UNIVERSIDAD TECNOLOGICA ISRAEL

FACULTAD DE SISTEMAS INFORMATICOS

Análisis sobre las Amenazas Humanas y Lógicas contra la Seguridad Informática VS La Protección de Información

Estudiante

Aníbal Manuel Guachichulca Romero

Tutor

Ing. Mario Mejía

Cuenca - Ecuador

Noviembre 2012

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMASINFORMÁTICOS

CERTIFICADO DE RESPONSABILIDAD

Yo Ing. Mario Mejía. Certifico que el Sr. Aníbal Manuel Guachichulca Romero con C.C. No. 0105668123 realizó la presente tesina con título "**Análisis sobre las Amenazas Humanas y Lógicas contra la Seguridad Informática VS La Protección de Información**", y que es autor intelectual del mismo, que es original, autentica y personal.

_____

Ing. Mario Mejía

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMASINFORMÁTICOS

ACTA DE CESION DE DERECHOS

Yo, Aníbal Manuel Guachichulca Romero, estudiante de Ingeniería de sistemas informáticos, declaro conocer y aceptar las disposiciones del Programa de Estudios, que en lo pertinente dice: "*Es patrimonio de la Universidad tecnológica Israel, todos los resultados provenientes de investigaciones, de trabajos científicos, técnicos o tecnológicos y de tesis o trabajos de grado que se realicen a través o con el apoyo de cualquier tipo de la Universidad tecnológica Israel. Esto significa la cesión de los derechos de propiedad intelectual a la Universidad tecnológica Israel*".

_____

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMATICOS

CERTIFICADO DE AUTORIA

El documento de tesis con títulos **"Análisis sobre las Amenazas Humanas y Lógicas contra la Seguridad Informática VS La Protección de Información"** ha sido desarrollado por Aníbal Manuel Guachichulca Romero con C.I. No. 0105668123 persona que posee los derechos de Autoría y responsabilidad, restringiéndose la copia o utilización de cada uno de los productos de esta tesina sin previa autorización.

Aníbal Manuel Guachichulca Romero

DEDICATORIA

Con todo amor y respeto a mi mama, Sra. Rosa Adolfina Romero Paucar. Es a usted a quien debo toda la persona que soy. Gracias por su guía y ejemplo durante todos los años de mi vida. Te quiero.

Con cariño para mi papa Sr. Manuel Antonio Guachichulca López quien me ha inculcado el respeto y el valor de mi personalidad.

Con todo mi corazón, aprecio y respeto a mi querida tía, quien ha sido para mí, la segunda mamá que dios me ha dado, la que siempre he amado y llevado en mi corazón todos los días, gracias por ese apoyo incondicional y por enseñarme a caminar en la vida desde niño.

Para Mayra ErráezTenesaca. Por tu infinita paciencia por tu tierna compañía y tú inagotable apoyo. Por compartir mi vida y mis logros estos años de estudio superior en todas las formas imaginables.

Para Anthonny Guachichulca Erraez, Que es mi inspiración y fuerza para seguir adelante en el estudio y el trabajo, por permitirme descubrir contigo lo hermoso que es ser papa, por esto y más esta tesina también es tuya, te amo mi nene precioso.

Para mis hermanos, Judith, Juan y Lizandro, Con quienes he compartido mi vida, quienes me vieron llorar y me han alegrado la vida, los quiero mucho ñaños.

Y finalmente mi dedicación va a la memoria de mi abuelita querida María Dolores López Loja.

AGRADECIMIENTO

En primer lugar agradezco a Dios, por mantenerme con vida y salud, agradezco también a mis padres y a mi tía, quienes han hecho lo posible por apoyarme día tras día en los gastos de mis estudios, como también le estoy profundamente agradecido a los profesores que me formaron y me bridaron sus conocimientos todos estos años hasta la fecha, en especial agradeciéndole a mi director de tesis al Ing. Mario Mejía.

Finalmente agradezco ala Universidad Tecnológica Israel por haberme abierto las puertas a hacia un futuro sabio.

RESUMEN

Debido a que el uso de Internet se encuentra en aumento, cada vez más compañías permiten a sus socios y proveedores acceder a sus sistemas de información. Por lo tanto, es fundamental saber qué recursos informáticos necesitan, protección para así controlar el acceso al sistema y los derechos de los usuarios.

Además, debido a la tendencia creciente hacia un estilo de vida nómada de hoy en día, el cual permite a los empleados conectarse a los sistemas de información casi desde cualquier lugar, se pide a los empleados que lleven consigo parte de la información fuera de la infraestructura.

Los riesgos, en términos de seguridad, se caracterizan como, amenaza que representa el tipo de acción que tiende a ser dañina, mientras que la vulnerabilidad representa el grado de exposición a las amenazas en un contexto particular. Finalmente, la contramedida representa todas las acciones que se implementan para prevenir la amenaza.

Las contramedidas que deben implementarse no sólo son soluciones técnicas, sino también reflejan la capacitación y la toma de conciencia por parte del usuario, además de reglas claramente definidas.

Para que un sistema sea seguro, deben identificarse las posibles amenazas y por lo tanto, conocer y prever el curso de acción del enemigo. Por tanto, el objetivo de esta tesina es brindar una perspectiva general de las posibles motivaciones de los hackers, las amenazas humanas y lógicas para dar una idea de cómo funcionan para conocer la mejor forma de reducir el riesgo de intrusiones.

SUMMARY

Because the use of Internet is in increase, more and more companies allow their partners and suppliers to consent to their systems of information. Therefore, it is fundamental to know what computer resources they need; protection stops this way to control the access to the system and the rights of the users.

Also, due to the growing tendency toward today's nomadic lifestyle in day, which allows the employees to be connected to the systems of information almost from any place, is requested to the employees that take I get part of the information outside of the infrastructure.

The risks, in safe-deposit terms, are characterized as, threatens that it represents the action type that spreads to be harmful, while the vulnerability represents the exhibition grade to the threats in a particular context. Finally, the measure represents all the stocks that are implemented to prevent the threat.

The measures that should be implemented is not only technical solutions, but they also reflect the training and the taking of conscience on the part of the user, besides clearly defined rules.

So that a system is safe, the possible threats should be identified and therefore, to know and to foresee the act of public enemies course. Therefore, the objective of this Project is to offer a general perspective of the possible motivations of the hackers, the human threats and logics to give an idea of how they work to know the best form of reducing the risk of intrusions.

TABLA DE CONTENIDOS

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

1.- Introducción

En la actualidad el tema sobre los “hackers” es muy común, podemos verlo en revistas, periódicos, etc. Aunque no podemos decir que todas estas personas que entran a la red tienen buenos propósitos, tampoco podemos decir que todos son malos, existen personas buenas, malas y los que pasan desapercibidos.

El principal objetivo de este proyecto es mostrar a los lectores los posibles riesgos que pueden tener al estar frente a un ordenador y como defenderse de ellos. Para conseguir esto, en este trabajo se ha estudiado las amenazas humanas, lógica y la protección de la información, reconociendo el medio en el que navegamos y donde habitan los mayores riesgos de Internet para conocer los diferentes tipos de personas con los que nos podemos topar en este submundo, Métodos de ataque, Analizar los diferentes medios y amenazas que nos rodean, y por último, Métodos de defensa, conocer las soluciones que nos ofrece Internet para defendernos de los problemas que se pueden encontrar, y así no sufrir las molestias que nos proporciona Internet.

Los ataques en la red son muy comunes hoy en día, esto lo podemos ver con la alteración de los muchos usuarios cuando llega un nuevo virus, o cuando dicen que alguien está atacando los sistemas de mensajería más comunes (MSN Messenger y yahoo Messenger) o redes sociales (Facebook, Twiter, Badoo etc.). Mucha gente está alerta de esto, y los sistemas de protección siempre tienen que estar al tanto de la situación. Existe mucha gente en la red que lo hace por ganar popularidad o solo con el objetivo de molestar al amigo, pero detrás de todo esto existen otras razones, como el libre comercio y la libre difusión de la información. La mayoría de los crackers y hackers desean la libre distribución de la información, y la eliminación del comercio en

Internet, por eso apoyan a los creadores del software gratuito y se empeñan en derrochar a las grandes empresas que comercian como Microsoft, para que dejen los códigos de fuente de sus programas de forma gratuita en la red, y así pueda ser modificada para beneficio de ellos o los demás cibernautas. Como podemos ver para los sistemas que siguen la licencia libre, los virus y las aplicaciones destructivas son muy pocas, pero para los sistemas comerciales existe una gran variedad de aplicaciones dañinas, con el fin de convencer a estas grandes compañías a distribuir sus creaciones de forma gratuita.

Un ejemplo son los video juegos, ya que aproximadamente el 80% de estos se encuentran de forma gratuita en la red, esto se debe a que los crackers han hecho vulnerables los sistemas de seguridad de estas aplicaciones para que así puedan ser usados por todas las personas.

Es tradicional que en todo lo bueno exista algo malo y viceversa, por esto también estudiaremos los problemas que están presentes cada vez que nos encontramos frente a un ordenador o conectados a Internet,seintentara aclarar varias dudas sobre el funcionamiento de las herramientas y de las estrategias utilizadas para defender una maquina en este mundo tan hostil.

1.1. Antecedentes

Hoy en día las técnicas de espionaje se han perfeccionado tanto que cualquier medio puede ser portador de un código maligno que amenace nuestra privacidad, desde recibir un email hasta recibir ataques premeditados son amenazas que poden a prueba nuestra capacidad de respuesta ante la peor situación. Estos últimos años hemos asistido a u ataque a nivel global derivado del llamado Malware, software poco detectable que es capaz de cambiar la configuración del ordenador, o robar la información personal para venderla a terceras personas.

En el Ecuador la seguridad de la Información es muy pobre porque no poseemos las suficientes empresas con conocimiento sobre este de tema que si tienen los países más poderosos y que brinden estos servicios para que puedan poner en práctica todos los conocimientos empresariales adquiridos. La seguridad de la información es una necesidad hoy en día, ya que las empresas manejan grandes cantidades de datos los cuales pueden ser analizados, de tal manera que se pueda encontrar información relevante para tomar diferentes cursos de acción. La seguridad de la información forma parte de las estrategias corporativas, ya que la comunicación e información son de gran valor en las organizaciones o empresas, porque representan poder.

En el Ecuador existen muy pocas empresas que poseen la seguridad de la información porque en algunos casos desconocen de su existencia o de su funcionalidad.

Lo cierto es que el mundo de hoy, donde las tecnologías de la información avanzan a grandes velocidades, es cada vez más vulnerable al ataque de estos individuos. El taques

hackers es uno de los temas preocupantes que se vienen sucediendo en el mundo y causando un pánico generalizado.

Un ejemplo de esto es que los piratas cibernéticos conocidos como TheWikiBoat planean dejar fuera de servicio los sitios web de las empresas mundiales durante al menos dos horas y difundir valiosos datos privados. Estos hacktivistas podrían tener vínculos con Anonymous, que es la red pirata de hackers informáticos.

Quizás el segundo temas más famosos en el mundo sobre los que más mitos e historias fantásticas se corren en el ámbito informático sean los Virus.

Todos y cada uno de estos violan la seguridad informática dentro y fuera del país

1.2. Formulación del Problema

La situación actual nos da a conocer que los sistemas informáticos son el activo más valioso y al mismo tiempo el más vulnerable, dada las cambiantes condiciones y nuevas plataformas de converge en la aparición de nuevas amenazas en los sistemas informáticos. Generalmente no se invierte ni el capital humano ni económico necesario para prevenir el daño y/o pérdida de la información confidencial, a raíz de ello han surgido muchos problemas relacionados con el uso de computadoras, amenazas que afectan negativamente tanto a usuarios como a empresas; la proliferación de la computadora como la principal herramienta, así como la creación de la red global Internet ha provocado que cada vez más personas se las ingenien para lucrar, hacer daño o causar perjuicios.

El acceso no autorizado a un sistema informático, consiste en acceder de manera indebida, sin autorización, a un sistema de tratamiento de información, con el fin de obtener una satisfacción de carácter intelectual y/o económico por el desciframiento de los códigos de acceso o password.

La idea de la investigación es realizar un estudio de las amenazas humanas y lógicas en contra de la seguridad informática vs protección de información, que permitirá conocer el estado actual de la seguridad informática, permitiendo también proponer alternativas de mejoras a éstas.

¿Se logrará posesionar en la mente de los usuarios la Protección de Información a través del análisis sobre las Amenazas humanas y lógicas contra la seguridad informática?

1.3. Sistematización

1.3.1. Diagnostico

Las amenazas de seguridad informática de forma lógica o humana se han convertido en una adición a personas con conocimientos altos de forma maliciosa para hacer daño o extraer información confidencial de un usuario o de las organizaciones, identificando las causas y efectos

Causas	**Efecto**
Espionaje, modificación o robo de datos por intrusos en la red	Para obtener fines económicos o diversión
Ataques y estafas en la red	Por el uso ilegal del internet y las

	herramientas de software
Daños de la información y equipos de computo	Por la existencia y evolución de los virus informáticos.
Mecanismo de defensa de la información vulnerados por nuevas amenazas	Por la implementación de la seguridad sin la capacitación actual y tecnología adecuada.

Tabla N°: 1 Cuadro Causa - Efecto
Autor: Aníbal Guachichulca

Procesos actuales

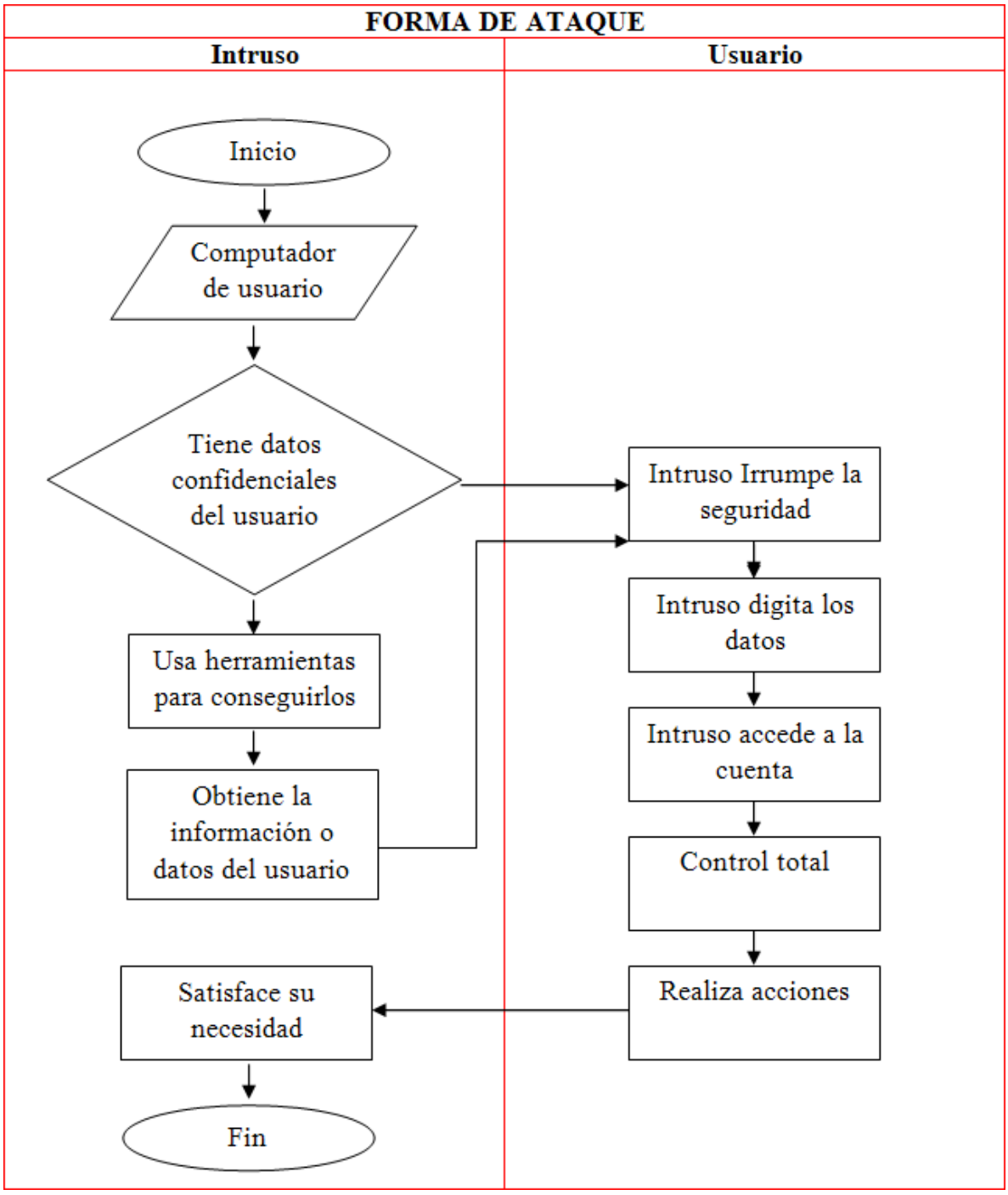


Ilustración N°: 1Diagrama de Flujo – Forma de ataque
Autor: Aníbal Guachichulca

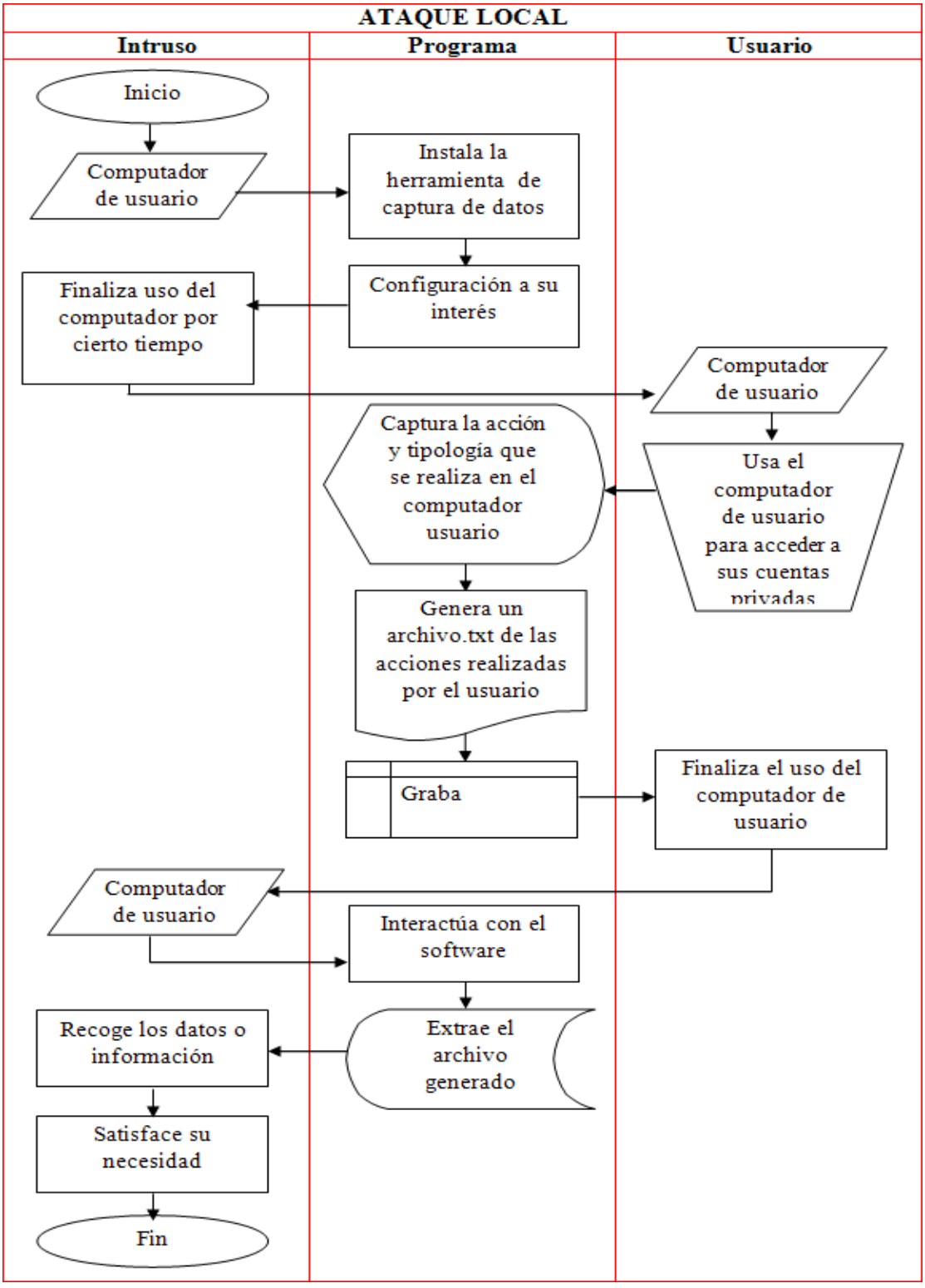


Ilustración N°: 2Diagrama de Flujo – Ataque Local
Autor: Aníbal Guachichulca

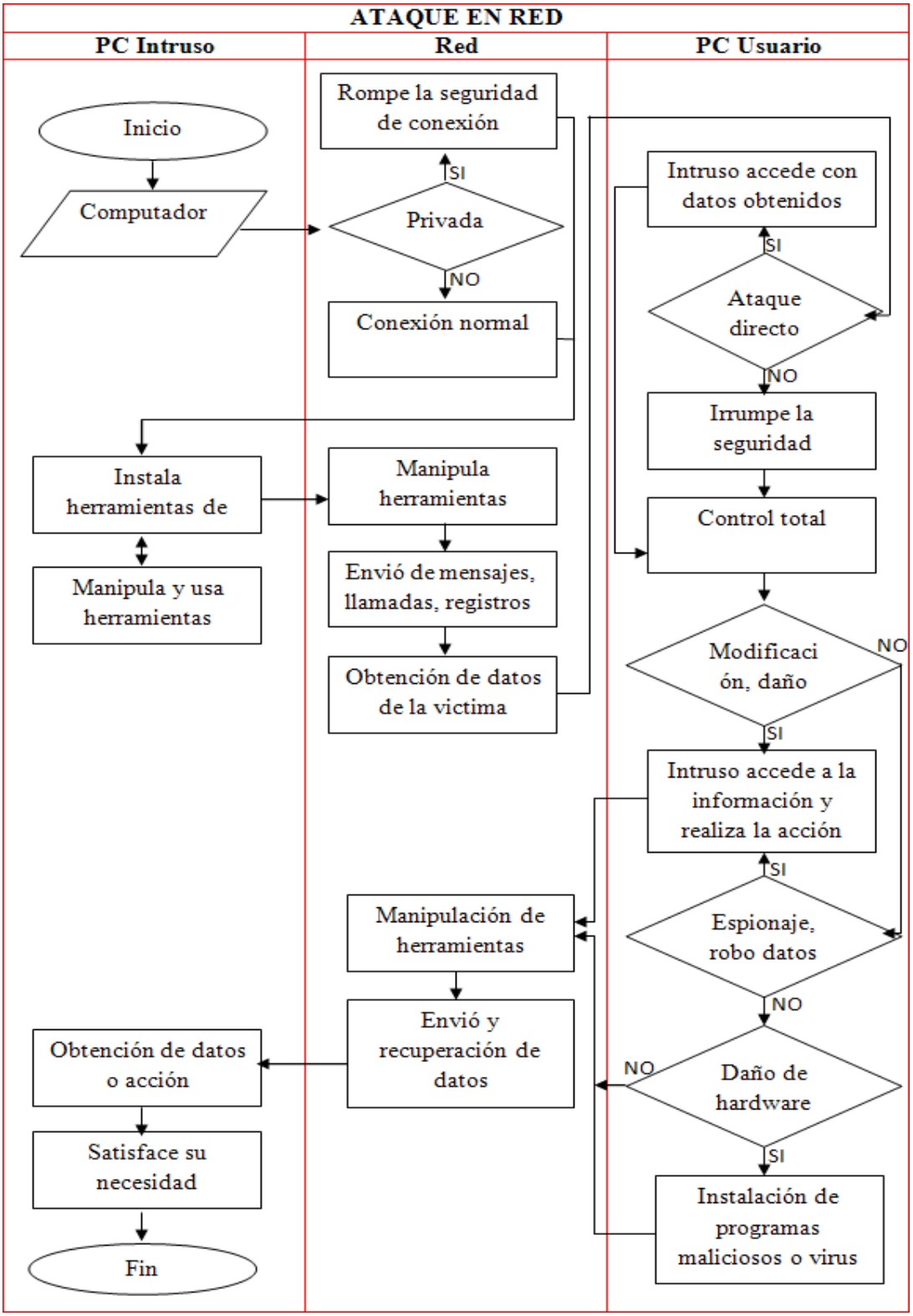


Ilustración N°: 3Diagrama de Flujo – Ataque en Red
Autor: Aníbal Guachichulca

Problemas

- ✓ Infringen o irrumpen la seguridad informática
- ✓ Uso inadecuado de la red
- ✓ Uso inadecuado o ilegal de herramientas que sirven para ataques informáticos
- ✓ Robo, daño, modificación de la información de un usuario
- ✓ Existencia de usuarios vulnerables a ataques

1.3.2. Pronostico

Al tener no tener un conocimiento sólido y no mantener una técnica que asegure la seguridad de la información ya sea con hardware o software en contra de intrusos de red, el efecto que produce, será que muchas las personas con programas o herramientas sofisticados podrán acceder a la información privada de una forma administrativa, teniendo todos los permisos de lectura, modificación y eliminación, con el fin de observar o causar daño.

- ✓ Los intrusos siguen obteniendo información y dañando equipos de cómputo de forma ilícita.
- ✓ Aceden a sitios o descargas web no confiables, siendo más vulnerables a ataques e infecciones de virus
- ✓ Facilitan la manipulación y obtención de información confidencial de un usuario a intrusos
- ✓ Existencia de grandes pérdidas tanto de software como de hardware
- ✓ Existencia de mayores posibilidades de ataques, robo y estafas informáticas.

1.3.3. Control del Pronóstico

El activo más importante que se posee en un dispositivo o computador es la información, y por lo tanto deben existir conocimiento y técnicas acerca de la seguridad informática para la protección de datos.

CAUSA	SOLUCIÓN
Infringen o irrumpen la seguridad informática	Incitar al uso de herramientas o software de seguridad informática para el escaneo de red y equipo en contra de amenazas instaladas o de enlace.
Uso inadecuado de la red	Informar al usuario a no visitar o registrarse en páginas poco confiables, a no responder a email o llamadas donde soliciten datos personales y confidenciales.
Uso inadecuado o ilegal de herramientas que sirven para ataques informáticos	Promover al uso de hardware y software de seguridad confiable y de tecnología adecuada para el usuario.
Robo, daño, modificación de la información de un usuario	Crear políticas y herramientas de seguridad para el uso de un equipo o red.
Existencia de usuarios vulnerables a ataques	Incitar a los usuarios a ser más desconfiados al momento de usar un equipo o una red para confiar sus datos.

Tabla N°: 2 Cuadro Causa – Solución
Autor: Aníbal Guachichulca

Diagrama Solución a ataques

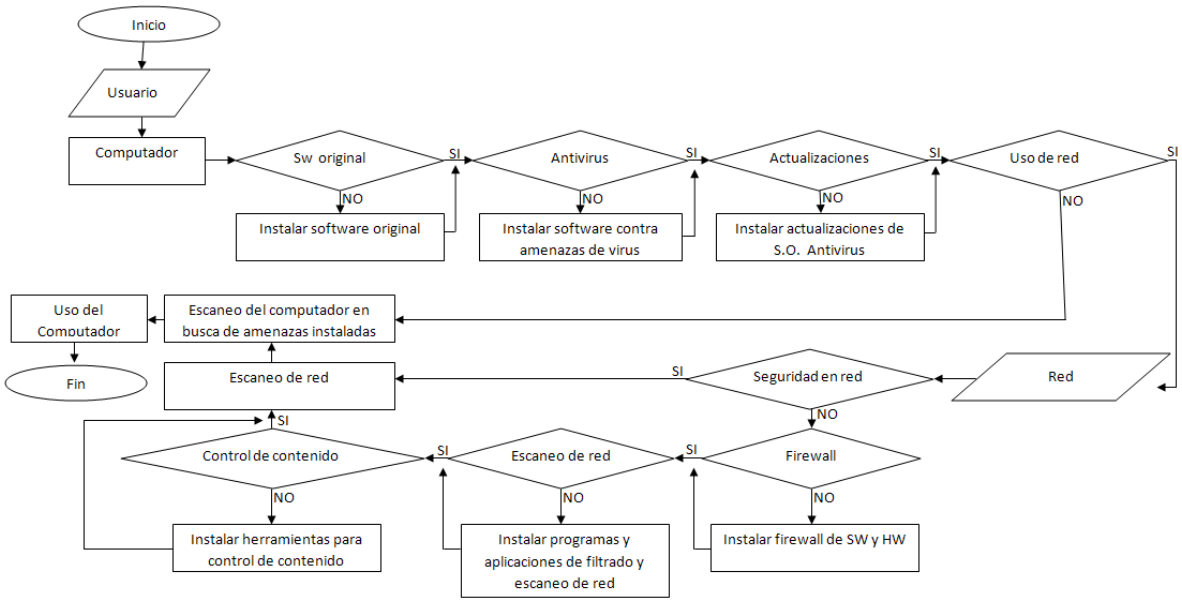


Ilustración N°: 4Diagrama de Flujo – Diagrama de solución a ataques
Autor: Aníbal Guachichulca

Cuadro de solución de los problemas

- ✓ Uso de software original
  - ➢ Sistema operativo
  - ➢ Aplicaciones y programas
  - ➢ Evitar la distribución de software ilegal.
- ✓ Uso de antivirus confiable y garantizado
  - ➢ Filtrado de paquetes
  - ➢ Herramientas anti KeyLoggers
- ✓ Mantener actualizaciones de protección contra amenazas
  - ➢ Antivirus
  - ➢ Sevice pack del sistema operativo

- firewall

- ✓ Uso de una red confiable y segura
  - Snifers de red
  - Scan de aplicaciones malignas
  - Freezado de disco duro
  - Uso de firewall de software y hardware
- ✓ Uso o navegación prudente de un equipo y red
  - No ingresar a sitios web poco confiables
  - No registrarse en páginas web sospechosas
  - No responder a email o llamadas sospechosas donde soliciten información personal
  - Borrado de cookies e historial de navegación
  - No descargar software o multimedia infectado por virus
  - Usar control de contenidos
- ✓ Uso de seguridad en contraseñas
  - Combinación de caracteres
  - Cambio periódico de contraseñas
- ✓ Configuración privada de cuentas de usuario
  - Acceso restringido a cierto tipo de usuarios
  - Acceso al uso restringido de aplicaciones
  - Acceso al uso restringido de multimedia
  - Acceso al uso restringido de recurso

1.4. Objetivos

1.4.1. Objetivo General

Realizar un Análisis acerca de las Amenazas humanas y lógicas contra la seguridad informática VS La Protección de Información

1.4.2. Objetivos Específico

- ✓ Identificar, Analizar, diagnosticar las amenazas en contra de la seguridad informática
- ✓ Elaborar un plan de seguridad para evitar intrusos informáticos en un equipo computacional
- ✓ Demostrar la forma de ataque de un intruso informático en un Ciber café para obtener información de un usuario
- ✓ Elaborar un micro currículo con la investigación proyecto que sirva de guiaparala educación media.
- ✓ Aplicar encuestas a usuarios de un Ciber café en la ciudad de Cuenca con el fin de identificar las amenazas que han experimentado
- ✓ Obtenerconclusiones respecto a las amenazas en contra de la seguridad informática mediante experiencias obtenidas en el trascurso del proyecto

1.5. Justificación

Informar sobre las amenazas humanas y lógicas que existe en contra de la seguridad informática acerca de los problemas de daños o delitos en contra de la información por

parte de personas maliciosas. Brindando información actualizada al lector beneficiándose las empresas, instituciones, y el usuario de una red de datos, de una forma viable con el presente proyecto.

1.5.1 Justificación teórica

El presente trabajo será un complemento teórico, con el desarrollo y análisis del proyecto, para incitar a uso de las seguridades informáticas, abarcando los puntos más importantes en cuanto a la protección de la información

1.5.2 Justificación metodológica

Realizando una investigación actualizada de nuevas amenazas humanas y lógicas en contra de la seguridad informática partiendo desde las más antiguas, con el uso del internet y encuesta a usuarios de red en empresas y cybers. Dando como resultado una investigación que permite explicar la validez por su aplicación de una forma concreta y útil.

1.5.3 Justificación practica

El resultado de la investigación ayudará a trasmitir conocimiento al lector acerca de las amenazas humanas y lógicas que existen en la red de datos, con la cual se podrá solucionar problemas de inseguridad en una empresa, medio u organización motivando a tener una mejor seguridad informática.

1.6. Alcance y Limitación

1.6.1. Alcance

Desarrollar un estudio ambicioso y completo sobre las amenazas humanas y lógicas en contra de la seguridad informática vs la protección de la información, para dar a conocer a los usuarios de una red que no se posee un conocimiento amplio, debido a que desconoce la magnitud del problema al que se enfrenta y concientizar a las instituciones que inviertan en capital humano y económico, para que puedan generar una buenaseguridad informática y a si prevenir problemas graves.

1.6.2. Limitación

En el presente sólo se tratará de exponer las amenazas que asechan nuestro sistema informático; para luego sí entrar en las formas de ataques propiamente dichos para así conocer sus vulnerabilidades a las que está expuesto un sistema, con que herramientas cuenta el intruso, su manipulación y finalmente conocer los recursos disponibles para proteger lainformación, especificando brevemente que no se analizara las respectivas sanciones en contra de los delitos informáticos.

1.7. Estudio de Factibilidad

1.7.1. Técnica

Para el desarrollo del proyecto se usara la siguiente tecnología:

Tecnología	Justificación de Uso
Computador	Desarrollar el presente proyecto
Internet	Consultas e investigación de temas
Impresora	Impresiones de las fuente de consultas o encuestas
Copiadora	La duplicación de las fuente de consultas o encuestas

Tabla N°: 3 Cuadro Técnico de Tecnología - Uso para desarrollo del proyecto
Autor: Aníbal Guachichulca

1.7.2. Operativa

La presente investigación trasmitirá al lector conocimiento e identificación los tipos de amenazas que existe en una red por parte de intrusos, que atacan buscando causar daño o delito en contra de la información privada del usuario y, provocara un impacto en la mejora de la seguridad.

Características de las herramientas para irrumpir la seguridad informática en un ciber café o lugar donde brinden un servicio de internet, con el fin de captura y obtener información de usuarios.

Antideepfreezer

- Permite clonar el Deepfreezer instalado en un equipo computacional
- Permite irrumpir la seguridad de forma automática
- Permite quitar el password de la aplicación
- Permite el ingreso a todas las configuraciones del Deepfreezer
- Permite Desactiva el Deepfreezer para instalar herramientas de ataque

KeyLoggers Proy Douglas 2.0

- Instalación oculta a selección del usuario
- Funcionamiento oculto en el ordenador instalado
- Método de captura de información de forma tipológica
- Generación de archivo de texto.txt
- Funcionalidad de acceso con combinación de teclas a selección
- Configuración de código de acceso
- Configuración de envió por mail el archivo generado por la captura de información

Ciber control hack

- Ejecutable directo
- Identificación automática de red
- Control de funciones de apagado, reinicio, cierre de sesión
- Control de colgamientos, bloqueos, cierre de cuenta
- Capacidad de acreditar tiempo y costo
- Capacidad de envió de mensajes por red a una o varias PC's

1.7.3. Económica

Para el desarrollo del presente proyecto se realizado un análisis de costo e inversión, presupuestado lo siguiente:

Tabla de presupuesto del proyecto			
Descripción	**Costo por unidad**	**Cantidad**	**Costo total**
Internet	1 dólar	10 horas	10 Dólares

Carpetas	40 Ctvs.	3 Carpetas	1 Dólar y 20 Ctvs.
Copias	2 Ctvs.	100 Copias	2 Dólares
Grapas	1 Dólar	1 Caja	1 Dólar
Perforadora de papel	3 Dólares	1 Perforadora	3 Dólares
Impresiones	10 Ctvs.	500 Impresiones	50 Dólares
Empastado	7 Dólares	3 Empastados	21 Dólares
Total:			**79 Dólares y 20 Centavos**

Tabla N°: 4 Cuadro de presupuesto del proyecto
Autor: Aníbal Guachichulca

2.- MARCO DE REFERENCIA.

2.1-MARCO TEÓRICO

A continuación se enunciaran las teorías a investigar para el desarrollo del presente proyecto investigativo.

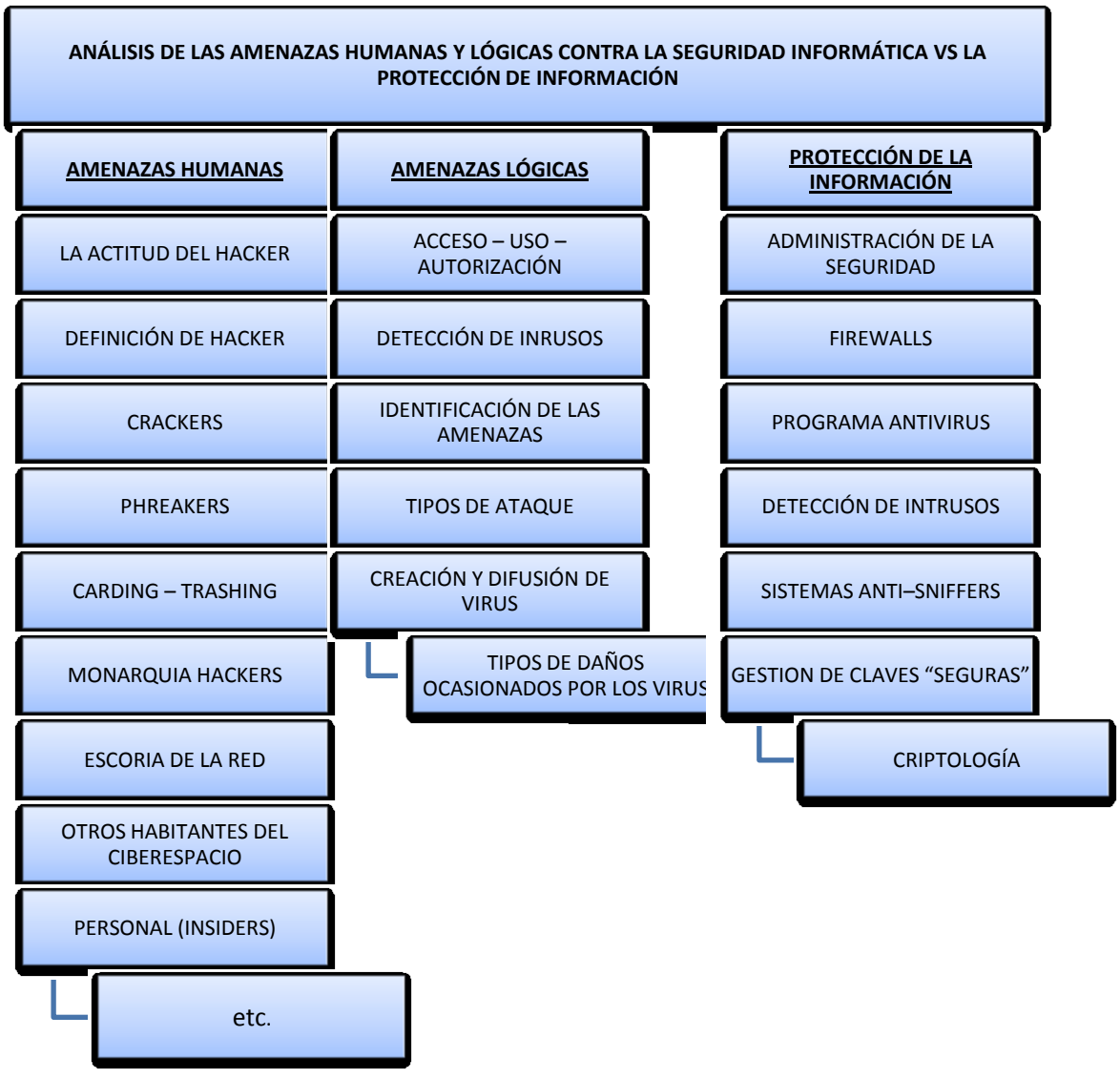


Ilustración N°: 5Mapa conceptual de las teorías aplicadas a la investigación
Autor: Aníbal Guachichulca

2.2. MARCO CONCEPTUAL

2.1-.INTRUSOS Y AMENAZAS DE LA RED

2.1.1-QUE SON LOS HACKERS

Un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas. Es posible en cualquier proyecto. No implica tampoco hacerlo con computadoras.

2.1.2.-COMO SURGIERON

El termino hackers se ha dividido en tres partes. Algunas personas los califican de delincuentes informáticos, a los que les gusta romper seguridades y destruir o modificar la información que se encuentre a su alcancé. Para otras personas el termino se considera inteligencia y habilidad, los genios de la informática.

Por ultimo esta la verdadera historia la cual hace referencia, que hace mucho tiempo cuando se usaban ordenadores de gran tamaño y teléfonos antiguos, a los técnicos de sistemas se los llamaban hackers, las mismos que utilizaban un método para arreglar estos equipos con un golpe a la maquina el cual tomo como nombre “hack” significado que traducido al español es “hachazo”.

Después un grupo de estudiantes de la universidad MIT sin malas intenciones, lograron construir una puerta trasera al servidor de su universidad y así obtener información para sus proyectos. Desde entonces comenzó la piratería informática, se crearon grupos los cuales buscaban obtener información para satisfacerse o para venderla, infringiendo la

seguridad informática con el propósito de ser calificados como los mejores en la comunidad hackers.

Para sustentar la idea de la corrupción del nombre "hackers" en la influencia de los medios, se realizó una encuesta a cierto grupo de personas.[1]

2.1.3.-ÉTICA DE UN HACKERS

En la comunidad hackers se sigue una filosofía y ética parecida a todos ellos, la mayoría de estas personas son maestros que desean inculcar su cultura a los demás interesados, como el libre acceso a la información, a los ordenadores y todo lo que pueda servir de enseñanza.

- ✓ Toda información debe ser libre, ya que la falta de libertad es un obstáculo para esta comunidad.
- ✓ Desconfían de las autoridades por promover la descentralización involucrando reglas en contra de la libre información y el intercambio de ideas.
- ✓ Los hacker deben ser juzgados por sus logros y creaciones más no por sus criterios irrelevantes como títulos, posición económica, edad, razas etc.
- ✓ Aunque la sociedad se denomine anarquista, en ciertos casos se debe respetar las regla de los demás

2.2.-MONARQUÍA DEL HACKERS

La comunidad hackers es una comunidad muy grandes que está dividida en varios grupos. Existen los "gurús" que son los maestros de los hackers, es gente mayor y con

[1] http://www.segu-info.com.ar/ataques/ataques.

gran experiencia. Después de ellos siguen los hackers los cuales son apegados a los gurús pero con la diferencia que ellos se especializan en alguna área tecnológica, en este mismo nivel se encuentran los phreakers que son especialistas en redes telefónicas. Por ultimo están los newbies que son personas que quieren llegar a ser parte de esta sociedad.

2.2.1.-GURÚS

Son gente con mayores experiencias reconocidas por sus hackeos y son los maestros de los hackers, ellos se encargan de formar a los futuros hacking aconsejándolos cuando tienen problemas en sus objetivos.

2.2.3.-PHREAKING

La palabra phreaker viene de free (gratis) y hackers.

Estos son piratas de telecomunicaciones, celulares teléfonos etc. Se dedican al robo criminal del número de tarjetas telefónicas utilizando algunos métodos llamados box (cajas). Un ejemplo de esto témenos la bluebox (caja azul) que es empleada para cambiar las frecuencias de los teléfonos con el fin de lograr diferentes objetivos.

2.2.3.-NEWBIES

Son personas que están empezando en el mundo del hacking, personas novatas que siguen un orden de aprendizaje, primero aprendiéndose toda la teoría para después aplicarla en un objetivo y así poder continuar, estas personas por lo general son muy dedicadas y empeñosas en lo que hace. Capaces de alcanzar lo que se propongan.

El inconveniente es que muy pocos de ellos llegan a convertirse en hackers, esto es porque algunos se desvían del camino y terminan siendo lammers o crackers.

2.3.-LA ESCORIA DE LA RED.

Estas son el tipo de personas que más se puede encontrar en la Ciber sociedad, sus característica y sus métodos, han hecho que sean desagradables y no sean bienvenidos en el submundo

2.3.1.-SCRIPT KIDDIES

Son personas que les gusta leer todos los artículos relacionados con el hacking y el cracking, prueban todo lo nuevo que ha salido en la red, consiguen todos los programas, pero los manipulan inocentemente sin saber específicamente para que sirven, provocando difusión de virus, daños graves en los equipos de otros usuario o de la red.

2.3.2.-BUCANEROS

La mayoría de estas personas no saben ni manipular un computador, no tienen ni idea delo que es el hacking, ellos solo se dedican a vender información o programas realizados por los hackers y crackers.

2.3.3.-LAMMERS

Estas son las personas que más se hacen notar en la red ya que se consideran que son hacker pero en realidad no tienen ni idea de lo que es un hacking, solo se dedican a bajar

e instalar virus en los computadores de sus amigos y manipular programas creados por hackers.

2.4.-HABITANTES DEL SUBMUNDO

2.4.1.-WANNABER

Son aquellas personas que desean ser hacker, pero su coeficiente no da este logro y a pesar de su positiva actitud es difícil que llegue a conseguir su objetivo.

2.4.2.-SAMURÁI

Este tipo de personas son una amenaza ya que atacan o sabotean la red a cambio de dinero, estos personajes a diferencia de los demás no tienen conciencia de la comunidad hackers.

2.4.5.-PIRATAS INFORMÁTICOS

Son aquellas personas que se dedican a desproteger información o software para copiarlo y distribuirlo comercialmente en CD´s, DVD´s, etc. Infringen el Copyright de propiedad intelectual modificando su estructura y procedimiento causando un gran perjuicio a las empresas creadoras de software.

2.4.6.-CREADOR DE VIRUS

Son personas que le gustan el desarrollo de software, que no se ven complacidos al ver que su creación o programa ha sido adquirido ampliamente por el público, crean

pequeñas aplicaciones llamadas virus el cual sabe cómo causar daño al software instalado, algunos de los mismo crean los famosos antivirus para su respectiva neutralización, he aquí se puede ver que todo es una forma de obtener ganancia en el mercado informático.

2.4.6.-PERSONAL (INSIDERS)

Son personas que trabajan con el administrador, programador, o encargado de sistemas en una organización que conociendo a la perfección cómo funciona el sistema interno de la empresa sus puntos fuertes y débiles; de manera que pueden realizar robos, sabotajes, en contra de los sistemas informáticos de forma directa más efectivo que un atacante externo.

Algunas de estas personas relacionadas con estos delitos en contra de la organización muchas veces lo realizan por diferentes motivos, que explicaremos a continuación.

2.4.6.1.-PERSONAL INTERNO

Son personas que trabajan con los sistemas de una organización, que realizan ataques informáticos causando daño a los sistemas de información. Un ejemplo de estos puede ser simplemente un electricista que provoque un corte de energía eléctrica para provocar grandes desastre en los datos, dejando sin sistema a más de un ejecutivo de la organización. Este ataque resulta ser peor que un pirata informático externo.

2.4.6.2.-EX-EMPLEADO

Son persona que trabajaban en una organización, que conocían perfectamente la estructura de los sistemas. Estas personas descontentas por lo general al ser despedidas o que no han quedado conformes con su liquidación, o simplemente ha pasado a trabajar en la competencia, tienen conocimientos necesarios como para cometer cualquier tipo de daño a los sistemas de la empresa.

2.4.7.- CURIOSOS

Son personas que les atrae las nuevas tecnología, que están en el camino del hacking o cracking considerándose newbies, personas que aún no tienen conocimientos sólidos ni la experiencia necesaria, pero que tratan de conseguir privilegios para obtener información sin causar daños al sistema.

2.4.8.-TERRORISTAS

Estas son persona que atacan directamente a un sistema informático para causar daño de cualquier tipo, alterando o modificando una base de datos, un servidor web etc. Por lo general dentro de este grupo se encuentran organizaciones políticas contrarias y empresas competidoras.

2.4.9.-INTRUSOS REMUNERADOS

A este tipo de personas se les consideran como la más peligrosa, ya que básicamente tienen gran experiencia en el hacking o cracking, realizan ataques peligrosos a una organización para dañar su imagen o para el robo de claves, información confidencial,

base de datos, diseños de nuevos productos etc. Todo esto a cambio de dinero que es pagada por parte de una tercera persona que contrata para el trabajo.

2.4.10.-CRACKERS

El cracking estudia la violación de la seguridad en los sistemas informáticos, tanto dentro del software como el hardware y fomenta la distribución de software libre.

Muchas de estas personas son confundidas como hackers, pero el cracker usa los métodos de la ingeniería inversa que consiste en eliminar, modificar o suspender uno o varios temas de seguridad que protejan a una aplicación comercial, la mayoría de veces accediendo de forma no autorizada con un fin maléfico de conseguir información y venderla.

También es gente que crea su propio programa llamado “crack”, que sirve para burlar la seguridad de alguna aplicación desarrollada. Comparte en internet todos sus logros aplicativos con el fin de ser reconocidos por la sociedad.

2.4.11.-COPY HACKERS

A este grupo se les conoce como el cuarto eslabón de la red, después de los hackers, crackers y phreakers.

Estás personas están muy ligadas al hacking del hardware que es por lo que más se interesan, específicamente en el sector de las tarjetas inteligentes que se emplea para telefonía móvil.

2.4.12.-CYPHERPUNKS

Son personas que se dedican a distribuir gratuitamente métodos y herramientas de encriptación, a través de técnicas PGP, para que los demás usuarios de la red puedan proteger su información financiera o privada del Estado.

2.4.13.-ANARQUISTAS

Son personas que les gusta la libertad de expresión y luchan distribuyendo información ilegal a través de una red o sistema informático. Dentro de estas distribuciones podemos encontrar información sobre construcción de explosivos, armamento, drogas, pornografía, piratería en general, etc.

2.4.14.-VIRUCKERS

El termino viruckers proviene de la unión de "virus y hackers".

Es una persona creadora de un programa dañino para un sistema de cómputo el cual como objetivo tiene, dañar, destruir, inutilizar los sistemas de una organización con o sin fines de lucro.

2.4.14.1.-LAS INTENCIONES PRINCIPALES DEL VIRUCKERS

1) Reproducción de código por sí mismo en otros sistemas sin ningún tipo de autorización.
2) Producir efectos secundarios convertidos en mensajes para el usuario del sistema en forma de una travesura o de daños irreparables.

2.4.15.-SNIFFERS

Son personas que rastrean, interceptan datos para tratar de recomponerlos y descifrar el mensaje que circula por una red.

El internet es la red preferida de este tipo de personas.

2.4.16.-SPAMMERS

Son personas responsables del envío de correos masivos no solicitados a usuarios del servicio, muchas de las veces con el fin de causar una sobrecarga a los buzones de entrada o simplemente para provocar un colapso en la red de los servidores.

Por lo general muchos de estos correos no solicitados contienen código dañino como virus informáticos que al abrirlos pueden causar severos daños a los equipos, otros forman parte de estafas que se realizan a los usuarios de internet.[2]

2.4.17.-DEFACER

Son personas que se dedican a la diversión o manifestación en la red, muchas de las veces son inconformes con partidos políticos. Se dedican a hackear sitios web con ayuda de sus conocimientos y herramientas aplicativas con un único propósito, que es el de retar o intimidar al administrador del sitio web.

[2]http://www.segu-info.com.ar/ataques/ataques.

2.5.-TIPOS DE ATAQUES

2.5.1.-CRASHING

El termino chrasing viene de la palabra crash (estrellar). Siendo así una técnica que consiste estrellar e irrumpir en la seguridad de los sistemas de una aplicación, una web, un servidor, un sistema remoto etc. básicamente es utilizado por los crackers para sus principales hazañas violando la seguridad de los sistemas.[3]

La mayoría de estas personas se involucran más con los Proveedores de servicio, como es el de internet (ISP), televisión por cable etc. Todo esto con el fin de conseguir el servicio de forma gratuita.[4]

A continuación veremos los tipos de seguridades que son violentadas con el crashing:

2.5.1.1.-TIEMPO DE USO LIMITADO

Por lo general existen programas que tienen un tiempo de uso limitado después de su instalación ya sea de minutos, horas, días o meses, esto se debe a que el programa usa un tipo de seguridad de tiempo limitado que fue determinado por el desarrollador, ya que al momento de instalar la aplicación se guardan consigo el registro de su creación (hora, fecha) y también algunos archivos del sistema, que limitara sus uso.

[3] http://www.segu-info.com.ar/ataques/ataques.
[4] http://es.wikipedia.org/wiki/Ataque_inform%C3%A1tico

2.5.1.2.-CANTIDAD DE EJECUCIÓN LIMITADA

El programados limita las veces que el usuario podrá ejecutar después de su instalación, antes de pedirle que ingrese el registre el código del producto.

2.5.1.3.-NÚMERO DE SERIE

Por lo general existen tres tipos de números de serie que son los fijos, variables y aleatorios.

Los fijos, son números creados que nunca se alteraran al momento de su instalación son números de registros únicos para todos los usuarios.

Los variables son números de registro únicos y diferentes para cada usuario adquiriente del producto, muchas veces estos se generan a partir de la descripción del equipo, por ejemplo en función del nombre del usuario, PC, organización, serie del disco etc.

Lo aleatorios son números que dependen de un algoritmo para obtener el número de registro del producto, este a su vez fue creado por los desarrolladores de una aplicación para acomplejar su descripción a los famosos cracker.

2.5.1.4.-MENSAJES MOLESTOS Y NAGS

Estos son mensajes que pueden aparecer al inicio de la aplicación o al final, o por una acción que el usuario cause al manipular su equipo, en estos caso el mensaje puede indicar que aún no se registra el producto, o que tenga precaución en el uso del mismo, por lo general estos mensajes desaparecen una vez que se registre adecuadamente.

2.5.1.5.-FUNCIONES DESHABILITADAS.

Por lo general a estas aplicaciones llevan el nombre de "demo", aplicación de prueba para el usuario, donde podrá manipular y comprender su funcionamiento.

El demo considera que las funciones importante tales como abrir, grabar, importar, exportar, imprimir, grabar, etc. Estén deshabilitadas hasta su respectivo registro de compra.

2.5.2.-SPAM MAILING

Es él envió indiscriminado de correo electrónico no solicitado a usuarios de un servidor de correo, ya sea con publicidad, servicio, webs, mensajes con archivos adjuntos, virus etc.[5]

2.5.3.-PIRATERÍA POR MAIL

Usan los famosos spam, realizan propagandas ilegales, estafas, envían virus con el objetivo de saturar o dañar servidor y la PC del usuario.

Dentro de esta categoría también encuentran las cadenas de coreos electrónicos que suelen mandar los amigos o conocidos.

La diferenciar un spam aun un email verdadero es difícil y todavía no existe algún método para dar la solución completa a esta problemática, algunos de los antivirus controlan el flujo de correos eliminando los spam más conocidos y la mayoría de los

[5]http://www.rompecadenas.com.ar/spam.htm

servidores de email han recopilado características de los spam para bloquearlos siendo así la técnica que elimina a muchos de estos correos.

2.5.4.-HOAXES (BROMA O ENGAÑO)

Son mensajes de coreos electrónicos engañosos, donde piden que reenvíes el mensaje recibido a todos los contactos de tu libreta en un tiempo específico, ya que si lo haces te va a pasar algo bueno tal fecha y si no lo haces tendrás mala suerte.

Estos tipos de mensajes son comunes en la red y existen de toda clase desde los que apelan por supuesto niños enfermos hasta los que podrían hacerte millonario por reenviar un mensaje.

2.5.4.1CATEGORÍAS DE LOS HOAXES

- Alertas sobre virus incurables
- Mensajes de temática religiosa
- Cadenas de solidaridad
- Cadenas de la suerte
- Leyendas urbanas
- Métodos para hacerse millonario
- Regalos de grandes compañías
- Mensajes de daños de Hotmail y Messenger:

2.5.4.2.-CARACTERÍSTICAS, OBJETIVOS, CONSECUENCIAS DE LOS HOAXES

- ✓ No tienen firma.
- ✓ Algunos invocan los nombres de grandes compañías.
- ✓ Piden al receptor que lo envíe a todos sus contactos.
- ✓ Te amenazan con grandes desgracias si no lo reenvías.
- ✓ Conseguir direcciones de mail.
- ✓ Congestionar los servidores.
- ✓ Alimentar el ego del autor.
- ✓ Hacen perder valor a cadenas creadas por gente que realmente lo necesita.

2.5.5.-OBTENCIÓN DE CONTRASEÑAS

Es uno de los temas más investigados por los Lammers, con el fin de obtener información de métodos para obtener contraseñas de correos electrónicos, redes sociales, webs privadas etc.

Los fallos de seguridad en los correos electrónicos han permitido que los crackers puedan penetrar en la misma y así obtener las contraseñas de cuentas de correo ajenas

2.5.6.-EL USO DEL KEYLOGGERS

Es una aplicación que se encarga de guardar todo lo escrito en el computador, para así poder acceder a ella y revisar qué actividad se ha realizado en el equipo.

En sus inicios el KeyLogger era usado en las universidades para monitorear las actividades que realizaban los estudiantes en los ordenadores del laboratorio.

Pero los crackers y los Lammers usan esta aplicación para encontrar las contraseñas de sus víctimas, ellos se encargan de instalar la aplicación en un computador previo a ser utilizado por un usuario del internet, al navegar en la web el usuario seguramente ingresara a una cuenta privada y digitara su contraseña, está a su vez será capturada por el KeyLoggers instalado y más tarde el crackers o lammers pasara a recoger la información.

2.5.7.-TROYANOS

Por lo general son encapsuladores de KeyLoggers, que al insertar en un computador el lammers tiene control total del equipo, para obtener contraseñas e información confidencial desde la distancia.

2.5.8.-INGENIERÍA SOCIAL

Es una técnica que no requiere conocimiento de ordenadores, simplemente es persuadir auna persona para obtener información confidencial, en muchos de los casos el lammers utiliza la aplicación Anónimos Mailer, que permite enviar a su víctima un correo electrónico con una dirección falsa, con el cual podrá obtener información confidencial de cuentas bancarias, números y claves de tarjetas de crédito etc.

2.5.9.-XPLOITS

Consiste en diseñar una copia idéntica de la página web del servidor de correo, esto es para que cuando el usuario ingrese su información confidencial, la aplicación capture los

datos de forma similar a un KeyLoggers, con el cual el lammers podrá obtener cuentas y contraseñas de sus víctimas.

2.5.10.-PREGUNTA SECRETA

Es el método que consiste en hacer una pregunta al usuario del servicio de correo cuando este haya olvidado su contraseña, en este caso si el lammers conoce a la víctima perfectamente puede adivinar su respuesta secreta y así obtener la contraseña de la cuenta.

2.5.11.-FUERZA BRUTA

Hace referencia en el intento de conseguir la contraseña ingresando varias veces al azar una clave cualquiera, para esto los lammers utilizan programas que insertaran contraseñas probándolas una por una hasta encontrar la correcta.

2.5.12.-FORMA FÁCIL

El método más fácil es enviar un mensaje al administrador del servidor de correo electrónico solicitando que le den un link donde pueden resetear su contraseña por haberla olvidado.

2.5.13.-TRASHING

Este método consiste en obtener carbones de tarjetas de crédito que son dejadas por un usuario al momento de pagar con la misma por un servicio o producto.

2.5.13.-CARDING

Es una técnica que está muy ligada con el cracking, que consiste en obtener solo información de tarjetas de crédito como números y claves etc. Con el fin de obtener dinero fácil de sus víctimas.

Muchos utilizan técnicas como el trashing, instalación de KeyLoggers, ingeniería social etc. Para conseguir esta información muchas de la persona buscan estos tipos de información como los carbones de las tarjetas en distritos industriales, las facturas en lugares comerciales, cajeros etc.

La información principal que buscan estos atacantes son:

- ✓ Nombre del usuario
- ✓ Fecha de expiración
- ✓ Número de cuenta (que tiene 12 0 18 números)
- ✓ Tipo de tarjeta (american express, visa etc.)

Al tener toda esta información los atacantes lo usan de varias formas:

- ➢ Haciendo llamadas a líneas especiales (adivinos, concursos, líneas calientes etc.)
- ➢ Utilizándola en el internet para hacer compra online.
- ➢ Transferir dinero de una cuenta a la otra.
- ➢ Difundirlos por el internet.

2.5.14.-PISHING

El “phishing” es una de las técnicas más empleadas por ciberdelincuentes para llevar a cabo estafas online.

También forma parte de estafa bancaria, basada en el envío de mensajes electrónicos fraudulentos. Básicamente es una forma de correo electrónico no solicitado, que pretende obtener información confidencial mediante la suplantación de las páginas de acceso a un servicio de banca electrónica.

Tiene la capacidad de duplicar una página web para hacer creer al visitante que se encuentra en la página original en lugar de la copiada. Normalmente esta duplicidad se utiliza con fines delictivos duplicando páginas web de bancos conocidos y enviando indiscriminadamente correos para que se acceda a esta página a actualizar los datos de acceso al banco.

2.5.15.-SNIFFERS

Los Sniffers permiten el control de la red y el de los ordenadores ligados a la misma, originalmente eran herramientas usadas para depurar problemas en la red, capturando y almacenando toda la información que viaja por la red para su respectivo análisis

Lamentablemente estas aplicaciones cayeron en las manos de los crackers o lammers que se aprovechan de esta oportunidad. Utilizando este método para el hurto de la información ya sean contraseñas o datos confidenciales.

Esta aplicación trabaja en conjunto con el modem, de manera que podrá extraer toda la información que va dirigida a ella, descartando el de las demás, un método para interceptar toda la información de la red es colocar a la tarjeta en modo promiscuo de esta manera el Sniffers tendrá un acceso total.

Los antivirus son incapaces de eliminar a estas aplicaciones, porque no son de uso ilegal tienen la autorización requerida y son distribuidas por empresas distinguidas en el desarrollo y distribución de software.

2.5.16.-IP SPOOFING

El TCP creaba una secuencia de números de serie y forjaba una secuencia de paquetes TCP. Este paquete del TCP incluía la dirección de destinación de su víctima y usando un ataque de ip spoofing se puede obtener el acceso de la raíz del sistema apuntado sin una identificación del usuario o una contraseña.

Un ataque spoofing del IP se hace en lo oculto, esto significando que el atacante asumirá la identidad de una persona confiable. De la perspectiva del anfitrión del blanco, está continuando simplemente sosteniendo una conversación normal con un anfitrión confiable. En verdad, están conversando con un atacante que está ocupado forjando los paquetes de las direcciones ip. Los datagramas del IP que contienen las direcciones forjadas del IP que alcanzarán el blanco intacto. Cada datagrama se envía sin la preocupación del usuario al otro extremo. [6]

2.5.17.-DNS POISSONING

El envenenamiento de DNS es una técnica que engaña un servidor DNS diciéndole que ha recibido la información auténtica cuando, en la realidad, no lo es. Una vez el servidor de DNS se ha "envenenado", la información generalmente se esconde durante algún tiempo, mientras extiende el efecto del ataque a todos los usuarios del servidor.

[6] http://www.segu-info.com.ar/ataques/ataques

Normalmente, una computadora conectada a Internet usa un servidor DNS proporcionado por el ISP del dueño del computador. Este servidor DNS generalmente sirve sólo a los clientes propios del ISP y contiene una cantidad pequeña de información del DNS en el caché de los usuarios anteriores del servidor (cuando se manejas IP's dinámicas). Un ataque de envenenamiento en un solo servidor DNS de un ISP puede afectar un gran número de usuarios, dependiendo de cuántos usuarios se encuentran esperando respuesta del servidor DNS comprometido.

2.5.18.-DoS

DoS son las siglas de denial of service, o en español, negación de servicio. Los ataques de negación de servicio, como su nombre lo indica, son ataques que niegan algún servicio o el acceso al ordenador. Estos ataques de DoS anualmente cuestan a las empresas sumas multimillonarias de dinero y son una amenaza para cualquier sistema o red. Principalmente un ataque de negación desorganiza o niega completamente el servicio a usuarios, redes, sistemas u otros recursos. La intención de estos ataques normalmente es dañina y casi no requiere de habilidad informática, ya que las herramientas para concluir un ataque de este tipo están al alcance de cualquiera.

Muchos dispositivos de redes tienen defectos en sus pilas de red las cuales debilitan su capacidad para resistir ataques DoS, o también los protocolos de Internet contienen defectos de los cuales se pueden tomar ventaja y así lograr un ataque óptimo.[7]

[7]http://www.segu-info.com.ar

2.5.19.-TELNET INVERSO

Cada vez que se quiere entrar a un sistema remoto, tienen la posibilidad de establecer una puerta trasera en el sistema. Con algunos códigos el cracker puede lograr entablar una conexión directa con el sistema y así poder realizar intrusiones posteriormente. Los mandatos a ejecutar son programas previamente instalados que no necesitan la transferencia de ningún archivo. En el sub mundo se le llama a esto Telnet inverso, ya que esta técnica utiliza telnet para conectarse al servidor de escucha (la puerta trasera), luego el cracker introduce los comandos desde una ventana en la corriente inversa de telnet, enviando la salida a la otra ventana

2.6.-VIRUS INFORMÁTICO

Es un programa de instrucciones creado por un programador anónimo, o desarrollador inconforme con el uso público de su software bajo licencia. El cual como objetivo tiene por dañar el funcionamiento del sistema en un ordenador o aplicación[8].

2.6.1.-CARACTERÍSTICAS DE LOS VIRUS INFORMÁTICOS.

- Capaces de auto duplicarse automáticamente al momento que el usuario realice una acción, por lo general se ocultan en unidades de reproducción automática como el disco duro, CD's, flash memory´s entre otros dispositivos.
- Modifica los programas ejecutables, adhiriéndose a ellos para ser ejecutados cuando el usuario abra su aplicación de uso personal o el sistema.
- Mensajes en la pantalla del computador.

[8]http://www.commoncraft.com/video/virus-y-amenazas-inform%C3%A1ticas

- Disminución de la velocidad en los procesos.
- Se almacena en memoria para obtener el control permanente del computador.
- Diseñado para ocultar su presencia ante el sistema y el usuario
- Su contagio se realiza a través de puerto de entrada y salida (USB, cdrom, dvdrom, tcp etc.)

Algunas personas tienen una clasificación de los virus dependiendo de la acción por la cual han sido creados. Así han sido divididos estos programas en benignos y malignos. En la subdivisión de los benignos están incluyen programas que no ejercen acciones destructivas sobre la información almacenada en la memoria y los malignos son los que ejercen acciones destructivas a la información.

2.6.2.-COMO SE CONSTRUYEN

Por lo general un virus informático posee un tamaño pequeño, tratando de contener el máximo de líneas de código en un mínimo espacio. Para su creación cualquier lenguaje de programación es adecuado para su programación, como también necesita de detalles físicos y lógicos del ordenador.

Un virus informático no se crea desde cero, su creación se basa a partir de uno existente, y las mejoras de sus técnicas son copiadas de otros.

2.7.-TIPOS DE VIRUS

2.7.1.-VIRUS DE BOOT

Esta clase de virus, se guarda en memoria para tomar el control del ordenador y escribir código maligno en los sectores de arranque y la tabla de partición para ejecutarse y tomar el control cada vez que el ordenador arranque desde un disco.

2.7.2.-VIRUS DE FICHERO

Esta clase de virus utilizan los archivos ejecutables para infectarlos y servir como medios de trasmisión para luego tomar el control de los ordenadores, por lo general estos tipos de virus se activan cuando ejecutan los ficheros ejecutables. El síntoma de este virus puede depender de su instrucción programada para el daño a causar. Se puede decir que existen dos vías de comportamiento dependiendo de si se trata de un virus residente o de acción directa.

2.7.3.-VIRUS DE FICHEROS RESIDENTES

Este tipo de virus para su infección primero comprueba si se le dan las condiciones para ejecutar su rutina de ataque. Mientras tanto este reserva una pequeña porción de la memoria para poder residir. Una característica importante de este virus residente es que necesita reservar bytes en función de su tamaño, en la mayoría de los casos está en el rango de 200 a 5000 bytes.

Cuando el virus actúa, ciertos servicios del sistema son interceptadosy el ordenador comienza a tener una serie de comportamientos extraños como:

- Caída de las letras de la pantalla
- Sonidos
- Mensajes de error sin sentido
- Desaparición de ficheros, etc.

La infección de estos virus se produce al momento de ser ejecutados o copiados.

2.7.4.-VIRUS DE FICHERO DE ACCIÓN DIRECTA

Esta clase de virus no residen en memorias ni tampoco interceptan servicios del sistema,

Estos comienzan la infección y su réplica cuando son ejecutados y por lo general toma el control de forma directa causando daños al ordenador, de igual forma la trasmisión de estos virus se produce al momento de ser ejecutados o copiados.

2.7.5.-VIRUS DE SOBREESCRITURA

Este tipo de virus posee la característica principal de dejar inservible la información y los programas que son infectados. Otra característica es que al infectar un programa, éste nunca aumentará su tamaño restringe la modificación o copia. Además encargará de sacar un mensaje de error extraño.

2.7.6.-VIRUS DE COMPAÑIA

Este tipo virus puede ser residente o de acción directa, aprovecha la característica del intérprete de comandos del DOS, por la cual si en un mismo directorio coexisten un

programa COM y otro EXE con el mismo nombre, siempre será ejecutado en primer lugar el COM.

2.7.7.-VIRUS COMPRESORES

Este tipo de virus, que pueden ser residentes o de acción directa, comprimen los ficheros que infectan en una carpeta. Siendo una consecuencia a los programas antivirus ya que les será más difícil detectarlos.

2.7.8.-VIRUS DE ENLACE DIRECTO

Los virus de este tipo, emplean una técnica muy sofisticada para infectar ficheros. Cuando un virus infecta un fichero, cambia en la entrada de directorio de ese fichero el campo o dato donde se indica cual es el número del primer clúster del fichero por el número del primer clúster del virus, almacenando en un área sin usar de la misma entrada de directorio el número original.

Este tipo de virus, no se mueve de su posición en el disco y hace que todos los programas infectados tengan como comienzo la misma copia del virus.

2.8.-VIRUS FAMOSOS

2.8.1.-PAKISTANI BRAIN (CEREBRO PAKISTANÍ)

En el año de 1986, dos hermanos, Amjad y Basit Farooq Alvi, crearon estos programas el cual se consideró como el primer virus de computador para infectar los discos

blandos. Este virus fue diseñado para promocionar su compañía de software, Brain Computer Services, en Lahore, Pakistán.

2.8.2.-GUSANO MORRIS

Fue un virus que se propaga a través de Internet, su creación fue lanzada el 2 de noviembre de 1988 por Robert Morris, un graduado de la Universidad de Cornell. Este aprovechó una falla en el sistema operativo Unix y se propagó en cuestión de días a cerca de 6.000 computadoras centrales, o entre 5% y 10% del total de Internet en ese momento. Morris, era el hijo de un experto en seguridad informática en la Agencia Nacional de Seguridad estadounidense, el cual fue condenado por violar la Ley de Abuso y Fraude Informático.

2.8.3.-DARK AVENGER

En él años 1989, un adolescente de Sofía, Bulgaria, lanzó el virus "Dark Avenger", que destruyó datos y contenía referencias a letras de la banda de rock metálico Iron Maiden. También creó el primer virus polimorfo, que evitaba ser detectado.

2.8.4.-CHERNOBYL

El 26 de abril de 1998, Ching Ing-hau, un sargento del ejército taiwanés, creó este virus, Fijado para activarse en el aniversario del desastre nuclear de Chernobyl, este trataba de borrar el disco duro de la computadora infectada.

Al final los expertos dedujeron que lo diseñó para vengarse de la industria antivirus después de que el ejército fuera infectado por un virus.

2.8.5.-MELISSA

En el año 1999, David Smith, de Nueva Jersey, creó este famoso virus, que se propagó por correo electrónico e infectó los documentos de Word de Microsoft. Smith tenía dos alias, "Vicodin" para su escritura del virus, y "Doug Winterspoon" para cuando se hacía pasar por un legítimo experto en virus. Smith no fue a la cárcel pero su castigo fue prestar servicio comunitario.

2.8.6.-ILOVEYOU

En el año 2000, El estudiante universitario filipino Onel de Guzmán lanzó este virus de E-mail. El virus engañaba a la gente para que abriera un archivo adjunto enviado por correo electrónico e instalaba una especie de detector de tecleo para poder tener acceso a contraseñas en las máquinas infectadas.

2.8.7.-ANNA KOURNIKOVA

En el año 2001, Jan De Wit, de Holanda, diseñó el virus usando el alias "On the Fly". El gusano embaucaba a los usuarios de E-mail para que hicieran clic en el archivo adjunto que supuestamente tenía una foto de la tenista rusa Kournikova. Al final Wit fue acusado de propagar datos a través de redes de computadora con la intención de causar daño.

2.8.8.-EL GUSANO BLASTER Y EL VIRUS DEL CORREO ELECTRÓNICO SOBIG

En agosto y septiembre del 2003, estos virus inhabilitaron computadoras y afectaron el tráfico de Internet en todo el planeta. Sobig se convirtió en uno de los virus más

propagados de la historia, incapacitando las redes corporativas de correo electrónico y llenando la bandeja de entrada de las computadoras de los usuarios con un exceso de mensajes antes de auto reproducirse y atacar a más víctimas potenciales.

El gusano "Blaster" o "LovSan" se propagó aprovechando una falla de seguridad de Windows.

2.8.9.-MYDOOM

También conocido como "Novarg" o "Shimgapi" se ha propagado con rapidez, principalmente en Norteamérica, representado uno de cada nueve mensajes a nivel mundial. El volumen de mensajes atascó las redes y pareció concentrase en entornos corporativos.

2.9.-CABALLOS DE TROYA O BACKDOOR

Este tipo de programa ingresa al computador en forma de engaño como una simple aplicación, un juego, un archivo multimedia. Son grandes encapsuladores de aplicaciones por lo general muchos de estos contienen virus o keyLogger que dañan y roban información usando para el mismo los 65536 puertos TCP/IP.

Los Troyanos Backdoor no son esencialmente virus, sino Herramientas de Control Remoto, y estos tienen dos componentes principales:

- El programa Servidor, que se instala en el sistema de la víctima.
- El programa Cliente que actúa en el ordenador del atacante.

2.9.1.-TROYANO/BACKDOOR CLIENTE

El Cliente se encuentra en el equipo del atacante y generalmente tiene una interfaz con opciones y desde las cuales puede ejecutar las funciones que se hayan programado para que interactúen con los sistemas de las víctimas.

2.9.2.-TROYANO/BACKDOOR SERVIDOR

El Servidor que se instala en el sistema de la víctima, es un programa que ocupa muy poco espacio y está asociado al Cliente, para poder recibir las instrucciones o través del mismo, ejecutar las funciones que el intruso desee.

2.10.-MEDIOS DE TRANSMICION

Los troyanos/Backdoor se pueden transmitir por diversos medios de la red ya que la seguridad de la Internet no tiene los medios para controlar estos ataques y seguir funcionando, los métodos de trasmisión más comunes de un Backdoor son los siguientes:

2.10.1.-MENSAJES DE CORREO

Son la forma más fácil de propagación por medio de un archivo anexado al mensaje y si el receptor comete el error de ejecutarlo, instalará el Servidor, permitiendo que el intruso pueda controlar el o los equipos infectados.

2.10.2.-TELNET y SSH

Funcionan en modo Cliente/Servidor y permite ejecutar comandos en el equipo infectado. Telnet es un programa de emulación de terminal para las redes TCP/IP. Opera en una computadora y la conecta con un servidor de la red. A partir de ese instante, un usuario puede ingresar comandos a través del programa Telnet y cada instrucción será ejecutada como si la hubiera ingresado directamente en la consola del servidor o el equipo asignado[9].

2.10.3.-REDES COMPARTIDAS

Las redes compartidas, más precisamente las redes p2p, son un riesgo en potencia para la difusión de virus, estas redes permiten todo tipo de archivos, por lo tanto es muy posible encontrar virus. Redes como Kazaa, E-mule, E-donkey, Ares, son redes que tienen un riesgo potencial, por lo general poseen servicios de descarga multimedia.[10]

2.10.4.-SERVICIOS HTTP, FTP, ICQ, CHAT, MENSAJERÍA INSTANTÁNEA

Es posible visitar una página Web en Internet, la misma que descargue automáticamente un troyano Backdoor Servidor y el sistema quedará infectado, bajo control del troyano Cliente. Del mismo modo podrá ocurrir en servidores FTP. Por lo general estos servidores, al ser reportados, serán deshabilitados por su ISP, en caso contrario el Proveedor de Servicios de Internet será merecedor a una sanción.

---

[9] http://www.segu-info.com.ar/ataques/ataques.htm
[10] http://www.mundointernet.es/IMG/pdf/ponencia95.pdf

La popularidad del uso del Chat en las redes sociales (Facebook twiter, badoo etc.) o de los servicios de Mensajería Instantánea (MSN Messenger, Yahoo Messenger, Netscape o AOL Messenger), entre otros, han hecho posible la transmisión de virus, macro virus, gusanos, troyanos y Backdoors, entre los usuarios conectados en una misma sesión.

2.11.-TROYANOS FAMOSOS

2.11.1.-BACK ORIFICE

Este troyano mejor conocido como BO, es uno de los troyanos más populares distribuidos en la red, y uno de los más usados por los antiguos lammers y script kiddies.

BO fue creada como una herramienta de administración remota para sistemas operativos Windows 9x. Esta herramienta fue presentada en el año1998 a la convención de hackers

2.11.2.-BLACK HAT

Esta es una herramienta permite el re inicio de un sistema remoto, tiene la capacidad de añadir y borrar claves del registro, enviar y recibir archivos, ver contraseñas ocultas y crear cuentas de archivos.

2.11.3.-NET BUS

Este es un tipo de virus troyano que fue creado por Carl-Frederic Neikter en el año de 1998. Esta herramienta posee métodos muy parecidos al BO, pero contiene un interfaz gráfico más sofisticado, al igual que sus herramientas.

2.11.3.1.-DIFERENCIA ENTRE NET BUS Y EL BO

- ✓ El Net Bus utiliza TCP para conectarse al sistema remoto.
- ✓ El BO utiliza UDP para conectarse al sistema remoto.

2.11.4.-SUBSEVEN

Esta famosa versión se desarrolló en 1997, fue programado en Borland Delphi. Su acción fue compromete la seguridad del sistema infectado, al habilitar una puerta trasera por la que un atacante puede tomar el control de la computadora de su víctima.

Esta versión utiliza el puerto TCP/11142. Cuando se ejecuta, generalmente engaña al usuario disfrazándose de en alguna supuesta herramienta, copiándose en el directorio de Windows.

2.12.-OCULTISMO DE VIRUS

El Antivirus, para muchos hackers llamado el segundo enemigo natural, después del firewall, es la amenaza de la vida del virus dándose cuenta de la presencia del virus y avisando al usuario al mismo tiempo que es borrado del ordenador. Por esto lo crackers inventaron cinco distintas técnicas populares para poder engañar a los antivirus y así poder continuar con sus maléficos planes.

2.12.1.-TUNNELING

El tunneling es un método de infiltración que sirve para infiltrar e infectar con los virus a los ordenadores sin ser detectados por el antivirus u otro tipo de seguridad.

El tunneling apunta a proteger al virus de los módulos residentes de los antivirus, que monitora todo lo que sucede en la máquina para interceptar todas las actividades "típicas" de los virus.[11]

2.12.2.-AUTO ENCRYPTACIÓN

Esta técnica muy utilizada, consigue que el virus se encripte de manera diferente cada vez que se infecta el fichero, para intentar pasar desapercibido ante los antivirus.

2.12.3.-MECANISMOS POLIFORMICOS

Es una técnica que se utiliza para evitar ser detectados, es la de variar el método de encriptación de copia en copia. Esto obliga a los antivirus a usar técnicas heurísticas ya que como el virus cambia en cada infección es imposible localizarlo buscándolo por cadenas de código. Esto se consigue utilizando un algoritmo de encriptación que pone las cosas muy difíciles a los antivirus. No obstante no se puede codificar todo el código del virus, siempre debe quedar una parte sin mutar que toma el control y esa es la parte más vulnerable al antivirus.

2.12.4.-ARMOURING

Mediante esta técnica el virus impide que se examinen los archivos que él mismo ha infectado y haciendo imposible la lectura de su código.[12]

[11] http://deco-hack.iespana.es/deco-hack/manuales/Tunneling.txt
[12] http://www.zonavirus.com/Tecnicas/Armouring.asp

2.12.4.1.-CARACTERISTICAS DE LA TÉCNICA ARMOURING

- El virus no puede ser abiertos para su estudio
- No se puede descubrir las líneas de código

2.13.-ANTIVIRUS (METODOS DEFENSA)

Los antivirus hoy en día son las herramientas más confiables de gran aceptación por los usuarios para la detección y eliminación de virus ya que en la actualidad estos antivirus incorporan diversas funcionalidades.

Por lo general los antivirus poseen un registro de virus que son llamadas base de datos que es donde tienen los nombres de todos los virus que salen todos los días, por esto es aconsejable mantener una actualización nuestra base de datos para el antivirus pueda detecte los nuevos virus o amenazas, ya que un antivirus que tenga sus registros desactualizado se le considera ejecutor de los virus.

2.13.1.-FUNCIONALIDADES DE UN ANTIVIRUS

- Trabajan en segundo plano.
- Escanean y eliminan diferentes tipos o clases de virus.
- Permiten escanear archivos adjuntos en e-mails para rastrear virus de macro,
- Evitan amenazas como los spams y algunos tipos de DoS que son instalados en los ordenadores en forma de fichero.

2.13.2.-LA HEURÍSTICA Y SU FUNCIONAMIENTO

El funcionamiento de la heurística es sencillo, primero se analiza cada programa sospechoso sin ejecutar las instrucciones, lo que hace es desensamblar o descompilar el código de máquina para deducir que haría el programa si se ejecutara. Avisando que el programa tiene instrucciones para hacer algo que es raro en un programa normal, pero que es común en un virus.

Entendiendo la Heurística como un indicador de probabilidad de contagio, esto nos lleva a considerarla como un sistema de detección mejorada que al incluirla en los antivirus nos permite establecer un sistema de alerta y de prevención ante la aparición de mutaciones de virus o de nuevos virus.

Esta técnica permite barrer diferentes tipos de códigos dentro de los archivos, que sean susceptibles de ser malignos. Códigos que son genéricos dentro de los archivos maliciosos y que siempre suelen ser parecidos. O por lo menos respetar parte de las cadenas de comandos que activan los virus.

2.13.3.-CÓMO FUNCIONA LA HEURÍSTICA EN UN ANTIVIRUS

Los virus tienen patrones de códigos que son como sus huellas digitales. Los software antivirus buscan estos patrones, pero sólo de los que tienen almacenados en su lista (por esto la actualización es tan importante). Estos productos también pueden valerse de la heurística, es decir, analizan los archivos para detectar comportamientos similares a los de los virus.

Cada día crece el número de nuevos virus y la alternativa para poder neutralizarlos, sin haber programado antes el antivirus para su reconocimiento, es la denominada búsqueda

heurística. A través de ella, el programa antivirus analiza el código de los programas buscando instrucciones, acciones sospechosas o indicios que delaten la presencia de virus en la computadora, de acuerdo a los patrones habituales empleados por los códigos maliciosos.

El método Heurístico es una tecnología de programación que dentro de sus rutinas de detección de especies virales, incluye las cadenas clásicas que son similares, parecidas o afines a virus auténticos. El método heurístico, si no está bien programado, es susceptible de incurrir en resultados falsos positivos o negativos. Además, al encontrar un virus desconocido, variante de otro existente, el antivirus que emplea este método de búsqueda no podrá eliminar eficientemente el virus y mucho menos reparar el archivo o área afectada.

Para que un antivirus detecte y elimine eficientemente a un virus así como también repare los daños ocasionados, debe incluir en la base de datos de sus rutinas de detección y eliminación el exacto micro código viral de esa especie. Sin embargo la técnica de búsqueda heurística de virus por categorías es una forma eficiente de detectar a especies virales que pertenecen a una misma familia, aunque no es un método absolutamente exacto o eficiente.

2.13.4.-SINTOMAS

Los principales síntomas de infección de virus son:

- La reducción del espacio libre en la memoria o disco duro. Un virus, cuando entra en un ordenador, debe situarse obligatoriamente en la memoria RAM, y por ello ocupa una porción de ella. Por tanto, el tamaño útil operativo de la memoria se reduce el mismo tamaño que tiene el código del virus.

- La aparición de mensajes de error no comunes. Pero en algunos sistemas Operativos más antiguos, los mensajes de error eran muy comunes, por eso algunos virus aprovechaban esto para ejercer una operación no admitida q finalizara en mensaje de error.
- Los fallos en la ejecución de programas. Al abrir alguna aplicación es muy probable que esta esté dañada o modificada por el virus.
- Las Frecuentes caídas del sistema. El sistema puede presentar fallos que pueden generar caídas del sistema, algunos virus son los culpables de producir estos fallos.
- Los tiempos de carga son mayores. Ya que para que el virus funciones, este necesita pasar primero por un proceso de carga que aumentara el tiempo de iniciación de algunas aplicaciones.
- Las operaciones rutinarias se realizan con más lentitud.
- La aparición de programas residentes en memoria desconocidos. Estos programas pueden ser el mismo virus que se está ejecutando en un primer plano.
- Actividad y comportamientos inusuales de la pantalla. Muchos de los virus eligen el sistema de vídeo para notificar al usuario su presencia en el ordenador. Cualquier desajuste de la pantalla, o de los caracteres de esta nos puede notificar la presencia de un virus.
- El disco duro aparece con sectores en mal estado. Algunos virus usan sectores del disco para camuflarse, lo que hace que aparezcan como dañados o inoperativos.
- Los cambios en las características de los ficheros ejecutables. Casi todos los virus de fichero, aumentan el tamaño de un fichero ejecutable cuando lo infectan.

- Aparición de anomalías en el teclado, existen algunos virus que definen ciertas teclas que al ser pulsadas, realizan acciones perniciosas en el ordenador.
- El cambio de la configuración de las teclas, por la del país donde se programó el virus.

2.13.5.-LABORATORIOS DE ANTIVIRUS

El principal trabajo de un laboratorio de antivirus informático es:

1. Detectar el virus.
2. Abrirlo y analizarlo.
3. Ejecutarlo y ver qué daño es capaz de hacer.
4. Finalmente crear la vacuna.

2.13.6.-DETECCIÓN DE VIRUS

El proceso que va desde detectar el virus hasta lograr una vacuna dura una media de 3 ó 4 horas. En ese tiempo el personal del laboratorio de investigación de virus trabaja a toda velocidad y realiza múltiples tareas.

Los medios internacionales de contacto, los clientes y las utilidades de análisis son indispensables para que una compañía antivirus consiga la información sobre una nueva plaga.

Los usuarios que tienen sospechas de tener un virus, se conectan a la web y esta herramienta analiza sus equipos. Además, como este software les pide el lugar desde dónde se están enganchando, aquí se obtiene una información muy importante: saber el

contenido vírico de cada país. A parte, Active Scan les permite recibir virus procedentes de todos los países.

Otro de los medios de recepción son los clientes, que cada vez que encuentran un código vírico sospechoso dentro de un equipo, lo envían, por medio de los propios antivirus, al departamento de análisis.

Los virus más complejos de desensamblar son los polimórficos, que en cada infección que realizan se cifran de una forma distinta. De esta forma, generan una elevada cantidad de copias de sí mismos.

Un laboratorio antivirus puede recibir de 12 a 14 virus nuevos todos los días.

Un laboratorio, ante un virus muy peligroso, puede llegar a probarlo en 60 máquinas. Y tener trabajando en él a cien personas.

2.13.7.-ABRIR Y EJECUTAR EL VIRUS

Los técnicos que trabajan en un laboratorio de antivirus informático, una vez han recibido el virus, lo que hacen es desensamblarlo, abrir la parte interna de su código. Para esto utilizan unas herramientas especiales que realizan esa tarea.

Después el investigador se convierte en un usuario y ejecuta el código vírico de la misma forma que lo haría éste.

Los investigadores van analizando el virus para ver dónde se deposita, qué es lo que hace, que modificaciones tiene en definitiva.

Los profesionales observan las acciones malignas del código vírico y después las escriben, describiendo cuáles son y cómo están hechas. Es en este momento, cuando entra en acción el departamento de desarrollo. El cual se encarga de conseguir una

vacuna que acote esas acciones malignas, y que ese virus se pueda reconocer de forma inequívoca con respecto a todos los códigos que poseen los ordenadores normalmente.

2.14.-FIREWALLS

El cortafuego es el encargado de la seguridad de la información entre la red externa e interna, ya que toda la información atraviesa estos dos tipos de redes y está a su vez pasa a través del cortafuego o firewall. Implementando su filtrado, supervisión y registro de sesiones entre una red y otra.

Como también es un mecanismo de protección en contra de los ataques del sistema de información del exterior, pero también puede proteger sistemas externos contra los ataques que se originan dentro de su red[13].

Pero como no hay técnica o método efectivo que proteja contra todos los ataques de afuera, ni contra los ataques que vienen desde adentro de su propia red, ni de otros métodos de la piratería o de otras formas de hostilidad.

El cortafuego provee dos categorías principales:

2.14.1.-PAQUETE TIPO CORTAFUEGOS

Un paquete tipo cortafuego filtra simplemente la información que transita entre las dos redes con las cuales está conectada. Para hacer esto, el cortafuego utiliza los protocolos empleados en las dos redes (TCP/IP, IPX/SPX, Appletalk, etc): tiene que saber la estructura de estos protocolos de modo que pueda filtrar datos dentro de ellos. Hoy, en día estos sistemas de filtración se construyen cada vez más a menudo en los routers. Y

[13]http://www.segu-info.com.ar/ataques/ataques.htm (investigado 25/09/2012)

esto es una localización natural para el filtrado, porque un Router es un punto de la interconexión entre dos redes. Pero esta categoría del cortafuego no sabe la estructura de los intercambios de los datos entre diversos servicios ftp, correo, el Web, etc. Este tipo de cortafuego sabe solamente protocolos de red.

2.14.1.1.-VENTAJAS

- ✓ Este tipo de cortafuego es transparente: las aplicaciones no tienen que ser vueltos a trabajar para aprovecharse de ellos (son plug and play).
- ✓ En muchos casos, el grado de seguridad proporcionado es perfectamente el adecuado.
- ✓ Son baratos.
- ✓ Usted puede filtrar cualquier servicio construido alrededor de los protocolos de red apoyados por el cortafuego.

2.14.1.2.-DESVENTAJAS

- ✓ Usted tiene que ser a fondo familiar con la red que se protegerá, y con los protocolos usados en esta red.
- ✓ No hay autentificación del usuario; la filtración se basa en la dirección de red del sistema del hardware.
- ✓ La filtración del paquete no encubre la arquitectura interna de la red.
- ✓ Con DHCP, las direcciones del IP no son fijas: el sistema del hardware puede tener un diverso IP address cada vez que se comienza el sistema.

- ✓ Una computadora comprometida en la red de área local puede penetrar el cortafuego (porque se cree un ordenador seguro).
- ✓ El cortafuego no da la protección contra debilidades inherentes en servicios sin filtro.
- ✓ Usted no puede registrar los registros de sesiones individuales: el cortafuego no comprende los datos intercambiados por servicios (tales como los datos de una sesión del telnet).

2.14.2.-APLICATION BASED FIREWALLS

Un aplication based firewall es un sistema del hardware en el cual el servidor para cada servicio (ftp, Web, etc). Se ha reconstruido Los clientes no se conectan directamente con la red exterior, en vez de eso, ellos pasan a través del cortafuego. El cortafuego después establece una conexión con la red exterior para el cliente, envía peticiones, recibe respuestas, las analiza y después las retransmite al cliente dentro de la red interna. Este cortafuego da buena seguridad, porque la supervisión ocurre en el nivel de la aplicación haciéndolo más flexible y de gran alcance. Si una conexión entre la red interna y la red exterior es atacada, sólo la conexión entre el atacante y el cortafuego será atacada. Así, solamente el cortafuego puede ser comprometido y si el cortafuego resulta ser superado por el ataque, este se notara muy rápidamente[14].

2.14.2.1.-VENTAJAS

- ➢ Las reglas de la seguridad son fáciles de definir.

[14]http://www.segu-info.com.ar/ataques/ataques.htm (investigado 25/09/2012)

- Se pone en ejecución la autentificación del usuario.
- La arquitectura interna de la red puede ser encubierta, porque todas las conexiones a la red exterior pasan a través del cortafuego.
- Hay conversión de dirección entre la red interna y la red exterior.
- Usted consigue numerosos "log files" y muy detallados.

2.14.2.2.-DESVENTAJAS

- Tales sistemas son costosos: requieren el hardware y el software.
- Son demasiado poderosos para las redes pequeñas.
- Usted necesita software especial del cliente para aprovechar el cortafuego.
- No hay ayuda para los nuevos servicios.
- La administración del sistema es más exigente que con el paquete-tipo cortafuegos.

2.14.3.-FILTRADO DE PAQUETES

La filtración del paquete permite definir las reglas de filtración basadas en listas del acceso. Estas reglas de filtración pueden diferenciar para el interfaz de la entrada y el interfaz de la salida del cortafuego. Pues así, el administrador de la red puede especificar diversas reglas y listas del acceso para las conexiones de la red interna a la red exterior, y viceversa. De esta manera, se puede restringir el acceso a la red interna sin la limitación del acceso a la red exterior.

Cuando los datos que vienen a partir de una red a otra desobedecen las reglas de filtración fijadas por el administrador de la red, en este caso se pueden tomar varias decisiones.

- ✓ Destruir el paquete.
- ✓ Enviar un mensaje de error al remitente.
- ✓ Alertar al administrador de la red.

2.15.-ANONIMIZADORES

El servicio de anonimato actúa como un filtro de seguridad entre tu navegador y el sitio Web que deseas visitar. Te conectas al anonimizador, introduces el URL al que deseas ir, entonces éste se adentra en la Red en busca de la página que deseas ver y te la muestra. Si posteriormente vas siguiendo enlaces de una página a otra, se presentarán asimismo a través del anonimizador.

2.15.1.-INCONVENIENTES DEL ANONIMIZADORES

- • No funcionan con todos los sitios ni con los servidores seguros.
- • Tampoco se reciben cookies (lo cual para algunos representa más bien un alivio).
- • Desactivan todos los programas en Java, JavaScript, etc. (de nuevo, ventaja o inconveniente según para quién).
- • Ralentizan la navegación.
- • Para un servicio óptimo hay que pagar.
- • Añaden a las páginas que visitamos banners con publicidad de sus patrocinadores.

2.16.-PROXIES

Los proxies primero fueron inventados para acelerar conexiones del Internet. El proxie primero chequea primero si uno de usuarios ha tenido acceso a esta página web últimamente. Si es así debe tener una copia de él en alguna parte en los servidores de este. Entonces el proxy server comienza la conexión solamente al chequeo, si su versión no es anticuada, que requiere solamente mirar el tamaño del archivo. Si tiene la última versión, le enviará el archivo, en vez de tener hacer que el servidor lejano se lo envíe, y así acelera la conexión. Si no, descargará los archivos solicitados por sí mismo y después se los enviará. Pero los proxies se pueden también utilizar como anonimizadores mientras que navega por Internet, porque manejan todas las peticiones del HTTP. La mayoría de las ocasiones son que su ISP tiene un proxie.

2.17.-CRYPTOGRAFIA

La cryptografia es otra etapa de gran importancia usada por los hackers. Esto consiste en cifrar un mensaje o un archivo en base a diferentes algoritmo para hacerlo ilegible para otras personas, es el método usado para esconder mensajes, o hasta señales de televisión.[15]

2.17.1.-CRIPTOGRAFÍA DE CLAVE SECRETA

En los cifrados de clave secreta, la seguridad depende de un secreto compartido exclusivamente por emisor y receptor.

[15]http://www.segu-info.com.ar

La principal amenaza criptoanalítica proviene de la alta redundancia de la fuente. Shannon sugirió por ello dos métodos básicos para frustrar un criptoanálisis estadístico: la difusión y la confusión.

2.17.2.-MÉTODOS BÁSICOS PARA FRUSTRAR UN CRIPTOANÁLISIS ESTADÍSTICO (DIFUSIÓN-CONFUSIÓN)

- La difusión consiste en anular la influencia de la redundancia de la fuente sobre el texto cifrado. Hay dos formas de conseguirlo.
  - ✓ La primera, conocida como transposición, evita los criptoanálisis basados en las frecuencias de las n palabras.
  - ✓ La segunda manera consiste en hacer que cada letra del texto cifrado dependa de un gran número de letras del texto original.
- La confusión consiste en hacer que la relación entre la clave y el texto cifrado sea lo más compleja posible, haciendo así que las estadísticas del texto cifrado no estén muy influidas por las del texto original. Eso se consigue normalmente con la técnica de la sustitución.

2.17.3.-CIFRADO EN BLOQUE, DES

El cifrado en bloque opera sobre textos formados por n palabras, convirtiendo cada una de ellas en una nueva n palabra.

Sin duda el cifrado en bloque más conocido es el llamado DES (Data Encryption Standard). Este sistema se puede catalogar como un cifrado en bloque que es a la vez un cifrado producto de transposiciones y sustituciones.

2.17.4.-CRIPTOGRAFÍA DE CLAVE PÚBLICA

En estos esquemas se utiliza una clave de cifrado (clave pública) k que determina la función trampa Tk, y una clave de descifrado (clave secreta o privada) que permite el cálculo de la inversa Tk'.

Cualquier usuario puede cifrar usando la clave pública, pero sólo aquellos que conozcan la clave secreta pueden descifrar correctamente.

2.17.5.-SISTEMAS RSA

Fue desarrollado en el año de 1977 por Ronald Rivest, Adi Shamir y Leonard Adleman, de ahí el nombre de RSA, que corresponde a las iniciales de los apellidos de sus autores.

Los sistemas de seguridad del RSA se basan en el hecho de que no existe una forma eficiente de factorizar números que sean productos de dos grandes primos.

2.18.-CD-ROM

Estos son más usados por los juegos ya que existen aplicaciones que al ser instaladas en el disco duro necesitan del cd para poder ejecutarlo, esto lo realiza por seguridad o por los siguientes motivos:

- Comprobar la presencia.
- Necesitan archivos.
- Comprobar la etiqueta.
- Comprobar el espacio libre.
- Comprobar archivos eliminados.

2.18.1.-PROTECCIÓN CONTRA COPIA

Existen algunos métodos de protección para los cd´s, para que no puedan ser crackeados. Los métodos más comunes son los siguientes:

2.18.2.-DETERIORO DEL CD

Deteriorar físicamente el CD para que no pueda ser copiado con claridad, la copia de estos sería muy difícil ya que los mejores quemadores no son capaces de quemarlo con precisión, igual esto también implica un riesgo para los autores del programa ya que es muy posible que los CD's originales presenten varias fallas.

2.18.3.-ARCHIVOS CON TAMAÑOS FALSOS

Es la técnica que simula los archivos parezcan muy grandes, para que al momento de ser copiados generen errores por el tamaño tan grande del archivo falso.

2.18.4.-VARIOS BLOQUES DE COPIADO

El formato ISO para la copia de CD's establece que estos solo deben ser creados en un mismo bloque, por lo tanto cuando se intenta copiar un CD con varios bloques, el programa de quemado generará errores.

2.18.5.-ERRORES FICTICIOS

Es posible que el software al ser quemado le diga al quemador que este tiene varios errores "ficticios" como un error de redundancia cíclica, y esto obligara al programa de quemado a terminar su ejecución.

2.18.6.-ARCHIVOS LLAVE

Es algo parecido al anterior pero funcionan de muchas formas diferentes dependiendo de las habilidades del programador.

2.18.7.-ANTI-HERRAMIENTAS CRACKING

Estas son muy efectivas si se utilizan técnicas novedosas o desconocidas para los crackers. Se pueden aplicar anti-depurador, anti-desensamblador, anti-monitores de registros o archivos, API, etc. También anti-modificación del ejecutable que sería algo como anti-editores hexadecimales.

2.19.-FIRMAS Y PRIVASIDAD

Una firma digital es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la originalidad del mensaje.

La firma digital no implica que el mensaje está cifrado, esto es, un mensaje firmado será legible en función de que está o no cifrado.

Así cualquier receptor del mensaje podrá comprobar que el mensaje no fue modificado desde su creación porque podrá generar el mismo resumen o misma huella digital aplicando la misma función al mensaje. Además podrá comprobar su autoría, descifrando la firma digital con la clave pública del firmante, lo que dará como resultado de nuevo el resumen o huella digital del mensaje.

2.19.1.-LAS HUELLAS DIGITAL DEL MENSAJE

- ✓ Las huellas digitales son un conjunto de datos asociados a un mensaje que permiten asegurar que el mensaje no fue modificado.
- ✓ La huella digital o resumen de un mensaje se obtiene aplicando una función, denominada hash, a ese mensaje, esto da como resultado un conjunto de datos singular de longitud fija.

2.19.2.-LAS PROPIEDADES FUNCIÓN HASH

- ✓ Dos mensajes iguales producen huellas digitales iguales.
- ✓ Dos mensajes parecidos producen huellas digitales completamente diferentes.
- ✓ Dos huellas digitales idénticas pueden ser el resultado de dos mensajes iguales o de dos mensajes completamente diferentes.
- ✓ Una función hash es irreversible, no se puede deshacer, por tanto su comprobación se realizará aplicando de nuevo la misma función hash al mensaje.

2.19.3.-FUNCIONES DE LAS FIRMAS DIGITALES

- ➢ Autentificar la identidad del usuario, de forma electrónica, ante terceros.
- ➢ Firmar digitalmente de forma que se garantice la integridad de los datos trasmitidos y su procedencia.
- ➢ Cifrar datos para que sólo el destinatario del documento pueda acceder a su contenido.

2.19.4.-GARANTÍA DEL USO DE UN CERTIFICADO

- La identidad del emisor y del receptor de la información (autentificación de las partes)
- Que el mensaje no ha sido manipulado durante el envío (integridad de la transacción)
- Que sólo emisor y receptor vean la información (confidencialidad)
- Que el titular de un mensaje no pueda negar que efectivamente lo firmó (no-repudio)

2.20.-NUEVAS AMENAZAS EN LA RED

Nuevas amenazas para tablets y Smartphone (sobre todo con sistema operativo Android), ataques a medida contra objetivos específicos, phishing y troyanos bancarios constituyen las principales amenaza de seguridad desde el 2012. Sin olvidar, por supuesto, el papel que jugarán las redes sociales como difusoras de malware y un más que posible saldrá a televisores y consolas con conexión a internet.[16]

2.20.1.-MALWARE

Malware es el acrónimo, en inglés, de las palabras "malicious" y "software", es decir software malicioso. Dentro de este grupo se encuentran los virus clásicos (los que ya se conocen desde hace años) y otras nuevas amenazas, que surgieron y evolucionaron, desde el nacimiento de las amenazas informáticas. Como malware, se encuentran

[16]http://www.informador.com.mx/tecnologia/2012/426282/6/aumentan-amenazas-informaticas-en-dispositivos-moviles.htm

diferentes tipos de amenazas, cada una con características particulares. Incluso existe malware que combina diferentes características de cada amenaza. Se puede considerar como malware todo programa con algún fin dañino.[17]

2.20.2.-EL POLIMORFISMO

Se trata de un malware que es capaz de mutar automáticamente, por lo que es extremadamente difícil de identificar y por lo tanto de destruir y sólo cuestión de tiempo antes de que aparezca en los dispositivos Android.[18]

2.20.3.-LOS DIALERS

Son pequeños programas que se encargan de marcar números telefónicos que dan acceso a algún tipo de servicio. En un principio, este tipo de aplicaciones eran distribuidas por proveedores de acceso a Internet para facilitar a sus clientes el proceso de conexión con el servidor pero ahora los usuarios con pocos escrúpulos usan losdialers para ganar fuente de ingresos, y de esta manera, comienzan a proliferar en Internet páginas preparadas para descargar, instalar y ejecutardialers de conexión a números de tarifas especiales de forma automática y oculta para el usuario.

La desventaja de los dialers es que solamente pueden causar problemas en equipos que se conecten a Internet a través de RTB (red telefónica básica), ya que la banda ancha o la conexión por cable funcionan de forma muy distinta, y no precisan marcar ningún número telefónico.

[17] http://www.kaspersky.com/sp/threats
[18] http://www.zonavirus.com/Tecnicas/Mecanismos_Polimorficos.asp

2.20.4.-SPAM LEGAL

La tendencia de los anunciantes a adquirir listas de correo electrónico de usuarios que han aceptado recibir publicidad y la compra de bases de datos de clientes a empresas en proceso de cierre. Tiene otros peligros añadidos. Estos mail pueden contener virus u otros códigos maliciosos, o direcciones de Internet que apunten a páginas web que estén preparadas para descargar algún tipo de programa en el equipo de manera no autorizada. Este ha sido, presumiblemente, el método que ha empleado el conocido gusano Sobig.F para conseguir el título del "virus que más rápidamente se ha propagado en la historia de la informática".

2.20.5.-EL PHISHING

Consiste en el robo de datos bancarios por medio de Internet. El método más habitual es el empleo del correo electrónico para contactar con usuarios y convencerles de que visiten páginas que imitan las de la entidad suplantada y en las que, además, deben introducir datos personales (número de cuenta, PIN, etc.,), que quedan así registrados.

Es habitual que después de la introducción de los datos se muestre una página de error, para que la víctima piense que no se ha podido realizar la conexión y así no sospeche nada. Otra técnica para robar datos bancarios consiste en la introducción en el ordenador a espiar de un ejemplar de malware de tipo troyano, con funcionalidades de keyLogger (o programa que registra las pulsaciones del teclado de un ordenador).

En la práctica, cuando el troyano detecta que el usuario está visitando la URL de una entidad bancaria, el keyLogger se activa y recoge todas las pulsaciones del usuario, que normalmente incluirán logins, passwords, números de cuenta y otros datos bancarios. Además de los citados métodos, últimamente se ha reportado

2.20.6.-El PHARMING

Es un método nuevo similar al phishing pero más sofisticado y con el mismo fin. En este caso, el ataque se realiza al ordenador del usuario o al proveedor de servicio de Internet, de modo que cuando el usuario solicita -como hace normalmente- una página de su entidad bancaria, se le redirecciona a otro sitio web que imita la página original. En la actualidad, la detección de las citadas amenazas que persiguen el fraude electrónico está supeditada al uso que hacen de las técnicas de malware tradicionales.

En el pharming, la neutralización es más compleja, máxime si el ataque lo llevan a cabo usuarios malintencionados desde el exterior y no algún tipo de malware introducido previamente.

2.20.7.-EL SCAM

Se conoce con el nombre de Scam los e-mails que, bajo una falsa promesa de ganar dinero sin esfuerzo, pretenden estafar a la persona que lo recibe. Es una mezcla de Spam (correo basura) y Hoax (engaño). El Scam se puede clasificar en:

- Scam Africano o nigeriano: Un supuesto miembro del gobierno, o un jefe de un banco o petrolera, pide al incauto en cuestión que le facilite los datos de su

cuenta bancaria para poder ingresar en ella una cantidad de dinero que quiere sacar del país, ofreciéndole a cambio una recompensa económica. Si éste accede, después de unos cuantos contactos por teléfono, correo electrónico o fax, se le pide alguna cantidad económica para un "gasto inesperado" o un soborno. Después de esto, a la víctima ni le devuelven ésta cantidad ni se le da lo que le habían prometido.

- Scam del Tío de América: Unos supuestos albaceas de un millonario y desconocido familiar informan al receptor de su fallecimiento y le comunican que lo incluyó en su testamento. El timo consiste en pedir al incauto que desembolse una cantidad de dinero para hacer frente a algún gasto inevitable. Los autores de éstos Scam se ayudan de técnicas de Ingeniería Social para hacer coincidir el apellido del supuesto difunto y el del destinatario.
- Timo de la Lotería: En éstos Scam, se informa al receptor de que ha sido premiado en la lotería española, aunque no haya participado. Posteriormente se le pide al destinatario un desembolso para hacer frente a algún gasto causado por algún trámite importante.

2.20.8.-ROOTKITS

Son herramientas que permiten esconder procesos y archivos a los hacker o cracker al momento de acceder a un sistema informático aprovechando algún puerto abierto, con el fin de obtener información ilícita. En la actualidad existen rootkits para todo tipo de sistema operativo.

2.20.8.1.-CLASES DE ROOTKITS

- **Kits binarios:** alcanzan su objetivo sustituyendo ciertos ficheros del sistema por sus contrapartes infectadas con troyanos.
- **Kits del núcleo:** utilizan los componentes del núcleo (también llamados módulos) que son reemplazados por troyanos.
- **Kits de bibliotecas:** emplean las Bibliotecas de Vínculos Dinámicos Dynamic Link Libraries – DLL) del sistema para "insertar" Troyanos.

2.20.9.-DUQU

Es un tipo de gusano informático que utiliza mecanismos rootkits siendo su función igual al de un KeyLoggers sofisticado.

2.20.10.-STUXNET

Es un tipo de virus o gusano informático que su propósito es atacar directamente a sistemas de control industrial automatizados de servicios públicos o privados, su diseño se basa en programación plc (controladores lógicos programable), de siemens sus funcionalidad es la siguiente

- ✓ Usa varias rutinas para identificar el modelo de PLC
- ✓ Identifica el dispositivo e infecta.
- ✓ Obtiene el control absoluto para interceptar todos los datos que fluyen desde o hacia el PLC
- ✓ Posee la capacidad de manipular los datos.

Como sabemos los PLCs automatizan tareas de tipo industrial muy diversas que pueden ir desde el control de una correa transportadora hasta la regulación de la temperatura y la presión de un reactor nuclear, y si de alguna manera estos PLC fuesen infectados por stuxnets este podría tener el control, básicamente su método de trasmisión se basa en las unidas de almacenamiento extraíbles esto se da por que los computadores que contienen funciones PLC no usan o están conectadas al internet.

2.20.11.-SPYWARE

Este software tiene similitud de un virus pero realmente no es, por esta razón los antivirus no lo detectan, su función después de ser instalado en un computador es la de espiar información que después será enviada a empresas de publicidad en internet, este tipo de programa puede capturar direcciones de correos electrónicos, contraseñas, datos de tarjetas de crédito o bancarias y todo lo que realice el usuario en su computador infectado por esta aplicación.[19]

Alguno de los síntomas más comunes que siente el ordenador cuando obtiene spyware pueden ser los siguientes:

- Nuevas páginas favoritas agregadas a la lista de tu explorador.
- Errores de navegación en tu explorador.
- Paginas de inicio modificadas, y/o cambiadas a otras.
- Comienzan a aparecernos pop ups a lo loco. Aun sin estar conectado, y sin tener el Explorer abierto.

[19]http://www.eset-la.com/centro-amenazas/tipos-amenazas

- Las famosas toolbars o searchbars comienzan a aparecer.
- Nuevos botones, y utilidades se bajan, como junksoft o programas basura.
- Notas el incremente de pornwebsites ves porno a menudo, e incluso en tu ordenador aparecen, el más común es el HotTartz.
- La velocidad de tu navegador varía.

2.20.12.-BOTNET

Se le conoce con el nombre de botnet a las computadoras que se encuentra comprometidas a través de software bots que forman una red de bots (normalmente es un gusano que corre en un servidor infectado con la capacidad de infectar a otros servidores). Estos programas permiten manipular y controlar un computador de forma remota para:

- enviar spam fraudulentos a sus víctimas.
- Para la descarga de materiales que ocupan gran espacio y consumen gran ancho de banda: Es decir, también se utilizan estas Botnets como mirrors de archivos grandes, normalmente de contenido ilegal.
- Para realizar ataques de tipo D.D.O.S. (Distributed D.O.S.: Denial Of Service).
- vender sus servicios a los Spammers.
- Roban información privada y se la comunican al usuario malicioso
- Enviar virus, software espía etc.

2.20.13.-DORKBOT

Es un código malicioso que se encuentra entre los más propagados en Latinoamérica y convierte a los equipos infectados en parte de una red botnet, roba credenciales de acceso de los usuarios y realiza ataques de phishing contra bancos.

El ataque lo realizan con un e-mail supuestamente proveniente de una compañía de telefonía móvil, en el que se le informa al destinatario que ha resultado ganador de un premio. En el mensaje incluye un saludo personalizado y solicita el ingreso a un sitio para reclamar la recompensa. Sin embargo, al acceder a dicho sitio el usuario ingresa a una página en la que se le indica que para obtener el premio debe descargar un software de comprobación, que en realidad es un archivo ejecutable que contiene la amenaza

2.20.14.-ADWARE (Software de anuncios)

Es un tipo de software que automáticamente se encarga de ejecutar o mostrar publicidad en un computador, animando así a los usuarios a instalar falsos programas como antivirus etc.

Estos programas se instalan generalmente sin que el usuario se de en cuenta. De forma engañosa. Tienen la capacidad de restaurarse cuando el usuario lo haya eliminado.

Su función es forzar al usuario a ver publicidad de productos o servicios, o también instalar las conocidas barras que se añaden al Internet Explorer como por arte de magia. Se suele utilizar anunciando que el usuario está infectado por adware, y que rápidamente compre el anti-adware que es anunciado. Todo esto para seguir con su infección.

2.20.15.-PAYLOAD

Son el o los efectos nocivos o hasta irreparables, que ocasionan a los sistemas de los equipos, sean éstos servidores, estaciones de red o computadoras domésticas:

El objetivo de un desarrollador de virus, es generar un payload, no solamente dañino, sino que además genere efectos secundarios como:

- Efecto directo de daño a los archivos o áreas del sistema, archivos.
- Corrupción o borrado de archivos con diversas extensiones, de diversas carpetas o de todo del disco. Formateo de los discos duros, etc.
- La propagación a través de otros servicios de Internet, tales como correo electrónico, Mensajería Instantánea, ICQ, Chat, redes compartidas Peer to Peer, liberación de Troyanos/Backdoor, etc.
- Efectos secundarios tales como la des habilitación o término de procesos de software antivirus, firewalls, de monitoreo y hasta herramientas de sistema.
- Algunos mensajes o cajas de diálogo en la pantalla, como colofón del payload.
- Toda expresión y/o daño que la mente de los creadores de virus puedan crear y desarrollar.

2.20.16.-RANSOMWARE

Es un software malicioso que una vez se ejecuta en nuestro equipo impide el funcionamiento normal del mismo, ya que entre otras, puede bloquear el acceso a

algunos de nuestros archivos (archivos de imagen, archivos de música, ofimática, etc) e incluso, a todo el contenido de nuestro disco duro, desde una ubicación remota.

Normalmente, suele mostrarnos una ventana de aviso en la que nos solicita el pago de una cantidad de dinero a cambio de una clave para desbloquear o descifrar la información de nuestro equipo.

2.20.17.-LOS ROGUE O SCAREWARE

Son sitios web o programas que simulan ser una aplicación de seguridad, generalmente gratuita, pero que en realidad instalan otros programas dañinos. Bajo la promesa de solucionar falsas infecciones, cuando el usuario instala estos programas, su sistema es infectado.

Estos programas, que en la mayoría de los casos son falsos antivirus, no suelen realizar exploraciones reales, ni tampoco eliminan los virus del sistema si los tuviera, simplemente informan que se ha realizado con éxito la desinfección del equipo, aunque en realidad no se realizado ninguna acción.

Para los delincuentes es sencillo desarrollar este tipo de software, ya que los programas sólo muestran unas pocas pantallas y unos cuantos mensajes falsos para engañar al usuario.

2.20.18.-VULNERABILIDAD EN WINDOWS

Un nuevo troyano aprovecha una vulnerabilidad en Windows para permanecer oculto y activo en las computadoras infectadas.

Denominado Trojan.Dropper.UAJ, modifica una librería de código vital (comres.dll) obligando a todas las aplicaciones que necesitan comres.dll a ejecutar también esta amenaza.

Lo novedoso de este troyano es el hecho de que toma el archivo comres.dll original, lo modifica y luego lo guarda en su directorio original.

La modificación de la DLL incluye un código que puede agregar o eliminar usuarios, cambiar contraseñas, añadir o eliminar los privilegios de usuario, y ejecutar archivos. Con esta modificación, los ciberdelincuentes consiguen que la parte maliciosa del archivo se ejecute al mismo tiempo y siempre que se ponga en marcha la DLL original.

La táctica usada hasta la aparición de este troyano innovador es más simple: el malware se copia en el mismo lugar y con el mismo nombre que la DLL original, sustituyéndola, pero de esta manera eran más fáciles de detectar.

Con la modificación de la DLL original y su posterior restitución a su lugar de origen, este troyano puede ocultarse mejor. Los ciberdelincuentes eligieron el archivo comres.dll, porque es ampliamente utilizado por la mayoría de los navegadores de Internet, y en algunas aplicaciones o herramientas de comunicación en red, lo que lo hace muy popular y, básicamente, indispensable para el sistema operativo

2.20.19.-EL BOT AINSLOT.L

Este malware está diseñado para registrar todas las acciones del usuario, descargar otros ejemplares de malware y controlar el sistema.

Además, hace funciones de troyano bancario, robando las credenciales de determinadas entidades financieras.

Una de sus particularidades es que analiza el equipo en busca de otros bots pertenecientes a otras redes y los elimina, de tal forma que sea el único que ocupe el sistema.

Ainslot.L llega a través de un correo fraudulento que simula proceder de la tienda de ropa inglesa Cult. En este correo, muy bien redactado, se le hace creer al usuario que ha realizado una compra en Cult de cerca de 200 libras esterlinas y que se le cargará dicha cantidad a su tarjeta de crédito. Incluye un link para revisar el pedido que conduce a la descarga del bot en la computadora.

2.20.20.-FALSO PLUGIN DE GOOGLE+ HANGOUTS

Un nuevo ataque informático que consiste en la distribución de malware usando como cebo una invitación a Google+ Hangouts, un servicio de Google que permite ver y comentar videos en grupo a través de la red social Google+.

El ataque comienza cuando los usuarios reciben una invitación en sus correos electrónicos invitándoles a descargarse el plugin de Google+ Hangouts.

En caso de seguir el link, llegarán a una página, que imita a la oficial de este servicio, y en la que se les mostrará un botón desde el que descargarse el plugin.

Si lo hacen, en su equipo aparece un archivo con el nombre hangouts.exe, que aunque hace referencia al servicio, para engañar al usuario, en realidad esconde un troyano.

En caso de activarlo, el mismo quedará con su computadora comprometida y sus datos podrán caer en manos de los ciberdelincuentes.

2.20.21.-GAUSS

Es una herramienta de espionaje informático financiada por un estado nacional y diseñado para robar datos sensitivos, en especial contraseñas del navegador de Internet, credenciales de banca en línea, cookies y datos específicos de configuración de los equipos infectados.

Los múltiples módulos de **Gauss** tienen el propósito de recolectar información de los navegadores, entre ella la historia de las páginas web visitadas y las contraseñas usadas. También envían a los atacantes datos detallados de los equipos infectados, incluyendo información específica de las interfaces de red, los discos de la computadora e información del BIOS. El módulo de Gauss también puede robar datos de los clientes de varios bancos

Otra característica clave de gauss es la habilidad de infectar memorias USB aprovechando la misma vulnerabilidad LNK que usaron Stuxnet. El proceso de infectar memorias USB es más inteligente. Usa para guardar la información recolectada en un fichero oculto.

2.20.22.-EL VIRUS DE LA POLICÍA.

Es una manera de estafar a los internautas quienes reciben un correo electrónico de la jefatura de policía incluso utilizando el membrete oficial, además de localizar el idioma pudiéndose presentar en inglés, español, holandés, italiano, entre otros idiomas. En el correo se menciona que el usuario incurrió en un hecho de tenencia y/o distribución de pornografía por lo que será multado con un monto aproximado que deberá depositarlo a una cuenta.

2.20.23.-ASPROX.N,

Es un troyano que, sin que el usuario se entere, envía spam (correo basura) a su nombre. En este mensaje de correo basura, que imita correos legítimos de facebook, el usuario aparentemente invita a todos sus contactos a ser sus amigos en la red social y a descargar un archivo anexo, el cual está contaminado por el virus, continuando con su ciclo de distribución.

2.20.24.-LOLBOT.Q

Es un troyano que utiliza servicios de mensajería instantánea (IM), como Windows Live Messenger, para expandirse. En estas redes de IM, supuestos amigos o personas que quieren convertirse en amigas envían mensajes en los que invitan a hacer clic en un enlace con un contenido muy atractivo. El enlace contiene un código que secuestra la cuenta del usuario en Facebook, y luego le informa amistosamente a la víctima que si facilita su número telefónico, la empresa le enviará una nueva contraseña para recuperar el acceso a Facebook. Si el usuario cae inocentemente en el engaño, recibe la nueva contraseña, pero lo que no sabe es que se está suscribiendo a un servicio de mensajería no gratuito, por el que deberá pagar unos 11 dólares a la semana.

2.20.25.-ATAQUE IRC (CANAL DE CHAT DEL INTERNET)

Cuando un usuario ejecuta su cliente de IRC, lo que realmente está haciendo es pedir permiso para entrar en un servidor de IRC, que es el que alberga toda la maquinaria del sistema de chat. Este servidor se encarga de validar las entradas de los usuarios, de evitar

que se dupliquen losnicks (alias que cada usuario utiliza para entrar al chat), de controlar que el número de usuarios sea el adecuado, etc.

Pero, en un momento dado y bajo ciertas circunstancias, el servidor también puede expulsar a un usuario. Esto se produce, por norma general, cuando un cliente de IRC envía mucha información al servidor en poco tiempo. Así, para evitar la saturación del sistema, el servidor cierra la conexión. Este es, básicamente, el fundamento de los ataques vía IRC.

2.20.25.1.-TIPOS COMUNES DE ATAQUES IRC

Nukes: El procedimiento consiste en mandar paquetes de información falseados a la dirección IP de la víctima, de forma que su sistema responda enviando una gran cantidad de información al servidor de IRC, consiguiendo que éste lo expulse inmediatamente.

Floods: Consisten en envíos masivos de información al sistema de la víctima, de forma que ésta, al contestar, supere el límite de entrada de flujo de información que permite el servidor.

Además, los canales de IRC son cada vez más utilizados por virus informáticos para facilitar los ataques de hackers a sistemas informáticos. Así, por ejemplo, muchos troyanos, cuando se instalan en los equipos, se conectan a canales de IRC predeterminados, donde quedan a la espera de recibir las ordenes de su autor sobre las acciones a realizar en el sistema.

2.20.26.-EL PRIMER TROYANO SMS

Este ha afectado principalmente a usuarios de Latinoamérica. Se trata de Boxer, código malicioso que infecta equipos móviles con sistemas operativos Android y suscribe a las víctimas a números de mensajería Premium locales.

2.20.27.-DESCRIPCIÓN DE CONTRASEÑA

El primer gran problema que comúnmente tienen los usuarios es que establecen contraseñas fáciles de recordar mejor, otro grave error es que una misma contraseña la usan para todas las cuentas que tienen. Si alguien logra vulnerar la privacidad de la contraseña, por ejemplo del Gmail, puede probar la misma contraseña con otras cuentas como de Twitter, Facebook, Foursquare, Hotmail, etc. pudiendo tener el acceso a todas estas cuentas de una sola vez.

2.20.28.-QUIÉN VE TU PERFIL

La aplicación es un engaño para las cuentas de Facebook, donde simplementehace la atractiva promesa de espiar a quienes privadamente consultan el perfil de un usuario y que para tener este servicio. El usuario debe descargar la tentadora aplicación en su computador haciendo clic a un enlace, que luego lo lleva a una página de Facebook que le pide su contraseña. Tras seguir las instrucciones en la pantalla, el virus toma el control del perfil del usuario, y puede acceder a su información y la que sus contactos hayan puesto a su alcance.

2.30.- ACONTECIMIENTOS HISTÓRICOS

Tarjetas de regalo

Una nueva estafa en Facebook utiliza como cebo unas supuestas tarjetas de regalo con 200 dólares para comprar en el popular sitio web eBay.

Los delincuentes abrieron un evento en la popular red social en la que ofrecen una tarjeta regalo de 200 dólares para gastar en eBay a los 10.000 primeros usuarios en inscribirse al evento. Una vez que el usuario entra en la página del evento se explica mejor qué tiene que hacer para conseguir la tarjeta regalo.

Primero, tiene que usar el botón de "Me gusta" para unirse al evento, enviar la invitación a otros 50 amigos, ampliando así el espectro de la amenaza, y, después, compartirla, acrecentando aún más el alcance de la misma.

El último paso que debe dar el usuario es ir a una URL donde debe reclamar el premio. Esta URL, en realidad, conduce a la instalación de la aplicación "WhosStaliking", una vieja conocida de los expertos en seguridad y los usuarios de Facebook. La misma promete decir quiénes son los mayores seguidores en Facebook del usuario pero para ello, eso sí, antes pedirá acceso para publicar en el nombre del mismo y acceder a sus datos privados.

La empresa Bitdefender recomienda desconfiar de cebos como tarjetas regalo y premios en Facebook sin correspondencia fuera de la red social.

Basta con entrar en la web de eBay para comprobar como no publicita tal promoción en su web corporativa, una acción que la compañía comunicaría dado el supuesto volumen

de la misma: 10.000 tarjetas regalo de 200 dólares son un total de 2 millones de dólares invertidos en la campaña, un monto lo suficientemente elevado como para realizar una difusión de la campaña acorde. [20]

Falsos videos de comportamientos heroicos

Otra nueva estafa en Facebook utiliza como cebo falsos videos de comportamientos heroicos, como la historia de un policía que murió por ayudar a un ciudadano. Los falsos videos van acompañados de mensajes que exhortan a verlos con frases como: "necesitamos más gente como ésta" o "Esto es un héroe".

Cuando los usuarios intentan ver el video, se les pide que instalen un complemento para su navegador (en otra ocasiones es una actualización de Youtube). En ambos casos, lo que en realidad están instalando es un código malicioso que dará acceso a los ciberdelincuentes a la cuenta de Facebook del usuario. Una vez conseguido el acceso, los ciberdelincuentes, además de hacerse con todos los datos privados de la víctima, publicarán automáticamente la historia fraudulenta en el muro de todas las páginas en las que el usuario haya dado un "Me gusta". Además, la publicarán varias veces en el muro del usuario.

Adicionalmente, a medida que los amigos del usuario vayan cayendo en la trampa, y aprovechando la característica de Facebook que indica cuántos amigos han visto o compartido un mismo contenido, los otros amigos que aún no estén infectados irán viendo que un mismo link ha sido compartido por varios de sus contactos lo que, sin duda, les llevará a pensar que es interesante y, por lo tanto, les hará caer también en la

[20] http://www.muycomputer.com/2012/12/28/seleccion-amenazas-informaticas-mas-llamativas-2012

trampa, aumentando así la difusión de la estafa. Hasta el momento, más de 49.000 usuarios de Facebook han caído en este fraude.[21]

El virus informático stuxnets

Stuxnet, casi saboteó todo el programa nuclear de Irán y que además se abrió camino a la India e Indonesia, inicialmente los creadores de este virus eran desconocidos, aunque posteriormente el New York Times eliminó todo rumor o especulación confirmando que se trata de un troyano desarrollado y financiado por Israel y Estados Unidos con el fin de atacar las centrales nucleares iraníes pero es algo irrelevante, porque Stuxnet está disponible en internet como una "descarga gratuita" que cualquiera con acceso a Internet puede obtener. Para muchos la primera arma de código abierto.

Cantidad de modificaciones de malware detectadas para Android OS

Este desarrollo tan activo del malware para Android es un indicio de que cada vez son más los escritores de virus que se dedican a escribir programas maliciosos para dispositivos móviles.

Al igual que con el malware para Windows, el desarrollo de los programas maliciosos para móviles ha conducido a que surja un mercado negro de servicios para propagarlos. Los principales canales de propagación son las tiendas no oficiales de aplicaciones y los programas de afiliados.No podemos dejar de mencionar que los programas maliciosos móviles se están haciendo cada vez más complejos: los delincuentes desarrollan activamente la tecnología de enmarañamiento y protección del código, lo que complica su análisis

[21] http://www.elfinancierocr.com/opinion/Opinion-Retos-tecnologicos-siglo_0_225577470.html

Una cuarta parte de los programas maliciosos para Android detectados son troyanos SMS. Estos programas maliciosos vacían las cuentas de las víctimas, enviando SMS a números de pago sin que los dueños se den cuenta. Hace un par de años estos programas se podían encontrar sólo en las repúblicas de la ex URSS, en el Sureste Asiático y en China, pero ahora se han extendido por todo el mundo: en el segundo trimestre de 2012 hemos defendido contra SMS nocivos a los usuarios de 47 países.

El 18% de los programas maliciosos para Android detectados en el segundo trimestre son backdoors que les dan a los delincuentes el control total del dispositivo móvil. En estos programas se basan las botnets móviles. Sin embargo, este troyano se caracteriza por otra razón: todos los servidores de administración de este programa malicioso estaban registrados a nombre de una sola persona. Por supuesto, los datos de registro eran falsos, pero eran los mismos usados para registrar varios de los dominios de administración de Zbot (ZeuS). De esto se puede concluir que el robo de SMS se hace con la intención de recibir los códigos de autorización de transacciones bancarias y que

2.6.-MARCO TEMPORAL/ESPACIAL

- Ley Orgánica de Transparencia y Acceso a la Información Pública
- Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos
- Ley de Propiedad Intelectual
- Ley Especial de Telecomunicaciones
- Ley de Control Constitucional (Habeas DaLey de Propiedad Intelectual)

Ilustración N°: 6leyes sobe la seguridad de la información
Autor: Aníbal Guachichulca

2.6.1. MARCO LEGAL

INFRACCIONES INFORMATICAS	REPRESION	MULTAS
Delitos contra la información protegida (CPP Art. 202) 1. Violentando claves o sistemas 2. Seg. nacional o secretos comerciales o industriales 3. Divulgación o utilización fraudulenta 4. Divulgación o utilización fraudulenta por custodios 5. Obtención y uso no autorizados	 6 m. - 1 año 3 años 3 a 6 años 9 años 2 m. - 2 años	 $500 a $1000 $1.000 - $1500 $2.000 - $10.000 $2.000 - $10.000 $1.000 - $2.000
Destrucción maliciosa de documentos (CCP Art. 262)	6 años	---
Falsificación electrónica (CPP Art. 353)	6 años	---
Daños informáticos (CPP Art. 415) 1. Daño dolosamente 2. Serv. público o vinculado con la defensa nacional 3. No delito mayor	 6 m. - 3 años 5 años 8 m. - 4 años	 $60 – $150 $200 - $600 $200 - $600
Apropiación ilícita (CPP Art. 553) 1. Uso fraudulento 2. Uso de medios (claves, tarjetas magnéticas, etc.)	 6 m. - 5 años 5 años	 $500 - $1000 $1.000 - $2.000
Estafa (CPP Art. 563)	5 años	$500 - 1.000

Ilustración N°: 7 Infracciones Informáticas
Fuente:

2.4. MARCO ESPACIAL

La investigación que se desarrollara sobre las amenazas humanas y físicas en contra de la seguridad informática vs la protección de información, se llevara a cabo dentro de la ciudad de cuenca, donde se realizara el análisis y estudio de campo, el tiempo que tomara para el TTG será de tres meses.

3.- METODOLOGÍA

3.1. PROCESO DE INVESTIGACIÓN

3.1.1. UNIDAD DE ANÁLISIS

El lugar afectado por la investigación fue un ciber café de la ciudadela la Uncovia que cuenta con la disponibilidad de 20 computadores que labra diariamente de 8am a 21pm en la ciudad de cuenca

3.2. POBLACIÓN Y MUESTRA

3.2.1. CÁLCULO Y TAMAÑO DE LA MUESTRA

Para el estudio y elaboración de la formula, se ha tomado como universo, el número de ordenadores que dispone el ciber café que se encuentran ubicada en la ciudadela Uncoviade la ciudad de Cuenca

Formula de la Muestra

$$n = \frac{N * Z^2 * P * Q}{(N -)E^2 + ?^2 * P * Q}$$

Z	Nivel de confianza 95%	1,96
N	Tamaño del universo	33
E	Error admisible	0,05
P	Probabilidad de Confianza	0,5
Q	Probabilidad en contra	0,5

Tabla N°: 5 Cuadro de fórmula de muestra
Autor: Aníbal Guachichulca

Nivel de Confianza.- Probabilidad de que la estimación efectuada se ajuste a la realidad.[22]

Error Muestral.- Es una medida de la variabilidad de las estimaciones de muestras repetidas en torno al valor de la población, nos da una noción clara de hasta dónde y con qué probabilidad una estimación basada en una muestra se aleja del valor que se hubiera obtenido por medio de un censo completo.[23]

Tamaño del universo.- Es el conjunto de individuos o elementos que le podemos observar, medir una característica o atributo.[24]

Probabilidad de Confianza.- Es la probabilidad de que el verdadero valor del parámetro estimado en la población se sitúe en el intervalo de confianza obtenido.[25]

[22] http://www.monografias.com/trabajos12/muestam/muestam.shtml
[23] http://es.wikipedia.org/wiki/Error_muestral
[24] http://es.wikipedia.org/wiki/Tama%C3%B1o_de_la_muestra
[25] http://www.fisicanet.com.ar/matematica/estadisticas/ap02_intervalo_de_confianza.php

$$n = \frac{33(1.96)^2 * 0{,}50 * 0{,}50}{(33 - \ )(0{,}05)^2 + 1{,}96)^2 * 0{,}50 * 0{,}50}$$

$$n = \frac{31.6932}{1.0404}$$

$$n = 30.4$$

Al reemplazar y redondear los datos indicados en la fórmula anterior se obtuvo que el número de encuestas que se debe realizar:

$$n = 30$$

3.3. TIPO DE INVESTIGACIÓN

La investigación que se efectuara para obtener información será:

- Descriptiva que describirá las características fundamentales de cada una de los temas a investigar.
- Documental para obtener información de fuentes como libros, revistas, entre otros
- Aplicada para proveer solución de inseguridad informática a usuarios de red a través del presente proyecto.

3.4. MÉTODO

Se usara el método inductivo para analizar globalmente los conceptos de la información recopilada, para aplicarlos y comprobar su validez

3.5. TÉCNICA

Se utilizara como técnica la investigación de campo para realizar un análisis a través de encuestas a los usuarios que hayan sido atacados en red.

3.6. INSTRUMENTO

- Cuaderno de notas
- Materiales de oficina
- Libros de seguridad informática
- Software para irrumpir la seguridad

3.7.- METODOLOGÍA Y PROCEDIMIENTO USADOS PARA EL DESARROLLO DEL PLAN DE SEGURIDAD

- ✓ Análisis RUP
- ✓ Casos de uso
- ✓ Diagrama de procesos
- ✓ Diagrama de actividades

4.- DESARROLLO

4.1.-LEVANTAMIENTO DE PROCESOS

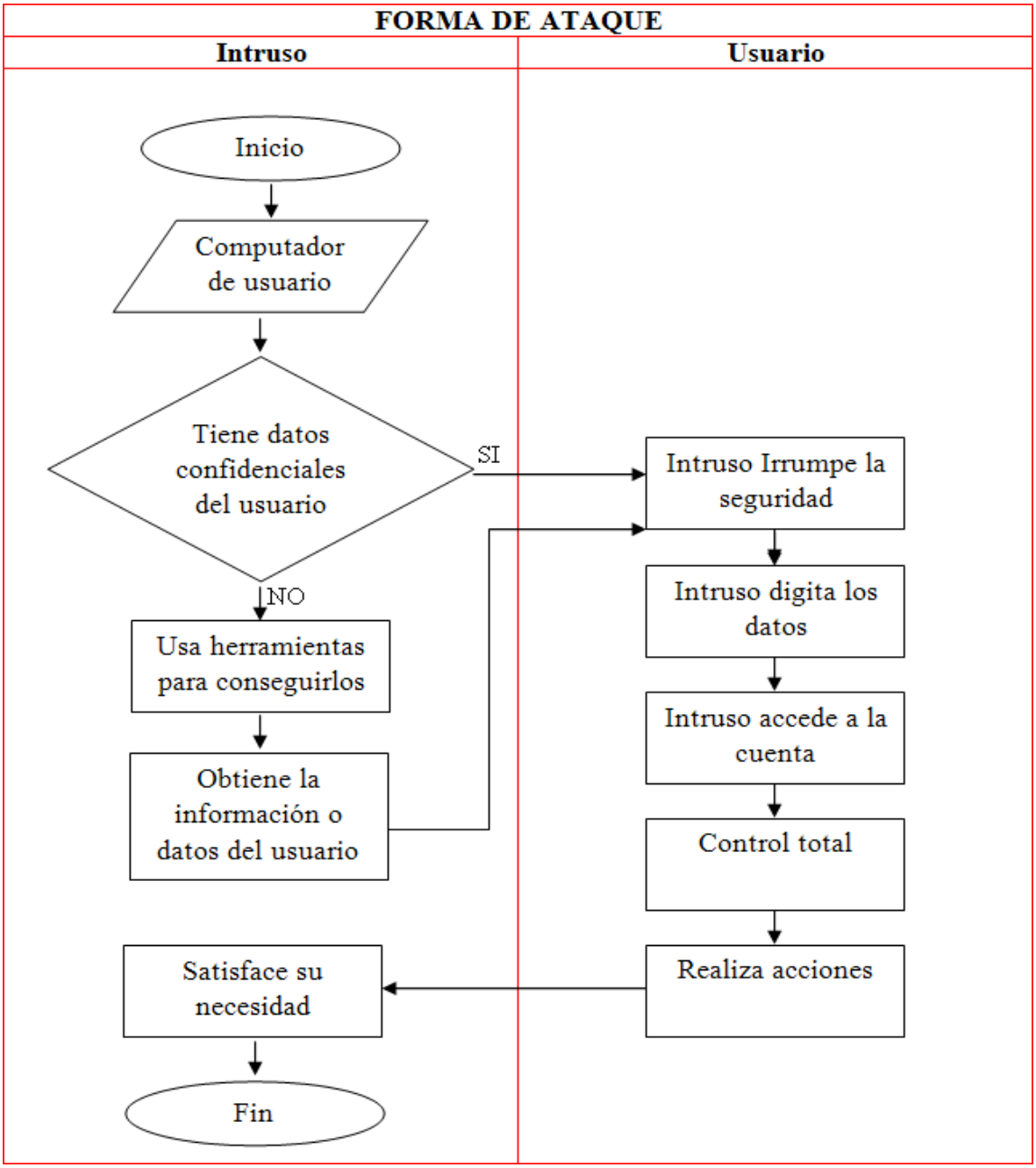


Ilustración N°: 8 Levantamiento de procesos - Diagrama de flujo de la forma de ataque
Autor: Aníbal Guachichulca

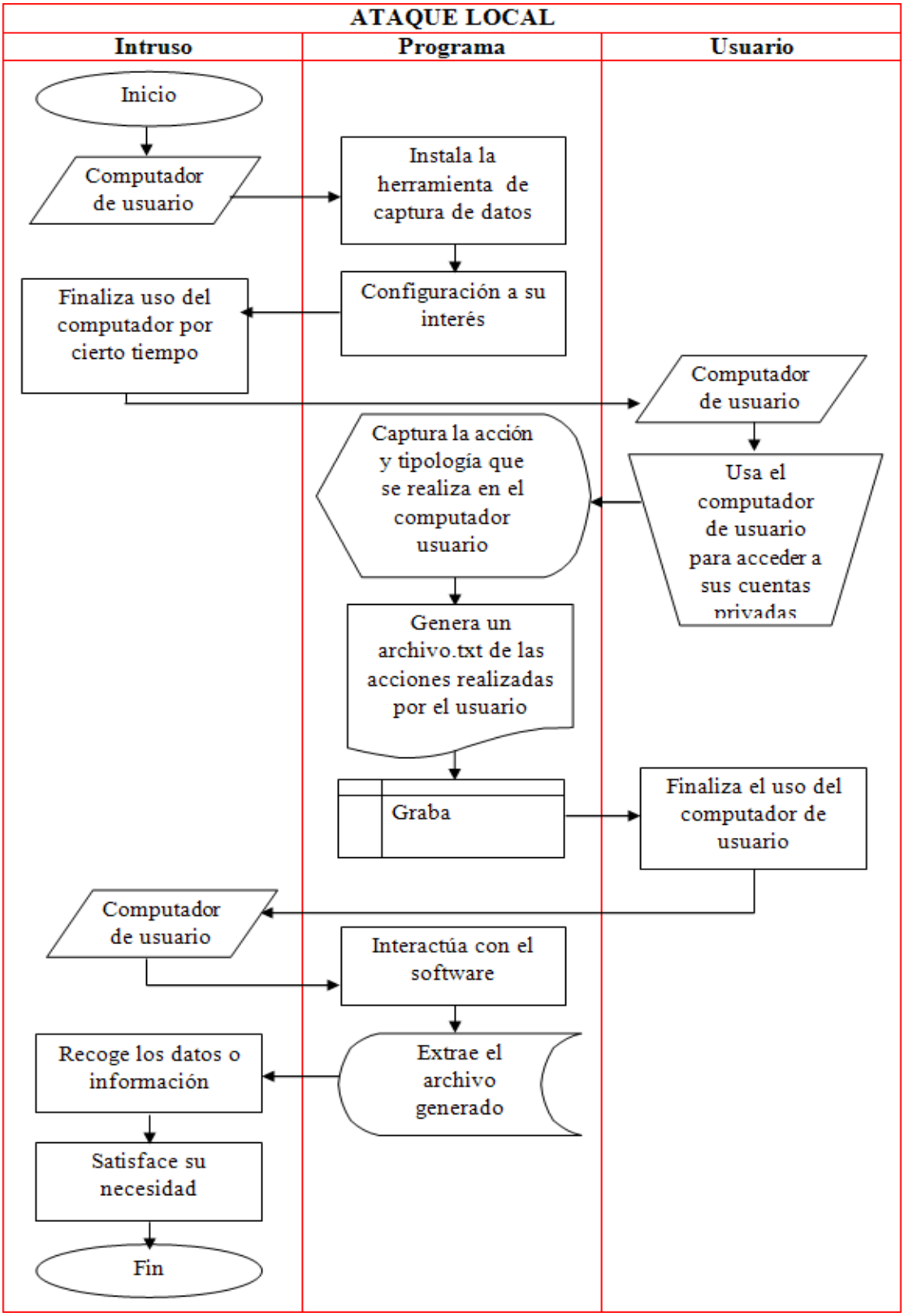


Ilustración N°: 9 Levantamiento de procesos - Diagrama de flujo de ataque local
Autor: Aníbal Guachichulca

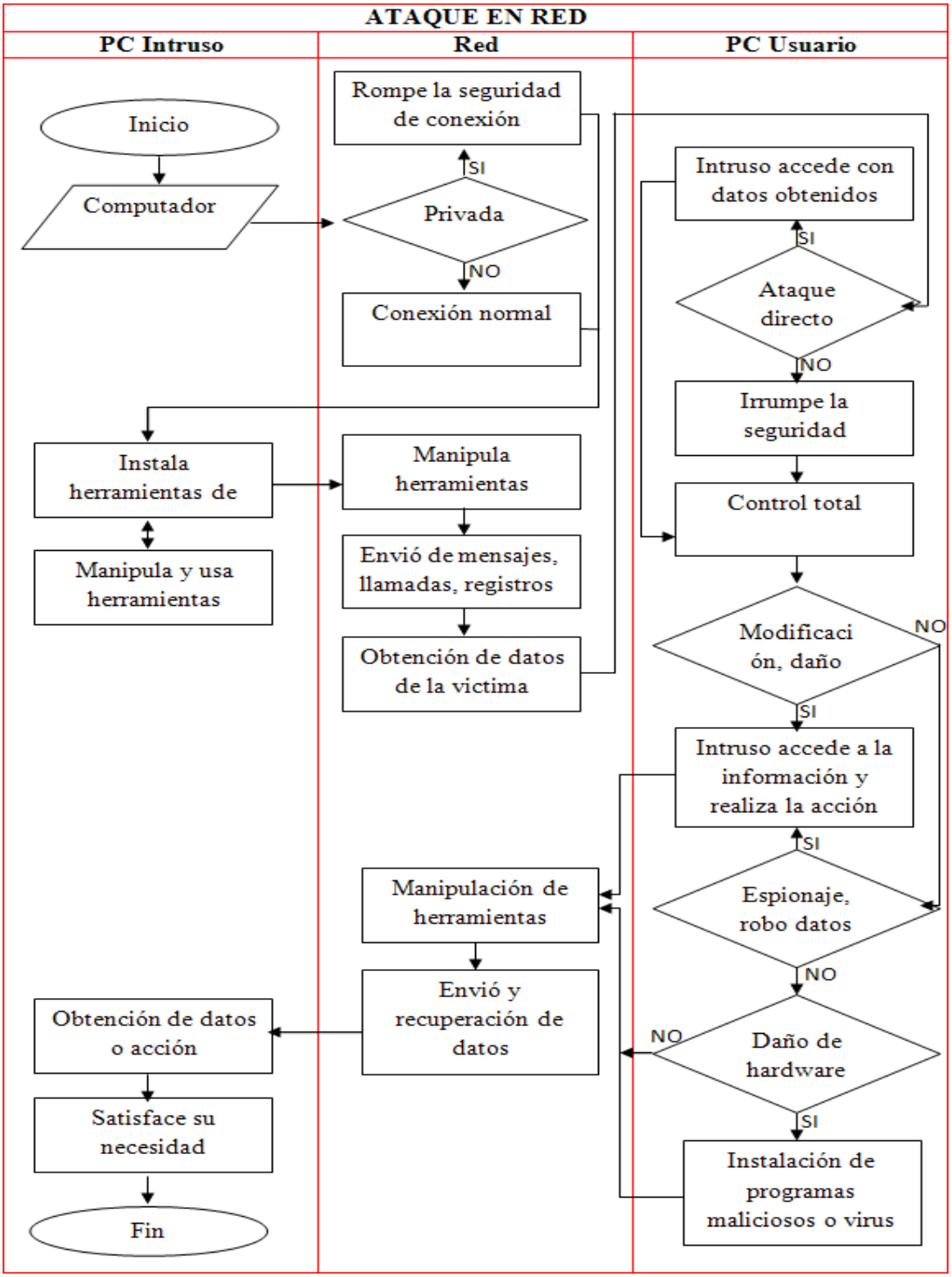


Ilustración N°: 10 Levantamiento de procesos - Diagrama de flujo de ataque en red
Autor: Aníbal Guachichulca

4.2.-DOCUMENTO DE VISIÓN DEL NEGOCIO

Problema de:	Intrusos Infringen o irrumpen la seguridad informática
Afecta a:	Los usuarios de un equipo computacional o red
Impacto del cual es:	Los intrusos siguen obteniendo información y dañando equipos de cómputo de forma ilícita.
Una solución exitosa seria:	Incitar al uso de herramientas o software de seguridad informática para el escaneo de red y equipo en contra de amenazas instaladas o de enlace.

Tabla N°: 6 Documento de visión
Autor: Aníbal Guachichulca

Problema de:	El uso inadecuado de la red
Afecta a:	Los usuarios de un equipo computacional o red
Impacto del cual es:	Aceden a sitios o descargas web no confiables, siendo más vulnerables a ataques e infecciones de virus
Una solución exitosa seria:	Informar al usuario a no visitar o registrarse en páginas poco confiables, a no responder a email o llamadas donde soliciten datos personales y confidenciales.

Tabla N°: 7 Documento de visión
Autor: Aníbal Guachichulca

Problema de:	El uso inadecuado o ilegal de herramientas que sirven para ataques informáticos
Afecta a:	Los usuarios de un equipo computacional o red
Impacto del cual es:	Facilitan la manipulación y obtención de información confidencial de un usuario a intrusos
Una solución exitosa seria:	Promover al uso de hardware y software de seguridad confiable y de tecnología adecuada para el usuario.

Tabla N°: 8 Documento de visión
Autor: Aníbal Guachichulca

Problema de:	El Robo, daño, modificación de la información de un usuario
Afecta a:	Los usuarios de un equipo computacional o red
Impacto del cual es:	Existencia de grandes pérdidas tanto de software como de hardware
Una solución exitosa seria:	Crear políticas y herramientas de seguridad para el uso de un equipo o red.

Tabla N°: 9 Documento de visión
Autor: Aníbal Guachichulca

Problema de:	Existencia de usuarios vulnerables a ataques
Afecta a:	Los usuarios de un equipo computacional o red
Impacto del cual es:	Existencia de mayores posibilidades de ataques, robo y estafas informáticas.

Una solución exitosa seria:	Incitar a los usuarios a ser más desconfiados al momento de usar un equipo o una red para confiar sus datos.

Tabla N°: 10 Documento de visión
Autor: Aníbal Guachichulca

4.3.-DECLARACIÓN DEL PRODUCTO

Para:	Análisis sobre las Amenazas Humanas y Lógicas contra la Seguridad Informática VS La Protección de Información.
Quien:	Usuarios de un equipo computacional o red
El:	Documento para la enseñanza de las amenazas informáticas
Que:	Plan de seguridad que sirva como herramienta de conocimiento, enseñanza y defensa contra las amenazas informáticas.
Nuestro producto:	Repositorio de la información para la educación de las amenazas informáticas a usuarios

Tabla N°: 11 Declaración del producto
Autor: Aníbal Guachichulca

4.4.-DESCRIPCIÓN DE CLIENTES, STAKEHOLDERS Y USUARIOS

Actor	**Responsabilidad**	**Actividad**
Intruso	Encargado de irrumpir la seguridad informática.	Espiar, robar, modificar, dañar información o

		hardware para satisfacer sus necesidades
Usuario	Usuario de una sistema, equipo o red, para realizar actividades persónales y privadas	Usa un equipo, sistema y red para sus actividades de trabajo, estudio, diversión o para la compra online

Tabla N°: 12 Descripción de cliente
Autor: Aníbal Guachichulca

4.5.-DEFINICIÓN DE CUADRO DE ACTORES

Actor	Perfil
 **Intruso**	Especializados en una área tecnológica Conocimientos solido de informática y sistemas Conocimientos de seguridades informáticas Conocimiento y manejo de herramientas para irrumpir la seguridad Conocimiento de software para ataques locales o a nivel de red Habilidades para el robo y descifrado de datos Habilidad y conocimientos para el desarrollo de software malicioso Promueven la distribución de software e información libre

Ilustración N°: 11 Cuadro de actor
Autor: Aníbal Guachichulca

Actor	Perfil
 **Usuario**	Conocimientos básicos de informática Uso monótono de cuentas de usuario Uso de seguridad baja o repetible Poco conocimiento de amenazas en contra de la información Ignoran las amenazas informática existentes Comodidad y uso de software gratuito o de bajo costo Uso inadecuado del internet Confían sus datos sin saber a quien

Ilustración N°: 12 Cuadro de actor
Autor: Aníbal Guachichulca

4.6.-CASO DE USO DEL MODELO NEGOCIO

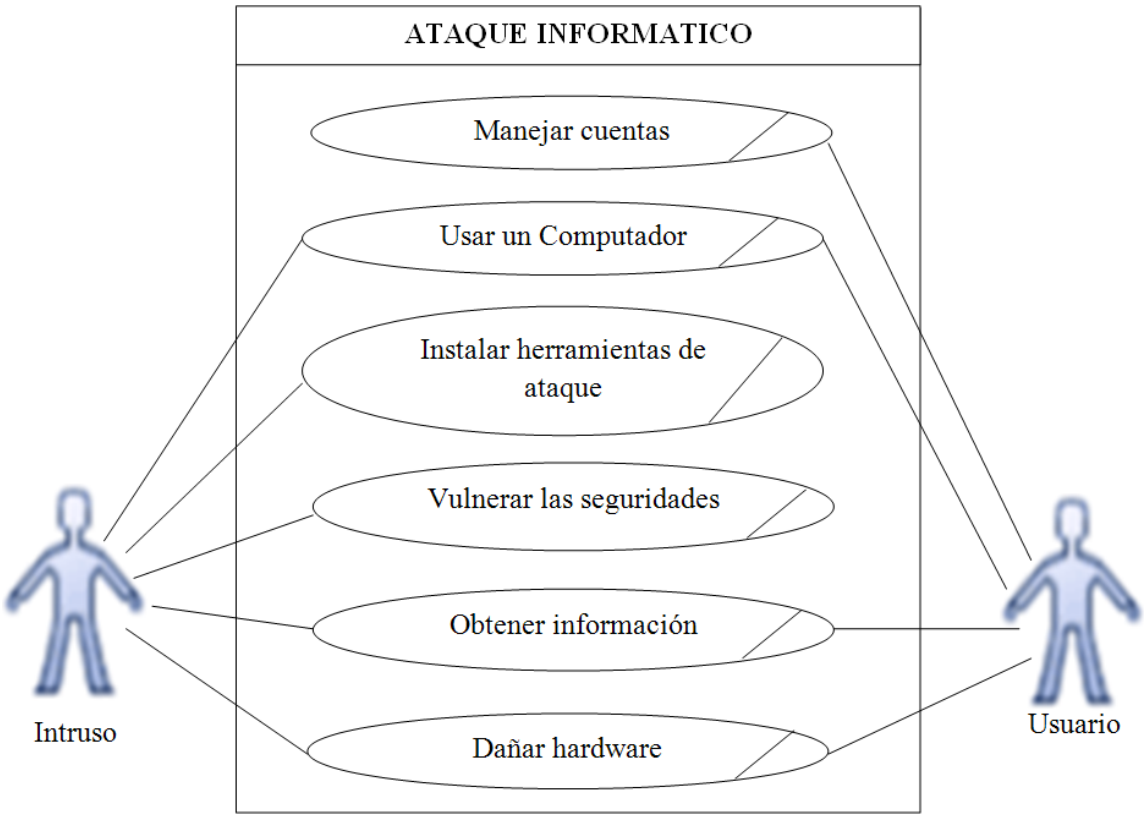


Ilustración N°: 13 Caso de uso general de Ataque Informático
Autor: Aníbal Guachichulca

4.6.1.-CASO DE USO DETALLADO DEL MODELO DE NEG OCIO

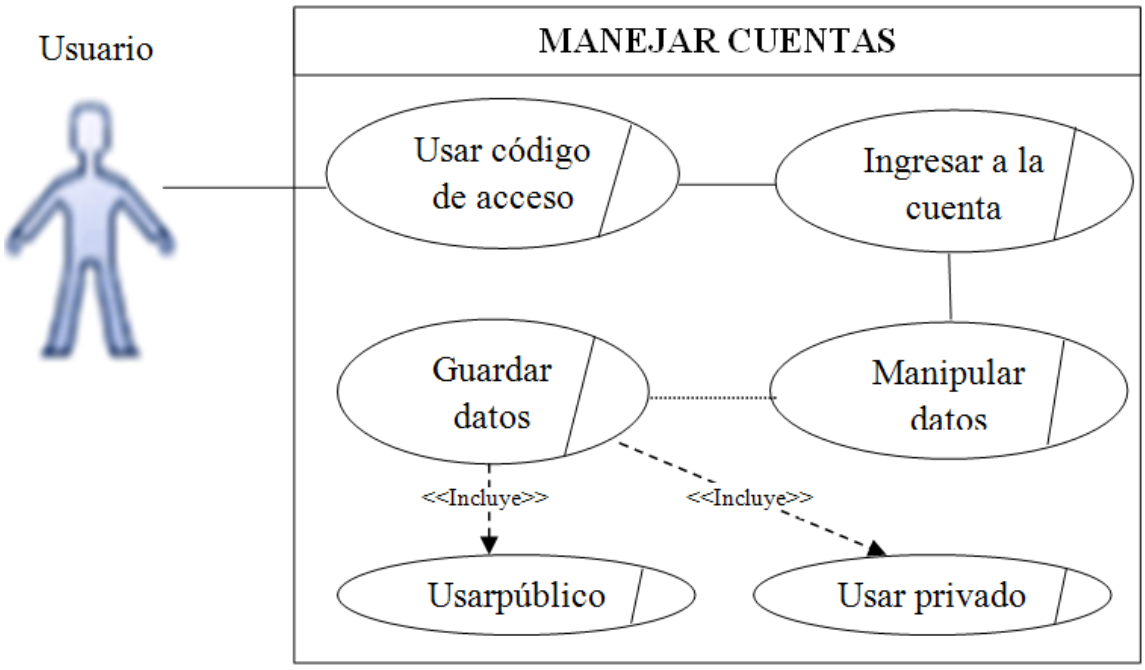


Ilustración N°: 14 Caso de uso detallado – Manejar Cuentas
Autor: Aníbal Guachichulca

Escenario: manejar cuentas
Quien lo comienza: los usuarios de un equipo computacional o red **Quien lo finaliza:** los usuarios de un equipo computacional o red **Excepciones:** Si el usuario confía sus datos a una tercera persona que supone confiable esta podrá administrar las cuentas a las que tenga acceso. **Descripción:** • El usuario necesita acceder a su cuenta para cierta actividad • Para ingresar en su cuenta necesita tener y usar su login y password • Se loguea y de esta manera si los datos son correcto este podrá ingresar • Realiza actividades y manipula su cuenta como administrador

- Necesita guardar datos o cambios realizados en su cuenta ya sea de forma pública o privada
    - Ejemplo de Publica: publicaciones
    - Ejemplo de Privada: mensajes de correo

Tabla N°: 13Escenario – Manejar Cuentas
Autor: Aníbal Guachichulca

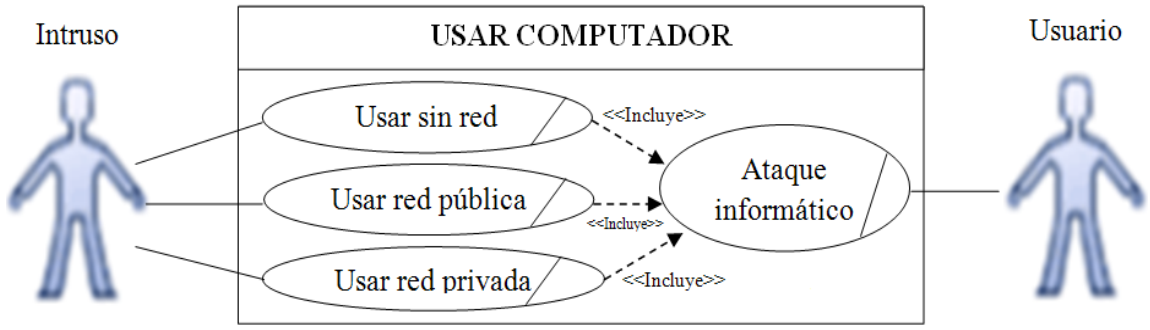


Ilustración N°: 15 Caso de uso detallado – Usar Computador
Autor: Aníbal Guachichulca

Escenario: Uso de computador
Quien lo comienza: Intruso informático **Quien lo finaliza:** los usuarios de un equipo computacional o red **Excepciones:** Si el intruso desea provocar un desastre físico como cortes de cables de electricidad de red de datos etc. **Descripción:**

- El intruso usa un computador
- Decide cómo realizar un ataque
- Si atacar un computador sin conexión a red es decir atacar de forma local rompiendo seguridades del computador (cuentas, claves para acceso a datos, etc.)
- O si atacar a nivel de red, para esto necesita conectarse a un punto conexión de red ya sea de uso público o irrumpiendo la seguridad de una privada para desde allí ejecutar un ataque.
    - ❖ Muchas de las redes de uso público no tiene contraseña de acceso pero si alguna lo tiene esta es dada a los usuarios en general
    - ❖ Las redes de uso privado siempre contendrá contraseñas y son de uso restringido para ciertos usuarios.

Tabla N°: 14 Escenario – Usar Computador
Autor: Aníbal Guachichulca

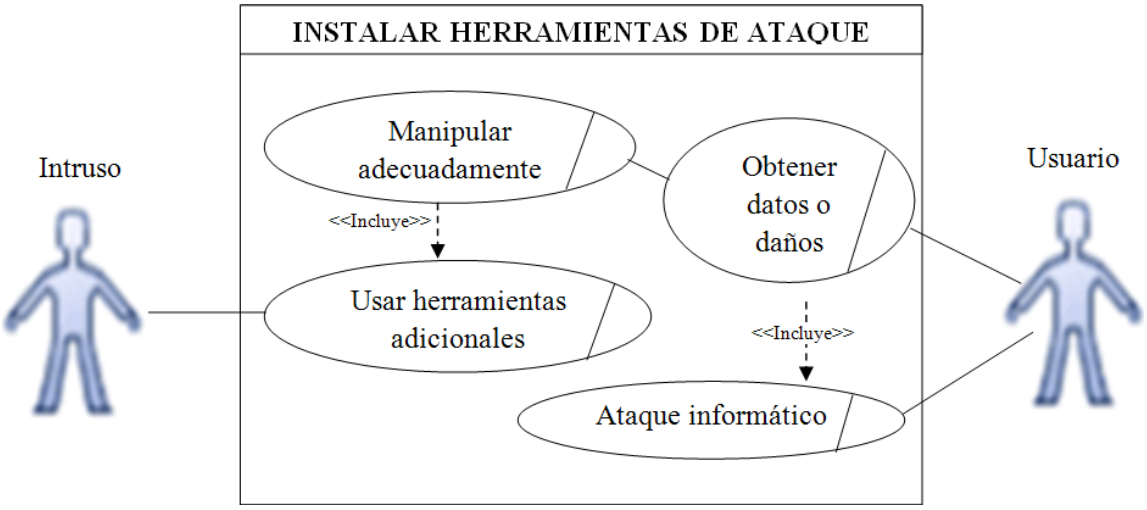


Ilustración N°: 16 Caso de uso detallado – Instalar herramientas de ataque
Autor: Aníbal Guachichulca

Escenario: Instalación de herramientas de ataque

Quien lo comienza: Intruso informático

Quien lo finaliza: los usuarios de un equipo computacional o red

Excepciones: Si el intruso desea provocar un desastre físico como cortes de cables de electricidad de red de datos etc. Este necesitara herramientas físicas

Descripción:

- El intruso usa un computador
- Instala herramientas de ataque de nivel local o de red
- Manipula las aplicaciones con o sin conocimientos
- Usa herramientas adicionales para el ataque (llamadas telefónicas, envió de email etc.)
- Obtiene acceso a la privacidad del usuario como administrador
- Obtiene datos para robarlos, modificarlos, dañarlos o borrarlos etc.
- Obtiene un ataque informático para satisfacer su necesidad (Curiosidad, Económica, Venganza etc.)

Tabla N°: 15 Escenario – Instalar Herramientas de Ataque
Autor: Aníbal Guachichulca

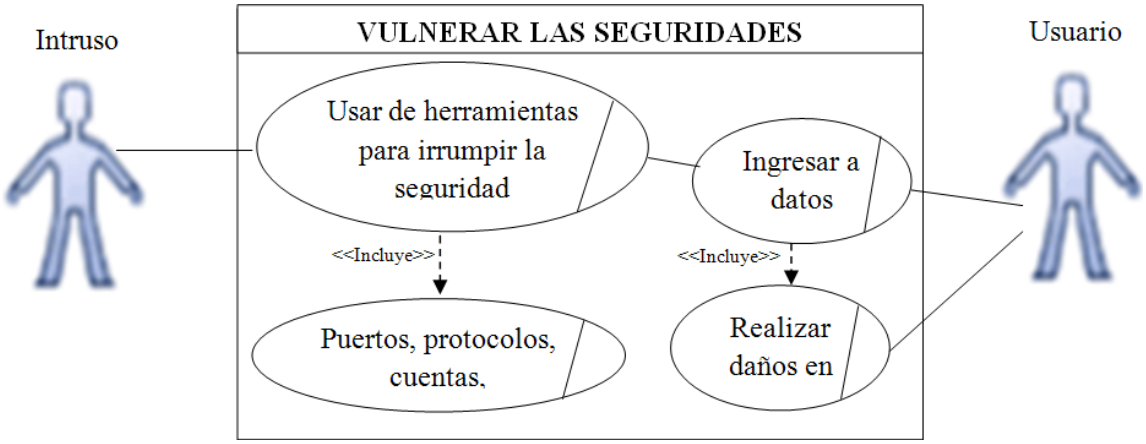


Ilustración N°: 17 Caso de uso detallado – Vulnerar las Seguridades
Autor: Aníbal Guachichulca

Escenario: Instalación de herramientas de ataque
Quien lo comienza: Intruso informático **Quien lo finaliza:** los usuarios de un equipo computacional o red **Excepciones:** Si el intruso desea vulnerar una seguridad física (acceder a un lugar restringido) este necesita conocer su estructura y su entorno físico **Descripción:** • El intruso usa un computador • Instala herramienta para irrumpir una seguridad de forma local o de red • Para irrumpir seguridad de red este necesita el uso de puertos, protocolos, cuentas de acceso etc.) • Una vez vulnerada la seguridad el intruso ingresa a una cuenta y obtiene acceso los datos • Realiza acciones con los datos de forma administrativa (agregación, eliminación, modificación, robo) en contra del usuario propietario.

• De acuerdo a su interés una vez que el intruso haya accedido a la cuenta este puede causar daños de todo nivel (alto, medio, bajo) en contra del usuario propietario

Tabla N°: 16 Escenario – Vulnerar Seguridades
Autor: Aníbal Guachichulca

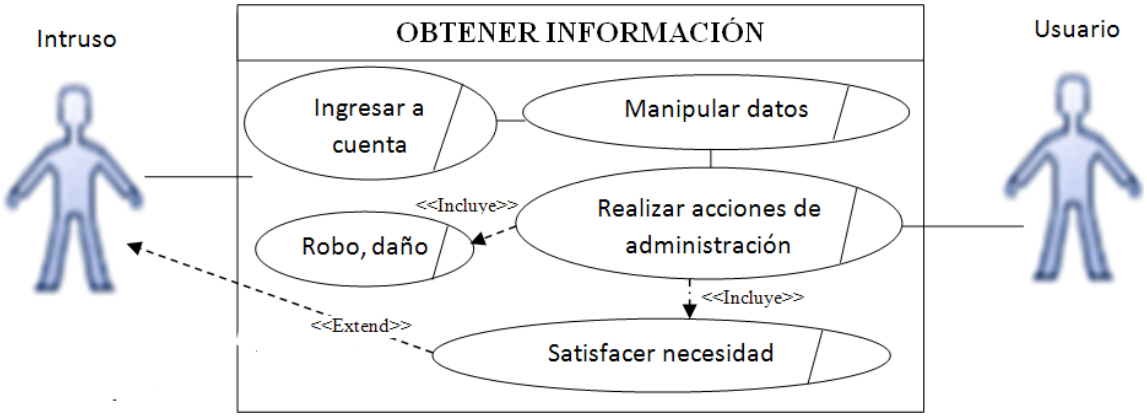


Ilustración N°: 18 Caso de uso detallado – Obtener Información
Autor: Aníbal Guachichulca

Escenario: Obtención de información
Quien lo comienza: Intruso informático **Quien lo finaliza:** los usuarios de un equipo computacional o red y el intruso informático **Excepciones:** Si el usuario confía sus datos a una tercera persona que supone confiable esta podrá administrar las cuentas a las que tenga acceso. **Descripción:**

- El intruso una vez que haya obtenido los datos confidenciales de acceso
- Se loguea para ingresar a una cuenta
- Obtiene el privilegio de administrador de la cuenta
- Realiza acciones (como espiar, robar, modificar o dañar la información) en contra del usuario
- Con esto el intruso satisface su necesidad (Curiosidad, Económica, Venganza etc.)

Tabla N°: 17 Escenario – Obtener Información
Autor: Aníbal Guachichulca

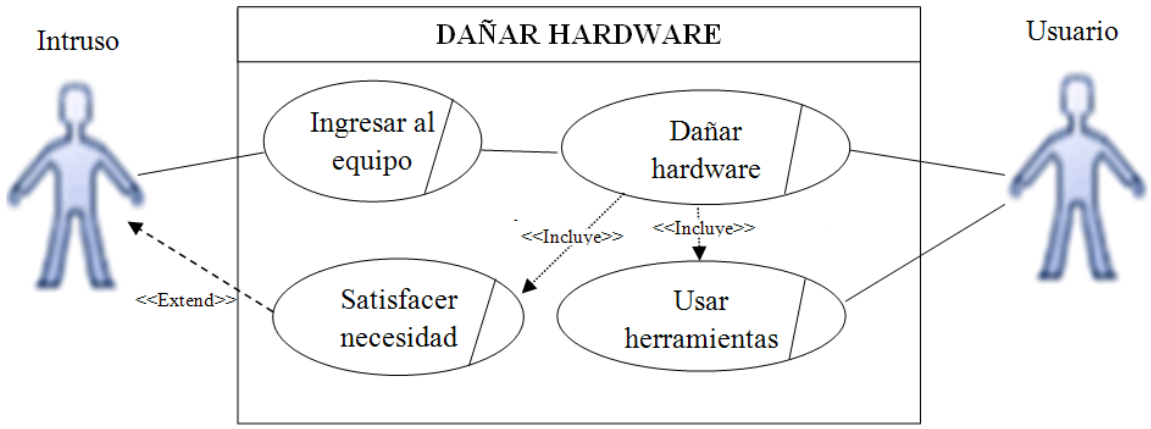


Ilustración N°: 19 Caso de uso detallado – Dañar Hardware
Autor: Aníbal Guachichulca

Escenario: Daño de hardware
Quien lo comienza: Intruso informático **Quien lo finaliza:** los usuarios de un equipo computacional o red y el intruso

informático

Excepciones: Si el usuario confía sus datos y su equipo a una tercera persona para que realice la acción concedida por el mismo.

Descripción:

- El intruso una vez que haya obtenido el equipo o los datos confidenciales de acceso
- Manipula el equipo o se loguea para ingresar a una cuenta
- Administra el equipo de forma física o lógica
- Realiza acciones de daño físico (Memorias RAM, Disco duro, Unidades lectoras, etc.) o lógico (activación de virus para daño de hardware, desinstalación de software, des configuración etc.) en contra del usuario
- Para dañar el hardware usa herramientas físicas o lógicas de acuerdo a como vaya a provocar el daño el intruso
- Con las acciones realizada el intruso satisface su necesidad (económico, envidia, venganza)

Tabla N°: 18 Escenario – Dañar Hardware
Autor: Aníbal Guachichulca

4.7.-DIAGRAMA DE ACTIVIDADES

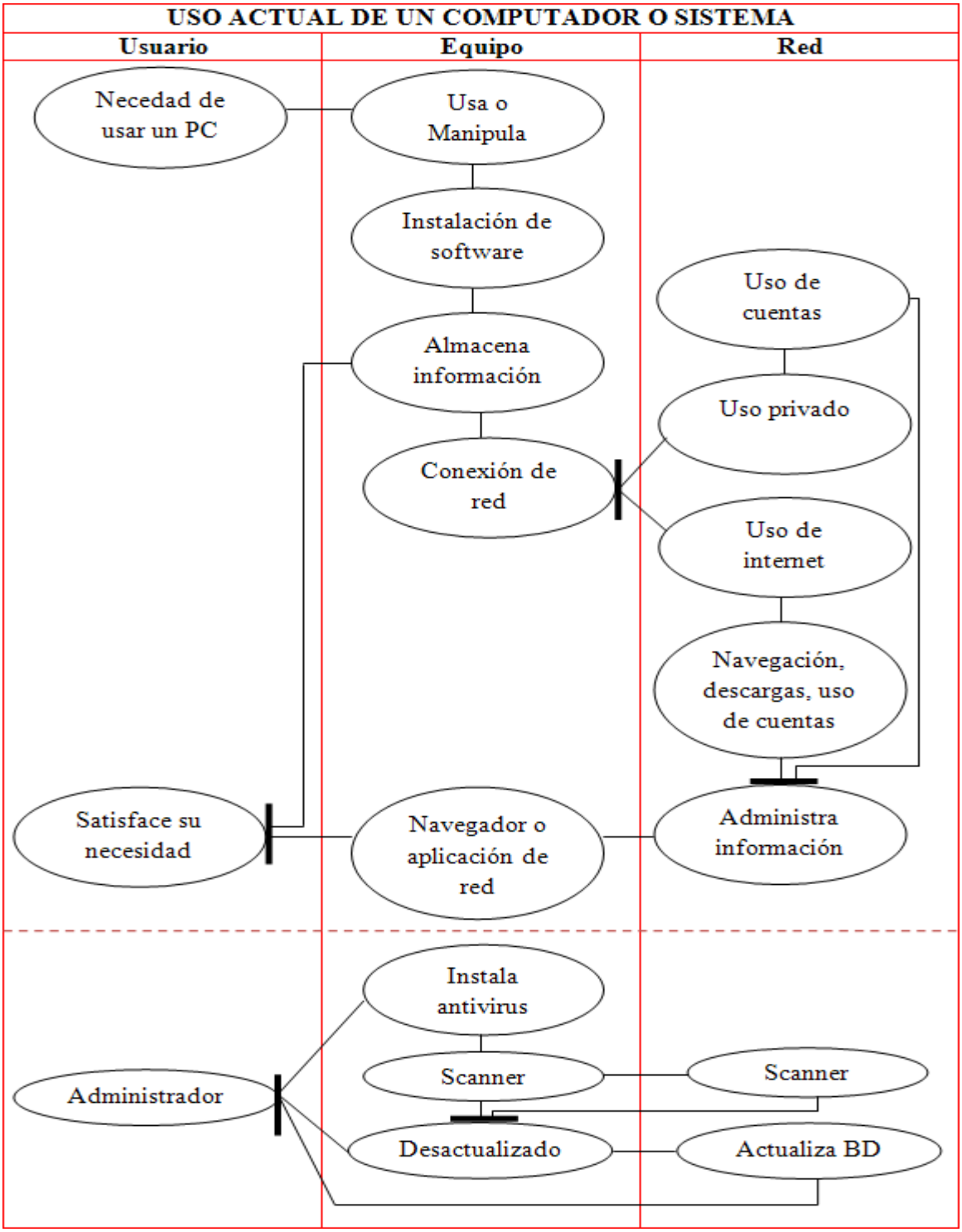


Ilustración N°: 20 Caso de uso detallado – Obtener Información
Autor: Aníbal Guachichulca

4.8.-LISTA DE RIESGOS

Problema	Descripción	Prioridad
Violación de seguridad informática	Acceso a cuentas privadas o restringidas de forma criminal	Medio
Ataque en la red por el mal uso	Navegación, registros y descargas ilegales que contienen software malicioso de captura o daño de datos	Alto
facilidad de adquisición de herramientas para violentar contra la seguridad informática	Información y Software de distribución gratuita o de bajo costo, para cualesquier usuario interesado	Alto
Robo de datos	Acción realizada por una persona con conocimientos informáticos para satisfacer su necesidad	Medio
Usuarios confiados	Personas que usan un equipo computacional, un sistema o red para realizar actividades diarias con pocos conocimiento de	Alto

	amenazas informáticas	

Tabla N°: 19 Lista de riesgos
Autor: Aníbal Guachichulca

4.9.-ANÁLISIS ESTADÍSTICO

Las encuestas se realizaron en la ciudad de Cuenca a los Usuarios de un ciber café "Internet Banda Ancha" de sector de la Uncovia de la ciudad de cuenca

Para conocer el número de encuestas a realizar se usó la formula de la población y muestra, la que dio como resultado 30 encuestas.

Con las encuestas se pretende recabar información con la podemos obtener datos acerca de las amenazas informáticas, experiencias y conocimiento sobre las mismas.

Los encuestados fueron elegidos a lazar dentro del local de servicio dependiendo la disponibilidad del mismo y su cooperación a responder las siguientes preguntas:

1.- Ha usado algún tipo de red informática.

Descripción	**Total**	**Porcentaje**
Internet	21	70%
empresarial	8	27%
Privada	1	3%
Total	30	100%

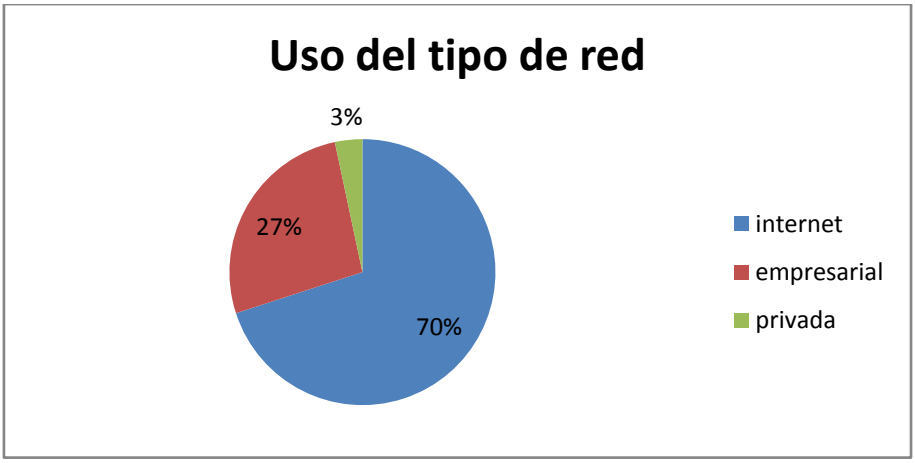


Tabla N°: 20 Tabulación estadístico de la pregunta 1
Autor: Aníbal Guachichulca

En el grafico podemos apreciar que el 70% de las personas usan el servicio de internet ya sea en sus propias casas o en lugares que brinden el servicio como Ciber Cafés etc. Como segunda red usada tenemos las redes empresariales, dentro de estas redes están prácticamente los empleados de una institución que usan las redes de trabajo en la empresa pública o privada

2.- Tiene conocimientos de amenazas que existen en la red

Descripción	Total	Porcentaje
Si	28	93%
No	2	7%
Total	30	100%

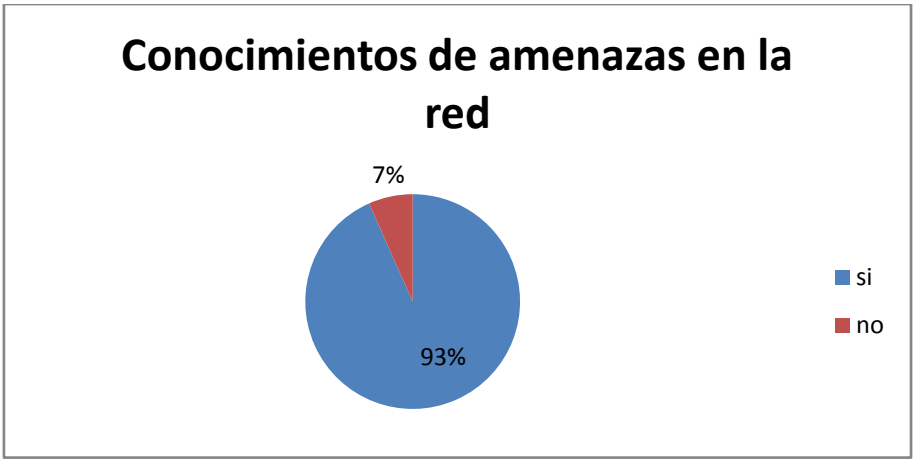


Tabla N°: 21 Tabulación estadístico de la pregunta 2
Autor: Aníbal Guachichulca

En el gráfico, según la pregunta de encuesta podemos observar un 93% de porcentaje de personas que tienen conocimiento de amenazas en la red, dentro de estas como las más nombradas resaltan

- Los virus (que se pueden descargar e instalar en el computador mientras se navega en el internet)
- Hackers (que realizan el hacking por la red a una página web, servidores, ordenadores etc.)
- Crackers
- Estafadores (que usan ingeniería social).
- Paginas sospechosas (que roban información confidencial)
- Programas que usan la red para robo de datos

3.- Ha tenido algún problema de estafa o robo de datos privados en la red

Descripción	Total	Porcentaje
Si	17	57%
No	13	43%
Total	30	100%

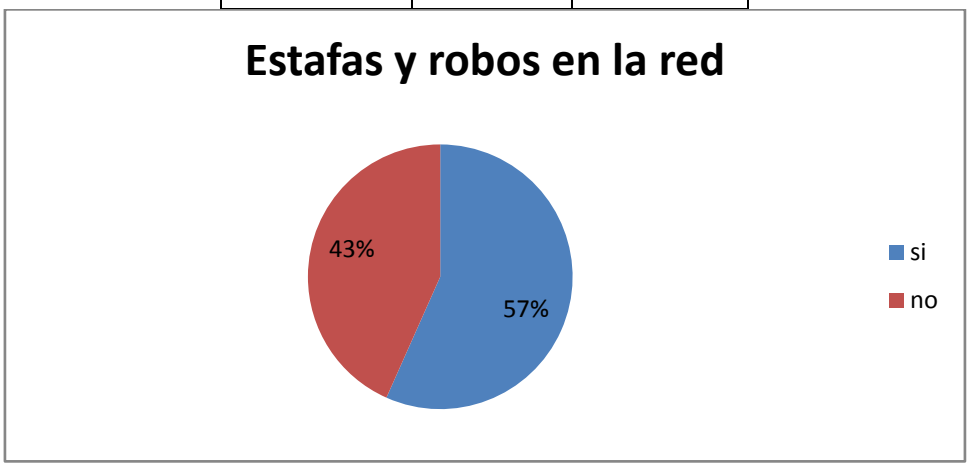


Tabla N°: 22 Tabulación estadístico de la pregunta 3
Autor: Aníbal Guachichulca

Según el grafico estadístico existe el 57 % de porcentaje de personas que han sido víctimas en la red, por alguna causa o motivo.

4.- cuál cree Ud. que lo hizo

Descripción	Total	Porcentaje
Hackers	15	50%
Crackers	3	10%
Informático	2	7%
Delincuente	8	27%
Ninguno	2	7%

Total	30	100%

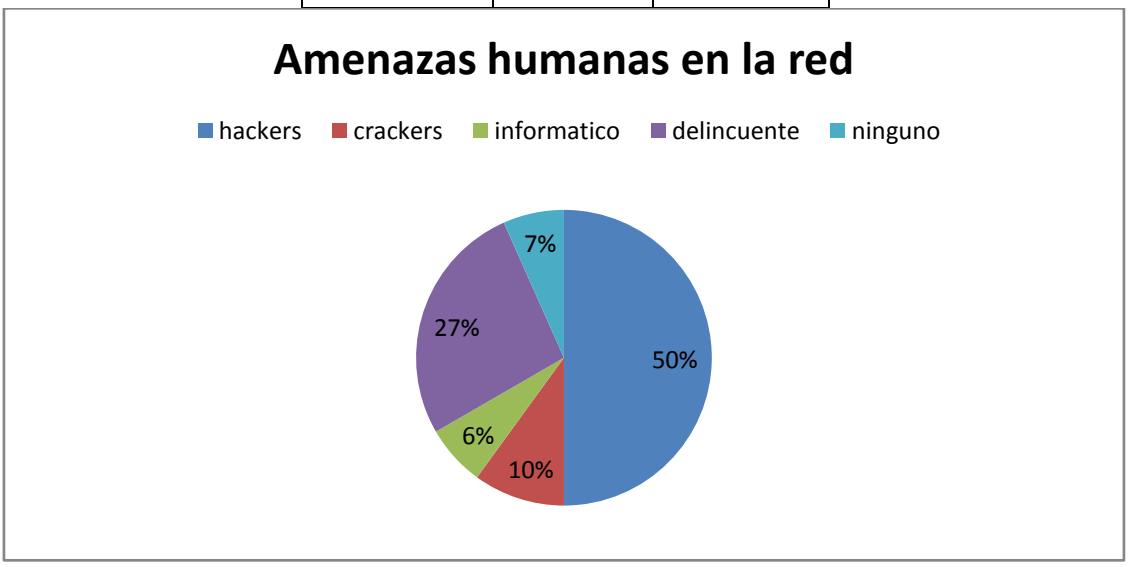


Tabla N°: 23 Tabulación estadístico de la pregunta 4
Autor: Aníbal Guachichulca

En esta pregunta de encuesta existen algunos tipos de coincidencias en las respuestas, acerca de quienes les pudieron haber robado información o hackeado, a más de las que se presentan en la estadística encontramos otra características de quienes creen que son los culpable.

- Ladrones o delincuentes
- Amigos o enemigos
- Enamorados o enamoradas celosas.
- Personas envidiosas o curiosas

Muchas de estas personas tienen algunos conocimientos de quienes realizan estos ataques en la red.

5.- Como cree que lo hizo

Muchas de las personas tienen diferentes respuestas y algunas coincidencias en los métodos que utilizan los atacantes una red como por ejemplo:

- Robando contraseñas
- Usando un computador
- Usando redes como el internet
- Usando aplicaciones de hacking

A más de estas personas existe un porcentaje del 2% que no tiene conocimientos de conque métodos o herramientas atacan en la red.

6.- Porque cree que lo hizo

Según la pregunta de encuesta muchas de las personas piensan que lo hacen por:

- Venganza
- Obtener información confidencial
- Para dañar o eliminar la información
- Para robar datos de importancia y venderlos
- Para copiar información y mejorarla

7.- Como lo considera a este problema de intrusos en la red

Descripción	**Total**	**Porcentaje**
Amenaza	28	93%
Normal	2	7%
Total	30	100%

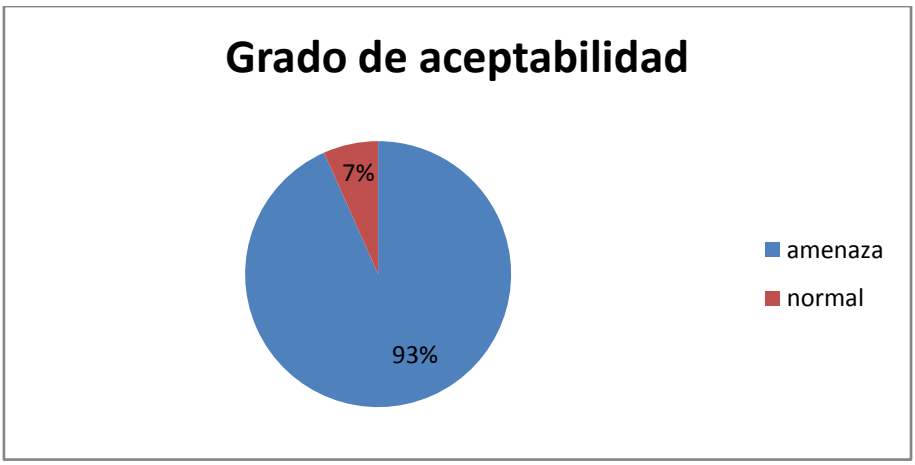


Tabla N°: 25 Tabulación estadístico de la pregunta 7
Autor: Aníbal Guachichulca

Existe un grado del 93% de las personas que las consideran como una amenaza a la información, por lo general estas han sido víctimas alguna vez, pero existen otro tipo de gente que lo consideran como normal, la razón es porque esta lo realiza o se debe a que todavía no han tenido un ataque por parte de los intrusos en la red

8.- como cree Ud. que podría dar mayor seguridad a sus datos o sitios web.

Las personas encuestadas tienen varias formas de brindar seguridad entre ellas algunas coincidencias:

- Reforzando la contraseña cada cierto tiempo
- Borrando historial
- Asegurándose del uso de sitios confiables
- Encriptado datos
- No ejecutar programas anónimos
- Evitando registrarse en sitios desconocidos

9.- ha tenido problemas con virus informáticos

Descripción	Total	Porcentaje
Si	29	97%
No	1	3%
Total	30	100%

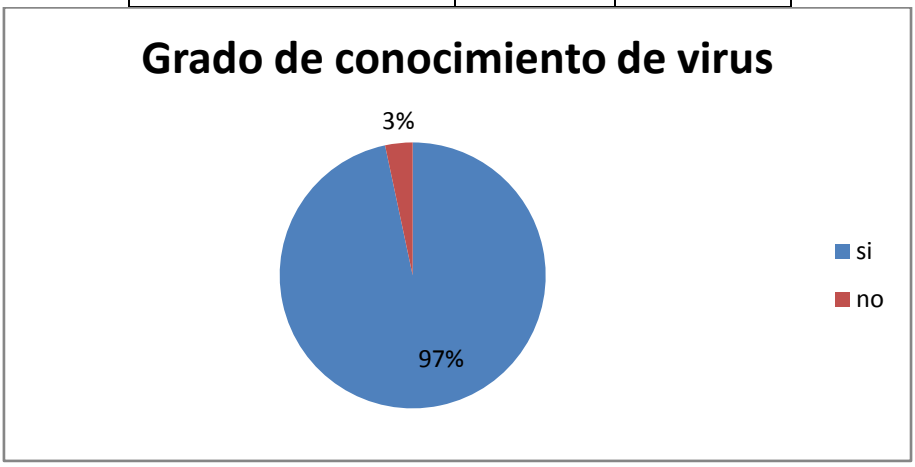


Tabla N°: 26 Tabulación estadístico de la pregunta 9
Autor: Aníbal Guachichulca

Con esta encuesta se ha demostrado que el 97% de las personas han sido víctimas de ataque de virus informáticos, considerándolas así como la principal amenaza que puede existir para el usuario de un computador y red.

10.- sabe qué tipo de virus fue

Descripción	Total	Porcentaje
Si	7	23%
No	23	77%

Total	30	100%

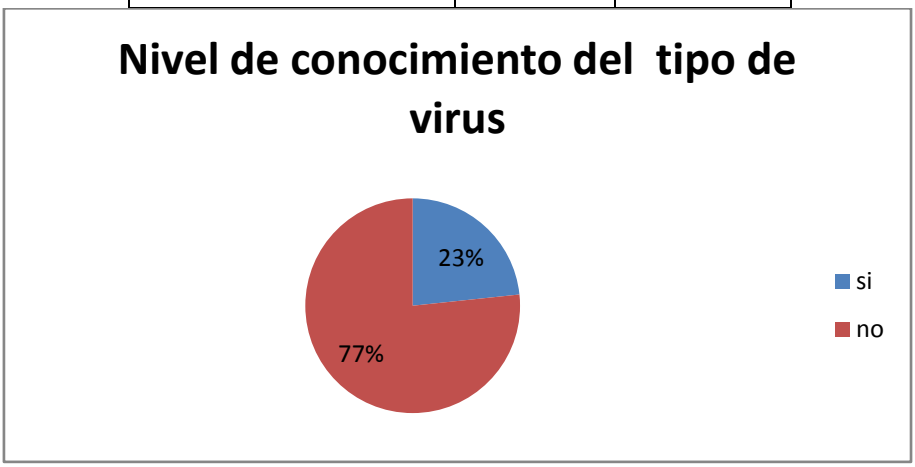


Tabla N°: 27 Tabulación estadístico de la pregunta 10
Autor: Aníbal Guachichulca

En el grafico podemos observar que el 77% de las personas desconocen el tipo de virus de los que han sido víctimas alguna vez y solo tienen conocimientos de sus efectos.

11.- que daños causa el virus informático en sus equipos o dispositivos

En esta pregunta se encontró varias causas que los usuarios ha experimentado en sus ordenadores entre ellas tenemos:

- Colgamiento del equipo
- Eliminación de información
- Se reinicia el equipo
- Se ingresa en actividades no deseadas
- Se hace lento el computador
- Dañan los archivos y programas o aplicaciones
- Daña dispositivos de almacenamiento
- Oculta la información
- Crea accesos directos

Sin duda esta es la principal amenaza para los usuarios de una PC.

12.-conoce algún tipo de método de protección para su información

Descripción	Total	Porcentaje
Si	14	47%
No	16	53%
Total	30	100%

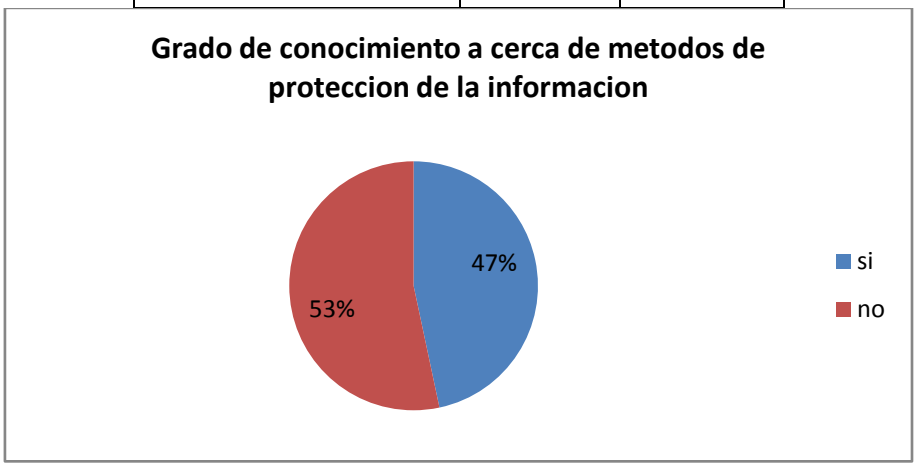


Tabla N°: 28 Tabulación estadístico de la pregunta 12
Autor: Aníbal Guachichulca

En el cuadro podemos observar que mucha de la gente usuaria de una red no conoce muy bien los métodos de protección que existen, ya que algunos que han sido atacados, en el robo de sus contraseñas son inseguros en utilizar métodos referentes a estos.

Conocimientos básicos que se encontró en las personas usuarios de un ordenador

- Tener un antivirus actualizado
- No registrase o navegar en páginas sospechosas.
- Respaldar la información

- Uso de contraseñas en el computador
- Asegurarse abandonar una cuenta

4.10.- PLAN DE SEGURIDAD

4.10.1.-SOLUCION DE ATAQUES DEL SISTEMA

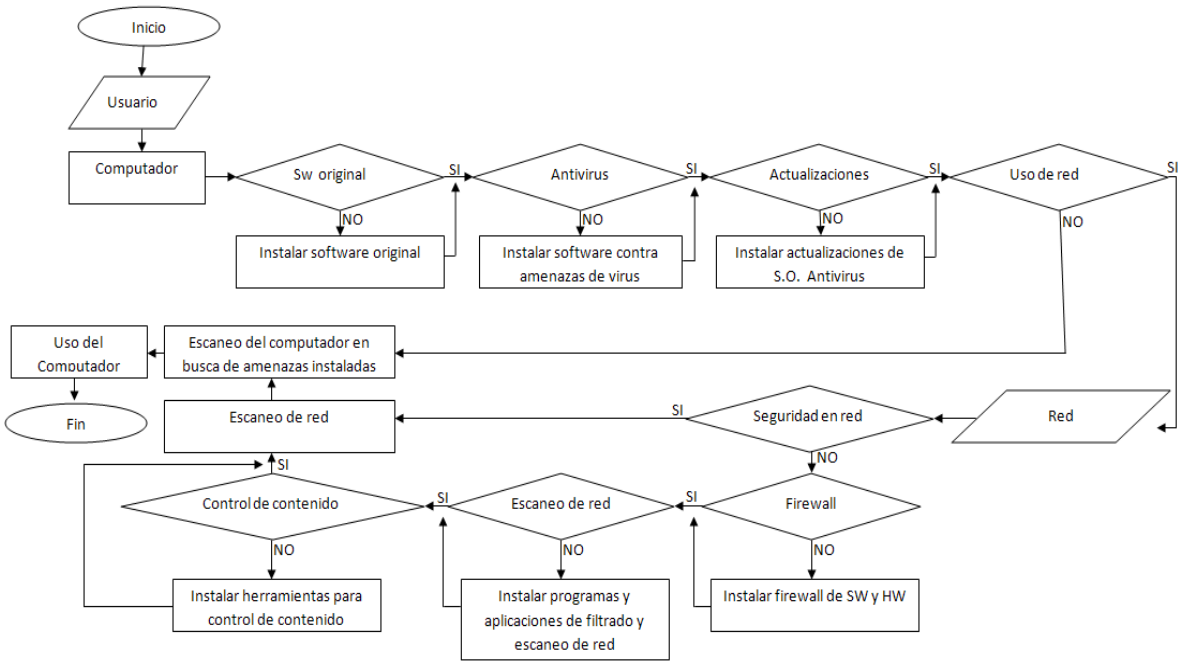


Ilustración N°: 21 Diagrama de solución de ataque informático
Autor: Aníbal Guachichulca

4.10.2.-CUADRO DE SOLUCIÓN DE LOS PROBLEMAS

- ✓ Uso de software original
  - ➢ Sistema operativo
  - ➢ Aplicaciones y programas
  - ➢ Evitar la distribución de software ilegal.
- ✓ Uso de antivirus confiable y garantizado
  - ➢ Filtrado de paquetes
  - ➢ Herramientas anti KeyLoggers
- ✓ Mantener actualizaciones de protección contra amenazas
  - ➢ Antivirus
  - ➢ Sevice pack del sistema operativo
  - ➢ firewall
- ✓ Uso de una red confiable y segura
  - ➢ Snifers de red
  - ➢ Scan de aplicaciones malignas
  - ➢ Freezado de disco duro
  - ➢ Uso de firewall de software y hardware
- ✓ Uso o navegación prudente de un equipo y red
  - ➢ No ingresar a sitios web poco confiables
  - ➢ No registrarse en páginas web sospechosas
  - ➢ No responder a email o llamadas sospechosas donde soliciten información personal
  - ➢ Borrado de cookies e historial de navegación

- No descargar software o multimedia infectado por virus
- Usar control de contenidos

✓ Uso de seguridad en contraseñas

- Combinación de caracteres
- Cambio periódico de contraseñas

✓ Configuración privada de cuentas de usuario

- Acceso restringido a cierto tipo de usuarios
- Acceso al uso restringido de aplicaciones
- Acceso al uso restringido de multimedia
- Acceso al uso restringido de recurso

4.10.3.- CASOS DE USO DEL SISTEMA

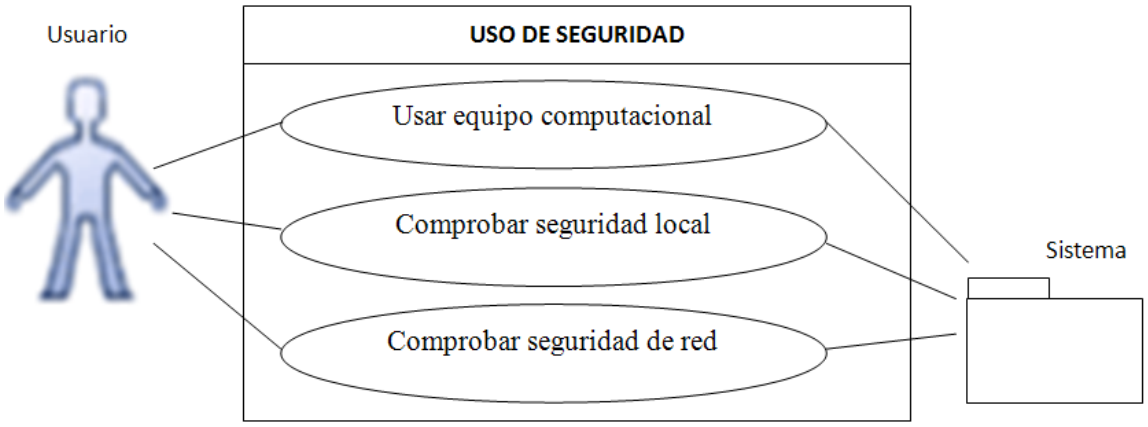


Ilustración N°: 22 Caso de uso general – Uso de seguridad
Autor: Aníbal Guachichulca

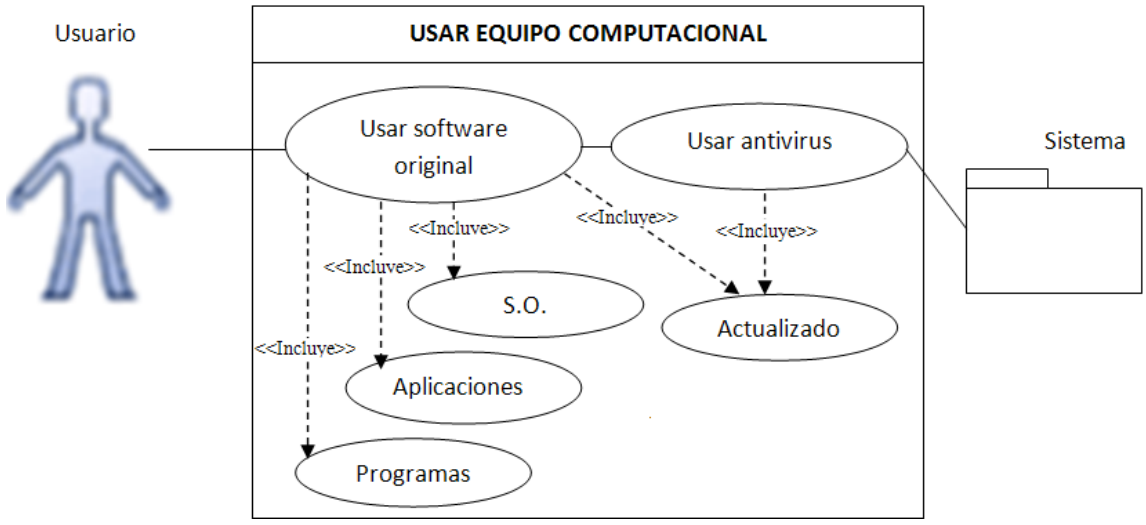


Ilustración N°: 23 Caso de uso general – Uso de seguridad
Autor: Aníbal Guachichulca

Escenario: Uso de equipo computacional (equipo)
Quien lo comienza: los usuarios de un equipo computacional o red **Quien lo finaliza:** los usuarios de un equipo computacional o red **Excepciones:** si el usuario facilite de forma confiable a una tercera persona que esta instale software malicioso **Descripción:** • El usuario necesita usar un equipo computacional • Para el mismo el usuario debe tener instalado software original (plataformas, programas, aplicaciones etc.) • El equipo debe tener instalado y activado un antivirus confiable • El equipo debe tener sus respectivas actualizaciones para mayor seguridad (firewall del S.O.) en especial la base de datos de un antivirus.

Tabla N°: 29 Escenario – Usar equipo computacional
Autor: Aníbal Guachichulca

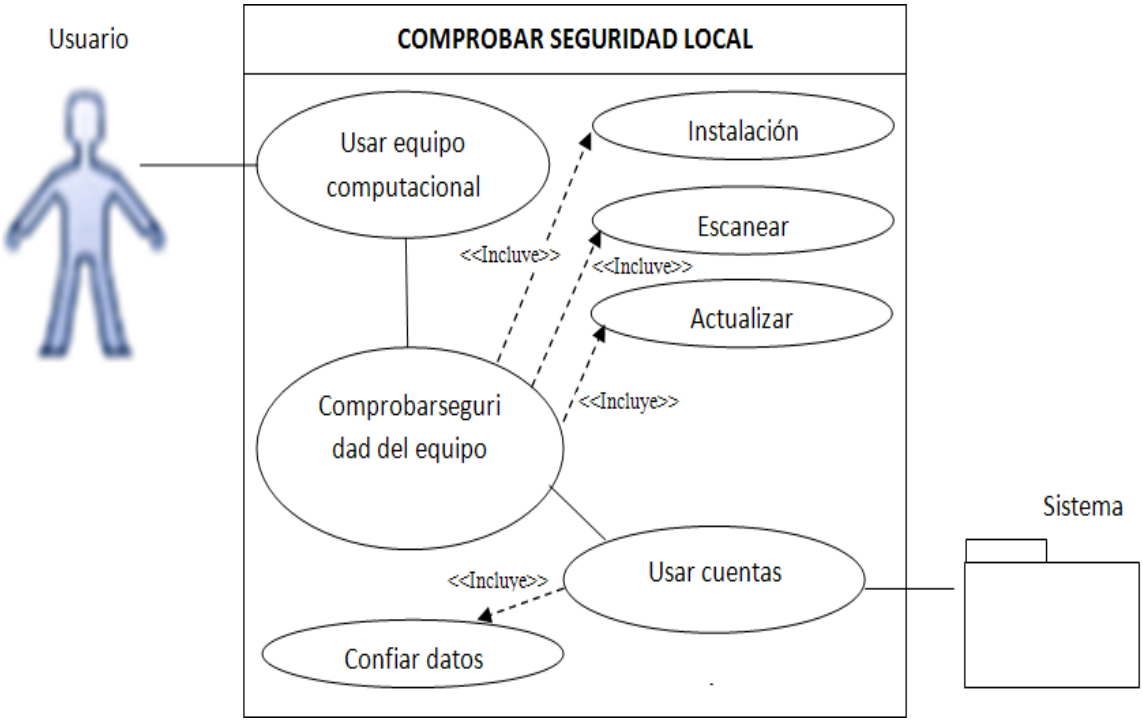


Ilustración N°: 24 Caso de uso detallado – Comprobar seguridad local
Autor: Aníbal Guachichulca

Escenario: Comprobación de seguridad local (equipo)
Quien lo comienza: los usuarios de un equipo computacional o red **Quien lo finaliza:** los usuarios de un equipo computacional o red **Excepciones:** si el usuario necesita hacer una comprobación física de seguridad correspondería a la verificación de la instalación de hardware correctamente para el uso de un equipo computacional. **Descripción:** • El usuario necesita usar un equipo computacional • Para el mismo se deberá comprobar si el equipo tiene seguridad anti programas

intrusos

- Si no existe el usuario deberá instalar herramientas para encontrar software malicioso
- Después de instalar este deberá escanear el equipo en búsqueda de software malicioso
- Actualizar la BD del programa de protección contra nuevas amenazas
- Una vez que el usuario haya realizado un chequeo
- Puede usar sus cuentas, manipular información confidencial, usar sus claves y contraseña para el uso de un sistema.
- Podrá administrar su información de forma segura
- Podrá confiar sus datos en el equipo que usa

Tabla N°: 30 Escenario – Comprobar seguridad local
Autor: Aníbal Guachichulca

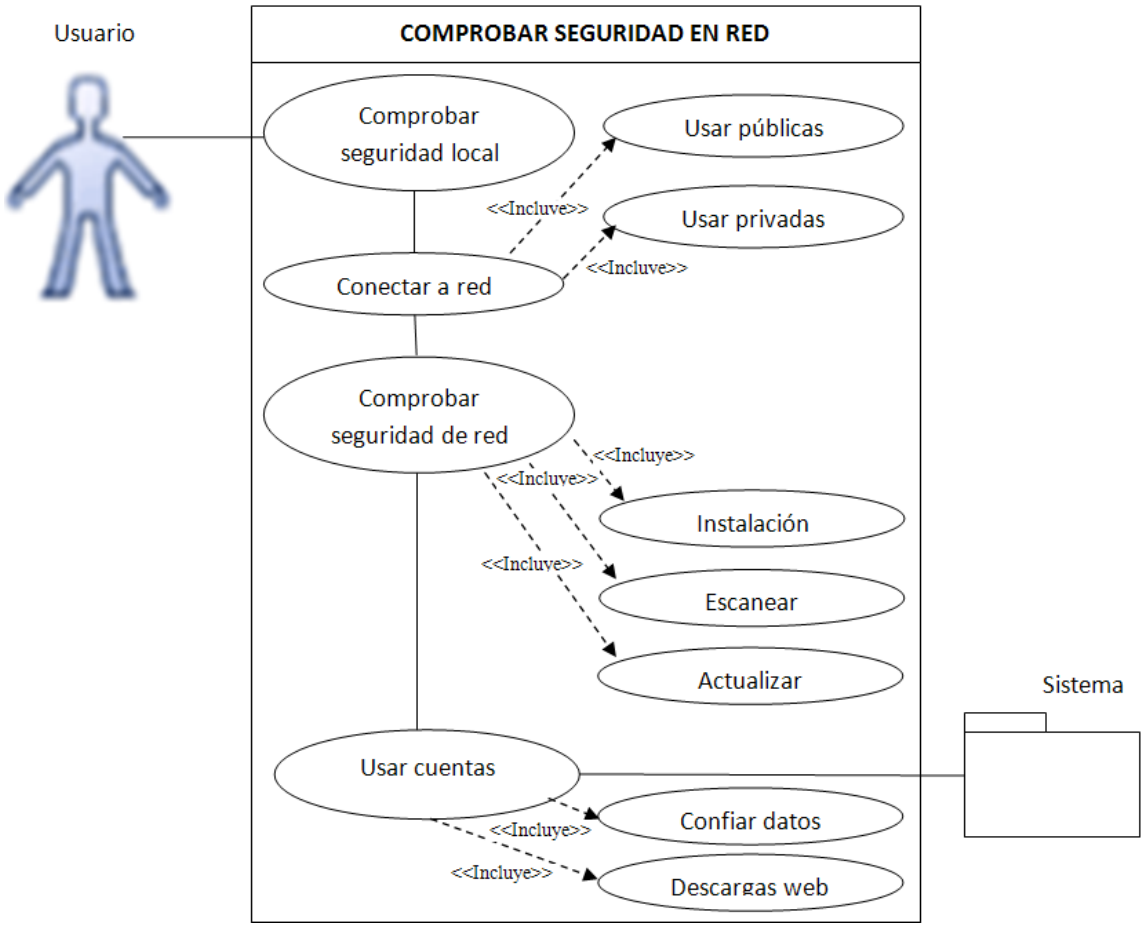


Ilustración N°: 25 Caso de uso detallado – Comprobar seguridad en red
Autor: Aníbal Guachichulca

Escenario: Comprobación de seguridad en red
Quien lo comienza: los usuarios de un equipo computacional o red **Quien lo finaliza:** los usuarios de un equipo computacional o red **Excepciones:** si el usuario necesita hacer una comprobación física de seguridad correspondería a la verificación de la instalación de hardware correctamente para el uso de red **Descripción:**

- El usuario necesita usar un equipo computacional con conexión a una red
- Comprobar si existe seguridad local
- Realizar un tipo de conexión ya sea público o privado
- Comprobar si existe seguridad en la red
- Para el mismo se deberá comprobar si el equipo tiene software anti intrusos
- Si no existe el usuario deberá instalar herramientas para encontrar software malicioso que usa la red
- Después de instalar este deberá escanear la red para su uso seguro
- Una vez que el usuario haya realizado un chequeo previo al uso
- Puede usar su conexión para el uso de sus cuentas, manipular información confidencial, usar sus claves y contraseña para el uso de un sistema.
- Podrá administrar su información de forma segura en la red
- Podrá confiar sus datos en el equipo de uso y red

Tabla N°: 31 Escenario – Comprobar seguridad en red
Autor: Aníbal Guachichulca

4.11.-PLAN DE ATAQUE DE UN INTRUSO

Se indicara como un intruso informático burla la seguridad del Cibercafé y capturar información de usuarios del servicio de internet que posee los siguientes recursos:

Recurso	**Descripción**
Computadores	Computadores Pentium 4 con procesadores desde CorelDuo en adelante

Sistema Operativo	Sistemas operativos Windows en general, pero resalta el uso de Windows XP por ser el más estable para computadores Pentium 4 clientes
Red	
Navegadores	Navegadores más utilizados como el internet Explorer, Mozila Firefox, Google Chrome.
ISP	Servidor de internet externo, institución que se dedica a la venta de ancho de banda de internet según necesidad
Servidor de internet	Servidor de internet interno, computador principal que se encarga de distribuir el internet a las demás computadoras clientes
Servidor de Control de Ciber	Software encargado de administrar las computadoras de una red y el uso de la misma.
Antivirus	Software encargado de neutralizar virus y amenazas en contra de software y hardware.
Deepfreezer	Software que se encarga de freezar un disco duro para evitar que no se guarden cambios o instalación de aplicaciones al momento de apagar o reiniciar el computador

Tabla N°: 32 Plan de ataque de un intruso informático
Autor: Aníbal Guachichulca

A continuación se indicara como los intrusos informáticos burlar al Deepfreezer para poder desactivar el antivirus e instalar herramientas de captura de información

(KeyLoggers), como también el uso del software Ciber control hack para realizar acciones de administrador de red

4.11.1.-DIAGRAMAS DE SOFTWARE PARA IRRUMPIR LA SEGURIDAD

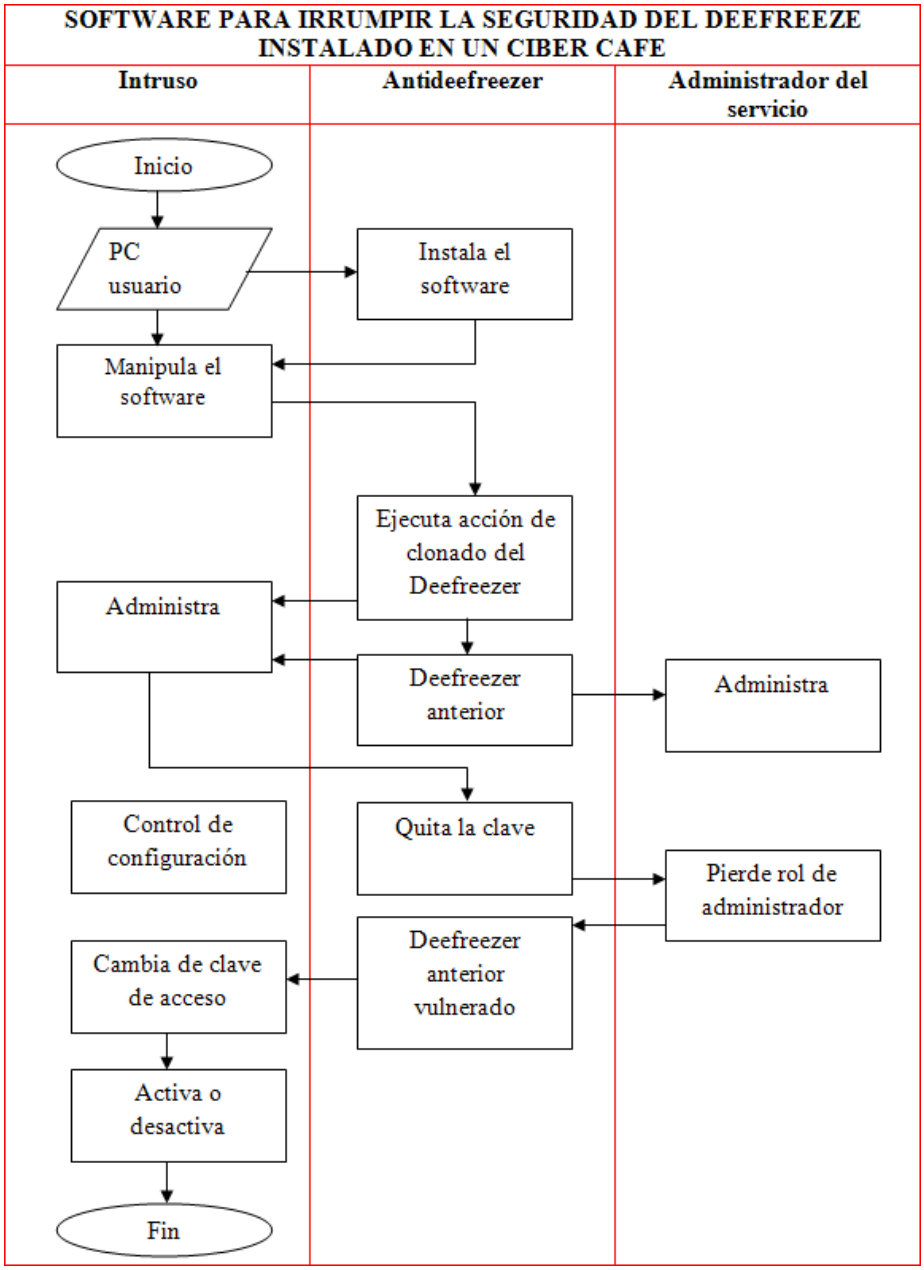


Ilustración N°: 26 Diagrama de flujo – Software para irrumpir la seguridad deepfrezer
Autor: Aníbal Guachichulca

Descripción 1:

- El intruso solicita un computador a administrador del cibercafé
- Ingresa al computador el computador
- Ejecuta la aplicación Antideepfreezer y rompe la seguridad
- La aplicación clona al Deepfreezer instalado anteriormente por el administrador del cibercafé (ver figura 01)
- El intruso abre la interfaz de la aplicación clonada con la combinación de techas (Shift + Click) dos veces
- Se presenta una interfaz donde solicita la contraseña delDeepfreezerclonado
- El intruso no ingresa ninguna clave y pulsa aceptar (ver figura 02)
- Se abre la interfaz de administración del Deepfreezer y configura para que al reiniciar el computador este descongelado (ver figura 03)
- Cambia la contraseña (ver figura 04)
- Aplica los cambios
- Reinicia el computador
- Pulsa combinación de teclas (ctrl+shift+F6) para abrir el Deepfreezer del instalado en el computador por el administrador del Ciber
- Ingresa a la interfaz como administrador con la contraseña dada posteriormente (ver figura 05)
- Verifica que el Deepfreezerestá desactivado (ver figura 06)

Tabla N°: 33 Descripción 1 de ataque en un Ciber Café
Autor: Aníbal Guachichulca

Descripción 2:
Verifica que el Deepfreezer está desactivado (ver figura 06) ✓ El intruso procede Desactivar total del antivirus de forma total (ver figura 07) • Inicio • Selecciona “ejecutar” • Escribe “msconfig” para administrar las opciones de inicio de los programas • Ingresa a la interfaz • Selecciona la opción “inicio” • Ahí desactiva el iniciador del antivirus, con solo deseleccionar del check • Aplica y guarda cambios ✓ Ingresa a la interfaz del antivirus y lo desactiva ✓ Borra archivos de escritorio que le pertenezcan ✓ Reinicia el computador

Tabla N°: 34 Descripción 2 de ataque en un Ciber Café
Autor: Aníbal Guachichulca

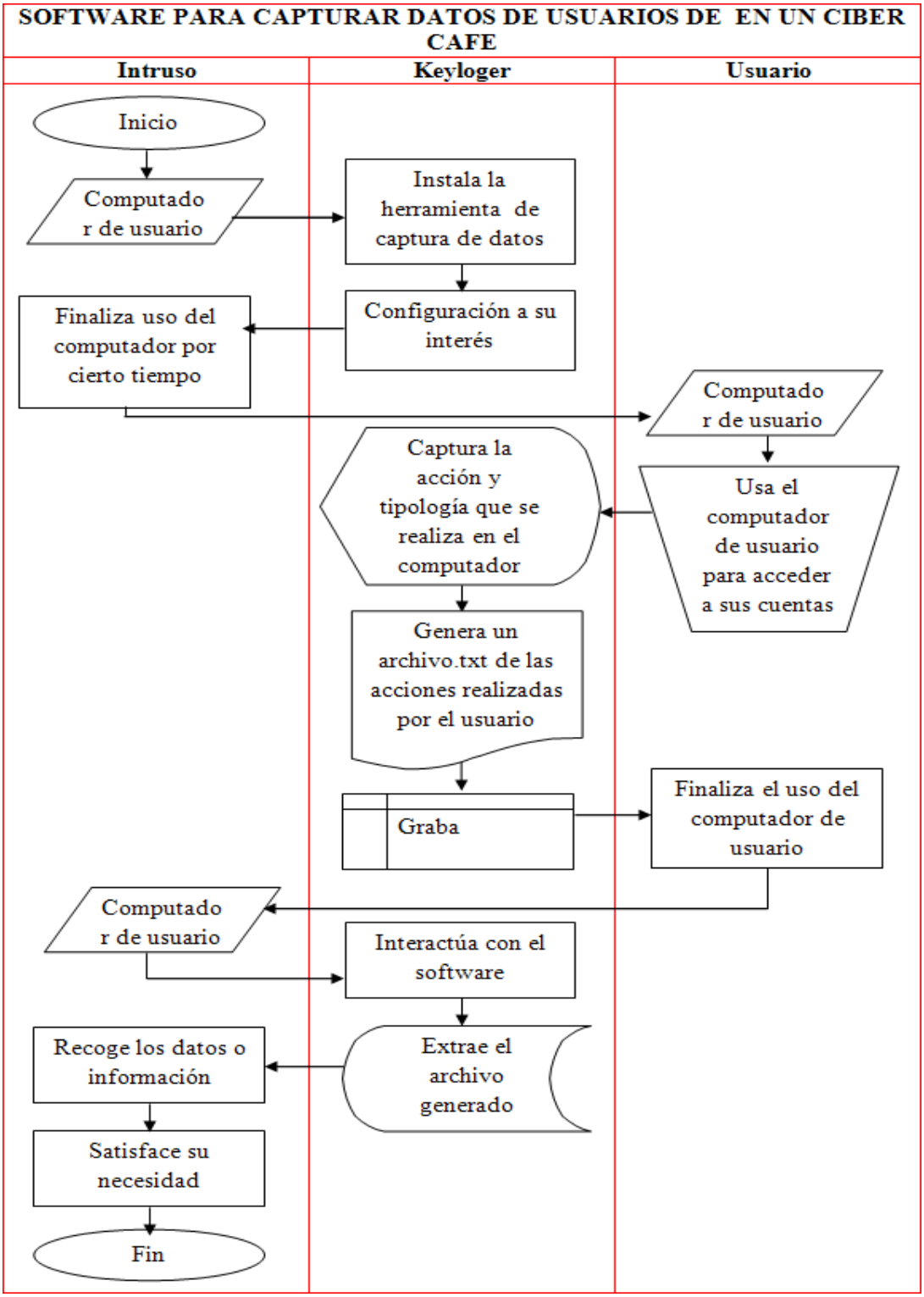


Ilustración N°: 27 Diagrama de flujo – Instalación de software para capturar datos
Autor: Aníbal Guachichulca

Descripción 3:

- El intruso ingresa y usa el computador
- Instala la aplicación de captura de información (keyLogger)
- Ejecuta la instalación
- Configura la ruta de instalación(ver figura 08)
- Finaliza la instalación
- Ejecuta la aplicación instalada(ver figura 09)
- Configura el método de captura de información e inicia la grabación oculta la carpeta que contiene los archivos instalados(ver figura 10)
- Oculta la aplicación de captura y cierra la aplicación(ver figura 11)
- Configura a los navegadores con acceso predeterminado a la red social seleccionada y limpia todo el historial(ver figura 12)
- Borra los archivos de escritorio que le comprometan, Finaliza el uso del equipo y se retira por un cierto tiempo
- Si el intruso desea podrá activar congelación del equipo durante el próximo reinicio del equipo.
- En el computador se inicia el proceso de captura de información
- Un usuario solicita un computador con acceso a internet
- El administrador del Ciber abre el controlador de Ciber asigna y sin saber el administrador le designa el equipo donde están instalados las aplicaciones de captura
- El usuario usa el computador
- Abre el navegador para su uso y digita una dirección web

- Se presenta una interfaz de acceso a cuenta
- Digita datos de acceso a su cuenta privada (login y password)(ver figura 13)
- Manipula su cuenta hasta su satisfacción
- Finaliza su sesión
- Cierra el navegador
- Solicita que cierren el uso de internet, paga y se retira
- El intruso regresa e inicia su recolección de información
- Solicita que le alquile el computador donde el instalo sus aplicaciones
- Ingresa al computador
- Ejecuta la combinación de teclas y abre la aplicación de captura de datos (keyLogger)(ver figura 14)
- Manipula la aplicación
- Genera un documento con los datos capturados (ver figura 15)
- Guarda la información en una unidad de almacenamiento extraíble
- Solicita cierre del servicio, paga y se retira

Tabla N°: 35 Descripción 3 de ataque en un Ciber Café
Autor: Aníbal Guachichulca

Descripción 4:
El intruso realiza el ataque en otro Ciber café - Solicita un computador - Accede a los sitios web de los usuarios - Usa sus datos para ingresar a las cuentas

- Ingresa a la cuenta de forma administrativa
- Manipula datos, Satisface su necesidad y Finaliza sesión

Tabla N°: 36 Descripción 4 de ataque en un Ciber Café
Autor: Aníbal G6achichulca

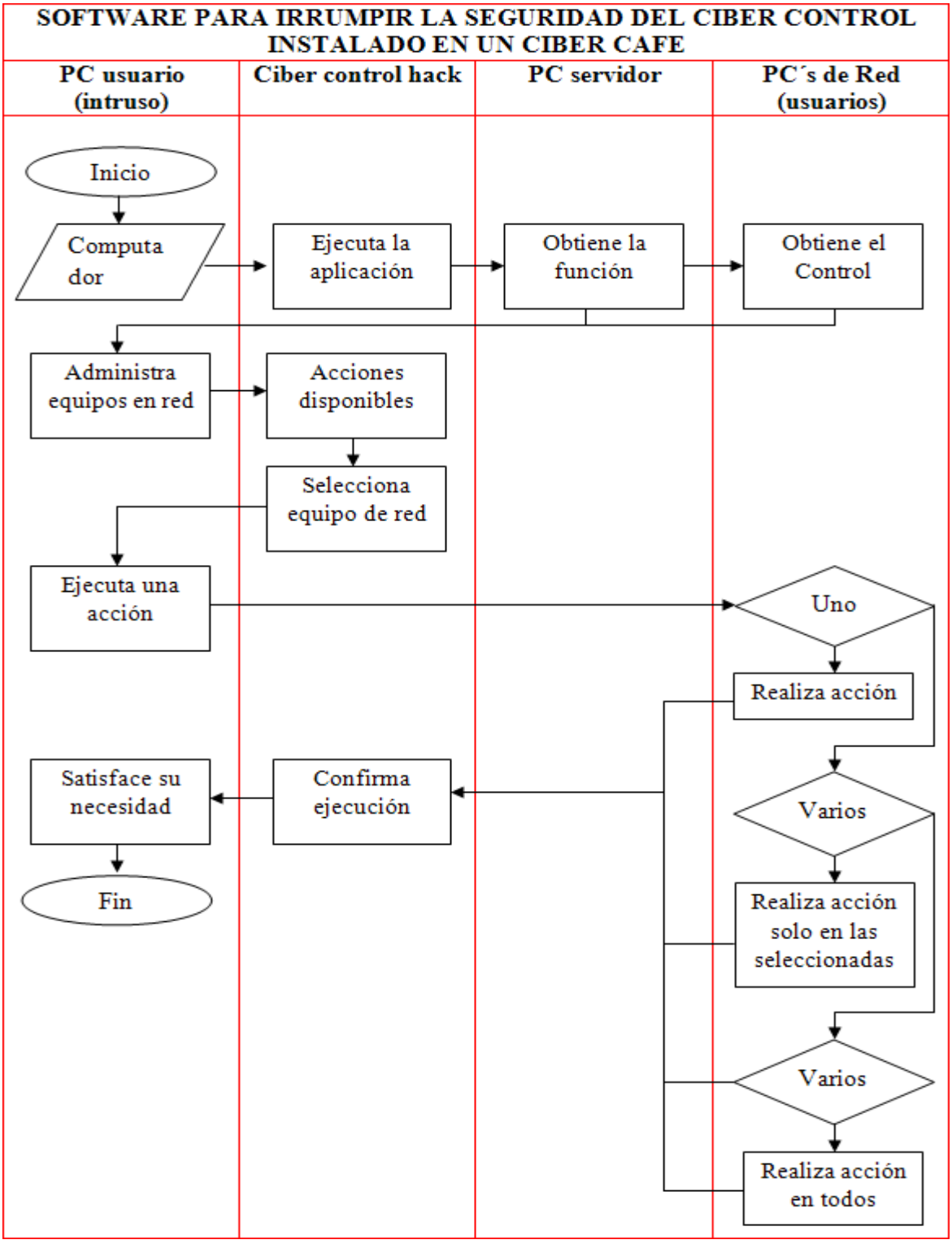


Ilustración N°: 28 Diagrama de flujo – Uso del software para control de equipos en red
Autor: Aníbal Guachichulca

Uso de Ciber control hack
Selección de una o varias IP´s para realizar acciones
Opciones de la aplicación: ➢ Acciones de apagado, reiniciado, cierre de sesión, finalización de CiberPuesto ➢ Muestra de mensaje “Poco tiempo de uso” ➢ Envió de mensajes ➢ Control de volumen de equipos ➢ Acciones de bloqueos, colgamientos y reinicios ➢ Selección de usuarios para acreditar tiempo de uso y costo ➢ Uso de VNC ➢ Interfaz de confirmación de acción realizada
Descripción: El intruso puede usar las opciones del menú de acuerdo a su criterio o necesidad(ver figura 16) ➢ Para molestar o actuar de mala fe a usuarios de la red ➢ Para que el usuario abandone el equipo y el poder solicitarlo para su uso ➢ Para su beneficio económico ➢ Para acciones en contra del servidor

Tabla N°: 37 Descripción 6 – Uso del software Control Ciber Hack
Autor: Aníbal G6achichulca

4.12.-MICRO CURRÍCULO PARA EDUCACIÓN MEDIA

<table>
<tr><td colspan="4">1. DATOS INFORMATIVOS</td></tr>
<tr><td colspan="2">COLEGIO</td><td colspan="2">TEMA DE CAPACITACIÓN</td></tr>
<tr><td colspan="2"></td><td colspan="2">AMENAZAS HUMANAS Y LÓGICAS EN CONTRA DE LA SEGURIDAD INFORMÁTICA VS LA PROTECCIÓN DE LA INFORMACIÓN</td></tr>
<tr><td colspan="2">DURACION HORAS</td><td colspan="2">DURACION DIAS</td></tr>
<tr><td colspan="2">15 HRS</td><td colspan="2">5 Días</td></tr>
<tr><td>NIVEL</td><td>SECCIÓN</td><td>HRS AL DÍA</td><td>TIEMPO RECESO</td></tr>
<tr><td>DOCENTE – ESTUDIANTE</td><td></td><td>3 HORAS</td><td>20 MINUTOS</td></tr>
<tr><td colspan="2">CAPACITADOR(A)</td><td colspan="2">EMAIL CONTACTO</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="4">2. CONCEPTUALIZACIÓN DIDÁCTICA</td></tr>
<tr><td colspan="4">En la actualidad el tema sobre los “hackers” es muy común, podemos verlo en revistas, periódicos, etc. Aunque no podemos decir que todas estas personas que entran a la red tienen buenos propósitos, tampoco podemos decir que todos son malos, existen personas buenas, malas y los que pasan desapercibidos.
El principal objetivo de este proyecto es mostrar a los lectores los posibles riesgos que</td></tr>
</table>

pueden tener al estar frente a un ordenador y como defenderse de ellos. Para conseguir esto, en este trabajo se ha estudiado las amenazas humanas, lógica y la protección de la información, reconociendo el medio en el que navegamos y donde habitan los mayores riesgos de Internet para conocer los diferentes tipos de personas con los que nos podemos topar en este submundo, Métodos de ataque, Analizar los diferentes medios y amenazas que nos rodean, y por último, Métodos de defensa, conocer las soluciones que nos ofrece Internet para defendernos de los problemas que se pueden encontrar, y así no sufrir las molestias que nos proporciona Internet.

Los ataques en la red son muy comunes hoy en día, esto lo podemos ver con la alteración de los muchos usuarios cuando llega un nuevo virus, o cuando dicen que alguien está atacando los sistemas de mensajería más comunes (MSN Messenger y yahoo Messenger) o redes sociales (Facebook, Twiter, Badoo etc.). Mucha gente está alerta de esto, y los sistemas de protección siempre tienen que estar al tanto de la situación. Existe mucha gente en la red que lo hace por ganar popularidad o solo con el objetivo de molestar al amigo, pero detrás de todo esto existen otras razones, como el libre comercio y la libre difusión de la información. La mayoría de los crackers y hackers desean la libre distribución de la información, y la eliminación del comercio en Internet, por eso apoyan a los creadores del software gratuito y se empeñan en derrochar a las grandes empresas que comercian como Microsoft, para que dejen los códigos de fuente de sus programas de forma gratuita en la red, y así pueda ser modificada para beneficio de ellos o los demás cibernautas. Como podemos ver para los sistemas que siguen la licencia libre, los virus y las aplicaciones destructivas son muy pocas, pero para los sistemas comerciales existe una gran variedad de aplicaciones dañinas, con el

fin de convencer a estas grandes compañías a distribuir sus creaciones de forma gratuita. Un ejemplo son los video juegos, ya que aproximadamente el 80% de estos se encuentran de forma gratuita en la red, esto se debe a que los crackers han hecho vulnerables los sistemas de seguridad de estas aplicaciones para que así puedan ser usados por todas las personas.

Es tradicional que en todo lo bueno exista algo malo y viceversa, por esto también estudiaremos los problemas que están presentes cada vez que nos encontramos frente a un ordenador o conectados a Internet, se intentara aclarar varias dudas sobre el funcionamiento de las herramientas y de las estrategias utilizadas para defender una maquina en este mundo tan hostil.

3. OBJETIVOS

GENERAL

- ☑ Estudiar las amenazas humanas, lógicas en contra de la seguridad informática, y la protección de la información.

ESPECÍFICOS

- ☑ Reconocer las principales amenazas humanas y lógicas que existen en la red.
- ☑ Realizar un estudio de los diferentes tipos de ataque que existen en la red.
- ☑ Identificar los diferentes tipos de virus que existen destacando los más famosos
- ☑ Analizar las amenazas informáticas estudiadas.
- ☑ participar en discusiones sobre la realidad nacional e internacional, con conceptos claros y precisos.

4. UNIDADES Y CONTENIDOS DE LA CAPACITACIÓN
SECCIÓN 1:
1. Intrusos de la red: 1.1. Monarquía Hackers. 1.2. Escoria de la red 1.3. Habitantes del submundo (ciberespacio).
SECCIÓN 2:
2. Ataques informáticos: 2.1. Tipos de ataques. 2.2. Piratería Informática. 2.3. Obtención de contraseñas (KeyLogger). 2.6. Ataque que causan daño a la red.
SECCIÓN 3:
3. Virus Informáticos: 3.1. Virus. 3.2. Tipos de virus informáticos. 3.3. Virus famosos. 3.4. Medios de trasmisión y ocultación.
SECCIÓN 4:
4. Métodos de protección Informática: 4.1. Tipos de protección. 4.2. Nuevas amenazas informáticas que aparecieron en el 2012. 4.3. Acontecimientos históricos

5.RESULTADO DEL APRENDIZAJE	
RESULTADO DEL APRENDIZAJE	RESULTADOS ESPERADOS (HABILIDADES DESTREZAS, DEBERES)
Distinción y comprensión del espectro de acción que cumplen las diferentes amenazas humanas y lógicas en contra de la seguridad informática.	Reconocer las principales amenazas existentes en una red.
Análisis de los tipos de ataques existente en la red y, participar activamente en debates y discusiones sobre la realidad, con criterios claros y precisos.	Realizar un estudio de los diferentes tipos de ataque que existen en una red, como base para una comprensión de la realidad.
Generación de espacios de reflexión sobre la situación más problemática en la informática con referencia a los virus.	Identificar los diferentes tipos de virus informáticos, su propagación, acción y su impacto en la realidad.
Desarrollo de espacios de reflexión para despertar el interés en métodos de protección Informática, para evitar ser víctimas de robos, fraudes, etc.	Analizar los principales métodos y tipos de defensa que existen para proteger la información privada.

6.RESULTADO DEL APRENDIZAJE				
RESULTADOS ESPERADOS	INSTRUMENTOS DE EVALUACIÓN	CALIFICACIÓN	FUENTE DE VERIFICACIÓN	F .AP
Reconocer las principales amenazas que existen en una red	Informe	0.5	Control de lectura del documento base	SF
	Trabajo extra	1.5	Investigación de los contenidos sugeridos por el capacitador y dispuestos en fuentes bibliográficas, diferentes páginas web, etc.	
Realizar un estudio de los diferentes tipos de ataques que existen en una red informática para una	Exposición	2	Asignación de temas dispuestos por él capacitador, en función de los diferentes grupos integrados por	SF

comprensión de la realidad.			estudiantes	
	Prueba escrita	1	Marco teórico	
Identificar los diferentes tipos de virus informáticos, su propagación, acción y su impacto en la realidad	Conexión de ideas	1	Fichas	SF
	Trabajo extra	2	Investigación de los contenidos sugeridos por el capacitador y dispuestos en fuentes bibliográficas, diferentes páginas web, etc.	
Analizar los principales métodos y tipos de defensa que existen para proteger la información privada.	Tejido de ideas	1	Cuestionario base	SF
	Prueba escrita	1	Marco teórico	
7. CRITERIOS DE EVALUACIÓN				
ACTITUDINAL	Actitudes, práctica de valores y normas, puntualidad, etc.			

(2 puntos):	
PROCEDIMENTAL (2 puntos):	Dominio de habilidades y destrezas: trabajos de investigación, participación en clases, pruebas de actuación, organizadores gráficos, representaciones creativas, debates, etc.
COGNITIVO (1 punto):	Comprensión de conceptos, aprendizaje de contenidos de tipo conceptual: pruebas en base a preguntas abiertas: ¿porqué…..?, ¿cómo…?, ¿cuándo?, etc.; cerradas: si o no; (opción múltiple) , lecciones, exposiciones, disertaciones, etc.
PROYECTO DE CIERRE DE CAPACITACION (5 Puntos):	
INVESTIGACIÓN: (1.5 puntos)	Proceso investigativo y reflexivo: Profundizar en la identificación de amenazas que existen en la red.
OBJETIVOS Y DESARROLLO: (2.5 puntos)	Capacidad de análisis: Reflexión para el uso de métodos de protección de la información en contra de sus amenazas.
SUSTENTACIÓN: (1 punto):	Exposición y material de apoyo.
EXAMEN FINAL (5 puntos):	
CRITERIO 1: EVALUACIÓN CONCEPTUAL/PROCEDIMENTAL	La metodología de evaluación que se va a utilizar se basa en tres preguntas de diferente tipo (opción múltiple, verdadero o falso, de

(3 puntos)	razonamiento, cerradas, etc.). Cada una con un grado de 3 a 5 % de dificultad
CRITERIO 2 EVALUACIÓN ACTITUDINAL (2puntos)	Se considerará para efectos de este parámetro de evaluación dos preguntas en función del pensamiento crítico del estudiante y la capacidad de análisis y de síntesis en consideración al tiempo reglamentario para la resolución de la evaluación.

8. ESTRATEGIAS METODOLOGICAS

MÉTODOS

- Observación.
- Descriptivo: Taller pedagógico inicial.
- Análisis.
- Síntesis.
- Investigación.
- Inductivo-Deductivo.

TÉCNICAS:

- Evaluación inicial o diagnóstico.
- Evaluación escrita y oral.
- Ejecución de dinámicas grupales de integración.
- Lluvia de ideas.
- Conexión de ideas.

- Tejido de ideas.
- Análisis de opiniones ajenas y emisión opiniones propias.
- Organizadores gráficos.
- Debate.
- Discusiones.
- Dramatizaciones.
- Argumento.
- Organizadores cognitivos:
    - Mente facto.
    - Mapa conceptual.
    - Mesa de la idea principal.
    - Sopa de letras.
    - Crucigramas.
    - Mándalas.
    - Pirámide.
    - Mapa de carácter.
    - Rueda de atributos.
    - Palabra clave.
    - Cadena de secuencias.

9. BIBLIOGRAFÍA

Capacitador.

FIRMA DEL ENCARGADO(A) DE LA CAPACITACIÓN	RECTOR(A) DEL COLEGIO A CAPACITAR
NOMBRE:	NOMBRE:

Tabla N°: 37 Cuadro – Micro currículo de educación media
Autor: Aníbal G6achichulca

5.- CONCLUSIONES Y RECOMENDACIONES

5.1.- CONCLUSIONES

Como pudimos ver en este proyecto, el uso de Internet y de ordenadores no es confiable, existen varios métodos para hacer la estadía en la red más desagradable, peor aun así las amenazas siguen existiendo. Otro factor importante es el económico, una gran parte de las empresas diseñadoras de software cobra por sus productos y su información. Este aspecto hace aumentar el índice de criminalidad en la red ya que muchos de los criminales pelean por “la libre información”.

todo usuario de un ordenador debemos tomar en cuenta es que todo virus informático son creaciones humanas y que su comportamiento es de acuerdo a las instrucciones que el desarrollador haya especificado, convirtiéndose así en diferente tipo de virus con diferentes daños, su modo de trasmisión se basa en programas infectados llegando al computador de varias maneras, a través de unidades de almacenamiento extraíbles, un archivo adjuntado a un correo electrónico, en un archivo bajado en Internet, por la red interna de una empresa y por esto siempre debemos tener un antivirus actualizado.

Existen muy pocas personas profesionales que realmente no toman en cuenta este tipo de amenazas que existen en la red, esto se debe a que por un lado todavía no han sido atacados y piensa que con unsimple antivirus es suficiente para darle seguridad a la red, pero realmente es necesario la capacitación sobre este tema, más aun si son empleados que administran sistemas, o trabajan dentro de la área.

En la actualidad muchas de las personas han considerado al internet como un servicio básico, al igual que el agua, la luz, el teléfono etc. Esto se debe a que muchas de las personas necesitan comunicarse o trabajar usando esta red, pero dentro de estos usuarios existen personas que no tienen conocimientos de las amenazas que la rodean a esta, y terminan siendo víctimas de fraudes, estafas, robos en la red.

El internet brinda todo tipo de información y software sea este bueno o malo, la mayoría de uso gratuito es de ahí que nacen las oportunidades de ataque, a través del uso de estos recursos por personas maliciosos, intrusos que buscan satisfacer necesidades (económicas, vengativas, por envidia, etc.)

Las nuevas amenazas ya no solo van en contra de las seguridades informáticas comunes, sino que estas han ido evolucionando de acuerdo a la tecnología que hoy en día se ha centrado en las plataformas móviles, aprovechando brechas de inseguridad con la creación de software o aplicaciones de robo, estafa y daño económico.

El estudio de este proyecto se debe tener muy en cuenta hoy en día y se debe ser puesta en conocimiento de los alumnos por parte de los profesores de computación o informática, para que así tomen conciencia del peligro que existe al usar un computador, navegar en una red pública o privada, para esto el tema estudiado ha planteado micro currículo de educación media con el cual los docentes pueden ayudarse a impartir estos conocimientos.

5.2.- RECOMENDACIONES

La Seguridad de la Información es uno de las tareas más cruciales a la que nos enfrentamos actualmente. Estamos en un ambiente dónde los recursos de información se ven amenazados por una variedad de factores.

Por esto es recomendable todos los usuarios de un equipo computacional e Internet aprendan y salgan de la ignorancia ya que esta es la principal herramienta de muchos intrusos, que se aprovechan de la ingenuidad de las personas.

La mejor prevención contra una infección de virus es nunca ejecutar un programa cuyo origen no sea legítimo o muy bien conocido, pues puede ser portador de código maligno.

Es recomendable hacer copias de seguridad periódicas del disco rígido, y tener instalado sistemas de defensa contra las amenazas informáticas, teniendo así un antivirus actualizado, un cortafuego activado etc.

BIBLIOGRAFIA

1. **Seguridad informática tomada de:**
   http://infoobera.blogspot.com/ (investigado 04/09/2012)

2. **Blog sobre las inseguridades y seguridades tomadas de:**
   http://blog.mentesinquietas.net/ (investigado 04/09/2012)

3. **Seguridad informática tomada de:**
   http://www.anerdata.com/seguridad-informatica.html (investigado 04/09/2012)

4. **Un portal de capacitación en seguridad informática gratuita tomado de:**
   http://www.doctortecno.com/noticia/portal-capacitacion-seguridad-informatica-gratuita (investigado 07/09/2012)

5. **Amenazas informáticas tomado de:**
   http://www.kaspersky.com/sp/threats (investigado 07/09/2012)

6. **Seguridad informática tomada de:**
   http://www.slideshare.net/marcelasgarcia/amenazas-informticas-presentation (investigado 07/09/2012)

7. **Amenazas informáticas más comunes tomadas de:**
   http://www.bloginformatico.com/amenazas-informaticas-mas-comunes.php (investigado 10/09/2012)

8. **Tipos de amenazas tomadas de:**
   http://www.eset-la.com/centro-amenazas/tipos-amenazas (investigado 10/09/2012)

9. **Amenazas informáticas tomado de:**
   http://www.osi.es/conoce-los-riesgos/amenazas-informaticas (investigado 13/09/2012)

10. **Virus y amenazas informáticas tomadas de:**
    http://www.commoncraft.com/video/virus-y-amenazas-inform%C3%A1ticas (investigado 13/09/2012)

11. **Spams tomado de:**
    http://www.rompecadenas.com.ar/spam.htm(investigado 16/09/2012)

12. **Mecanismos polimórficos tomado de:**
    http://www.zonavirus.com/Tecnicas/Mecanismos_Polimorficos.asp(investigado 16/09/2012)

13. **Virus informáticos tomados de:**http://www.zonavirus.com/Tecnicas/Armouring.asp(investigado 20/09/2012)

14. **Tunneling tomado de: http://deco-hack.iespana.es/deco-**.hack/manuales/Tunneling.txt(investigado 22/09/2012)

15. **Tipos de amenazas informáticas tomado de:** http://www.limoneando.com/2009/05/tipos-de-amenazas-informaticas.html (investigado 22/09/2012)

16. **Virus tomado de:**http://www.dragones.org/Biblioteca/Articulos/virus3.html(investigado 22/09/2012)

17. **Ataque informático tomado de:**http://es.wikipedia.org/wiki/Ataque_inform%C3%A1tico (investigado 22/09/2012)

18. **Software de Aplicación Administrativa Tipos de Ataques Informáticos de:** http://es.scribd.com/doc/19397003/Tipos-de-Ataques-informaticos(investigado 25/09/2012)

19. **Seguridad de la información tomada de:** http://www.segu-info.com.ar/ataques/ataques.htm (investigado 25/09/2012)

20. **Redes informáticas tomadas de:**http://www.mundointernet.es/IMG/pdf/ponencia95.pdf (investigado 26/09/2012)

21. **Aumentan amenazas informáticas en dispositivos móviles tomados de:** http://www.informador.com.mx/tecnologia/2012/426282/6/aumentan-amenazas-informaticas-en-dispositivos-moviles.htm(investigado 26/09/2012)

22. **Selección de las amenazas informáticas más llamativas de 2012 tomado de:** http://www.muycomputer.com/2012/12/28/seleccion-amenazas-informaticas-mas-llamativas-2012 (investigado 26/09/2012)

23. **Retos tecnológicos del siglo tomado de:**http://www.elfinancierocr.com/opinion/Opinion-Retos-tecnologicos-siglo_0_225577470.html(investigado 27/09/2012)

24. **El ranking de las amenazas informáticas en 2012 tomado de:**http://www.google.com.ec/search?q=amenaza+informaticas&hl=es&tbo=u&biw=1366&bih=633&source=univ&tbm=nws&sa=X&ei=8wzzUPGlOIq88ASFyYHQCA&sqi=2&ved=0CIEBEKgC (investigado 28/09/2012)

ANEXOS

Encuesta para un análisis de la Seguridad Informática

1. Ha usado algún tipo de red informática: Si ☐ No ☐ Tipo ☐

2. Tiene conocimientos de las amenazas que existen en la red: Sí ☐ No ☐

Cual(es):_____

_____

_____

3. Ha tenido algún problema de estafa o robo de datos privados en la red: Si ☐ No ☐

4. ¿Cuál cree Ud. que lo hizo?

_____

_____

5. ¿Cómo cree que lo hizo?

_____

_____

6. ¿Por qué cree que lo hizo?

_____

_____

7. Como lo considera a este problema de intrusos en la red

_____

_____

8. Como cree Ud. que podría darle mayor seguridad a sus datos o sitios web privados

_____

_____

9. Ha tenido problemas con virus informáticos: Si ☐ No ☐

10. Sabe qué tipo de virus fue: Sí ☐ No ☐ Nombre del virus ☐

11.Que daño causo el virus informáticos en su equipo o dispositivo

_____

_____

_____

12. Conoce algún tipo o método de protección para su informaciónSi ☐ No ☐

Cual(es):_____

_____

Figura N. 01

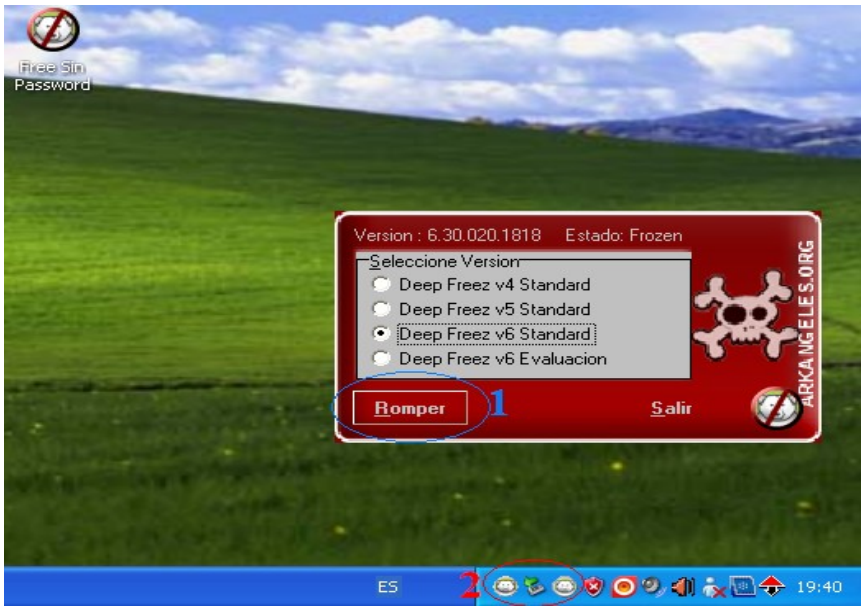


Figura N. 02

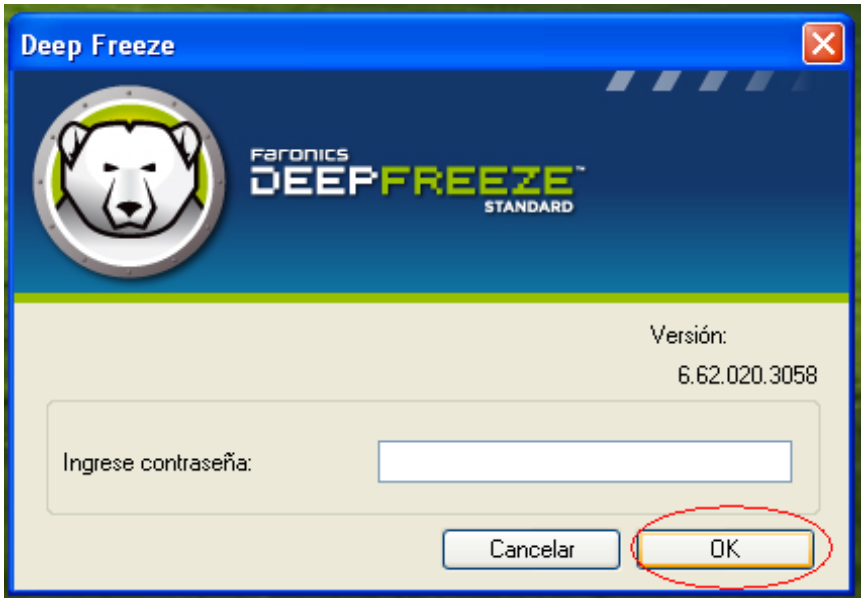


Figura N. 03

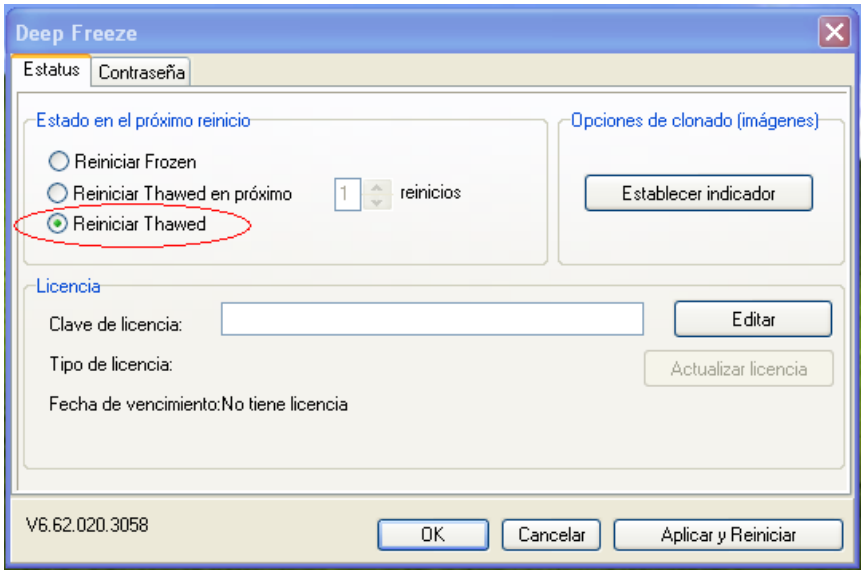


Figura N. 04

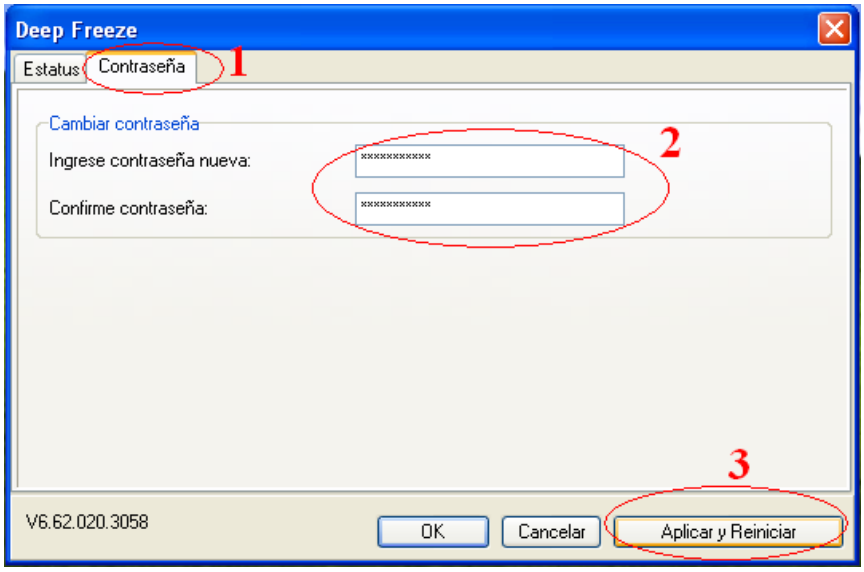


Figura N. 05

Figura N. 06

Figura N. 07

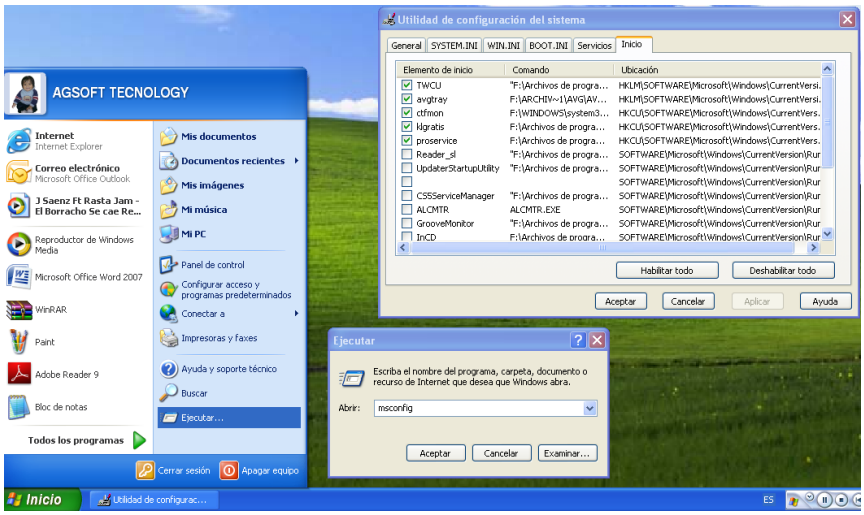


Figura N. 08

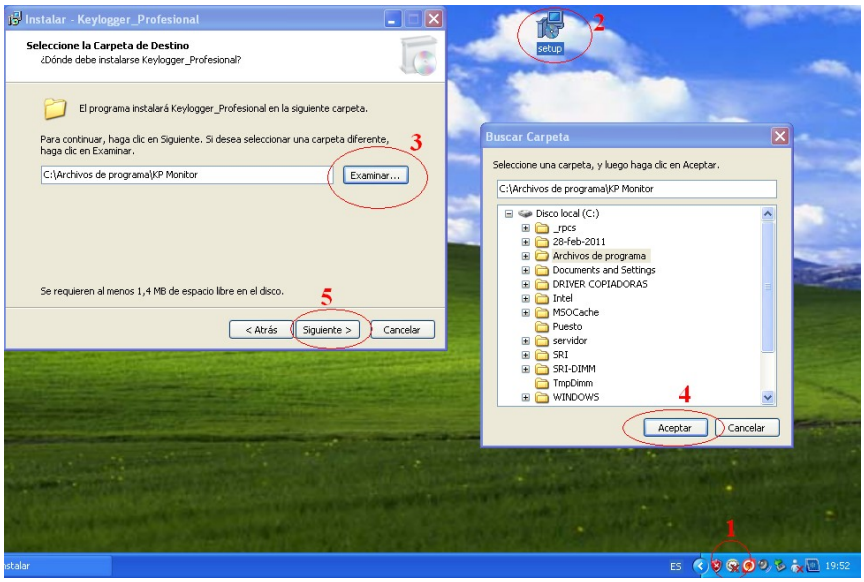


Figura N. 09

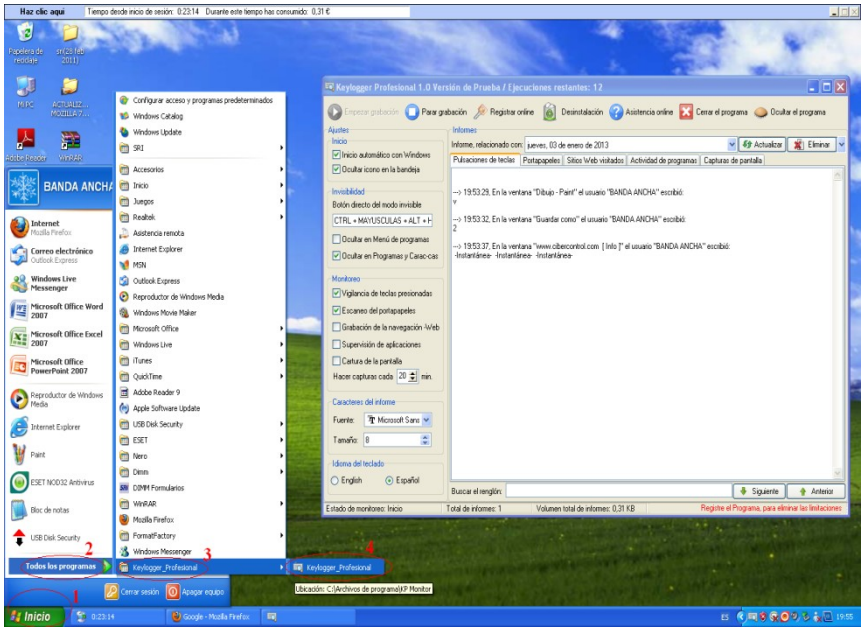


Figura N. 10

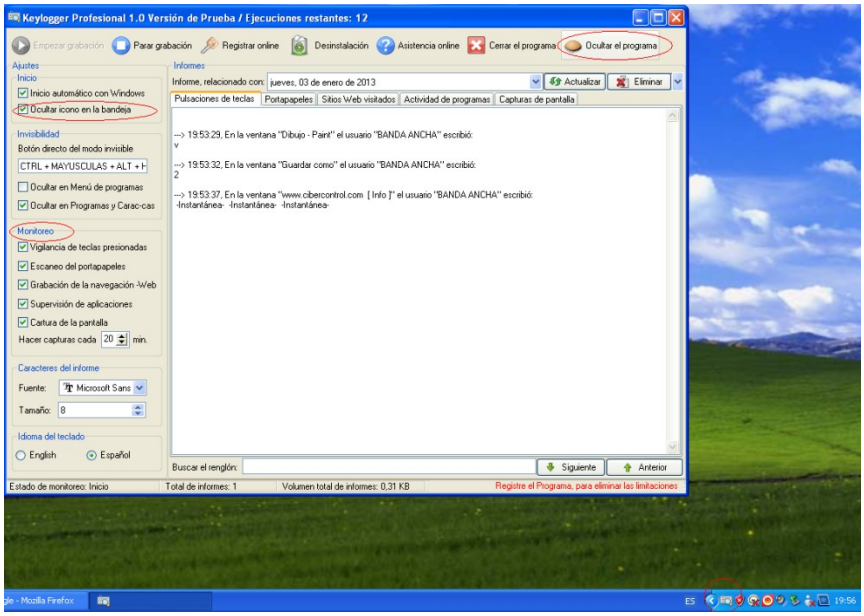


Figura N. 11

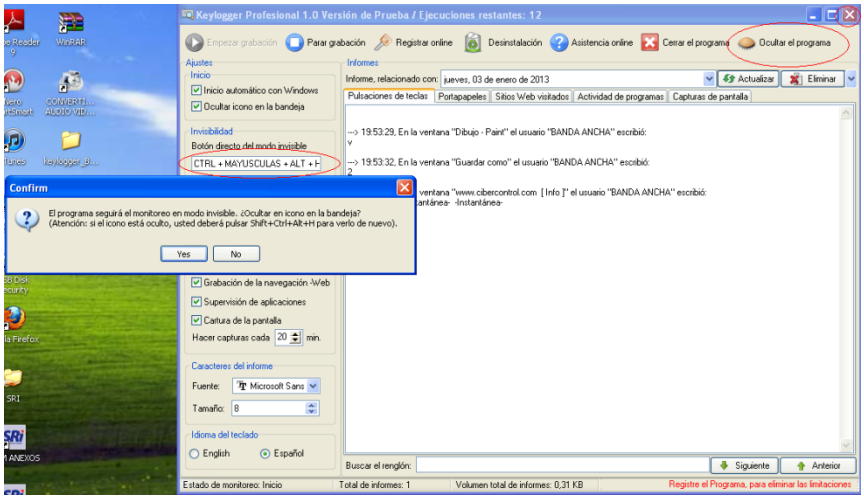


Figura N. 12

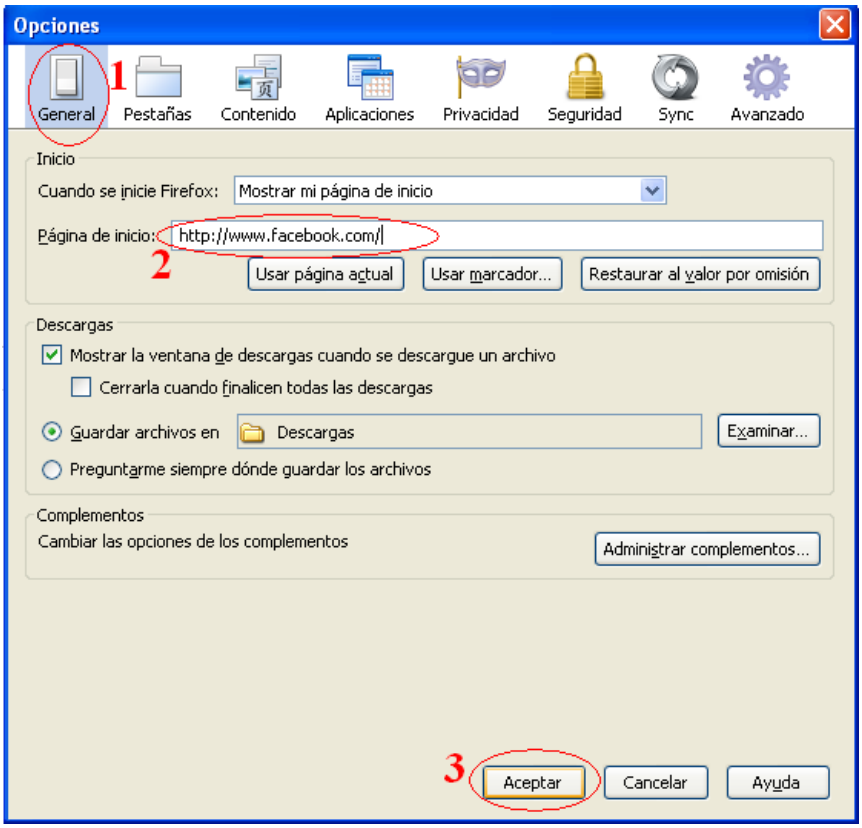


Figura N. 13

Figura N. 14

Figura N. 15

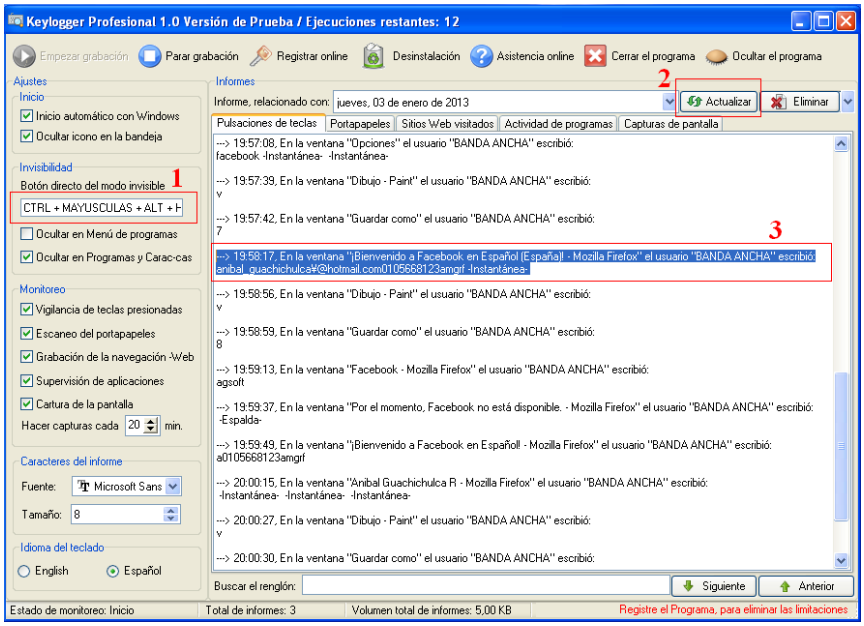
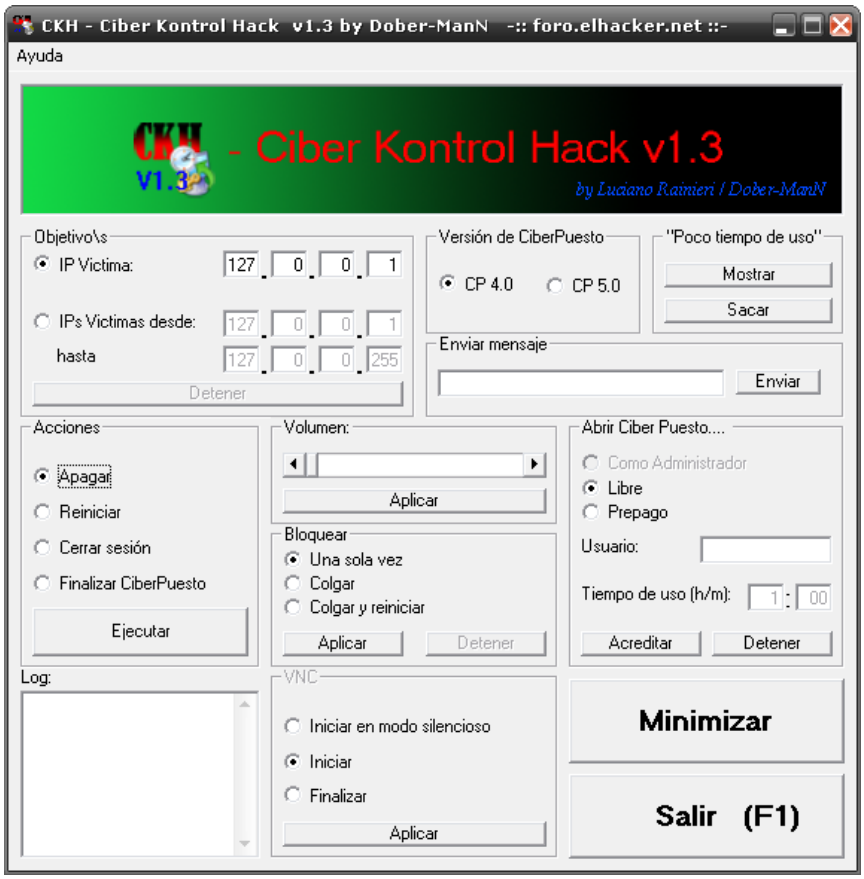


Figura N. 16


CKH - Ciber Kontrol Hack v1.3 by Dober-ManN -:: foro.elhacker.net ::-
Ayuda
- Ciber Kontrol Hack v1.3
by Luciano Rainieri / Dober-ManN
Objetivo\s
IP Victima:
IPs Victimas desde:
hasta
Detener
Versión de CiberPuesto
CP 4.0
CP 5.0
"Poco tiempo de uso"
Mostrar
Sacar
Enviar mensaje
Enviar
Acciones
Apagar
Reiniciar
Cerrar sesión
Finalizar CiberPuesto
Ejecutar
Volumen:
Aplicar
Bloquear
Una sola vez
Colgar
Colgar y reiniciar
Aplicar
Detener
Abrir Ciber Puesto....
Como Administrador
Libre
Prepago
Usuario:
Tiempo de uso (h/m):
Acreditar
Detener
Log:
VNC
Iniciar en modo silencioso
Iniciar
Finalizar
Aplicar
Minimizar
Salir (F1)

GLOSARIO

BUGS: Es un fallo en el software o en el hardware.

BACKDOOR: Puerta trasera de un software por donde se puede acceder de manera indebida

HACKING: Es la acción que realiza el hacker utilizando técnicas y herramientas informáticas para romper seguridades.

INGENIERIA SOCIAL: Es un método para obtener información por medio de persuasión

ISP: Proveedor de servicios internet.

MAQUINA: Término que se usa para hacer referencia a un computador u ordenador

BOOT: Es el sector de arranque de un disco

ROUTER: Es un tipo de hardware usado para la interconexión de redes

TCP/IP: Es un protocolo de comunicación usado en la conexión de redes

UDP: Protocolo de comunicación no es orientado a conexión.