma Orellana

DIRECTOR DE TESIS

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

ACTA DE CESIONES DE DERECHOS

Yo, MARIA DE LOURDES CARCHI ATARIGUANA, declaro conocer y aceptar la disposición de la Normativa de la Universidad Tecnológica Israel que en su parte pertinente textualmente dice: “Forma parte del Patrimonio de la Universidad la propiedad intelectual de las investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad”.

Cuenca, 7 de Noviembre de 2011

_____

María de Lourdes Carchi Atariguana.

C.I: 010-7466066-7

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE AUTORÍA

Los contenidos, argumentos, exposiciones, conclusiones son de Responsabilidad del autor.

_____

María de Lourdes Carchi Atariguana

C.I: 010533752-1

DEDICATORIA

La presente tesis está especialmente dedicada a mi familia, ya que supieron brindarme todo su apoyo durante el desarrollo de esta tesis quienes con toda su buena voluntad supieron brindarme su sustento en cada paso de mi vida para así poder alcanzar todos mis objetivos y metas propuestas.

AGRADECIMIENTO

Primeramente agradezco a Dios, a todos los profesores de la universidad Israel por brindarme su amistad y paciencia, apoyo y conocimientos; en especial a mi tutor el Ing. Marco Lituma, por compartir sus conocimientos que me ha otorgado su amistad sincera y gran ayuda en especial en el ámbito estudiantil.

RESUMEN

El keylogger es un diagnostico utilizado en el desarrollo de software que se encarga de registrar las pulsaciones que se realizan sobre el teclado, para memorizarlas en un fichero o enviarlas a través de internet. El registro de lo que se teclea puede hacerse tanto con medios de hardware como software.

Los sistemas comerciales disponibles incluyen dispositivos que pueden conectarse el cable del teclado y al teclado mismo. Se dice que puede utilizar un teclado virtual para evitar esto, ya que solo se requiere clics del ratón. Sin embargo, las aplicaciones más nuevas también registran pantallazos que anulan la seguridad de esta medida. Además, esto sería falso ya que los eventos de mensajes del teclado deben ser enviados al programa externo para que se escriba el texto, por lo que cualquier keylogger podría registrar el texto escrito mediante un teclado virtual.

Un keylogger registra esta información con especial exactitud. El registrador de teclas se instala y registra todas las pulsaciones que se realizan en el teclado o bien crea capturas de pantalla que después envía por Internet al que necesita la información. La aplicación oculta se ejecuta en segundo plano y no siempre puede encontrarse con el administrador de tareas.

Los keyloggers existen tanto en forma de hardware como de software. Mientras un módulo keylogger se utiliza más bien en el ámbito del espionaje industrial,

los programas keylogger se ocultan en herramientas aparentemente inofensivas que descargamos de Internet.

Al instalarlas, el keylogger realiza una entrada con un nombre falso en el registro, para así ejecutarse automáticamente cada vez que se inicia el sistema. Después de inicializarse, registra todas las actividades que se realizan en el PC y en Internet. El denominado perfil de usuario de la víctima comprende los datos de las aplicaciones abiertas, páginas web visitadas, chats, clics con el ratón, imágenes cargadas, correos electrónicos y aplicaciones activas, incluidas la hora y la fecha. En casos extremos, el keylogger incluso hace posible que se controle completamente el ordenador mediante un control remoto.

SUMMARY

The keylogger is a diagnosis used in the development of software that takes care of recording the keystrokes on the keyboard are made to memorize them in a file or send them via internet. The record of what you type can be both hardware and software means.

Commercially available systems include devices that can connect the keyboard cable and the keyboard itself. It is said that you can use a virtual keyboard to prevent this, since it only requires mouse clicks. However, newer applications that override also record screen shots of this security measure. Moreover, this would be false because the keyboard event messages should be sent to the external program to be written text, so any keylogger can record the written text using a virtual keyboard.

A keylogger records this information with particular accuracy. The keystroke logger installed and records all keystrokes made on the keyboard or create screenshots sent over the Internet then you need the information. The application runs hidden in the background and can not always find the task manager.

Keyloggers exist in both hardware and software. While a keylogger module is used rather in the field of industrial espionage, keylogger programs are hidden in seemingly innocuous tools we download from Internet.

When installed, the keylogger make an entry under a false name in the registry, so that automatically run each time the system boots. After initialization, records all activities performed on the PC and the Internet. The so-called user profile data includes the victim open applications, websites visited, chats, mouse clicks, shockingly, emails and active applications, including time and date. In extreme cases, the keylogger even makes it possible to completely control the computer using a remote control.

TABLA DE CONTENIDOS

LISTA DE ANEXOS

LISTA DE CUADROS Y GRAFICOS

CAPITULO I

1. INTRODUCCIÓN

1.1 Planteamiento del Problema

1.1.1 Antecedentes

Las Redes Sociales aparecieron desde el año 1995, con estas las personas recuperaron el contacto con antiguos conocidos de escuelas, colegios y universidades. Continuaron desarrollándose en el año 1997 que permitían a los usuarios crear perfiles, lista de amigos, enviar mensajes, etc. y en el año 2003 aparecieron MySpace y Xing, son dos redes muy populares, pero el que marcó la diferencia llego en el año 2004 conocido como Facebook.

Figura 1: Imagen Redes Sociales

Hoy en día existen más de 200 sitios de redes sociales, para todo el público enfocadas hacia las relaciones de amistad (Facebook, MySpace, Twitter, Badoo, Hi5), las que utilizan el ámbito profesional (Xing, Linkedln, Neworking Activo, Video, Rize), la gente según sus aficiones e intereses (Athlinks, Good reads, Horseland, Last.fm, CafeMom). Todos estos buscan lo mismo por tener a las personas conectadas. En las redes sociales las más populares en el

mercado son: Facebook, MySpace y Twitter, son las que tienen mayor excelencia.

La influencia de las redes en las personas ha llegado a puntos extremos, ya que el uso de estas, están en cada momento de la vida diaria de la gente, pero en un sentido más preocupante es cuando esta influencia afecta las labores diarias de las personas como por ejemplo en los trabajos o durante los horarios de estudio.

Este comportamiento adictivo que se tiene sobre el uso de estos sitios web, en muchas instituciones educativas ha ocasionado que se note claramente un bajo rendimiento educativo, debido a que durante los períodos diarios de clases los estudiantes se distraen y prestan menos atención a los docentes, lo cual ocasiona molestias en los profesores y a la larga problemas de aprendizaje en los estudiantes.

Una de las formas que se han usado para frenar estos comportamientos adictivos es conocer cuáles son los sitios de preferencia por los estudiantes a través de software espía, con la meta de bloquear estos sitios y contribuir a mejorar normas de seguridad a favor de la institución y los estudiantes en los centros educativos.

Uno de los más comunes Software Espía es “Keylogger”, un tipo de software específico que se encarga de registrar las pulsaciones que se realizan en el

teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet.

Este tipo de software es conocido como Malware comúnmente como software de captura de textos, en ocasiones si es usado para dañar, puede ocasionar grandes problemas a las personas por el robo de claves, pero si se lo usa para propósitos de protección es una herramienta eficaz.

Keylogger es un software de monitoreo muy potente que puede grabar y registrar toda la actividad de la computadora. Este trabajo registrador es herramienta clave en el modo sigiloso y completamente invisible para los demás. No sólo podría registrar movimiento clave, pero la información de software tales como las aplicaciones iniciadas, sitios web visitados y populares de registro de Instant Messenger.

Los problemas de distracción durante las actividades diarias de las personas ya sea en instituciones educativas u otro tipo de entidad, está ocasionando que el desempeño laboral se vea afectado, por lo cual las medidas de seguridad sobre software e internet deben ser eficaces y planteadas buscando el progreso laboral de la persona y la institución.

El campo informático disfrutaban investigando estos aspectos con el ánimo de incorporar mayor conocimiento; en la actualidad se ha desvirtuado completamente dando origen a nuevos personajes que utilizan los medios

informáticos y el conocimiento sobre su funcionamiento como herramientas para delinquir y obtener algún beneficio económico.

1.2 Sistematización

1.2.1 Diagnóstico o Planteamiento de la Problemática General

1.2.1.1 Causas – Efectos

a) Causas

- Distracción en los estudiantes a causa de las redes sociales en los niveles de estudio.
- Adicción al uso del Internet a través de estos Sitios Web.
- Libre acceso a Perfiles por Usuarios camuflados.
- Mayor vinculación de menores a estas redes sociales.
- Incremento de Timidez en adolescentes
- Escaso control de los Padres en el uso de estas herramientas web por parte de los adolescentes.

b) Efectos

- Bajo rendimiento académico en los estudiantes.
- Incremento en la resistencia por abandonar este tipo de servicio de redes sociales.
- Incremento de riesgos de seguridad en los adolescentes, ya que podrían ser víctimas de extorciones o problemas relacionados con Pedófilos.
- Los filtros de seguridad no podrían ser suficientes para evitar este tipo de crecimiento
- Los jóvenes aprenden a vivir en el mundo irreal y pierden confianza en el mundo real.
- La Inseguridad se incrementa en el entorno familiar a causa de esta tecnología.

1.2.1.2 Pronóstico y Control del Pronóstico

*** Pronóstico**

Al prestar más atención los estudiantes a este tipo de comunicación como redes sociales, estos se exponen a problemas graves:

- Bajo Rendimiento académico de los estudiantes
- Visitas de usuarios camuflados a través de la red a los perfiles de los estudiantes
- Problemas de comunicación entre padres e hijos
- Problemas en los servicios de internet que presta la institución (Saturación de la Red).
- Entrada libre a través de la Red de Virus u otro software que ponga en peligro la integridad de los Equipos.

*** Control del Pronóstico**

Para poder prevenir y corregir estas situaciones se plantea un análisis a través de encuestas y el uso de un Keylogger para conocer en que páginas tienen mayor distracción los estudiantes. Lo Que se plantea es:

- Limitar Acceso a sitios web que causen Distracción (Redes Sociales)
- Restringir Accesos a sitios web de contenido inadecuado para estudiantes
- Mejorar la Protección de los Equipos contra el ingreso de virus a través de Sitios Web visitados.
- Informar a los Padres sobre la Situación Académica de los Hijos.

1.3 Objetivos

1.3.1 Objetivo General

Conocer a través de la herramienta Keylogger el uso de las redes sociales en los estudiantes.

1.3.2 Objetivos Específicos

- Crear procedimientos para implementar la herramienta Keylogger.
- Diseño del procedimiento de Monitoreo y Análisis de información registrado por Keylogger.
- Recolección de Datos y Análisis.
- Proponer una forma de dar un Uso Académico a la Red Social más visitada según los resultados del Análisis.
- Crear propuestas de seguridad para el uso de Redes Sociales en Instituciones Educativas.
- Comparación de ventajas y desventajas de Keylogger frente a otras herramientas de igual propósito.

1.4 Justificación

1.4.1 Justificación Teórica

La comunicación es una necesidad que se encuentra en nuestro vivir diario por lo cual usamos cualquier tipo de herramienta que tengamos disponible para lograr dicho requerimiento.

Una de estas herramientas famosas de hoy en día es el internet, y la más frecuente dentro de esta red mundial son las Redes Sociales, usadas normalmente para comunicarnos con otras personas en línea. El problema se centra cuando substituimos el hecho de la comunicación por la distracción y

posteriormente lo convertimos en adicción, algo que generalmente es difícil de reconocer.

Las Redes Sociales son comunidades virtuales, plataformas de internet que agrupan a personas Las redes sociales están provocando una revolución en la manera de comunicarse a través de Internet.

Estos Sitios Web cumplen la finalidad de agrupar personas para comunicarlas entre sí, algo que sin duda alguna es beneficioso para las personas, pero en las instituciones educativas esto ya se está volviendo un dolor de cabeza, por las distracciones que tienen los estudiantes.

Los mecanismos de seguridad que se plantean para conocer los gustos de los estudiantes sobre los sitios web más visitados, son el uso de software que recoja datos que sirvan para la protección tanto de la institución como de los estudiantes.

Keylogger es una herramienta de software ideal para la recolección de datos, se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet.

Si bien esta herramienta representa violaciones a la privacidad, también representa ser una medida eficaz para mejorar la seguridad en una institución, ya que debido a las distracciones por causa del internet el desempeño

educativo disminuye, y según esto se busca bloquear todo aquello que no contribuya al desarrollo académico.

Además de la progresiva implantación de recursos en las aulas educativas, otro de los ejes de intervención del programa es la formación de tutores en aspectos metodológicos y sociales de la integración de estos recursos digitales en la práctica docente.

Detrás de la realidad en que vivimos y de los avances tecnológicos y los cuales están en constante innovación no debemos descartar los orígenes de nuestros sistemas los cuales creemos que ya no son importantes conocer estas etapas nos encaminan a concientizarnos de la importancia de todos los recursos internos de una organización y externos, estos los externos son los que estudiaremos desde los primeros periodos de civilización y de cómo el hombre vivía, de cómo fue descubriendo por medio de sus necesidades la caza la pesca, el fuego los materiales como el cobre y el bronce como le dio transformaciones a la piedra los troncos para utilizarlos como medios de protección y luego como se fueron realizando sistemas de intercambio entre ellos hasta lograr lo que hoy en día llamamos comercializar nuestros productos, tecnificados y modernizados para poder competir con muchas más empresas.

1.4.2 Justificación Metodológica

El planteamiento de este trabajo está enfocado en la recolección de datos para conocer cuál es el uso real que los estudiantes le dan a las Redes Sociales.

Para esto la Investigación es necesaria, aquella que se va a realizar mediante:

- El uso del método Cualitativo - Cuantitativo a través de la Encuesta, que servirá para conocer datos reales de los docentes y estudiantes sobre el uso de las redes sociales.

- Estudio de Documentación existente, a través de Libros, Páginas Web, Blogs, etc., lo cual ayudará a fundamentar mejor la investigación.

- El uso de Herramienta de software Keylogger, para conocer de forma más precisa cuanto tiempo los estudiantes le dedican a las redes sociales durante los períodos de estudio.

  La Herramienta trabajará de la siguiente manera:

  - ✓ Se instalará fácilmente en cada uno de los computadores de los estudiantes y actuará de forma no visible y silenciosa.
  - ✓ Se llevará un completo registro de cada acción que los estudiantes realicen en su actividad académica diaria.
  - ✓ Los Registros al final de la jornada podrán ser revisados y analizados y respaldados.

Se va a investigar a profundidad las características de las variables del estudio cuyos resultados servirán de fuentes de información a futuros investigadores en este campo, así como hallazgos científicos orientado del campo didáctico para mejorar la calidad de los servicios educativos.

1.4.3 Justificación Práctica

El Proyecto justifica de manera práctica en diferentes instituciones educativas para lograr la satisfacción mediante seguridades de privacidad entre adolescentes y la sociedad en internet de redes sociales.

1.5 Alcance y Limitaciones

1.5.1 Alcance

El trabajo que se pretende realizar, ayudará a conocer un poco más y dar una idea más clara de cuál es la vinculación que tienen nuestros hijos con las redes sociales y el tiempo que estos le dedican durante su periodo de desarrollo académico.

El proyecto a desarrollar contendrá lo siguiente:

- Información acerca de las Redes Sociales.
- Tipos y características de las Redes Sociales.
- Información acerca de software Keylogger.
- Uso de Keylogger como herramienta de software para extracción de datos silenciosa.
- Resultados acerca de cuáles son las redes sociales más usadas por los estudiantes.
- Uso de la red social más visitada enfocado en propósito académico.

1.5.2 Limitaciones

El proyecto estará limitado en lo siguiente:

- Análisis de las redes sociales vinculadas en los estudiantes en sus periodos académicos.
- La herramienta keylogger solo será utilizada para extraer datos de redes sociales.
- Los datos serán extraídos de un grupo de estudiantes representados por un número de diez estudiantes de un periodo de dos semanas.
- Realizar el estudio de las redes sociales para crear propuestas académicas relacionadas con este tipo de páginas web.
- No se desarrollará software en base a los resultados obtenidos a través del estudio.

1.6 Estudio de Factibilidad

1.6.1 Factibilidad Técnica

Para la Resolución del tema Propuesto se necesitará contar con herramientas de hardware y software que ayuden a guardar y extraer resultados valiosos que ayuden a cumplir los objetivos propuestos, para esto necesitaremos lo siguiente:

- ✓ Software de Extracción de datos silenciosa implantado en Computadores
- ✓ Computadores listos para implantar nuestra herramienta de extracción de datos
- ✓ Software de Seguridad debidamente configurado para que no cause problemas durante el monitoreo y captura de datos valiosos para el proceso de investigación a través de la Herramienta propuesta.

- ✓ Formato de Encuestas listas para realizar el Sondeo de información Acerca de las Redes Sociales en nuestro medio.

1.6.2 Factibilidad Operativa

El desarrollo del proyecto apunta a brindar un conocimiento real del uso de las Redes sociales por los estudiantes ya sea durante los Períodos Educativos Diarios, en donde usan computadoras que tienen acceso a Internet. Según esto el Análisis brindará Factibilidad de la siguiente manera:

- ✓ Brindará Información actualizada y real de la vinculación de las Redes Sociales en los Adolescentes.
- ✓ El resultado ayudará a conocer la Red Social preferida por los estudiantes y según este resultado se planteará formas de darle un uso Académico para estos Usuarios.
- ✓ La Información que brinde el Análisis permitirá conocer cuál es el grado de adicción de los estudiantes en cuanto a estos Tipos de Sitios Web.
- ✓ El Análisis resultante puede ser tomado como referencia en Instituciones Educativas para que generen estrategias Académicas a través de estas Redes Sociales

CAPITULO II

2. MARCO DE REFERENCIA

2.1 Marco Teórico

2.1.1 Las Redes Sociales en la Web

"Las redes sociales online son servicios prestados por medio de Internet que permiten que los usuarios presenten un perfil público en el que plasman datos personales e información de sí mismos, disponiendo de herramientas que permiten interactuar con el resto de usuarios afines o no al perfil publicado. (…)." (Wikitel, 2011).

Figura 2: Redes Sociales en la Web

"Las redes sociales son Web que permiten a los usuarios entrelazarse para poder comunicarse entre sí, en la cual pueden intercambiar fotos, videos, mensajes instantáneos, comentarios en fotos."(Fernandez, 2010)

Estas redes son comunidades virtuales, es decir, plataformas de Internet que agrupan a personas que se relacionan entre sí y comparten información e intereses comunes.

2.1.2 Las Redes sociales más conocidas en la Web

Las redes sociales más visitadas por adultos pero sobre todo por los jóvenes y con mayor crecimiento en los últimos años son Facebook, MySpace y Twitter, siendo estas las que marcan la diferencia hoy en día, en lo que se refiere a comunicación virtual.

2.1.3 Seguridad Web

“Seguridad hace referencia a aquello que tiene la cualidad de seguro o que está exento de peligro, daño o riesgo. En este sentido, la seguridad pública es un servicio que debe brindar el Estado para garantizar la integridad física de los ciudadanos y sus bienes”.(Definicion.de, 2011)

Figura 3: Seguridades Web

“La seguridad web es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios”. (Alegsa, 2011)

2.1.4 Keylogger

“El Keylogger es un software utilizado para grabar cualquier cosa que un usuario escriba o digite a través de su teclado, información que luego es enviada a terceros. En sus inicios, este programa espía se utilizaba para desarrollar software, pero actualmente es una de las herramientas más utilizadas en todo lo que se refiere al espionaje digital, el robo de claves, cuentas bancarias e, incluso, foros, así como también de documentos personales”. (http://www.mexicoglobal.net/informatica/keylogger.asp)

“Es un tipo software que se encarga de registrar las pulsaciones que se realizan en el teclado, para memorizarlas en un fichero y/o enviarla a través de internet”. http://tecnologia.glosario.net/terminos-viricos/keylogger-(capturador-de-teclado)-9765.html

El Keylogger registra de lo que se teclea puede hacerse tanto como medios de hardware como software. Los sistemas comerciales incluyen dispositivos que pueden conectarse el cable del teclado.

2.1.4.1 Tipos de Keylogger

- **Keylogger por hardware:** dispositivos físicos que se encargan de registrar las pulsaciones.
- **Keylogger por software:** programas informáticos que se encargan de registrar las pulsaciones.

La aplicación del Keylogger es cualquier programa computacional, puede ser distribuido como parte de un virus informático. Se puede utilizar un teclado virtual, la aplicación registra pantallazos que anulan la seguridad de esta medida, esto puede ser falso ya que los elementos de mensajes del teclado deben ser enviados al programa externo para que se escriba el texto, por cualquier Keylogger podría registrar el texto escrito mediante un teclado virtual.

2.2 Marco Conceptual

Este proyecto va dirigido a instituciones educativas para aumentar seguridad en las redes sociales en adolescentes y tener una evaluación fácil para la justificación del Proyecto.

2.3 Marco Temporal / Espacial

Este presente trabajo estará planeado a desarrollarse en un tiempo de 3 meses, en el cual se empezó a realizar desde el mes de agosto de 2011 hasta la siguiente fecha de terminación que se ha autorizado.

2.4 Marco Legal

La realización de la presente tesis se halla enmarcado en la constitución de la República del Ecuador, reformada por la Asamblea Constituyente en el año

2008, en la “LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS”, bajo los siguientes artículos:

- **Título Preliminar**

Art. 1.- Objeto de la Ley.- Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

- **Título I**

DE LOS MENSAJES DE DATOS

PRINCIPIOS GENERALES

Art. 2.- Reconocimiento jurídico de los mensajes de datos.- Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento.

- **Título III**

DE LOS SERVICIOS ELECTRÓNICOS, LA CONTRATACIÓN ELECTRÓNICA Y TELEMÁTICA, LOS DERECHOS DE LOS USUARIOS, E INSTRUMENTOS PÚBLICOS.

Capítulo I

DE LOS SERVICIOS ELECTRÓNICOS

Art. 44.- Cumplimiento de formalidades.- Cualquier actividad, transacción mercantil, financiera o de servicios, que se realice con mensajes de datos, a través de redes electrónicas, se someterá a los requisitos y solemnidades establecidos en la ley que las rija, en todo lo que fuere aplicable, y tendrá el mismo valor y los mismos efectos jurídicos que los señalados en dicha ley.

- **Título V**

DE LAS INFRACCIONES INFORMÁTICAS

Capítulo I

DE LAS INFRACCIONES INFORMÁTICAS

Art. 57.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Reformas al Código Penal

Art. 58.- A continuación del Art. 202, inclúyanse los siguientes artículos innumerados:

"Art. ....- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido

con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Art. 61.- A continuación del Art. 415 del Código Penal, inclúyanse los siguientes artículos innumerados:

"Art. ....- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

CAPITULO III

3. METODOLOGÍA DE INVESTIGACIÓN

3.1 Análisis de la Problemática

Para el Análisis del Trabajo propuesto, nos basaremos en el uso de métodos y Técnicas de Investigación para recopilar la mayor cantidad de información y opiniones que ayuden a fundamentar nuestros objetivos. Mediante estas herramientas de investigación se podrá identificar de una manera más certera las dificultades que tiene la empresa, y con esto ayudando a prevenir y corregir las mismas.

3.2 Metodología Investigativa

3.2.1 Método

3.2.1.1 Cualitativo – Cuantitativo

Se usará este método para tener evidencias que muestren resultados más precisos sobre cuál es la realidad de la problemática a resolver.

3.2.2 Técnica

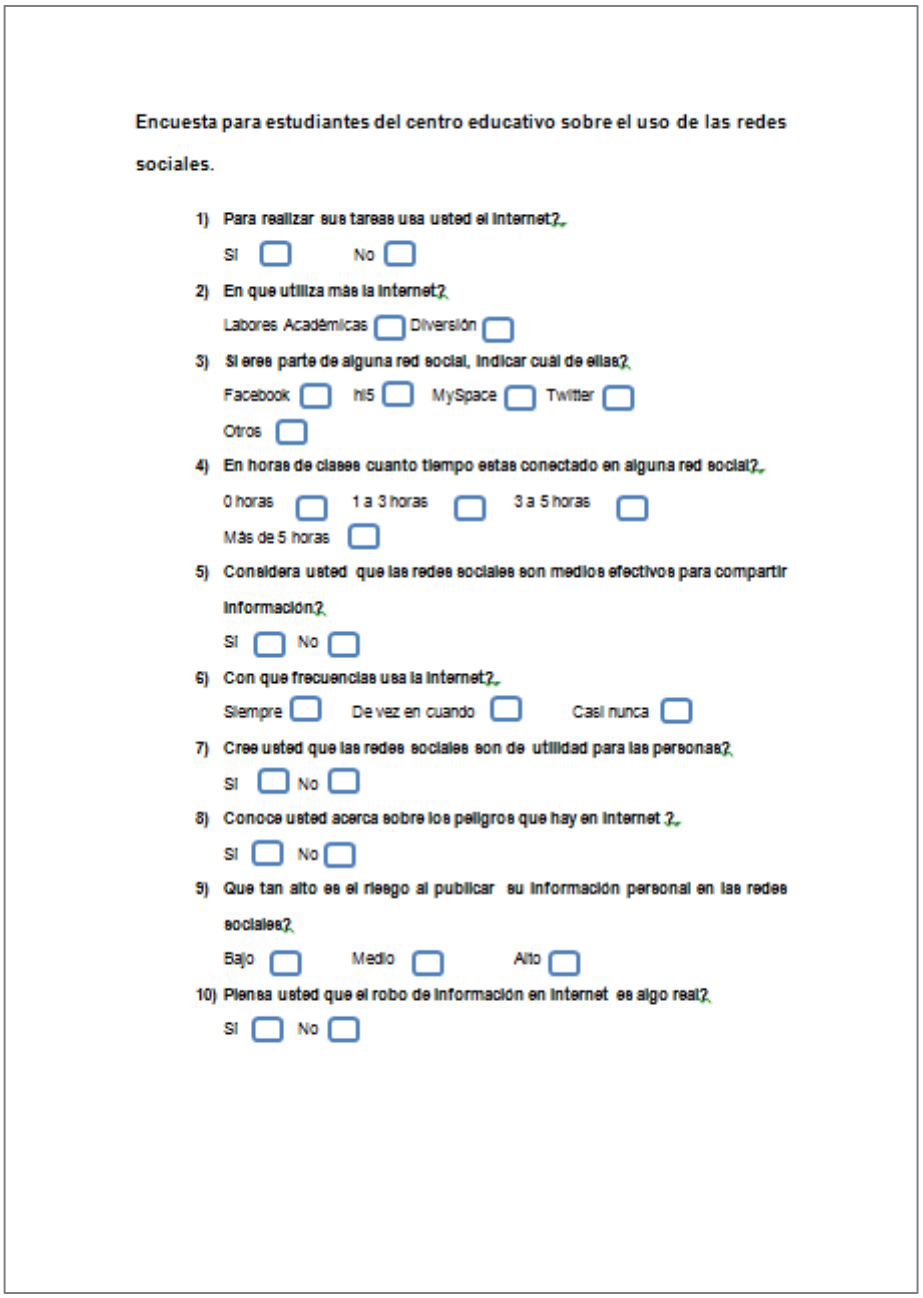
3.2.2.1 Encuestas

Está Técnica de Investigación se usará para recolectar la mayor cantidad de datos posibles acerca del uso de las redes sociales que influyen en los estudiantes. Esto con el fin de ayudar a encontrar soluciones en base a situaciones negativas que se encuentren en los resultados del estudio.

3.3 Población Involucrada

En este proceso de estudio se ha tomado como referencia las opciones de 30 encuestados, que representa cada uno, a distintas instituciones educativas que poseen sitios web u otro servicio similar que por este medio usan sus datos.

3.4 Formato de la Encuesta



Encuesta para estudiantes del centro educativo sobre el uso de las redes sociales.

1) Para realizar sus tareas usa usted el Internet?
   SI ☐ No ☐
2) En que utiliza más la Internet?
   Labores Académicas ☐ Diversión ☐
3) Si eres parte de alguna red social, indicar cual de ellas?
   Facebook ☐ hi5 ☐ MySpace ☐ Twitter ☐
   Otros ☐
4) En horas de clases cuanto tiempo estas conectado en alguna red social?
   0 horas ☐ 1 a 3 horas ☐ 3 a 5 horas ☐
   Más de 5 horas ☐
5) Considera usted que las redes sociales son medios efectivos para compartir información?
   SI ☐ No ☐
6) Con que frecuencias usa la Internet?
   Siempre ☐ De vez en cuando ☐ Casi nunca ☐
7) Cree usted que las redes sociales son de utilidad para las personas?
   SI ☐ No ☐
8) Conoce usted acerca sobre los peligros que hay en Internet ?
   SI ☐ No ☐
9) Que tan alto es el riesgo al publicar su información personal en las redes sociales?
   Bajo ☐ Medio ☐ Alto ☐
10) Piensa usted que el robo de información en Internet es algo real?
   SI ☐ No ☐

Figura 4: Formato de la Encuesta

3.5 Desarrollo y Análisis de las Encuestas realizadas a Estudiantes

1. **Para realizar sus tareas usa usted el internet?**

	Porcentaje	Nº Encuestados
SI	100	30
NO	0	0

Tabla 1: Resultado (Primera Pregunta)

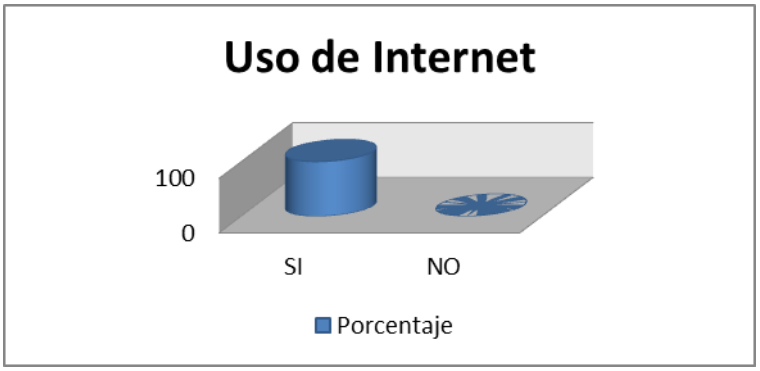


Gráfico 1: Resultado (Primera Pregunta)

Análisis

En los resultados obtenidos como vemos en el gráfico correspondiente que el cien por ciento de los estudiantes usa el internet para realizar sus tareas y no usan otro material de apoyo para realizar las tareas educativas.

2. En que utiliza más la internet?

	Porcentaje	Nº Encuestados
Labores Académicos	23	7
Diversión	33	10
Labores Académicos y Diversión	40	12
Ninguna	3	1

Tabla 2: Resultado (Segunda Pregunta)

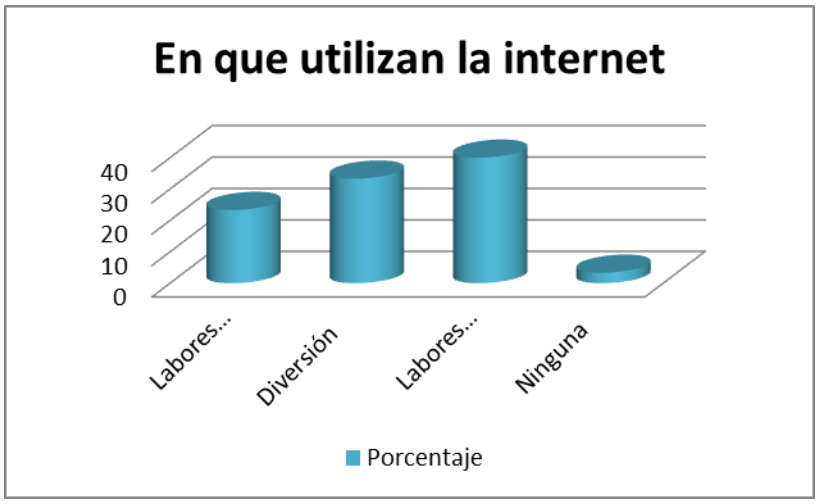


Gráfico 2: Resultado (Segunda Pregunta)

Análisis

Los estudiantes usan el internet en labores académicos un veinte y tres por ciento, usan el internet por diversión es un treinta y tres por ciento, los estudiantes que usan el internet en labores académicos y diversión es de un cuarenta por ciento, y hay un estudiante que no usa lo que el internet en ninguna de las dos opciones.

3. Si eres parte de alguna red social, indicar cuál de ellas?

	Porcentaje	Nº Encuestados
Facebook	53	16
Facebook y hi5	13	4
hi5	3	1
Facebook, MySpace y Otros	3	1
Facebook, hi5, MySpace, Twitter y Otros	7	2
Facebook y Otros	7	2
Facebook y Twitter	7	2
Otros	7	2

Tabla 3: Resultado (Tercera Pregunta)

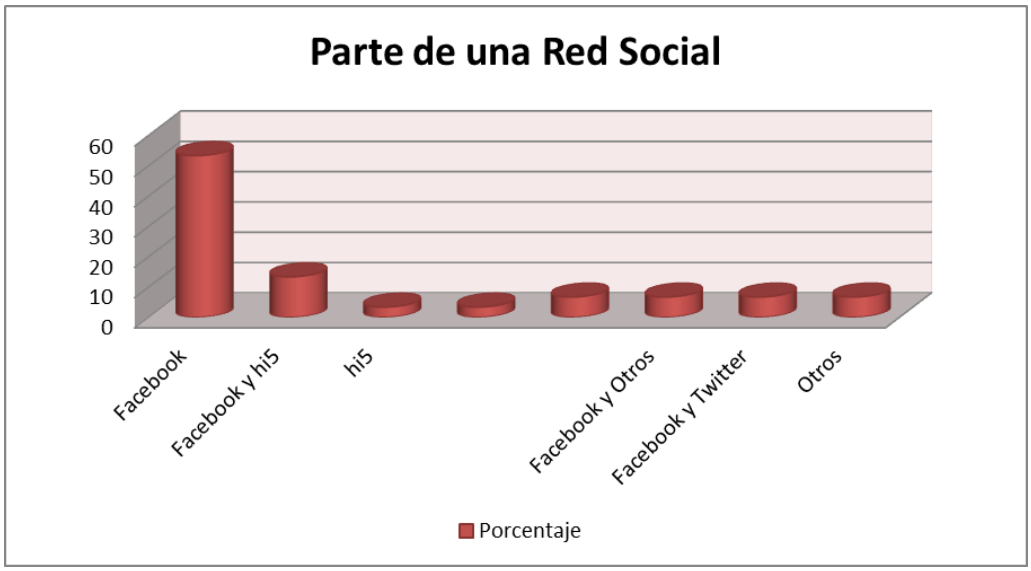


Gráfico 3: Resultado (Tercera Pregunta)

Análisis

Los estudiantes forman parte de una red social como el Facebook tenemos lo que es el cincuenta y tres por ciento de alumnos, entre el Facebook y hi5 tenemos un trece por ciento, los que tiene solo hi5 es un tres por ciento en esta red social es muy poca la comunicación, igual a la de Facebook, hi5, MySpace y Otros el tres por ciento de estudiantes los

que utilizan estas diferentes redes sociales, y de acuerdo al grafico vemos que un seis por ciento tienen todas estas redes sociales en usos.

4. **En horas de clases cuanto tiempo estas conectado en alguna red social?**

	Porcentaje	Nº Encuestados
0 horas	67	20
1 a 3 horas	27	8
3 a 5 horas	3	1
ninguno	3	1

Tabla 4: Resultado (Cuarta Pregunta)

Gráfico 4: Resultado (Cuarta Pregunta)

Análisis.

En las encuestas que se realizó a los estudiantes del centro educativo hay un sesenta y seis por ciento en cero horas los que no se encuentran conectados en una red social, y muy pocos estudiantes que están conectados en una red social.

5. **Considera usted que las redes sociales son medios efectivos para compartir información?**

	Porcentaje	Nº Encuestados
SI	93	28
NO	7	2

Tabla 5: Resultado (Quinta Pregunta)

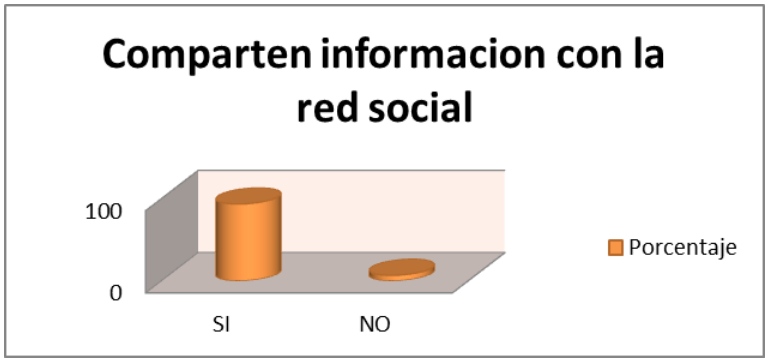


Gráfico 5: Resultado (Quinta Pregunta)

Análisis

Para los estudiantes consideran un noventa y tres por ciento que las redes sociales son medios para compartir información y un seis por ciento que no consideran que es un medio de información.

6. Con que frecuencias usa la internet?

	Porcentaje	Nº Encuestados
siempre	47	14
De vez en cuando	53	16

Tabla 6: Resultado (Sexta Pregunta)

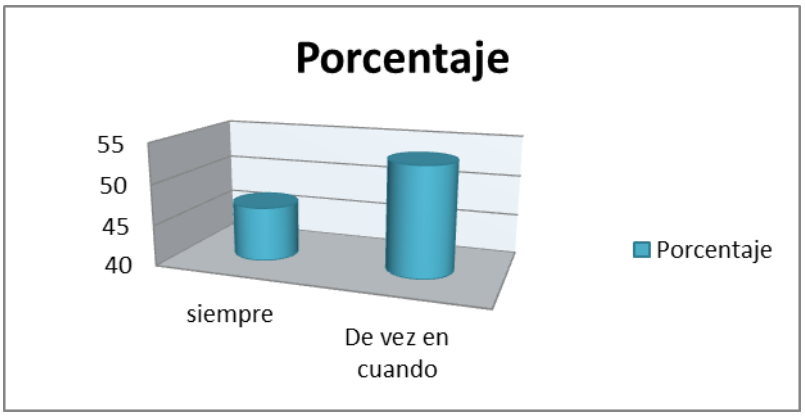


Gráfico 6: Resultado (Sexta Pregunta)

Análisis

Tenemos en este gráfico que los estudiantes usan siempre el internet es de un cuarenta y seis por ciento, y los estudiantes que usan el cincuenta y tres por ciento es de vez en cuando, no usan con frecuencia el internet.

7. **Cree usted que las redes sociales son de utilidad para las personas?**

	Porcentje	Nº Encuestados
SI	97	29
NO	3	1

Tabla 7: Resultado (Séptima Pregunta)

Gráfico 7: Resultado (Séptima Pregunta)

Análisis

Para muchos estudiantes vemos que las redes sociales son un medio de utilidad para la comunicación de personas, pero un tres por ciento para el estudiante que no es de utilidad este medio.

8. Conoce usted acerca sobre los peligros que hay en internet?

	Porcentaje	Nº Encuestados
SI	43	13
NO	57	17

Tabla 8: Resultado (Octavo Pregunta)

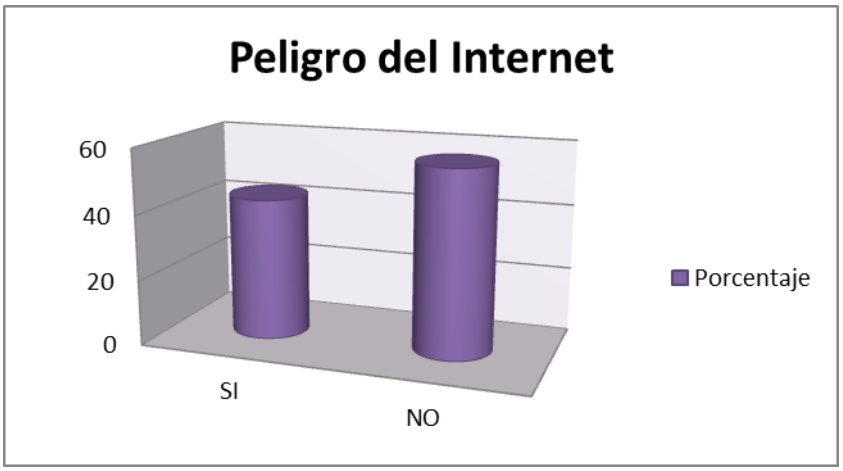


Gráfico 8: Resultado (Octava Pregunta)

Análisis

Las redes sociales en los estudiantes tienen un cuarenta y tres que dicen que las redes sociales si son un peligro para ellos, pero en cambio para otros estudiantes como el cincuenta y seis por ciento no ven que es un peligro las redes sociales.

9. **Que tan alto es el riesgo al publicar su información personal en las redes sociales?**

	Porcentaje	Nº Encuestados
Medio	47	14
Alto	53	16

Tabla 9: Resultado (Novena Pregunta)

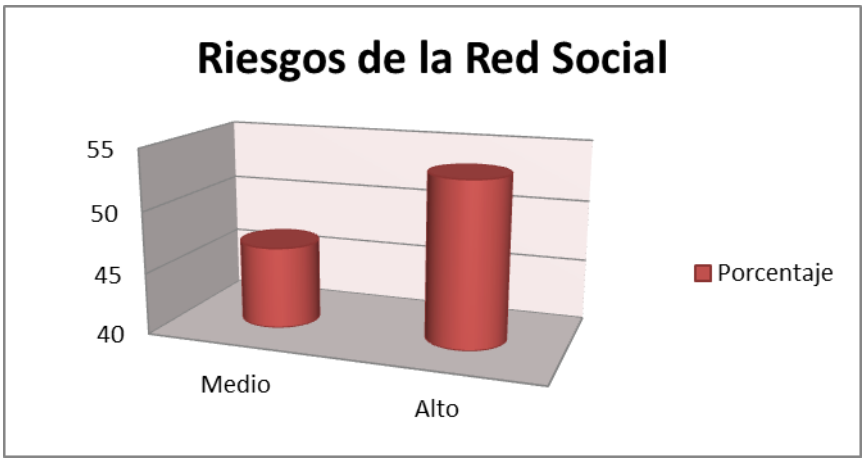


Gráfico 9: Resultado (Novena Pregunta)

Análisis

Publicar la información en las redes sociales es muy riesgoso pero de acuerdo a las encuestas que se realizó vemos que es alto el porcentaje de riesgoso de publicar mediante estas redes, y también se tiene un cuarenta y seis es medio peligroso publicar la información de los estudiantes.

10. Piensa usted que el robo de información en internet es algo real?.

	Porcentaje	Nº Encuestados
SI	87	26
NO	10	3
Blanco	3	1

Tabla 10: Resultado (Décima Pregunta)

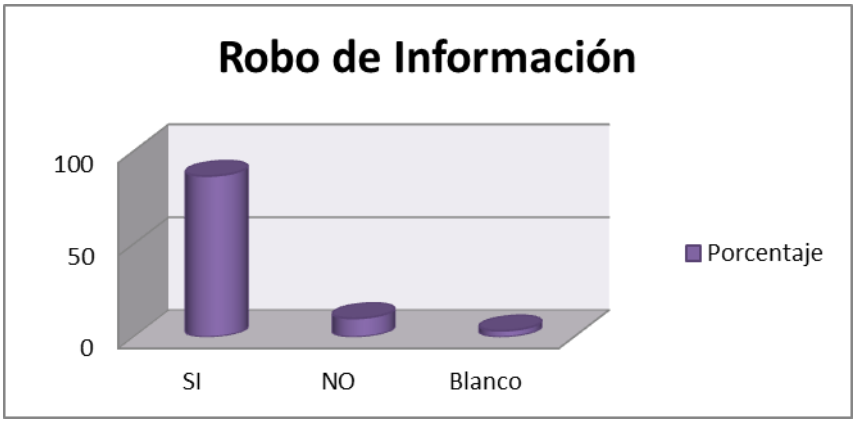


Gráfico 10: Resultado (Décima Pregunta)

Análisis.

En este análisis vemos un ochenta y seis por ciento que mediante las redes sociales existe el robo de información, y esto si puede ser algo real es lo que opinan los estudiantes sobre las redes sociales.

3.5.1 Resumen del Análisis

Red	Uso de Internet	Comparten informacion con la Red Social	Utilidad de Red Social	Peligro del Internet	Robo de Información
SI	100	93	97	43	87
NO	0	7	3	57	10
Blanco					3

Tabla 11: Resultado General Encuestas

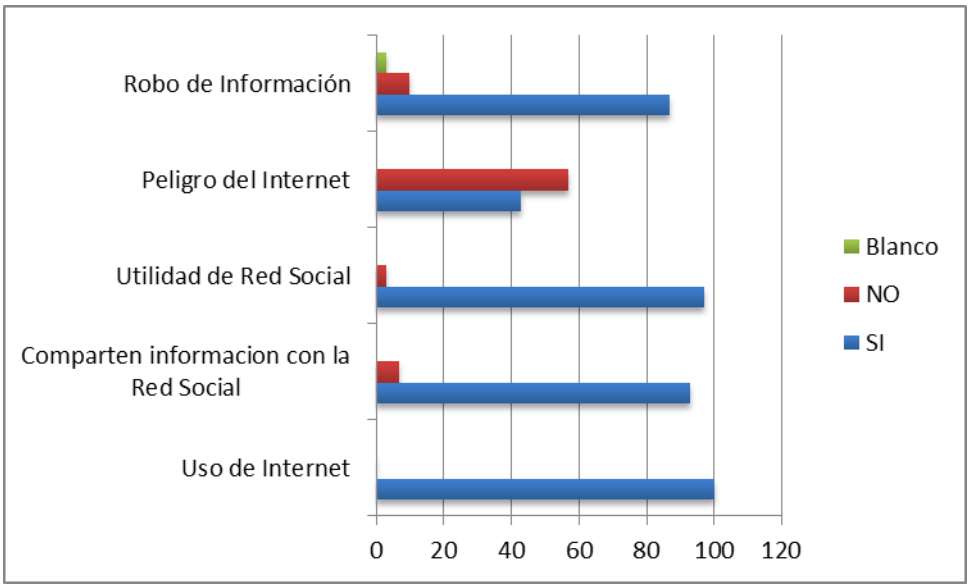


Gráfico 11: Gráfico General Encuestas

Este proceso de investigación se realizó a través de las encuestas, se tuvo como objetivo averiguar sobre los conocimientos de las redes sociales en los estudiantes de los diferentes centros educativos, ya que es peligros para muchos adolescentes que exponen sus datos personales a través del internet.

La recolección de datos a través de las encuestas, se realizó a estudiantes que usan las redes sociales y realizan labores académicos mediante el internet, de este modo lo que se desea saber, si en estos centros educativos, las redes

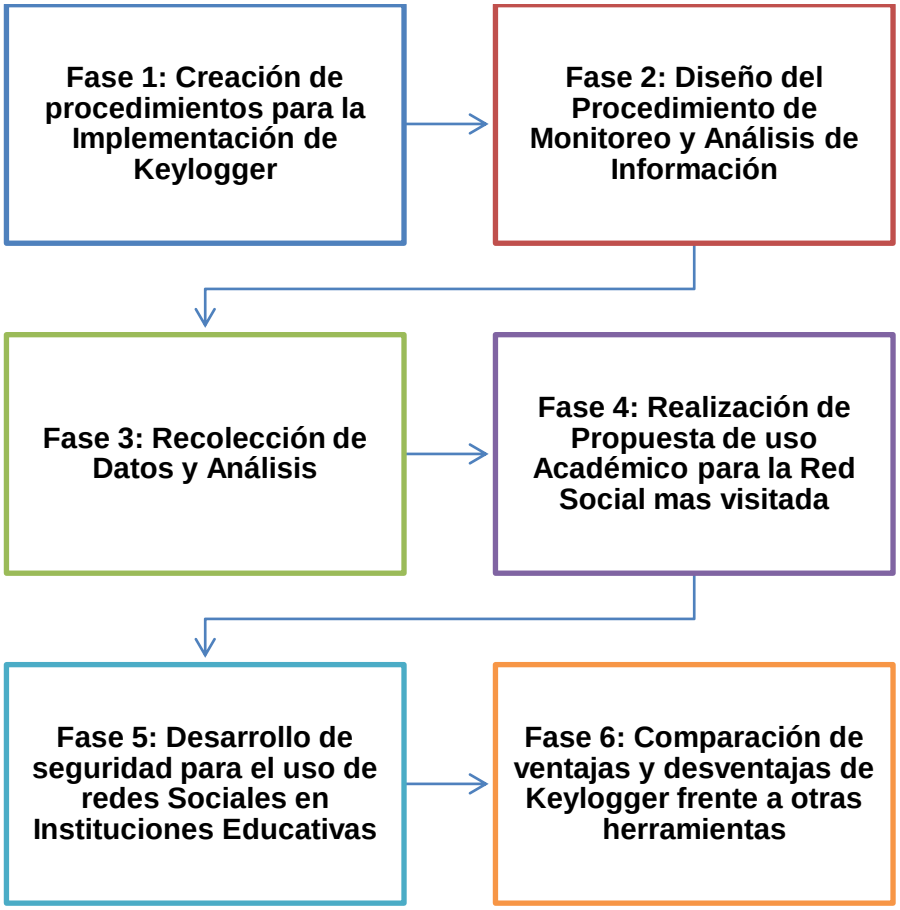
sociales es lo primordial para los adolescentes a través del internet para asi tomar precauciones adecuadas.

De acuerdo con los resultados de las encuestas, se pudo conocer que los conocimientos de internet y redes sociales son suficientemente altos, los estudiantes usan estas redes sociales para la comunicación entre amigos y familiares, las cuales son más usadas por este medio de información, las cuales no se percatan que no deben exponer su información completa en estas redes en cuestiones de seguridad de datos y prevención, lo cual muestra que a los padres de familia se familiaricen con el internet y las redes sociales para saber qué es lo que hacen sus hijos en el internet.

El estudio propuesto en este trabajo puede contribuir a mejorar el conocimiento y seguridad en las redes sociales.

3.6 Proceso de Ingeniería

Para la realización del proyecto vamos a trabajar con el Modelo Cascada para la sucesión de pasos y desarrollo.



CAPITULO IV

4. DESARROLLO

4.1 Fase 1: Creación de Procedimientos para la Implementación de Keylogger.

Keylogger es un pequeño programa que captura toda la actividad de los usuarios que utiliza en un computador almacenando todas las teclas pulsadas. El programa almacena la información clasificándola por fechas, captura además las teclas pulsadas en las distintas aplicaciones tales como contraseñas de msn, correos, y todo lo que teclee.

La herramienta Keylogger puede hackear cuentas de correo como (Hotmail, Yahoo, gmail) o redes sociales (Facebook, hi5, Twitter, MySpace) y de la manera más fácil y eficaz es utilizando este software que funciona como un espía (no es virus o troyano) sino permite:

- Registra conversaciones de Messenger (msn, Yahoo), skype, google.
- Captura claves de cualquier cuenta (e-mail, redes sociales…. Todas las pulsaciones del teclado).
- Páginas web que hayan visitado (perdiendo el tiempo viendo o navegando en el Facebook).
- Capturas de imagen de lo que están haciendo en el escritorio.

Figura 5: Tipos de redes Sociales

El Keylogger se puede programar para que envíe toda la información a su correo electrónico, a la hora que desee (cada segundo, minuto, hora o día) o si quiere en forma de bloc de notas o como página web. Además tiene la opción de ejecutar el programa en modo oculto, que lo hace totalmente invisible al usuario, y permite controlarlo sin que el estudiante se de en cuenta.

- **Características del SYS_KEYLOG ADVENCED:**

  - ✓ **Graba absolutamente toda la actividad realizada en el ordenador:**
    - Grabara todas las actividades realizadas en el ordenador. Ejemplo: email, chat, msn, direcciones web, password, detallada por usuario, fecha y hora.
  - ✓ **Captura las pantallas y ventanas según intervalo de tiempo:**
    - Captura las pantallas y ventanas activas en formato JPG y en modo oculto, por ejemplo la imagen del escritorio, imágenes web, ventanas activas, etc. Estas pantallas no ocupan espacio ya que tienen un promedio de 20kb.

- ✓ **Envía automáticamente al archivo log hacia un email:**
    - Envía hacia un correo electrónico cada cierto tiempo un archivo.txt con todo lo grabado detalladamente hasta el momento. Estos es en forma automática oculta para el usuario.
- ✓ **Protege el acceso al programa, desinstalación y archivo log con password:**
    - Solo el usuario que instaló podrá ver el contenido del archivo log y de igual manera desinstalara el programa, ya que estos estarán protegidos con password.
- ✓ **Permite ocultar el ejecutable del administrador de tares :**
    - Las aplicaciones que ejecutamos se muestra el administrador de tareas. El programa permitirá no ser visible en esta lista, para evitar que sea detectado y eliminado de memoria.
- ✓ **Programa mediante combinación de teclas:**
    - Se llama el programa mediante una combinación de teclas que hayamos configurado, podrá llamar al programa para hacerlo visible, si es que se encuentra en la memoria.
- ✓ **Eliminar el archivo log e imágenes capturadas, automáticamente:**
    - Evita redundancias podemos programarlo para que mientras vaya grabando también vaya eliminando todo lo que haya capturado. Esta opción se podrá utilizar en el siguiente procedimiento: graba, envía, elimina.

Este programa se puede descargar comprimiendo donde encontrarse el instalador, el serial y las instrucciones son las siguientes:

Es probable que durante la instalación el antivirus lo detecte pero es normal ya que este piensa que es algún tipo de virus o algo así pero no se preocupe, usted podrá configurarlo con toda seguridad.

Para instalarlo es sencillo solo hay que aceptar los términos y pasos.

Introducir clave de registro, una vez instalado se lo puede probar en el computador solo escribiendo en Word o navegando. Situándose con el ratón sobre el icono y haga clic derecho. Introduce la clave de registro.

Figura 6: Herramienta Sys_keylog 1.3 Advanced

A continuación explicaremos la instalación de la herramienta sys_keylogAdvenced.

El keylogger se descargará del sitio web ya buscado, con su respectivo tutorial para que sea más factible para su funcionamiento en la captura de pantalla y teclado.

Para comenzar la instalación abrir la carpeta e instalar.exe que ya se descargó del sitio web obtenido sobre esta herramienta.

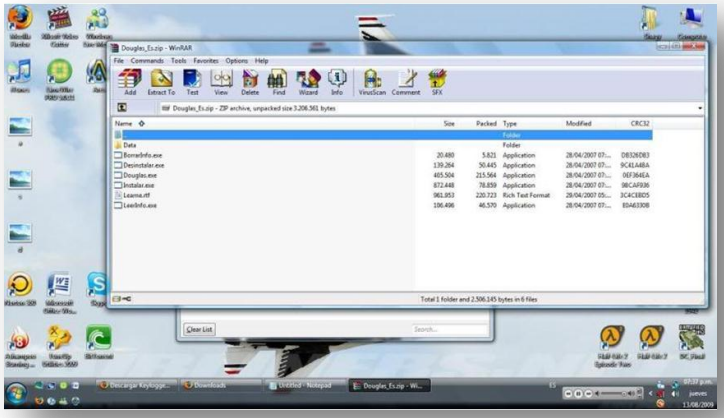


Figura 7: Carpeta para instalar Sys_keyloggerAdvanced

Aquí comenzaremos la instalación de la herramienta sys_keylogAdvenced en el computador con un sistema operativo Windows, este software es el más actual para el proyecto de las redes sociales en los estudiantes del instituto.

- **Instalación de la herramienta SYS_KEYLOGADVENCED**

Al ejecutar el archivo de instalación “setup _KL13.exe” el programa le mostrará ventana de bienvenida la información respectiva y los términos – condiciones que se deberá leer antes de continuar.

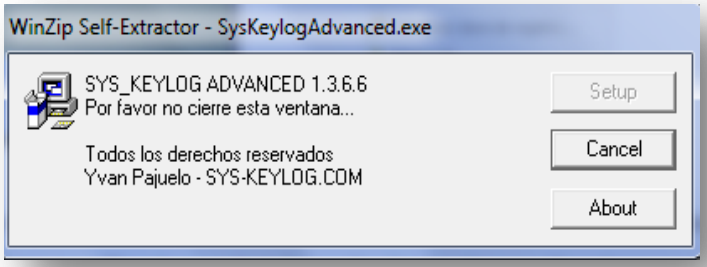


Figura 8: Instalación de Sys_keylogger

En el comienzo de la instalación aparecerá el programa de instalación:

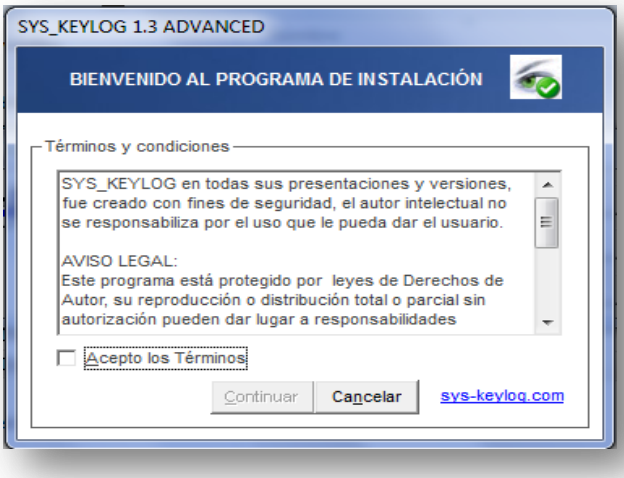


Figura 9: Comienzo de Instalación

Luego debe dar clic en el botón “continuar”, seguidamente se mostrará una ventana con la “Configuración Preliminar”, el cual se podrá observar las siguientes opciones:

Puede ir password antes de visualizar y/o desinstalar :

El programa le pedirá el password antes de visualizar el programa principal y antes de desinstalarlo. Recuerde que si no ha configurado ninguno, el password por defecto será ADMINISTRADOR.

Mostrar en el listado de Agregar o Quitar Programas :

Con el check marcado el programa se ocultará del listado de “Agregar o Quitar programas” dentro del panel de control, que es en donde se muestra todos los programas que se han instalado en un PC.

- **Grabar la actividad de todos los usuarios:**

Grabará toda la actividad de todos los usuarios en sistemas multiusuarios como Windows XP, 2000, 2003 server, Windows 7, etc.

- **Crear acceso directo en el escritorio de este usuario:**

Creará el acceso directo del programa solo en el escritorio del usuario actual. Recuerde que si se quite el acceso directo al programa, debe saber la ubicación de la misma para que luego ejecute.

Creará el acceso directo del programa en el escritorio de todos los usuarios. Es recomendable dejarlo desactivado si es que no quiere que otros usuarios de su PC se den cuenta que los están vigilando.

- **Password(casillero):**

Password o contraseña compuesta por letras y/o números para acceder al programa. Debe estar compuesta mínimo de 6 caracteres y máximo 15.

- **Confirmar(casillero):**

Es la confirmación del password. En esta parte de la instalación puede “obviar” el password, quedando establecido de esta manera que será por defecto: ADMINISTRADOR.

Puede actualizarlo en ese momento o mediante el menú “password” – “cambiar” luego de instalar el programa.

Luego el programa comienza con la instalación rápidamente y finalmente mostrará la ventana de instalación “Satisfactoria”, debiendo dar clic en el botón “Aceptar”.

A continuación se configurará la preliminar instalación de la herramienta Sys_keylog Advanced, presionamos iniciar para comenzar la instalación.

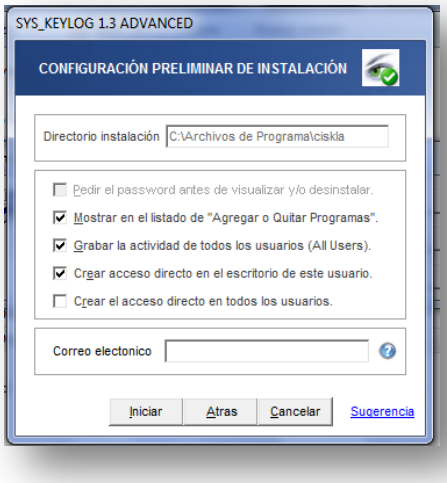


Figura 10: Configuración Herramienta

En esta pantalla les explicamos cómo estamos realizando la instalación del Sys_keylogAdvenced.

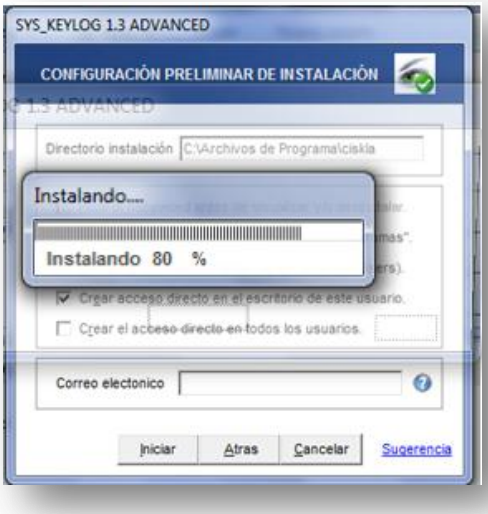


Figura 11: Instalación de Sys_Keylogger

La instalación de esta herramienta es muy rápida. Y presionamos la tecla aceptar lo que se terminó la instalación.

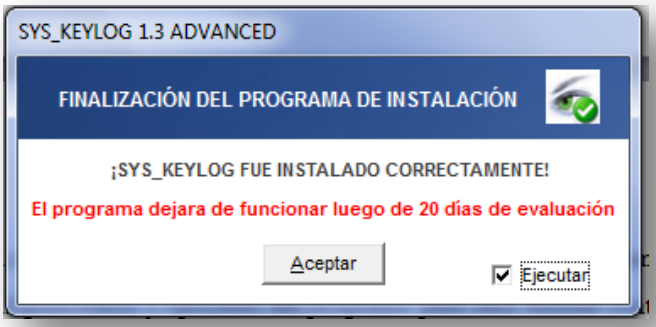


Figura 12: Finalización del programa de instalación

De acuerdo a esta herramienta se presenta la ventana de cómo funciona el sys_keylogAdvenced.

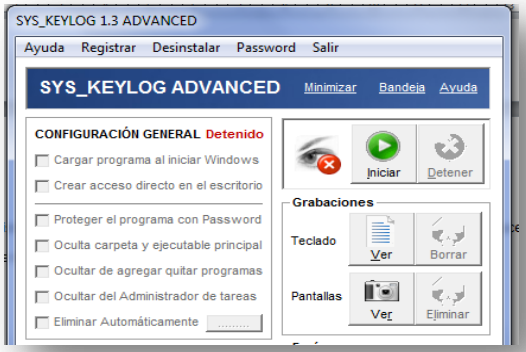


Figura 13: Sys_keylogger Advanced

- **Su funcionamiento**

Para que el programa pueda grabar todas las actividades realizada en el ordenador, tiene que hacer dando clic en “Activar”.

La opción “cargar programa al iniciar Windows” permite que cuando iniciemos Windows el programa cargue en memoria automáticamente, y en modo oculto.

Cuando el programa este en dicho modo, solo podrá ser llamado (visualizado) presionando la COMBINACIÓN DE TECLAS configurada, sino ha configurado ninguna será por defecto “Alt F12”.

PASSWORD por defecto para desinstalar y acceder al programa es ADMINISTRADOR, se recomienda actualizarlo.

- **Tiempo de evaluación y Licencia**

Si le interesó este programa, piense que se le puede ser útil y desea utilizarlo en forma ilimitada, le recomendamos una adquirir una licencia ante de los 20 días de evaluación, es importante remover esta copia antes del último día.

- **Desinstalación de la herramienta Sys_keylogAdvenced**

Se ha puesto un menú en la parte superior llamado “Desinstalar”, mediante esta opción se podrá desinstalar Sys_keylog Advanced con un solo clic.

Otras formas de desinstalación son las siguientes:

- Entre a “Agregar o Quitar programas” dentro de panel de control, selecciones “Sys_keylog Advanced” y luego clic en “Agregar o Quitar” o “Quitar”.
- Ejecutando nuevamente el archivo de instalación (setup_KL13.exe), allí el programa detectará una instalación y le preguntará si desea desinstalación.

Es la pantalla principal del programa se puede subdividir en las siguientes secciones:

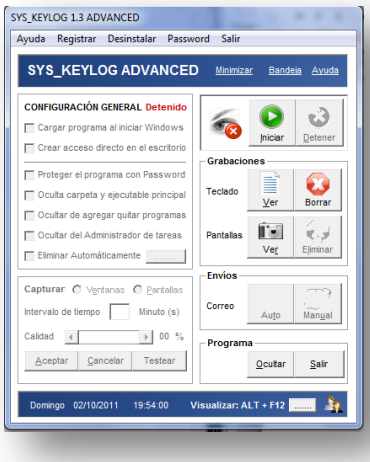


Figura 14: Pantalla Principal Sys_ Keylogger

Sección Menú: Se encuentra en la parte superior de la pantalla principal y consta de “Ayuda”, “Registrar”, “Actualizaciones”, “Desinstalar”, “Password” y “Salir”.

Figura 15: Menú Sys_keyloggerAdvanced

Sección Ayuda:

- **Manual:** Mostrara la presente ayuda, una ayuda interactiva, la opción “Preguntar” si es que desea hacernos una pregunta, y el foro oficial de ayuda.

- **Ayuda Interactiva:** Cada vez que Ud. Posicione el puntero en cualquier parte del programa y el puntero se pongan un signo de interrogación, para poder darle un clic y recibir ayuda según donde está posicionado.

- **Acerca de**: Muestra la información del producto, si el programa está registrado, versión, etc.

Menú Registrar:

- **Registrar:** Aquí podrá activar su licencia. Se mostrara una ventana con un SERIAL de 14 dígitos, el cual deberá remitirlo o adjuntando su nombre y No. De compra. Como respuesta recibirá su CODIGO DE

ACTIVO, el cual debe ingresarlo en el casillero respectivo y luego debe dar clic en el botón "Regístrese". Importante: Necesariamente para activar el programa comprando una licencia.

- **Comprar:** Nos llevara a la página web donde podrá realizar su adquisición de licencia comercial.

  Todas las formas de compra son 100% totalmente seguras, en línea (128 bits, la mayor protección para comprar por internet), como directas (depósitos, transferencias, etc.

Menú Desinstalar: Permite desinstalar el programa, debe saber que si desinstala el programa en los días de evaluación, ya no podrá volver a instalarlo. Solo se podrá evaluar una vez por PC y versión.

Figura 16: Menú de Desinstalación

Menú Password:

Mediante este menú se puede ver el password actual, así como la posibilidad de cambiarlo. Recuerde que el password por defecto, si es que no ha configurado uno diferente, será "Administrador".

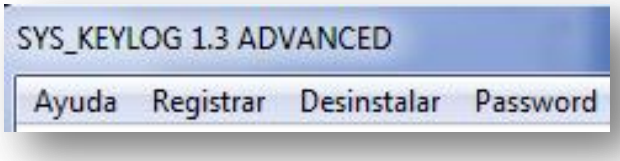


Figura 17: Menú de Password

Menú Salir

Salir: Sale del programa totalmente, no confundir con la opción “Ocultar”.

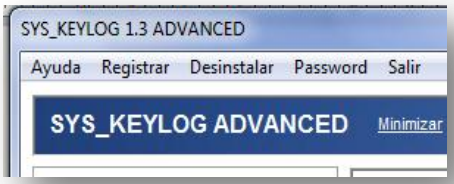


Figura 18: Menú de Salir

Ocultar: Sale del programa, pero seguirá grabando la actividad de la PC y solo podrá ser llamado-visualizado nuevamente con la combinación de la tecla configurada (Alt + F1, Alt + F2, etc.). Por defecto será Alt + F12.

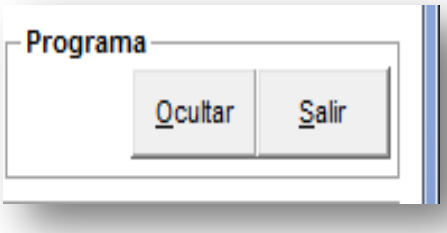


Figura 19: Pantalla de Ocultar Sys_keylogger

Sección Cabecera: Mostrara el nombre y la versión del programa, la opción “Minimizar” y “Bandeja”, un botón en forma de signo de interrogación de color azul, el cual activará la ayuda interactiva.

Figura 20: Cabecera del Programa

- **Minimizar:** Minimiza el programa en la barra de tareas. No hay otra forma de minimizarlo.

- **Bandeja:** coloca al programa en la bandeja del sistema, al costado del reloj. Una vez allí dando clic derecho sobre la misma se mostrara opciones tales como: “Abrir”, “Salir”, “Estado” (con opciones para iniciar y detener el programa con un solo clic), “log”(con opciones para verlo y borrarlo).

- **Ayuda: Muestra la presente ayuda.**

Sección opciones: Opciones similares al momento de instalación, las cuales son:

Figura 21: Opciones del Programa Sys_keyloggerAdvanced

- **Cargar Programa al iniciar Windows:** Permite que cuando iniciemos Windows el programa cargue en memoria automática, y en modo Oculto.

- **Crear acceso Directo en el escritorio:** Creara el acceso directo al programa en el escritorio solo del usuario actual. Recuerde que si quita el acceso directo al programa, para volverlo a ejecutar, debe saber la ruta de SYS_KEYLOG ADVANCED.

- **Proteger el programa con password**: el programa principal le pedirá el password que haya configurado para visualizarlo o para desinstalarlo. El password por defecto será ADMINISTRADOR.

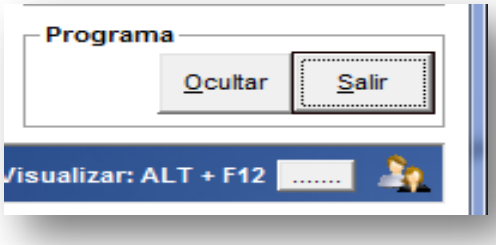


Figura 22: Pantalla de Salir Sys_keylogger

- **Ocultar carpeta ejecutable principal:** con esta opción se podrá ocultar la carpeta principal del programa así como el ejecutable principal. Esto para evitar que sea detectado por el usuario a controlar.

- **Ocultar del Administrador de Tareas:** Toda aplicación que ejecutamos carga en el "Administrador de Tareas" en forma automática (ctrl + alt supr). Activando esta opción el proceso principal de nuestro programa estará oculto, para evitar que sea detectado en la memoria.

- **Ocultar de Agregar o quitar programas:** Activada esta opción el programa no se muestra en el listado de "Agregar o Quitar Programas" del panel de control, que es donde se muestra todos los programas que se hayan instalado en una PC. Active esta opción si desea evitar la desinstalación de SYS_KEYLOG ADVANCED.

- **Eliminar en forma automática:** Mediante esta opción se puede configurar para que el programa elimine las imágenes capturadas y el

archivo log en forma automática cada cierto tiempo (día/hora). Esto para evitar redundancia.

Sección Botones: Muy importante, son los botones que se encuentran en la parte derecha del programa principal. Aquí se determina si el programa estará activo o no para que grabe toda la actividad del ordenador.

Figura 23: Sección de Botones Sys_keylogger Advanced

- **Botón Iniciar:** con esta opción el programa comenzará a grabar absolutamente todo lo que realicemos en el ordenador.
- **Botón Detener:** El programa dejará de grabar. Se desactivará temporalmente todas las funciones automáticas (captura pantallas, eliminación automática, envío automático de archivo log, etc.).
- **Ocultar (Programa):** Con esta opción podemos ocultar el programa y seguirá cumpliendo sus funciones. Antes de ello le mostrara, por seguridad, la combinación de teclas con que el programa podrá ser visualizado nuevamente.
- **Salir (Programa):** Veremos el contenido preliminar del archivo log.

- **Ver (Teclado):** Veremos el contenido preliminar del archivo log. Tendrá las opciones: para visualizarlo en .txt (Muestra el archivo log en notepad). Visualizarlo en “HTM” A(Muestra en formato web), “Backup”(realizaba backup del archivo log), “imprimir” (imprime todo el contenido de log) y Borrar(eliminar todo el contenido del archivo log).
- **Borrar (Teclado):** Permite ver todas las imágenes capturadas entre ventanas e pantallas completas. Dentro de esta ventana los podrá guardar, ampliar, etc.
- **Ver (pantalla):** Veremos todas las pantallas ventanas capturas por el programa. Importante: para que el programa puede capturar estas pantallas primero debe configurar “Sección capturar pantallas”, que se describirá a continuación el punto 5.
- **Borrar (Pantalla):** Permite eliminar todas las imágenes capturadas.
- **Auto (Correo):** Con esta opción se podrá configurar el envío automático del archivo Log hacia su correo. Se debe ingresar los campos respectivos, para luego conectarse a un servidor. Puede consultar la ayuda (dentro de esta) para que pueda saber que correos y Servidores.
- **Manual (Correo):** Permite enviar el archivo log con un solo clic. Puede elegir que el servidor SMTP sea detectado automáticamente.

Sección Captura Pantallas: Aquí se podrá configurar si el programa grabará “Ventanas” o “Pantallas”, en que intervalo de tiempo (en minutos), así como la resolución de estas. El porcentaje recomendado es de 75% en calidad.

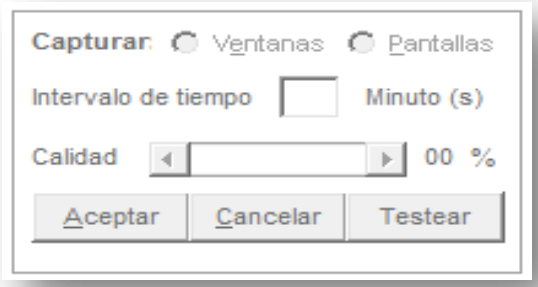


Figura 24: Sección de Captura de Pantallas

- **Botón Aceptar:** Comienza la captura de imágenes automáticamente.
- **Botón Cancelar:** Cancela la captura de imágenes.
- **Botón Teclear:** Mostrará como el programa captura imágenes.

Sección Inferior Adicional: Mostrará el día, la fecha, hora y también la "combinación de teclas" con lo que el programa podrá ser llamado (visualizado). Esta combinación de teclas puede ser "Alt + F1", "Alt + F12", etc. Para configurarlo presione el botón que tiene los puntos suspensivos.

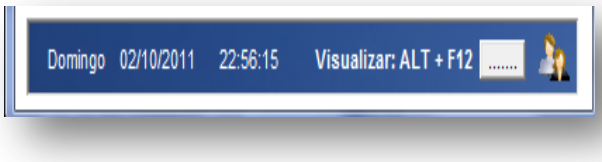


Figura 25: Sección Inferior Adicional

4.2 Fase 2: Diseño del Procedimiento de Monitoreo y Análisis de Información.

1. Conocer la cantidad de equipos y la distribución de los mismos para cada alumno.

2. Configurar el firewall o antivirus para que no bloquee el funcionamiento del programa.

3. Instalar el software Sys_keylogger Advanced en cada computador antes de iniciar el nivel de clases.

4. Configuración Inicio y Recolección de Datos

a) Diseño

✓ Caso de Uso

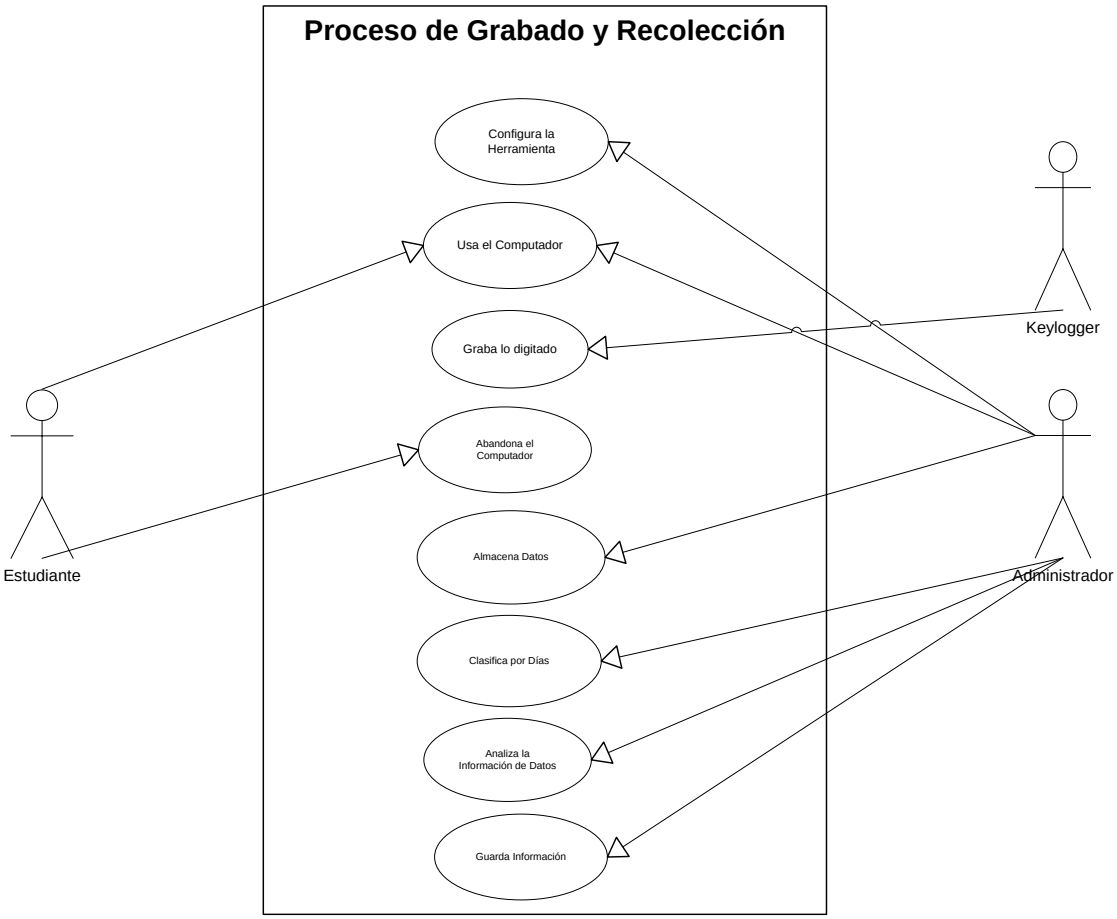


Diagrama 1: Caso de Uso Proceso de Gravado y Recolección

✓ Diagrama de Secuencia

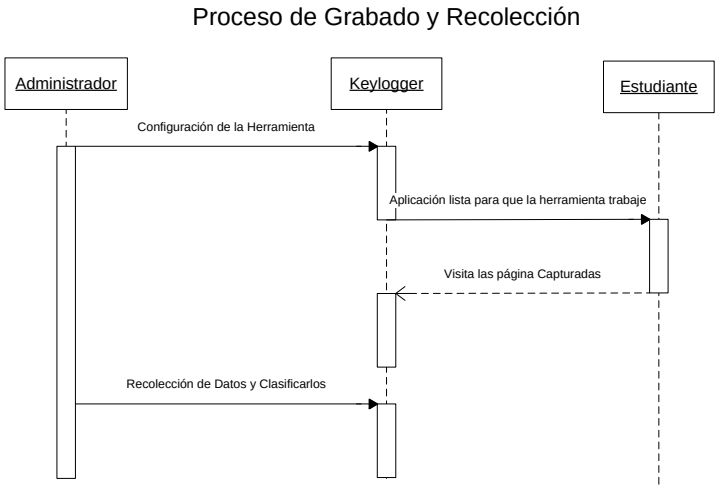


Diagrama 2: Secuencia

✓ Diagrama de Actividad

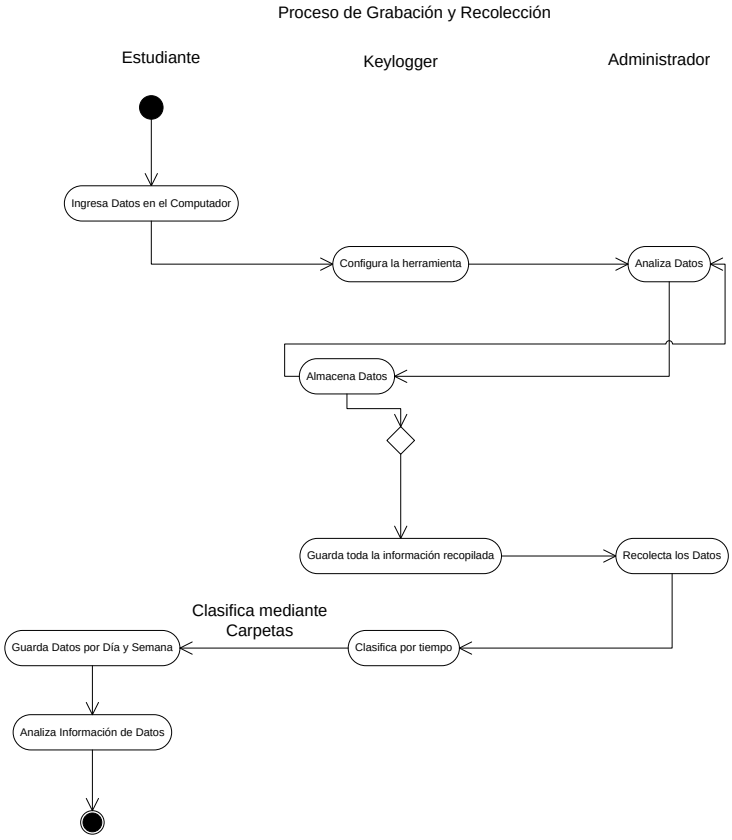


Diagrama 3: Actividad

b) Configuración de la Herramienta

✓ Tiempo

Aquí se podrá configurar si el programa grabará “Ventanas” o “Pantallas”, en que intervalo de tiempo (en minutos), así como la resolución de estas. El porcentaje recomendado es de 75% en calidad.

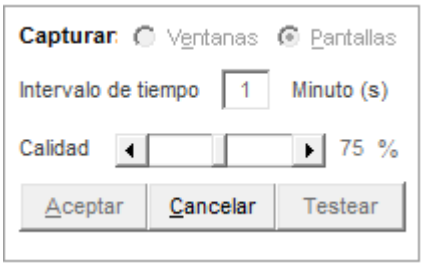


Figura 26: Captura de Datos y Tiempo

✓ Modo de Recolección

Elegimos la Forma en la que queremos Capturar los Datos.

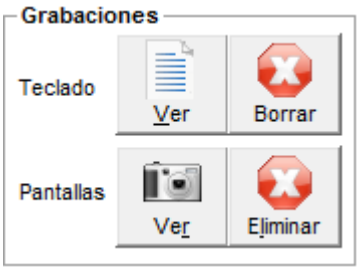


Figura 27: Recolector de Datos

✓ Inicio y Ocultación

Iniciar el funcionamiento de Keylogger en los computadores antes que los estudiantes los usen en el periodo de clases.

Figura 28: Inicio del Programa

Ocultar el software para que no sea visible hacia los estudiantes.

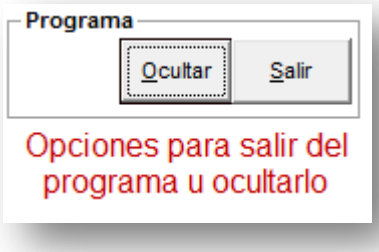


Figura 29: Opciones de ocultar y salir

Se configurará e iniciará la herramienta en cada computador, antes de comenzar la clase, sin que el estudiante se dé cuenta que se encuentre instalado en el computador dicho software nombrado anteriormente.

c) Recolección de Datos

En el momento que ya se encuentra instalado el Keylogger, se ha seguido todos los pasos obtenidos de esta herramienta, se ocultará automáticamente sin que el estudiante se tome precaución que este le esté vigilando en la captura de pantallas y teclados.

- Recolección de datos después de cada horario de clases.
- Recoger los informes de cada máquina que el mismo programa proporciona.

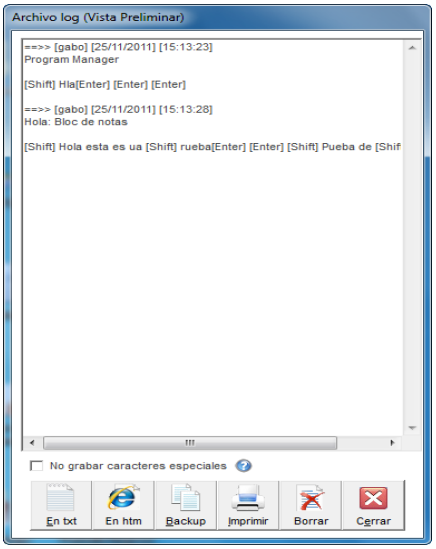


Figura 30: Recolección de datos

- Clasificaremos los datos por fechas, referencia de máquina y periodo de tiempo.
- Clasificación de los datos de interés para el estudio.
    - Páginas visitadas.
    - Tiempo de uso de internet en redes sociales.

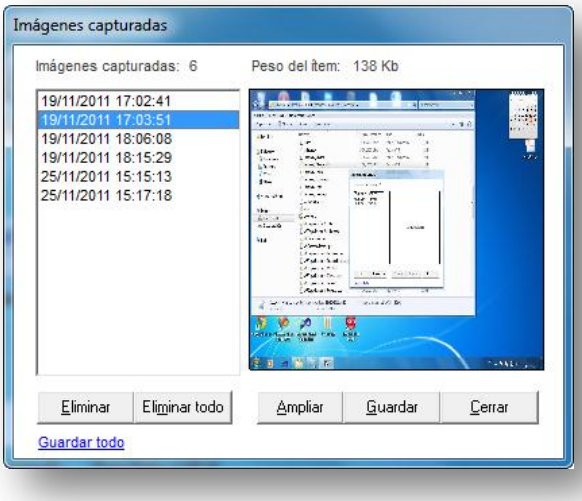


Figura 31: Captura de datos

- Los datos almacenaremos en un lugar seguro para un posterior análisis de los mismos.
- Respaldar información y clasificarlos de la siguiente manera:

2 Semanas	
Carpeta 1	Carpeta 2
1ra. Semana	2da. Semana
Blog de Notas Datos del Día 1	Blog de Notas Datos del Día 1
Blog de Notas Datos del Día 2	Blog de Notas Datos del Día 2
Blog de Notas Datos del Día 3	Blog de Notas Datos del Día 3
Blog de Notas Datos del Día 4	Blog de Notas Datos del Día 4
Blog de Notas Datos del Día 5	Blog de Notas Datos del Día 5

Figura 32: Clasificación de Datos

Cada blog de notas contendrá los resultados de todas las computadoras obtenidos durante cada día.

Al final del conteo de los resultados de las dos semanas será un resultado total de las dos semanas.

- Guardar los datos en lugares de conocimiento y manipulación solo de personal autorizado.
- Realizar regularmente copias de estos respaldos.
- Analizar los datos de forma cuantitativa al final de cada periodo.
    - Por día
    - Por semana

Se utilizará esto puntos para cuantificar las páginas que se visita, las repeticiones o número de veces en cada período y sabe cuáles son las páginas de preferencia para los estudiantes.

4.3 Fase 3: Recolección de Datos y Análisis

a) Primer Día

Red	Facebook	Twitter	Myspace	Hi5	Ninguno
Porcentaje	90	0	0	10	
Cantidad	9			1	

Tabla 12: Recolección Datos (Primer Día)

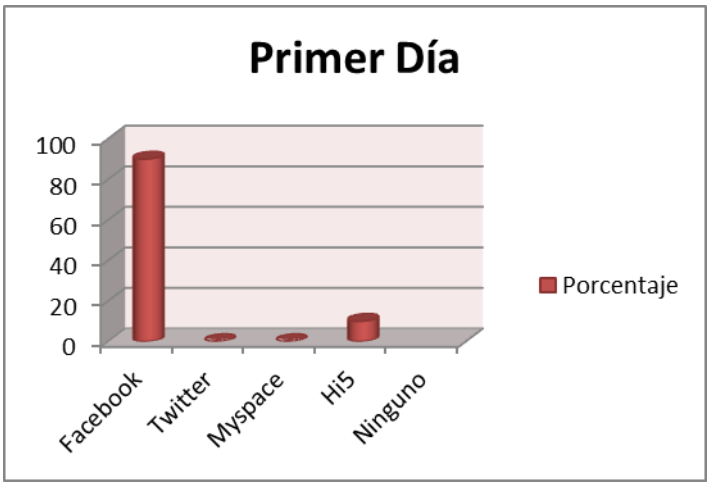


Gráfico 12: Datos del primer día.

Análisis.

En el primer día, el grupo de estudiantes ingresaron a las redes sociales un cien por ciento el cual se distribuye en un noventa por ciento los que usaron Facebook y el diez por ciento el Hi5. En estos resultados vemos que todos los estudiantes ingresan a las redes sociales.

b) Segundo Día

Red	Facebook	Twitter	Myspace	Hi5	Ninguno
Porcentaje	90	0	0	0	10
Cantidad	9	0	0	0	1

Tabla 13: Recolección (Segundo Día)

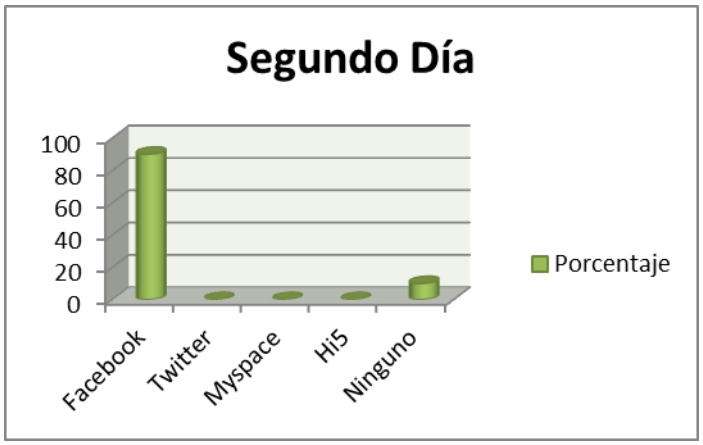


Gráfico 13: Datos del Segundo día.

Análisis.

En el Segundo Día, la información recolectada es que el noventa por ciento usan Facebook y el diez por ciento ninguno quien no ha estado conectado a las redes sociales. Vemos que en el centro educativo cada día los estudiantes usan la red social.

c) Tercer Día

Red	Facebook	Twitter	Myspace	Hi5	Ninguno
Porcentaje	100	0	0	0	0
Cantidad	10				

Tabla 14: Recolección de Datos (Tercer Día)

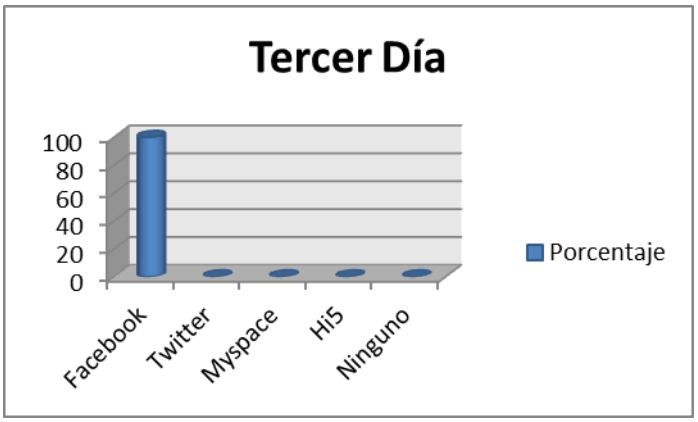


Gráfico 14: Datos del tercer día.

Análisis.

Tercer Día, Según el resultado del día anterior vemos que un cien por ciento los estudiantes usan las redes sociales y la red más usada es el Facebook como esta en el gráfico indicando los resultados.

d) Cuarto Día

Red	Facebook	Twitter	Myspace	Hi5	Ninguno
Porcentaje	80	0	0	0	20
Cantidad	8				2

Tabla 15: Recolección de Datos (Cuarto Día)

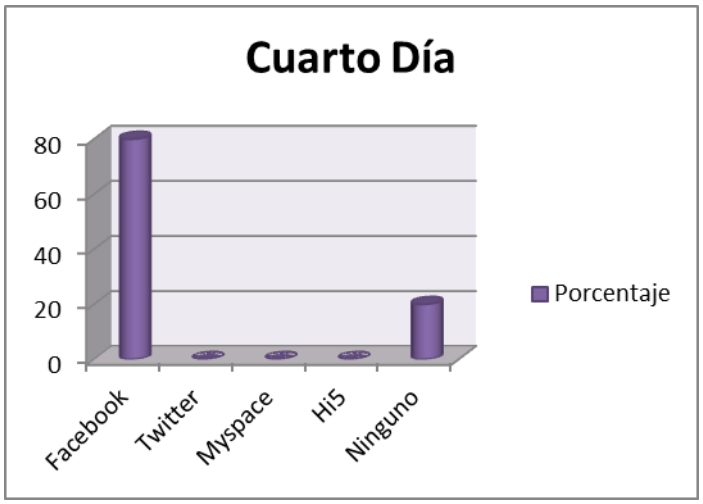


Gráfico 15: Datos del Cuarto Día

Análisis

Cuarto Día, Vemos que los resultados en este día el ochenta por ciento usan la red social que es el Facebook, pero el veinte por ciento no han ingresado a ninguna red social, el cual se puede ver que no siempre ingresan todos los estudiantes a estas redes.

e) Quinto Día

Red	Facebook	Twitter	Myspace	Hi5	Ninguno
Porcentaje	100	0	0	0	0
Cantidad	10				

Tabla 16: Recolección de Datos (Quinto Día)

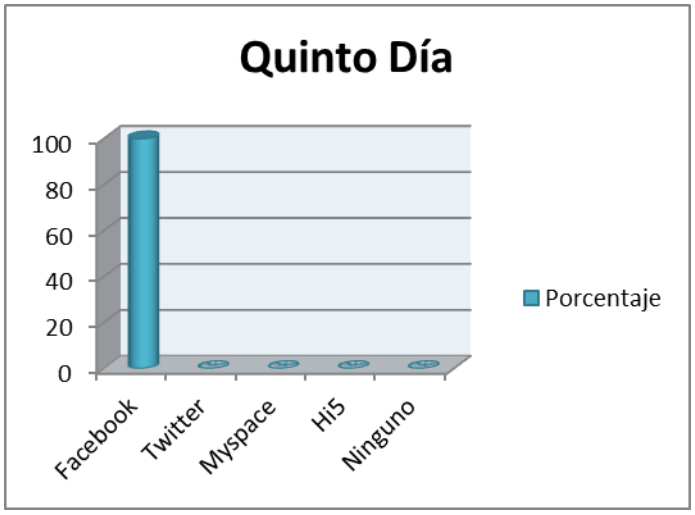


Gráfico 16: Datos del Quinto día

Análisis.

Quinto Día, los resultados que se vieron en este día, los estudiantes han ingresado un cien por ciento lo que es en esta red social, la cual es la más usada por los adolescentes de este centro educativo.

f) Sexto Día

Red	Facebook	Twitter	Myspace	Hi5	Ninguno
Porcentaje	100	0	0	0	0
Cantidad	10				

Tabla 17: Recolección de Datos (Sexto Día)

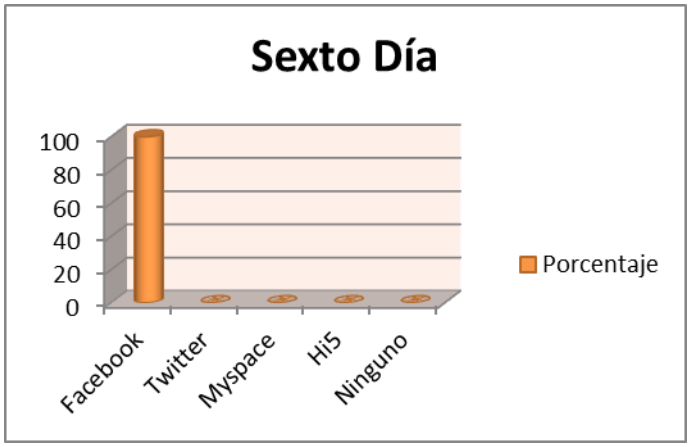


Gráfico 17: Datos del sexto día.

Análisis.

Sexto Día, los resultado son el cien por ciento, en el cual los estudiantes todos han ingresado a una red social, la más conocida es el Facebook y ninguna otra red que se ha visto en estos resultados.

g) Séptimo Día

Red	Facebook	Twitter	Myspace	Hi5	Ninguno
Porcentaje	90	0	0	0	10
Cantidad	9				1

Tabla 18: Recolección de Datos (Séptimo Día)

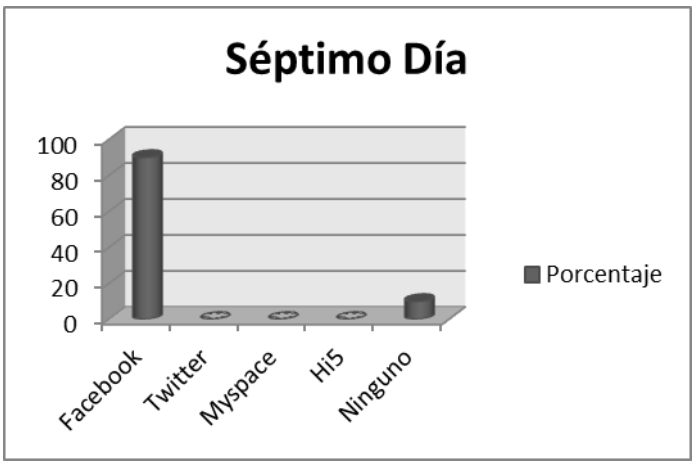


Gráfico 18: Séptimo Día.

Análisis.

Séptimo Día, en estos resultados los estudiantes ingresaron un noventa por ciento en el Facebook y un diez por ciento no han ingresado a ninguna red social.

h) Octavo Día

Red	Facebook	Twitter	Myspace	Hi5	Ninguno
Porcentaje	60	0	0	0	40
Cantidad	6				4

Tabla 19: Recolección de Datos (Octavo Día)

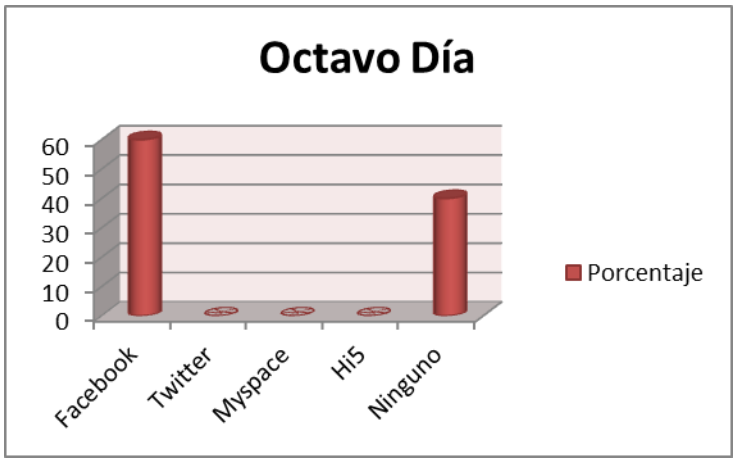


Gráfico 19: Datos del Octavo Día

Análisis.

Octavo Día, los resultados en este día dan una gran diferencia a los días anteriores porque tenemos un sesenta por ciento quienes han ingresado a esta red social, como vemos en el gráfico correspondiente, un cuarenta por ciento de los estudiantes no han ingresado a ninguna red social.

i) Noveno Día

Red	Facebook	Twitter	Myspace	Hi5	Ninguno
Porcentaje	70	0	0	0	30
Cantidad	7				3

Tabla 20: Recolección de Datos (Noveno Día)

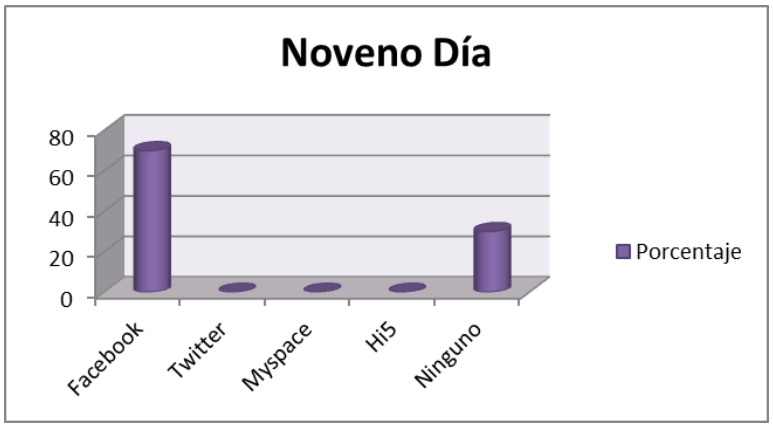


Figura 33: Datos del Noveno Día

Análisis.

Noveno Día, los resultados de este día vemos que es un ochenta por ciento quienes ingresan a las redes sociales, los que no han ingresado este día es un veinte por ciento.

j) Décimo Día

Red	Facebook	Twitter	Myspace	Hi5	Ninguno
Porcentaje	100	0	0	0	0
Cantidad	10				

Tabla 21: Recolección de Datos (Décimo Día)

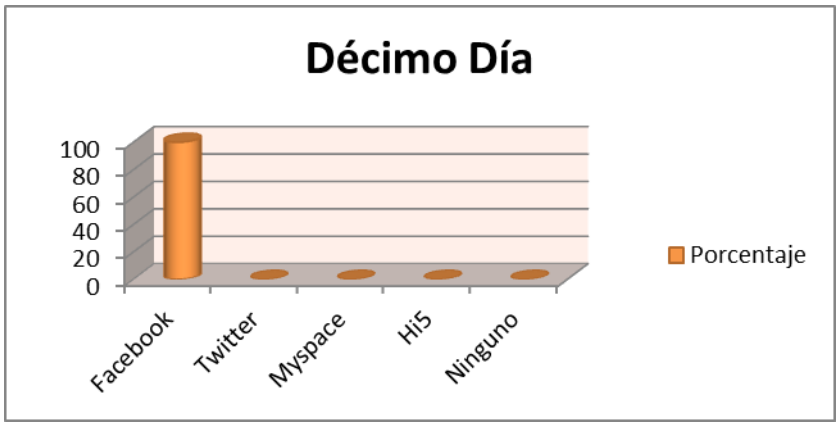


Figura 34: Datos del Décimo Día.

Análisis.

Décimo Día, los resultados vemos que un cien por ciento de los estudiantes ingresan a las redes sociales y la más usa es el Facebook.

k) Visitas Totales de las Dos Semanas

Red	Facebook	Twitter	Myspace	Hi5	Ninguno
Porcentaje	88	0	0	1	11
Cantidad	88	0	0	1	11

Tabla 22: Resultado Total de Visitas en Redes Sociales

Gráfico 20: Resultado Total de dos Semanas.

Análisis

Este proceso se realizó mediante la herramienta Keylogger, se tuvo como objetivo averiguar sobro el ingreso a las redes sociales de los estudiantes en el momento de las horas de clases en el centro educativo, ya que esta red es muy conocida por los adolescentes y exponen sus datos a través del internet.

La recolección de datos a través de dicha herramienta, se realizó a estudiantes que realizan labores académicos mediante el internet, si en este centro educativo, las redes sociales es lo primordial para los adolescentes a través del internet para así tomar precauciones adecuadas.

Con estos resultados tenemos conocimiento suficiente que los estudiantes usan las redes sociales durante las horas de clase, por lo cual vemos que el Facebook es la red más usada por los adolescentes por esta razón es lo que se realizó esta herramienta para tener información de los estudiantes en sus labores académicos. A través de estos datos vemos que los estudiantes no deben exponer su información completa en estas redes en cuestiones de seguridad de datos y prevención, para ellos mismo lo cual los profesores deben estar al pendiente sobre esta información encontrada y así difundir medidas de seguridad de los estudiantes de nuestro centro.

4.4 Fase 4: Realización de propuesta del Uso Académico para la Red Social más visitada.

La importancia de una red, sobre todo de una red académica, es enorme porque permite a los académicos trabajar con flexibilidad, cooperativamente, en el desarrollo académico, científico, técnico, social y cultural en una comunidad, equipo, grupo o región. Permite la integración para la solución de problemas y temáticas comunes, extiende beneficios a funcionarios, educadores, profesores; puede constituirse por instituciones, secretarías; facilita el intercambio de datos, información, conocimiento, y propicia la reflexión.

Es un medio para crear fuentes de financiamiento y ofrece una herramienta a la comunidad. Tiene como fines intercambiar, construir, apoyar conocimientos, abonar a la solución de problemas, incrementar el número de investigadores,

fortalecer posibilidades. Y como objetivos propiciar el uso prioritario de la infraestructura disponible para la interconexión de las redes existentes en la institución e interconectar redes de información, de bibliotecas.

Los profesores deben utilizar las redes sociales con fines didácticos, manteniendo un contacto en vivo y directo con estudiantes fuera de la institución o de las computadoras virtuales.

4.4.1 Creación de Grupos en Facebook.

Permiten tener interacción solo los miembros del grupo, de tal manera esta es una herramienta excelente para el trabajo de docentes fuera de los horarios académicos.

Figura 35: Creación de Grupos.

Los profesores pueden usar el grupo para guiar de mejor manera a los estudiantes, responder inquietudes y presentar resultados de una determinada tarea.

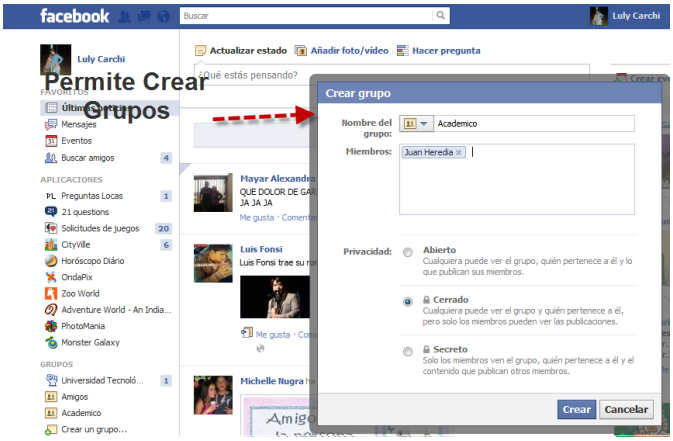


Figura 36: Grupo creado en la Red Social.

En el Facebook existe una opción denominada “grupos”. Se puede añadir miembros y se elige privacidad.

Figura 37: Añadir miembros al Grupo

Existe tres opciones: Abierto (público), cerrado(nadie puede ver su actividad pero el grupo como tal es visible y se conoce sus miembros) o secreto(el grupo es invisible salvo para sus miembros, a los que solo el administrador puede añadir).

Figura 38: Administra Grupo de Privacidad.

Una vez creado el grupo, es posible configurar varias opciones pulsando "Editar grupo" (entrando en el grupo, en el lateral derecho).

Es importante seleccionar la opción "solo los administradores pueden aprobar las solicitudes para unirse al grupo", a fin de evitar que otros usuarios puedan añadir a terceros.

Los estudiantes no forman parte del círculo de amigos del docente, es necesario añadirlos y otorgarles el rol adecuado. Facebook ha añadido recientemente una serie de roles predefinidos.

Figura 39: Miembros del Grupo.

Para que los estudiantes no accedan a la información y actividad personal es necesario asignarles el rol “Acceso restringido”.

También es recomendable otorgarles otro rol, por ejemplo “Estudiantes”, por si al finalizar la actividad se desea eliminar a los usuarios y distinguirlos de otros potenciales amigos de acceso restringido que no son estudiantes. Con esto, el docente se asegura de que los estudiantes no acceden a su información, pero los estudiantes deberían hacer lo mismo con el profesor incorporándoles a su lista de “acceso restringido”. Alternativamente, el docente puede pulsar el nombre de cualquiera de sus estudiantes y, pulsando el botón “Suscrito” que aparece en la parte superior derecha seleccionar “Cancelar la suscripción”. Así dejará de recibir cualquier información del estudiante en su muro.

Figura 40: Realización de Actividades en el Grupo de Facebook.

4.5 Fase 5: Desarrollo de Seguridad para el uso de Redes Sociales en Instituciones Educativas.

¿Cómo proteger a los estudiantes?

Los profesores pueden proteger a sus estudiantes contra los depredadores de la Internet y el material para adultos siguiendo algunos consejos de seguridad. Insista en que los adolescentes tomen las siguientes precauciones cuando se conecten:

- No deben revelar nunca información personal como dirección, número de teléfono, nombre o dirección de la escuela. Deberían utilizar siempre un nombre falso.
- No deben aceptar conocer a nadie de un foro en persona.
- No deben intercambiar fotografías personales por correo ni enviar fotografías escaneadas por la Internet.
- No responder nunca a mensajes en tono amenazante.
- Deben avisar siempre a los padres si reciben algún comentario o mantienen una charla que les atemoriza.
- Si un estudiante tiene un nuevo "amigo", pídale que se lo presente en línea.

Para proteger a los estudiantes es necesario:

- Aprender a usar la computadora y a bloquear el acceso a páginas censurables.
- Ubique la computadora en un lugar de la casa de uso familiar y no en habitaciones individuales para poder vigilar y supervisar a sus hijos.
- Comparta la dirección de correo electrónico con su hijo para poder supervisar los mensajes.

- Confeccione una lista de "favoritos" con las páginas preferidas de su hijo para tener acceso directo a ellas.
- Navegue con ellos para enseñarles a comportarse adecuadamente.
- Averigüe qué protección en línea ofrecen la escuela, el centro de cuidado infantil después del horario escolar y las casas de los amigos de su hijo, o cualquier lugar en el que el niño podría usar una computadora sin su supervisión.
- Una buena forma de proteger a los estudiantes es enseñarles cómo usar la Internet de manera segura. La Internet ofrece información muy útil y puede ayudar a los estudiantes a ampliar sus horizontes de maneras desconocidas por las generaciones anteriores.
- Para mejorar las medidas de seguridad y violación de privacidad a los estudiantes y personas con poco conocimiento informático es recomendable advertir y comunicar sobre estos peligros.
- El aislamiento potencial en las redes sociales, la educación y el comportamiento social, Mejorará la educación es la medida más importante para conseguir no sólo reducir la violencia juvenil, sino tener mejores profesionales y gente mejor formada que pueda evolucionar el mundo, haciendo un trabajo superior a las generaciones anteriores.
- Limitar el acceso a ciertas páginas durante horarios de clases como por ejemplo: Facebook.
- Crear perfiles de red para el uso de internet limitando accesos de acuerdo a los usuarios como por ejemplo Profesores, estudiantes, etc.
- Si se tiene redes de acceso de internet limitar la banda red que usan los estudiantes.

- Controlar el acceso de los estudiantes a material adulto y minimizar el riesgo de atraer delincuentes cuando navega por la Internet. Los expertos concuerdan en que lo más importante que los padres y las personas a cargo del cuidado de los estudiantes pueden hacer para protegerlos contra los peligros de la Internet es controlar sus actividades y educarles sobre los riesgos del ciberespacio.

- **Software bloqueador**

El software bloqueador prohíbe o bloquea el acceso a páginas consideradas "impropias" que aparecen en una lista establecida por el propietario de la computadora. Las actualizaciones de la lista varían según el fabricante. Recuerde que el número de páginas Web nuevas que se publican cada día excede la capacidad de cualquier compañía de software para actualizar una lista de "sitios impropios" y algunas de las páginas para adultos escapan al bloqueador.

Software de filtrado Los programas de software de filtrado utilizan palabras clave para bloquear las páginas que contienen estas palabras solas o en diferentes contextos. Una de las críticas que reciben los filtros es que bloquean páginas que no son necesariamente ofensivas.

El filtrado de salida restringe la información personal (nombre, dirección, número de teléfono) para que no aparezca en la red. Los defensores de la

seguridad en la Internet consideran que es más peligroso dar datos personales a extraños que visitar una página Web pornográfica.

Software de seguimiento y rastreo La mayoría de las computadoras en las escuelas incluyen hoy en día software de seguimiento y rastreo, además de bloqueadores para saber por dónde navegan los estudiantes. Estos programas brindan información sobre la cantidad de tiempo que han estado conectados, las páginas visitadas y el tiempo que han trabajado sin estar conectados. También hay un programa de software parecido disponible para las computadoras domésticas.

- **Herramientas de bloqueador de Internet**
  - Inet Protector
  - Titanium máximum security
  - Bitdefender internet security 2012
  - PicBlock

A continuación se detalla uno de ellos:

- ✓ **Inet Protector**

Es básicamente un programa preparado para bloquear la conexión a los sitios no deseados en internet desde un ordenador con sólo establecer una contraseña.

Es un programa cuya licencia es de evolución, es decir, el uso de funcionalidades es ofrecida por tiempo limitado. Está libre de antivirus, está validado.

Una de las versiones más conocidas es la de inet protector 4.6 disponible en diferentes portales de internet. Es compatible con sistemas operativos Windows 2000, XP, vista y Windows 7.

Figura 41: Pantalla Inet Protector

El mecanismo de este software de evolución es muy fácil de utilizar. Permite elegir manualmente las funciones de protección como programarlo en el tiempo bloqueado las conexiones a determinados horarios.

Es posible, un bloqueo prácticamente, solo tiene que seleccionar aquellos lugares inaccesibles.

Optimizar al máximo los tiempos de navegación y se simplifican de manera considerable las tareas de protección debido a que las configuraciones determinadas se protegen a través de un nombre de usuario y contraseña.

Dispone de una función de control parental con la que restringe determinados portales de internet que puede contener contenido peligroso para menores.

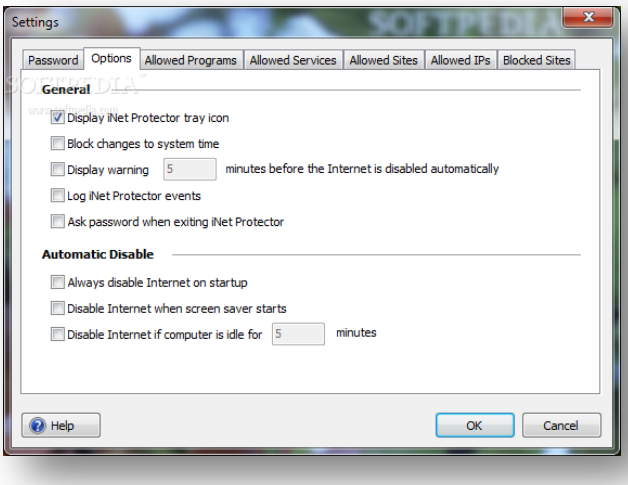


Figura 42: Opciones Inet Protector

Es la solución idónea para aquellos que necesitan restringir de manera muy específica y segura el uso de internet en entornos educativos.

4.6 Fase 6: Comparación de Ventajas y Desventajas de Keylogger frente a otras herramientas

- ✓ **VENTAJAS**

Sys_keyloggerAdvanced y Sniffer mediante un registrador de teclas.

PROFESORES	ESTUDIANTES	SOFTWARE
		
• Verificar si el uso del Internet es aceptable • Observar la productividad de profesores • Detectar intentos de acceso no autorizado • Hacer copia de seguridad del texto tecleado • Elaborar estadísticas de uso del ordenador	• Controlar el uso del ordenador en la familia • Proteger a los estudiantes contra los riesgos o acosadores en la red • Observar el uso de www, e-mail y chat • Guardar copia de los documentos creados	• Controlar ordenadores a distancia • Recuperar contraseñas desconocidas, independientemente del sistema operativo • Recoger pruebas relacionadas al ordenador • Detectar intentos de acceso no autorizado al ordenador y al equipamiento

Figura 43: Ventajas del Sys_keyloggerAdvanced

✓ **Ventajas y Desventajas**

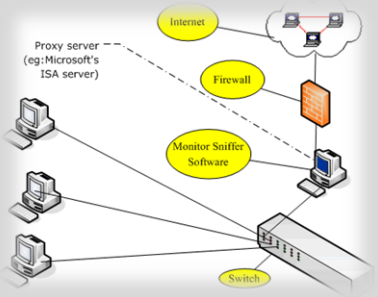
	Sys_KeyloggerAdvanced	Sniffer
		
Lectura	Actúa en la Maquina (PC)	Actúa en la Red
Captura	Acciones de Teclado y Pantalla	Paquetes que están en el Trafico de la Red
Contramedida con Encriptación	No es débil contra el encriptación	Es débil contra la encriptación
Forma de Trabajo	Trabajo Invisible en la PC	Trabaja a nivel de Red
Seguridad	Se Visualiza la Herramienta con el Uso de Contraseña	Solo aquel que tiene el software puede manipularlo
Seguridad de detección por antivirus	Es detectable por algunos antivirus	No es detectable, pues trabaja a nivel del tráfico de red.

Figura 44: Ventajas y Desventajas de Keylogger y Sniffer

5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Mediante el Keylogger pudimos observar a los estudiantes que en el momento de clases usan las redes sociales.

Las redes sociales se han vuelto parte de nosotros, es una forma de expresarnos y de comunicarnos, pero es muy importante darnos cuenta de que manera influye en nuestro mundo y como nos afectara en un futuro.

Las Redes Sociales han cobrado un papel fundamental en la vida cotidiana, ya sea de jóvenes como de adultos. Es sumamente importante entender qué son y cuáles son sus funciones para comprender la dimensión de estas. Consideramos que las Redes Sociales son "estructuras sociales" compuesta por un número de personas, las cuales se conectan por uno o varias razones por ejemplo amistad, parentesco, intereses comunes o compartir conocimientos laborales y/o académicos. Las Redes Sociales nos permiten interactuar con varias personas, aunque no las conozcamos, nos da la posibilidad de compartir nuestros intereses.

5.2 RECOMENDACIONES

Luego de haber realizado un estudio sobre las dificultades que se presentan dentro de las instituciones educativas, en cuanto al excesivo uso del Internet para visitar Páginas o Sitios Web no relacionados con algún tema Académico, se encontró que la mayor parte del tiempo académico en los períodos de clases los estudiantes enfocaban su tiempo a este tipo de páginas como Facebook.

De acuerdo con esto se recomienda lo siguiente:

- ✓ **Profesores:** Buscar y mejorar los conocimientos sobre internet Y Redes Sociales, para poder orientar a los estudiantes en cuanto a seguridad y mejor administración del Tiempo Educativo.
- ✓ **Estudiantes:** Usar Redes Sociales en tiempos libres, pero sobre todo para buscar formas de aprendizaje, y si es por distracción tener todos los cuidados posibles como poner información real o confidencial que otras personas ajenas puedan ver y causar daño.
- ✓ **Padres de Familia:** Tener una mejor Relación en cuanto a confianza se refiere, para poder guiar a los hijos sobre cuidados preventivos acerca del uso de Internet principalmente en Redes Sociales como Facebook, donde los adolescentes están expuestos a cualquier tipo de peligro invisible.

Según lo mencionado anteriormente se buscó a través del trabajo realizado dar solución a este gran inconveniente que en establecimientos educativos se tienen, por tanto, una solución que se dio a conocer fue la creación de Grupos en Facebook para procesos Académicos, debido a que es una herramienta gratuita, accesible y sobre todo muy apegada a la adolescencia de hoy en día.

GLOSARIO

- **Keylogger.** Programa que recoge y guarda una lista de todas las teclas pulsadas por un usuario. Dicho puede hacer pública la lista, permitiendo que terceras personas conozcan estos datos lo que ha escrito el usuario afectado (información introducida por el teclado: contraseña, texto escrito en documentos, mensajes de correo, combinaciones de teclas, etc.).

- **Malware.-** Software maliciosos que tiene como objetivo infiltrarse o dañar una computadora.

- **Firewalls.-** Es un dispositivo de software y hardware que protege los recursos de una red privada de los usuarios de otras redes.

- **Teclado Virtual.-** Teclado a través del uso del internet.

- **Antivirus.**- Software de protección contra infecciones de virus. Se encarga principalmente tanto de prevenir infecciones como limpiarlas en el PC.

- **Virus.-** tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus informáticos son programas, destructivos, que se introducen en el computador y pueden provocar perdida de información almacenada en discos duros.

- **Sniffer. -** Herramienta se software y hardware que interceptan tráfico en una red y lo muestran en distintos formatos. Puede capturar paquetes o tramas.

- **Sys_ Keylog 1.3.-** En todas sus versiones y presentaciones fue creado con el objeto de proteger a los niños y adolescentes, monitoreando las actividades que realizan en el ordenador mientras nos ausentamos. Esto para evitar que sean presa de tantos pedófilos y corruptores de menores que existen en red.

BIBLIOGRAFIA

- ✓ *Glosario*. (16 de Marzo de 2007). Recuperado el Martes de Septiembre de 2011, de http://tecnologia.glosario.net/terminos-viricos/keylogger-(capturador-de-teclado)-9765.html
- ✓ *Michfer*. (7 de Agosto de 2008). Recuperado el Martes de Septiembre de 2011, de http://michfer.wordpress.com/2008/08/07/redes-sociales-definicion/
- ✓ *Mexicoglobal*. (2010). Recuperado el Miercoles de Septiembre de 2011, de http://www.mexicoglobal.net/informatica/keylogger.asp
- ✓ *Tecnopadres*. (22 de Abril de 2010). Recuperado el Lunes de Septiembre de 2011, de http://tecnopadres.aollatino.com/2010/04/22/cuatro-adicciones-comunes-redes-sociales/
- ✓ *Alegsa*. (Marzo de 2011). Recuperado el Octubre de 2011, de http://www.alegsa.com.ar/Dic/seguridad%20informatica.php
- ✓ *Alegsa*. (2011). Recuperado el Martes de Septiembre de 2011, de http://www.alegsa.com.ar/Dic/keylogger.php
- ✓ *Bitdefender*. (2011). Recuperado el Martes de Septiembre de 2011, de http://www.bitdefender.es/
- ✓ *Definicion.de*. (2011). Recuperado el Septiembre de 2011, de http://definicion.de/seguridad-privada/
- ✓ *Portalprogramas*. (2011). Recuperado el Martes de Septiembre de 2011, de http://gratis.portalprogramas.com/PicBlock.html
- ✓ *Trendmicro*. (2011). Recuperado el Lunes de Septiembre de 2011, de http://es.trendmicro.com/es/home/
- ✓ *Wikitel*. (2011). Recuperado el Martes de Septiembre de 2011, de http://wikitel.info/wiki/Redes_sociales

✓ Fernandez, B. (2010). *Las redes sociales. Lo que hacen sus hijos en internet.* Club Universitario.

ANEXOS

Anexo 1: Encuestas Realizadas

Encuesta para estudiantes del centro educativo sobre el uso de las redes sociales.

1) **Para realizar sus tareas usa usted el internet?.**

   Sí ☑ No ☐

2) **En que utiliza más la internet?.**

   Labores Académicas ☑ Diversión ☐

3) **Si eres parte de alguna red social, indicar cuál de ellas?.**

   Facebook ☑ hi5 ☐ MySpace ☐ Twitter ☐

   Otros ☐

4) **En horas de clases cuanto tiempo estas conectado en alguna red social?.**

   0 horas ☑ 1 a 3 horas ☐ 3 a 5 horas ☐

   más de 5 horas ☐

5) **Considera usted que las redes sociales son medios efectivos para compartir información?.**

   Sí ☑ No ☐

6) **Con que frecuencias usa la internet?.**

   Siempre ☐ De vez en cuando ☑ Casi nunca ☐

7) **Cree usted que las redes sociales son de utilidad para las personas?.**

   Sí ☑ No ☐

8) **Conoce usted acerca sobre los peligros que hay en internet?.**

   Sí ☐ No ☑

9) **Que tan alto es el riesgo al publicar su información personal en las redes sociales?.**

   Bajo ☐ Medio ☑ Alto ☐

10) **Piensa usted que el robo de información en internet es algo real?.**

    Sí ☐ No ☑