Delitos a través redes sociales en el Ecuador: una aproximación a su estudio

Crimes through social networking sites in Ecuador: an approach to their study

Luis Jara Obregón [1], Enrique Ferruzola Gomez [2,] Guillermo Rodríguez López [3]*
[1] Catedrático de la Carrera de Ingeniería de Sistema, Universidad Católica de Cuenca, [2]Escuela de Computación e Informática en Computación, Universidad Agraria del Ecuador, [3]Catedrático de la Carrera de Ingeniería de Sistemas, Universidad Católica de Cuenca
[1] Lsjaraob@ucacue.edu.ec, [2] Eferruzola@uagraria.edu.ec, [3] mgrodriguezl@ucacue.edu.ec

Resumen– *El presente trabajo muestra la conceptualización de los principales delitos, que se comenten comúnmente usando como medio las redes sociales. Se reunió información como métodos y técnicas que usan los delincuentes o denominados ciberdelincuentes en la internet para acercarse a sus víctimas y crear un ambiente propicio para lograr su cometido. Así, principalmente, se investigó el marco jurídico para hacer frente a estas prácticas delicias, que si bien son consideradas prácticas comunes actualmente se realizan, aprovechando el acceso de información que ofrecen redes sociales como Facebook, en la cual se enfoca nuestro estudio por ser considerada la red social con mayor número de usuario activo. Posterior a esto se consultó el nuevo código integral penal del Ecuador, para verificar la existencia de un marco legal que penalice este tipo de comportamientos antijurídicos en las redes sociales. Se realizó la observación de los diferentes sitios web de las fuerzas del orden del país, con el fin del obtener información que aporte al desarrollo del presente estudio, se emplearon técnicas como la entrevista y encuesta, las cuales fueron aplicadas a los agente fiscales y elementos de la Policía Judicial para determinar cuáles son los procesos actuales que se siguen en la investigación de este tipo de delitos, obteniendo resultados que se contraponen a la realidad con muy pocas instrucciones fiscales y procesos referentes a este tema en estudio.*

Palabras claves– *Delitos informáticos, medios telemáticos, redes sociales, procesos de investigación.*

Abstract– *The present work shows the conceptualization of the main crimes, which are commonly commented on as means of social networking sites. It gathered information such as methods and techniques used by criminals or so-called cybercriminals on the internet to approach their victims and create an environment conducive to achieving their mission. So, mainly, we investigated the legal framework to deal with these practical delights, which are considered common practices are currently carried out, taking advantage of the access of information offered by social networks such as Facebook, which focuses our study for being considered The social networking sites with the largest number of active users, after which the new integral penalty code of Ecuador was consulted, to verify the existence of a legal framework that penalizes this type of anti-legal behaviors in social networking sites. The observation of the different websites of law enforcement agencies was carried out in order to obtain information that contributed to the development of the present study. Techniques such as the interview and survey were used, which were applied to the fiscal agents and elements Of the Judicial Police to determine what are the current processes that are followed in the investigation of this type of crimes, obtaining results that are opposed to reality with very few tax instructions and processes regarding this subject under study.*

Keywords– *Cybercrime, electronic media, social networking sites, research processes.*

Tipo de Artículo: Original
Fecha de Recepción: 4 de mayo de 2017
Fecha de Aceptación: 25 de septiembre de 2017

1. Introducción

Actualmente las relaciones sociales han innovado con la aplicación de las tecnologías de información y comunicación. Existen un gran número de redes sociales de acceso libre en internet, donde cualquier cibernauta puede crear una cuenta, configurar un perfil

con información personal auténtica o ficticia y acceder a un mundo de comunicaciones e interacciones con amigos, familiares, compañeros o simplemente relacionarse con usuarios completamente desconocidos que cuente con un perfil dentro de una red social como Facebook, convirtiéndose sin lugar a dudas en el instrumento favorito para el contacto e intercambio de experiencias.

La principal ventaja de estas redes sociales es la comunicación, la publicación de contenidos gratuitos como: fotos, videos, estados, música entre otros. Sin embargo, a pesar de la importancia y el papel que desempeñan estas redes sociales como medios de comunicación y difusión, en muchas ocasiones la libertad de publicar cualquier tipo de contenido (datos) escrito y/o audiovisual, está ocasionando que colisionen la libertad de expresión con el derecho del honor y privacidad consagrados en la Constitución del Estado Ecuatoriano.

El usuario como actor más vulnerable en este entorno, puede no conocer de los artículos de ley integrados en el código integral penal del Ecuador, publicado el 10 de agosto del año 2014. Que no tipifican explícitamente los delitos cometidos a través de redes sociales pero sí hacen referencia a delitos relacionados con medios telemáticos como son: el *phishing*, robo de identidad, las injurias, las calumnias, la extorción, el acoso, la publicación de pornografía, la pedofilia, el *grooming*, difusión de *malware*, trata de blancas, sicariato, *happy slapping*, la estafa.

Estos delitos mencionados anteriormente son comunes pero su *modus operandi*, ha cambiado con el uso de medios telemáticos para sus operaciones, cuyo proceso en ocasiones no tiene la tecnología como fin.

Un importante medio de operación para estas prácticas delictivas son las redes sociales, de acuerdo con el INEC (Instituto Nacional de Estadísticas y censos del Ecuador), alrededor del 98% de las personas mayores de 12 años tienen una cuenta en Facebook en el Ecuador. No obstante, con el crecimiento de usuarios en redes sociales, la presencia de los ciberdelitos también ha cobrado fuerza.

Según informes de la Policía, las bandas utilizan los datos de las víctimas para perpetrar delitos, como la extorsión. Pero hay casos más extremos como el secuestro. Además, hay otros delitos reportados en el país como trata de personas, pornografía infantil y acoso sexual. Este tipo de delitos generalmente quedan en la impunidad por la volatilidad de la información, la globalización del internet y el anonimato.

La falta de procesos claros y el desconocimiento por parte del usuario sobre el marco legal existente, para penalizar este tipo de prácticas antijurídicas, crean dificultad para identificar a los autores materiales e intelectuales del hecho, siendo este, uno de los principales problemas al emprender investigaciones de delitos realizados por medios telemáticos en el Ecuador.

La presente investigación buscó establecer los principales delitos cometidos a través de una red social como Facebook en el Ecuador, para describir los métodos o técnicas utilizados por los ciberdelincuentes y de que manera el marco legal influye en la identificación del autor material e intelectual, esclarecimiento del hecho, y aportar con conocimiento para su investigación.

2. Conceptualización

En cada país se usan definiciones distintas sobre el tema de delitos informáticos, sin embargo, han surgido esfuerzos de expertos y de organizaciones como la ONU, UNESCO, ITU. Buscando proponer la universalidad de delitos relacionados con la tecnología, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas a la legislación de cada país.

Sin embargo, al consultar bibliografía de diferentes fuentes específicamente al insigne estudioso español Carlos Sarzana, el cual indica que los crímenes a través de computadora comprenden "Cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo" [1].

María de la Luz Lima conceptualiza que el "delito electrónico", [2] "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" [1].

Por otro lado, debe mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa a la computadora,

tales como "delitos informáticos", "delitos electrónicos", "delitos relacionados con la computadora", "crímenes por computadora", delincuencia relacionada con el ordenador" “delitos telemáticos”.

Analizando las definiciones antes mencionadas por diversos autores podemos plantear una aproximación al delito informático para el presente estudio como: “todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático ya sea como medio o como fin, implicando actividades criminales” [3].

2.1 Redes sociales de internet

“Son formas de interacción social, definida como un intercambio dinámico entre personas, grupos e instituciones. Un sistema abierto y en construcción permanente que involucra a conjuntos que se identifican en las mismas necesidades y problemáticas y que se organizan para potenciar sus recursos. La intervención en red es un intento reflexivo y organizador de esas interacciones e intercambios, donde el sujeto se funda a sí mismo diferenciándose de otros [4]”.

Es importante tener en cuenta que las redes sociales dan al anónimo popularidad, a la discriminada integración, al sujeto diferente igualdad. Pero, además, permite que la fuerza del grupo genere cambios que de otra manera podrían ser difíciles y afiance nuevos vínculos [5], que en muchas ocasiones pueden ser aprovechados por delincuentes usando técnicas de ingeniería social.

Según un estudio desarrollado por la empresa de seguridad informática “Shopos”, sobre los riesgos de hurto de identidad en una de las redes sociales más grandes de Internet, llega a la conclusión que los usuarios de Facebook facilitan el robo de su información personal, en su investigación, Sophos creó un perfil falso –el cual tenía la imagen de una rana de plástico– para hacer invitaciones y enviar mensajes a cerca de 200 usuarios aleatorios de Facebook [6]. La idea era determinar cuántas personas respondían y qué cantidad de información personal podía ser obtenida de ellas. El resultado: 41% de los usuarios no tiene inconveniente en suministrar datos personales, como dirección de correo electrónico, fecha de nacimiento o teléfono celular, a cualquier desconocido, incluyendo una rana [6].

Facebook ha comunicado una impresionante cifra de 1000 millones de personas que se conecta cada día. Ya no hay momentos de “conexión a Internet”, como podía suceder hace algunos años, en la actualidad “viven conectados”.

Los factores antes mencionados fomentan un mundo virtual y como en toda sociedad existirán peligros, actualmente existen diferentes tipos de plataformas de redes sociales en Internet en los que se podrían realizar prácticas delictivas, pero Facebook, es la más común, según estudios que se la ubican con la red social más utilizada, los delincuentes crean cuentas de usuario para reunir información de sus víctimas, pero los métodos utilizados difieren según la naturaleza del delito en cuestión, las tres categorías de delitos iniciados en redes sociales son: la ciberdelincuencia, el robo y los delitos sexuales [7].

2.2 Metodología de acción ante los delitos cometidos a través de redes sociales

En la investigación de campo realizada, a las diferentes entidades de justicia, no se pudo determinar la existencia de una metodología específica de actuación por parte de los entes judiciales del país, para la investigación de delitos cometidos a través de las redes sociales, se evidenció que los procesos investigativos se realizan bajo el mismo parámetro de la investigación de delitos comunes.

En países como Argentina existen entidades como la organización sin fines de lucro “Argentina cibersegura” que nació a mediados del año 2010, se creó bajo el modelo de ciudad cybersegura que fue implementado por la empresa ESET Estados Unidos, con el principal objetivo de educar a la población en temáticas relacionadas a la ciberseguridad [8].

Otros de los países a la vanguardia de los delitos informáticos es España, la cual dentro de su Guardia Civil y Policía Nacional, cuentan con un grupo de delitos telemáticos y Brigada de Investigación Tecnológica creada para investigar todos aquellos delitos que se comenten a través de internet, el esfuerzo principal del GDT ha sido desde su creación, la investigación de la delincuencia que se vale de las redes sociales y sistemas de información para su comisión. También cabe destacar los esfuerzos que realizan para fomentar un uso seguro de las nuevas tecnologías,

consciente de que a la larga este esfuerzo ayudará a minimizar el impacto de la delincuencia [9].

Entre los objetivos perseguidos por este tipo de organizaciones tenemos:

- Generar contenidos que colaboren a conformar un espacio digital más seguro.
- Impulsar leyes que regulen el espacio digital y protejan a quienes naveguen en los mismos.
- Concientizar y educar a niños, adolescentes y adultos en temas relacionados a la seguridad informática.
- Promover la alfabetización de la población.

Argentina cibersegura siendo una iniciativa de Securing Our eCity realiza con ESET un guía de seguridad en las redes sociales enfocando su documento en las 4 principales redes sociales con mayor popularidad en el año 2011 como son Facebook, MySpace, Twitter y LinkedIn [8].

El documento conformado por 16 páginas denominado guía de seguridad en las redes sociales identifica los principales riesgos en las redes sociales [10]:

- *Malware* acrónimo en inglés de las palabras malicious y *software*, es decir código malicioso.
- *Phising*, consiste en el robo de información personal y/o financiera del usuario través de la falsificación de un ente de confianza.
- Robo de información, el uso diario de redes sociales y los usuarios subiendo diversos datos de índole personal, que pueden ser de utilidad para los atacantes.
- Para muchas empresas de seguridad el robo de información en redes sociales, se relaciona directamente con el robo de identidad.

Existen 2 principales vectores de ataque para el robo de información estos son [10]:

- Ingeniería Social: El contacto directo con el usuario víctima, extrayendo información a través de la comunicación, la "amistad" o cualquier comunicación que permita establecerse a través de la red social.
- Información pública: una mala configuración de las redes sociales, puede permitir acceso a mucha información personal, que personas mal intencionadas podrían acceder y hacer mal uso de dicha información.

En los casos de acoso a menores de edad, los niños utilizan las redes sociales desde muy temprana edad, incluso evadiendo los requisitos de seguridad que plantean las redes sociales al momento de crear una cuenta, existen una serie de amenazas como el *cyberbulling*, *grooming*, *sexting* [10].

En países como España en el año 2013 la policía propuso usar troyanos para la investigación, lo cual no tuvo aceptación por la legislación ya que viola los artículos que protegen la privacidad de usuarios en la red [11].

En México existe una organización denominada "ASI" (Alianza por la seguridad del internet) la cual en el año 2010 emitió un documento para poder conocer los delitos cibernéticos, como evitarlos y como denunciarlos [12].

Donde se mencionan como los delitos más comunes en el internet [12]:

- Ofertas falsas de empleo
- Fraudes financieros
- Agencias falsas de modelos
- El fraude nigeriano en internet.

El principal desafío que cita el documento del efecto internet emitido por "ASI" lo representa en, cómo comprobar la existencia y propiedad de la información que es robada [12].

Otra parte importante de la publicación de www.asi-mexico.org es la sesión de "internet en tu familia", determina que para poder orientar a los hijos sobre el buen uso de la tecnología no se necesita ser experto en ella, lo que preocupa hoy en día no son los medios digitales que los adolescentes utilizan, sino las actividades que con estos se realiza y que mayormente tienen que ver con el nuevo paradigma digital, es decir la preocupación debe concentrarse en con quien hablan, de que hablan, que relaciones construye, en que comunidades participan. Cuando hablamos de riesgos para menores de edad navegando en internet, los clasifica de la siguiente forma [12]:

- Contenido inapropiado: A todos los usuarios en especialidad los padres preocupan el contenido pornográfico, violento, obsceno, de drogas y demás con que nuestros hijos pueden encontrase en línea.
- Contacto inapropiado: Los grandes beneficios de internet no están disponibles únicamente para usuarios bien intencionados. Acosadores, depredadores y estafadores es un peligro para los menores de edad.

- Conducta inapropiada: El teórico anonimato puede dar lugar a conductas hostiles por parte de los usuarios.
- En documento emitido por "ASI" en su sesión internet en la familia describe una de las etapas fundamentales para el cometimiento de acoso especialmente en redes sociales el cortejo.

El proceso de "el cortejo" se lo especifica en siete etapas [12]:

1. Encuentro: sitios populares entre los menores de edad donde son ubicados por el acosador.
2. Compartir intereses: desarrollan la nueva "amistad" haciendo ver al menor cuantas cosas tiene en común.
3. Ganar confianza: Se gana su confianza con un apoyo constante a sus ideas.
4. Obtener secretos: Desarrolla intimidad con el menor, lo convence de que son mejores amigos, nada debe interponerse.
5. Romper barreras de resistencia: como esta relación es diferente a todas las demás, se establecen nuevos parámetros y fronteras.
6. Amenazas: Lo adentra en la posibilidad de exponer todo lo que han hablado como amigos, se supone que son cosas privadas, o peor aún, lastimar a su familia.
7. Encuentro físico: Sin importar cómo llegó aquí, el menor siempre es la víctima.

2.3 Efectos que se generan con estos delitos

Los efectos que se generan con estos delitos son muchos a considerar debido al fuerte impacto que tienen en sus víctimas estos pueden ser [13]:

- Viralización. - Se trata de difusión de contenidos, la viralización se produce en el momento que estos contenidos llegan a internet para luego en forma masiva pasa de dispositivo en dispositivo en redes sociales (WhatsApp, Twitter o Facebook).
- El anonimato. - Adolescentes quienes sufren, injurias, acosos, extorsión a través de redes sociales, pero por temor a la credibilidad o regaño de sus familiares, el rechazo de sus amigos la vergüenza, no se denuncia el hecho.
- El desprestigio social y laboral. - Existen casos donde personas son descalificadas no solo en su humanidad sino también profesionalmente, [13].
- Bajo rendimiento escolar. - Un alumno víctima del acoso tendrá efectos no solo en su contexto familiar sino también escolar, reflejándose en bajo rendimiento [13].
- Las tensiones que los adultos pueden trasmitir a los niños. - La ambivalencia señalada, hace que los padres y las madres, muchas veces hagan de las TIC un "chivo exploratorio", sobre el que depositan la causa de dos malestares: uno coyuntural (el encierro forzoso derivado de los contextos urbanos cada vez más inseguros); otro estructural (los progresivos desapegos de los hijos conforme van creciendo) [13].

3. Marco Legal

En Ecuador no existe una ley especial o capítulo del código penal ecuatoriano, que penalice los delitos relacionados con la tecnología o delitos informáticos. Muchos países de nuestra región cuentan hace varios años con leyes específicas para la penalización de prácticas delictivas relacionadas a la tecnología y la protección de datos como son:

- Colombia: En año 2009, se crea un nuevo bien jurídico tutelado denominado "De la protección de la información y de los datos".
- Perú: En octubre del 2013, se promulga la ley de delitos informáticos con 7 capítulos teniendo por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal.

Cómo legislar algo que físicamente no existe y cómo respaldar responsabilidad penal sobre un individuo u organización criminal detrás de un computador operando desde cualquier parte del mundo, son los principales interrogante al momento de plantear una legislación para este tipo de prácticas.

Una de las leyes vigentes en Ecuador es la "Ley de comercio electrónico, firmas y mensaje de datos" promulgada en el registro oficial el 22 de abril del 2002 cuya última modificación se dio el 11 de octubre del 2011.

Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas, cuenta con un capitulo denominado "Infracciones informáticas" donde se utiliza el término "daño informático" [14]. La

mencionada ley hace referencia a muchos artículos del Código integral penal anterior al año 2014; lo cual queda sin efecto, en el nuevo código integral penal publicado el 10 de agosto del año 2014.

El Nuevo COIP reemplazó a Código Penal vigente desde el año 1971, en este nuevo COIP se contemplan nuevos tipos penales y dentro de los cuales se hace referencia a delitos a través de medios telemáticos de manera generalizada:

- Artículo 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos. [15]
- Artículo 476.- Interceptación de las comunicaciones o datos informáticos. [15]
- Artículo 173.- Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos. [15]
- Artículo 230.- Interceptación ilegal de datos. [15]
- Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. [15]

Los otros tipos penales como la calumnia, la extorción, la estafa, violación a la intimidad, hacen solamente referencia entre el proceso de violación del artículo que también pueden ser por medios telemáticos, sistemas informáticos, soportes informáticos.

3.1 Estructura del sistema penal acusatorio en el Ecuador

El Código Orgánico Integral Penal es un cuerpo legal que define garantías básicas y principios generales del sistema de administración de justicia penal, dirigido a la infracción penal, el proceso y la ejecución punitiva. Este instrumento recoge definiciones conceptuales teóricas desarrolladas en la siguiente estructura según la guía para actuaciones del Fiscal dentro del Código Orgánico Integral Penal emitido por la Fiscalía General del Estado.

CÓDIGO ORGÁNICO INTEGRAL PENAL			
Libro preliminar: Garantías y principios generales del sistema penal.	Libro Primero: Concepto elemental de infracción circunstancias y responsabilidad. Catálogo de delitos.	Libro Segundo: Procedimiento para el juzgamiento de las personas con base en el debido proceso.	Libro Tercero: Ejecución punitiva, régimen y tratamiento penitenciario.

Figura 1. Estructura del Sistema Penal Acusatorio.

De esta manera está organizado el nuevo Código Integral Penal publicado en el registro oficial el 10 de agosto del 2014, el cual contempla un total de 77 nuevos delitos graves a la lista de crímenes que conllevan al encarcelamiento en el Ecuador [15].

Un punto muy importante que se describe en la guía para actuaciones del Fiscal dentro del Código Orgánico Integral Penal es el esclarecimiento sobre la participación de los actores en el hecho y su tipificación para lo cual se lo detalla en el siguiente cuadro [16]:

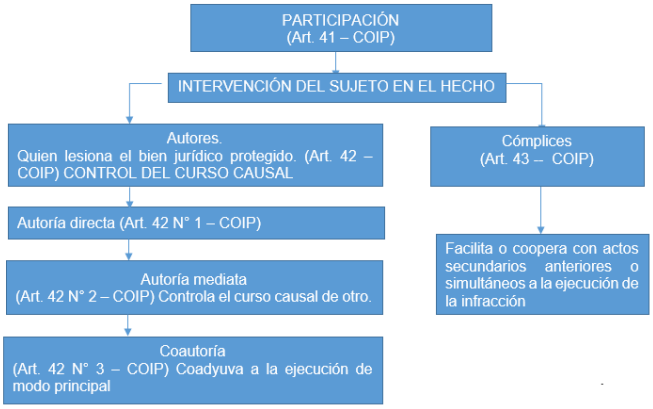

Figura 2. Participación de actores sobre el hecho según COIP.

Este cuadro resulta muy importante al momento de investigar delitos cometidos a través o en medios informáticos, el esclarecimiento sobre la participación de los actores en el hecho [17], en ocasiones, el dueño del equipo informático, o de la conexión de internet no es consiente del acto que se puede estar cometiendo con sus recursos técnicos, cabe considerar que un perfil de una red social puede ser robado, adulterado, clonado, lo mismo puede suceder con una conexión de red o a su vez un equipo telemático.

3.2 La investigación previa

El nuevo Código Integral Penal describe a la investigación previa como "La investigación de elementos de cargo y descargo que dan lugar a bases mínimas necesarias para realizar o no la imputación. Arts. 580, 584, 585.

Esta investigación tiene tiempos estipulados para su desarrollo los cuales son [16]:

- 1 año (Delitos con pena de hasta 5 años)
- 2 años (Delitos con pena mayor a 5 años)
- Indefinida (delitos de desaparición de personas).

Las investigaciones pueden archivarse solo por las tres causas aquí descritas [16]:

- No hay elementos de convicción (Art. 586,1)
- El hecho no constituye delito (Art. 586,2)
- Obstáculo legal insubsanable (Art. 586, 3)
- La conciliación (Art. 665, 2).

Todos los procesos y acciones descritas anteriormente están especificadas en la guía de actuación Fiscal dentro del Código Integral Penal, lo cual no es pertinente para investigaciones relacionadas con la tecnología porque pueden duran horas, días o años.

3.3 Problemas para identificar estos delitos y sus responsables

El principal desafío para poder identificar los delitos informáticos, consisten en que no siempre se utiliza como fin la tecnología, para esto se divide en 3 tipos según el objetivo del delito. [18]:

- La Tecnología es el fin
- La Tecnología es el medio
- La Tecnología es incidental.

Entre los desafíos a los que se enfrentan las fuerzas del orden, al momento de investigar delitos cometidos usando medios telemáticos y en especial nuestro enfoque que son las redes sociales tenemos a [18]:

- Globalización
- Falta de Marco Legal
- Falta de Capacitación
- Falta de Recursos
- Tecnología y la Sociedad

4. Materiales y métodos

Se realizó una investigación mixta comprendiendo procesos cuantitativos como estadísticas de reportes de delitos relacionados con la tecnología, informes de diferentes organizaciones como la UNICEF en su informe titulado “la seguridad de los niños en línea”, el observatorio para el cibercrimen en Latinoamérica y el Caribe [19], y la aplicación de una encuesta en una muestra determinada. Para los procesos cualitativos se aplicaron entrevistas a un agente fiscal y un representante de la policía judicial, así como la revisión bibliográfica de artículos y libros relacionados con el tema, lo cual nos permitió dar un alcance descriptivo.

Se aplicó método inductivo en el análisis de datos para establecer conclusiones o teorías universales que relacionan fenómenos, ya que actualmente en el país no existen estadísticas sobre índices de delitos cometidos a través de redes sociales como Facebook. Se cuenta con muy poca información al respecto por lo que debemos estudiar casos singulares. Se considera pertinente basarnos de la experiencia de agentes Fiscales, Policías Judiciales y Peritos, lo cual aporta una perspectiva no solo local sino global del actual tratamiento de los delitos cometidos a través de redes sociales como Facebook.

4.1 Entrevista

Se realizó un diálogo directo, con un agente fiscal y un teniente de la policía judicial con el fin de percibir cuales son los procesos o acciones de las fuerzas del orden, para proceder en este tipo de eventos o a su vez verificar la existencia de una técnica o método establecido para la investigación de delitos a través de redes sociales.

Para nuestro trabajo utilizamos el tipo de entrevista informativa, en la que el entrevistador pretende obtener información sobre un tema determinado para nuestro caso “delitos cometidos a través de redes sociales” donde se captó información valiosa sobre el tratamiento actual de este tipo de comportamientos antijurídicos.

4.2 Encuesta

Para realizar una encuesta el primer paso es seleccionar una muestra, para esto necesitamos definir las características que integran a nuestra población de estudio, estableciendo la particularidad que tendrán para nuestro caso el grupo de usuarios de la red social de Facebook.

El tipo de muestra se determinó como probabilística estratificada, cuando no basta que cada uno de los elementos muestrales tenga la misma probabilidad de ser escogidos, sino que además es necesario segmentar la muestra en relación con estratos o categorías que se presentan en la población y que además son relevantes para los objetivos de estudios. [20]

Para esto basamos las categorías en los resultados de la encuesta nacional de empleo y desempleo 2012-2015 realizada por el INEC [21] donde califica el grupo etario con mayor número de personas que utilizaron computadora es el que está entre 16 a 24 años con el 76,1%, el grupo de 25 a 34 años 57,6%, un grupo de 35 a 44 años con un 45% y el último considerado entre 45 – a 54 años con un 31,9%. Todos estos resultados

corresponden al año 2015. Basados en estos indicadores segmentaremos nuestra población para obtener nuestra muestra.

Se eligió una población comprendida por adolescentes de los colegios de bachillerato, personas comunes de las avenidas y un grupo de adultos pertenecientes a una organización de trabajadores en total se realizaron 467 encuesta donde se intentó estimar la apreciación de los usuarios de las redes sociales.

Al no existir información verificada de entidades oficiales de justicia sobre delitos cometidos a través de redes sociales en el Ecuador, el investigador se basó en conocimiento como perito y en referencias de otros estudios, para desarrollar y aplicar una encuesta, tomado la población de **42.610 habitantes (**Según último censo de población y vivienda 2010 aplicado por el INEC**)** con los que cuenta el Cantón La Troncal provincia del Cañar.

El censo de población y vivienda 2010 divide los siguientes intervalos de habitantes por edad, para nuestro estudio tomaremos en cuenta las edades de entre 15 y 54 años que basados en los resultados del censo [22]tenemos un total de 23.172 habitantes para determinar nuestra muestra utilizaremos el programa Launch Stat 2.0 el cual nos indica una muestra de: 378 habitantes a encuestar asumiendo un margen de error de 5%.

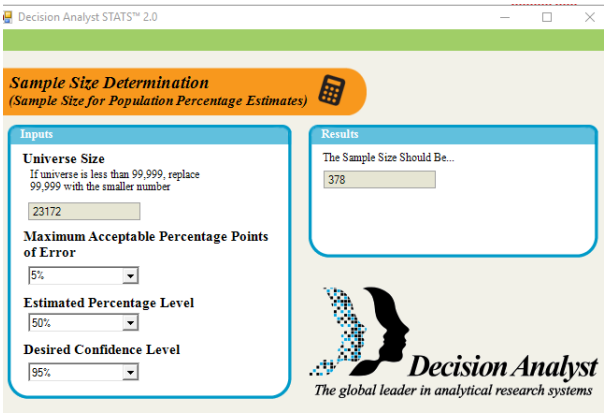

Figura 3. *Software* estadístico STATS 2.0.

5. Resultados

Una vez establecido el valor mínimo de la muestra en 378 habitantes asumiendo un error del 5%, se procede a estratificar la muestra de la siguiente forma. Se ha considerado a un total de 467 sujetos para abordar el total de integrantes de la Junta Cantonal del Artesano.

Tabla 1. Clasificación de la Muestra

Entidad de aplicación	N. Encuestas
Junta Cantonal del Artesano	67
Colegio Tomas Rendón Solano	150
Universidad Católica de Cuenca Sede san Pablo de La Troncal	150
Habitantes en General	100
Total, de la Muestra	**467**

Para el cuestionario de la encuesta nacional de empleo y desempleo, se realizaron las siguientes preguntas:

1. ¿Es usted usuario de Facebook?
2. ¿Con cuántos amigos cuenta usted aproximadamente en la red social Facebook (se categorizaron 6 intervalos desde el 1 a 1000 y el ultimo abierto superior a mil)?
3. ¿De sus amigos en la red de Facebook indique aproximadamente cuantos conoce realmente (se colocaron 5 intervalos de 1 a 1000)?
4. ¿Tiene usted conocimiento de los delitos comunes que se comenten a través de Facebook?
5. ¿Ha sido víctima usted de algún delito a través de Facebook?
6. ¿Indique el tipo o tipos de delitos que cree haber sido víctima a través de Facebook? (se colocaron un total de 20 delitos comunes)
7. ¿Cuándo se presentó el incidente dio parte a las autoridades de Justicia?
8. ¿Por qué no se dio conocimiento del hecho a las autoridades?
9. ¿Cuándo se reportó el incidente, la respuesta a su requerimiento fue? (Inmediata, no tan inmediata y demoró mucho).
10. ¿La ayuda que prestaron las entidades de justicia permitió que el caso? (Se solucionó, no se solucionó, se archivó).
11. ¿Conoce sobre la configuración de privacidad y seguridad para las cuentas de Facebook?
12. ¿Cuándo usted crea un perfil de Facebook usa? (Su nombre, Seudónimo, Otro personaje).

Realizado el trabajo de campo se obtuvieron datos importantes donde el 97% de los encuestados utiliza la red social Facebook, sobre el número de amigos un 26%

indicó que tiene menos de 200 amigos mientras que un 15% indicó que tiene entre 801 y 1000 amigos, otro 20% entre 401 y 600 amigos, los encuestados también reconocieron según datos ponderados que conocen a menos del 45% de todos sus amigos en Facebook, un 71% de los encuestados reconoció que sí tienen conocimiento del cometimiento de delitos a través de redes sociales, un 23% reconoció haber sido víctima de amenazas, acosos, extorsión y *hacking* de sus cuentas de usuario. El 96% de los que reconocieron haber sido víctimas de estos delitos indicó que no dieron parte a las autoridades porque prefirieron ignorarlo o creyeron que no sería necesario.

El restante 4% que sí dio parte a las autoridades y se obtuvieron que un 75% indicar que no se recibió respuesta inmediata y el 25% restante que denunció en hecho indica que demoró mucho.

Tabla 2. Tabla de datos

Opciones	Indicadores	Porcentajes
Inmediata	0	0%
No tan inmediata	3	75%
Demoró mucho tiempo	1	25%
Total	4	100%

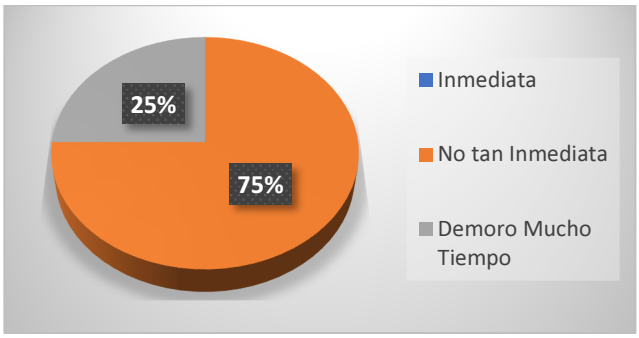

Figura 4. Respuesta al incidente.

Un resultado muy interesante fue el porqué, no se dio conocimiento del hecho a las autoridades se representa por el siguiente gráfico.

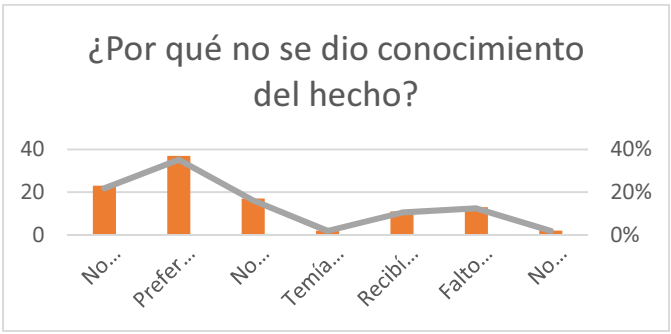

Figura 5. Por qué no se dio conocimiento.

Los indicadores más relevantes: un 35% fue que prefería ignorarlo y un 22% que el usuario no consideró necesario dar conocimiento del hecho, un 16% no sabía que se podía denunciar, solo un 2% indicó que no lo hizo por temor a represalias, un 10% indica que recibió amenazas, un 12% indica que no contó con asesoramiento, y un 2% que no recibió la ayuda necesaria cuando intentó denunciar.

6. Análisis de la situación actual

Según la investigación de campo realizada no existe un estudio completo respecto a delitos comunes en redes sociales en el Ecuador y las autoridades locales no cuentan con el conocimiento de los convenios de cooperación internacional y el aporte que pueden otorgar las empresas web 2.0 a la investigación de un delito, por otra parte según los datos recabados de páginas que pertenecen a las fuerzas del orden como www.ministeriointerior.gob.ec, entidades de justicia como www.policiaecuador.gob.ec/dnpj/ y el sitio web de www.fiscalia.gob.ec [23], y la Unidad de Cibercrimen que actualmente se restaura como Observatorio del cibercrimen, lamentablemente no cuenta con un sitio web oficial, únicamente publican contenidos en una página de Facebook en https://www.facebook.com/CibercrimenPJ.EC, no se cuenta con una guía de prevención e investigación de delitos comunes cometidos a través de redes sociales que permita investigación de forma local y oportuna.

El Policía Judicial entrevistado indicó que los datos de cualquier delito o sospecha del mismo realizado a través de redes sociales como Facebook se envía directamente mente a Quito y no tiene respuesta oportuna.

También se verificó en las autoridades judiciales del Cantón la Troncal no se cuenta con gran número de

denuncias realizas por conductas delictivas asociadas a las redes sociales, pero se encontró otra gran variante respecto a este tema, ya que actualmente se apoyan las fuerzas del orden en las redes sociales para sus procesos de investigación de cualquier delito con el objetivo de recabar datos de posibles sospechosos. Las encuestas verificaron que sí existen víctimas de delitos comunes a través de redes sociales como Facebook, pero que por el desconocimiento y el descontento con los procesos inciden en las decisiones de denunciar este tipo de delitos y prefieren ignorarlos u ocultarlos.

6.1 Estadísticas de usuarios falsos en Facebook

En el año 2012 los profesionales de WebSide realizo una infografía graficando la información que Facebook otorgara a la US Segurities and Exhange Comission de manera trimestral, la cual fue traducida al idioma español en el sitio Soxialmedia. De esta manera, interpretando los datos del reporte logramos tener una idea clara sobre cuantos usuarios reales y activos hay en Facebook [24].

En el informe presentado a la Comisión de Valores de Comercio de los Estados Unidos, se indicó que el 5% de los 955 millones de usuarios tienen cuentas duplicadas y que alrededor de 83 millones de cuentas son falsas [25].

Tabla 3. Cuentas falsas en Facebook

Cuentas duplicadas	45.000.000
Cuentas de spam	15.000.000
Cuentas de usuario mal clasificadas	23.000.000

En la entrevista realizada al agente fiscal nos indicó que el nuevo Código Orgánico Integral Penal regula en formas especificas los delitos que se cometen a través de medios informáticos incluso en formas más detalladas los elementos constitutivos, para cada tipo penal de esa naturaleza, delitos contra la seguridad de los activos, de los sistemas de información y comunicación.

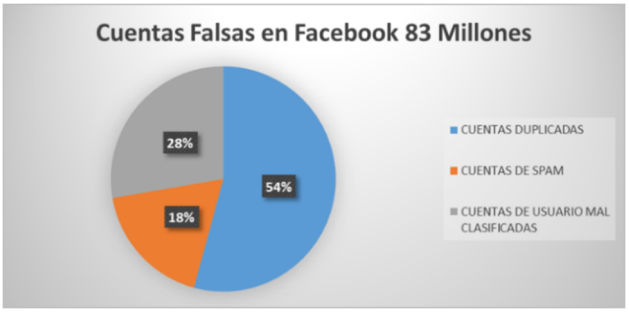

Figura 6. Cuentas Falsas.

Sobre los métodos indicó que llevan un proceso adecuado, porque la misma norma procesal contenida en el COIP, la Fiscalía cuenta con peritos especializados, afines a delitos informáticos con los cuales sirven de elementos de convención, para establecer en primero que tipo de delitos informáticos y determinar los procesos del mismo, que está a cargo del sistema especializado integral de investigación de medicina legal y ciencias forenses, no la respuestas a los requerimientos por este organismo no siempre es oportuna.

También nos indicó el apoyo que representan las nuevas tecnologías en casos de algunos delitos y por experiencia a través del sistema de mensajería instantánea de nombre WhatsApp, mediante indicio inicial de un número telefónico se llegó a determinar la imagen fotográfica de un sospechoso el cual una vez que fue verificada su identidad en los sistemas de archivos de la Policía se llegó a determinar su identidad. Asímismo con este índice se logró determinar el perfil público en la red social Facebook, logrando constatar en el mismo la foto de evidencia que relacionó al sospechoso con el delito perseguido.

En la entrevista realizada al agente de la policía judicial se constató que tienen plenamente identificados los artículos de COIP que contemplan delitos o conductas antijurídicas en las redes sociales, que la PJ (Policía Judicial), cuenta con herramientas TI (Tecnologías de Información) para dar seguimiento e investigación a este tipo de delitos, con la desventaja que estas herramientas las manejan los agentes en las ciudades principales del Ecuador, sobre su experiencia con las redes sociales en delitos, indica que personalmente a trabajado en delitos comunes y se ha utilizado redes sociales como Facebook y WhatsApp para logran la identificación de sospechosos.

Considera que estas herramientas TI aportan mucho al desarrollo de investigaciones, pero que aún falta mucha capacitación para los agentes del orden respecto a estos temas, no solo para el cuerpo de ley, también lo usuarios necesitan conocer que los delitos que utilizan redes sociales como medio están contemplados en el COIP y pueden ser sancionados.

7. Conclusiones

- Las personas que indicaron tener más de 400 amigos se relacionan con que conocen solo el 45% de ellos.
- Más del 70% de los encuestados indica tener conocimiento de los delitos comunes que se realizan a través de redes sociales como Facebook.
- A pesar de que el tema parece un poco alarmante en estos tiempos solo un 23% de todos los encuestados indicó haber sido víctima de algún tipo de delitos a través de la red social como Facebook.
- Los tres principales delitos identificados en el presente estudio son, acoso, amenaza y robo de cuenta de usuario.
- El 96% de los encuestados, que reconoció haber sido víctima de un delito, indicó que no dio conocimiento a las autoridades, lo que puede relacionarse al desconocimiento de la penalización de estos delitos.
- La investigación bibliográfica indicó que no existe información estadística completa o de fuentes oficiales sobre los delitos comunes a través de redes sociales como Facebook, lo que se relaciona directamente por el tipo penal que se identifican los delitos.
- Los agentes del orden conocen los efectos y delitos que se cometen a través de redes sociales, pero no tienen definida una metodología de investigación exclusiva para delitos de este tipo y los agentes especializados son muy poco en el área de la informática, pero se encuentran en las unidades de las ciudades principales, existen víctimas de este tipo de delitos, pero en las fiscalías se reciben muy pocas denuncias de este tipo.
- La principal vulnerabilidad para el cometimiento de los delitos en redes sociales es el usuario, que desconoce plenamente el marco legal existente en el Ecuador para delitos cometidos a través de medios telemáticos.
- Hasta la fecha de realización del presente estudio, los agentes del orden locales no conocen el procedimiento de petición de información sobre un perfil de usuario a Facebook con fines de investigación.

8. Agradecimiento

Agradecimiento a los agentes de la PJ del Cantón La Troncal quienes muy respetuosamente brindaron la información solicitada. Fiscalía provincial de la provincia del Cañar. Al Fiscal Milton Bernal Patiño quien nos brindó su tiempo para realizar la encuesta y estuvo siempre presto a responder nuestras inquietudes.

9. Referencias

[1] C. V. G. G. y. M. V. Por Nora Paterlini, “www.aadat.org,” 2015. [En línea]. Available: http://www.aadat.org/delitos_informaticos20.htm. [Último acceso: 22 01 2017].

[2] A. Nacional, Ley Orgánica de comunicación, Quito: Almacen Editora Nacional, 2013.

[3] J. O. Luis, “Los procesos seguidos en la investigación de los principales delitos comunes, cometidos a través de redes sociales, denunciados en el cantón la troncal, provincia del Cañar y su influencia en la identificación del autor material e intelectual.,” Unemi, Milagro, 2015.

[4] A. D. Cea Jiménez, Los delitos en las redes sociales: aproximación a su estudio y clasificación, 2012.

[5] O. D. E. Americanos., “Guía de manejo de las redes Sociales e Internet.,” OEA, Washington, 2009.

[6] S. P. Release, “Shophos,” 01 02 2010. [En línea]. Available: http://www.sophos.com/es-es/press-office/press-releases/2010/02/security-report-2010.aspx. [Último acceso: 18 02 2015].

[7] A. G. YUSTE, “Delitos informáticos: malware, fraudes y estafas a través de la red y cómo prevenirlos,” LEGANÉS, 2012.

[8] ESET, “argentinacibersegura,” 6 Noviembre 2013. [En línea]. Available: https://www.argentinacibersegura.org/. [Último acceso: 03 06 2016].

[9] G. d. d. telemáticos, “Fundación guardia Civil.,” 2015. [En línea]. https://www.gdt.guardiacivil.es/webgdt/home_alerta.php.

[10] Welivesecurity, “welivesecurity,” 2013. [En línea]. Available: https://www.welivesecurity.com/wp-content/uploads/2014/01/documento_redes_sociales_baja.pdf. [Último acceso: 12 08 2015].

[11] Elpais, “www.eldiario.es,” 06 06 2013. [En línea]. Available: http://www.eldiario.es/zonacritica/Troyanos-investigacion-policial-justifica-medios_6_140395962.html. [Último acceso: 21 11 2014].

[12] Efectointernet.org, “efectointernet,” 2010. [En línea]. Available:http://asimexico.org/sitio/archivos/Efecto_Internet_a_1_n_1_Revista_baja.pdf.

[13] A. chicos.net, “Impacto de la Tecnología en niñas y niños de América Latina.,” 2015.

[14] C. Nacional, "http://www.oas.org," 2012. [En línea]. Available: http://www.oas.org/juridico/pdfs/mesicic4_ecu_comer.pdf. [Último acceso: 06 11 2016].
[15] D. H. y. C. S. d. D. N. Ministerio de Justicia, Código Orgánico Integral Penal, Quito: Ministerio de Justicia, 2014.
[16] M. D. G. B. A. M. Dr. Xavier Andrade Castillo, "Guía para Actuaciones del Fiscal dentro del Código Orgánico Integral Penal," Escuela de Fiscales de la Fiscalía General del Estado, Quito, 2014.
[17] D. A. Z. Pasquel, "La Teoría de la Participación," Judicatura Online, pp. 55-60, 2009.
[18] P. M. A. D. Cibercrimen, "Delitos Informaticos Aventuras y Desventuras," Policía metropolitana, BUENOS AIRES, 2014.
[19] I. N. D. Ciberseguridad, "INCIBE," 28 05 2014. [En línea]. Available: https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/osint_la_informacion_es_poder.
[20] E. A. R. MOGUEL, Metodología de la investigación, vol. QUINTA EDICIÓN, U. J. A. D. TABASCO, Ed., MÉXICO, 2005.
[21] INEC, "Encuesta Nacional de Empleo y Desempleo 2012-2015," ecuadorencicfras, Quito, 2016.
[22] INEC, "ecuadorencifras," 2012. [En línea]. Available: http://www.ecuadorencifras.gob.ec/base-de-datos-censo-de-poblacion-y-vivienda-2010/. [Último acceso: 12 10 2016].
[23] F. G. d. Estado, "Fiscala," 13 Junio 2015. [En línea]. Available: http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.html.
[24] WebSide, "WebSide," 29 Octubre 2012. [En línea]. Available: http://soxialmedia.com/infografia-estadisticas-de-usuarios-falsos-en-facebook/.
[25] N. Unidas, "12º Congreso de las Naciones Unidas sobre prevención del delito y justicia penal.," Salvador(Brazil), 2010.
[26] A. R. A. R. Egil Emilio Ramírez Bejerano, "Eumed," 05 2009. [En línea]. Available: http://www.eumed.net/rev/cccss/04/rbar2.htm. [Último acceso: 17 02 2015].
[27] D. P. Consuelo Ramos, "Portal.oas.org," 11 2009. [En línea]. Available: http://portal.oas.org/LinkClick.aspx?fileticket=RHIdC3cS3Qw%3D&tabid=1483. [Último acceso: 18 02 2015].
[28] D. E. Universo., "El Universo," 12 Junio 2014. [En línea]. Available: http://www.eluniverso.com/noticias/2014/06/12/nota/3093076/fiscalia-allana-dos-viviendas-caso-publi-fast.
[29] M. D. Interior, "Ministerio del Interior del Ecuador," 02 abril 2015. [En línea]. Available: http://www.ministeriointerior.gob.ec/policia-nacional-frena-actividad-ilicita-de-tres-organizaciones-delictivas-y-a-sujeto-dedicado-a-la-pornografia-infantil/.
[30] (RVD), "ecuadorinmediato.com," 3 Septiembre 2013. [En línea]. http://www.ecuadorinmediato.com/index.php?module=Noticias&func=news_user_view&id=204235&umt=proyecto_codigo_penal_contempla_hasta_2_anos_prision_para_injurias_y_calumnias. [Último acceso: 23 Agosto 2014].
[31] www.eltelegrafo.com.ec, "Delitos electronicos.," 25 junio 2014. [En línea]. Available: http://www.telegrafo.com.ec/justicia/item/hay-600-casos-de-delitos-electronicos-en-17-meses.html. [Último acceso: 19 Noviembre 2014].
[32] C. N. D. Ecuador, Ley de comercio electronico, mensaje de datos y firmas digitales, Quito, 2002.
[33] U. I. D. telecomunicaciones, "El ciberdelito guia para paises en desarrollo.," @UIT, Ginebra, Suiza, 2009.
[34] A. D. C. Jiménez, "gredos.usal.es," 2012. [En línea]. http://gredos.usal.es/jspui/bitstream/10366/121119/1/Los%20delitos%20en%20las%20redes%20sociales%20una%20aproximaci%C3%B3n%20a%20su%20estudio%20y%20clasificaci%C3%B3n.%20Andrea%20de%20Cea%20ji.pdf. [Último acceso: 22 Diciembre 2014].