

# ESTUDIO DE LA UTILIZACIÓN DE LAS TIC EN LA ADMINISTRACIÓN DE JUSTICIA DE LA CIUDAD DE GUAYAQUIL.

***Mercedes Cecilia Coronel Gómez, Mgs.***

Magíster en Planificación, Acreditación y Evaluación de la Educación Superior, especialista en Derecho civil, compañías, niñez y adolescencia y Abogada de los Tribunales y Juzgados (Ecuador).

Docente Tiempo Completo de la Facultad de Derecho y Gobernabilidad de la Universidad Tecnológica ECOTEC, Ecuador.  
mecoronel@ecotec.edu.ec

## **ARTÍCULO DE REFLEXIÓN**

Recibido: 16 de mayo de 2019.

Aceptado: 2 de julio de 2019.

## **RESUMEN**

Este trabajo tiene como objetivo brindar una visión global del estado de formación de los especialistas en los delitos informáticos en la administración de justicia en la sociedad ecuatoriana; en cuanto a su regulación, iniciativas de investigación, tecnología y capacitación del talento humano que investiga dichos delitos, así como también identificar los retos y brechas que debe ser superada por la administración de justicia en la sociedad ecuatoriana para el tratamiento de los mismos. Para la ejecución de este estudio se acogió un diseño cualitativo que consistió en la revisión de bibliografías correspondientes a la temática, investigaciones, documentos oficiales de instituciones públicas, legislación y jurisprudencia nacional e internacional existente en las instituciones que conforman el ordenamiento jurídico ecuatoriano. La técnica utilizada fue el análisis documental y análisis de la información histórica y estadística de entes públicos y privados, así como la investigación descriptiva que se requiere utilizar cuando los procesos tienen una excesiva complejidad y se requiere describirlo del modo más objetivo y minucioso posible, para generar afirmaciones y posiciones. Se abordó el marco conceptual de los delitos y la criminalidad informática y las leyes en la legislación ecuatoriana con la finalidad de establecer la necesidad de estudios Tecnológicos Superiores Informático Jurídico de los operadores de justicia en el Ecuador.

Palabras clave: ley, delito, tecnología, administración, justicia.

## **ABSTRACT**

This work aims to provide a global vision of the training status of specialists in computer crimes in the administration of justice in Ecuadorian society; regarding its regulation, research initiatives, technology and training of human talent that investigates such crimes, as well as identifying the challenges and gaps that must be overcome by the administration of justice in Ecuadorian society for the treatment of them. For the execution of this study, a qualitative design that consisted of the review of bibliographies corresponding to the subject, research, official documents of public institutions, legislation and national and international jurisprudence existing in the institutions that make up the Ecuadorian legal system was accepted. The technique used was the documentary analysis and analysis of the historical and statistical information of public and private entities, as well as the descriptive research that is required to use when the processes have an excessive complexity and it is required to describe it in the most objective and thorough way possible, to generate affirmations and positions. The conceptual framework of crimes and computer crime and the laws in Ecuadorian legislation were addressed in order to establish the need for Higher Technological Studies of Computer Law of justice operators in Ecuador.

Keywords: law, crime, technology, administration, justice.

## **INTRODUCCIÓN**

La administración de justicia en la sociedad se ha visto profundamente transformada con la aparición de las nuevas tecnologías de la información y las comunicaciones (TIC); las omnipresentes computadoras interconectadas en la red mundial llamada Internet son el signo más evidente del impacto que tienen hoy; para las telecomunicaciones, el tráfico comercial y el entretenimiento, estas tecnologías son prácticamente indispensables. En ellas, al igual que en muchas otras, es imposible alcanzar resultados económicos aceptables y beneficiosos, tanto para los particulares como para la administración de justicia en la sociedad en general, sin su utilización. Esto es perfectamente aplicable al sistema judicial, que para cumplir con su función de administrar justicia básicamente debe tratar información en cantidades crecientes (Gómez, 2011).

Pero en relación al impacto en el sistema judicial de las tecnologías de la información, se aborda el uso de las potencialidades de las TIC, que es imprescindible para la Administración de Justicia informar sobre cuáles son los elementos, componentes, las diligencias y/o documentos (Obtención de Evidencia, Acta de Posesión, Informe de Pericia, etc.), habilitantes en el proceso de designación

y realización de la pericia Informática; así como también cuáles son las implicaciones legales ante un hecho jurídico informático. Conocer cuáles son las iniciativas internas (Policía Judicial, Ministerio Público) y externas (OEA), que permiten mejorar el manejo en la administración de justicia ante los delitos informáticos en este medio, habilitando y definiendo aspectos legales que posibiliten la regulación y la tipificación de los delitos informáticos (Gómez, 2011).

También es importante identificar de forma general cuáles son los aspectos contemplados en las leyes de los países a nivel latinoamericano que cuentan en su legislación con las leyes que regulan los delitos informáticos, establecer cuáles son los retos (legales, tecnológicos, etc.) que se presentan ante el manejo de un delito informático antes, durante y después de un proceso de pericia informática; es primordial que se tenga un claro entendimiento de que se requiere en la petición de la pericia, alcance de la pericia, tipo, comprensión del informe, etc. Así como también establecer cuáles son las condiciones de los factores (educación, sistema legal, tecnología, entre otros) y qué aspectos están siendo contemplados por dichos factores (Gómez, 2011).

Es importante destacar que en el Ecuador se están iniciando los primeros pasos, donde en algunas universidades se han adicionado en sus mallas curriculares de las carreras de Derecho, la disertación de derecho informático y propiedad intelectual (Mallas Curriculares), que permiten preparar a los profesionales desde una etapa muy temprana, sobre aspectos generales como las regulaciones existentes y que atañen a las tecnologías, así como también, el desarrollo y progreso de países vecinos en cuanto a la legislación habilitante para perseguir estos actos ilícitos no solo bajo la perspectiva local sino transnacional.

Lo primero que sorprende a cualquier analista del sistema de administración de justicia ecuatoriana es, posiblemente, el enorme retraso que esta parte de la administración pública ofrece frente al resto del sector público. Configurada tradicionalmente como una suerte de administración pública singular, individualizada por su función y, sobre todo, por el estatuto jurídico del personal a su servicio. Lo cierto es que la administración de justicia ha caminado tradicionalmente con unas dosis muy fuertes de autonomía frente al resto de administraciones públicas, autonomía que se ha venido justificando en que al fin y a la postre esa administración era el instrumento de gestión de un poder judicial. En todo este proceso de individualización de la administración de justicia ha jugado, una vez más, un papel determinante la evolución histórica, o si se prefiere las tradiciones porque en honor a la verdad del texto constitucional, no se puede derivar con claridad meridiana que a la administración de justicia no le sean de aplicación los principios y reglas constitucionales predicables de la administración pública, en general. Es cierto que en la Constitución se recoge una reserva específica a un tipo concreto de código orgánico que será la que deba determinar “la constitución, funcionamiento y Gobierno de los Juzgados y Tribunales, así como el estatuto de

jueces y tribunales, que formarán un cuerpo único, y del personal al servicio de la administración de justicia” (Judicial, 2010). Por esta razón, el objetivo principal de esta investigación es proporcionar una visión global del estado de formación de los especialistas en los delitos informáticos en la administración de justicia en la sociedad ecuatoriana.

## **REVISIÓN TEÓRICA**

### **Situación actual del delito informático en la administración de justicia en la sociedad, Guayaquil.**

La investigación de la delincuencia informática, no es una tarea fácil, ya que la mayoría de los datos probatorios son intangibles y transitorios. Los investigadores de delitos cibernéticos buscan vestigios digitales que de acuerdo a sus características suelen ser volátiles y de vida corta. Hay que considerar que la Internet brinda beneficios a los usuarios, pero su fácil acceso también podría perjudicarlos. Según las estadísticas de marzo del 2019, la Agencia de regulación y control de las telecomunicaciones en Ecuador - ARCOTEL, hay alrededor de 11´148.222 usuarios de Internet, los cuales corren un alto riesgo de ser perjudicados mediante actos delictivos como la ingeniería social, estafa, un ataque de ‘Phishing’ u otros, relacionados con las tecnologías (ARCOTEL, 2019, p. 2).

Las cifras sobre los delitos informáticos, en Ecuador también son inciertas, las pocas denuncias que se presentan, ya sea por la falta de conocimiento o interés impide la lucha contra este tipo de delitos, es importante considerar los retos particulares que están latentes a todo nivel e incluso para los actores involucrados, en el manejo de los delitos informáticos, sean estos el Ministerio Público, la Policía Judicial, la Corte de Justicia, investigadores, y hasta la misma sociedad.

La Administración de Justicia en el momento que se encuentra actualmente necesita tener profesionales en Derecho que tengan conocimiento en la parte informática, para que con su sustento legal puedan analizar debidamente este tipo de delitos con uso de las TICS; la necesidad de profesionales especializados en el marco de la criminalidad informática que estén en capacidad de diferenciar los delitos informáticos del resto y de definir su tratamiento dentro del marco legal; tener especialistas académicos y no empíricos en el tratamiento de los delitos informáticos, así como tener instituciones de educación superior y/o tecnológicos que generen a la administración de justicia en la sociedad ecuatoriana profesionales especializados en la rama.

A continuación, en el gráfico se presentan las causas del problema y sus consecuencias de una manera más fácil de comprender:

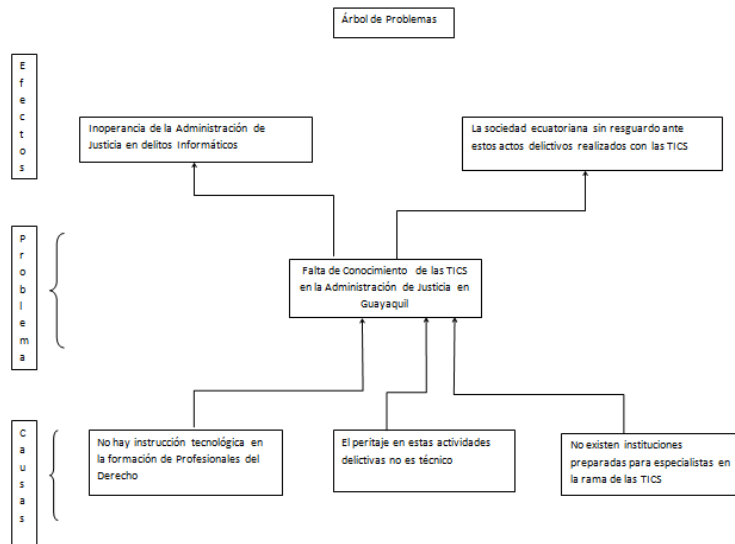


Figura 1. Causas del problema y consecuencias.

Fuente: Elaboración propia.

El cambio en el entorno social y el crecimiento constante de la tecnología, es profundo: las relaciones de la tecnología en la administración de justicia en la sociedad de un modo radical, y se encuentran frente a actividades que no sólo tienen incidencia directa en la sociedad, sino que, a diferencia de otros actos delictivos no se tiene profesionales especializados en la temática, no se está preparado sensiblemente para entender y responder a los mismos. ¿Cómo se puede identificar y procesar actos delictivos tecnológicos sin especialistas? ¿Cómo responder a la administración de justicia en la sociedad sin talento humano preparado para estas tipologías delictivas?

Al establecer nuestro problema como el no tener personal especializado no actualizado a las nuevas tendencias tecnológicas en cuyas causas van:

No existencia de un Plan de Capacitación adecuado; estableciendo formas de capacitación que tienen que ser modificadas para un mejor desempeño del profesional del derecho en la administración de justicia; necesitando establecer una adecuada relación con la gestión pedagógica de los procesos de aprendizaje y en enseñanza al interior de los cuales se consideren varios puntos: la planificación, las estrategias y técnicas, el dominio de la especialidad y la gestión educativa. Elaborando planes de capacitación reconfigurando la estructura actual del sistema implementado en función de generar y favorecer aprendizajes de calidad.

A continuación, se detallan bajo este contexto algunos inconvenientes para el manejo de delitos informáticos por la falta de especialistas en la rama:

- Ausencia de infraestructura y tecnologías adecuada en los entes u organismos de la administración de justicia en investigación como: el Ministerio Público y la Policía Judicial. Las investigaciones o experticias a nivel informático en su mayoría se dan por denuncias realizadas bajo otro contexto de delitos tales como: robo, daño a la propiedad, estafas, entre otros, que son llevadas por Unidades del Ministerio Público como: la Unidad de Delitos Misceláneos, Unidad de Delitos Financieros y de Telecomunicaciones, Unidad de Daños contra la Propiedad, debido a la falta de una regulación, o unidad que opere este tipo de infracciones.
- Falta de iniciativas que permitan el desarrollo de brigadas y unidades estructuradas y especializadas, para la investigación de los delitos de índole informático, nacional y transnacional, desde su inicio con el levantamiento de evidencias hasta la aplicación de procedimientos de mayor complejidad.
- Inconvenientes en la comunicación entre los especialistas informáticos y los judiciales; mantener un lenguaje común entre los especialistas de informática y los operadores judiciales es trascendental, principalmente, al exponer por parte del especialista en derecho informático, los criterios utilizados en el desarrollo de la investigación ante una investigación judicial.
- Procedimiento inadecuado para la calificación de especialistas en actividades ilícitas informáticas por parte del Ministerio Público y demás entidades u organismos; otro aspecto, a considerar es la problemática legal, que se presenta cuando este tipo de delitos traspasa las fronteras y las jurisdicciones, lo que pone en relieve la importancia de la cooperación internacional.

### **Ausencia de planes, programas, estrategias de Capacitación en la Administración de Justicia.**

- Desarrollo de programas de capacitación al órgano legal (Fiscales, Jueces, Abogados) sobre los delitos informáticos y la informática legal.
- Capacitación a los profesionales de tecnología en aspectos básicos de informática legal, forense, criminalística, manejo de evidencias digitales, etc. en la administración de justicia en la sociedad ecuatoriana.
- Fomentar el desarrollo de programas que involucren la disertación de especialistas en derecho informático, en legislación existente que atañe a la criminalidad informática en la administración de justicia en la sociedad ecuatoriana.
- Desarrollo de programas de especialización que contemplen profesionales en informática forense y/o legal que pueden darse en cooperación con organismos especializados o entre convenios universitarios en la administración de justicia en la sociedad ecuatoriana.

*Falta de interés en la sociedad.*

- Advertir a los usuarios sobre las posibilidades u probabilidad de ocurrencia de delitos informáticos.
- Difusión de medidas de salvaguarda tal como el cierre de brechas de seguridad, como medidas de prevención ciudadana ante delitos de índole tecnológico.
- Concientización en las organizaciones de que las medidas de seguridad más que un gasto son una inversión que proveen mecanismo para evitar este tipo de delitos.
- Concientización del efecto e impacto de los delitos informáticos sobre la sociedad.

*Falta de intervención y asignación de recursos del Estado.*

- Convenios institucionales (universidades, gremios, etc.)
  - Cooperación y transferencia de conocimiento con países vecinos, o con quienes se hayan establecido convenios internacionales, sobre la tecnología existente o el desarrollo de las mismas que permitan la persecución de los delitos informáticos.
- Implementación de laboratorios especializados forenses informáticos.

**Actividades ilícitas tipificadas como delitos de redes sociales en el Código Orgánico Integral penal.**

- Robo y/o suplantación de Identidad (212 COIP – No Delito Informático)
  - Robots (Unidas, 2009)
  - Perfiles falsos (Unidas, 2009)
- Pornografía infantil (89 COIP No Delito Informático)
- Cyberbullying, Grooming, Sexting (No tipificados)
- Amenazas – revelación de secretos (179 y 180 No Delito Informático)
- Delitos cometidos contra la imagen (26 de la LOC No delito informático)
- Robo de Información – Phishing (190 tipificado en COIP – ambiguo)

Tabla 1. Actividades Tipificadas en el COIP.

Distribución de material pornográfico a menores de edad	1 a 3 años	ART. 168 COIP
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	1 a 3 años	ART. 173 COIP
Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	7 a 10 años	ART. 174 COIP
Violación intimidad Revelación ilegal de bases de datos	1 a 3 años Privada de 1 a 3 años, Pública de 3 a 5 años	ART.178 COIP
Apropiación fraudulenta por medios electrónicos	1 a 3 años	ART. 190 COIP

Fuente: Elaboración propia.

El progreso tecnológico que ha experimentado la sociedad, supone una evolución en la forma de infringir la ley, dando lugar, tanto a las diversificaciones de los delitos tradicionales como la aparición de nuevos actos ilícitos. Esta situación ha motivado un debate en torno a la necesidad de diferenciar o no los delitos informáticos del resto y de definir su tratamiento dentro del marco legal.

Para Elena Davara en su libro “Delitos Informáticos” manifiesta que:

El delito informático es cualquier actividad ilícita 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” (Marcos, 2017, p. 32).

Alberto Nava Garcés en su libro “El derecho en la era digital” y con contribución de Julio Téllez Valdés conceptualizan al delito informático en forma típica y atípica, entendiendo que en la forma típica son “las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin” y la forma atípica “actitudes ilícitas en que se tienen a las computadoras como instrumento o fin” (Garcés, 2018, p. 60).

El Convenio de Ciber-delincuencia del Consejo de Europa también conocido como el Convenio de Budapest, define a los delitos informáticos como “los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas redes y datos” (Europa, 2006, p. 12).



Conviene destacar entonces, que diferentes autores y organismos han manifestado diferentes apreciaciones para señalar las conductas ilícitas en las que se utiliza la computadora, esto es delitos informáticos, delitos electrónicos, delitos relacionados con la computadora, crímenes por computadora, delincuencia relacionada con el computador. Tal como podemos notar en las definiciones establecidas por autores anteriores, no existe una definición de carácter universal propia de delito informático, sin embargo, debemos resaltar que han sido los esfuerzos de especialistas que se han ocupado del tema y han expuesto conceptos prácticos y modernos atendiendo entornos nacionales concretos, pudiendo encasillar parte de los temas en esta área de la criminalística. Es preciso señalar que la última definición brindada por el convenio de cyberdelincuencia del Consejo de Europa anota especial cuidado en los pilares de la seguridad de la información: la confidencialidad, integridad y disponibilidad (Europa, 2006).

### **Motivos esenciales del especialista en TICs en administración de justicia (Guayaquil).**

La necesidad de la administración de justicia requiere de una formación exigente y detallada no solo en la materia en la que se requiere de su conocimiento sino también de procedimientos legales, legislación nacional e internacional, fundamentos de criminalística y psicología que le permitan un conocimiento más profundo de los casos analizados, ya que como profesional del derecho especialista es un garante de la verdad en un proceso. Por lo expuesto, es clave que el especialista en derecho informático acredite experiencia, conocimientos teóricos y prácticos, habilidades en la aplicación de procedimientos y metodologías, y que sus informes sean metódicos y estructurales, entre otros. El perfil del especialista en derecho informático debe cumplir con algunas de las funciones que se destacan a continuación:

- 1) Identificación y recolección de evidencias en medios magnéticos.
- 2) Comprensión y práctica en procedimientos de revisión y análisis forenses.
- 3) Comprensión y práctica de los estándares de ética que rigen las ciencias forenses en informática.
- 4) Comprensión de los aspectos legales y de privacidad asociados con la adquisición y revisión de medios magnéticos.
- 5) Comprensión y práctica de mantenimiento de la cadena de custodia de la evidencia cuando se realiza una investigación informática.
- 6) Comprensión de los diferentes sistemas de archivos asociados con sistemas operativos, acceso a archivos temporales, de cache, de correo electrónico, de Web, etc.
- 7) Conducir de manera detallada, recuperación de datos de todas las porciones de un disco.
- 8) Comprensión de aspectos de Internet.
- 9) Comprensión de técnicas de rompimiento de contraseñas y claves de seguridad.
- 10) Comprensión general de los temas relacionados con investigaciones forenses.

Las investigaciones forenses aplicables a la informática, tecnología y comunicaciones, requieren de profesionales con altos conocimientos en tecnologías de la información, que se ajusten a la aplicación de procedimientos científicamente probados válidos y reconocidos sobre las evidencias que vulneran o comprometen sistemas de tipo informático, para ellos existen certificaciones u avales profesionales, que pueden ser obtenidos por los profesionales en las ramas de informática (Gómez, 2011).

¿Quién se beneficia? Los elementos de prueba dentro de un proceso son de vital importancia, ya que mediante su investigación se llega a determinar la confirmación o desvirtuación de lo que corresponde a la verdad, es trascendental, tener en consideración la formalidad y claridad de los procedimientos o técnicas de análisis utilizados en un proceso de investigación, para brindar mayor claridad y precisión a las observaciones dentro del proceso, ante un hecho de delito informático. El principal beneficiado es la administración de justicia en la sociedad ya que se asegura que la administración de justicia en este tipo de delitos establezca justicia de acuerdo al marco legal del país.

## **CONCLUSIONES**

Es imprescindible que la Administración de Justicia a nivel de Estado junto con las Instituciones de Educación Superior genere y propulse proyectos orientados a promover una educación que combine la educación técnico informático tecnológico y la especializada de carácter jurídico, la investigación para el desarrollo de nuevas tecnologías, y la participación en actividades de la administración de Justicia. También, la educación de las instituciones, debe basarse en las conclusiones y aportes de la tecnología y en la relación más estrecha del estudio con la vida, el trabajo y la producción de la Administración de Justicia. Además, revalorar económica y socialmente al integrante de la Administración de Justicia.

Las Instituciones de Educación Superior deben generar y propulsar propuestas de reforma al Código Orgánico de la niñez y adolescencia incluyendo normativa delimitando el uso de las redes sociales o plataformas virtuales, establecer concordancias con nueva Ley Orgánica de delitos informáticos. Por otro lado, en cuanto a propuesta de reforma a la Ley Orgánica de Comunicación, que incluya normativa delimitando el uso de las redes sociales o plataformas virtuales, así como establecer concordancias con nueva Ley Orgánica de delitos informáticos.

En tal sentido, Ecuador necesita reformar la Ley Orgánica de Telecomunicaciones incluyendo el procedimiento administrativo para la recopilación de la prueba en los procesos de delitos tecnológicos, asimismo, generar obligatoriedad en las empresas portadoras y proveedores de Internet-ISP para la obligatoriedad y entrega de registros tecnológicos y establecer concordancias con Ley Orgánica de delitos informáticos.

En cuanto a la propuesta de una Ley Orgánica de delitos informáticos, el país necesita con urgencia una ley con carácter orgánico cuyo objeto sea la protección integral de los derechos de las instituciones públicas o privadas; así como del ciudadano en general, de todas las actividades ilícitas que utilicen tecnologías de información y que vulneren los derechos amparados en la constitución, también la prevención y sanción de los delitos cometidos mediante el uso de tecnologías de información, promoviendo la siguiente estructura.

Por último, en relación con la propuesta de reforma al Código Orgánico Integral Penal – COIP. Al realizar la propuesta de una ley de delitos informáticos, es imprescindible reformular algunas partes del COIP, promoviendo la inclusión y cambios y estableciendo concordancias con la Ley Orgánica de delitos informáticos.

## REFERENCIAS BIBLIOGRÁFICAS

- ARCOTEL, A. d. (2019). *Estadísticas Mensuales*. Quito-Ecuador: ARCOTEL.
- Cabello, G. (2015). *La revolución digital y los delitos informáticos*.
- Communications, H. L. (2016). *Marketing en redes sociales*. Anaya Multimedia, 2017.
- Estado, U. d. (2018). *Plan Operativo Unidad de Delitos Informático*. Quito: Fiscalía General del Estado.
- Europa, C. d. (2006). *Convenio de Budapest sobre ciberdelincuencia*. Budapest-Hungría: Consejo de Europa.
- Fiscalía, U. d. (2016). *Manual de Comercio Electrónico*. Quito-Ecuador: Fiscalía General del Estado.
- Garcés, A. N. (2018). *El derecho en la era digital*. Mérida-México: Editorial Porrúa México.
- Gómez, M. C. (2011). *Propuesta de Creación de un Instituto Tecnológico Superior en base a la Administración de Justicia de la ciudad de Guayaquil*. Guayaquil-Ecuador: Universidad de Guayaquil.
- Judicial, F. (2010). *Código Orgánico de la Función Judicial*. Quito.
- Kerlinger. (2017). Investigación del comportamiento. En Kerlinger, *Investigación del comportamiento*. Ed. Interamericana.
- López, M. (2017). *Análisis Forense Digital*.
- Marcos, E. D. (2017). *Delitos Informáticos*. Pamplona-España: Editorial Aranzadi.

- Moreno, M. (2014). *EL GRAN LIBRO DEL COMMUNITY MANAGER: TECNICAS Y HERRAMIENTAS PARA SACARLE PARTIDO A LAS REDES SOCIALES Y TRIUNFAR EN SOCIAL MEDIA*. Editorial: EDICIONES GESTION 2000.
- Nacional, A. (2008). *Constitución de la República del Ecuador*. Quito - Ecuador: CEP.
- Nacional, A. (2010). *Código Orgánico de la niñez y adolescencia*.
- Nacional, A. (2014). *Código Orgánico Integral Penal*. Quito-Ecuador: Registro Oficial.
- Nacional, A. (2015). *Ley Orgánica de Comunicación*. Quito: Registro Oficial.
- Nacional, A. (2015). *Ley Orgánica de Educación Intercultural*. Quito: CEP.
- Ramírez, G. (2016). *Informática Forense*. Guatemala: Ed.LIMUSA.
- Ramírez, S. G. (2017). *La libertad de expresión en la jurisprudencia de la Corte Interamericana de Derechos Humanos*. México.
- Sampieri, R. (2014). Metodología de la investigación. En R. Sampieri, *Metodología de la investigación*. MC Graw.
- Tejedor, F. (2015). Perspectivas de la comunicación. En F. Tejedor, *Perspectivas de la comunicación*. Madrid-España: Editorial Narces.
- Unidas, A. G. (1948). *Declaración Universal de Derechos Humanos*. ONU.
- Unidas, O. d. (2009). *Tipificación de delitos informáticos*. Informática Jurídica.
- UNO, O. (s.f.). Diccionario enciclopédico Ilustrado Océano Uno. En O. UNO, *Diccionario enciclopédico Ilustrado Océano Uno*. Barcelona-España: Editorial Océano.