UNIVERSIDAD INTERNACIONAL SEK

MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Plan de Investigación de fin de carrera titulado:

"METODOLOGÍA DE CLASIFICACIÓN DE DELITOS INFORMÁTICOS EN REDES SOCIALES SU TIPIFICACIÓN SEGÚN LAS LEYES DEL ECUADOR, DETERMINACIÓN DE VACIOS LEGALES Y EL PROCESO PARA PROPUESTA DE LEY"

Realizado por:

CAROL DE LAS MERCEDES RODRÍGUEZ CEVALLOS

Director de Proyecto:

MSc. LUIS FABIÁN HURTADO VARGAS

Como requisito para la obtención del título de:

MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD DE REDES Y COMUNICACIÓN

Quito, NOVIEMBRE de 2018

DECLARACIÓN JURAMENTADA

Yo, CAROL DE LAS MERCEDES RODRIGUEZ CEVALLOS, con cédula de identidad #171591526-8, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Carol de las Mercedes Rodríguez Cevallos

C.C.: 171591526-8

DECLARATORIA

El presente trabajo de investigación titulado:

"METODOLOGÍA DE CLASIFICACIÓN DE DELITOS INFORMÁTICOS EN REDES SOCIALES SU TIPIFICACIÓN SEGÚN LAS LEYES DEL ECUADOR, DETERMINACIÓN DE VACIOS LEGALES Y EL PROCESO PARA PROPUESTA DE LEY"

Realizado por:

CAROL DE LAS MERCEDES RODRIGUEZ CEVALLOS

Como requisito para la Obtención del Título de:

MAGÍSTER EN SEGURIDAD INFORMÁTICA

Ha sido dirigido por el profesor

ING. LUIS FABIÁN HURTADO VARGAS, MSc.

Quien considera que constituye un trabajo original de su autor

Ing. Luis Fabián Hurtado Vargas, MSc.

DIRECTOR

DEDICATORIA

A Dios, a mi familia, a mi querida hija Alejandra como fuente de inspiración, lucha y entrega, a las personas y compañeros que me han apoyado en este caminar estudiantil, en especial a Víctor R, Byron L, Israel M.

AGRADECIMIENTO

Al Ing. Fabián Hurtado por la dirección en el presente proyecto.

Al Ing. Edison Estrella y a la Dra. Ximena Vintimilla por sus aportes y comentarios en la investigación.

A mis docentes de la carrera por su entrega y cultivar el conocimiento.

A la Universidad Internacional SEK, por crear profesionales que dan un aporte a la sociedad.

INDICE GENERAL DE CONTENIDOS

CAPÍTULO I 1

INTRODUCCIÓN 1

1.1. PROBLEMA DE INVESTIGACIÓN 1

1.1.1. Planteamiento del problema 1

1.1.1.1. Diagnóstico 1

1.1.1.2. Pronóstico 2

1.1.1.3. Control del pronóstico 3

1.1.2. Formulación del problema 3

1.1.3. Sistematización del Problema 3

1.1.4. Objetivo General 3

1.1.5. Objetivos Específicos 4

1.1.6. Justificación 4

1.2. MARCO TEÓRICO 5

1.3. ESTADO DEL ARTE 7

1.4. ADOPCIÓN DE UNA PERSPECTIVA TEÓRICA 7

1.5. MARCO CONCEPTUAL 8

1.6. HIPÓTESIS 9

CAPITULO II 10

MÉTODO 10

2.1. TIPO DE ESTUDIO 10

2.2. MODALIDAD DE INVESTIGACIÓN 10

2.3. MÉTODO 10

2.4. SELECCIÓN DE INSTRUMENTOS DE INVESTIGACIÓN 11

2.5. VALIDEZ Y CONFIABILIDAD DE LOS INSTRUMENTOS 11

CAPITULO III 12

RESULTADOS 12

3.1. LEVANTAMIENTO DE INFORMACIÓN 12

3.1.1. Internet 12

3.1.1.1. Principios rectores para un Internet Libre y Abierto 12

3.1.1.1.1. Internet Libre y Abierto 12

3.1.1.1.2. Acceso 12

3.1.1.1.3. Gobernanza Multisectorial 14

3.1.1.1.4. Igualdad y no discriminación 14

3.1.2. Red Social 14

3.1.2.1. Concepto Matemático 14

3.1.2.2. Concepto Psicológico 16

3.1.2.3. Componentes de una red social 16

3.1.2.4. Redes sociales en línea 16

3.1.2.5. Características de redes sociales en estudio 16

3.1.2.6. Vulnerabilidades en redes sociales 18

3.1.3. Delito Informático 19

3.1.3.1. Definición de delito 19

3.1.3.2. Elementos del Delito 20

3.1.3.3. Definición de delito informático 20

3.1.3.4. Delitos Informáticos en Redes Sociales 20

3.1.3.5. Analizar clasificaciones existentes de delitos informáticos 33

3.1.3.5.1. Según La Organización de Naciones Unidas – ONU en el Informe del Décimo Congreso sobre Prevención del Delito y Tratamiento del Delincuente. Viena del 10 a 17 de abril de 2000 33

3.1.3.5.2. Según Patricia Sanz Rodríguez (2014). Redes Sociales y Derecho Penal (tesis de grado), Universidad de Valladolid. Facultad de CC. Sociales, Jurídicas y de la Comunicación. España, determina las siguientes conductas delictivas: 34

3.1.3.5.3. Según Andrea de Cea Jiménez (2012). Los delitos en las redes sociales: Aproximación a su estudio y clasificación (tesis de maestría), Universidad de Salamanca. España, determina los siguientes delitos en redes sociales: 35

3.1.3.5.4. Según Dr. Santiago Acurio Del Pino (sin año). Profesor de Derecho Informático de la PUCE, en su documento electrónico: Delitos Informáticos: Generalidades, determina los siguientes tipos de delitos informáticos:.....36

3.1.3.6. Metodología para clasificar 37

3.1.3.6.1. Etapas del análisis de clasificación.....37

3.1.3.7. Propuesta de clasificación de delitos informáticos en redes sociales 37

3.1.3.7.1. Etapa 1. Elección de variables.....37

3.1.3.7.2. Etapa 2. Elección de elementos de similitud o disimilitud. 38

3.1.3.7.3. Etapa 3. Elección del método de clasificación. 40

3.1.3.7.4. Etapa 4. Decidir y validar los grupos que formarán parte de la clasificación.40

3.1.3.7.5. Etapa 5. Validar que los elementos pertenezcan a un grupo tomando en cuenta la similitud o disimilitud entre los elementos.....40

3.1.3.7.6. Etapa 6. Análisis y resultados 41

3.1.3.8. Establecer vacíos legales.....43

3.1.3.9. Proceso para la creación de una ley 44

3.1.3.9.1. ¿Cuándo se requiere de una ley? 44

3.1.3.9.2. Iniciativa para presentar un proyecto de ley 44

3.1.3.9.3. Trámite Ordinario para la aprobación de leyes 45

CAPITULO IV 47

4.1. CONCLUSIONES.....47

4.2. RECOMENDACIONES.....49

BIBLIOGRAFÍA 50

ANEXOS 54

ANEXO A – FORMULARIO Nº 1 54

ÍNDICE DE FIGURAS

Figura 1. Usuarios de Internet y Redes Sociales en Ecuador 6
Figura 2. Cuentas Internet Fijo y Móvil por cada 100 habitantes 13
Figura 3.Grafo simple 15
Figura 4. Teoría de los 6 grados 15
Figura 5. Delitos según la ONU 33
Figura 6. Tabla de conductas delictivas según Patricia Sans Rodríguez 34
Figura 7. Tabla de Delitos Informáticos en Redes Sociales 35
Figura 8. Tipos de Delitos Informáticos según Santiago Acurio del Pino 36
Figura 9. Etapas del análisis de clasificación 37
Figura 10. Clasificación de Delitos en Redes Sociales 42
Figura 11. Trámite ordinario para la creación de leyes 46

ÍNDICE DE TABLAS

Tabla 1 Diagnóstico, síntomas y causas detectadas 2
Tabla 2 Cuentas y usuarios del servicio de acceso a internet 13
Tabla 3 Crecimiento exponencial de personas relacionadas en redes. 15
Tabla 4 Características de las redes sociales 17
Tabla 5 Delitos Informáticos en Redes Sociales 21
Tabla 6 Vacíos legales 43
Tabla 7 Convergencia/divergencia de los delitos en redes sociales según las leyes del Ecuador .48

RESUMEN

El presente trabajo utiliza el método de investigación científico deductivo, que consiste en el estudio general de delitos en redes sociales y para llegar a un conocimiento técnico – jurídico.

Durante el estudio se detecta delitos en redes sociales que afectan al software, datos, patrimonio, persona y sociedad.

Para obtener un conocimiento específico de conductas delictivas y delitos es importante desarrollar una metodología de clasificación que consiste en:

a) Elección de delitos y conductas delictivas en redes sociales, se obtiene un listado.
b) Se agrupa los delitos en redes sociales por similitud y disimilitud, se obtiene los grupos de primer nivel.
c) Se aplica el método jerárquico de clasificación.
d) Se valida los grupos encontrados, en el presente trabajo es necesario jerarquizar un segundo nivel para agrupar los delitos de manera consistente.
e) Se valida los delitos en redes sociales que pertenecen al grupo y/o subgrupo de clasificación.
f) Se obtiene la clasificación de delitos en redes sociales. Figura 10.

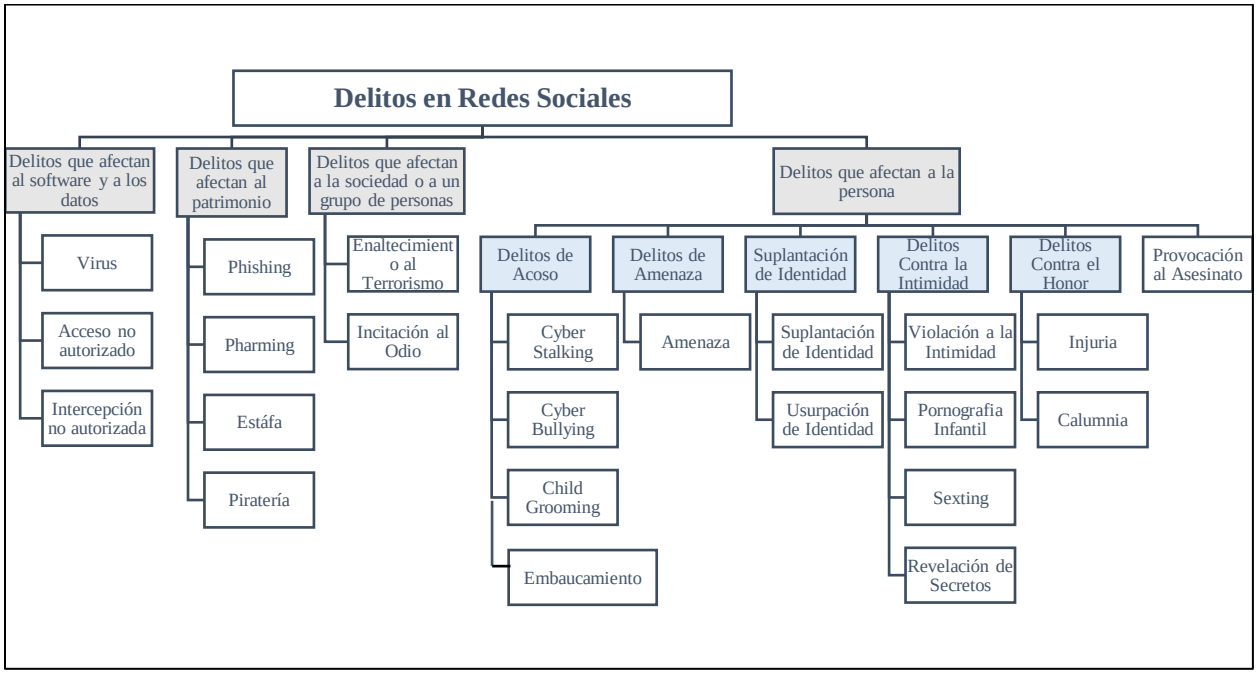


Figura 10. Clasificación de los delitos en redes sociales

Fuente: Carol Rodríguez

Las conductas delictivas y delitos detectados se contrastan con las leyes del Ecuador encontrando los siguientes vacíos legales:

Tabla 6
Vacíos legales

Conducta	Observación
Usurpación de Identidad	Se recomienda complementar el Código Orgánico Integral Penal 2014, Sección Novena, Delitos contra el derecho a la propiedad, Artículo 212
Cyber - Stalking Cibeacoso	No se encuentra tipificado como tal.
Child Grooming	No se encuentra tipificado como tal. Se recomienda complementar el Código Orgánico Integral Penal 2014, Sección Cuarta, Delitos contra la integridad sexual y reproductiva, Articulo 173
Sexting	No se encuentra tipificado como tal. Se recomienda complementar el Código Orgánico Integral Penal 2014, Sección Sexta, Delitos contra el derecho a la intimidad personal y familiar, Artículo 178
Injuria	No se encuentra tipificado como tal, el COIP lo define como calumnia.
Amenaza	No se encuentra tipificado, el COIP determina una conciliación entre el acusado y la victima en el artículo 78, numeral 4.
Phishing	No se encuentra tipificado como tal. Se recomienda complementar el Código Orgánico Integral Penal 2014, Sección Novena, Delitos contra el derecho a la propiedad, Artículo 186
Enaltecimiento al terrorismo	No se encuentra tipificado como tal.
Provocación al asesinato	No se encuentra tipificado como tal, se encuentra tipificado como acto ejecutado directamente.
Incitación al odio	Se recomienda complementar el Código Orgánico Integral Penal 2014, Sección Quinta, Delitos contra el derecho a la igualdad, Parágrafo Segundo, Delito de odio, Artículo 177

Fuente: Carol Rodríguez

Una vez que se determina los vacíos legales la presente investigación complementa con la descripción del proceso ordinario para la formulación de la Ley en Ecuador que consiste en:

a) Presentación del proyecto.
b) Calificación del Consejo de Administración Legislativa.
c) Primer debate del informe para primer debate.
d) Segundo debate del informe para segundo debate.
e) Remisión del proyecto de Ley al Presidente de la República.

Palabras claves: Delito informático, Facebook, YouTube, Twitter, trámite ordinario para creación de ley, conducta delictiva en redes sociales, clasificación de delitos en redes sociales, vacíos legales en redes sociales, Child Grooming, coacción, pharming, phishing, Sexting, amenaza, cyber acoso

ABSTRACT

The present work uses the method of deductive scientific research that is the general study of crimes on social networks and to reach law technical knowledge.

During the study we can detect cybercrimes on social networks that affect the software, data, property, person and society to get a specific knowledge of criminal behavior and crimes is important to develop a methodology of classification that consists in:

a) Choice of crimes and criminal behavior on social network, we get a list.
b) We bundle the crimes on social media by similarities and dissimilarities, we get the first level groups.
c) We apply the hierarchical classification method.
d) We validate the found groups; in the present work it is necessary to rank a second level to join the crimes in a consistent way.
e) We validate the crimes on social media that belong to the group or classification subgroup.
f) We get the social network crimes classification.

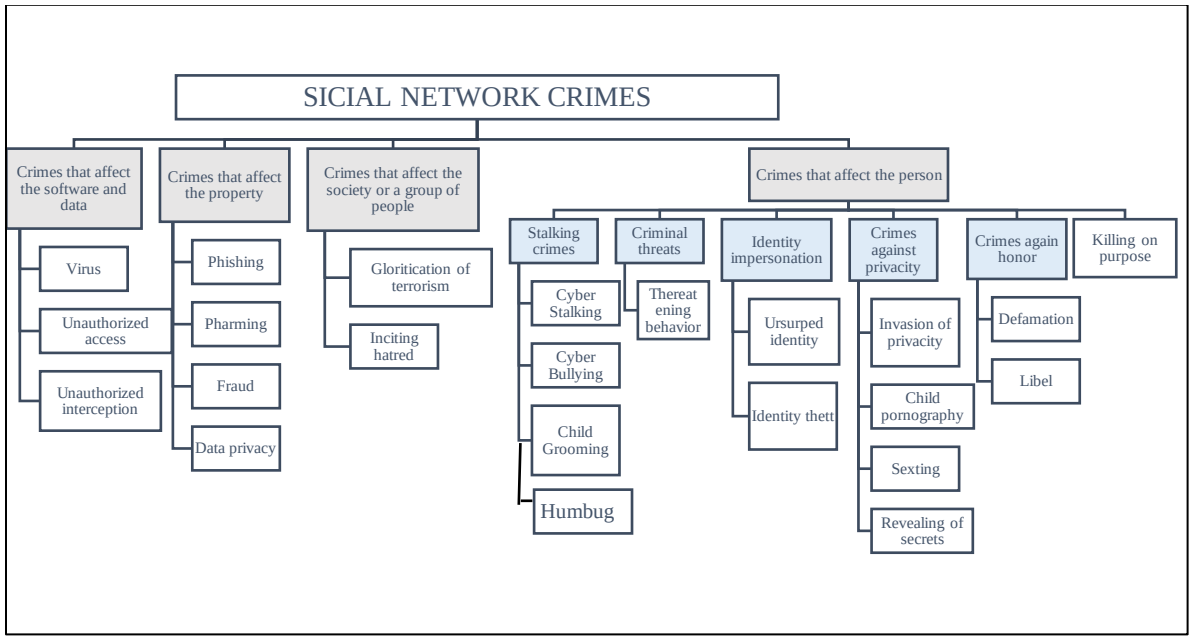


Figure 10. Classification of crimes in social networks
Source: Carol Rodríguez

The criminal behavior and detected crimes the contrast with Ecuador laws we can find the next legal vacuum:

Table 6
Empty legal

Conduct	Observation
Usurped identity	It's not typified as such It´s recommended to complement the integral criminal code 2014, Ninth Section, Crimes against property, Art 212
Cyber bulling	It's not typified as such.
Child Grooming	It's not typified as such. It´s recommended to complement the integral criminal code 2014, Fourth section, Crimes against sexual integrity, Art 173
Sexting	It's not typified as such. It´s recommended to complement the integral criminal code 2014, Sixth section, Crimes against personal and family privacy right, Art 178
Defamation	It's not typified as such, the COIP defines it as slander.
Criminal threats	It´s not typified, The COIP determines a conciliation between the accused and the victim in article 78, numeral 4.
Phishing	It's not typified as such. It´s recommended to complement the integral criminal code 2014, Ninth section, Crimes against property right, Art. 186
Glorification of terrorism	It's not typified as such.
Killing on purpose	It's not typified as such, it is typified as an act executed directly
Inciting hatred	It´s recommended to complement the integral criminal code 2014, Fifth section, Crimes equal right second paragraph, Hatred crime, Art. 177

Source: Carol Rodríguez

Once determined, the legal vacuum the present investigation complements with the description of the ordinary process to the formulation of Ecuador´s law which consists in:

a) Project presentation.
b) Qualification of the legislative administration council.
c) First debate from the report to first debate.
d) Second debate from the report to second debate.
e) Remission from the project of law to the Republic President.

Key words

Cybercrime, Facebook, YouTube, Twitter, Ordinary procedure to law creation network, Criminal behavior on social network, Qualification of social network crimes legal vacuum on social networks, Child grooming, Coercion, Pharming, Phishing, Sexting, threat, Cyber bullying

CAPÍTULO I

INTRODUCCIÓN

1.1. PROBLEMA DE INVESTIGACIÓN

1.1.1. Planteamiento del problema

El internet es un medio que se lo utiliza para comunicación, consulta, fuente para la obtención de información, para transacciones financieras, realización de trámites e interacción humana a través de medios electrónicos. El internet como medio de comunicación acarrea muchas ventajas, inconvenientes y peligros, como el desvanecimiento de la privacidad, delitos relacionados a la economía, imagen personal, propiedad intelectual, etc.

Cualquier persona que disponga de un ordenador, tablet, celular o cualquier dispositivo electrónico con acceso a internet puede subir información a la web inclusive de manera anónima, lo que puede ocasionar problemas de falsedad.

Al ser la web un ámbito muy extenso se ha decidido limitar su estudio a las redes sociales de Facebook, Twitter y YouTube, ya que éstas son las de mayor uso e influencia entre los usuarios. Otra razón es que este tipo de redes son un blanco fácil para el cometimiento de delitos por ese motivo se considera importante conocer que peligros se esconden detrás de estas formas de comunicación.

Se ha detectado una falta de conocimiento sobre los delitos informáticos en redes sociales.

Falta de legislación para sancionar vacíos legales en redes sociales que se presentan en el Ecuador.

1.1.1.1.Diagnóstico

En la siguiente tabla se muestra los síntomas y causas detectadas.

Tabla 1
Diagnóstico, síntomas y causas detectadas

SINTOMAS	CAUSAS
Falta de conocimiento en la sociedad de los delitos en redes sociales.	El Estado no difunde adecuadamente las leyes.
Falta de una adecuada clasificación de los delitos que se presentan en redes sociales actualmente en el Ecuador.	La legislación no se actualiza conforme el avance tecnológico.
Falta de legislación que contemple actos no adecuados o inmorales que se presentan en redes sociales.	

Fuente: Carol Rodríguez

Muchos casos de delitos informáticos quedan en la impunidad por falta de conocimiento de una ley que lo sanciona y únicamente en el 2016 se presentaron en la Fiscalía General del Estado del Ecuador 530 denuncias de delitos informáticos.

Los delitos informáticos se encuentran tipificados en Código Orgánico Integral Penal COIP, sin embargo, no se determina en el mismo una clasificación de éstos en redes sociales. Se encuentra actualmente un suplemento de delitos en el Código Orgánico Integral Penal que contempla nuevos artículos como el Artículo. 35. Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos.

La Ley Orgánica de Comunicaciones en el Artículo. 4. Sobre contenidos personales en internet menciona "Esta ley no regula la información u opinión que de modo personal se emita a través de internet", es decir que no la regula y deja a manos del COIP la sanción frente a un delito.

El avance tecnológico se da a pasos agigantados lo que ocasiona que en cortos periodos de tiempo aparezcan nuevas formas de cometer actos inmorales que conllevan a detectar vacíos legales. Esta particularidad el Estado debe concientizar para que legisle de acuerdo al avance tecnológico.

1.1.1.2.Pronóstico

La existencia de vacíos legales en el campo de los delitos relacionados con redes sociales se debe promover a través del: Ejecutivo, Legislativo o la Población Civil, la creación de una ley que sancione dichos actos.

La falta de evaluación de la ley y desconocimiento de los legisladores no permite que las leyes sean reformadas y por tanto exista inequidad en su aplicación.

1.1.1.3.Control del pronóstico

La clasificación de los delitos informáticos en redes sociales ofrece una herramienta a los legisladores para la creación de nuevas normativas.

La evaluación de las normativas existentes concebirá leyes más justas y acordes a los hechos y al avance tecnológico.

1.1.2. Formulación del problema

Según el INEC, en la Encuesta Nacional de Empleo Desempleo y Subempleo – ENEMDU (2010-2014) el 32,4% de los hogares a nivel nacional tienen acceso a internet fijo. Según publicación de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), en su página web www.acotel.gob.ec, la penetración de internet móvil en Ecuador es del 52.72% para el año 2018. El acceso a los servicios de internet está incrementándose convirtiéndose en un blanco fácil para el cometimiento de delitos, por lo que es necesario revelar y describir cuales son los peligros que pueden llevarse a cabo a través de estos medios.

El cometimiento de actos no tipificados en la ley, deben legislarse con el objeto que no queden en la impunidad y sean sancionados.

1.1.3. Sistematización del Problema

Las preguntas directrices que nos ayudan a abordar diferentes ángulos del problema son:

- ¿Existe modelos de clasificación de delitos informáticos en redes sociales que colaboren a la expedición de leyes en el Ecuador?
- ¿Qué actos descritos en la clasificación de delitos informáticos no están tipificados en las leyes del Ecuador?
- ¿Qué procedimiento existe para la formulación de una ley que nazca como iniciativa de la sociedad civil?
- ¿Los delitos informáticos en redes sociales reconocidos por la Organización de Estados Americanos OEA, son legislados por el Ecuador?

1.1.4. Objetivo General

Desarrollar una metodología de clasificación de delitos informáticos en redes sociales tipificados según las leyes del Ecuador, para la determinación de vacíos legales y el proceso de propuesta de ley.

1.1.5. Objetivos Específicos

- Detectar los delitos informáticos en redes sociales y desarrollar un modelo de clasificación mediante referentes de otros estudios afines.
- Tipificar los delitos informáticos en redes sociales según las leyes en Ecuador.
- Determinar vacíos legales.
- Describir el proceso para crear la ley en Ecuador como propuesta de la sociedad civil, que cubra los vacíos legales de los hallazgos encontrados en redes sociales.

1.1.6. Justificación

Las redes sociales en Internet es el medio más utilizado para interconectarse e interactuar y sus usuarios se han convertido en un blanco fácil para el cometimiento de delitos, por lo que es necesario revelar los peligros y describir cuales son los delitos que pueden llevarse a cabo a través de estos medios.

La justicia es el supremo ideal que consiste en la voluntad firme y constante de dar a cada uno lo suyo. Pena, castigo o fallo acerca de la culpa o inocencia de un acusado. Caballenas, G. (2011)

La ley es una regla, norma, precepto de la autoridad pública, que manda, prohíbe o permite algo. Todo reglamento, ordenanza, estatuto, decreto, orden u otro mandamiento de una autoridad en ejercicio de sus atribuciones. Caballenas, G. (2011)

Se concluye que no se da justicia, si no existe ley. El ideal humano es encontrar justicia con igualdad, sin perder la equidad en la aplicación de la ley.

La legislación ecuatoriana en algunos artículos tipifica los delitos informáticos, sin embargo, no es suficiente porque con el avance tecnológico se genera otras infracciones, las cuales deben de legislarse para que no quede en la impunidad.

La tipificación de los delitos en redes sociales en la ley ayuda a la autoridad competente a aplicar la sanción correspondiente y la observancia de vacíos legales.

Por lo citado anteriormente el presente trabajo será un apoyo para todo el Sistema Jurídico del Ecuador.

Cabe mencionar que la investigación a desarrollar es documental ya que, a través de la observación, consulta, lectura de fuentes de documentos y materiales bibliográficos se recabará datos e información existente, partimos de estudios afines para realizar una clasificación que cubra actos que no se encuentran tipificados en la ley.

Con el presente proyecto de investigación se beneficiará en los siguientes campos:

Técnico

- Se tendrá conocimiento de los delitos informáticos que se presentan en redes sociales.
- Aporte para futuros trabajos respecto al tema.

Jurídico

- La clasificación de los delitos informáticos en redes sociales servirá de referente para detectar vacíos legales.
- Se contará con leyes que cubra todos los delitos informáticos en redes sociales.

Social

- Para conocimiento de los delitos informáticos en redes sociales y la ley que lo sanciona.
- A la sociedad, porque existirán leyes aplicables y que no exista impunidad en actos que estén fuera del buen convivir humano.

1.2. MARCO TEÓRICO

Ley Orgánica de Comunicaciones

En el Ecuador existe la Ley Orgánica de Comunicación, Tercer Suplemento, Registro Oficial Nº22 en el "Art.4.- "Contenidos personales en internet. Esta ley no regula la información u opinión que de modo personal se emita a través de internet. Esta disposición no excluye las acciones penales o civiles a las que haya lugar por las infracciones a otras leyes que se comentan a través del internet".

Usuarios de Internet y Redes Sociales en Ecuador.

- El 32,4% de los hogares a nivel nacional tienen acceso a internet
- El 35,2% de las personas usó Internet como fuente de información, mientras el 39,9% lo utilizó como medio de comunicación en general.

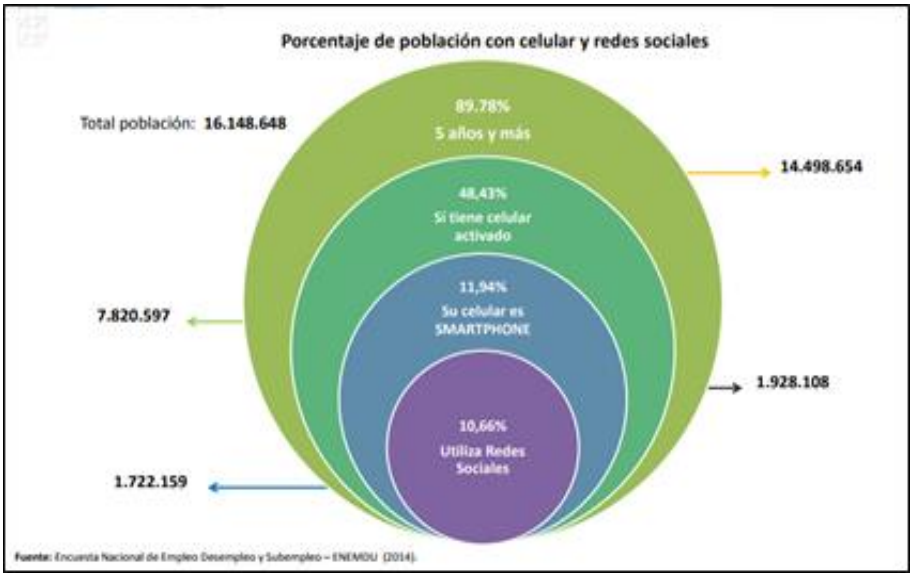


Figura 1. Usuarios de Internet y Redes Sociales en Ecuador

Fuente: Encuesta Nacional de Empleo Desempleo y Subempleo – ENEMDU (2014).

En el año 2016 se presentaron en la Fiscalía General del Estado del Ecuador 530 denuncias de delitos informáticos. En las provincias de Guayas hubo 18 casos; en Pichincha, 145; en Manabí, 24; en El Oro, 22. La mayoría de denuncias (368) concierne al delito de "apropiación fraudulenta por medios electrónicos". Un estudio hecho por la Policía Nacional, Interpol, el centro de respuesta a Incidentes Informáticos de Ecuador (Ecucert), con el soporte de organismos similares de América Latina, indica que el 85% de los ataques a los sistemas informáticos son ocasionados por errores de los consumidores, quienes no toman adecuadas medidas al acceder a las redes sociales, medios de comunicación como el correo electrónico y en el uso de usuario y contraseña según, El Telégrafo (2016).

Para sancionar un delito informático en el Ecuador se cuenta con el Código Orgánico Integral Penal (COIP) que entró en vigencia el 10 de agosto de 2014, Código Civil y la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

En la norma penal ecuatoriana está el derecho a la intimidad personal y familiar. Quien lo viole puede ser sancionado con prisión de uno a tres años, refiere el art. 178 del Código Orgánico Integral Penal.

Un ejemplo de la aplicación de leyes referentes a delitos en redes sociales es: "Jeannine Cruz que cumplió en marzo de 2016 una sentencia de 30 días de prisión por haber proferido expresiones

en descrédito o deshonra del alcalde Bolívar Castillo". La figura está en el artículo 396 del COIP. Lo mismo sucedió con Sebastián Cevallos, tuitero y dirigente de Unidad Popular, quien fue sentenciado a 15 días de prisión por sus tuits en contra del exministro Carlos Carrasco según, El Comercio (2016)

1.3. ESTADO DEL ARTE

Se localizó una propuesta de clasificación de los delitos en redes sociales en el trabajo de Fin de Master "Los delitos en redes sociales: aproximación a sus estudio y clasificación" por Cea Jiménez. A (2012).

El sr. Ex –presidente Rafael Correa propuso el 23 de mayo de 2017 un proyecto de LEY QUE REGULA ACTOS DE ODIO EN REDES SOCIALES E INTERNET, el que contiene 10 artículos. La normativa propone que los proveedores de servicios de redes sociales elaboren un informe trimestral en lengua castellana sobre la gestión de los reclamos o reportes sobre contenido ilegal que presenten los usuarios. Asamblea Nacional (2017).

Se menciona en Cabrera, M. (2014) acerca de la apropiación ilícita de redes sociales mediante la manipulación de claves de acceso personal como consecuencia de la falta de tipificación del delito informático en la legislación penal ecuatoriana.

Se analiza en Lanza, E. (2016). Estándares para una Internet libre, abierta e incluyente/ Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos. Editorial OEA

República Del Ecuador Asamblea Nacional (2014), Código Orgánico Integral Penal (COIP) se analiza los delitos informáticos que se encuentran tipificados en Ecuador.

Se localizó en Salazar, L., & Mauricio, A. (2016). Análisis de los delitos informáticos y de telecomunicaciones en el Ecuador bajo las nuevas formas jurídicas.

Con la visión específica se puede evidenciar que no existen trabajos relacionados y realizados en Ecuador, lo cual obstaculiza la aplicabilidad de las leyes en ciertos delitos en redes sociales aún no identificados.

1.4. ADOPCIÓN DE UNA PERSPECTIVA TEÓRICA

La investigación documental ayuda a través de la observación, consulta, lectura de fuentes de documentos y materiales bibliográficos a recabar datos e información existente, partimos de clasificaciones existentes e información de fuentes oficiales referente al tema de organismos a

nivel internacional como la Organización de Naciones Unidas y el Consejo de Europa para proceder a desarrollar un modelo de clasificación.

Se emplea la Normativa Legal en Ecuador, en este caso el código Orgánico Integral Penal (COIP) sobre delitos informáticos.

Para los vacíos legales que se detecten en el Ecuador existe procedimientos con los cuales se puede proponer una normativa legal que según Pérez Bustamante & Ponce (2014), puede ser presentada a través de:

- Los asambleístas con el apoyo de una bancada legislativa o de al menos el cinco por ciento de sus miembros
- El Presidente de la República
- Las otras funciones del Estado en los ámbitos de su competencia
- La Corte Constitucional, la Procuraduría General del Estado, la Fiscalía General del Estado, la Defensoría del Pueblo y la Defensoría Pública, en las materias que les corresponda.
- Los ciudadanos y organizaciones sociales que cuenten con el respaldo de por lo menos el cero punto veinticinco por ciento de los inscritos en el padrón electoral nacional.

1.5. MARCO CONCEPTUAL

El punto de partida es en base a la sustentación teórica que se apoya en fuentes bibliográficas para la obtención de conocimiento.

Internet libre y abierto

Se refiere a tener acceso a información y aplicaciones legales mediante el uso del Internet de forma completa, veraz y oportuna sin interferencias, bloqueos o con mecanismos de intercepción de paquetes que viajan en la red.

Redes Sociales

Las Redes Sociales pueden definirse como un conjunto bien delimitado de actores, grupos, organizaciones, comunidades, sociedades globales, etc.- vinculados unos a otros a través de una relación o un conjunto de relaciones sociales. Mitchell (1969:2)

Delito Informático

Los delitos informáticos se los define como cualquier actividad delictiva en la que se utilizan como herramienta los computadores y redes, o éstos son las víctimas de la misma, o bien el medio

desde donde se efectúa dicha actividad delictiva; se refieren a los actos dirigidos contra la confidencialidad, integridad y la disponibilidad de los datos y sistemas informáticos. Consejo de Europa - CdE. (2001).

¿Qué es clasificar?

Es la actividad de agrupar y organizar elementos con características similares o que comparten un mismo patrón, ayudan a la representación formalizada de contenido y eliminan la redundancia.

Dentro de las formas de clasificar se encuentran los métodos jerárquicos y asociativas.

Elementos de una clasificación jerárquica

- Objeto principal. - Asociación en la que se muestran agrupado los objetos.
- Objeto auxiliar. - Ayudan a especificar los objetos a través de características intrínsicas como forma, color, tiempo, etc.
- Código o notación. - conjunto de signos que identifican de forma individual a los objetos.
- Índice. - lista de objetos de la clasificación.

1.6. HIPÓTESIS

El desarrollo de un modelo de clasificación de delitos informáticos en redes sociales mediante las leyes del Ecuador, nos lleva a determinar vacíos legales los cuales pueden ser plasmados en un proyecto de ley en el Ecuador.

CAPITULO II

MÉTODO

2.1. TIPO DE ESTUDIO

Para el presente trabajo se ha elegido el método exploratorio y descriptivo.

Exploratorio

Se emplea el estudio exploratorio ya que el presente trabajo nos da una visión general sobre la clasificación de los delitos informáticos.

Este estudio incrementará el grado de familiaridad de las leyes a los usuarios de redes sociales.

Descriptivo

El presente trabajo se apoya en un nivel de estudio descriptivo debido a que se detalla la clasificación o categorización de los delitos en redes sociales.

2.2. MODALIDAD DE INVESTIGACIÓN

Documental

La investigación a desarrollar es documental:

- Lectura de materiales bibliográficos como tesis, publicaciones que expongan sobre clasificaciones existentes de delitos informáticos.
- Información de fuentes oficiales como la Organización de Naciones Unidas y el Consejo de Europa a través de sus publicaciones referentes al tema.
- Lectura y comprensión del Código Orgánico Integral Penal y la determinación de vacíos legales.
- Lectura sobre procedimientos para la presentación de una propuesta de ley.

2.3. MÉTODO

Método Inductivo-Deductivo

La inducción es un procedimiento por medio del cual se pasa del conocimiento de casos particulares a un conocimiento más general, siendo esto clave para la formulación de hipótesis.

La deducción es un procedimiento, mediante el cual se pasa de un conocimiento general a otro de menor nivel.

2.4. SELECCIÓN DE INSTRUMENTOS DE INVESTIGACIÓN

El instrumento que se utilizará para la investigación tiene como función esencial obtener información que se convertirá luego en resultados relevantes.

Análisis Documental

Se analizará y estudiará las fuentes bibliográficas de las investigaciones realizadas y relacionadas con el proyecto.

Encuesta

Se realizará preguntas específicas a la sociedad, a fin de extraer información sobre el conocimiento de delitos informáticos y la ley que lo sanciona.

Entrevista

Se realizará una conversación con abogados, fiscales y jueces con el objeto de obtener y extraer la información relevante sobre conocimientos de vacíos legales que existiesen al aplicar las leyes en delitos informáticos en redes sociales.

2.5. VALIDEZ Y CONFIABILIDAD DE LOS INSTRUMENTOS

El instrumento de preguntas de la entrevista va a ser validado por conocedores en el ámbito legal como los abogados, fiscales y jueces.

La validez del instrumento de tesis es aceptada por un comité de tesis o tribunal de tesis.

El instrumento de paper es validado por la institución que realiza la publicación.

El instrumento de expediente judicial es obtenido como fuente segura de información.

CAPITULO III

RESULTADOS

3.1. LEVANTAMIENTO DE INFORMACIÓN

3.1.1. Internet

Internet procede de las palabras en inglés Interconnected Networks, que significa “redes interconectadas”. Se podría decir que Internet es la unión de todas las redes y computadoras distribuidas por todo el mundo y se define como una red global en la que se conjuntan todas las redes.

3.1.1.1. Principios rectores para un Internet Libre y Abierto

3.1.1.1.1. Internet Libre y Abierto

Se refiere a que las transferencias de la información entre dos puntos de la red no pueden ser interceptados, manipulados, monitoreados, ralentizados por el proveedor del servicio.

El estado ecuatoriano garantiza este principio a través de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

3.1.1.1.2. Acceso

El acceso hace referencia al cerrar la brecha digital. Esta brecha digital se entiende como acceso a la infraestructura de internet y alfabetización digital.

En Ecuador existe el fondo para el desarrollo de las telecomunicaciones rurales que según resolución del CONATEL 394, Registro Oficial 193 de 27 de octubre de 2000 que, el artículo 58 de la Ley para la Transformación Económica del Ecuador reforma el artículo 38 de la Ley Especial de Telecomunicaciones y establece que todos los servicios de telecomunicaciones se brindarán en régimen de libre competencia; y, dispone que el Consejo Nacional de Telecomunicaciones, en uso de sus facultades, expedirá el reglamento pertinente, el que deberá contener las disposiciones necesarias para la creación de un fondo para el desarrollo de las telecomunicaciones en las áreas rurales y urbano - marginales, con aportes que se determinen en función de los ingresos de las empresas operadoras de telecomunicaciones. Arcotel (2000).

Estadísticamente la brecha digital en Ecuador se encuentra de la siguiente manera:

Tabla 2
Cuentas y usuarios del servicio de acceso a internet

Cuentas Internet Fijo y Móvil									
Año	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
Internet Fijo	3,35%	4,47%	5,98%	6,88%	8,25%	9,16%	9,76%	10,61%	11,07%
Internet Móvil	2,35%	10,48%	22,15%	26,66%	30,79%	34,97%	47,04%	52,50%	52,72%

Fuente: SIETEL-ARCOTEL

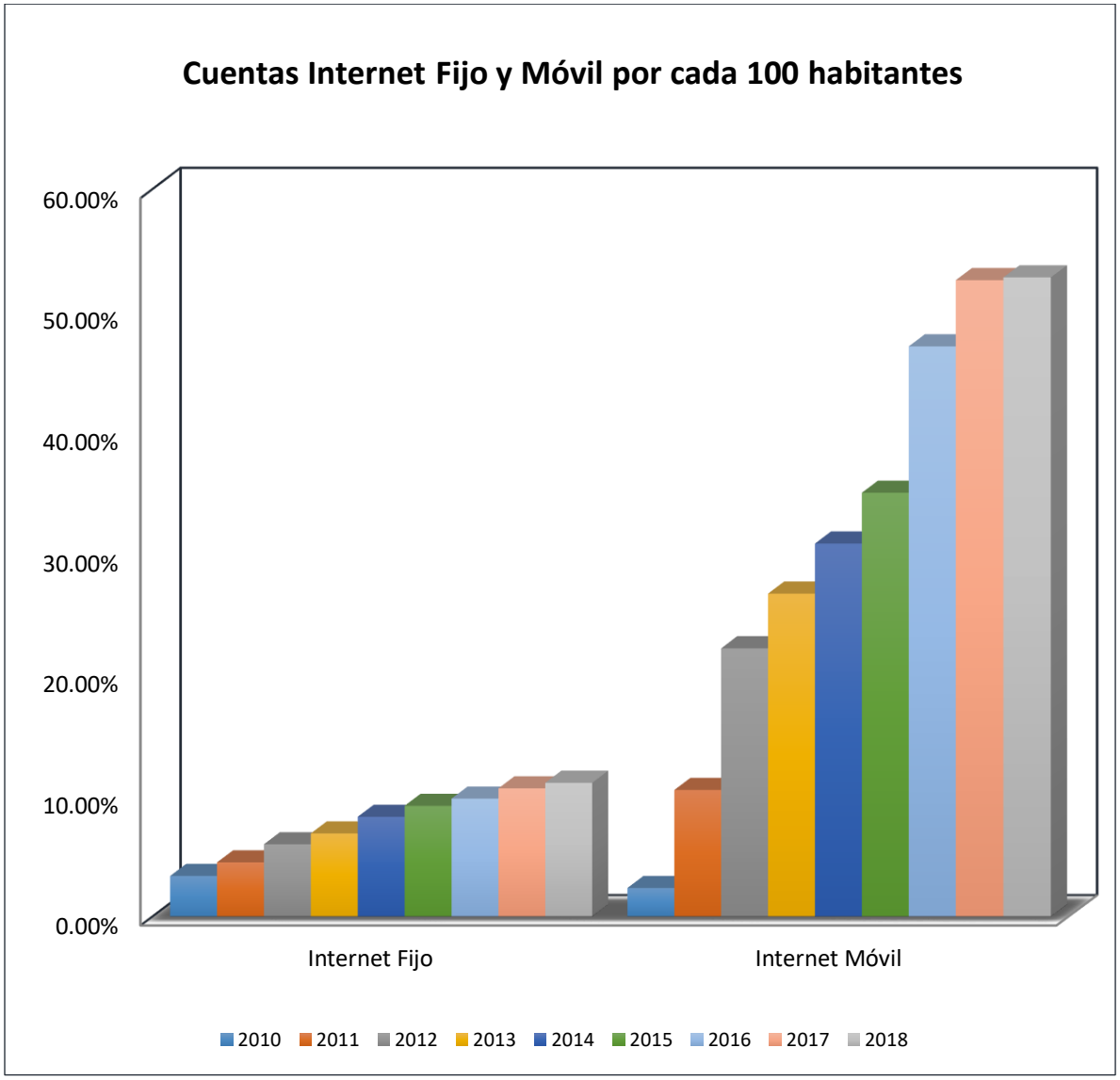


Figura 2. Cuentas Internet Fijo y Móvil por cada 100 habitantes

Fuente: SIETEL-ARCOTEL (jun 2018) obtenido de http://www.arcotel.gob.ec/servicio-acceso-internet/

En Ecuador desde el año 2010 ha creado en áreas rurales y urbano marginales centros comunitarios de internet, los cuales son utilizados sin costo para los usuarios, por tanto, el estado hace un esfuerzo importante para garantizar el acceso universal a internet.

Respecto a la pluralidad lingüística en el ámbito de internet Ecuador no ha incursionado, debido a que no existen contenidos en la red en los idiomas nativos como por ejemplo el Quichua.

3.1.1.1.3. Gobernanza Multisectorial

Se refiere a que las políticas sobre el transporte de datos y el uso de internet debe ser un consenso entre los actores, ya sean: gubernamental, privados, sociedad civil, universidad. En Ecuador la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) lleva procesos para la expedición de resoluciones, entre una de las actividades de los procesos es llevar a cabo consultas públicas en las cuales se debate las normas que rigen.

3.1.1.1.4. Igualdad y no discriminación

Las personas somos iguales ante la ley, lo que implica que no se debe discriminar por motivos de: edad, raza, sexo, idioma, religión, opinión política, índole económica, discapacidad, nacionalidad y condición social. En este contexto el uso de internet en Ecuador se ve afectado por la existencia de grupos sociales quichua hablantes ya que los contenidos en su mayoría no contemplan para este idioma.

3.1.2. Red Social

3.1.2.1. Concepto Matemático

La Teoría de Grafos, expone que la red se compone por nodos conectados por aristas, donde los nodos son los sujetos y las aristas, las relaciones que les unen. Kuz, A., Falco, M., & Giandini, R. (2016).

Las redes sociales como Facebook, Twitter y otros, son una aplicación a la teoría de grafos en donde los actores mantienen relaciones con sus adyacentes.

Ejemplo de grafo en la Figura 3.

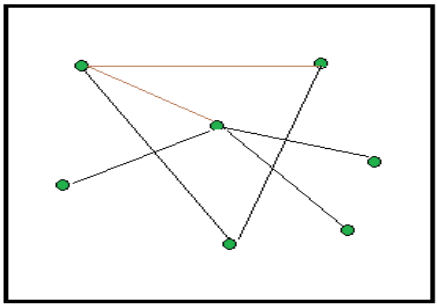


*Figura 3.*Grafo simple

Fuente: Carol Rodríguez

Teoría de los 6 grados

La “Teoría de los Seis Grados de Separación” como se interpreta en la Figura 4, establece que cualquier persona del planeta está conectada con cualquier otra, a través de una cadena de conocidos con no más de cinco eslabones o puntos de unión. López, R. (2015).

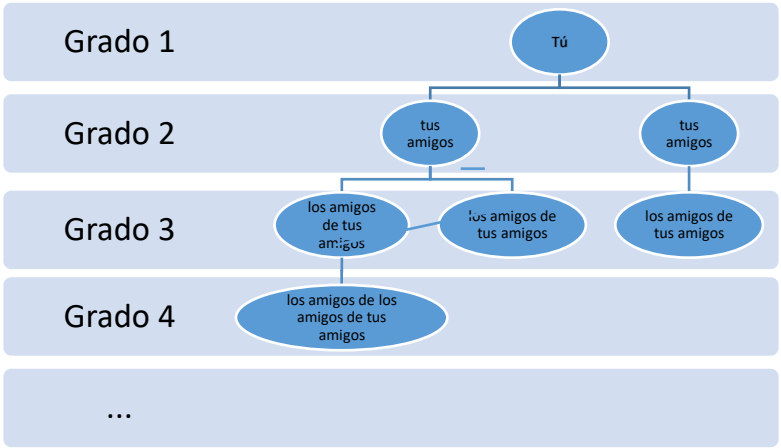


Figura 4. Teoría de los 6 grados

Fuente: Carol Rodríguez

Por ejemplo:

Tabla 3
Crecimiento exponencial de personas relacionadas en redes.

1 persona	100 conocidos	100 relaciones	Nivel 1
100 personas	100 conocidos	10000 relaciones	Nivel 2
10000 personas	100 conocidos	1000000 relaciones	Nivel 3
1000000 personas	100 conocidos	100000000 relaciones	Nivel 4
…	…	…	…

Fuente: Carol Rodríguez

Como puede observarse las relaciones crecen exponencialmente, en teoría una persona puede relacionarse con cualquier otra persona en el mundo con un máximo de 6 niveles.

3.1.2.2. Concepto Psicológico

Las Redes Sociales pueden definirse como un conjunto bien delimitado de actores -individuos, grupos, organizaciones, comunidades, sociedades globales, etc.- vinculados unos a otros a través de una relación o un conjunto de relaciones sociales. Mitchell (1969:2).

Las redes sociales online permiten a los usuarios interactuar entre sí, compartiendo información personal y generando relaciones afines como deporte, ciencia, literatura, ocio, etc.

3.1.2.3. Componentes de una red social

(i) Actores: entidades sociales, individuos, empresas.

(ii) Lazos: son los vínculos o relaciones entre pares de actores.

(iii) Sistema de vinculación: tipos de relaciones entre los actores como trabajo, ocio, estudios, etc.

3.1.2.4. Redes sociales en línea

Los usuarios a partir de la etapa de la web 2, dejaron de ser observadores para convertirse en generadores y consumidores de información.

Son servicios de comunicación a través de internet que permite a los usuarios crear un perfil con datos personales e interactuar.

El director del Laboratorio de Redes Sociales del Lab-RSI, Luis Fernández, estipula que se trata de “espacios virtuales organizados para desarrollar proyectos, integrar comunidades de otra manera, poner en pie servicios que de otra manera no existirían, tomar decisiones en tiempos complejos y proyectarse hacia el mercado global usando toda la potencia de la virtualidad”. Fernández (2008).

3.1.2.5. Características de redes sociales en estudio

En la Tabla 4. Se muestra características de las redes sociales determinadas para el estudio del presente trabajo.

Tabla 4
Características de las redes sociales

CARACTERÍSTICAS	FACEBOOK	TWITTER	YOUTUBE
Facilidad en la creación de cuenta.	✓	✓	✓
Facilidad en la creación y edición de perfiles.	✓	✓	✓
Configuración de limitaciones de acceso (autorizaciones).	✓		
Creación y pertenencia a un grupo o canal.	✓		✓
Permite elegir el hacer o no público información personal como: fecha de nacimiento, domicilio, estado civil, sexo, profesión, aficiones, etc.	✓		
Realiza los contenidos en forma pública o privada.	✓	✓	✓
Se transmite información de manera direccional y multidireccional.	✓	✓	
Permite localizar amistades por medio del correo electrónico, nombre, apellido e invitaciones.	✓	✓	✓
Los usuarios pueden seguir a otros usuarios.	✓	✓	✓
Permite al usuario publicar fotos y crear álbumes.	✓	✓ Publicar fotos	
Permite ingresar descripciones en las fotos.	✓		
Permite etiquetar fotos.	✓		
Permite a los usuarios subir o publicar videos.	✓	✓	✓
Permite a los usuarios visualizar videos.	✓	✓	✓
Permite a los usuarios publicar comentarios.	✓	✓	✓
Integra el chat.	✓		
Comunicación en tiempo real.	✓	✓	
Permite la integración de mensajes y correo electrónico.	✓		
Dispone a aplicaciones como juegos, test, etc.	✓		
Dinamismo del sitio, muestra actualizaciones de los amigos como estado, eventos, publicación de fotos, creación de grupo, etc.	✓		
Denuncia de mensajes, publicaciones o usuarios.	✓	✓	✓
Búsqueda de videos.			✓
Copyright (derechos de autor).			✓

No requiere de una cuenta para visualizar videos.			✓
Plataforma publicitaria.	✓	✓	✓
Información basada en microbloggin con el envío de caracteres limitados.		✓	
Limita la funcionalidad en cuentas que denoten comportamientos inadecuados.		✓	
Suspensión total de la cuenta por no mostrar mejora en comportamientos inadecuado.	✓	✓	
Permite silenciar palabras específicas de publicaciones.		✓	
Permite organizar los tweets según nivel de importancia que se le asigne.		✓	
Permite la generación de encuestas, con respuestas anónimas.		✓	
Muestra estadísticas sobre los perfiles de las actividades de los tweet, seguidores, tarjetas de twitter.		✓	

Fuente: Carol Rodríguez

3.1.2.6. Vulnerabilidades en redes sociales

En el Ecuador la evolución del acceso a internet por medio de dispositivos móviles se encuentra en 52.72% a junio de 2018 frente al 11,07 % de acceso por dispositivos fijos según ARCOTEL www.arcotel.gob.ec, se puede observar que el ingreso a la plataforma se la realiza a cualquier hora y lugar.

Los usuarios a través de las plataformas de Facebook, Twitter y YouTube se han convertido en generadores y consumidores de información incrementando la probabilidad de ser atacados.

Los ciberdelincuentes encuentran en éstas plataformas sociales una fuente muy valiosa de información para cometer ataques de: robo de información, envío de correos maliciosos, ingeniería social, infiltración, manipulación de información, etc.

Entre las principales vulnerabilidades detectadas se determinan:

1. **Abreviación de enlaces:** los hackers aprovechan los servicios de abreviación de enlaces para incluir código malicioso como el malware, permitiendo que los usuarios no se den cuenta que están haciendo clic para ejecutar una instalación.
2. **Acoso a menores de edad:** las plataformas como Facebook, Twitter, YouTube y otras,

facilitan a los usuarios a utilizar estos servicios para el cometimiento de acoso (cyberbulling), grooming, sexting.

3. **Amenazas avanzadas persistentes:** es un conjunto de técnicas y programas diseñados para atacar a una organización, manteniéndose oculto en el sistema atacado cuyo objetivo es el espionaje, robo, manipulación de información sensible y control de la infraestructura.
4. **Botnets:** toma el control de la máquina atacada a la espera de la instrucción del robot principal para el cometimiento de actos ilícitos.
5. **Confianza:** cuando existen mensajes o enlaces populares de sus amigos, los usuarios tienden a confiar en la ejecución y visualización del mismo.
6. **Cruce de páginas web**: este tipo de ataques aprovechan la confianza que brindan las aplicaciones al ingresar en el buscador de los usuarios, se origina el cruce cuando se comparte una imagen en una secuencia de eventos, otros usuarios podrán hacer clic para difundirlo.
7. **Impostores:** la colecta se seguidores facilita el cometimiento de actos ilícitos como hacerse pasar por uno de ellos.
8. **Infiltración de información**: Los usuarios comparten información acerca de la organización, proyectos, productos, finanzas, escándalos y otra información importante en las redes.
9. **Phishing Bait**: Mail direccionado que lleva al usuario a ingresar a su cuenta de Facebook para que el hacker extraiga su contraseña esperando que no se identifique la página en su buscador.
10. **Virus de redes sociales**: A través de robots informáticos, los hackers toman el control de los ordenadores enviándoles correos no deseados que incitan ingresar a enlaces, los cuáles son controlados para el robo de información.

3.1.3. Delito Informático

3.1.3.1. Definición de delito

La Real Academia de la Lengua define el vocablo delito, como la acción u omisión voluntaria castigada por la ley con pena grave. En latín delito, es "delictum" palabra que sugiere un hecho contra la ley, un acto doloso que se castiga con una pena.

Según (Código Orgánico Integral Penal 2014), Título I, La Infracción Penal En General Delito, **Artículo 19.- Clasificación de las infracciones**. – "Las infracciones se clasifican en delitos y contravenciones.

Delito es la infracción penal sancionada con pena privativa de libertad mayor a treinta días.

Contravención es la infracción penal sancionada con pena no privativa de libertad o privativa de libertad de hasta treinta días".

3.1.3.2. Elementos del Delito

Tres son los elementos que definen al delito:

- El sujeto que rompe o destruye la norma jurídica y que se llama delincuente.
- El objeto o derecho violado.
- El fin que es la perturbación del orden jurídico.

Elementos del delito en el COIP y determinación de la pena

- Conducta: acción u omisión que ponga en peligro o produzca un resultado lesivo.
    - Tipicidad: Conducta se adecua a los elementos descritos en el tipo penal.
    - Antijuridicidad: Amenace o lesione, sin justa causa un bien jurídico protegido.
    - Culpabilidad: conocimiento o desconocimiento de la ley.

3.1.3.3. Definición de delito informático

Los delitos informáticos se los define como cualquier actividad delictiva en la que se utilizan como herramienta los computadores o redes, o éstos son las víctimas de la misma, o bien el medio desde donde se efectúa dicha actividad delictiva; se refieren a los actos dirigidos contra la confidencialidad, integridad y la disponibilidad de los datos y sistemas informáticos. Consejo de Europa - CdE. (2001).

3.1.3.4. Delitos Informáticos en Redes Sociales

Tabla 5
Delitos Informáticos en Redes Sociales

ACTO	DESCRIPCIÓN	TIPIFICACION LEYES ECUADOR	SE PRESENTA EL ACTO EN REDES SOCIALES
Acceso no autorizado	Persona que sin autorización ingresa a un sistema y realiza desvío de información y ofrece servicios a terceros sin el consentimiento de los proveedores legítimos.	Según (Código Orgánico Integral Penal 2014), Sección Tercera, Delitos contra la seguridad de los activos de los sistemas de información y comunicación **Artículo 234.- "Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. –** La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años".	SI
Amenaza	Propósito de causar daño a la persona, familia o bienes, esta exteriorización de causar un mal debe ser solapada de seriedad.	**Observación:** Articulo relacionado, según (Código Orgánico Integral Penal 2014), Título III, Reparación Integral, Capítulo Único Reparación Integral, Artículo 78.- Mecanismos de reparación integral, numeral 4, dice: "El agresor puede reparar la dignidad y reputación de la víctima con un reconocimiento público por una verdad histórica".	SI
Calumnia	Es la acusación de un delito a una persona con	Según (Código Orgánico Integral Penal 2014) Sección Séptima, Delito contra el derecho al honor y buen	SI

	conocimiento de su falsedad.	nombre, **Artículo 182.- "Calumnia**. - La persona que, por cualquier medio, realice una falsa imputación de un delito en contra de otra, será sancionada con pena privativa de libertad de seis meses a dos años. No constituyen calumnia los pronunciamientos vertidos ante autoridades, jueces y tribunales, cuando las imputaciones se hubieren hecho en razón de la defensa de la causa. No será responsable de calumnias quien probare la veracidad de las imputaciones. Sin embargo, en ningún caso se admitirá prueba sobre la imputación de un delito que hubiere sido objeto de una sentencia ratificatoria de la inocencia del procesado, de sobreseimiento o archivo. No habrá lugar a responsabilidad penal si el autor de calumnias, se retractare voluntariamente antes de proferirse sentencia ejecutoriada, siempre que la publicación de la retractación se haga a costa del responsable, se cumpla en el mismo medio y con las mismas características en que se difundió la imputación. La retractación no constituye una forma de aceptación de culpabilidad".	
Child grooming	Utilizando las redes sociales una persona va generando comunicación con un menor de 13 años con la finalidad de mantener relaciones sexuales, abuso o agresión sexual	**Observación:** En el Ecuador no existe un artículo que sancione este acto de forma específica; sin embargo, existe el Art. 173 que relaciona este tipo de acto.	SI

	con el menor. En este caso el agresor puede utilizar otras herramientas como la suplantación de identidad, amenaza para el cometimiento del delito.		
Coacción	Fuerza o violencia que se hace a una persona para obligarle a decir o ejecutar algo.	**Observación:** No se encuentra normado en las leyes del Ecuador.	NO
cyber-bullying	Uso de tecnología para agredir psicológicamente a uno o varias personas de forma repetitiva en el tiempo. Se designa cuando la conducta se produce entre personas menores de edad.	Según (Ley Orgánica de Prevención, Control y Sanción del Acoso, Intimidación o Violencia en los Centros de Estudio de Ecuador 2013) **Artículo 15**: "El estudiante de los centros de educación que utilice medios electrónicos y telemáticos, dispositivos de comunicación tecnológica, para burlarse, acosar, hostigar, intimidar o amenazar, será sancionado con una falta muy grave de las dispuestas en el Reglamento a la Ley Orgánica de Educación Intercultural".	SI
cyber-stalking **Ciberacoso**	Uso de tecnología para agredir psicológicamente a uno o varias personas de forma repetitiva en el tiempo. Se designa cuando la conducta se produce entre personas mayores de edad.	**Observación:** No existe una normativa que sancione el Ciberacoso para personas mayores de edad.	SI
Embaucamiento	Utilizando las redes sociales y basándose en el	Según (Código Orgánico Integral Penal 2014) Sección Cuarta, Delitos contra la integridad sexual y	SI

	engaño y el anonimato para atentar contra la integridad física con fines sexuales del menor.	reproductiva, **Articulo 173.- "Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.** - La persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años. Cuando el acercamiento se obtenga mediante coacción o intimidación, será sancionada con pena privativa de libertad de tres a cinco años. La persona que suplantando la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, será sancionada con pena privativa de libertad de tres a cinco años".	
Enaltecimiento del terrorismo	Es un discurso oral o escrito en el que una persona(s) justifica acciones y organizaciones terroristas.	No se encuentra tipificado. **Observación:** Articulo relacionado. Según (Código Orgánico Integral Penal 2014) Sección, Capítulo Séptimo, Terrorismo y su financiación, **Artículo 366.- "Terrorismo.-** La persona que individualmente o formando asociaciones armadas, provoque o mantenga en estado de terror a la población o a un sector de ella, mediante actos que pongan en peligro la vida, la integridad física o la libertad de las personas o pongan en peligro las edificaciones, medios de comunicación, transporte,	SI

		valiéndose de medios capaces de causar estragos, será sancionada con pena privativa de libertad de diez a trece años".	
Estafa	Los usuarios son engañados a través de redes sociales argumentando ser ganadores premios, ofertas de bienes y servicios, trabajos, etc.	Según (Código Orgánico Integral Penal 2014) Sección Novena, Delitos contra el derecho a la propiedad, **Artículo 186.- "Estafa.** - La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años. La pena máxima se aplicará a la persona que: **Numeral 4**.- Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares".	SI
Incitación al odio	Discriminación a persona o grupo por: raza, religión, ideología, orientación sexual, etc.	No se encuentra tipificado **Observación:** Articulo Relacionado Según (Código Orgánico Integral Penal 2014), Sección Quinta, Delitos contra el derecho a la igualdad, Parágrafo Segundo, Delito de odio, **Artículo 177.- "Actos de odio.-** La persona que cometa actos de violencia física o psicológica de odio, contra una o más personas en razón de su nacionalidad, etnia, lugar de nacimiento, edad, sexo, identidad de género u orientación sexual, identidad cultural, estado civil, idioma, religión, ideología, condición socioeconómica, condición	SI

		migratoria, discapacidad, estado de salud o portar VIH, será sancionada con pena privativa de libertad de uno a tres años. Si los actos de violencia provocan heridas a la persona, se sancionará con las penas privativas de libertad previstas para el delito de lesiones agravadas en un tercio. Si los actos de violencia producen la muerte de una persona, será sancionada con pena privativa de libertad de veintidós a veintiséis años".	
Injuria	Es la acción de perjudicar la dignidad, estima de una persona. Se considerada como delito cuando la injuria sea entendida en el ámbito público como grave.	Ya no se considera como delito en el Código Orgánico Integral Penal (COIP), solo se define la calumnia. **Observación:** Este tipo de actos se presentan en redes sociales por medio de publicaciones de información como burlas, imágenes, caricaturas, videos con agravios a las personas.	SI
Intercepción no autorizada	Persona que sin autorización intercepte la transmisión de datos entre dos puntos de una red sin el consentimiento del emisor y receptor.	Según (Código Orgánico Integral Penal 2014), Sección Tercera, Delitos contra la seguridad de los activos de los sistemas de información y comunicación **Artículo 230.- "Interceptación ilegal de datos.**	SI
Pharming	Es la suplantación de páginas web, con la cual el atacante obtiene información confidencial con el propósito de realizar un fraude. La diferencia con el Phishing radica en que el ataque es dirigido al hardware.	Según (Código Orgánico Integral Penal 2014), Sección Novena, Delitos contra el derecho a la propiedad, **Artículo 190.- "Apropiación fraudulenta por medios electrónicos. -** La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o	Si

		derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años".	
Phishing	El delincuente utilizando tecnología de información y haciéndose pasar por una entidad legal, engaña a los usuarios atacados para obtener información confidencial con el propósito de realizar un fraude.	No se encuentra tipificado **Observación:** Articulo relacionado. Según (Código Orgánico Integral Penal 2014) Sección Novena, Delitos contra el derecho a la propiedad, **Artículo 186.- "Estafa.** - La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años".	SI
Piratería	Software protegido por derechos de autor, ejecutado sin el consentimiento. El presente trabajo no profundizará en el delito de compra, venta, transporte y almacenamiento de productos de software ilegales.	Observación: El Código Orgánico Integral Penal, actualmente no tipifica la piratería como un delito**.** La función del Servicio Nacional de Derechos Intelectuales (SENADI) es garantizar la adquisición y ejercicio de los derechos de propiedad intelectual de conformidad con el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, Registro Oficial Nº 899 (2016)	SI
Pornografía infantil	Material que exhibe menores de edad en actitud sexual explícita o	Según (Código Orgánico Integral Penal 2014), Sección Tercera, Diversas formas de explotación, **Artículo 103.- "Pornografía con**	SI

	implícita, con propósito obsceno.	**utilización de niñas, niños o adolescentes.** - La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual; será sancionada con pena privativa de libertad de trece a dieciséis años". **Artículo 104.- "Comercialización de pornografía con utilización de niñas, niños o adolescentes**. - La persona que publicite, compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda, por cualquier medio, para uso personal o para intercambio pornografía de niños, niñas y adolescentes, será sancionada con pena privativa de libertad de diez a trece años".	
Provocación al asesinato	Incitación por algún medio de comunicación para el cometimiento del delito.	**Observación:** Como provocación no se encuentra tipificado, solamente como acto ejecutado directamente.	SI
Revelación de secretos	Revelación de información personal y reservada a terceros con la cual puede ejercer algún tipo de control sobre el agraviado.	Según (Código Orgánico Integral Penal 2014) Sección Sexta, Delitos contra el derecho a la intimidad personal y familiar, **Artículo 179.- "Revelación de secreto.** - La persona que, reteniendo conocimiento por razón de su estado u oficio, empleo o profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año".	SI

		Observación: considero que, en el COIP, no se señalan los medios por los cuales se puede dar este tipo de conducta, dejando en posible indefensión a la víctima.	
Sexting	El sexting puede ser definido como el envío, normalmente a través de internet o de un dispositivo móvil, de mensajes de contenido sexual, producidos y protagonizados por el emisor. Para que se convierta en delito ésta información debe ser difundida sin autorización, generalmente el material es generado en lugares privados.	**Observación:** No existe norma que sancione el acto. El Articulo 178 del COIP hace mención a la violación a la intimidad.	SI
Suplantación de identidad	Persona que obtiene información o documentos de un tercero para hacerse pasar por él.	Según (Código Orgánico Integral Penal 2014) Sección Novena, Delitos contra el derecho a la propiedad, **Artículo.212**.- "**Suplantación de identidad.** - La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero tendrá pena privativa de libertad de uno a tres años".	SI
Usurpación de identidad	Persona que obtiene información de un tercero en el perfil abierto de la red social para hacerse pasar por él utilizando el servicio.	**Observación:** No se encuentra normado; sin embargo, existe el Artículo 212 que hace referencia a este tipo de acto.	SI

Violación a la intimidad	Revelación de información íntima sin consentimiento a terceros.	Según (Código Orgánico Integral Penal 2014) Sección Sexta, Delitos contra el derecho a la intimidad personal y familiar, **Artículo 178.- "Violación a la intimidad. -** La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley".	SI
Virus Informático	Son programas orientados en redes sociales que actúan enviando mensajes de aceptación por medio de frases engañosas aparentando ser verídicas y de confianza enviándose desde perfiles conocidos. Este tipo de virus troyano una vez que es ejecutado infecta al computador y al perfil del usuario enviando mensajes masivos a sus contactos.	Según (Código Orgánico Integral Penal 2014), Sección Tercera, Delitos contra la seguridad de los activos de los sistemas de información y comunicación **Artículo 230.- "Interceptación ilegal de datos. -** Será sancionada con pena privativa de libertad de tres a cinco años: 1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. 2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe	SI

		mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder. 3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares. 4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior". Según (Código Orgánico Integral Penal 2014), Sección Tercera, Delitos contra la seguridad de los activos de los sistemas de información y comunicación **Artículo 232.- "Ataque a la integridad de sistemas informáticos. -** La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que:	

		1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo. 2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad”.	

Fuente: Carol Rodríguez

3.1.3.5. Analizar clasificaciones existentes de delitos informáticos

3.1.3.5.1. Según La Organización de Naciones Unidas – ONU en el Informe del Décimo Congreso sobre Prevención del Delito y Tratamiento del Delincuente. Viena del 10 a 17 de abril de 2000.

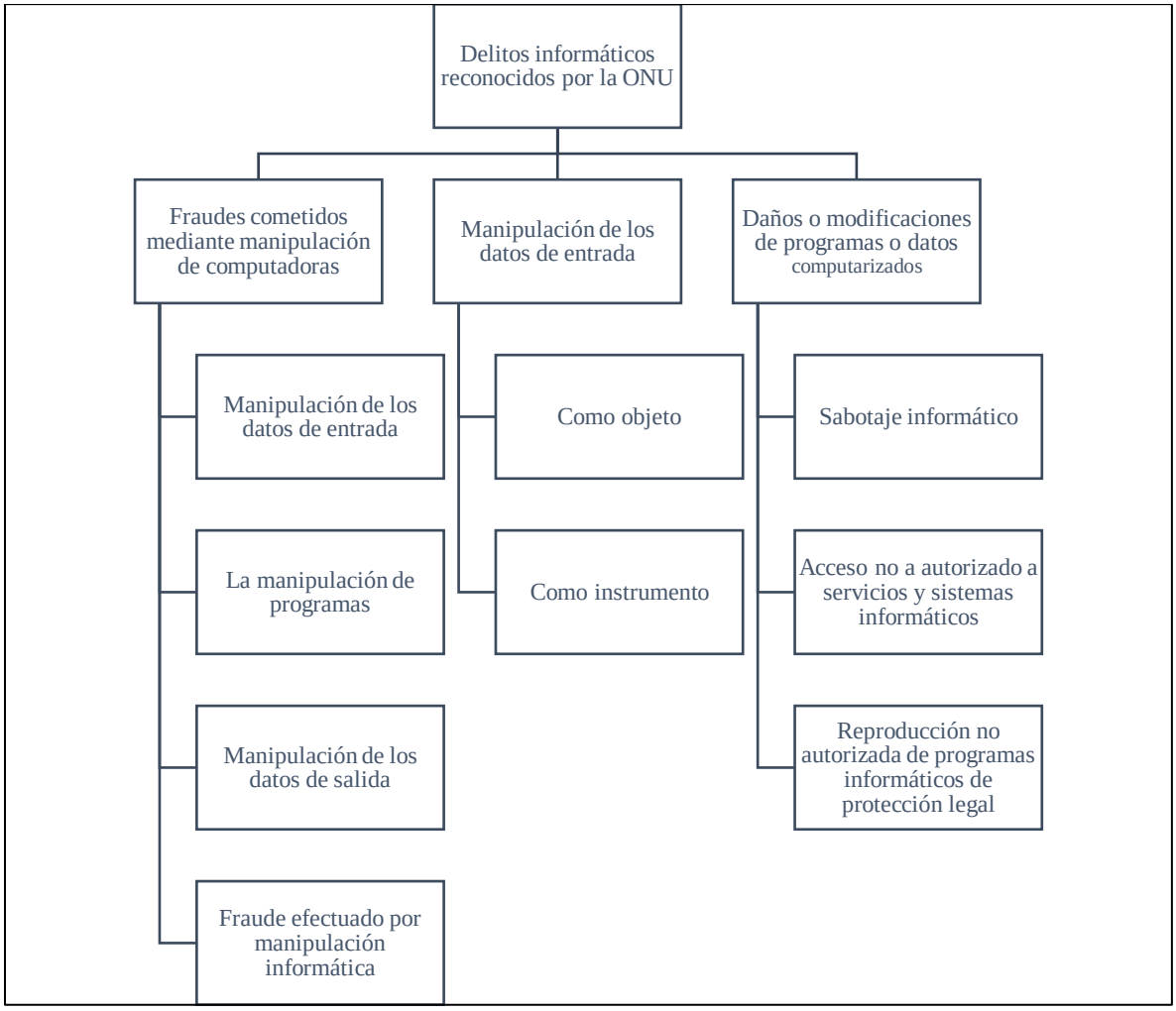


Figura 5. Delitos según la ONU

Fuente: Carol Rodríguez

3.1.3.5.2. Según Patricia Sanz Rodríguez (2014). Redes Sociales y Derecho Penal (tesis de grado), Universidad de Valladolid. Facultad de CC. Sociales, Jurídicas y de la Comunicación. España, determina las siguientes conductas delictivas:

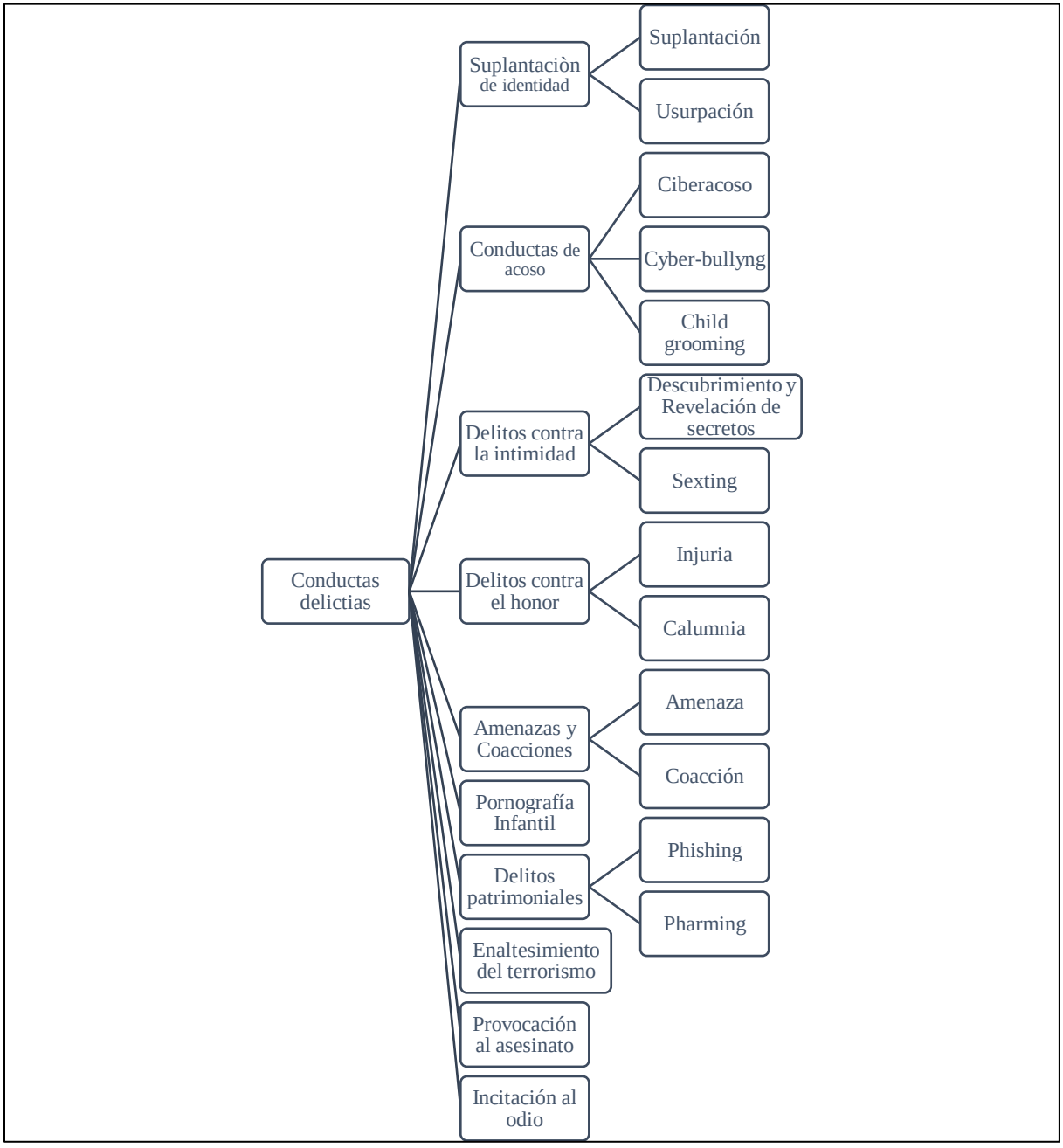


Figura 6. Tabla de conductas delictivas según Patricia Sans Rodríguez

Fuente: Carol Rodríguez

3.1.3.5.3. Según Andrea de Cea Jiménez (2012). Los delitos en las redes sociales: Aproximación a su estudio y clasificación (tesis de maestría), Universidad de Salamanca. España, determina los siguientes delitos en redes sociales:

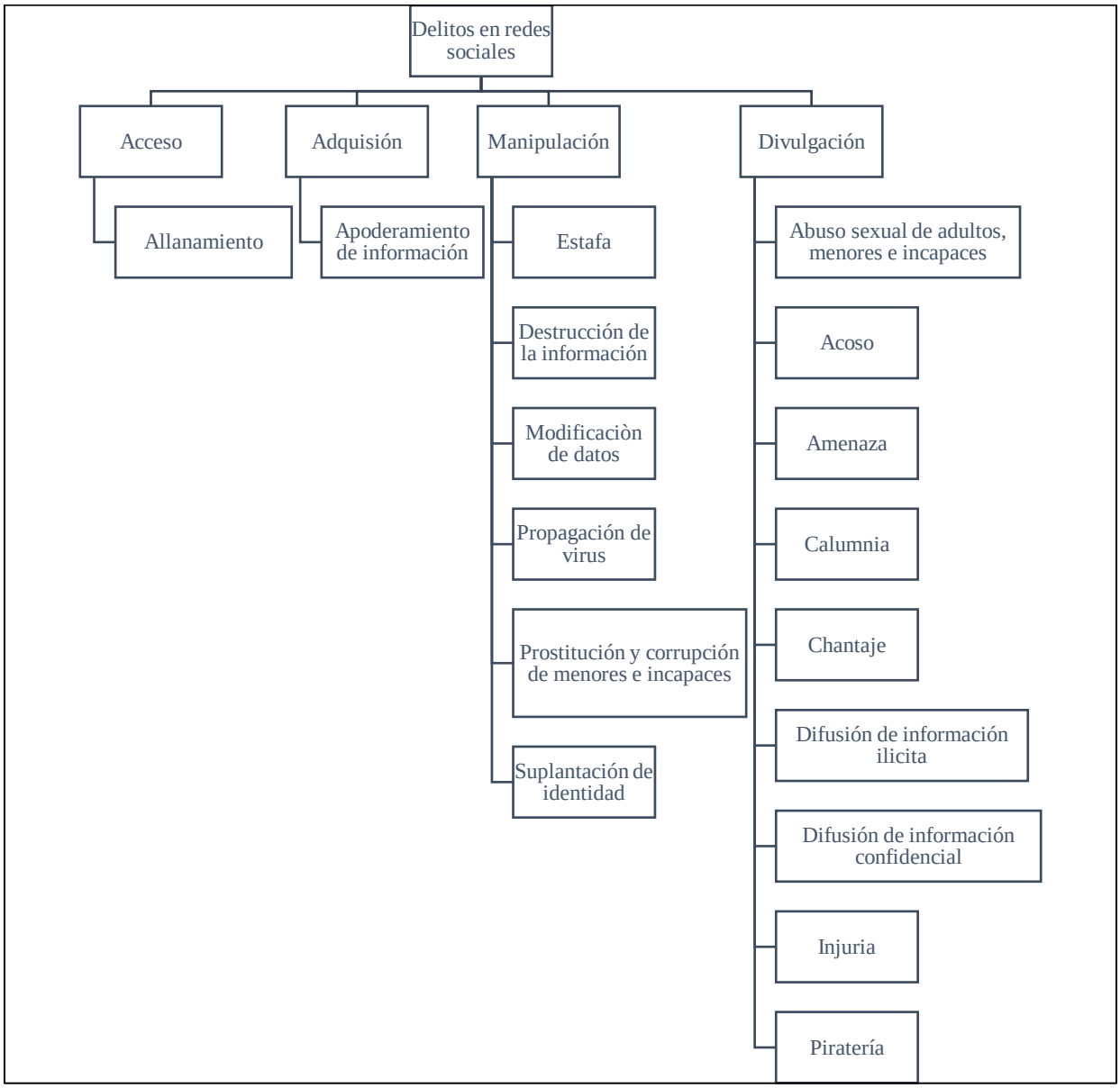


Figura 7. Tabla de Delitos Informáticos en Redes Sociales

Fuente: Andrea de Cea Jiménez

3.1.3.5.4. Según Dr. Santiago Acurio Del Pino (sin año). Profesor de Derecho Informático de la PUCE, en su documento electrónico: Delitos Informáticos: Generalidades, determina los siguientes tipos de delitos informáticos:

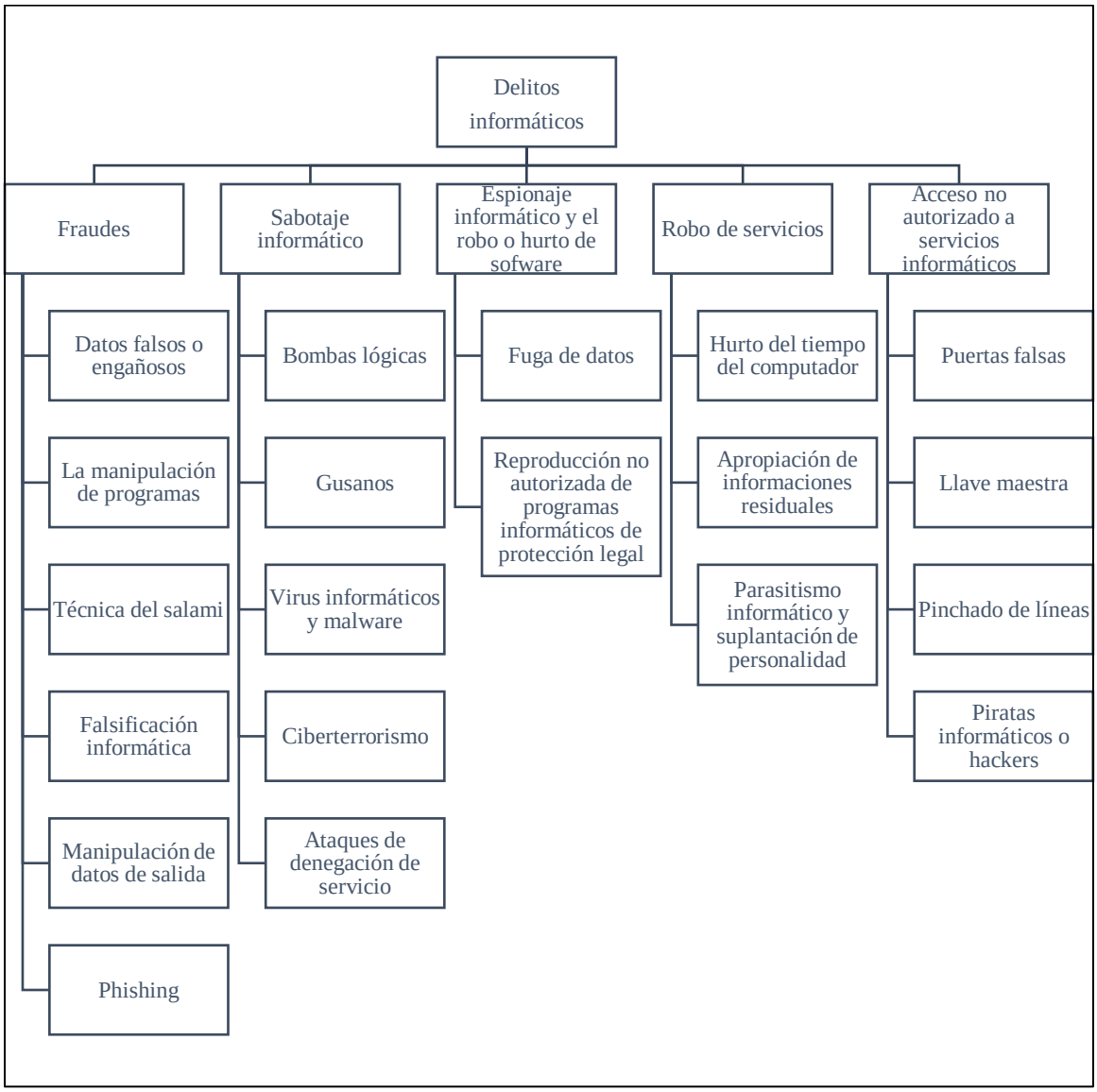


Figura 8. Tipos de Delitos Informáticos según Santiago Acurio del Pino

Fuente: Carol Rodríguez

3.1.3.6. Metodología para clasificar

El presente trabajo se centrará en el método jerárquico ya que permite organizar los delitos en redes sociales en forma deductiva; es decir, partimos de los conocimientos general de delitos y llegamos a un conocimiento exhaustivo en redes sociales.

3.1.3.6.1. Etapas del análisis de clasificación

Para la clasificación se guiará a través de las siguientes etapas para llegar a la clasificación:

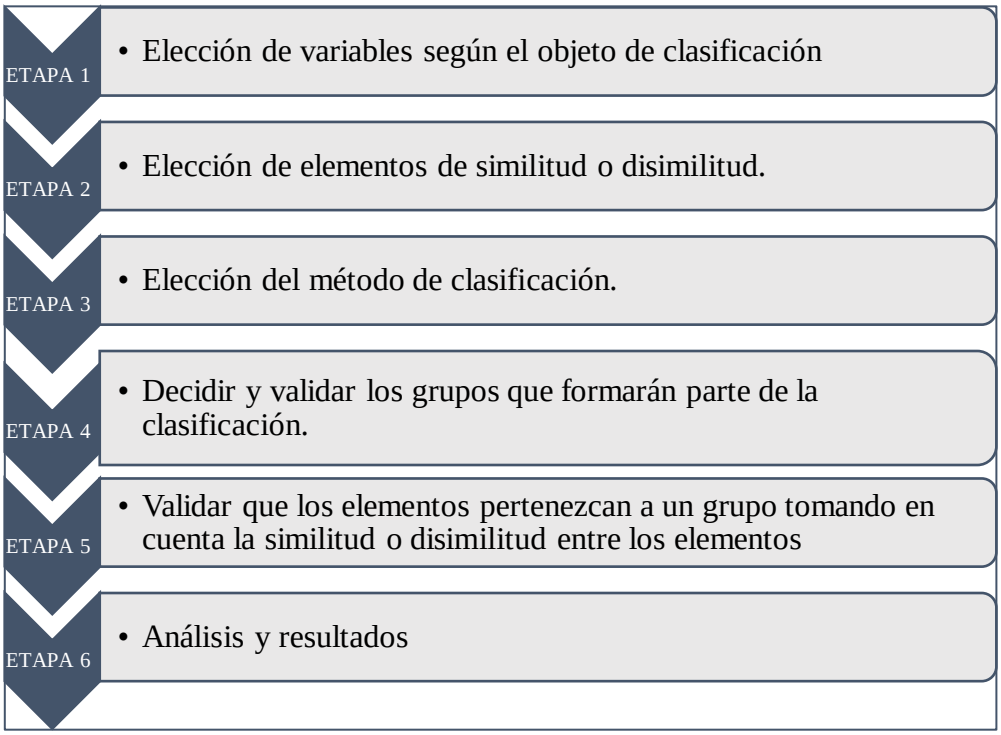


Figura 9. Etapas del análisis de clasificación

Fuente: Carol Rodríguez

3.1.3.7. Propuesta de clasificación de delitos informáticos en redes sociales

3.1.3.7.1. Etapa 1. Elección de variables.

El Internet y las redes sociales son medios de comunicación utilizadas por los usuarios, plataformas como Facebook, YouTube, Twitter su uso es popular en nuestro medio, en estos se realizan actividades como negocios, educación y la comunicación. El uso masivo de éstas plataformas electrónicas son aprovechadas por delincuentes para el cometimiento de diversas formas de delitos y actos que están en contra del buen vivir del ser humano.

El presente trabajo se centra en el estudio de delitos informáticos en redes sociales, los mismos que afectan a la persona, patrimonio, grupos de personas.

Los delitos también afectan a los medios utilizados como el hardware, software y datos.

En redes sociales se ha detectado los siguientes actos en contra de la ley y del buen vivir:

Índice:

- Acceso no autorizado
- Amenaza
- Calumnia
- Child Grooming
- Cyber Bullying
- Cyber Stalking
- Embaucamiento
- Enaltecimiento al terrorismo
- Estafa
- Incitación al odio
- Injuria
- Intercepción no autorizada
- Pharming
- Phishing
- Piratería informática
- Pornografía infantil
- Provocación al asesinato
- Revelación de secretos
- Sexting
- Suplantación de identidad
- Usurpación de identidad
- Violación a la intimidad
- Virus

3.1.3.7.2. Etapa 2. Elección de elementos de similitud o disimilitud.

Se determina cuatro grupos principales:

- Delitos que afectan al software y a los datos
- Delitos que afectan al patrimonio
- Delitos que afectan a la sociedad o a un grupo de personas.
- Delitos que afectan a la persona

Se agrupa a los elementos por similitud y disimilitud

Delitos que afectan al software y a los datos

- Acceso no autorizado
- Intercepción no autorizada
- Virus

Delitos que afectan al patrimonio

- Estafa
- Pharming
- Phishing
- Piratería informática

Delitos que afectan a la sociedad o a un grupo de personas

- Enaltecimiento al terrorismo
- Incitación al odio

Delitos que afectan a la persona

- Amenaza
- Calumnia
- Child Grooming
- Cyber Bullying
- Cyber Stalking
- Embaucamiento
- Injuria
- Pornografía infantil
- Provocación al asesinato
- Revelación de secretos
- Sexting
- Suplantación de identidad

- Usurpación de identidad
- Violación a la intimidad

3.1.3.7.3. Etapa 3. Elección del método de clasificación.

El presente trabajo utiliza el método de investigación deductivo ya que va de un conocimiento general de los delitos informáticos al conocimiento específico de los delitos en redes sociales.

El método de clasificación que se utiliza es el Jerárquico porque permite establecer niveles de conocimiento de los delitos en redes sociales; permite general grupos y clases dependiendo de las características de cada delito.

3.1.3.7.4. Etapa 4. Decidir y validar los grupos que formarán parte de la clasificación

Se determinó cuatro grupos principales en la Etapa 2.

- Delitos que afectan al software y a los datos
- Delitos que afectan al patrimonio
- Delitos que afectan a la sociedad o a un grupo de personas
- Delitos que afectan a la persona

Los delitos que afectan a la persona se agrupan por similitud en:

- Delitos Contra el Honor
- Delitos Contra la Intimidad
- Delitos de Acoso
- Delitos de Amenaza
- Suplantación de Identidad

Los delitos por disimilitud son:

- Provocación al asesinato

3.1.3.7.5. Etapa 5. Validar que los elementos pertenezcan a un grupo tomando en cuenta la similitud o disimilitud entre los elementos

En esta etapa de la clasificación se reagrupa los delitos contra la persona en:

Delitos de Similitud

Delitos de Acoso

- Child Grooming
- Cyber Bullying

- Cyber Stalking
- Embaucamiento

Delitos de Amenaza

- Amenaza

Suplantación de Identidad

- Suplantación de Identidad
- Usurpación de Identidad

Delitos Contra la Intimidad

- Pornografía Infantil
- Revelación de Secretos
- Sexting
- Violación a la Intimidad

Delitos Contra el Honor

- Calumnia
- Injuria

Delitos de Disimilitud

- Provocación al asesinato

3.1.3.7.6. Etapa 6. Análisis y resultados

La presente tabla muestra el resultado final de la clasificación de los delitos detectados en Redes Sociales en el estudio.

Clasificación de Delitos Detectados en Redes Sociales

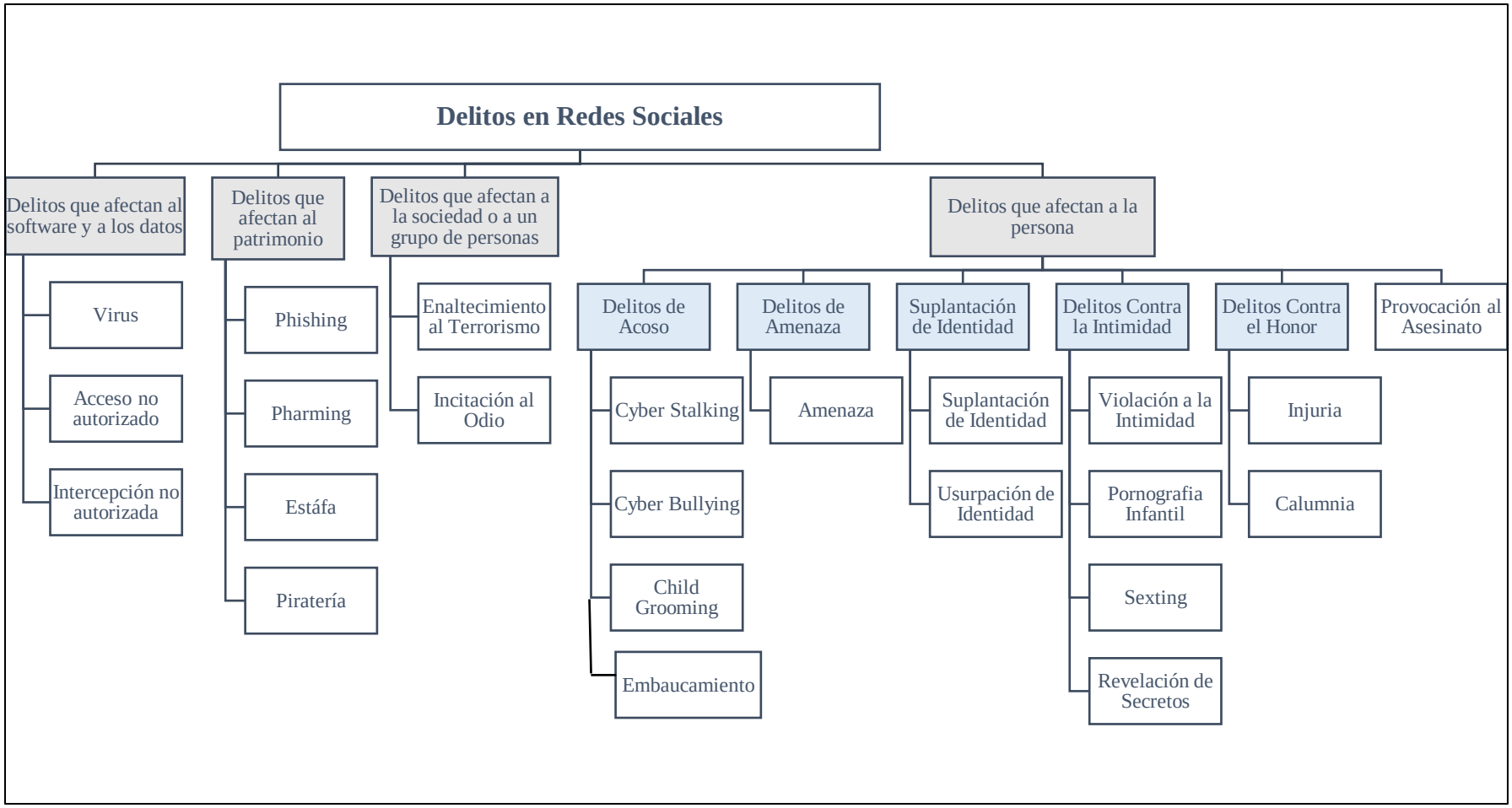


Figura 10. Clasificación de Delitos en Redes Sociales

Fuente: Carol Rodríguez

3.1.3.8. Establecer vacíos legales

La presente Tabla 6. lista las recomendaciones y la ausencia de tipificación para conductas detectadas en el ámbito de las Redes Sociales.

Tabla 6
Vacíos legales

Conducta	Observación
Usurpación de Identidad	Se recomienda complementar el Código Orgánico Integral Penal 2014, Sección Novena, Delitos contra el derecho a la propiedad, Artículo 212
Cyber - Stalking Cibeacoso	No se encuentra tipificado como tal.
Child Grooming	No se encuentra tipificado como tal. Se recomienda complementar el Código Orgánico Integral Penal 2014, Sección Cuarta, Delitos contra la integridad sexual y reproductiva, Articulo 173
Sexting	No se encuentra tipificado como tal. Se recomienda complementar el Código Orgánico Integral Penal 2014, Sección Sexta, Delitos contra el derecho a la intimidad personal y familiar, Artículo 178
Injuria	No se encuentra tipificado como tal, el COIP lo define como calumnia.
Amenaza	No se encuentra tipificado, el COIP determina una conciliación entre el acusado y la victima en el artículo 78, numeral 4.
Phishing	No se encuentra tipificado como tal. Se recomienda complementar el Código Orgánico Integral Penal 2014, Sección Novena, Delitos contra el derecho a la propiedad, Artículo 186
Enaltecimiento al terrorismo	No se encuentra tipificado como tal.
Provocación al asesinato	No se encuentra tipificado como tal, se encuentra tipificado como acto ejecutado directamente.
Incitación al odio	Se recomienda complementar el Código Orgánico Integral Penal 2014, Sección Quinta, Delitos contra el derecho a la igualdad, Parágrafo Segundo, Delito de odio, Artículo 177

Fuente: Carol Rodríguez

3.1.3.9. Proceso para la creación de una ley

Según el autor Caballenas, G (2011), la ley es una regla, norma, precepto de la autoridad pública, que manda, prohíbe o permite algo.

El presente trabajo se detalla el trámite ordinario para la aprobación de una ley.

3.1.3.9.1. ¿Cuándo se requiere de una ley?

- Para tipificar infracciones e implantar las sanciones correspondientes.

3.1.3.9.2. Iniciativa para presentar un proyecto de ley

Según la Constitución de la República del Ecuador (2008) en su Art. 134.- “La iniciativa para presentar proyectos de ley corresponde:

A las ciudadanas y los ciudadanos que estén en goce de los derechos políticos y a las organizaciones sociales que cuenten con el respaldo de por lo menos el cero punto veinticinco por ciento de las ciudadanas y ciudadanos inscritos en el padrón electoral nacional”.

3.1.3.9.3. Trámite Ordinario para la aprobación de leyes

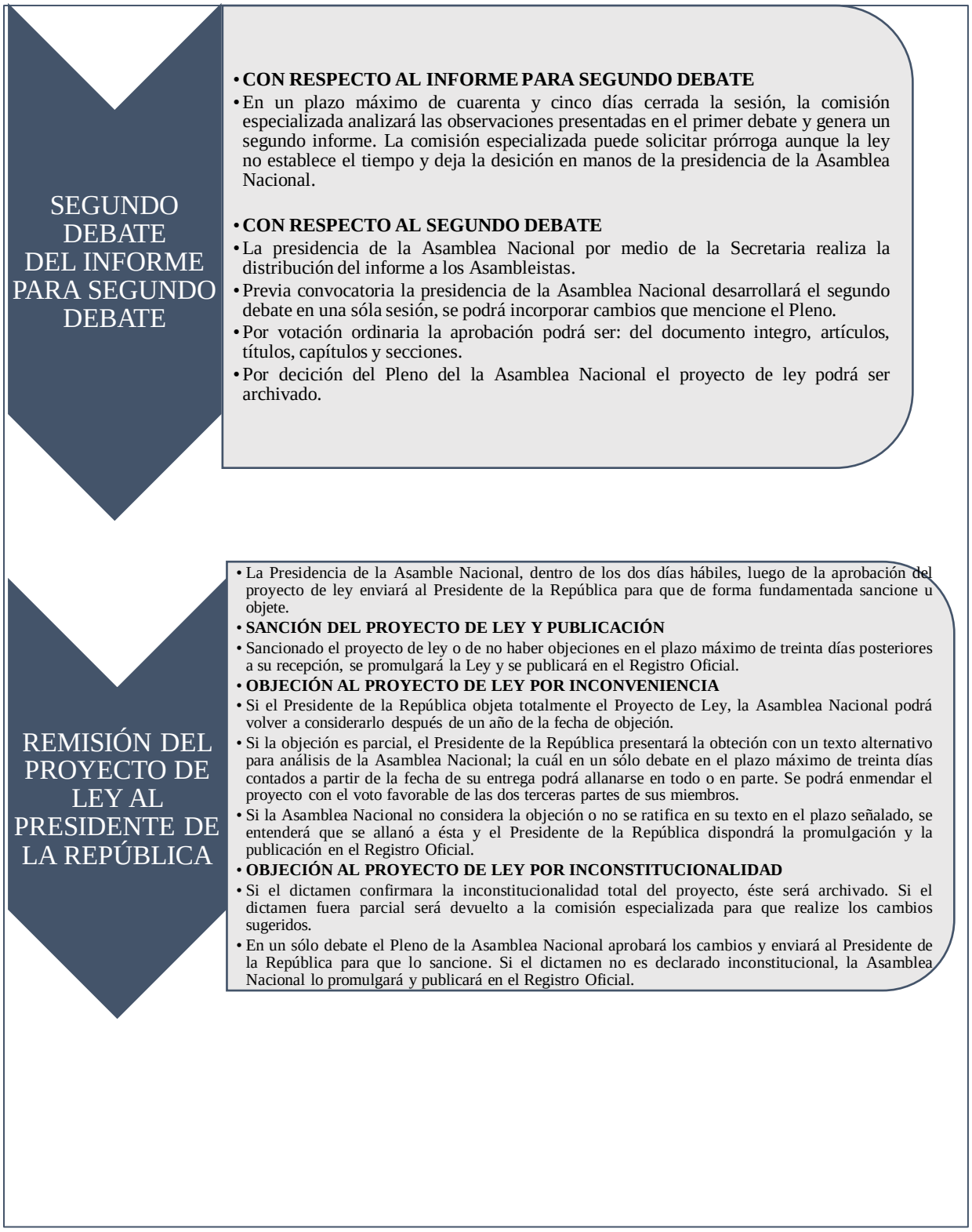


Figura 11. Trámite ordinario para la creación de leyes

Fuente: Carol Rodríguez

CAPITULO IV

4.1. CONCLUSIONES

Los usuarios por medio de las redes sociales de Facebook, Twitter y YouTube y otras se han trasformado en generadores y consumidores de información incrementando la posibilidad de ser atacados por ciberdelincuentes.

Al finalizar el presente trabajo de investigación se concluye con la propuesta de la metodología de clasificación que se describe en la Figura 9. La misma que sirve para realizar la clasificación de los delitos y conductas delictivas como se muestra de forma resumida en la Figura 10.

Con la tipificación de delitos informáticos en redes sociales se determina:

- Delitos que constan su sanción en las leyes del Ecuador.
- Se detecta que existen leyes relacionadas para sancionar un delito
- Conductas delictivas que no constan tipificados.

Al desarrollar la presente investigación se llega a la conclusión y determinación de vacíos legales detallados en la Tabla 6.

En Ecuador existen varios caminos para la formulación de leyes, sin embargo, se estudia la posibilidad de que la sociedad civil tome la iniciativa en la formulación del proyecto de ley siguiendo el proceso descrito en la Figura 11.

Al iniciar la presente investigación se propone la siguiente hipótesis "*El desarrollo de un modelo de clasificación de delitos informáticos en redes sociales mediante las leyes del Ecuador, nos lleva a determinar vacíos legales los cuales pueden ser plasmados en un proyecto de ley en el Ecuador",* la misma que es admitida debido a que se logra establecer la metodología, vacíos legales y el proceso ordinario para la formación de ley.

La clasificación de delitos y conductas delictivas en redes sociales de manera técnica, incide directamente en una formulación de ley que garantiza los derechos de las personas.

Para un correcto manejo de las conductas delictivas se plantea la metodología de clasificación que va del conocimiento general de los delitos al conocimiento específico, esta metodología se resume en: elección de los delitos, agrupar los delitos por similitud y disimilitud, elección del método de clasificación, validar los grupos de clasificación, validar los delitos del grupo de

clasificación y la presentación de resultados. La clasificación propuesta difiere con las leyes en el Ecuador encontrándose vacíos legales.

La siguiente tabla muestra la convergencia y divergencia de los delitos / conductas delictivas estudiadas y comparadas con las leyes en Ecuador.

Tabla 7
Convergencia/divergencia de los delitos en redes sociales según las leyes del Ecuador

Delito/conducta delictiva	¿Existe ley que sancione?	¿Existe ley relacionada que sancione?
Acceso no autorizado	SI	
Amenaza	NO	SI
Calumnia	SI	
Child Grooming	NO	SI
cyber-bullying	SI	
cyber-stalking Ciberacoso	NO	
Delito de embaucamiento	SI	
Descubrimiento y revelación de secretos	SI	
Enaltecimiento del terrorismo	NO	SI
Estafa	SI	
Incitación al odio	NO	SI
Injuria	NO	NO
Pharming	SI	
Phishing	NO	
Piratería	SI	
Pornografía infantil	SI	
Provocación al asesinato	NO	
Sexting	NO	SI
Suplantación de identidad	SI	
Usurpación de identidad	NO	SI
Violación a la intimidad	SI	
Virus Informático	NO	SI

Fuente: Carol Rodríguez

De los delitos analizados se concluye que las convergencias son aquellos en los que “SI” existe normativa aplicable. Las divergencias son aquellos en los que “NO” existe una normativa o existe normativa relacionada.

Entre los principales hallazgos del presente estudio se detectó que en Ecuador existe un desconocimiento del 67.6% de las leyes que sancionan delitos en redes sociales, así como también un alto porcentaje que desconoce sobre conductas delictivas como el Child Grooming (88%), Coacción (89,2%), Pharming (92%) según encuesta realizada (ver Anexo A).

4.2. RECOMENDACIONES

Deseo sugerir recomendaciones del presente trabajo en base a los resultados y las conclusiones determinadas:

- Desarrollar mecanismos y promover la difundir a la sociedad del conocimiento de los delitos en redes sociales y las leyes que lo sancionan ya que la colectividad desconoce los mismos.
- Ampliar la tabla de clasificación de delitos en redes sociales si a futuro se detecta nuevos delitos.
- Desarrollar la propuesta de ley complementándola de manera jurídica y según los vacíos detectados en redes sociales.

BIBLIOGRAFÍA

Acurio, S (sin año). *Delitos Informáticos: Generalidades*, Recuperado de: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Apespol. (2015). *El Código Orgánico Integral Penal (COIP) y los delitos informáticos*, Recuperado de: http://www.apespol.ec/articulo.php?id=11

Arcotel. (2000). *Fondo para el desarrollo de telecomunicaciones rurales*, Recuperado de: http://www.arcotel.gob.ec/wp-content/uploads/2016/02/fondo-para-el-desarrollo-de-telecomunicaciones-rurales.pdf

Cabanellas De Las Cuevas, G. (2011). *Diccionario Jurídico Elemental*. Argentina: Editorial Heliasta.

Cabrera, M. (2014). *La apropiación ilícita de redes sociales mediante la manipulación de claves de acceso personal como consecuencia de la falta de tipificación del delito informático en la legislación penal ecuatoriana* (tesis de pregrado). Universidad Central Del Ecuador, Facultad De Jurisprudencia, Ciencias Políticas Y Sociales, Carrera De Derecho, Ecuador.

Cea Jiménez, A. (2012). *Los delitos en las redes sociales: aproximación a su estudio y clasificación* (tesis de maestría). Universidad de Salamanca, España.

Código Orgánico De La Economía Social De Los Conocimientos, Creatividad E Innovación, Registro Oficial Nº 899, 9 de diciembre de 2016

Consejo de Europa - CdE. (2001). *Convenio sobre la Ciberdelincuencia*. Serie de Tratados Europeos No. 185. Budapest, Hungría: Publicación de la Secretaría del CdE

Constitución de la República del Ecuador; Registro Oficial No. 426; 28 de diciembre 2006.

Constitución de la República del Ecuador; Registro Oficial No. 449; 20 de octubre 2008.

Constituyente, E. A. (2008). *Constitución de la República del Ecuador*. Recuperado de http://www.oas.org/juridico/PDFs/mesicic4_ecu_const.pdf

Cordero, F. (2008). *Constitución del Ecuador* Recuperado de: http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf

Cotino, L. (2011). *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías*. Recuperado de

https://www.uv.es/cotino/elibertades2010.pdf

Diarioti.com. (2018). *¿Qué tan seguras son sus redes sociales, y qué hacer para protegerlas de los delincuentes cibernéticos?* Recuperado de https://diarioti.com/que-tan-seguras-son-sus-redes-sociales-y-que-hacer-para-protegerlas-de-los-delincuentes-ciberneticos/77274

El Telégrafo (2016). *En Ecuador, el 85% de los delitos informáticos ocurre por descuido del usuario*. Noticia publicada. Recuperado el 14 de 11 de 2017, de: https://www.eltelegrafo.com.ec/noticias/judicial/1/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario.

Si va a hacer uso de la misma, por favor, cite nuestra fuente y coloque un enlace hacia la nota original. www.eltelegrafo.com.ec

Herrera, E. (2016). *El Phishing como Delito Informático y su Falta de Tipificación en el Código Orgánico Integral Penal* (tesis de pregrado). Universidad Central Del Ecuador, Facultad De Jurisprudencia, Ciencias Políticas Y Sociales, Carrera De Derecho, Ecuador.

Lanza, E. (2016). *Estándares para una Internet libre, abierta e incluyente/ Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos*. Editorial OEA. Obtenido de http://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf

Leukfeldt, E. R. (2014). *Cybercrime and social ties. Trends in organized crime*, *17*(4), 231-249.

Ley Orgánica de la Función Legislativa; Suplemento Registro Oficial No. 642; 27 de Julio 2009.

Miró Llinares, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio.* Recuperado de http://www.marcialpons.es/static/pdf/9788415664185.pdf

Naciones Unidas (1994). *Revista Internacional de Política Criminal. Manual de las Naciones Unidas Sobre Prevención del Delito y Control de Delitos Informáticos*. Oficina de las Naciones Unidas en Viena. Centro de Desarrollo Social y Asuntos Humanitarios. Nos. 43 y 44. Naciones Unidas, Nueva York.

Naciones Unidas (1991). *Octavo Congreso de las Naciones Unidas Sobre Prevención del Delito y Tratamiento del Delincuente*. La Habana, 27 de agosto a 7 de septiembre De 1990. (A/Conf.144/28/Rev.1) Nueva York, Naciones Unidas.

Naciones Unidas (1990). *Prevención del Delito y Justicia Penal en El Contexto del Desarrollo: Realidades y Perspectivas de la Cooperación Internacional*. Documento de Trabajo

Preparado por la Secretaría (A/Conf.144/5). Octavo Congreso de las Naciones Unidas Sobre Prevención del Delito y Tratamiento del Delincuente. La Habana, Cuba, 27 agosto-7 septiembre.

Naciones Unidas (2000). *Informe del Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente.* Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente. Viena, 10 a 17 de abril de 2000.

Noboa, A. (Ed.). (1901). *Recopilación de leyes del Ecuador* (Vol. 3). Imprenta nacional.

República Del Ecuador Asamblea Nacional (2014), *Código Orgánico Integral Penal (COIP)*, Recuperado de http://www.funcionjudicial.gob.ec/lotaip/Penal.pdf

República del Ecuador (2002), *Ley de Comercio Electrónico, Firmas y Mensajes de Datos*, Quito Ecuador.

Rodríguez Arbeláez, J. D. (2014). *Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación*. Recuperado de http://bdigital.ces.edu.co:8080/repositorio/bitstream/10946/1334/2/Delitos%20en%20las%20Redes%20Sociales.pdf

Salazar, L., & Mauricio, A. (2016). *Análisis de los delitos informáticos y de telecomunicaciones en el Ecuador bajo las nuevas formas jurídicas* (tesis de maestría), Universidad de las Fuerzas Armadas ESPE. Carrera de Ingeniería Electrónica en Redes y Comunicación de Datos, Ecuador.

Sanz, P. (2014). *Redes Sociales y Derecho Penal* (tesis de grado), Universidad de Valladolid. Facultad de CC. Sociales, Jurídicas y de la Comunicación. España.

Sietel-Arcotel (2018). *Cuentas y usuarios del servicio de acceso a internet*. Recuperado de http://www.arcotel.gob.ec/servicio-acceso-internet/

Téllez Valdés, julio (2009), *Derecho Informático*. México: Mc Graw-Hill/Interamericana editores, s.a de c.v Biblioteca Jurisprudencia: 340.02 T626

Yip, M., Shadbolt, N., & Webber, C. (2012). Structural analysis of online criminal social networks. In *Intelligence and Security Informatics (ISI), IEEE International Conference on* (pp. 60-65). IEEE.

Zaidán, S. (2017). *El Procedimiento Legislativo En La Asamblea Nacional Del Ecuador*. Obtenido de*:*

https://latinamerica.hss.de/fileadmin/user_upload/Projects_HSS/Latin_America/Ecuador/Dokumente/2017/El_Procedimiento_Legislativo_en_la_Asamblea_Nacional_del_Ecuador.pdf

Zavala, J. (2016). *Código Orgánico General de procesos COGEP*. Notas de Estudio 2016. *Quito, Ecuador: Murillo Editores*.

Zúñiga. L. (2014). "*Código Orgánico Integral Penal*", Ministerio de Justicia, Derechos Humanos y Cultos, vol. 1, ISBN: 978-9942-07-592-5

ANEXOS

ANEXO A – FORMULARIO Nº 1

Encuesta de Delitos en Redes Sociales

Para la realización de la presente encuesta se utiliza como herramienta un formulario de google.

ENCUESTA DE DELITOS EN REDES SOCIALES

Marque la respuesta según su conocimiento.

* Obligatorio

1. **¿Es usuario de alguna red social como Facebook, Twitter, YouTube? ***

   ○ SI
   ○ NO

2. **Marque cual o cuales son delitos en redes sociales (puede seleccionar varias opciones) ***

   ☐ Suplantación de identidad
   ☐ Usurpación de identidad
   ☐ Cyber Stalking
   ☐ Cyber Bulling
   ☐ Child Grooming
   ☐ Embaucamiento
   ☐ Revelación de secretos
   ☐ Violación a la intimidad
   ☐ Sexting
   ☐ Injuria
   ☐ Calumnia
   ☐ Amenaza
   ☐ Coacción

- ☐ Pornografía infantil
- ☐ Phishing
- ☐ Pharming
- ☐ Enaltecimiento al terrorismo
- ☐ Provocación al asesinato
- ☐ Incitación al odio
- ☐ Virus
- ☐ Acceso no autorizado
- ☐ Intercepción no autorizada
- ☐ Piratería informática

3. ¿Ha sido víctima de algún delito en redes sociales? *

- ○ SI
- ○ NO

4. ¿Conoce la existencia de leyes que sancionan los delitos en redes sociales? *

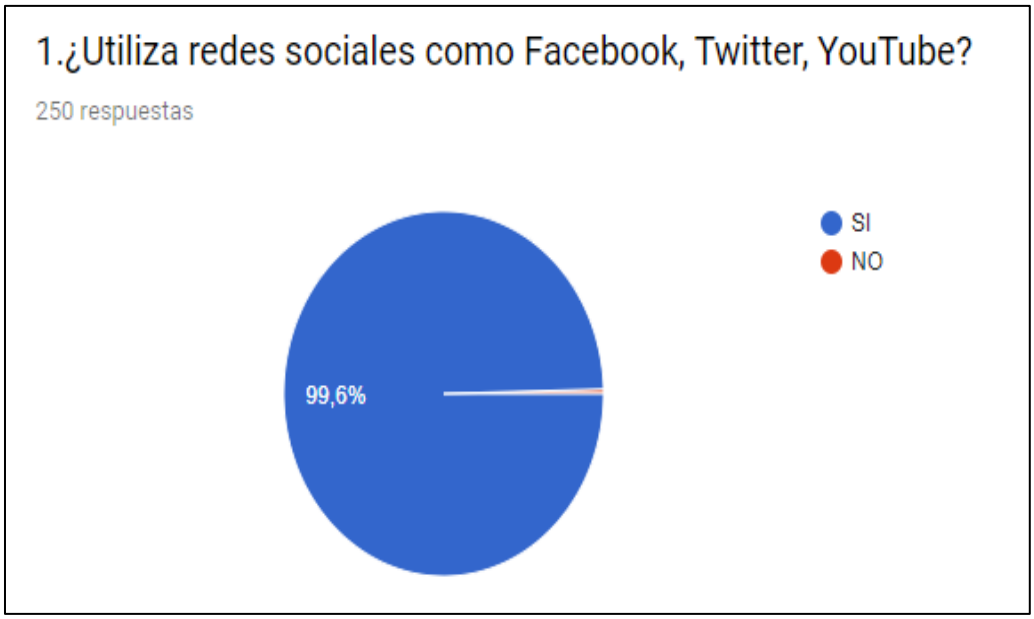
- ○ SI
- ○ NO

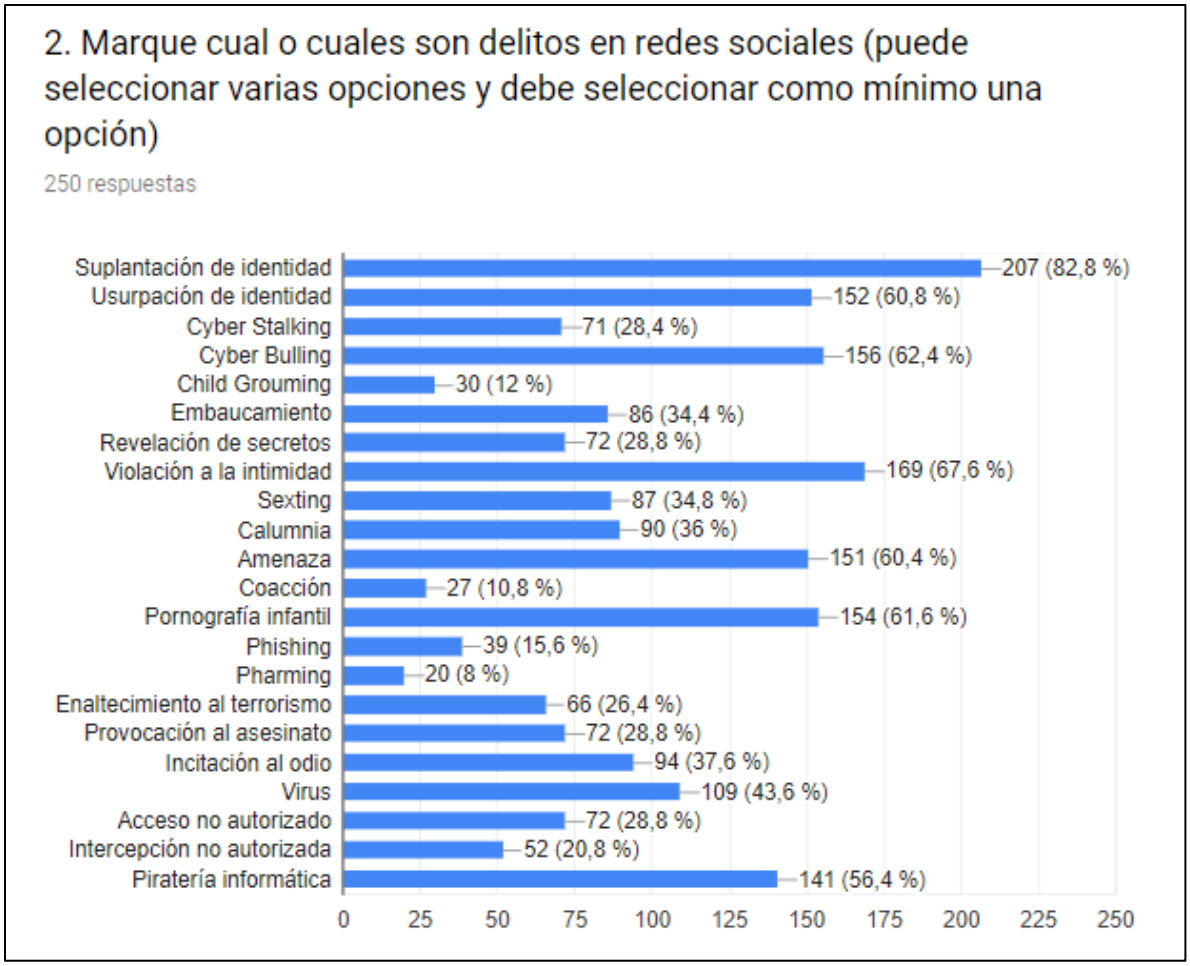
5. ¿Confía en la aplicación de la ley en Ecuador para sancionar delitos en redes sociales? *

- ○ SI
- ○ NO

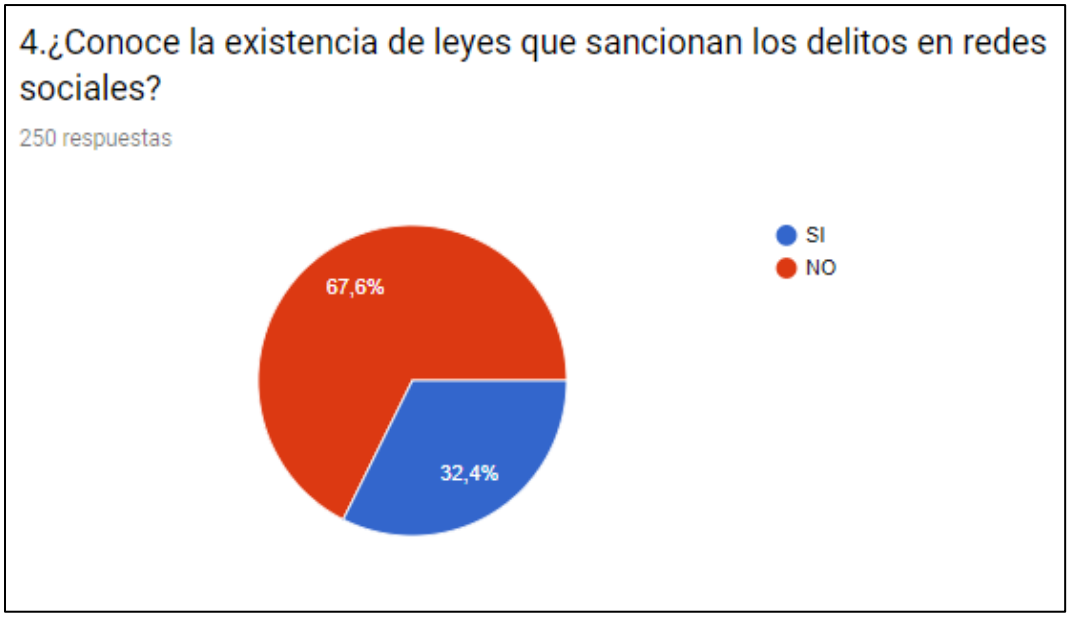
RESULTADOS DE LA ENCUESTA

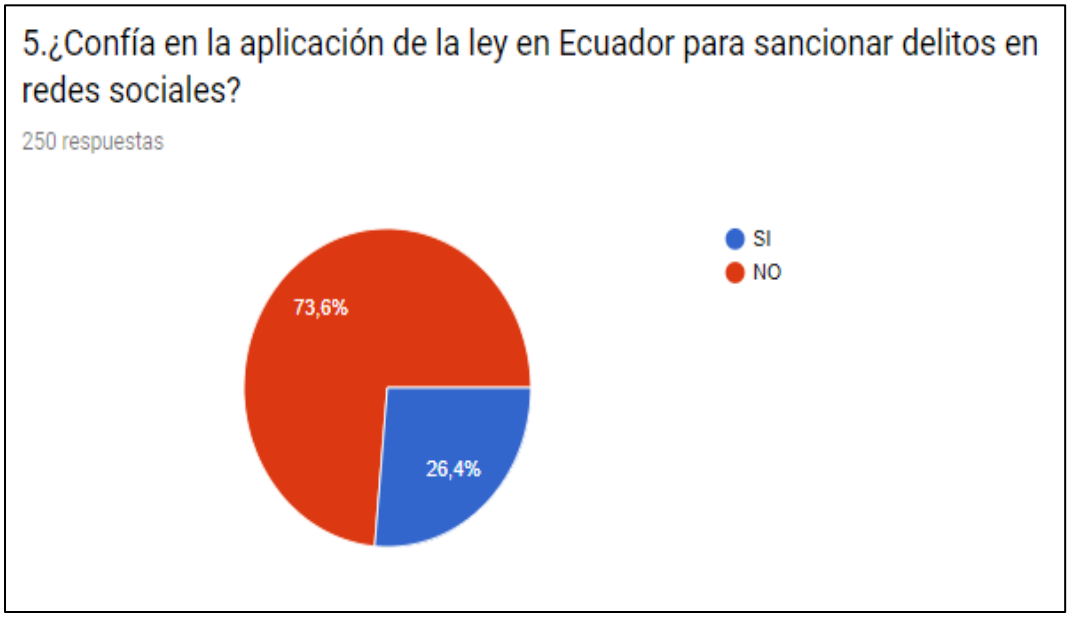
Muestra: 250 alumnos de la Universidad Central del Ecuador con acceso a servicio de internet, edades comprendidas entre 17 a 24 años, con educación de tercer nivel.




2. Marque cual o cuales son delitos en redes sociales (puede seleccionar varias opciones y debe seleccionar como mínimo una opción)
250 respuestas
Suplantación de identidad 207 (82,8 %)
Usurpación de identidad 152 (60,8 %)
Cyber Stalking 71 (28,4 %)
Cyber Bulling 156 (62,4 %)
Child Grouming 30 (12 %)
Embaucamiento 86 (34,4 %)
Revelación de secretos 72 (28,8 %)
Violación a la intimidad 169 (67,6 %)
Sexting 87 (34,8 %)
Calumnia 90 (36 %)
Amenaza 151 (60,4 %)
Coacción 27 (10,8 %)
Pornografía infantil 154 (61,6 %)
Phishing 39 (15,6 %)
Pharming 20 (8 %)
Enaltecimiento al terrorismo 66 (26,4 %)
Provocación al asesinato 72 (28,8 %)
Incitación al odio 94 (37,6 %)
Virus 109 (43,6 %)
Acceso no autorizado 72 (28,8 %)
Intercepción no autorizada 52 (20,8 %)
Piratería informática 141 (56,4 %)
0 25 50 75 100 125 150 175 200 225 250

3. ¿Ha sido víctima de algún delito en redes sociales?
250 respuestas
SI
NO
80,4%
19,6%


4.¿Conoce la existencia de leyes que sancionan los delitos en redes sociales?
250 respuestas
SI
NO
67,6%
32,4%


5.¿Confía en la aplicación de la ley en Ecuador para sancionar delitos en redes sociales?
250 respuestas
SI
NO
73,6%
26,4%