



**UNIVERSIDAD ESTATAL DE BOLÍVAR**

**FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y  
POLÍTICAS**

**ESCUELA DE DERECHO**

**TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO DE  
LOS TRIBUNALES Y JUZGADOS DE LA REPÚBLICA, OTORGADO  
POR LA UNIVERSIDAD ESTATAL DE BOLÍVAR A TRAVÉS DE LA  
FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y  
POLÍTICAS, ESCUELA DE DERECHO**

**TEMA: EL SABOTAJE INFORMÁTICO A TRAVES DE VIRUS,  
GUSANOS, BOMBA LÓGICA Y CRONOLÓGICA Y LA NECESIDAD  
DEL ENDURECIMIENTO DE PENAS EN LA CIUDAD DE GUARANDA  
EN EL AÑO 2012.**

**AUTOR: DANIELA ALEXANDRA FLORES BARRAGAN**

**ASESOR. DRA. ANGÉLICA GAIBOR**

**Guaranda 2013**


## CERTIFICACIÓN DE AUTORÍA DE TESIS

En calidad de directora de tesis designado por disposición del Consejo Directivo de Facultad de Jurisprudencia, Escuela de Derecho se la Universidad Estatal de Bolívar. CERTIFICO: Que la Señorita: **DANIELA ALEXANDRA FLORES BARRAGÁN**, ha cumpliendo con todos los requisitos formales en la elaboración de su investigación jurídica previo a la obtención del Título de abogada en los tribunales y Juzgados de la República del Ecuador, con el tema: "**El sabotaje informático a través de virus, gusanos, bomba lógica, y la necesidad del endurecimiento de penas en la ciudad de Guaranda**".

Como director he prestado el asesoramiento requerido por la alumna, quien lo aceptado con prolijidad durante el periodo de elaboración. Además me permito certificar que el presente trabajo de investigación es auténtico y que las expresiones vertidas en la misma son de autoría del compareciente, que lo ha realizado sobre la base de recopilación bibliográfica de la legislación ecuatoriana y demás documentos, dejando a salvo los derechos de terceros sobre la bibliografía consultada y puntos de vista de los autores citados en el presente trabajo investigativo.

Por consiguiente se aprueba la impresión y presentación de este trabajo investigativo para los fines pertinentes.

Atentamente.

  
**DRA. ANGELICA GAIBOR**  
**DIRECTORA DE TESIS**

## DEDICATORIA

Dedico este trabajo a la memoria de mi distinguido padre, educador por vocación y convicción, a mi madre, mi hermana Valeria y a mi hijita Arianys, que es la razón de mi existencia.

Daniela

## **AGRADECIMIENTO**

Aprovecho la oportunidad para expresar mi sincero agradecimiento a la Noble Universidad Estatal de Bolívar; a través de ella a la Facultad de Jurisprudencia, Ciencias Sociales y Políticas, a su Escuela de Derecho, a sus catedráticos que garantizan la formación científica y humana de sus estudiantes.

Mi gratitud eterna a la distinguida maestra Dra. Angélica Gaibor, quien con su ilustrado criterio científico supo guiar este trabajo.

**DECLARACIÓN JURAMENTADA DE AUTORÍA OTORGADA POR LA SEÑORITA: DANIELA ALEXANDRA FLORES BARRAGAN.**

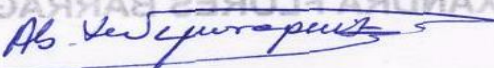
**CUANTIA: INDETERMINADA.**

2013-02-05-D00821

En San Miguel de Bolívar, República del Ecuador, hoy día martes doce de noviembre del año dos mil trece, ante mi ABOGADO WASHINGTON MORA RUIZ, Notario Segundo encargado de este Cantón, comparece la señorita **DANIELA ALEXANDRA FLORES BARRAGAN**. La compareciente manifiesta ser soltera, mayor de edad, de estado civil soltera, domiciliada en la parroquia Matriz del cantón San Miguel, provincia de Bolívar, legalmente capaz, a quien de conocerla doy fe y dice: Que instruida de la naturaleza, objeto y resultados legales de este instrumento, en forma libre y voluntaria manifiesta que tiene a bien otorgar la presente Declaración Jurada. Al efecto, juramentada que fue en legal y debida forma, previa la explicación de la gravedad del juramento, de las penas del perjurio y de la obligación que tiene de decir la verdad, expone: Yo **DANIELA ALEXANDRA FLORES BARRAGAN**, manifiesta que los criterios e ideas emitidos en el presente Trabajo de Investigación titulado "**EL SABOTAJE INFORMÁTICO A TRAVES DE VIRUS, GUSANOS, BOMBA LÓGICA Y CRONOLÓGICA Y LA NECESIDAD DEL ENDURECIMIENTO DE PENAS EN LA CIUDAD DE GUARANDA EN EL AÑO 2012**", es de mi exclusiva responsabilidad en calidad de Autora. Es todo cuanto puedo decir en honor a la verdad; y, leída que le fue esta declaración a la compareciente, se afirma y se ratifica en lo expuesto y firma conmigo en unidad de acto: de todo lo cual doy fe.

  
Daniela Alexandra Flores Barragan

C.C. No. - 020179714-9

  
Ab. Washington Mora Ruiz

NOTARIO SEGUNDO (E) DEL CANTÓN SAN MIGUEL

**Ab. Washington Mora Ruiz**  
**NOTARIO SEGUNDO**  
CANTÓN SAN MIGUEL DE BOLIVAR

**UNIVERSIDAD ESTATAL DE BOLÍVAR**  
**FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y**  
**POLÍTICAS**  
**ESCUELA DE DERECHO**

**DECLARACIÓN JURAMENTADA**  
**DE AUTENTICIDAD DE AUDITORIA**

Yo DANIELA ALEXANDRA FLORES BARRAGÁ portadora de cédula de ciudadanía N° 0201797149, mayor de edad, egresada de la Escuela de Derecho, de la Facultad de Jurisprudencia Ciencias Sociales y Políticas de la Universidad Estatal de Bolívar, con domicilio en San Miguel, Provincia de ' Bolívar, declaro en forma libre y voluntaria que la presente investigación y elaboración de la tesis así como las expresiones vertidas en la misma son de autoría de la suscrita, que lo he realizado basada en la recopilación bibliográfica de la legislación ecuatoriana, libros, gacetas judiciales, folletos, doctrina y jurisprudencia, dejando a salvo los derechos de terceros sobre la bibliografía consulta y puntos de vista de los autores citados en el presente trabajo investigativo.

Atentamente.

  
Daniela Alexandra Flores Barragán

## RESÚMEN

El presente trabajo investigativo, asume la responsabilidad de estudiar el sabotaje informático en Ecuador, considerado un delito informático propio de un comportamiento anormal en que ciertos individuos hacen uso indebido de cualquier medio informático, lo que ha propiciado en todas las legislaciones penales del mundo la regulación por parte del Derecho.

Ecuador no escapa a estos delitos en tal sentido se trabajó desde un problema de investigación en la ciudad de Guaranda escenario altamente asequible para estos tipos de delitos, el proceso de la investigación científica ha sido muy exigente en el sentido de trabajar estrictamente con las variables del problema, en cuya luz se formuló los objetivos tanto general como específicos, de lo cual se deriva la hipótesis en principio como un supuesto, pero puesta la mirada a la Reforma del Código Penal en materia de delitos informáticos solicitando el endurecimiento de las penas.

En esta lógica se direccionó el proceso de investigación a la propuesta como una alternativa de solución a la tremenda ola de delitos informáticos. La necesidad de fundamentar científicamente ésta investigación me condujo a la construcción de un marco teórico, en el que se puso a su orden mis conocimientos fácticos acerca del problema y el estudio de la comunidad científica desde los aportes de las tecnologías al servicio de la sociedad y la regulación del Derecho.

En tal sentido puedo definir desde mi propia concepción el sabotaje informático como el daño a un sistema de información.

La investigación de campo permite confirmar la existencia y evolución de los delitos informáticos en Ecuador, por lo que urge trabajar en la Reforma al Código Penal, siendo este el objetivo que me orientó a la elaboración de la propuesta.



## INTRODUCCIÓN

El aparecimiento del Internet, su importante utilidad en casi todas las actividades humanas constituye un avance al desarrollo de cualquier nación del mundo. Ecuador viene participando dentro del contexto de las nuevas tecnologías de la Información y la Comunicación. Sin embargo, una nueva forma de hacer delincuencia encontraron el modo de contaminar todo lo que se puede hacer con los sistemas de información y comunicación.

Diversas investigaciones se han realizado en los últimos tiempos, todas demuestran detalladamente los tipos de violaciones que se cometen a diario en el mundo, razón por la cual algunas legislaciones a nivel de Europa y otras naciones han tomado la decisión de construir cuerpos legales para enfrentar a los delitos informáticos. Ecuador también ha puesto interés en esta situación. En tal sentido esta investigación cuenta con importante información a través de sus cuatro capítulos.

El Capítulo I asume el estudio del problema de investigación, se demuestra a través de un conjunto de argumentos la necesidad de hacer un estudio aplicado a la realidad de la ciudad de Guaranda, escenario que no escapa a los delitos informáticos. A la luz del problema de investigación se formularon los objetivos y la hipótesis.

El Capítulo II contiene un importante marco teórico, el mismo que se constituye en la columna vertebral de este estudio por lo tanto responde al desarrollo del proceso de investigación. Brinda además información acerca de los delitos informáticos.

El Capítulo III responde a la investigación de campo aplicada en la ciudad de Guaranda, de la cual fue posible establecer las conclusiones y recomendaciones pertinentes.

Por último el Capítulo IV responde a la propuesta como una alternativa de solución al problema de investigación.

**INDICE DE CUADROS Y GRÁFICOS DE LAS ENCUESTAS APLICADAS A PERSONAS VINCULADAS CON LAS INSTITUCIONES, POLICÍAS, ABOGADOS Y PERSONAS PERJUDICADAS POR LOS DELINCUENTES INFORMÁTICOS.**

<b>CUADRO Y GRÁFICO N° 1.....</b>	<b>62</b>
<b>CUADRO Y GRÁFICO N° 2.....</b>	<b>63</b>
<b>CUADRO Y GRÁFICO N° 3.....</b>	<b>64</b>
<b>CUADRO Y GRÁFICO N° 4.....</b>	<b>65</b>
<b>CUADRO Y GRÁFICO N° 5.....</b>	<b>66</b>
<b>CUADRO Y GRÁFICO N° 6.....</b>	<b>67</b>
<b>CUADRO Y GRÁFICO N° 7.....</b>	<b>68</b>
<b>CUADRO Y GRÁFICO N° 8.....</b>	<b>69</b>
<b>CUADRO Y GRÁFICO N° 9.....</b>	<b>70</b>
<b>CUADRO Y GRÁFICO N° 10.....</b>	<b>71</b>
<b>ANEXOS N° 1.....</b>	<b>a</b>

## INDICE DE CONTENIDOS Y MATERIAS

Portada.....	I
Constancia de aprobación por parte del tutor.....	II
Dedicatoria.....	III
Agradecimiento.....	IV
Declaración juramentada.....	V
Resumen.....	VII
Introducción.....	IX

## CAPÍTULO I

EL PROBLEMA.....	1
OBJETO .....	1
CAMPO.....	1
PLANTEAMIENTO DEL PROBLEMA.....	3
FORMULACIÓN DEL PROBLEMA.....	5
JUSTIFICACIÓN.....	6
OBJETIVOS.....	7
HIPÓTESIS.....	8
OPERACIONALIZACIÓN DE VARIABLES.....	9
DISEÑO METODOLÓGICO.....	11

## CAPÍTULO II

MARCO TEÓRICO.....	15
FUNDAMENTACIÓN FILOSÓFICA.....	15
EL DELITO.....	17
TIPOS DE DELITOS.....	24
EL DELITO INFORMÁTICO.....	26
CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS.....	28
LEGISLACIONES INTERNACIONALES DEL DELITO INFORMÁTICO.....	30
EL DELITO INFORMÁTICO EN ECUADOR.....	38
USO DE TARJETAS.....	43
DELITOS INFORMÁTICOS TIPIFICADOS EN LA LEGISLACIÓN PENAL ECUATORIANA.....	44
PREJUDICIALIDAD POR FALCEDAD DE INSTRUMENTO PÚBLICO ELECTRÓNICO.....	49
PROBATORIA DEL DOCUMENTO ELECTRÓNICO.....	52
PUNIBILIDAD DE UN DELITO INFORMÁTICO.....	53
LA SEGURIDAD INFORMÁTICA COMO BIEN JURÍDICO.....	53
EL SABOTAJE INFORMÁTICO.....	54
TIPOS DE VIRUS INFORMATICOS.....	56

### **CAPÍTULO III**

<b>ANÁLISIS E INTERPRETACIÓN DE RESULTADOS.....</b>	<b>61</b>
<b>COMPROBACIÓN DE LA HIPÓTESIS.....</b>	<b>72</b>
<b>CONCLUSIONES.....</b>	<b>74</b>
<b>RECOMENDACIONES.....</b>	<b>75</b>

### **CAPÍTULO IV**

<b>PROPUESTA.....</b>	<b>76</b>
<b>TÍTULO DE LA PROPUESTA.....</b>	<b>76</b>
<b>JUSTIFICACIÓN.....</b>	<b>77</b>
<b>OBJETIVOS.....</b>	<b>78</b>
<b>DESARROLLO.....</b>	<b>79</b>
<b>PLAN OPERATIVO.....</b>	<b>88</b>
<b>BIBLIOGRAFÍA.....</b>	<b>89</b>

# CAPÍTULO I

## EL PROBLEMA

**OBJETO:** El sabotaje informático a través de virus, gusanos y bombas lógicas.

**CAMPO:** En vista de estas circunstancias, surge el Derecho Informático como una rama del Derecho que permite otorgar las soluciones jurídicas adecuadas a los problemas originados por el uso de las tecnologías, en las diversas actividades del ser humano.

El Derecho Informático cumple un rol muy importante en la prevención de problemas y en la solución de los mismos, generados por el uso de medios electrónicos. También facilita la incorporación de nuevas instituciones jurídicas que permitan crear confianza a quienes son usuarios de los medios electrónicos.

Las disfunciones o problemas documentales en el campo jurídico se presentan hoy como un obstáculo para que el Derecho pueda cumplir la función que le es propia por lo que debe ser tratado por la ciencia jurídica.

El campo del Derecho es extenso y complejo, y hoy más que antes la cantidad de la información que produce diariamente es prácticamente

incontrolable. La toma de una decisión jurídica, sea que ésta se exprese como norma jurídica, sentencia judicial, informe en derecho, investigación jurídica, respuesta a una consulta legal, requiere largas horas de recopilación de información utilizando herramientas informáticas adecuadas, sin las cuales carecerá de validez y eficacia.

Es por esto que el acceso a la información no puede verse sólo como un problema cuantitativo, sino que debe ser analizado como un problema cualitativo en cuanto puede significar la negación del sistema jurídico al no dar eficacia a principios jurídicos básicos reconocidos en nuestro ordenamiento.

### **Causas**

- La falta de penalización ejemplarizadora para quienes cometen delitos informáticos.
- Falta responsabilidad en las instituciones financieras.
- Necesidad de articular una legislación específica para los delitos informáticos.
- Demasiada ingenuidad de las personas al permitir llegar al acceso de información a otras personas.



## **PLANTEAMIENTO DEL PROBLEMA**

La seguridad informática toma mayor interés cada día, en el mundo y especialmente en Ecuador. El crecimiento indiscriminado de los delitos informáticos pone en riesgo la integridad, la confidencialidad y disponibilidad de la información. El desarrollo acelerado de la tecnología y la falta de controles especiales permite el desarrollo de los delitos informáticos.

Estos delitos se encuentran en constante crecimiento creando serios problemas a las empresas que utilizan importantes sistemas de información y redes de comunicación por Intranet e Internet, entre los delitos informáticos conocidos como acciones antijurídicas se los identifica sabotaje informático, fraude informático, estafas electrónicas o phishing, espionaje informático o sniffing, Infracción a los derechos de autor, infracción del copyright en base de datos, Uso ilegítimo de sistemas informáticos, accesos no autorizados, Interceptación de e-mail, falsificación informática, pornografía infantil, entre otros tipos de delitos.

Los países han sentido la necesidad de sancionar estas conductas ilícitas a través de legislaciones que penalizan los delitos informáticos. Ecuador dispone de una Ley de Comercio electrónico, firmas electicas y mensajes de datos nº 2002-67. Pese a que la Ley de Comercio Electrónico recoge algunas disposiciones sobre el manejo de información electrónica, en el Ecuador los delitos informáticos no están tipificados ni sancionados en el Código Penal, según indicó Santiago Acurio, director de tecnologías de la información de la Fiscalía.

Explicó que en casos de interceptación de datos existe la opción de recurrir a preceptos constitucionales que rechazan la violación al derecho de la intimidad de la persona, incluida la correspondencia virtual.

Acurio indicó que en dos ocasiones la Fiscalía ha enviado un proyecto de ley a la Asamblea para que se tipifiquen estos delitos, pero no se ha dado el trámite respectivo. Señaló que en el Ecuador hace falta una política criminal articulada en cuanto al uso de tecnologías.

Esto debido a que en el país –aseguró– son cada vez más comunes los fraudes informáticos, suplantación de identidad por internet o por teléfono, y los ‘troyanos bancarios’ que se instalan en diferentes aparatos simulando ser otro tipo de programas para obtener información de entidades financieras.

Acurio precisó que aunque existen herramientas que permiten identificar a los autores de estos delitos, mientras no haya sanciones fuertes al respecto, las diferentes gestiones que se realicen difícilmente darán resultado.

Dentro de este contexto se encuentra la ciudad de Guaranda, donde varias instituciones y personas particulares, han sufrido una serie de violaciones en los programas informáticos, procesamiento de datos, destrucción o modificación de datos, a través de virus, gusanos y Bomba lógica o cronológica. La ausencia o incompletas leyes junto a la ausencia de uniformidad legal entre estados, hace que continúen cometiendo el delito sin penalidades o con muy bajas sanciones.

## **FORMULACIÓN DEL PROBLEMA**

**¿DE QUÉ MANERA SE PUEDE CONTROLAR EL SABOTAJE INFORMÁTICO, Y OTRAS CONDUCTAS QUE PONEN EN PELIGRO O LESIONAN LA INTEGRIDAD, CONFIDENCIALIDAD Y/O DISPONIBILIDAD DE LOS DATOS Y SISTEMAS INFORMÁTICOS, QUE LESIONAN LOS BIENES JURÍDICOS DE LAS PEQUEÑAS EMPRESAS E INSTITUCIONES EN LA CIUDAD DE GUARANDA EN EL PRESENTE AÑO 2012?**

## JUSTIFICACIÓN

La presente investigación justifica su realización considerando que es un tema de interés mundial, a nivel de Latinoamérica algunos países cuentan con una regulación legislativa que tipifica los delitos informáticos. En otros países en cambio han procedido a la Reforma de los Códigos de Procedimiento Penal, para aplicar sanciones a los delitos informáticos como: extorción, robo, fraude, suplantación de identidad, etc.

En el caso de Ecuador el delito informático se desarrolla aceleradamente, lo que ha motivado a trabajar en la Expedición del Código Penal Integral Ecuatoriano. En tales consideraciones esta investigación contiene importantes argumentos científicos y legales que sirven para establecer dicha reforma penal, endureciendo las penas. En Ecuador las cifras de delitos informáticos son inciertas, las escasas denuncias son una realidad, es posible que algunas personas víctimas no se den cuenta o les falta conocimiento para denunciar.

De esta manera este estudio asume importancia e interés social, las personas interesadas en investigar este tipo de problemas, pueden encontrar algunas orientaciones científicas y legales, desde la originalidad de los datos investigados en un contexto en el que es frecuente el cometimiento de los delitos informáticos, en tal sentido es pertinente trabajar en la precisión de un marco legal que contemple los delitos informáticos en un tratamiento integral. Para este estudio dispongo de los recursos necesarios, las colaboraciones pertinentes, el tiempo disponible y sobre todo la voluntad científica para aportar con un granito de arena a las ciencias del Derecho.

## **OBJETIVOS**

### **OBJETIVO GENERAL**

Establecer penalidades ejemplarizadoras para sancionar las conductas ilícitas a quienes cometen delitos informáticos.

### **OBJETIVOS ESPECÍFICOS**

- Realizar un diagnóstico que permita evidenciar el cometimiento de delitos informáticos en las instituciones y personas de la ciudad de Guaranda.
- Determinar el tipo de delitos informáticos que se cometen con mayor frecuencia en la ciudad de Guaranda.
- Desarrollar una propuesta innovadora que permita establecer sanciones ejemplarizadoras en el Código Penal Ecuatoriano, a quienes cometen delitos informáticos.

## **HIPÓTESIS**

La Expedición al Código Penal Integral Ecuatoriano en materia de delitos informáticos, permitirá establecer sanciones ejemplarizadoras a quienes violen el derecho a la intimidad personal familiar y el fraude a través de medios electrónicos.

## **VARIABLES**

### **VARIABLE INDEPENDIENTE**

Delitos informáticos

### **VARIABLE DEPENDIENTE**

Intimidad personal familiar y fraude a través de medios electrónicos.

## OPERACIONALIZACIÓN DE VARIABLES

Variables	Definición	Dimensión	Indicadores	Escalas o Items
Delitos informáticos	Son aquellos fraudes cometidos mediante manipulación de computadoras usando las TIC u otra tecnología.	Fraudes y manipulación de:	<p>Fraudes cometidos mediante manipulación de computadoras.</p> <p>Manipulación de los datos de entrada.</p> <p>Daños o modificaciones de programas o datos computarizados.</p>	<p>¿Conoce si en Ecuador existen delitos informáticos?</p> <p>SI ( ) NO ( )</p>
Intimidación personal familiar y fraude a través de medios electrónicos.	La intimidación es una necesidad humana y un derecho natural del hombre por lo que es independiente y anterior a su regulación positiva.	Necesidad y derecho natural.	<p>Acciones privadas.</p> <p>Respeto a la libertad de las personas.</p> <p>La intimidación tiene un valor absoluto, incuestionable e inviolable.</p> <p>Fuera del ámbito del</p>	<p>¿En Ecuador se viola la intimidación personal?</p> <p>SI ( ) NO ( )</p>

<p>Fraude electrónico.</p>	<p>Se trata del engaño a los consumidores y hacerles que revelen información personal y financiera a través de internet.</p>	<p>Mensajes de correo electrónico.</p>	<p>interés público.</p> <p>Derecho extrapatrimonial.</p> <p>Derecho imprescriptible e inembargable.</p> <p>Fraude por ingreso de datos falsos.</p> <p>Sabotaje informático.</p> <p>Virus informáticos.</p>	<p>¿Es posible que se cometan fraudes por Internet?</p>
----------------------------	--	--	--	---



## **DISEÑO METODOLÓGICO**

### **TIPO DE INVESTIGACIÓN**

Esta investigación se aplicó en la ciudad de Guaranda, las características de este estudio, permiten trabajar con la investigación de campo y la investigación descriptiva, Lo descriptivo se expresa a través de la exposición del problema planteado, lo cual me permitió tener un mejor concepto en el que se puso en juego mis apreciaciones fácticas frente a las opiniones de la comunidad científica mundial.

### **TÉCNICA E INSTRUMENTOS**

Para este estudio se utilizó la encuesta, la misma que permitió elaborar un cuestionario fácil para el encuestado. En la aplicación de los instrumentos de recolección de la información se estableció una relación entre encuestado y encuestador de dicha actividad fue posible obtener importante información complementaria, que lógicamente sirvió para fundamentar de mejor manera la elaboración de las conclusiones generales de este trabajo investigativo.

### **MÉTODOS**

Los métodos seleccionados para este estudio son los siguientes:

**Método Inductivo y Deductivo:** Estos métodos permitieron estudiar el problema planteado, desde su estado general a cada una de las partes que lo componen. Es decir fue posible estudiar en los dos sentidos las causas y efectos de los delitos informáticos.

**Método Histórico Lógico:** Este método viabilizó el estudio evolutivo histórico del problema planteado, es decir desde cuando se detectaron los delitos informáticos en Ecuador.

**Método Bibliográfico:** Este método permitió seleccionar importante bibliografía científica y legal, en cuya luz se construyó el marco teórico, siendo posible establecer un criterio propio y bien fundamentado.

## **POBLACIÓN**

Totalidad de la investigación que va a ser investigada es:

En este tema de investigación se trabajó con un universo de 720 personas en el sector público; como abogados en libre ejercicio profesional y personas perjudicadas por los delitos informáticos. A continuación se detalla la fórmula aplicada para obtener las muestras respectivas.

<b>COMPOSICIÓN</b>	<b>CANTIDAD</b>
Servidores públicos del cantón Guaranda.	300
Profesionales del Derecho del Colegio de Abogados de Bolívar.	400
Personas afectadas.	20
Total	720

## MUESTRA

Para el estrato de los servidores públicos del cantón Guaranda, se aplicará la siguiente fórmula para obtener la muestra respectiva:

$$n = \frac{N}{(E)^2 (N - 1) + 1}$$

n = Tamaño de la muestra

N = Tamaño de la población

E= Error máximo Admisible al cuadrado 0.2

## ESTRATO 1

Servidores públicos del cantón Guaranda.

$$n = \frac{N}{(E)^2 (N-1) + 1}$$

$$n = \frac{300}{(0.2)^2 (300-1) + 1}$$

$$n = \frac{300}{(0.04) (299) + 1}$$

12.96

## ESTRATO 2

Abogados en libre ejercicio profesional en el cantón Guaranda.

$$n = \frac{N}{(E)^2 (N-1) + 1}$$

$$n = \frac{400}{(0.02) (400-1) + 1}$$

$$n = \frac{400}{(0.04) (399) + 1}$$

$$n = \frac{400}{16,96}$$

$$n = 24$$

Una vez aplicada la fórmula en los estratos se obtuvo la siguiente muestra:

COMPOSICIÓN	CANTIDAD
Servidores públicos del cantón Guaranda.	23
Profesionales del Derecho del Colegio de Abogados de Bolívar.	24
Personas perjudicadas por delitos informáticos.	20
TOTAL	67

**Tratamiento estadístico de la información:** En cuanto al estudio estadístico se acudió a la estadística descriptiva, representada por cuadros de frecuencias, gráficos y lógicamente sus respectivos análisis e interpretaciones de resultados.

## **CAPÍTULO II**

### **MARCO TEÓRICO**

#### **FUNDAMENTACIÓN FILOSÓFICA**

La presente investigación se fundamenta filosóficamente en los Derechos Humanos, en la relación del tema de los delitos informáticos con el derecho a la intimidad, el delito informático, se considera como los actos dirigidos a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos, así como el abuso de dichos sistemas, redes y datos.

En esta lógica encuentra fundamento en el Tratado sobre Delito Informático del año 2000, el mismo que incorporó una gama de técnicas de vigilancia de las agencias encargadas de la aplicación de la ley. Dicho Tratado exigió trabajar en los siguientes puntos:

Título 1- Delitos contra la confidencialidad, integridad y disponibilidad, de los datos y sistemas informáticos.

Título 2- Delitos relacionados con las computadoras con el contenido (Falsificación y fraude).

Título 3- Delitos relacionados con el contenido (pornografía).

Título 4- Delitos relacionados con el derecho de autor y los derechos asociados.

Título 5- Responsabilidades secundarias y sanciones, (cooperación delictiva, responsabilidad empresarial).

Los nuevos sistemas de información y comunicación benefician a la sociedad, pero también desde el abuso de sus herramientas necesita la presencia del Derecho, naciendo así la necesidad de trabajar con el Derecho Informático, cuyo objetivo principal es lograr la regulación del universo informático; estudia la doctrina y jurisprudencia que se origine como consecuencia del uso de la informática.

El Consejo de Europa y el XV Congreso Internacional de Derecho señalaron como delitos informáticos a los siguientes:

1. Fraude en el campo de la informática.
2. Falsificación en materia informática.
3. Sabotaje informático y daños a datos computarizados o programas informáticos.
4. Acceso no autorizado a sistemas informáticos.
5. Intercepción sin autorización.
6. Reproducción no autorizada de un programa informático no autorizado.
7. Espionaje Informático.
8. Uso no autorizado de una computadora.
9. Tráfico de claves informáticas obtenidas por medio ilícito.
10. Distribución de virus o programas delictivos.

Por otra parte este trabajo se fundamenta en la Constitución de la República del Ecuador, el Código Penal, Código de Procedimiento Penal, Ley de Comercio Electrónico, firmas electrónicas y mensaje de datos.

La Tutela Constitucional del bien jurídico denominado intimidad en el Derecho Comparado. Los delitos informáticos, tipificados en el Código Penal, pueden denunciarse bien a través del propio ofendido, o por intervención de la Fiscalía. Ley Orgánica de Transparencia y Acceso a la Información Pública, Ley de Propiedad Intelectual, Ley Especial de Telecomunicaciones.

Con la finalidad de estudiar responsablemente el tema de los delitos informáticos en Ecuador, a continuación se presenta un importante aporte científico, cuyas categorías indican la gravedad de estos delitos y su tratamiento jurídico. Ley de Control Constitucional (Reglamento Habeas Data).

## **EL DELITO**

Cuando se trata de establecer una definición del delito, necesariamente esta palabra se relaciona con el comportamiento humano, el delito por tanto es el cometimiento de una acción que puede producirse por propia voluntad o por imprudencia. Lo cierto es que resulta contrario a la Ley. El delito por tanto conduce a la violación de las normas, lo que establece la aplicación del castigo o pena.

En latín delito, es "delictum" palabra que sugiere un hecho contra la ley, un acto doloso que se castiga con una pena. A este respecto la Escuela Técnico Jurídica sostiene que "el delito es una acción típicamente antijurídica y culpable castigada por la Ley con una pena"<sup>1</sup>.

---

<sup>1</sup> Escuela Técnico Jurídica. El Delito.

A lo largo de la historia los pensadores y juristas han aportado importantes definiciones. En tal sentido es prudente acudir a la Real Academia de la Lengua, esta institución define el vocablo delito, como la “acción u omisión voluntaria castigada por la ley con pena grave”<sup>2</sup>.

Jiménez de Asúa considera que delito es: "El acto típico antijurídico, imputable, culpable, sancionado con una pena y conforme a las condiciones objetivas de publicidad"<sup>3</sup>.

Cabanellas por su parte, explica: “La palabra Acto, abarca tanto a lo que uno hace como a lo que deja de hacer (acción y omisión). En las dos formas se expresa la voluntad”<sup>4</sup>.

El delito en la concepción jurídica es todo acto humano voluntario que se adecua al presupuesto jurídico de una ley penal. En la concepción filosófica consiste en la vulneración de un deber. Dentro de la concepción dogmática del Delito enumera los elementos constitutivos del delito.

Muñoz Conde y García Arán coinciden que la Dogmática jurídico-penal ha llegado a la conclusión de que el concepto del delito responde a una doble perspectiva:

---

<sup>2</sup> Real Academia de la Lengua. El Delito.

<sup>3</sup> Jiménez de Asúa Luis. El Delito.

<sup>4</sup> Cabanellas Guillermo. Diccionario de Derecho Ilustrado. El delito.



1. “El delito se presenta como un juicio de desvalor que recae sobre la conducta.
2. El delito se presenta como un juicio que se hace sobre el autor de ese hecho”<sup>5</sup>.

Al primer juicio de desvalor se le llama antijuridicidad. Al segundo, culpabilidad.

Por otra parte la Enciclopedia Jurídica Virtual considera: “El concepto ofrece dos acepciones:

1. Noción amplia. En este sentido delito equivale a toda especie delictiva, a hecho punible. Se emplea usualmente con este significado si bien el Código utiliza frecuentemente la expresión infracción criminal, hecho delictivo o, simplemente, infracción.
2. Noción restringida o propia. Designaba la más grave de las clases de hechos punibles”<sup>6</sup>.

Para Carrara el delito lo define como: “La infracción de la Ley del Estado promulgada para la seguridad de los ciudadanos y que resulta de un acto externo del hombre positivo o negativo, moralmente imputable y políticamente dañoso”.

---

<sup>5</sup> Muñoz Conde y García Arán Derecho Penal. Parte General, Valencia, España: Tirant Lo Blanch, 6ª, 2004, p. 205.

<sup>6</sup> Enciclopedia Jurídica.

Garófalo Jurista del positivismo sostiene que el delito es: “La violación de los sentimientos altruista de probidad y de piedad, en la medida media indispensable para la adaptación del individuo a la colectividad”<sup>8</sup>

Otras definiciones citadas por el Portal Alipso enriquecen las orientaciones hacia una definición propia:

“Alimena: Es delito todo hecho prohibido bajo la amenaza de una pena.

Beling: El delito es la acción típica, antijurídica, culpable, subsumible bajo una sanción penal adecuada y que satisfaga las condiciones de punibilidad. (Definición de 1906).

Carmignani: Infracción de las leyes del Estado, protectoras de la seguridad privada y pública, mediante un hecho humano cometido con intención directa y perfecta.

Carnelutti: Es un hecho que se castiga con la pena, mediante el proceso».

---

<sup>8</sup> Garófalo Rafael. Criminología: Estudio Sobre El Delito Y La Teoria De La Represión, PDM, Ángel, 1885, México.

Ferri: «Son delitos las acciones determinadas por motivos individuales (egoístas) y antisociales, que turban las condiciones de vida y lesionan la moralidad media de un pueblo dado, en un momento dado.

Feuerbach: Una sanción contraria al derecho de otro, conminada por una ley penal.

Florián: Es un hecho culpable del hombre, contrario a la ley (antijurídico), conminado por la amenaza penal.

Gómez: Es un hecho humano, antijurídico, real o potencialmente lesivo de un bien o interés protegido por la ley.

Grispigni: Es aquella conducta que hace imposible o pone en grave peligro la convivencia y la cooperación de los individuos que constituyen una sociedad; conducta humana correspondiente al tipo descrito por una norma penal.

Ihering: Es delito, el riesgo de las condiciones vitales de la sociedad que, comprobado por parte de la legislación, solamente puede prevenirse por medio de la pena.

Impallomeni: Es un acto prohibido por la ley con amenaza de una pena, para la seguridad del orden social constituido en el Estado.

Ingenieros (José: «Es una transgresión a las instituciones impuestas por la sociedad al individuo, en la lucha por la existencia».

Mayer: Es un acontecimiento típico, antijurídico e imputable.

Mezger: El delito es la acción típicamente antijurídica y culpable.

Núñez: Es un hecho típico, antijurídico y culpable.

Ortolan: Es toda acción o inacción exterior que vulnera la justicia absoluta, cuya represión importa para la concepción del bienestar social, que ha sido de antemano definida y a la cual la ley le impone pena.

Ramos: El delito es la violación de la norma que da origen a la ley penal, norma que recoge los elementos constitutivos de la medida media del sentimiento colectivo.

Rivarola: Hecho punible es el concepto que puede comprender, en su mayor generalidad, todos los hechos a los cuales la ley haya prefijado una pena.

Soler: Delito es una acción típicamente antijurídica, culpable y adecuada a una figura penal.

Tejedor: Delito es toda acción u omisión prevista y castigada por una ley penal que está en entera observancia y vigor.

Von Lizst: El delito es un acto humano, culpable, contrario al derecho y sancionado con una pena”<sup>9</sup>

Las aportaciones de estos distinguidos estudiosos de las Ciencias del Derecho en materia del delito, todos concuerdan que el delito es una actividad ilícita contraria al ordenamiento jurídico del país donde se produce, y que conduce a una pena. Para que el Acto sea delictivo, debe estar descrito como tal en los Códigos Penales. Más allá de las leyes, se conoce como delito a toda aquella acción que resulta condenable desde un punto de vista **ético** o moral.

El delito puede tener las características de ser civil o de carácter penal, por lo tanto existe diferencia entre ellos. De acuerdo a la Enciclopedia Wikipedia, El "delito civil" es el acto ilícito, ejecutado con intención de dañar a otros, que constituye " cuasidelito civil" el acto negligente que causa daño. Los actos considerados como "delitos civiles" y "cuasidelitos civiles", pueden ser también "delito penal" si se encuentran tipificados y sancionados por la ley penal. Un "delito penal" no será, a la vez, "delito civil", si no ha causado daño; como tampoco un "delito civil" será, a la vez, "delito penal", si la conducta no es prohibida por la ley penal”<sup>10</sup>

## **TIPOS DE DELITOS**

---

<sup>9</sup> Portal Alipso Apuntes de Penal Cátedra Spolansky - Tecna

<sup>10</sup> Enciclopedia Wikipedia. Teoría del Delito.

Los delitos se clasifican de acuerdo a las formas de la culpabilidad:

1. **DOLOSO**: este delito se define por la concordancia entre las intenciones del autor del delito y la acción delictiva llevada a cabo. En otras palabras la persona involucrada tiene el propósito de realizarla.
2. **CULPOSO O IMPRUDENTE**: En el delito culposo el autor no tuvo la intención de perpetrar el acto delictivo. Es decir que el mismo no es una consecuencia de su voluntad, sino de la falta de cuidado.

El dolo es la intención de cometer esa conducta delictiva y la imprudencia es aquella acción que se comete por ser negligente en la conducta o por no observar el deber objetivo de cuidado.

Según la forma de la acción:

1. **POR COMISIÓN**: este delito hace referencia a una acción producida por el sujeto, se parte de una prohibición, la cual no es tomada en cuenta por el mismo, y de todos modos el acto es realizado.
2. **POR OMISIÓN**: se refiere a una abstención. Es decir, aquí el delito se lleva a cabo cuando el sujeto omite una acción que debería haber realizado.

Según la calidad del sujeto activo

**1. COMUNES:** los delitos comunes pueden perpetrarse por cualquier persona. No incluye una determinada calificación con respecto al autor.

Según la opinión de los entendidos se categoriza a los delitos como graves y no muy graves. El objetivo de esta investigación es ubicar al delito informático a qué categoría pertenece y que consecuencias repercute en la sociedad ecuatoriana.

No hay duda que la evolución de la ciencia y de la tecnología es innegable su aporte a casi la totalidad de las actividades humanas es una realidad, es así que las posibilidades de investigación y comunicación se han incrementado y con ello el ser humano tiene acceso a una infinidad de herramientas, fuentes de consulta y entretenimiento.

Según los criterios de expertos, para tratar los elementos del delito primero se tiene que estudiar lo que es el delito, según el diccionario jurídico Leuxus dice que, es la parte capital del derecho penal. Desde una perspectiva mas a fondo podemos decir que el delito es; la acción u omisión penada por la ley. El concepto está sometido por completo al principio de legalidad, de tal forma que el principio acuñado por los juristas romanos "*nullum crimen sine lege*", es su regla básica. Por esto resulta irrelevante el intento de averiguar una noción sustancial de delito, como pueda ser en otras épocas el delito natural, pues delito es solo aquello castigado por la ley. Resulta evidente que la ley penal no puede ser arbitraria y castigar respondiendo al criterio exclusivo de poner a prueba a los ciudadanos, sino que pretende la defensa de bienes jurídicos concretos.

Los delitos se clasifican en delitos graves y menos graves, en atención a la pena que se impone, utilizándose por tanto un principio más cuantitativo (gravedad de la pena que señala cada código), que cualitativo.

## **EL DELITO INFORMÁTICO**

En este escenario sorprendente de la tecnología el ser humano que tiene una conducta orientada al delito no duda en encontrar en dichas tecnologías de la información y la comunicación canales para cometer delitos, a lo que los expertos denominan delitos informáticos. Estos delitos son ilícitos que utilizando las computadoras, los sistemas y las tecnologías dan cumplimiento a sofisticados delitos. En tal sentido el delito informático está ligado a la informática, por lo que es necesario conocer las diferentes definiciones que se dan a estos nuevos delitos.

“Callegari Nidia define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".

Para Sarzana Carlos, los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, como mero símbolo".



María de Luz Lima considera que el "delito electrónico" en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal, en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".

Jijena Leiva quien menciona en su obra "Chile, La protección penal a la Intimidad y el Delito Informático" que el delito informático es *"... toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma"*<sup>11</sup>

A la luz de estas opiniones el delito informático determina actividades criminales, lo que ha llevado a varios países a tratar de encuadrar en figuras típicas tradicionales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc. lo que ha propiciado la necesidad de regulación por parte del derecho.

Diferentes denominaciones se han utilizado para demostrar estas conductas ilícitas en las que se usa la computadora, tales como delitos informáticos", "delitos electrónicos", "delitos relacionados con las computadoras", "crímenes por computadora". "delincuencia relacionada con el ordenador.

---

<sup>11</sup> Callegari Nidia, Sarzana Carlos, María de Luz Lima, Jijena Leiva. Citados por Nora Paterlini, Carolina Vega, Gabriela Guerriero y Mercedes Velázquez. DELITOS INFORMÁTICOS Antecedentes Internacionales para una Legislación Nacional Proyectos Legislativos

En tal sentido la computadora se ve involucrada como material u objeto de la acción criminológica, el delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de las personas.

El "delito electrónico es cualquier conducta criminal que para su ejecución hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel.

## **CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS**

Estos delitos no son fáciles de demostrar, ya que escasamente se pueden encontrar las pruebas pertinentes. Los delitos pueden cometerse en forma rápida y sencilla, con un solo equipo informático, sin la presencia física en el lugar de los hechos. Estos delitos se proliferan y evolucionan de una manera admirable, esto complica su identificación e investigación.

En este tipo de delitos intervienen dos tipos de sujetos, sujeto activo y sujeto pasivo. El primero con seguridad tiene conocimientos técnicos de informática, es decir se trata de un sujeto con un alto nivel para manipular los sistemas de información a través de las computadoras. En el caso de los sujetos pasivos estos pueden ser personas, instituciones gubernamentales, financieras y todas aquellas que usan sistemas automatizados de información.

La Organización de las Naciones Unidas (ONU) define tres tipos de delitos informáticos:

- Fraudes cometidos mediante manipulación de computadoras.
- Manipulación de los datos de entrada.
- Daños o modificaciones de programas o datos computarizados.
- Los fraudes cometidos mediante manipulación de computadoras pueden clasificarse en:
  - Manipulación de los datos de entrada o sustracción de datos.
  - La manipulación de programas: modificación de programas existentes en un sistema o la inserción de nuevos programas.
  - Manipulación de los datos de salida.
  - Fraude efectuado por manipulación informática: también llamado "técnica del salchicón", aprovecha las iteraciones automáticas de los procesos de cómputo.
- Los fraudes cometidos mediante la manipulación de los datos de entrada:
  - Como objeto: alteración de los documentos digitales.
  - Como instrumento: uso de las computadoras para falsificar documentos de uso comercial. Los daños o modificaciones de programas o datos computarizados:
    - Sabotaje informático: acción de eliminar o modificar funciones o datos en una computadora sin autorización, para obstaculizar su correcto funcionamiento.
    - Acceso no autorizado a servicios y sistemas informáticos.
    - Reproducción no autorizada de programas informáticos de protección legal: ver piratería.

## **LEGISLACIONES INTERNACIONALES DEL DELITO INFORMÁTICO**

La única fuente de consulta, se encuentra en las legislaciones de los países desarrollados en tecnología. Alemania, desde agosto de 1986, adoptó la Segunda Ley contra la Criminalidad Económica, contempla los siguientes delitos: espionaje de datos, estafa informática, falsificación de datos probatorios, alteración de datos. Sabotaje informático, utilización abusiva de cheques o tarjetas de crédito.

Austria: En la Ley de Reforma del Código Penal de Diciembre de 1987, observa los siguientes delitos: destrucción de datos, estafa informática.

Francia: Ley No. 88-19 enero de 1988 sobre el fraude informático, así como también: acceso fraudulento a un sistema de elaboración de datos, sabotaje informático, destrucción de datos, falsificación de datos informatizados, uso de documentos informatizados falsos.

**EEUU: En 1994, Acta Federal de Abuso Computacional**, modificó el Acta de Fraude y Abuso Computacional de 1986, cuya finalidad es la de eliminar los argumentos hipertécnicos acerca de qué es y qué no es un virus, un gusano, un Caballo de Troya, y en que difieren de los virus, la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informático, a las redes, información, datos o programas.

Existen convenios internacionales entre los países del mundo que utilizan la informática para sus actividades, convenios internacionales disponen de normas para evitar los delitos informáticos, como: Tratado de Libre Comercio de América del Norte (TLC), firmado por México, Estados Unidos, Canadá en 1993, con un apartado sobre propiedad intelectual, la sexta parte del capítulo XVII, en el que se contemplan los derechos de

autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución.

El Acuerdo General de Aranceles Aduaneros y Comercio (GATT), Uruguay, el artículo 10, relativo a los programas de ordenador y compilaciones de datos, establece que este tipo de programas, ya sean fuente u objeto, serán protegidos como creaciones de carácter intelectual. En Europa existe la BUSINESS SOFTWARE ALLIANCE (BSA), es una asociación que actúa legalmente contra la piratería informática desde Europa, Asia y Latinoamérica.

Según Nora Paterlini, Carolina Vega, Gabriela Guerriero y Mercedes Velázquez: “España: Su Código Penal es el más actualizado del continente europeo, las distintas figuras convencionales no alcanzan para perseguir la amplia gama de delitos informáticos, como conductas de hacking, accesos ilegítimos a sistemas informáticos y distribución de virus, bombas lógicas, etc.

**Italia** El Código Penal Italiano tipifica los siguientes delitos:

Art 615 ter: Acceso no autorizado a un sistema de computadoras o telecomunicaciones.

Art 615 quater: Posesión y disponibilidad de códigos de acceso a sistemas de computadoras o telecomunicaciones.

Art 615 quinter: Difusión de Programas que puedan causar daños o interrumpir sistemas de computación.

**Inglaterra** La Computer Misuse Act (Ley de Abusos Informáticos) comenzó a regir en el año 1991.- Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Contiene además la ley un apartado que especifica la modificación de datos sin autorización. Los virus están incluidos en esa categoría. Asimismo dispone que liberar un virus tiene penas desde un mes a cinco años, dependiendo del daño que causen.-

Otros países Europeos que contienen normativa sobre delitos informáticos, aunque incompleta y solo relacionada a algunos aspectos generales son:

**Bélgica** El Parlamento Belga incorporó en su Código Penal nuevos delitos informáticos, vigentes desde febrero de 2001. Los cuatro principales problemas relacionados con los delitos informáticos que son tratados por esta reforma son: el robo por computadora, el fraude por computadora, el hacking y el sabotaje informático.

**Estonia** El Código Penal de Estonia prevé en los artículos 269 a 273 los delitos de:

Destrucción de programas y datos en una computadora.

Sabotaje informático

Uso no autorizado de computadoras o sistemas de computación.

Daños o interferencias ocasionados con conexiones de computadoras.

Transmisión de virus informáticos

**Holanda** El 1 de mayo de 1993 entró en vigencia la ley de Delitos Informáticos, en la cual se penaliza: el hackingel preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría) la distribución de virus.

**Dinamarca** Código Penal sección 263. Considera conducta punible al acceso no autorizado a información o programas instalados en un sistema de procesamiento de datos. Agrava las penas según las intenciones o circunstancias.

**Finlandia** Código Penal Capitulo 38 sección 8, considera punible el acceso no autorizado a un sistema de computadoras para robar o transmitir parte del sistema. La tentativa es punible

**Hungría** Código Penal. Sección 300 C, contempla el fraude informático.

**Luxemburgo** Acta del 15 de julio de 1993 sobre la lucha contra el crimen financiero y computacional. Prevé:

Acceso ilegítimo a un sistema de procesamiento de datos. Agrava la pena cuando dicho acceso produce la supresión, modificación o alteración de los datos o parte del sistema.

**ASIA** Algunos de los países del continente Asiático que han legislado sobre delitos informáticos son:

**India** Acta de Información Tecnológica n° 21 año 2000, Pena y define al hacking.

**Israel** The Computer Law de 1995. Sección 4, condena el acceso ilegítimo a una computadora.

**Japón** Ley n° 128 de 1999 (Con efecto desde el 3 de febrero de 2000) Prohíbe el acceso no autorizado a sistemas de computadoras y los actos que faciliten dicho acceso no autorizado. Establece penas de multa o prisión para los infractores.

**China** Decreto n° 147 de Febrero de 1994 "Regulación del Pueblo de la Republica de China en protección de la seguridad de Datos Informáticos" y la Ordenanza de Telecomunicaciones, Sección 27 A: Tipifica el delito de acceso ilegal a la información o programas de un sistema de computadora, estableciendo una pena de multa o prisión no mayor a seis meses, pena ésta que se eleva hasta dos años según las circunstancias o intenciones del sujeto

**Malasia** Acta de Crimen Computacional de 1997, condena el acceso ilegítimo a sistemas de computación



**Filipinas** Republic Act n° 8792, sobre "Reconocimiento y uso de transacciones electrónicas, penalidades y otros propósitos", en su Par. V, denominada Provisiones Finales, penaliza:

Hacking y craking: entendido como acceso no autorizado o interferencia en un sistema de computadoras o telecomunicaciones para alterar, robar o destruir, usando para ello un computador o sistema de telecomunicaciones, incluyendo la introducción de virus.

**Singapur** Computer Misuse Act prevé la penalización:

Acceso no autorizado a una computadora.

**Chile:** Primer país de América del Sur que ha actualizado su legislación. A través de la ley 19.223 (28 de mayo de 1993) están tipificados figuras penales relativas a la informática:

1. Destrucción o inutilización maliciosa de hardware y software, así como alteración de su funcionamiento por cualquier medio 2. Acceso a información "contenida en un sistema de tratamiento de la misma" con ánimo de "apoderarse, usar o conocerla indebidamente" 3. Difusión maliciosa de datos contenidos en un sistema de información Asimismo, este país reconoce al software como obra intelectual (ley 17.336).

**Perú:** El Código Penal incluyó, a fines de año 2000, un capítulo específico para el tratamiento de los delitos informáticos (Capítulo X) que incorporó los artículos 207°-A, 207°-B y 207°-C. Allí se reprime: 1. Utilizar o ingresar indebidamente a una base de datos o red de computadoras para alterar un esquema, interceptar o copiar información en tránsito o contenida en

una base de datos. Se agrava la pena si se actúa con propósito de beneficio económico. 2. Utilizar, ingresar o interferir indebidamente una base de datos o red de computadoras con el fin de dañarlos o alterarlos. Las conductas anteriores se agravan cuando el agente hace uso de información privilegiada obtenida en función de su cargo o pone en peligro la seguridad nacional.

**México:** El Código Penal se reformó en 1999, incorporando los artículos 211 bis 1, 211 bis 2, 211 bis 3, 211 bis 4, 211 bis 5, 211 bis 6 y 211 bis 7. Se sanciona al que, Sin autorización: a) Modifique, destruya o provoque pérdida de información contenida en sistemas de informática protegidos por algún mecanismo de seguridad; b) Conozca o copie dicha información. Se agravan las conductas anteriores si se tratare de sistemas de informática del Estado o de instituciones que integran el sistema financiero y más aún si el agente estuviere autorizado para acceder a los mismos o cuando la información obtenida se utilice en provecho propio o ajeno.

El software es considerado obra intelectual y, consecuentemente, recibe protección legal. Sin perjuicio de advertirse preocupación por el impacto de la alta tecnología en la comisión de delitos, ninguna de las legislaciones analizadas contempla íntegramente la problemática que la materia ofrece. No se prevé expresamente el fraude informático, aunque todas condenan el acceso ilegítimo a datos ajenos informatizados (hacking). La corta vigencia de las normas peruanas (2000) y mexicanas (1999) impiden hacer una evaluación precisa de la efectividad de las mismas. En este punto corresponde destacar las recomendaciones dadas en dos congresos internacionales.

Estos son los de Río de Janeiro del año 1994, y del de Montevideo de 1998. En el primero se distinguen distintos delitos que deben ser tipificados, como el fraude en la introducción alteración, o supresión de datos; las falsificaciones informáticas; los daños causados a datos o programas; el sabotaje informático; los accesos ilegítimos; la interceptación, reproducción no autorizada de un programa informático; etc. En el segundo, se analizó profundamente la cuestión de la responsabilidad penal emergente de estos delitos, el respeto por el principio de legalidad y la protección de la propiedad intelectual. ”<sup>12</sup>

Mientras en la legislación internacional de los países citados el delito informático es tratado en una forma más amplia, en la legislación ecuatoriana lo único que se reprime como delito informático es la utilización del hardware y el software pirata.

## **EL DELITO INFORMÁTICO EN ECUADOR**

Desde el año 2002 los primeros tipos penales informáticos se incluyeron en la legislación ecuatoriana dentro del proyecto de la ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, posteriormente se incluyeron en el Código Penal. Las razones para trabajar en esta materia fue los ataques a website en Ecuador a través de la técnica del Defacing fuera a la página del Municipio de Quito en el año 2001, el primer delito informático que se cometió en el Ecuador fue en el año 1996, caso que fue denunciado pero nunca hubo sentencia se conoce como el redondeo

---

<sup>12</sup> Nora Paterlini, Carolina Vega, Gabriela Guerriero y Mercedes Velázquez. DELITOS INFORMÁTICOS Antecedentes Internacionales para una Legislación Nacional Proyectos Legislativos

en las planillas realizadas en EMETEL, no se sabía a donde se dirigían ciertas cantidades conocidas demasiadas pequeñas, pero traducidas a grandes cantidades de dinero constituía un delito, en esta acción se utilizó la técnica del **salami o rounding down**.

Según Diario El Comercio: “En el 2011, el fraude bancario fue el delito informático que más ocurrió en Ecuador, según datos de Kaspersky Lab, compañía especializada en seguridad informática. Aunque la empresa, por temas de seguridad no proporcionó estadísticas del número exacto de este tipo de delitos, se calcula que en el país se perdió el año pasado cerca de USD 5 millones, mientras que en el 2010 fueron USD 2 millones. En diciembre del 2011, se registraron 1 179 ataques a IPS (Sistemas de prevención de intrusiones, por sus siglas en inglés) a 25 clientes de Astaro, empresa que da servicios de seguridad informática para empresas.

Para Xavier Almeida, gerente Comercial de GMS, compañía que brinda soluciones integradas en telecomunicaciones, este número muestra el crecimiento del cibercrimen en el país y refleja la falta de conocimiento de la ciudadanía de los riesgos que se corren en el mundo de las transacciones en Internet. Por esta razón, GMS realiza la campaña denominada “Conciencia Viral”, que busca alertar a los usuarios sobre los riesgos que corren en la Web y las precauciones que deben tomar con sus gestiones en el ciberespacio. Almeida recomienda a los usuarios tomar varias medidas para prevenir este tipo de inconvenientes. Por ejemplo tratar de no realizar transacciones bancarias desde un ciber café, revisar constantemente las contraseñas. Además, la actualización

constante de las herramientas de las plataformas de trabajo por parte de las entidades bancarias”<sup>13</sup>.

En el Artículo publicado en Diario El Universo de la Ciudad de Guayaquil Alejandra el 26 de agosto de 2012, comunica que un promedio de siete delitos informáticos se registra por día en Ecuador en tal sentido a continuación se cita el artículo completo: “Valdiviezo recuerda que una mañana vio con asombro desde el sitio web del banco donde labora cómo iba desapareciendo su dinero, sin que ella realice transacción alguna. La afectada cuenta que era fin de mes y decidió revisar si le habían cancelado su sueldo. “A eso de las 10:00 pude ver que me habían pagado. Luego, en la tarde, ingresé a la página para hacer unos pagos de servicios básicos pero me di cuenta de que faltaban \$ 100. Incrédula refresqué la página y para mi sorpresa volvieron a desaparecer otros \$ 100. Me estaban robando en ese mismo rato”, dice. Luego de presentar la queja en la entidad bancaria, voceros de esta explicaron que su tarjeta fue clonada y que los retiros se realizaron desde un cajero ubicado en la esquina de las calles Versalles y Ramírez Dávalos, en el centro norte de Quito. Finalmente el dinero le fue devuelto a Valdiviezo. Esta es una de las 3.129 denuncias por delitos informáticos que recibió la Fiscalía en el Ecuador el año pasado.

La cifra fue la más alta desde el 2009 cuando se registraron 168 casos; cantidad que se incrementó al siguiente año, en el 2010, con 1.099 quejas por “apropiación ilícita utilizando medios informáticos”, como describe el delito la entidad. En los primeros seis meses de este año la Fiscalía General ha registrado a nivel nacional 1.354 casos de delitos financieros.

---

<sup>13</sup> **Diario EL COMERCIO** [http://www.elcomercio.com.ec/negocios/Hoy-analisis-delito-informatico-Quito\\_0\\_659334201.html](http://www.elcomercio.com.ec/negocios/Hoy-analisis-delito-informatico-Quito_0_659334201.html).

Las provincias que más denuncias registran son Pichincha con 563 quejas, Guayas con 275 y Santa Elena con 131. Pero no siempre en estos casos los delincuentes actúan en el territorio nacional. A Isabel Heredia, por ejemplo, le aparecieron dos pagos de \$ 200 cada uno en tiendas ubicadas en Lima (Perú), cuando ella asegura que nunca estuvo en ese país.

En el banco y en la Fiscalía, a donde acudió a presentar la denuncia, le dijeron que lo más probable es que le hayan robado los datos de su tarjeta de crédito bandas de ladrones que operan en diferentes países. Al igual que otros delitos como el narcotráfico o la trata de personas, la Fiscalía General del Estado considera que la apropiación de bienes financieros o información se ha convertido en una forma de delinquir con carácter transnacional.

Esta situación mantiene alerta a las autoridades, que incluso piensan en propuestas regionales para combatir esta nueva forma de delinquir. El fiscal general, Galo Chiriboga, considera que este podría ser uno de los temas en los que tendría competencia la Corte Penal de Unasur (Unión de Naciones Suramericanas) que se busca crear para hacer frente a los principales delitos que ahora afectan a esta región. En el proyecto de Nuevo Código Penal Integral que se trata en la Asamblea Nacional, también se ha incluido sanciones para los delitos informáticos que van de uno a siete años de privación de la libertad, dependiendo del delito.

“El país tiene que hacer un gran esfuerzo por tipificar adecuadamente los ciberdelitos. No sé si se logre hacerlo en este Código Penal, pero hay que avanzar en un código más moderno”, señala Chiriboga. Un estudio

realizado por las empresas GMS y Kaspersky ubicó las pérdidas económicas por delitos informáticos en el Ecuador en un millón de dólares entre 2009 y 2010. Silvana Cárdenas, quien el año pasado formó una Asociación de Afectados por Delitos Informáticos con el objetivo de recuperar los dineros, comenta que en el 2011 la cifra del perjuicio habría llegado hasta los ocho millones de dólares.

“Había gente que hablaba del robo de hasta \$ 60 mil, era una situación desesperante. En mi caso fueron \$ 4.000, todo ese dinero se llevaron a través de la página electrónica del banco y se demoraron casi seis meses para solucionarnos el problema y solo nos devolvieron una parte del dinero robado”, refiere la afectada con indignación.

En esa ocasión con una resolución de la Superintendencia de Bancos se dispuso que de 1 hasta 2.000 dólares los bancos repusieran el 100% del valor; de \$ 2.001 hasta \$ 10 mil, solo el 80%; y más de \$ 10 mil se restituiría el 60% del valor. Además, el organismo rector del sistema bancario nacional dispuso el cambio de 332 cajeros automáticos antiguos a nivel nacional, que deberán ser reemplazados por equipos nuevos que garanticen mayores medidas de seguridad. Sobre este tema, el presidente de la Asociación de Bancos Privados del Ecuador, César Robalino, dice que este cambio está en marcha, “los bancos están importando los cajeros nuevos y considero que en unos seis meses se completará el proceso”, manifiesta.

A esto se agrega que a finales de junio pasado venció el plazo para que los bancos contraten coberturas de seguro contra fraudes informáticos, según la disposición JB-2012-2090 de la Junta Bancaria emitida el 17 de

enero de este año. Sin embargo, los representantes de los bancos estiman que la resolución no involucra directamente la protección a las cuentas de sus clientes, sino la seguridad contra robos masivos que afecten a las entidades financieras. Otra medida rige desde julio pasado con el reglamento para usuarios de telecomunicaciones, que determina que los prestadores de servicios deben remitir los códigos IP (Protocolo de Internet) a la Superintendencia de Telecomunicaciones (Supertel), para investigar delitos informáticos.

Esta medida provoca cuestionamientos del Colegio de Ingenieros Eléctricos y Electrónicos y la Asociación de Usuarios Digitales, que sugieren mecanismos para el uso ético de esta información y señalan que las redes pueden ser vulneradas.

## **USO DE TARJETAS**

Evite el acceso a las páginas web de entidades financieras desde sitios como cibercafés o de terminales que sean utilizadas por varios usuarios.

Recuerde que las entidades bancarias nunca piden a los usuarios información, como claves de seguridad y datos personales a través de correos electrónicos.

Respecto a las redes sociales, los expertos recomiendan no excederse en la información que en ellas se publica porque esta puede ser utilizada por los delincuentes.



Tampoco debe fiarse de supuestos premios o promociones en las páginas web en los que también solicitan datos personales para la entrega directa de lo que supuestamente ha ganado.

Es importante que la tarjeta de crédito sea manejada únicamente por su titular, jamás debe ser prestada ni la pierda de vista cuando se realiza un pago en algún local comercial. Cualquier descuido podría ser aprovechado para clonarla.

Para acceder a servicios bancarios se recomienda utilizar claves lo suficientemente seguras, preferible combinar números, letras mayúsculas y minúsculas.

Verifique, antes de abrirlo, que cada nuevo mensaje de correo electrónico que recibe provenga de una fuente conocida, caso contrario, no intente saber de qué se trata”<sup>14</sup>.

Estas evidencias demuestran que Ecuador no escapa a los delitos y se enfrenta con la delincuencia virtual en condiciones incompetentes, no se puede esconder, como bien lo señala el Dr. Acurio Del Pino Santiago en su Artículo publicado en Internet Los delitos informáticos en Ecuador “la falta de la suficiente preparación en el orden técnico jurídico a pesar de los esfuerzos de la Fiscalía como de la Policía Judicial en este rubro, esto en razón de la falta por un lado de la infraestructura necesaria, como

---

<sup>14</sup> Diario el Universo. Un promedio de siete delitos informáticos se registran por día. Domingo 26 de agosto de 2012. <http://www.eluniverso.com/2012/08/26/1/1422/un-promedio-siete-delitos-informaticos-registran-dia.html>

centros de vigilancia computarizada, las modernas herramientas de software y todos los demás implementos tecnológicos necesarios para la persecución de los llamados Delitos Informáticos como el laboratorio de informáticos forense de la Fiscalía General del Estado, adquirido a finales del 2010 pero que hasta el momento no se encuentra instalado, a pesar de que sus componentes se encuentran en pleno funcionamiento.

## **DELITOS INFORMÁTICOS TIPIFICADOS EN LA LEGISLACIÓN ECUATORIANA**

La ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos de Abril del 2002, (Ley 67) incluye figuras penales que castigan los ilícitos informáticos, en cuya luz el Código Penal integra normas establecidas para los actores sociales de los nuevos sistemas de la información, constan los siguientes ilícitos informáticos:

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

Art.58, Concuenda. Art.202.1 CP: **Contra la Información Protegida.-** El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art.58 últ.inc, del Código Penal concuerda con él. Art. 202.2 del mismo cuerpo legal: **Obtención y utilización no autorizada de información.-** La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.

Art.59, Concuerda. Art.262 CP: **Destrucción Maliciosa de Documentos.-** Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere

maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo.

Art.60, Concuerda. Art.353.1 CP: **Falsificación electrónica.**- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

- 1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;
- 2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;
- 3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo.

Art.61, Concuerda. Art.415.1 CP: **Daños informáticos.**- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los

programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculado con la defensa nacional.

Art.61 últ.inc, Concuerda. Art.415.1 CP: **Destrucción de instalaciones para transmisión de datos.**- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica.

Art.62, Concuerda. Art.553.1 CP: **Apropiación ilícita.**- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de

redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

Art.62 últ.inc, Concuerda. Art.553.2 CP: **Pena.-** La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1. Inutilización de sistemas de alarma o guarda;
2. Descubrimiento o descifrado de claves secretas o encriptadas;
3. Utilización de tarjetas magnéticas o perforadas;
4. Utilización de controles o instrumentos de apertura a distancia; y,
5. Violación de seguridades electrónicas, informáticas u otras semejantes.

Art.63.Concuerda. Art.563 inc.2 CP: **Estafa.-** Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.

Art.64, Concuerda. Art.606.20 CP: **Violación Derecho a la Intimidad.-** Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos”<sup>15</sup>.

---

<sup>15</sup> Código Penal Ecuatoriano Art. 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64.

## PREJUDICIALIDAD POR FALSEDAD DE INSTRUMENTO PÚBLICO ELECTRÓNICO

Falsedad alude a la falta de verdad referida a personas o cosas, la falsificación se refiere al comportamiento, a la acción. Puede ser útil la separación entre "objeto falso" y "conducta de falsificación" para la apreciación del juzgador, pero no parece hacer diferencia respecto de la concepción de ambos términos. En lo relativo al documento informático, es importante examinar el documento electrónico, como nueva concepción documental, su naturaleza jurídica, los caracteres particulares, los elementos del documento informático, su particular lenguaje, los sistemas de seguridad.

Revisando el Código de Procedimiento Penal Ecuatoriano “El Art. 40 manifiesta: *“En los casos expresamente señalados por la ley, si el ejercicio de la acción penal dependiera de cuestiones prejudiciales cuya decisión compete exclusivamente al fuero civil, no podrá iniciarse el proceso penal antes de que haya auto o sentencia firme en la cuestión prejudicial”*

Cuenca Espinoza Alexander analiza lo relacionado a la prejudicialidad por falsedad del instrumento público electrónico indicando que primero se debe definir lo que es el instrumento público, en tal sentido recurre al Art.164 CPC que nos dice: *“Instrumento público o auténtico es el autorizado con las solemnidades legales por el competente empleado. Si fuere otorgado ante notario e incorporado en un protocolo o registro público, se llamará escritura pública. **Se consideran también instrumentos públicos los mensajes de datos otorgados, conferidos,***

**autorizados o expedidos por y ante autoridad competente y firmados electrónicamente”<sup>16</sup>.**

Las orientaciones de Cuenca Espinoza lleva a establecer un análisis más de fondo acerca de qué se entiende por mensaje de datos pero firmados electrónicamente, para lo cual se busca orientación en la CNUDMI que define de la siguiente manera: “La información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el telex o el telefax”<sup>17</sup>

Mientras que al señalar la palabra “firmados electrónicamente” y consultando el espíritu del legislador hace referencia a la firma digital, el Dr. Juan José Páez en su obra “Derecho y Nuevas Tecnologías” dice que la firma digital es “el reemplazo de la firma ológrafa utilizada en medio del papel que representa la intención y voluntad pero por un medio electrónico, firma que cumple 4 requisitos indispensables para que sea válida estos son 1.Integridad 2.Autenticación 3.No repudio 4.Confidencialidad”.<sup>18</sup>

“Art.180 CPC indica: “Si se demandare la falsedad de un instrumento público, el juez procederá a comparar la copia con el original, y a recibir las declaraciones de los testigos instrumentales.

---

<sup>16</sup> Código de Procedimiento Penal Art. 40, 164

<sup>17</sup> Cuenca Espinoza, CNUDMI

<sup>18</sup> Juan José Páez . “Derecho y Nuevas Tecnologías



Practicadas estas diligencias y cualesquiera otras que el juez estime convenientes para el esclarecimiento de la verdad, se correrá traslado de la demanda y seguirá el juicio por la vía ordinaria.

En caso de declararse falso un instrumento, en la misma sentencia se ordenará la remisión de copias del enjuiciamiento civil al fiscal competente para que ejerza la acción penal, sin que pueda ejercerla antes de tal declaración”<sup>19</sup>

Como dice con claridad la norma transcrita: “no puede iniciarse el juicio penal, si antes no existe la declaración del Juez civil”.

En las orientaciones obtenidas se puede deducir que se puede iniciar un juicio en lo referente a prejudicialidad por falsedad de instrumento público electrónico, si es que primero hay sentencia por parte del Juez de lo Civil y declare falso el instrumento público, y con ello pasar a la acción penal.

## **PROBATORIA DEL DOCUMENTO ELECTRONICO**

Son aquellas que por su carácter externo y material, por su visibilidad, facilitan ulteriormente la prueba de los actos jurídicos. Para poder trabajar sobre apreciaciones seguras en la probatoria del documento electrónico

---

<sup>19</sup> Art.180 CPC.

es importante citar el “Art.2 Ley de Comercio Electrónico, firmas *electrónicas y mensaje de datos indica* “Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta ley y su reglamento”<sup>20</sup>,

*Cuenca Espinoza con el afán de establecer concordancia con la legislación chilena cita el Art.1 inc2. Ley de Firma Electrónica chilena pues dice* “la ley se inspira en el principio de la equivalencia del soporte electrónico al soporte de papel”<sup>21</sup>

Técnicamente, el documento electrónico es un conjunto de impulsos eléctricos que incurren en un soporte de computadora, y sometidos a un correcto proceso, permiten su traducción a lenguaje natural a través de una pantalla o de una impresora. Este documento no se puede violentar, pues tiene dueño.

## **PUNIBILIDAD DE UN DELITO INFORMÁTICO**

El Dr. Hugo Carrión, en cuanto a la punibilidad de un delito informático hace algunas consideraciones muy interesantes. Sostiene que si el acceso ilegítimo al sistema informático es el medio para alterar, modificar o suprimir la información, no habrá hacking sino cracking que supone una

---

<sup>20</sup> Art.2 Ley de Comercio Electrónico

<sup>21</sup> Art.1 inc2. Ley de Firma Electrónica chilena.

acción concreta de daño sobre la información y el elemento subjetivo en el autor –dolo- constitutivo del conocimiento y la voluntad de provocarlo.

En otra opinión de expertos un acto es punible siempre y cuando existan elementos probatorios o elementos de convicción. En el caso de los delitos informáticos los elementos de convicción son las pruebas necesarias para probar un delito. De no existir no se puede imponer una pena. En situaciones electrónicas resulta muy difícil mostrarlas fidedignamente.

## **LA SEGURIDAD INFORMÁTICA COMO BIEN JURÍDICO**

Para Peña Daniel: “Desde la óptica de la **seguridad informática** como bien jurídico protegido en el delito informático, se ha de precisar que no se deberá acudir al empleo de elementos subjetivos de intención trascendente que pretendan vincular la conducta realizada con los **bienes jurídicos intimidad y patrimonio**, ya que los comportamientos objetivamente descritos en el **artículo 207°-A**, son suficientes para su lesión. Somos de la opinión de la eliminación de tales elementos subjetivos y la configuración del delito de acceso a base de datos, sistema o red de computadoras, vinculado a la afectación de la **seguridad informática**, ejerciendo así una protección antelada de los mencionados **bienes jurídicos individuales**. Ello no es óbice para que se pueda configurar **tipos penales específicos** que sancionan la lesión del **patrimonio o la intimidad** a través de medios informáticos.

Por último, siendo un tipo de resultado material, es posible la configuración de la tentativa, con las dificultades ya expresadas para la

consumación y prueba del ilícito, por la especialidad del delito en análisis. Asimismo, dada su característica típica, la instigación y la complicidad es perfectamente posible. El que financia, el que induce, el que presta los equipos, el que aporta los datos o claves necesarias, etc<sup>22</sup>.

## **EL SABOTAJE INFORMÁTICO**

El Sabotaje informático, es el acto de borrar, suprimir o modificar sin autorización funciones o datos del sistema informático (hardware y/o software) con intención de obstaculizar el funcionamiento normal del sistema. Es acceder sin ser autorizados a servicios y sistemas informáticos que van desde la simple curiosidad, como es el caso de los piratas informáticos (hackers), hasta el sabotaje informático (ckacking).

No se trata de una conducta que afecta el bien jurídico intermedio de la información, sino que lesiona directamente el patrimonio económico destinado a actividades laborales. Las técnicas que permiten cometer sabotajes informáticos son:

**Virus.** Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Visto de otra fuente. Un virus informático es un programa o software que se autoejecuta y se propaga insertando copias de si mismo en otro programa o documento. Un virus informático se adjunta a un programa o archivo de forma que pueda propagarse infectando los ordenadores a medida que viaja de un ordenador a otro.

---

<sup>22</sup> Peña Daniel Tesis de Grado.

**Gusanos.** Se fabrica en forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. El gusano informático es algo similar a un virus, los expertos lo consideran como una subclase de virus, se propaga sin ayuda de otra persona, este tipo de gusanos aprovechan de un archivo o características de transporte de un sistema, para viajar a otro. Dado a la capacidad de viajar a través de redes, en la mayoría de los casos, el gusano consume demasiada memoria de sistema, haciendo que los servidores y los ordenadores de las personas dejen de funcionar.

Dentro de la amplia gama de gusanos, el gusano Blaster Worm, fue fabricado para hacer un túnel en el sistema y contribuir a que usuarios malos controlen remotamente los ordenadores particulares.

Momento dado del futuro. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar donde se halla la bomba.

## **TIPOS DE VIRUS INFORMÁTICOS**

Los daños a las computadoras regularmente son por la presencia de los virus, estos virus pueden ser los siguientes:

**“Worm o gusano informático:** es un malware que reside en la memoria de la computadora y se caracteriza por duplicarse en ella, sin la asistencia de un usuario. Consumen banda ancha o memoria del sistema en gran medida.

**Caballo de Troya:** este virus se esconde en un programa legítimo que, al ejecutarlo, comienza a dañar la computadora. Afecta a la seguridad de la PC, dejándola indefensa y también capta datos que envía a otros sitios, como por ejemplo contraseñas.

Por otra parte los expertos consideran que permanecen en el sistema, no ocasionando acciones destructivas sino todo lo contrario suele capturar dato generalmente password enviándolos a otro sitio, o dejar indefenso el ordenador donde se ejecuta, abriendo agujeros en la seguridad del sistema, con la siguiente profanación de nuestros datos.

El caballo de troya incluye el código maligno en el programa benigno, mientras que los camaleones crean uno nuevo programa y se añade el código maligno.

**Bombas lógicas o de tiempo:** se activan tras un hecho puntual, como por ejemplo con la combinación de ciertas teclas o bien en una fecha específica. Si este hecho no se da, el virus permanecerá oculto"<sup>23</sup>. Bomba lógica o cronológica. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un ordenador.

Las legislaciones a nivel de todo el mundo han tipificado como delito el sabotaje informático y lo han sometido a sanciones penales. En el Ecuador, el Código Penal a través del Art. 415 tipifica a este delito como "Daño Informático", imponiendo una prisión de 6 meses a 3 años y multa de 60 a 150 dólares para aquél que en forma maliciosa, destruya, altere,

---

<sup>23</sup> <http://www.tiposde.org/informatica/19-tipos-de-virus-informaticos/#ixzz2HKm6piJt>

suprima o inutilice programas, bases de datos o sistema de redes o sus partes, o impida, obstaculice o modifique su funcionamiento. Se agrava la pena de 3 a 5 años y multa de 200 a 600 Dólares en caso de que afectare datos contenidos en las computadoras o en el sistema de redes destinado a prestar un servicio público o que tengan que ver con la Defensa Nacional.

De acuerdo a Zambrano Regina “permanecen en el sistema, no ocasionando acciones destructivas sino todo lo contrario suele capturar datos generalmente password enviándolos a otro sitio, o dejar indefenso el ordenador donde se ejecuta, abriendo agujeros en la seguridad del sistema, con la siguiente profanación de nuestros datos.

**Phishing**, muy conocido en nuestro medio, especialmente, por el perjuicio ocasionado a funcionarios públicos y que ascendieron en un aproximado a US\$ 6´000.000,00. Consiste en el envío de correos electrónicos que, aparentando originarse de fuentes fiables, ejemplo, entidades bancarias, intentan obtener datos confidenciales del usuario, valiéndose de un enlace que, al ser pulsado, **lleva a páginas web falsas o falsificadas.**

**Tampering** o data diddling, modificación desautorizada de datos o al software de un sistema llegándose, incluso, borrar cualquier información. **Scanning**, escudriña el contenido de un libro, periódico, en busca de algo especial para sus intereses. **Pharming o cambiazo**, táctica fraudulenta en los contenidos del servidor de nombres de dominio, ya sea a través de la configuración del protocolo IP o del archivo, para redirigir a los navegadores a páginas web falsas en lugar de las auténticas cuando el usuario accede a las mismas.

**Skimming**, en lo negativo es la técnica delictiva que utiliza tecnología avanzada y facilita al ladrón o hacker robar las claves personales de los cajeros sin necesidad de estar presente, utilizando un dispositivo electrónico diseñado para este fin. Cuando el usuario se aleja, el delincuente ingresa y carga los datos en un sistema con el que puede leerlos y, posteriormente, introducirlos en una tarjeta con banda magnética sin uso, facilitándole hacer una tarjeta clon y procede a estafar.

Otros también tipificados son el **Tampering o Data diddling**, modificación desautorizada de datos personales o al software instalado en un sistema; **Sniffing**, roba información de un terminal específico o de una red por medio de un apartado o cable que cumple funciones de espía; el **Anonimato**, referente a la habilidad de ocultar la identidad de las personas durante el uso de la red internacional de datos o páginas que se visitan por medio de servidores especializados o programas de cómputo que muestran una dirección IP que no corresponde con el equipo utilizado. Existen muchísimos otros definidos desde la legislación de Naciones Unidas.

Los sujetos o personas que realizan o acometen los delitos informáticos, según la actividad que hayan efectuado, son los Hackers<sup>2</sup>, Script Kiddies o criminales informáticos, que “aprovechan sus conocimientos (experto) de la informática (redes, programación, etc.) para utilizar la vulnerabilidad de un sistema con un fin: obtener información privada.

Existen muchos tipos, por ejemplo hacker de sombrero blanco o sombrero negro. El del sombrero blanco sería que avisa del peligro de un posible atentado en la red informática. El otro, lo usará con fines maliciosos”



**“Crackers o vandálico virtual, programadores maliciosos<sup>3</sup>”,** son individuos de la sociedad moderna que poseen conocimientos avanzados en el área tecnológica e informática, igual que los Hackers, invaden sistemas, descifran claves y contraseñas de programas, algoritmos de encriptación, roban datos personales, destruyen y cuando crean algo es únicamente para fines personales, son extremadamente precavidos con el manejo de la información, precisamente, para ocasionar el daño inmaterial e ilegal a los sistemas informáticos.

**Pirata informático<sup>4</sup>** es quien adopta por negocio la reproducción, apropiación y distribución, con fines lucrativos, y a gran escala, a través de distintos medios y contenidos de software, videos, música, de los que no posee licencia o permiso de su autor, generalmente haciendo uso de un ordenador. Siendo la de software la práctica de piratería más conocida, por ello se los clasifica como: Piratas de software, de música, de videojuegos, de películas, de libros o artículos, todo lo cual tiene que ver con los derechos de Propiedad Intelectual

**Spammers<sup>5</sup>,** persona o grupos dedicados a la distribución de correos electrónicos no deseados a usuarios o empresas, por lo cual, son combatidos. Esta actividad es sumamente lucrativa, y en la gran mayoría de legislaciones se la considera ilegal<sup>24</sup>.

Con esta ligera y breve explicación de los delitos informáticos mediante conceptos generales y universales originados desde las mismas Naciones Unidas, cuya comisión especializada, UNCITRAL o CNUDMI, elaboró la

---

<sup>24</sup> Zambrana Reyna Regina. Delitos informáticos contemplados en la Ley Ecuatoriana.

ley modelo y Ecuador la internalizó mediante la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, R.O. 557 de 17-abril-2002, complementado con el reglamento, -diciembre-02-, constando en el capítulo II De las Infracciones Informáticas, artículos 57 en adelante, sancionando o penalizando a los mismos, reformaron a los artículos 202, 262, 353, 415, 553, 563, 606 #19º del Código Penal del Ecuador, que en la ley especial corresponde a los siguientes artículos: 58, 59, 60, 61, 62, 63 y 64.

En fin en Internet es posible hacer ataques a la información, con ello se agrede a la confidencialidad o integridad. Definitivamente no se puede dejar de usar Internet, en la actualidad no existe una definición en la cual los juristas y estudiosos del derecho estén de acuerdo, es decir no existe una concepto adecuado para así nombrar a los delitos informáticos.

### **CAPÍTULO III**

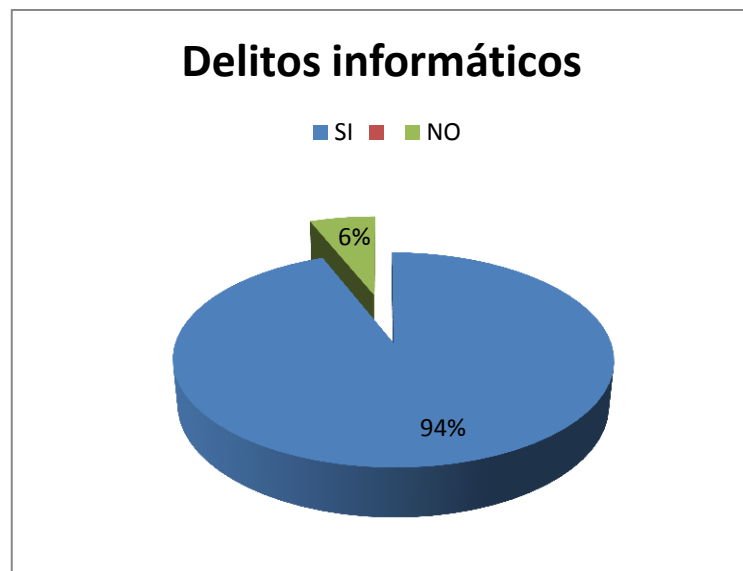
**ANÁLISIS E INTERPRETACIÓN DE RESULTADOS DE LAS ENCUESTAS APLICADAS A PERSONAS VINCULADAS CON LAS INSTITUCIONES, ABOGADOS Y PERSONAS PERJUDICADAS POR LOS DELINCUENTES INFORMÁTICOS EN GUARANDA.**

Pregunta N° 1 ¿De acuerdo a su opinión en Ecuador se cometen delitos informáticos?

<b>Variables</b>	<b>Frecuencia</b>	<b>%</b>
<b>SI</b>	<b>63</b>	<b>94</b>
<b>NO</b>	<b>4</b>	<b>6</b>
<b>TOTAL</b>	<b>67</b>	<b>100</b>

Encuesta aplicada en la ciudad de Guaranda el 20 de septiembre de 2012.

**Gráfico N°1**



### **Análisis e interpretación de resultados:**

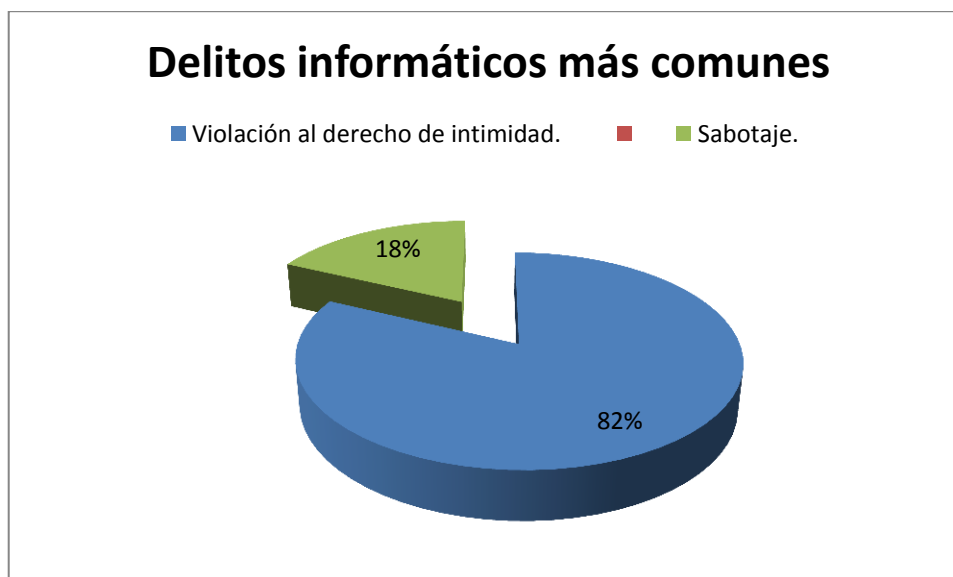
La información demuestra que Ecuador, no escapa a la corriente mundial de los delitos informáticos, un alto porcentaje de los encuestados así lo considera. A penas un número muy reducido de personas desconocen la presencia en el país de estos delitos. Lo que se deduce que son desinformadas a este respecto.

Pregunta N° 2 ¿Qué tipo de delitos informáticos son los más comunes?

<b>Variables</b>	<b>Frecuencia</b>	<b>%</b>
Violación al derecho de intimidad.	<b>55</b>	<b>82</b>
Sabotaje.	<b>12</b>	<b>18</b>
<b>TOTAL</b>	<b>67</b>	<b>100</b>

Encuesta aplicada en la ciudad de Guaranda el 20 de septiembre de 2012.

**Gráfico N° 2**



**Análisis e interpretación de resultados:**

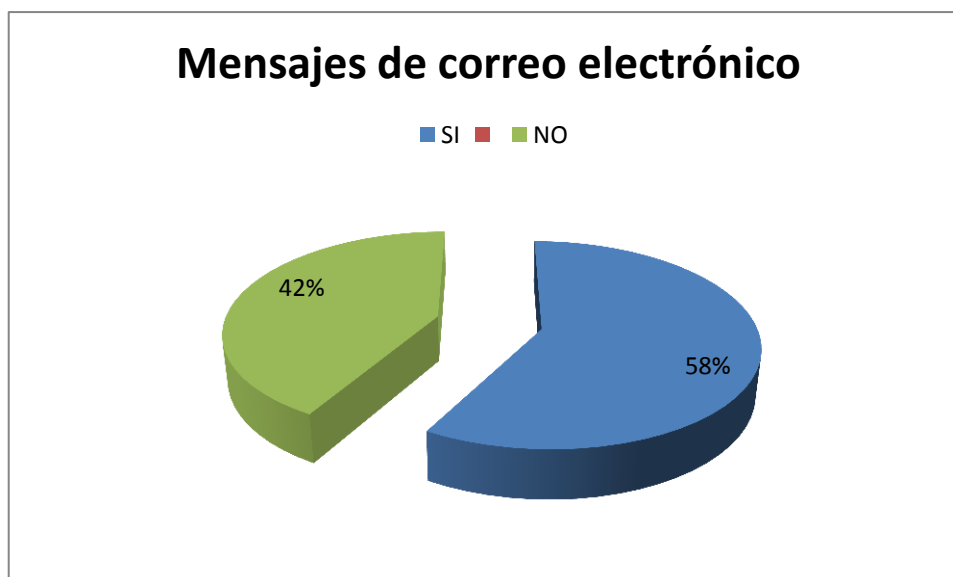
Ecuador es un país inseguro en materia del delito informático, tal situación lo confirma la opinión de los encuestados, al indicar que la violación al derecho de intimidad es el más frecuente, seguido del sabotaje informático. Lo que pone en riesgo a las personas, las instituciones, con un tipo de delincuente muy hábil que escasamente deja huella.

Pregunta N° 3 ¿Usted ha sido víctima de falsos mensajes a través de correo electrónico?

Variables	Frecuencia	%
SI	39	58,2
NO	28	41,7
TOTAL	67	100

Encuesta aplicada en la ciudad de Guaranda el 20 de septiembre de 2012.

**Gráfico N° 3**



**Análisis e interpretación de resultados:**

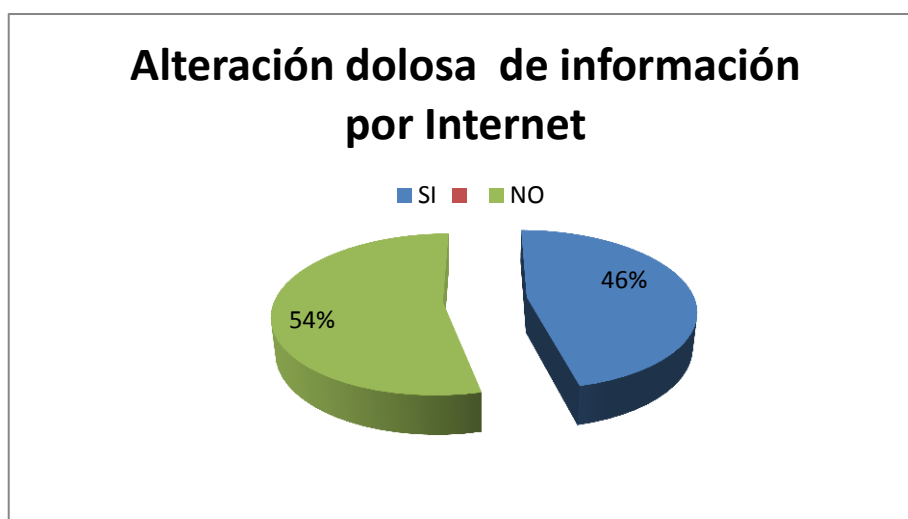
A este respecto existe una amplia población que confirma haber sido víctima de falsos mensajes a través de correo electrónico, tal situación confirma que todo ciudadano está en grave peligro con su seguridad. Es posible que por estos medios se amedrente, se estafe o se cometa otros delitos superiores a los indicados anteriormente

Pregunta N° 4 ¿En alguna ocasión sucedió con usted o con otra persona la destrucción o alteración dolosa de información por Internet?

<b>Variables</b>	<b>Frecuencia</b>	<b>%</b>
<b>SI</b>	<b>31</b>	<b>46,2</b>
<b>NO</b>	<b>36</b>	<b>53,7</b>
<b>TOTAL</b>	<b>67</b>	<b>100</b>

Encuesta aplicada en la ciudad de Guaranda el 20 de septiembre de 2012.

**Gráfico N° 4**



**Análisis e interpretación de resultados:**

A este respecto se identifica una población que representa el 11% de los encuestados que sufrieron alteración dolosa de información confidente, confrontando con los actuales niveles de crecimiento de los delitos informáticos estas cifras revelan que en los próximos años los perjudicados alcanzarán estadísticas preocupantes, con cifras superiores a las actuales.

Pregunta N° 5 ¿Conoce si en la ciudad de Guaranda existen casos de piratería de software?

<b>Variables</b>	<b>Frecuencia</b>	<b>%</b>
<b>SI</b>	<b>60</b>	<b>90</b>
<b>NO</b>	<b>7</b>	<b>10</b>
<b>TOTAL</b>	<b>67</b>	<b>100</b>

Encuesta aplicada en la ciudad de Guaranda el 20 de septiembre de 2012.

**Gráfico N° 5**



**Análisis e interpretación de resultados:**

Definitivamente en la ciudad de Guaranda existe piratería de software, esto confirma lo que se ha escrito en diferentes trabajos de investigación que Ecuador registra este tipo de delitos especialmente en lo que respecta a software. Frente a esta pregunta una pequeña población de encuestados no conocen los delitos que el anterior grupo confirma.

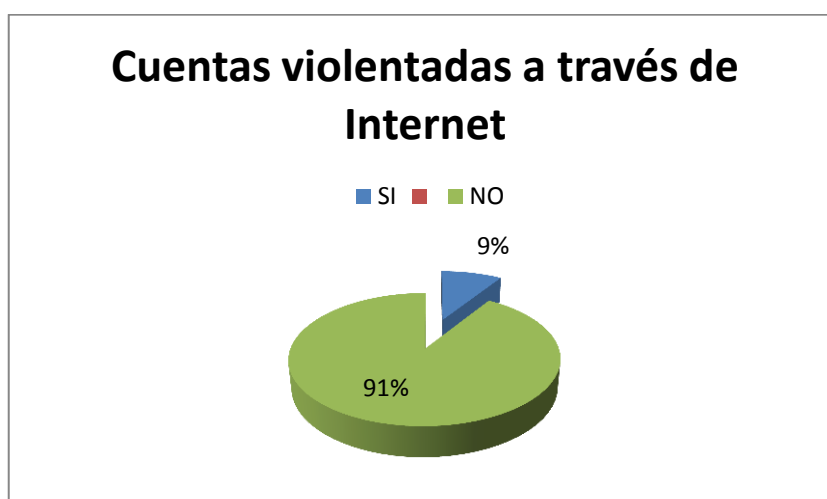


Pregunta N° 6 ¿Sus cuentas bancarias o sueldos han sido violentados a través de Internet?

<b>Variables</b>	<b>Frecuencia</b>	<b>%</b>
<b>SI</b>	<b>6</b>	<b>8,9</b>
<b>NO</b>	<b>61</b>	<b>91</b>
<b>TOTAL</b>	<b>67</b>	<b>100</b>

Encuesta aplicada en la ciudad de Guaranda el 20 de septiembre de 2012.

**Gráfico N° 6**



**Análisis e interpretación de resultados:**

La información demuestra que en Guaranda si existen personas que sus cuentas bancarias han sido violentadas por los delincuentes informáticos, en este tipo de delitos no está inmersa la mayor parte de la población, sin embargo estas personas en cualquier momento pueden ser vulnerados sus cuentas, las tarjetas de crédito u clonadas, como en las denuncias se conocen. Es posible que la realidad en materia de violación de libretas u otros documentos sea mayor que el indicado Guaranda, cien personas no representa la totalidad de estafados en una ciudad grande, pero este estudio confirma el nuevo sistema de delitos que azota al país.

Pregunta N° 7 ¿Ha tomado la decisión de establecer sus denuncias?

<b>Variables</b>	<b>Frecuencia</b>	<b>%</b>
<b>SI</b>	<b>24</b>	<b>35,8</b>
<b>NO</b>	<b>53</b>	<b>79,1</b>
<b>TOTAL</b>	<b>67</b>	<b>100</b>

Encuesta aplicada en la ciudad de Guaranda el 20 de septiembre de 2012.

**Gráfico N 7**



**Análisis e interpretación de resultados:**

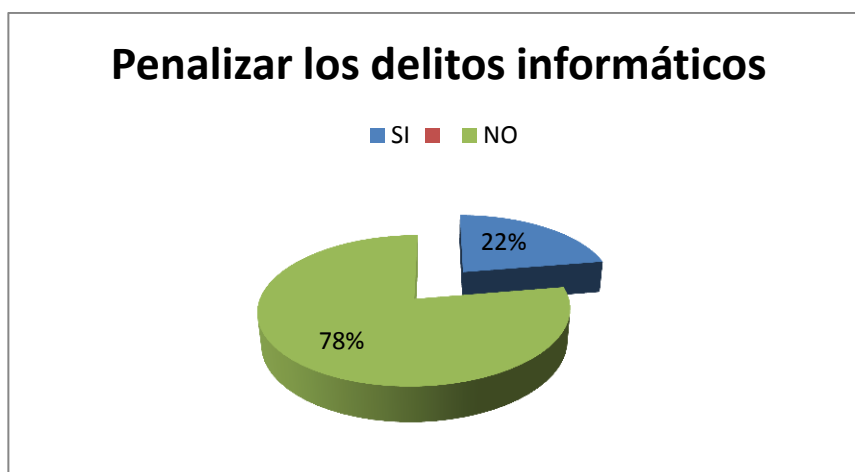
Esta información demuestra la una amplia presencia de personas sometidas a los delitos informáticos que no han llevado sus denuncias ante los organismos pertinentes, es posible que algunos factores les impidan acudir a la justicia.

Pregunta N° 8 ¿De acuerdo a su opinión Ecuador cuenta con una legislación importante para penalizar los delitos informáticos?

Variables	Frecuencia	%
SI	15	22,3
NO	52	77,6
TOTAL	67	100

Encuesta aplicada en la ciudad de Guaranda el 20 de septiembre de 2012.

**Gráfico N 8**



**Análisis e interpretación de resultados:**

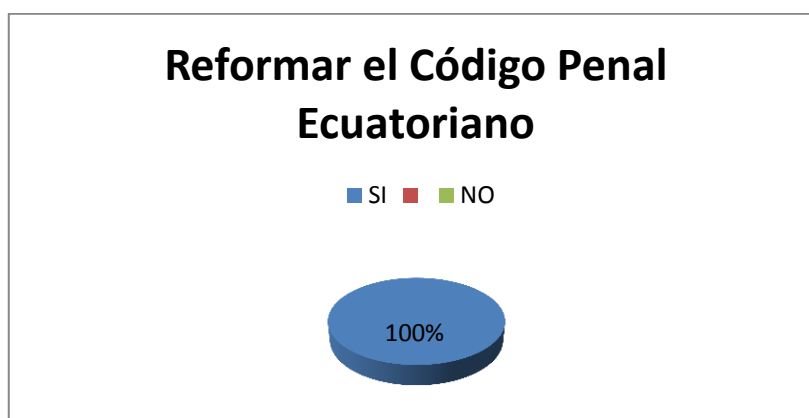
En opinión de los encuestados se conoce que Ecuador al momento no dispone de una legislación que garantice completamente la seguridad de los ecuatorianos en materia de los delitos informáticos. Sin embargo un grupo de encuestados afirman que las leyes actuales si son importantes para legislar los delitos haciendo uso de la tecnología. Tal situación demuestra que en opinión de pocos no hace falta la Reforma al Código Penal.

Pregunta N° 9 ¿Ecuador debe Reformar el Código Penal en materia de delitos informáticos para elevar las penas y que tipifique claramente los delitos informáticos?

<b>Variables</b>	<b>Frecuencia</b>	<b>%</b>
<b>SI</b>	<b>67</b>	<b>100</b>
<b>NO</b>		-
<b>TOTAL</b>	<b>67</b>	<b>100</b>

Encuesta aplicada en la ciudad de Guaranda el 20 de septiembre de 2012.

**Gráfico N 9**



**Análisis e interpretación de resultados:**

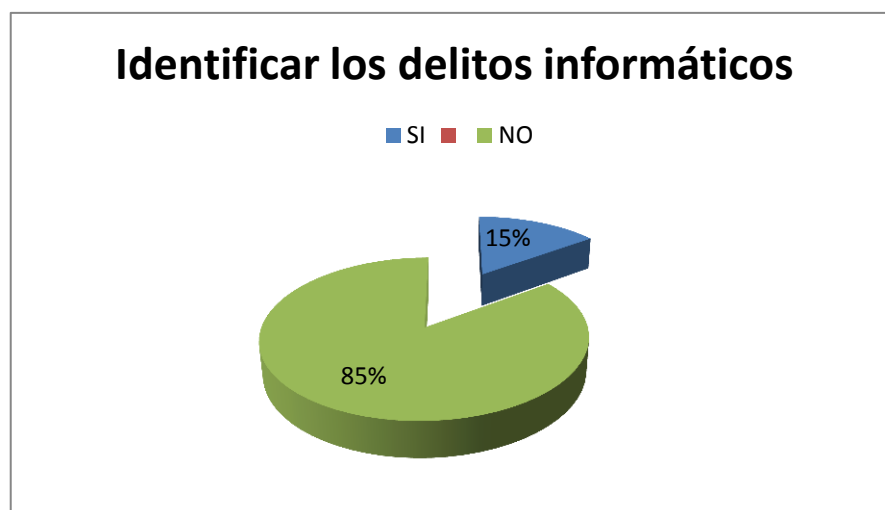
La opinión es total en el sentido de Reformar el Código Penal en materia de delitos informáticos, es posible que con esta legislación se contribuya a bajar los actuales índices, llegar al control total no es posible, pero con sanciones más severas unidas a modernos sistemas tecnológicos para detectar los delitos pueden hacer pensar a los delincuentes que no les resulta fácil operar como hasta hoy.

Pregunta N° 10 ¿La Policía Nacional está preparada para identificar con facilidad los delitos informáticos?

<b>Variables</b>	<b>Frecuencia</b>	<b>%</b>
<b>SI</b>	<b>10</b>	<b>14,9</b>
<b>NO</b>	<b>57</b>	<b>85</b>
<b>TOTAL</b>	<b>67</b>	<b>100</b>

Encuesta aplicada en la ciudad de Guaranda el 20 de septiembre de 2012.

**Gráfico N° 10**



**Análisis e interpretación de resultados:**

La población encuestada tiene razón en el sentido de que le resulta difícil a la policía, intervenir en los delitos informáticos, ya que el uso de las Tic en la mayor parte de delitos no deja evidencias. Se entiende que la policía debe contar con una excelente infraestructura tecnológica como tienen ciertos países que han evolucionado en este campo. Entonces la legislación penal dará importantes resultados, de lo contrario se sancionará al que realmente se lo descubra en el ilícito.

## COMPROBACIÓN DE HIPÓTESIS

Con la finalidad de comprobar la hipótesis se tomó la decisión de insertar en las encuestas la idea de Reformar el Código Penal Ecuatoriano. En tal sentido la pregunta N° 9 da la posibilidad de que sean los propios encuestados quienes confirmen si se debe trabajar en este proyecto. Al respecto todos exigen la Reforma a la legislación penal ecuatoriana en materia de delitos informáticos. Más allá de que una prueba estadística defina algún tipo de comprobación, resulta interesante trabajar con la opinión social de quienes son víctimas.

A continuación se presentan las apreciaciones en cuanto a comprobación de la hipótesis.

<b>HIPÓTESIS</b>		
La Reforma al Código Penal Ecuatoriano en materia de delitos informáticos, permitirá establecer sanciones ejemplarizadoras a quienes violen el derecho a la intimidad personal familiar y el fraude a través de medios electrónicos.		
<b>Variables</b>	<b>Frecuencia</b>	<b>%</b>
SI	100	100
NO	-	-
<b>TOTAL</b>	<b>100</b>	<b>100</b>

Los resultados obtenidos en la comprobación de la hipótesis también orientan la elaboración de la propuesta, que en unidad con los objetivos generales de la investigación se cumple con la sistematicidad del proceso de investigación científica, lógicamente bajo la filosofía del método científico. Por lo tanto de un supuesto en principio (hipótesis) pasa a convertirse en ciencia.

## CONCLUSIONES

1. Definitivamente en el Ecuador a diario se cometen delitos informáticos; lo preocupante es su amplio crecimiento delincuencial y de víctimas, Guaranda es vulnerable a estos delitos.
2. Los delitos informáticos violan el derecho de intimidad de las personas, a través del uso de computadoras y de las modernas Tecnologías de la Información y la Comunicación, sin que los delincuentes dejen huellas, lo que dificulta la intervención de la Policía Nacional.
3. En Ecuador existe una amplia población de ciudadanos que confirman haber sido víctimas de falsos mensajes a través de correo electrónico.
4. Las alteraciones dolosas de información confidente, confrontando con los actuales niveles de crecimiento de los delitos informáticos, estas cifras alcanzarán estadísticas preocupantes, superando a las actuales.
5. Definitivamente en la ciudad de Guaranda existe piratería de software,
6. En Guaranda se violentan cuentas bancarias, se clonan tarjetas de crédito, además se comenten fraudes y otros tipos de delitos apoyados en las TIC.
7. Varias personas se resisten a denunciar que fueron víctimas de los delitos informáticos, tal vez no tienen confianza en la justicia, o consideran que es imposible porque los delincuentes no dejan huellas.
8. Ecuador al momento no dispone de una legislación que garantice completamente la seguridad de los ecuatorianos en materia de los delitos informáticos.



## RECOMENDACIONES

1. Es importante que se establezcan algunas estrategias para controlar la intervención de los delincuentes informáticos y se garantice la seguridad a los ciudadanos ecuatorianos
2. Es importante que las instituciones que tienen bajo su responsabilidad las telecomunicaciones nacionales, adquieran equipos con tecnología sofisticada para detectar a tiempo varios de los delitos informáticos que se operan en las instituciones del Estado, empresas y otras dependencias.
3. Los ciudadanos que son víctimas de falsos mensajes usando el correo electrónico deben establecer sus denuncias ante los organismos pertinentes, y que estos dispongan de técnicos con capacidad para seguir las pistas en la red, ya que las características del modus operandi puede repetirse en otros escenarios, por lo tanto una base de datos puede ayudar a las investigaciones.
4. De igual manera se sugiere a los víctimas de este delito no mantener en reserva personal los ilícitos, se deben denunciar las alteraciones dolosas de información confidente,
5. La piratería de software es un delito, denuncie si usted es víctima.
6. Evite el acceso a las páginas web de entidades financieras desde sitios como cibercafés o de terminales que sean utilizadas por varios usuarios.
7. Recuerde que las entidades bancarias nunca piden a los usuarios información, como claves de seguridad y datos personales a través de correos electrónicos.
8. Respecto a las redes sociales, los expertos recomiendan no excederse en la información que en ellas se publica porque esta puede ser utilizada por los delincuentes.

## **CAPÍTULO IV**

### **PROPUESTA**

#### **TÍTULO DE LA PROPUESTA**

**REFORMA AL CÓDIGO PENAL ECUATORIANO EN LO REFERENTE A LOS DELITOS CONTRA LA INTIMIDAD DE LA PERSONA Y LA FAMILIA Y EL FRAUDE A TRAVÉS DE MEDIOS ELECTRÓNICOS.**

## JUSTIFICACIÓN

El delito informático en Ecuador desde 1999 ha sido muy discutido, dado al apareamiento de diferentes tipos de delitos, se han realizado cursos, seminarios, encuentros, el país dispone de una Ley Especial, Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas.

De igual manera diferentes instituciones sean estas financieras, de Telecomunicaciones, Cámaras de Comercio, entre otras han puesto mucho interés, en pulir lo correspondiente a la parte penal de la Ley, y es que el Código Penal Ecuatoriano por su ambigüedad no contempla figuras como son los delitos informáticos, es decir este instrumento legal penal debe ser actualizado.

En tal sentido esta propuesta contiene algunas modestas actualizaciones en lo que corresponde a una parte de los delitos contra la intimidad personal y familiar, de igual manera en contra del fraude a través de medios electrónicos. Dado a las rigurosidades de autenticidad de documentos esta propuesta encuentra orientaciones en el Proyecto de Reforma al Código Orgánico Integral Penal, presentado ante la Asamblea Constituyente.

Desde mi opinión considero que en este proyecto, son muy blandas las sanciones, por lo que me he permitido ampliar a más años la privación de la libertad de quienes incurrir en los delitos informáticos, aclaro que no es copia, ya que se encuentran opiniones propias y en parte empatan con los criterios del documento base.

## **OBJETIVOS**

### **OBJETIVO GENERAL**

Demostrar la importancia del Código Penal del Ecuador, porque permite sancionar las penas en contra de quienes cometen delitos de violación a la intimidad personal, familiar y cometen fraude a través de medios electrónicos.

### **OBJETIVOS ESPECÍFICOS**

- Socializar la propuesta ante personas e instituciones que han sufrido la violación a la intimidad personal, familiar y han cometido fraudes electrónicos en su contra.
- Elaborar un plan operativo que permita cumplir con la socialización de la propuesta.

## DESARROLLO

Los delitos informáticos son difícilmente descubiertos, los delincuentes considerados sujetos activos actúan sigilosamente y disponen de herramientas importantes con capacidad para borrar todo rastro que delate el delito.

Frente a esta realidad el Estado, la sociedad no puede permanecer indiferente, en tal sentido, es importante actualizar la legislación penal, lo que permitirá en el futuro bajar los índices de delincuencia informática, unido a modernos sistemas que la misma tecnología dispone para detectar la intervención de delincuentes informáticos.

Mucho se comenta en los ámbitos legislativos la necesidad de Reformar el Código Penal, para tipificar delitos cometidos desde las computadoras utilizando los sistemas informáticos.

En los tiempos actuales se evidencia la necesidad de estudiar nuevas relaciones de la Ciencia del Derecho con las nuevas Tecnologías. Existe también la necesidad de prevenir y sancionar los malos usos en la red de redes que es el Internet, y como objetivo principal del presente trabajo se trata de tipificar los delitos informáticos en la legislación Penal Ecuatoriana. La legislación penal debe de adaptarse a los cambios, a la evolución de la sociedad, así como a una reforma del mismo.

El fiscal Galo Chiriboga, en la Comisión presidida por el asambleísta Mauro Andino, propuso se incluya en el Código Orgánico Integral Penal la

tipificación de nuevos delitos atinentes al femicidio, la violencia intrafamiliar, la trata de personas, el derecho a la protección de datos personales, transferencia, acceso ilícito de datos; descubrimiento de secretos comerciales o industriales, suplantación de páginas electrónicas, así como la estafa y el daño informático, informa la Asamblea en su portal web.

En su intervención, por el espacio de una hora, el funcionario dijo que se debe garantizar la vigencia de los derechos y la justicia, por tanto, es necesario impulsar una administración de justicia independiente, eficiente, eficaz, oportuna, imparcial, adecuada e integral, que se enmarque dentro del Plan Nacional para el Buen Vivir, por lo que el sector justicia acordó definir una única línea doctrinaria, a fin de garantizar el acceso expedito al sistema judicial e incorporar las nuevas corrientes del Derecho Penal, que centren su atención en el resultado de las acciones de relevancia penal.

Al referirse a los adolescentes infractores, precisó que la propuesta de la Fiscalía es la de reconocer el principio de especialidad contenido en los artículos 77, número 13, y 81 de la Constitución, por tanto, su tratamiento debe mantenerse dentro del Código de la Niñez y Adolescencia. No se aceptó reducir a 16 años la edad para la punición de los adolescentes.

Propuso como nuevo tipo penal el femicidio, que ha estado oculto en la legislación penal, pues los medios de comunicación y la gente lo han definido como actos violentos contra mujeres, es decir, como delitos pasionales, evitando caracterizarlos como lo que son: actos violentos que pretenden tener más poder sobre las personas, en este caso, del hombre sobre la mujer, por ello, la entidad a su cargo prepara un texto para

ponerlo a consideración de la Comisión de Justicia, mismo que será entregado en los próximos días.

En lo atinente a la violencia intrafamiliar, sostuvo que es toda acción u omisión reiterada o prolongada en el tiempo, que se traduzca en violencia física o psicológica, ejecutada por un miembro de la familia en contra de los integrantes del núcleo familiar, hecho que debe ser sancionado con pena privativa de libertad de seis meses a un año.

Así mismo, explicó que comete infracción de trata de personas quien, con fines de explotación, realiza una o más de las siguientes acciones: financiar, promover o participar de cualquier modo o facilitar, sea la captación, el traslado, la recepción o la entrega de personas, en el territorio de la república o para su salida o entrada al país. Esta conducta será sancionada con pena privativa de libertad de 10 a 15 años.

En lo referente al derecho a la protección de datos personales, Galo Chiriboga indicó que se debe agregar en el Código Orgánico Integral Penal la infracción contra los principios de la protección de datos personales; el acceso ilegal a bancos de datos personales; la revelación de información personal; la transferencia ilícita de datos, con las respectivas sanciones.

A su vez, agregó que el descubrimiento de secretos comerciales o industriales debe ser sancionado con pena privativa de la libertad y la multa respectiva, dejando en manos de la Comisión de Justicia establecer los tiempos y montos pertinentes.

En cuanto a la suplantación de páginas electrónicas, subrayó que en internet -mediante engaños- ciertas personas han suplantado sitios legítimos, capturando información confidencial de una persona natural o jurídica para beneficio propio o de un tercero, por lo que urge establecer las sanciones y multas para esta conducta, lo mismo en cuanto a la estafa informática.

Al finalizar su intervención, el Fiscal del Estado pidió ser recibido en una nueva oportunidad, a fin de presentar sus aportes al Libro II, relacionado con el procedimiento; y, el Libro III, sobre la aplicación y Ejecución de Penas.

Mauro Andino, al agradecer los aportes del funcionario de Estado, recordó que de acuerdo con los tiempos de aprobación del informe para primer debate, en lo posible, Galo Chiriboga debe entregar sus observaciones en esta semana, a fin de poderlos analizar e incluir en el informe aquellas que mejoren el texto del proyecto.

Los ciudadanos ecuatorianos estamos conscientes de que el Código Penal se debe actualizar para controlar el auge de los delitos informáticos, ante tal situación y cumpliendo con los objetivos del proceso de investigación se presenta una propuesta, la misma que merece atención de parte del lector, claro está que no es la única ni la mejor propuesta, pero puede contribuir a motivar a vivir en mejores condiciones.



Asimismo, se incorporaría al Código de Procedimiento Penal, en el capítulo pertinente a las pruebas, la evidencia digital como otro elemento de convicción y posterior prueba en la etapa de juicio, para su respectivo cómputo forense.

## **LEGISLACIÓN VIGENTE Y CONVENIOS INTERNACIONALES**

“Interfutura considera: mientras se reforma el Código Penal, Ecuatoriano se trabaja con leyes supletorias:

- 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, y;
- 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.

## EL NUEVO CÓDIGO ORGÁNICO INTEGRAL PENAL

La nueva ley, en proceso de aprobación, traerá cambios significativos para el tratamiento del delito informático. El capítulo 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”<sup>25</sup>

Cuenca Espinoza es muy enfático al indicar que cuando entre en vigencia el nuevo Código Penal ecuatoriano denominado CÓDIGO ORGÁNICO INTEGRAL DE GARANTÍAS PENALES, se estará unificando el derecho penal sustantivo, adjetivo y ejecutivo, además y se tipificarán nuevos tipos penales relacionados al delito informático.

Entre los que se pueden destacar son los siguientes:

- ✓ Delitos Bancarios en el E-Banking (estafa bancaria y el desvío de dinero)

---

<sup>25</sup> <http://www.interfutura.ec/blog/delitos-informaticos-en-ecuador-lo-que-vendria-en-la-nueva-legislacion/>

- ✓ Acoso Escolar electrónico o cyber bullying (maltrato psicológico y verbal mediante plataformas electrónicas).
- ✓ Grooming o Acoso Sexual (a menores por internet)
- ✓ Chantaje informático (a una persona adulta o infante que parte del bullying y grooming)
- ✓ Sabotaje informático (dañar medios informáticos con un fin determinado)
- ✓ Terrorismo informático (medios electrónicos por pulsaciones para activar instrumentos electromagnéticos)
- ✓ Narcotráfico (captar mulas a través del internet para lavado de dinero)
- ✓ Trata de blancas (engañar mujeres con fines sexuales a través de redes sociales y plataformas virtuales como chats).
- ✓ Pornografía infantil (para intercambio de material pornográfico de menores de edad, en Ecuador el caso más conocido es Gigatribe).
- ✓ Espionaje informático (filtración de información pública como Wikileaks).
- ✓ Infiltración electrónica.
- ✓ Piratería Informática (Legalización de esta a través del SRI, caso tiendas de material cinematográfico pirata).
- ✓ Usurpación de claves (Keylogging, Phishing a través de spam, scams e ingeniería social).
- ✓ Violación de correo electrónico.
- ✓ Robo de Identidad (alto costo en el mercado negro, lo más común información de Hotmail y Facebook, oscila entre 300 a 600USD).
- ✓ Seguridad en Sistemas biométricos (huellas dactilares o contra respuestas al sistema biométrico instalado).
- ✓ Falsificación de documentos electrónicos.
- ✓ Falsificación de firma electrónica (certificados electrónicos provenientes de estas).
- ✓ Planeación o simulación de delitos convencionales.
- ✓ Apropiación indebida (rooteo de servidores es un tipo de hurto).

- ✓ Clonación de tarjetas de crédito (a través de skimmers).
- ✓ Delitos tributarios (falsificación electrónica de asientos contables)

Hasta tanto este trabajo investigativo se convierte en un documento de orientación para establecer las reformas pertinentes al actual Código Penal.

Una vez que he cumplido con mi investigación y al determinar la factibilidad de este proyecto, sugiero que luego del Art. 202 del Código Penal insdertar los siguientes artículos innumerados:

## **REFORMA AL CÓDIGO PENAL**

### **DELITOS CONTRA EL DERECHO A LA INTIMIDAD PERSONAL Y FAMILIAR**

**Artículo** innumerado.- Violación de la intimidad.- Toda persona que divulgue palabras, imágenes de cualquier índole, diálogos, telecomunicaciones, informaciones, todo tipo de grabaciones que no tengan el conocimiento y consentimiento previo de sus actores u autores, serán sancionadas con pena que prive la libertad de dos a cinco años.

De igual manera los miembros de la Policía Nacional, el Ejército Militar que grave, retenga información, analice y difunda La servidora o servidor

militar o policial que, sin la debida autorización legal, será sancionada con la misma pena.

**Artículo innumerado.- Fraude por medios electrónicos.-** Toda persona que utilice con fines fraudulentos una computadora y con ella un sistema informático, redes electrónicas, telecomunicaciones u otro medio afín para la facilitación de la apropiación de un bien ajeno, o que se involucre en la transferencia no consentida de bienes, valores o derechos en perjuicio de ésta o de un tercero, en beneficio propio o de otra persona cometiendo alteración, manipulación o modificación en el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos, equipos de telecomunicaciones, inutilización de sistemas de alarmas, descifrado de claves secretas, lo concerniente a claves encriptados como captación de televisión pirata, tarjetas magnéticas o perforadas, la utilización de controles, violación a la seguridad electrónica, alteraciones a la identificación de números sean estos físicos o electrónicos de teléfonos u otros equipos, asimismo cuando esté en poder ilegal y su comercialización etc. serán sancionada con una pena que prive de libertad de cuatro a seis años.

## PLAN OPERATIVO PARA SOCIALIZAR LA PROPUESTA

Objetivos	Técnica	Actividades	Responsable	Fecha
Socializar la propuesta ante diferentes personas que han sido perjudicadas por los delincuentes informáticos.	Expositiva	Presentar algunas estadísticas referentes a los delitos informáticos en Ecuador.	Equipo de investigación.	Septiembre 6 de 2012.
Entregar un documento en el que se Reforma el Código Penal Ecuatoriano en lo concerniente a los delitos informáticos.	Expositiva	Análisis del nuevo documento penal a través de un articulado.	Equipo de investigación.	Septiembre 6 de 2012.

## **BIBLIOGRAFÍA**

Boletín Oficial N° 412-07 de la Honorable Cámara de Diputados y Senado de Chile, p.: 1903-1904. Profesor de la cátedra de Derecho Penal en la Universidad de Talca

**CARRARA FRANCISCO**, Programa de Derecho Criminal, parte general, Volumen I Editorial Temis Bogotá , p 43.

**CÓDIGO PENAL ECUATORIANO** Art. 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64.

**CUENCA ESPINOZA**, CNUDMI

**DR. PÁEZ JUAN JOSÉ** en su obra "Derecho y Nuevas Tecnologías.

**ETCHEBERRY, Alfredo** "Curso de Derecho Penal", Santiago 1976, p.: 50.

**FARIÑA, Luís María** "El Derecho a la Intimidad", Madrid 1983, pp. 28. (citado por Jijena Leiva, Renato en "Chile, la protección penal de la intimidad y el delito informático")

**JIJENA LEIVA**, La protección penal a la Intimidad y el Delito Informático"Chile.

**JIJENA Leiva, Renato** "Chile, la protección penal de la intimidad y el delito informático", Editorial Jurídica de Chile, Santiago 1992, p.: 123

**LONDOÑO, Fernando** "Revista chilena de Derecho Informático" artículo "Los delitos informáticos en el proyecto de Reforma en Actual Trámite Parlamentario", Dpto. de Derecho Informático U. de Chile, Santiago 2004, p.: 173. Director Secretario Asociación de Derecho e Informática de Chile (ADI). Miembro de la Mesa de Trabajo sobre Sistemas de Nombres de Dominio en Chile.

**MAGLIONA, Claudio** "Derecho y Tecnologías de la Información" artículo "Análisis de la Normativa sobre delincuencia informática en Chile", Fundación Fernando Fueyo Laneri Universidad Diego Portales, Santiago 2002, p.: 384 Abogado, académico y consultor de empresas, servicios públicos en temas de Nuevas Tecnologías, Derecho Informático, Comercio Electrónico y Gobierno Electrónico

**MERINO Grau, Felipe** "Revista chilena de Derecho Informático" artículo "EL secreto industrial y bienes informáticos", Dpto. de Derecho Informático U. de Chile, Santiago 2004, p.: 69.

**MIR PUIG, Santiago** "Derecho Penal. Parte General", Editorial PPU, Barcelona 1985, p.: 73.

**MUÑOZ CONDE, Francisco, GARCÍA ARÁN, Mercedes,** *Derecho Penal. Parte General*, Valencia, España: Tirant Lo Blanch, 6ª, 2004, p. 205.

**PEÑARANDA, Héctor** "Derecho y Tecnologías de la Información" artículo "El Derecho Informático como rama autónoma del Derecho", Fundación Fernando Fueyo Laneri Universidad Diego Portales, Santiago 2002, p.: 73.

**POLITOFF, Sergio** "Derecho Penal", Editorial Jurídica ConoSur, Santiago 1997, p.: 53

**ZAMBRANA REYNA REGINA.** Delitos informáticos contemplados en la Ley Ecuatoriana.

## **WEBGRAFÍA**

**DIARIO EL COMERCIO** [http://www.elcomercio.com.ec/negocios/Hoy-analisis-delito-informatico-Quito\\_0\\_659334201.html](http://www.elcomercio.com.ec/negocios/Hoy-analisis-delito-informatico-Quito_0_659334201.html).

**DIARIO EL UNIVERSO.** Un promedio de siete delitos informáticos se registran por día. Domingo 26 de agosto de 2012.



<http://www.eluniverso.com/2012/08/26/1/1422/un-promedio-siete-delitos-informaticos-registran-dia.html>

**PORTAL ALIPSO.COM:** <http://www.alipso.com/> Apuntes y Monografías > Derecho > 2012.

**READ MORE:** <http://geeksroom.com/2011/04/responsabilidades-en-los-delitos-informaticos-caso-ecuador/47673/#ixzz1aLKg9Q43>

<http://www.tiposde.org/informatica/19-tipos-de-virus-informaticos/#ixzz2HKm6piJt>

# ANEXOS

**UNIVERSIDAD ESTATAL DE BOLÍVAR**  
**FACULTAD DE JURISPRUDENCIA CIENCIAS POLÍTICAS Y**  
**SOCIALES, ESCUELA DE DERECHO**

**ENCUESTA APLICADA A EMPRESARIOS, POLICÍAS, ABOGADOS,  
PERSONAS PERJUDICADAS POR LOS DELITOS INFORMÁTICOS**

**Objetivo.** Conocer la opinión de estas personas con respecto a los delitos informáticos que se cometen en la ciudad de Quito.

**Instrucciones:** Por favor conteste la siguiente encuesta, su aporte es importante en esta investigación.

**Edad ( ) Sexo M ( ) F ( )**

**CUESTIONARIO**

1. ¿De acuerdo a su opinión en Ecuador se cometen delitos informáticos?  
SI ( ) NO ( )
2. ¿¿Qué tipo de delitos informáticos son los más comunes?  
Violación al derecho de intimidad ( )  
Sabotaje ( )
3. ¿Usted ha sido víctima de falsos mensajes a través de correo electrónico?  
SI ( ) NO ( )
4. ¿En alguna ocasión sucedió con usted o con otra persona la destrucción o alteración dolosa de información por Internet?  
SI ( ) NO ( )

5. ¿Conoce si en la ciudad de Quito existen casos de piratería de software?  
SI ( ) NO ( )
6. ¿Sus cuentas bancarias o sueldos han sido violentados a través de Internet?  
SI ( ) NO ( )
7. ¿Ha tomado la decisión de establecer sus denuncias?  
SI ( ) NO ( )
8. ¿De acuerdo a su opinión Ecuador cuenta con una legislación importante para penalizar los delitos informáticos?  
SI ( ) NO ( )
9. ¿Ecuador debe Reformar el Código Penal en materia de delitos informáticos para elevar las penas y que tipifique claramente los delitos informáticos?  
SI ( ) NO ( )
10. ¿La Policía Nacional está preparada identificar con facilidad los delitos informáticos?  
SI ( ) NO



