UNIVERSIDAD DE CUENCA

FACULTAD DE JURISPRUDENCIA, CIENCIAS POLÍTICAS Y SOCIALES

ESCUELA DE DERECHO

"DELITOS CONTRA LA SEGURIDAD DE LOS ACTIVOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN: DELITOS A TRAVÉS DE LAS REDES SOCIALES"

MONOGRAFÍA PREVIA A LA OBTENCIÓN DEL TÍTULO DE ABOGADA DE LOS TRIBUNALES DE JUSTICIA DE LA REPUBLICA Y LICENCIADA EN CIENCIAS POLÍTICAS Y SOCIALES

AUTORA:

CARMEN ALEXANDRA ZUMBA CHUNCHI

DIRECTOR:

DR. MIGUEL ENRIQUE CORREA ALVARADO

CUENCA – ECUADOR

2015

RESUMEN

El presente trabajo básicamente está orientado a generar en la sociedad mayor conocimiento, precaución y concientización en la utilización y manejo de las múltiples herramientas informáticas y servicios que brinda Internet, siendo uno de estos servicios las muy conocidas redes sociales On-line, mismas que en la actualidad han resultado en unos casos una verdadera herramienta de ayuda para el desempeño de diversas actividades propuestas por cada uno de los usuarios de este tipo de redes sociales; y en otros casos las mismas han sido transformadas en la herramienta idónea para generar algún daño a determinada persona, grupo de personas, o hasta toda una colectividad.

Es por ello que para una mejor comprensión, he considerado oportuno desarrollar temas generales, tales como: antecedentes históricos de las Redes Sociales On-line, concepto, características, ventajas, desventajas, y la clasificación de estas.

Ya en un segundo capítulo, el tema adquiere un análisis desde el punto de vista jurídico, a partir del cual se dará respuesta a interrogantes como: ¿Qué es delito informático?, ¿Quiénes lo cometen?, ¿Quiénes resultan víctimas de estos delitos?; sin dejar de lado los delitos tipificados por el Código Orgánico Integral Penal.

El tema llega a su desenlace con el tratamiento de la prueba pericial dentro de nuestra legislación ecuatoriana, su importancia, los medios de prueba permitidos por la ley penal, y los momentos en los cuales esta se va desarrollando con observancia de los principios que le rigen.

También se hace alusión a los peritos informáticos, los requisitos que estos deben cumplir para ser calificados como tales, y las formalidades que deben cumplirse para que el perito designado pueda intervenir en un proceso penal como un verdadero auxiliar en la administración de justicia.

Palabras claves: redes sociales Online, delitos informáticos, delitos contra la seguridad de los activos

SUMMARY

This paper is primarily aimed at generating in society greater awareness, caution and awareness on the use and management of multiple software tools and services offered by the Internet, one of these services very popular social networks on-line, same as in today some cases have resulted in a real tool to help carry out various activities proposed by each of the users of these social networks; and in other cases they have been transformed into the ideal tool to generate some damage to a specific person, group of persons, or even an entire community.

That is why I have seen fit to better understand, develop general topics such as: historical background of Social Networking On-line, concept, features, advantages, disadvantages, and calcification of these.

And in a second chapter, the issue takes on an analysis from the legal point of view, from which it will answer questions like: What is computer crime is committed by ?, Who ?, Who are victims of these crimes? ; without neglecting the crimes under the Criminal Code of Integral.

The theme comes to a climax with the treatment of expert evidence in our Ecuadorian law, its importance, the evidence allowed by the criminal law, and the moments in which this is being developed in compliance with the principles governing it.

Reference is also made to computer experts, the requirements they must meet to qualify as such, and the formalities to be completed for the designated expert can intervene in criminal proceedings as a real help in the administration of justice.

Keywords: Online social networking, computer crimes, crimes against the security of assets

ÍNDICE GENERAL

CLAUSULAS DE RESPONSABILIDAD

Universidad de Cuenca
Facultad de jurisprudencia
Escuela de Derecho

CLAUSULAS DE RESPONSABILIDAD

Yo, *Carmen Alexandra Zumba Chunchi*, autora de la monografía "**DELITOS CONTRA LA SEGURIDAD DE LOS ACTIVOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN: DELITOS A TRAVÉS DE LAS REDES SOCIALES**", reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de *Abogada de los Tribunales de Justicia de la República, y, Licenciada en Ciencias Políticas y Sociales*. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autora.

Cuenca, 8 de Mayo de 2015

Carmen Alexandra Zumba Chunchi
C. I.: 010539995-0

6

Carmen Alexandra Zumba Chunchi

Universidad de Cuenca
Facultad de jurisprudencia
Escuela de Derecho

Yo, *Carmen Alexandra Zumba Chunchi*, autora de la monografía "**DELITOS CONTRA LA SEGURIDAD DE LOS ACTIVOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN: DELITOS A TRAVÉS DE LAS REDES SOCIALES**", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autora.

Cuenca, 8 de Mayo de 2015

Carmen Alexandra Zumba Chunchi
C. I.: 010539995-0

7

Carmen Alexandra Zumba Chunchi

DEDICATORIA

Esta monografía la dedico a mis padres, quienes con su paciencia y apoyo continuo e infinito me mantuvieron firme en el recorrido de este camino lleno de obstáculos y múltiples experiencias propias de la universidad de la vida, hasta por fin llegar a la meta deseada, que algún día se miraba muy lejana.

A mis hermanos, quienes me han comprendido y tolerado mas allá de lo debido; impulsándome a seguir adelante, sin permitir que ceda ante situaciones adversas.

AGRADECIMIENTOS

Agradezco a Dios por darme vida y salud, por iluminarme en cada paso que he dado a lo largo de este trayecto, permitiéndome vivir esos momentos que en algún día tan solo eran una mera ilusión.

También me encuentro muy agradecida infinitamente, con cada uno de mis profesores que me mostraron y me supieron guiar por el sendero de esta noble carrera.

INTRODUCCIÓN

Para la humanidad la comunicación ha constituido desde su inicio un elemento esencial para su desarrollo; siendo utilizado primitivamente los gestos, sonidos hasta lograr desarrollar un lenguaje propio; para posteriormente inventar medios de comunicación que permitan que el mensaje enviado sea receptado en el menor tiempo posible; situación que históricamente nos demuestra que este ha sido desde siempre un tema de preocupación, la misma que inicia con señales de humo, hasta llegar a los canales masivos de comunicación, tales como: fax, teléfono, televisión, con los que se consideró que la humanidad ha dado grandes pasos; hasta que en los años 60 con el aparecimiento del **INTERNET,** se ha logrado una gran revolución en la comunicación; pues este a más de acortar la distancia y el tiempo entre emisor y receptor, implica también un ahorro económico para la sociedad, y por ende gran comodidad y eficacia en la elaboración, búsqueda, obtención, e intercambio de información entre varias personas de diversas partes del planeta, con lo que podemos decir con certeza, que a más de la conquista terrestre se ha logrado una conquista espacial.

Pues El Internet como medio de comunicación nos ha brindado muchos beneficios y servicios, como las conocidas **Redes Sociales,** que hoy en día constituyen el medio más usado para comunicarse, pero a más de aquello, representa una herramienta necesaria para el desarrollo de múltiples actividades, ya sean académicas, comerciales, económicas, etc., que incluso son capaces de organizar personas intercomunicadas.

Sin embargo así como su fácil utilización genera grandes beneficios, también ocasiona grandes perjuicios, los cuales son ocasionados por personas con alto conocimiento y capacidad en el área informático, perjuicios que en nuestra legislación y en las de los demás países, son considerados como delitos; de los cuales muchas personas que han resultados victimas de aquellos no los

consideran como tales, por falta de conocimiento o porque consideran que no existe cuerpo normativo que lo sancionen.

Por ende con este trabajo de investigación se dará a conocer los delitos informáticos que pueden cometerse, quienes lo hacen, las víctimas de estos delitos; y la pertinencia e introducción de la prueba al proceso en este tipo de delitos.

CAPITULO I

GENERALIDADES

1.1.- HISTORIA DE LAS REDES SOCIALES

Marcar el verdadero inicio de las redes sociales, es un tema demasiado complejo, esto obedece a que su origen no es claro, y su evolución acelerada. No existe consenso sobre cuál fue la primera red social, y podemos encontrar diferentes puntos de vista al respecto. Por otro lado, la existencia de muchas plataformas se cuenta en tiempos muy cortos, bien sabido es que hay servicios de los que hablamos hoy que quizá mañana no existan, y otros nuevos aparecerán dejando obsoleto, en poco tiempo, cualquier panorama que queramos mostrar de ellos. Su historia se escribe a cada minuto en cientos de lugares del mundo. Lo que parece estar claro es que los inicios se remontan mucho más allá de lo que podríamos pensar en un primer momento, puesto que los primeros intentos de comunicación a través de Internet ya establecen redes, y son la semilla que dará lugar a lo que más tarde serán los servicios de redes sociales On-Line que conocemos actualmente. Por todo ello, vamos a plantear su historia contextualizada mediante una cronología de los hechos más relevantes del fenómeno que suponen las redes sociales basadas en Internet.

1971. Se envía el primer e-mail entre dos ordenadores situados uno al lado del otro.
1978. Ward Christensen y Randy Suess crean el **BBS** (Bulletin Board Systems) para informar a sus amigos sobre reuniones, publicar noticias y compartir información.
1994. Se lanza **GeoCities**, un servicio que permite a los usuarios crear sus propios sitios web y alojarlos en determinados lugares según su contenido.

1995. La Web alcanza el millón de sitios web, y **The Globe** ofrece a los usuarios la posibilidad de personalizar sus experiencias on-line, mediante la publicación de su propio contenido y conectando con otros individuos de intereses similares. En este mismo año, Randy Conrads crea **Classmates**, una red social para contactar

con antiguos compañeros de estudios. Classmates es para muchos el primer servicio de red social, principalmente, porque se ve en ella el germen de Facebook y otras redes sociales que nacieron, posteriormente, como punto de encuentro para alumnos y ex-alumnos.

1997. Lanzamiento de **AOL Instant Messenger**, que ofrece a los usuarios el chat, al tiempo que comienza el **blogging** y se lanza **Google**. También se inaugura **Sixdegrees**, red social que permite la creación de perfiles personales y listado de amigos, algunos establecen con ella el inicio de las redes sociales por reflejar mejor sus funciones características. Sólo durará hasta el año 2000.

1998. Nace **FriendsReunited**, una red social británica similar a Classmates. Asimismo, se realiza el lanzamiento de **Blogger**.

2000. Estalla la **"Burbuja de Internet"**. En este año se llega a la cifra de setenta millones de ordenadores conectados a la Red.

2002. Se lanza el portal **Friendster**, que alcanza los tres millones de usuarios en sólo tres meses.

2003. Nacen **MySpace, LinkedIn** y **Facebook**, aunque la fecha de esta última no está clara puesto que llevaba gestándose varios años. Creada por el conocido Mark Zuckerberg, Facebook se concibe inicialmente como plataforma para conectar a los estudiantes de la Universidad de Harvard. A partir de este momento nacen muchas otras redes sociales como **Hi5** y **Netlog**, entre otras.
2004. Se lanzan **Digg**, como portal de noticias sociales; **Bebo**, con el acrónimo de "Blog Early, Blog Often"; y **Orkut**, gestionada por Google.

2005. **Youtube** comienza como servicio de alojamiento de vídeos, y **MySpace** se convierte en la red social más importante de Estados Unidos.

2006. Se inaugura la red social de microblogging **Twitter**. **Google** cuenta con 400 millones de búsquedas por día, y **Facebook** sigue recibiendo ofertas multimillonarias para comprar su empresa. En España se lanza **Tuenti**, una red

social enfocada al público más joven. Este mismo año, también comienza su actividad **Badoo**.

2008. **Facebook** se convierte en la red social más utilizada del mundo con más de 200 millones de usuarios, adelantando a **MySpace**. Nace **Tumblr** como red social de microblogging para competir con Twitter.

2009. **Facebook** alcanza los 400 millones de miembros, y **MySpace** retrocede hasta los 57 millones. El éxito de Facebook es imparable.

2010. Google lanza **Google Buzz**, su propia red social integrada con Gmail, en su primera semana sus usuarios publicaron nueve millones de entradas. También se inaugura otra nueva red social, **Pinterest**. Los usuarios de **Internet** en este año se estiman en 1,97 billones, casi el 30% de la población mundial. Las cifras son asombrosas: **Tumblr** cuenta con dos millones de publicaciones al día; **Facebook** crece hasta los 550 millones de usuarios: **Twitter** computa diariamente 65 millones de tweets, mensajes o publicaciones de texto breve; **LinkedIn** llega a los 90 millones de usuarios profesionales, y **Youtube** recibe dos billones de visitas diarias.

2011. **MySpace** y **Bebo** se rediseñan para competir con Facebook y Twitter. **LinkedIn** se convierte en la segunda red social más popular en Estados Unidos con 33,9 millones de visitas al mes. En este año se lanza Google, otra nueva apuesta de Google por las redes sociales. La recién creada **Pinterest** alcanza los diez millones de visitantes mensuales. Twitter multiplica sus cifras rápidamente y en sólo un año aumenta los tweets recibidos hasta los 33 billones.

2012. Actualmente, **Facebook** ha superado los 800 millones de usuarios, **Twitter** cuenta con 200 millones, y **Google** registra 62 millones. La red española **Tuenti** alcanzó en febrero de este año los 13 millones de usuario[1]

1.2.- CONCEPTO DE REDES SOCIALES.

[1]Isabel Ponce. "Historia de las redes sociales." Redes Sociales. 2012. <http://recursostic.educacion.es/observatorio/web/es/internet/web-20/1043-redessociales?start=2>(5 Dic 2014)

Definir a las redes sociales es un verdadero reto, es así que las mismas han venido siendo objeto de estudio desde hace décadas, y por parte de distintas disciplinas, lo que ha generado una variedad de teorías, al tratar de explicar su relevancia e influencia en la sociedad, constituyéndose como base para su desarrollo virtual. Con la llegada de la Web 2.0, las redes sociales en Internet ocupan un lugar relevante en el campo de las relaciones personales, tanto así que, el término red social es acuñada como una expresión del lenguaje común que asociamos a nombres como Facebook o Twitte, a pesar que su significado es amplio y complejo, pues no existe una única acepción.

- **Diccionario web 2.0**, define como "un *Portal web donde los usuarios, previamente registrados, pueden crear un perfil personal (que pueden hacer público o semipúblico) y además ponerse en contacto con amigos con los que pueden compartir todo tipo de contenidos digitales".*

  En este sentido se define red social online como un portal web, que es un espacio que ofrece acceso a una serie de recursos y servicios, éste puede incluir enlaces, buscadores, foros, etc. para facilitar el acceso a la información. Este diccionario aplica una nueva característica, ésta es la obligación de los usuarios de dichas redes a registrarse antes de comenzar con la comunicación, y se establecen los tipos de perfiles que pueden crearse (público o semipúblico) aunque sin profundizar en quiénes podrán visualizar la información en cada caso. Es importante destacar que se habla de contenidos digitales, especificando así el tipo de archivos que se encontrarán en estas redes.

- **Luis Fernández**, manifiesta 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".*

Con esta definición de indica que las redes sociales on-line tan solo pueden funcionar en los espacios virtuales, por lo que es evidente que únicamente se puede acceder a éstas a través de la red, por lo tanto la información debe ofrecerse en formatos de lectura en línea. Es importante fijarse en que se utiliza la expresión “espacios virtuales” en plural, lo que quiere decir, obviamente, que se trata de más de uno, y que para ello es necesaria la aportación de varios individuos ya que uno solo no sería capaz de crear todos los espacios virtuales existentes y, en el caso de que estos pudiera darse, no se cumplirían los objetivos establecidos por el mencionado autor, que son: organizar comunidades, realizar proyectos y fomentar el mercado, que necesitan de un intercambio social. Según el autor estos objetivos no se llevarían a cabo si no fuera a través de estos espacios virtuales *que de otra manera no existirían* es decir, que no se llevarían a cabo de igual forma si no se dieran a través de la red.

- **José Antonio del Moral**: “*Las redes sociales en Internet son sistemas que permiten establecer relaciones con otros usuarios, a los que se puede conocer o no en la realidad*”*.*

  En esta definición se establece como objetivo de las redes sociales on-line, la relación entre individuos, sin hablar de ningún otro. Además es el primer autor que utiliza el término “realidad” para referirse al mundo no digital; en igual categoría, al manifestar que las relaciones pueden darse tanto entre individuos que se conocen, o no, incluyendo de esta manera una característica principal de las redes sociales on-line, que rompe la barrera de la comunicación física.

Como podremos darnos cuenta, más se ha tratado de definir el medio en el que se encuentra la red social, alejando su atención de los elementos de la comunicación[2].

1.3.- CARACTERÍSTICAS DE LAS REDES SOCIALES:

Una vez que se han analizado algunas definiciones de redes sociales, podremos desprender de las mismas las siguientes características básicas:

1. Están basadas en el usuario: Las redes sociales son construidas y dirigidas por los mismos usuarios, quienes además las nutren con el contenido.

2. Son Interactivas: Las redes sociales poseen además de un conjunto de salas de chat y foros, una serie de aplicaciones basadas en una red de juegos, como una forma de conectarse y divertirse con los amigos.

3. Establecen relaciones: Las redes sociales no sólo permiten descubrir nuevos amigos sobre la base de intereses, sino que también permiten volver a conectar con viejos amigos con los que se ha perdido contacto desde muchos años atrás.

4. Intercambio de información e intereses: Las redes sociales permiten que el contenido publicado por un usuario se difunda a través de una red de contactos y sub-contactos mucho más grande de lo que se pueda imaginar.

5. Ofrece una variedad de servicios: Intercambio de información, fotografías, servicios de telefonía, juegos, chat, foros.[3]

6. Permiten que el contacto entre usuarios sea ilimitado, en la medida en la que el concepto espacio y tiempo se convierte en relativo al poder comunicarse desde y hacia cualquier lugar, así como en cualquier

[2]"Los delitos en las redes sociales: aproximación a su estudio y clasificación". (2012). Salamanca: De Cea Jiménez Andrea. (Las Redes Sociales en Línea, 2012, , p. 16)

[3]Elvis J BelialDiazMarquis" Redes Sociales."*Características de las redes sociales*. <http://www.monografias.com/trabajos84/redessociales/redes-sociales.shtml#caracteria> (5 Dic 2014)

momento, con la única condición de que ambas partes acepten relacionarse entre sí.[4]

7. Son sistemas abiertos siempre a nuevos miembros.

8. Son populares.[5]

1.4.- VENTAJAS Y DESVENTAJAS DE LAS REDES SOCIALES

Como bien se ha señalado, a partir del aparecimiento del Internet, la sociedad ha venido experimentando grandes logros, principalmente en el campo de la comunicación; es así que Internet y su evolución, se ha convertido en un medio y canal masivo de comunicación, con características propias; en razón de que el ser humano no requiere estar en un mismo espacio y tiempo para comunicarse; peor aun esperar un tiempo corto o prolongado para receptar el mensaje y emitir el mismo; pues un claro ejemplo de aquella comunicación rápida lo logramos atreves de las Redes Sociales On-line con ayuda de las distintas herramientas y servicios que proporciona Internet.

Sin embargo el mismo desarrollo de Internet así como ha generado grandes beneficios para la sociedad, este también ha implicado grandes perjuicios para la humanidad, constituyéndose en una herramienta de ataque en las mentes y manos de aquellas personas que buscan causar daño a algún usuario, ya sea por diversión o beneficio propio, remunerado o gratuito; realidad que genera inseguridad a la población en general tanto en su vida cotidiana, como también en el campo jurídico y administración de justicia, cuyo desarrollo se ve retrasado a la evolución rápida de la tecnología informática.

Es por ello que en este punto, enunciaré algunas ventajas y desventajas de las Redes Sociales On-line, mismas que derivan de sus propias características.

Ventajas:

[4]Master's Degree Online "Cursos de Redes Sociales para padres."*Características Generales de las redes sociales*. <http://www.adrformacion.com/cursos/redsocp/leccion1/tutorial3.html>(8 Dic 2014)
[5]D. Boyd **y** B. Ellison**.** "Redes Sociales en internet." Características Generales.<http://www.edukanda.es/mediatecaweb/data/zip/971/page_05.htm> (8 Dic 2014)

1) **Mantenerte conectado:** Las redes sociales son una excelente forma de mantenerse conectado con viejos amigos, amigos que no viven cerca de donde vive determinada persona, y hasta con los mismos amigos de un salón de clases.

2) **Comunicación**: actualmente constituye una nueva forma de comunicación, que incluso resulta un ahorro económico.

3) **Actualizado:** Algunos sitios de redes sociales están constantemente ofreciendo noticias relevantes y de última hora, depende de las personas y cuentas a las que el usuario sigue.

4) **Conexión personal:** Teniendo un perfil de redes sociales, permite mantenerse informado y comunicación con sucesos recientes que les han pasado a la gente de la red.

5) **Amigos con mismos intereses**: Varios sitios de redes sociales están centrados en conectar a las personas mediante sus similitudes en gustos y temas de interés. Por ejemplo, Flickr es una red social que permite a los usuarios subir y compartir fotografías. Crear un perfil en este tipo de plataformas es una buena forma de crear nuevas conexiones.

6) **Redes:** En el mundo actual, no se trata sobre lo que se sabe, sino, a quién se conoce. Tener un perfil en redes sociales permite hacer y mantener conexiones de negocios.

7) **Publicidad gratuita:** Las redes sociales permiten a los usuarios a postear cualquier cosa en el mundo virtual y puede ser visto por cualquiera. Tener un perfil, ofrece tener cierta exposición y más oportunidades de hacer marketing a tu trabajo y a ti mismo.

8) **Expresión creativa**: El internet ofrece una plataforma libre y virtual para que absolutamente todos los usuarios expresen sus ideas, opinión sobre una noticia.

9) **Experiencia global:** El Internet ha disminuido de manera masiva el tamaño del mundo. Esto ha hecho que el flujo de ideas e información sea un proceso más fácil.

10) **Un impacto positivo:** Las redes sociales permiten a los usuarios unirse y crear alianzas muy fuertes para luchar por cierta causa.[6]

Desventajas:

1) **Pérdida de la privacidad**: Cada dato, información, foto, vídeo o archivo subido a una red social pasa a ser parte de los archivos de los administradores. A su vez un mal uso de las redes conlleva a la facilidad de encontrar datos propios, de familiares o amigos. Debemos incluir en esto los hackers y el phishing que roban contraseñas para manipular información o espiar a las personas.

2) **Acceso a contenidos inadecuados**: La falta de control en la red y la cantidad de información de todo tipo lleva a que mucha gente use Internet para acceder y publicar contenidos de todo tipo: violentos, sexuales, relacionado al consumo de estupefacientes, fanatismo, incitación al odio etc. Esto puede devenir de enlaces publicados o compartidos por otros usuarios o links, avisos, etc.

3) Acoso por parte de compañeros, conocidos o desconocidos: Aquí existen dos casos fundamentales.

- Cyberbullying: Acoso llevado por compañeros o desconocidos a través de las redes con amenazas, insultos, etc.
- Cybergrooming: efectuado por los adultos para contactarse con menores de edad para obtener fotos e información de ellos para utilizar en su beneficio.

[6]Andrés Abad**.** "10 Características de lo Bueno y lo Malo." 10 Características. Positivas. 2013 <http://fgjhghgh.blogspot.com/>(8 Dic 2014)

4) **Posible incumplimiento de la ley**: Muchas veces inconscientemente los usuarios llevan acciones ilegales. Los cuatro incumplimientos más conocidos son:

   - Publicar datos, fotos, vídeos de otras personas violando su privacidad sin el consentimiento previo de ellas.
   - Hacerse pasar por otra persona creando un falso perfil utilizando información obtenida por distintos medios.
   - Incumplimiento de las normas de copyright, derecho de autor, y descargas ilegales a través de la obtención o intercambio de contenidos protegidos creando páginas para descargarlos.
   - Acoso a compañeros, conocidos,o incluso desconocidos, ciberbullying a través de correos electrónicos, comentarios, mensajes, etc.[7]

5) Pueden ser adictivas y devorar gran cantidad de nuestro tiempo, pues son ideales para el ocio.[8]

1.5.- CLASES DE REDES SOCIALES:

Como inicialmente se dejó indicado, no es posible establecer con total exactitud el verdadero inicio de las redes sociales; sin embargo, se puede decir que la digitalización de éstas es muy reciente y en poco tiempo se han convertido en el fenómeno mediático de mayor envergadura; es así que las redes sociales on-line se caracterizan por propiciar la interacción de miles de personas en tiempo real, con base en un sistema global de relaciones entre individuos, inclusive generando consecuencias jurídicas entre los distintos usuarios. Por lo tanto podemos afirmar que las redes sociales no son otra cosa que un medio para crear situaciones, relaciones, conflictos y efectos jurídicos.

[7]Wikipedia-La Enciclopedia Libre" Servicio de Red Social."*Riesgo en el uso de las redes sociales*. <http://es.wikipedia.org/wiki/Servicio_de_red_social#Riesgos_en_el_uso_de_las_redes_sociales> (10 Dic 2014)

[8]Bligoo. “Redes Sociales”. Ventajas y Desventajas de las Redes Sociales <http://redessociales.bligoo.com.mx/content/view/1534653/Ventajas-y-Desventajas-de-las-redes-sociales.html#.VLbvRNKUf5k> (10 Dic 2014).

Redes sociales On-Line: son aquellas que tienen su origen y se desarrollan a través de medios electrónicos; las cuales se clasifican en atención a al objeto, sujeto y ubicación geográfica

1 Por su público objetivo y temático:

a) Redes sociales Horizontales: Son aquellas dirigidas a todo tipo de usuario y sin una temática definida. Se basan en una estructura de celdillas permitiendo la entrada y participación libre y genérica sin un fin definido, distinto del de generar masa. Los ejemplos más representativos del sector son Facebook, Orkut, Identi.ca, Twitter.

b) Redes sociales Verticales: Están concebidas sobre la base de un eje temático agregado. Su objetivo es el de congregar en torno a una temática definida a un colectivo concreto. En función de su especialización, pueden clasificarse a su vez en:

c) *Redes sociales Verticales Profesionales:* Están dirigidas a generar relaciones profesionales entre los usuarios. Los ejemplos más representativos son Viadeo,Xing y Linked In.

d) *Redes sociales Verticales De Ocio:* Su objetivo es congregar a colectivos que desarrollan actividades de ocio, deporte, usuarios de video-juegos, fans, etc. Los ejemplos más representativos son Wipley, Minube, Dogster,Last.FM y Moterus.

e) *Redes sociales Verticales Mixtas:* Ofrecen a usuarios y empresas un entorno específico para desarrollar actividades tanto profesionales como personales en torno a sus perfiles: Yuglo, Unience.

2.- Por el sujeto principal de la relación:

a) Redes sociales Humanas: Son aquellas que centran su atención en fomentar las relaciones entre personas uniendo individuos según su perfil social y en función de sus gustos, aficiones, lugares de trabajo, viajes y

actividades. Ejemplos de este tipo de redes los encontramos en ,Dopplr, y Tuenti

b) Redes sociales de Contenidos: Las relaciones se desarrolla uniendo perfiles a través de contenido publicado, los objetos que posee el usuario o los archivos que se encuentran en su ordenador. Los ejemplos más significativos son Scribd, Flickr, Bebo,r, Dipity, StumbleUpon y FileRide.

c) Redes sociales de Objetos: Conforman un sector novedoso entre las redes sociales. Su objeto es unir marcas, automóviles y lugares. Entre estas redes sociales destacan las de difuntos, siendo éstos los sujetos principales de la red. El ejemplo más llamativo es Respectance.

3.- Por su localización geográfica

a) Redes sociales Sedentarias: Este tipo de red social muta en función de las relaciones entre personas, los contenidos compartidos o los eventos creados. Ejemplos de este tipo de redes son: Blogger, Plaxo,Bitacoras.com, Plurk

b) Redes sociales Nómadas: A las características propias de las redes sociales sedentarias se le suma un nuevo factor de mutación o desarrollo basado en la localización geográfica del sujeto. Este tipo de redes se componen y recomponen a tenor de los sujetos que se hallen geográficamente cerca del lugar en el que se encuentra el usuario, los lugares que haya visitado o aquellos a los que tenga previsto acudir. Los ejemplos más destacados son: Foursquare, Latitude, Fire Eagle y Skout.[9]

[9]Pablo Fernández Burgueño. “Blog de Derecho.” Clasificación de Redes Sociales. 2009 <http://www.pabloburgueno.com/2009/03/clasificacion-de-redes-sociales/> (12 Dic 2014)

CAPITULO II

EL DELITO INFORMÁTICO

2.1.- CONCEPTO DE DELITO

Previo al análisis de delito informático, es menester recordad**,** que es delito, en términos generales; para ello citaremos algunas de ellas, y por ende desde el punto de vista de nuestra legislación ecuatoriana.

Francisco Carrara, *define al delito como ¨la infracción de la ley del Estado, promulgado para proteger la seguridad de los ciudadanos, y que resulta de un acto externo del hombre, positivo negativo, moralmente imputable y socialmente dañoso. ¨*

Con esta definición Carrara trata de unificar y superar los elementos de las definiciones formales y reales; constituyéndose en el propulsor de una nueva tendencia orientada a delimitar los elementos esenciales de la estructura jurídica del delito. Es por ello que en su definición destaca los siguientes elementos.

a) Infracción de la ley del Estado.- Este elemento es considerado tanto en la teoría clásica como en la formal; pues para que una conducta sea considerada como delito, debe estar previamente tipificada en la ley como tal.

b) Promulgada para proteger la seguridad de los ciudadanos.- En este punto se establece el carácter material del delito, con el que Carrara nos da a entender, que su razón de ser, es proteger ciertos bienes o intereses que la sociedad considere valiosos; imponiéndoselo para ello la presunción jurídica ¨la ley se presume conocida por todos quienes impera, su ignorancia no excluye a persona alguna.¨

c) Que resulta de un acto.- Para Carrara es uno de los elementos estructurales del delito; la infracción de la ley proviene del acto, en el cual debe confluir las fuerzas física y moral, apreciadas subjetiva y objetivamente.

d) Del hombre.- el delito puede ser cometido tan solo por el ser humano y no por los animales y cosas; por lo tanto será sancionado en caso de infringir la ley, en razón de que este es quien esta dotado de razón y por ende capaz de direccionar sus actos a determinado fin.

e) Externo.- la ley no sanciona lo que pertenece al fuero interno de la persona; la ley penal tan solo interviene cuando la persona comete u omite una conducta prohibida.

f) Positivo o negativo.- Es decir que el delito puede provenir sea de una acción u omisión.

g) Moralmente imputable.- La imputabilidad moral se basa en el libre albedrio; mientras que la imputabilidad es elemento central del delito, sin ella no se puede sancionar al sujeto pasivo.

h) Socialmente dañoso.- Se recalca que la ley penal está orientada a proteger los bienes intereses de una sociedad determinada, según una escala de valores; es decir, que una vez más se destaca el aspecto material del delito.[10]

Ernesto Albán Gómez, en su obra Manual de Derecho Penal Ecuatoriano, define al delito considerando cuatro presupuestos, sin los cuales al acto no podrá ser punible, por lo tanto para este autor ¨ delito es el acto típico, antijurídico y culpable. Si se dan estos presupuestos el acto será punible.¨

a} El delito es acto.- El sustento material del delito, es la conducta humana; porque es la expresión de voluntad del ser humano, que causa daño o peligro a un bien jurídico protegido por el Estado.

b} Es acto típico.- Esa conducta debe estar previa y expresamente descrita por la ley penal. Pues a mas de ser un elemento del delito, este constituye un principio del debido proceso conocido como ¨principio de legalidad¨, reconocido y garantizado por nuestra Constitución en el artículo 76, numeral 3, que establece ¨*nadie podrá ser juzgado ni sancionado por un acto u omisión que, al momento de*

[10]"Manual de Derecho Penal Ecuatoriano". (2012). Quito: Albán Gómez. Ernesto (, p. 16)

cometerse, no este tipificado en la ley como infracción penal, administrativa o de otra naturaleza; ni se le aplicará una sanción no prevista por la Constitución o la ley.¨

c} El acto antijurídico.- Esa conducta debe ser contraria al Derecho, lesiona un bien jurídico penalmente protegido.

d} Acto culpable.- Este es un elemento subjetivo, pues el autor del delito tan solo podrá ser imputado y sancionado siempre y cuando exista una relación de causalidad y efecto entre el acto y el resultado.

Por su parte el **Código Orgánico Integral Penal,** define a la infracción penal como "conducta típica, antijurídica y culpable cuya sanción se encuentra prevista en el cuerpo legal antes citado.". Y a la vez divide a las infracciones en delitos y contravenciones, los que son definidos en el artículo 19 del mismo cuerpo legal de la siguiente manera:

- 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.

2.2.-CONCEPTO DE DELITO INFORMÁTICO.

De acuerdo a la información adquirida de WIKIPEDIA, la palabra informática proviene del alemán "informatik" que fue acuñada por primera vez en el año de 1957, por el Científico informático Karl Steinbuch, para referirse a la aplicación de las computadoras para almacenar y procesar la información; esto porque la informática en sus inicios tan solo permitía tareas básicas, repetitivas y monótonas del área administrativa. Pronto este vocablo fue adaptado a diversas lenguas, y aun más con el desarrollo de la tecnología, el significado de la informática se amplió aun mas; puesto que la misma hace referencia a los fundamentos de las ciencias de la computación, la programación y metodologías para el desarrollo de software, la arquitectura de computadores, las redes de

computadores, la inteligencia artificial y ciertas cuestiones relacionadas con la electrónica.[11]

Sin embargo, pese haber adquirido conocimientos acerca del concepto de delito y la palabra informática, resulta bastante complejo definir al delito informático. Varios autores emplean términos muy generales que no ayudan a especificar lo que es delito informático; y aun más, como sinónimo de delito informático, se ha hecho uso de las expresiones delito electrónico, delito digital, delito telemático, cyber-crimen; cuando en realidad estos términos no son sinónimos; pues cada uno de ellos cuenta con su propio campo de aplicación, tal como lo señala Andrea De Cea Jiménez en su tesis titulada "Los delitos en las redes sociales: aproximación a su estudio y clasificación", en donde justifica el porqué se debe hacer uso de la terminología ***delito informático***, manifestando lo siguiente:

a.-La electrónica estudia y emplea sistemas cuyo funcionamiento se basa en la conducción y el control del flujo de los electrones u otras partículas cargadas eléctricamente[12], es decir, sólo abarca dispositivos electrónicos para los que no es estrictamente necesaria una comunicación, como por ejemplo: televisión, radio, CD, etc. Mientras que la informática, aunque en un principio no requiere de una conexión a Internet, posteriormente este si va ha ser necesario para la comisión del delito.

b.-Lo digital se refiere a aquellas máquinas que utilicen el sistema binario[13], dejando fuera a aquellas que no lo usan como, por ejemplo, la radio o el teléfono, Además debemos considerar, que hoy en día casi todos los aparatos son digitales, por ejemplo un lector de CDs o un reloj o una calculadora, y constituyen un mundo demasiado limitado. En tanto que la informática incluye tanto lo digital como todo lo referente a programación, almacenamiento y producción de información,, así como también todo lo relativo a tecnología computacional.

[11]Wikipedia. "Imformática." *Etimología*.<http://es.wikipedia.org/wiki/Inform%C3%A1tica >(28 Dic 2014)

[12]Wikipedia. "Electrónica.".<http://es.wikipedia.org/wiki/Electr%C3%B3nica>(5 Enero 2015)

[13] Es un sistema en el que los números se representan utilizando solamente las cifras cero (apagado) y uno (*encendido*). Su uso se debe a que los aparatos digitales trabajan internamente con dos niveles de voltaje.

c.-La telemática es asociada a todo lo relacionado con las técnicas y servicios relacionados con las telecomunicaciones, por lo tanto, ésta incluye todo tipo de medios de comunicación, tales como prensa, cine, revistas. Mientras que la informática se limita a los que requieren de dispositivos informáticos.

d.-El cyber-crimen sólo se refiere a acciones desarrolladas en el espacio virtual, mientras que la informática se refiere también a los dispositivos de entrada (teclado, micrófono), dispositivos de salida (monitor, impresora, audífonos), dispositivos de almacenamiento (CD, Memorias flash).

Es por ello que la autora entes citada considera que delito informático es "***Aquellas acciones tomadas como delito (con sus correspondientes características) que pueden ser llevadas a cabo a través o en contra de un dispositivo informático, sistema operativo o programa informático***"

2.3.- CARACTERÍSTICAS DEL DELITO INFORMATICO

Julio Téllez Valdés en su obra "Derecho Informático" considera las siguientes características:

1.- Son conductas criminales de cuello blanco, en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden cometerlas.

2.- Son acciones ocupacionales en cuanto que muchas veces se realizan cuando el sujeto está trabajando.

3.- Son acciones de oportunidad porque se aprovecha una ocasión creada o altamente intensificada en el campo de las funciones y organizaciones del sistema tecnológico y económico.

4.- Provocan serias pérdidas económicas, ya que casi siempre producen beneficios económicos a aquellos que los realizan.

5.- Ofrecen facilidades de tiempo y espacio, ya que pueden cometerse en milésimas de segundo y sin una necesaria presencia físicamente; esto obedece a que el servicio de la red puede llegar a cualquier parte del mundo; y además, no es estrictamente necesario que la víctima este utilizando el ordenador en el mismo momento en el que se esté cometiendo el delito. Andrea de Cea Jiménez, nos da un claro ejemplo de esta característica: él envió de virus a cuentas de correo electrónico.

6.- Son muchos los casos y pocas las denuncias, debido a la falta de regulación jurídica a nivel internacional.

7.- Son muy sofisticados y relativamente frecuentes en el ámbito militar.

8.- Presentan grandes dificultades para su comprobación, por su carácter técnico, es decir que se puedes realizar varias tareas en el mismo dispositivo de acceso, al mismo tiempo.

9..- Ofrecen a los menores de edad facilidades para su comisión.

10.- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación jurídica en el ámbito internacional[14].

2.4.- SUJETOS QUE INTERVIENEN.

En materia penal, en la comisión de un delito; siempre se observará un sujeto activo y un sujeto pasivo; que a su vez estos pueden ser una o varias personas naturales o jurídicas.

2.4.1. Sujeto activo.

El tratadista Santiago Acurio Del Pino, en su obra “Delito informático”, cita a Mario Garrido Montt, para quien, el sujeto activo será aquella persona que realiza toda o una parte de la acción descrita por el tipo penal.[15]

[14] “Derecho Informático”. (2008). México: Julio Téllez Valdés , (p. 188)

[15] ACURIO DEL PINO SANTIAGO "Delitos Informáticos: Generalidades." Sujetos del Delito Informático< http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf >(10 enero 2015)

En este caso, existe una variedad de sujetos activos, a quienes se los identifica utilizando terminología anglosajona; a saber tenemos los siguientes:

1.-Hacker: Este fenómeno históricamente tiene su origen en el desciframiento de los mensajes que llevaban las palomas mensajeras, y aun mas aquellos mensajes cifrados que eran muy frecuentes en la segunda guerra mundial.

Sin embargo en aquellos momentos estas conductas no eran catalogadas como delitos; sino tan solo con la aparición y evolución del ordenador y de la Red, se dio paso y mayor importancia a estas conductas; y a quienes lo ejecutaban, se los llegó a denominar como hackers; denominación que erróneamente es asociada con los delincuentes cibernéticos.

Se dice que es un error realizar esta generalidad en razón de que existen hackers que a pesar de irrumpir en un ordenador o sistema, no están cometiendo delito alguno. Por lo tanto, para que la actuación de un hacker pueda ser considerada como un delito, mucho dependerá de la intención y grado de culpabilidad, a mas de considerar la tipificación que realice cada estado en su respectivo cuerpo normativo.

Lo antes mencionado hace referencia a que los hacker, son de diversos tipos:

a) **Hacker de Sombrero Blanco.-** Conocido también como Hacker Ético. Este tipo de sujetos rompen seguridades de maneras no dolosas; como por ejemplo, para poner a prueba la seguridad de su propio sistema, o de otros sistemas mediante contratos. Incluso el Consejo Internacional de Consultores de Comercio Electrónico, brinda capacitaciones certificaciones que cuentan con acreditaciones de la Agencia Nacional de Seguridad de los Estados Unidos y de la Iniciativa Nacional para los Estudios y Carreras en

   Cyber-seguridad De Los Estados Unidos.

b) **Hacker de sombrero Negro.**-También son conocidos como **Cracker;** estos se diferencia de los primeros, por su actitud dolosa de la cual obtiene

un beneficio personal, rompiendo sistemas, software y hardware; por ende este grupo posee conocimientos vinculados con la programación y la parte física de la electrónica. Por estas características los grandes programadores de sistemas y la prensa, les han llegado a considerar como el grupo más rebelde de todos.

c) **Hacker de sombrero Gris:** este grupo reúne las características de los dos anteriores; ya que su objetivo es navegar por la Internet y violar un sistema informático con el único propósito de notificar al administrador, que su sistema ha sido vulnerado; luego se ofrecerá para reparar el sistema que él mismo violó, por un módico precio.

d) **Hacker de elite.-**Término utilizado para describir a los expertos, dentro del ámbito social de los hackers.

e) ***Hacker de sombrero azul.-*** Es un experto encargado de encontrar los posibles errores de un sistema antes de su lanzamiento.

f) **Hacktivista.-** Es un hacker que utiliza la tecnología para anunciar un mensaje, ya sea de índole social, ideológico, religioso o político, o de cualquier otra naturaleza que sea de su interés; que en general, envuelve la desfiguración de cybersitios o ataques de denegación de servicio.[16]

2.-Lamers.- Son sujetos que poseen pocos conocimientos informáticos y electrónicos; situación que le vuelve un sujeto obsesivo que le impulsa a buscar amplia información con ayuda de la Red, para posteriormente realizar un sin número de pruebas; razón por la cual se les considera como uno de los grupos más peligrosos, pues ejecutan actividades tales como: bombardean cualesquier correo electrónico enviando miles de mensajes, hasta que colapse el sistema, interceptan el correo electrónico enviando mensajes falsos, etc.

3.-Script kiddies.-Es un simple usuario de Internet, inexperto, carente de conocimiento y experiencia sobres Hackeo y Crackeo; buscan información de

[16]Hacker (seguridad informática). (2015, 19 de febrero). *Wikipedia, La enciclopedia libre*. Fecha de consulta: 21:16, enero 10, 2015 desde <http://es.wikipedia.org/w/index.php?title=Hacker_(seguridad_inform%C3%A1tica)&oldid=80132007.>

hacking, los ejecutan sin ni siquiera leer los ficheros Readme de cada aplicación; y de esta forma liberan virus.

4.-Un neófito o *newbie*.-*Es un principiante, casi no tiene conocimiento sobre hacke**o**.***

5.-Trasher: Son personas que se dedican a hurgar en los basureros y papeleras de los cajeros automáticos para conseguir números de cuentas, claves de tarjetas, y poder cometer actividades fraudulentas a través de internet.[17]

2.4.2.- Sujeto Pasivo.

Es la persona natural o Jurídica, pública o privada, nacional o extranjera; titular del bien jurídicamente protegido, sobre quien recae la acción delictiva de naturaleza informática.

Con la evolución de la Red, en este tipo de delitos, no se atacan a persona individualmente considerados; sino más bien, se afecta a una pluralidad de personas, dependiendo el fin perseguido por el autor del delito; así en unos casos pueden resultar agraviados los adolescentes mediante los mensajes , chat imágenes , videos y demás documentos enviados a sus respectivas cuentas mantenidas en las redes sociales on-line; y como se ha mencionado, las entidades financieras y demás persona jurídicas también puedes resultar víctimas de esta gran ola de criminalidad.

Es por ello que los expertos recomiendan seguir las siguientes instrucciones para evitar ser víctimas de estos delitos.

- No introducir datos, como claves, números de tarjetas desde una red wif publica.
- Entrar a todas las páginas web tecleando la dirección en la barra del navegador.

[17] Hackers y Crackers (lunes, 8 de septiembre de 2008). Ingrid Chaves y YanciVillalo. Fecha de consulta: 20:10, enero 15, 2015 desde <<http://hackersycrackers-yi.blogspot.com/.>

- Actualizar el sistema operativo, para no tener vulnerabilidades de seguridad.
- Verificar los sitios oficiales en los que se desea navegar.
- Contar con una contraseña diferente para cada sitio.
- Disponer de un antivirus que tenga control de navegación en Internet, detección de sitios falsos, etc.
- Cambiar la contraseña cada cierto tiempo.
- Verificar la dirección de Internet de la Institución a la que se va a acceder y el certificado de seguridad.
- Comprobar que se trate de una página segura.
- De ser posible, no ingresar desde el enlace, y dirigirse a la página oficial.
- No hacer clic en enlaces sospechosos, o que se revivan por e-mail de fuentes que no sean de confianza. [18]
- *Obtener y utilizar de forma regular software antivirus. Compruebe que las formas de los antivirus se encuentren actualizadas.*
- *Mantenga una postura altamente escéptica con cualquier archivo recibido a través de internet, ya sea en un anexo de correo electrónico o cualquier archivo ofrecido.*

Signos indicadores de que ha sufrido un ataque.

- En el sistema parecen cuentas desconocidas.
- Aparecen demasiados fallos de inicio de cesión en informes de registro.
- Reinicios imperados de la computadora.
- Perdida de registros.
- Tarifico pesado durante horas de poca actividad.

[18] Delitos Informáticos en la Web podrían aumentar en el Ecuador (17 de noviembre del 20014).El Universo Noticias. Fecha de consulta: 16:00, enero 20, 2015 desde <http://www.eluniverso.com/noticias/2014/11/17/nota/4226966/ataques-web-podrian-aumentar.>

2.5 DELITOS TIPIFICADOS EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL.

El tratadista **Renato Javier Jijena Leiva**, en su obra “Chile, la protección penal de la intimidad y el delito informático ”, considera que el rápido desarrollo del campo informático, facilita la comisión de un sin número de delitos que atentan a la intimidad y a la vida privada de las personas, comprometiendo otros derechos reconocidos y protegidos, lo que ha puesto en alerta a los distintitos Estados; siendo una de sus grandes preocupaciones la protección de cierta información considerada reservada frente al resto de personas; tipificando en sus respectivos cuerpos normativos, la revelación de dicha información sin previa autorización por parte de su titular; con lo que se busca una reglamentación referente a la búsqueda, registro , almacenamiento y transmisión de información personal.

2.5.1 *Artículo 229.- Revelación ilegal de base de datos.*

La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Esta disposición legal, tipifica todas aquellas conductas orientadas a vulnerar el derecho al secreto, la intimidad y privacidad de las personas, revelando determinada información con la cual se puedan ver afectados otros derechos reconocidos y garantizados en la Constitución; así como: el derecho a desarrollar libremente la personalidad, el derecho a la honra, a la buena reputación; el derecho a la libertad de empresa, el derecho a la libertad de opinión y de

expresión; el derecho a la comunicación, el derecho a guardar reserva sobre sus convicciones políticas y religiosas, etc.

Sin embargo, el **Doctor Carlos Riofrío Villalta**, en su artículo titulado “El Derecho de los Secretos: fundamentación de una teoría general” publicado en la Revista Podium de la Universidad de Especialidades Espíritu Santo; nos da a entender que toda información, no merece una protección legal; pues considerada que, determinada información para ser catalogada como secreto, intimo, o privado; y por ende de lugar al derecho al secreto, a la intimidad, o a la privacidad, y consecuentemente merecedora de protección legal; es preciso que reúna ciertos requisitos básicos, tales como: **a)** debe tratarse de una información exclusivamente oculta, **b)** debe ser custodiada, **c)** por parte de una persona o por un conjunto cerrado de ellas; acompañada de la voluntad de mantener tal secreto, seriedad, legitimidad, y por ultimo debe tratarse de información actual y potencial.

Cabe señalar que una de los temas innovadores que recoge el primer inciso del artículo 229, es que esta conducta será sancionada, no solo si el sujeto activo se vale de sistemas informáticos, si no también, telemáticos, o electrónicos, en razón de que para la comisión de un delito de esta índole no solo hace falta el auxilio de Internet, pues muy bien cualquier información de tales características, contenida en cualquier dispositivo de almacenamiento., puede ser difundida por cualquier medio de comunicación convencional, como la televisión, radio, teléfonos móviles, teléfonos convencionales, etc.

La pena por este delito se agrava, si el mismo es cometido ***por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas;*** considerando la gran facilidad que tienes aquellos para acceder a este tipo de información, en comparación a cualquier otro ciudadano; debiendo acotar que mucha de la información a su cargo, a mas de pertenecer exclusivamente a determinada persona, esta exclusividad también puede pertenecer en ciertos casos, hasta al mismo Estado , que con la revelación de información confidencial, no solo resultaría afectada una solo persona, o grupo de aquellas ; sino que se estaría afectando a toda una colectividad.

2.5.2.- **Artículo 230.- intercepción ilegal de datos.**

Será sancionado 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, desvié grave, 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.***

Es decir que, será responsable y sancionada, toda persona que obtenga información protegida, por cualesquiera de los medios posibles de forma ilegal, lo que determina que este derecho, no es absoluto; pues el mismo se encuentra limitado por el derecho a la información, siendo evidente que para lograr obtener aquella información protegida por el Ordenamiento Jurídico, es menester, la autorización de una Autoridad Judicial revestida de jurisdicción y competencia para hacerlo; siempre y cuando dicha información solicitada por la parte interesada, sea para fines legales, vinculada a la naturaleza del proceso , para el cual se requiere.

Como indica esta disposición legal, la sola obtención indebida de información, ya implica un acto delictivo sancionado, aun sin importar el fin que le vaya a dar el sujeto activo, en razón de que para lograr hacerlo, el agente, necesariamente se verá en la necesidad de vulnerar otros derechos, como por ejemplo a los derechos de autor, rompiendo sistemas de seguridad para obtener programas o herramientas idóneas desarrolladas por otra persona, y utilizarlas para su cometido.

Esta clase de actividades delictivas en doctrina , reciben el nombre de **ESPIONAJE INFORMÁTICO,** que es definido por **Marcelo Huerta y Claudio Libano** como "*El acceso no autorizado a los sistemas informáticos; consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual, por el desciframiento de los códigos de acceso o passwords,*

causando daños inmediatos en las víctimas o bien por la mera voluntad de curiosear o divertirse.[19]

Fraude Informático.-

Claramente el artículo 230, numeral 2 describe las actividades propias del fraude informático al señalar que:

La persona que diseñe, desarrolle, venda, ejecute, programe o envíe 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.

Pues, todas las acciones enumeradas en este numeral, orientan al sujeto pasivo a incurrir en un error engañándolo para lograr obtener un beneficio de forma ilícita, en beneficio propio o de un tercero.

Este delito puede cometerse de distintas maneras, como por ejemplo:

Manipulación de datos: esta manipulación puede ser de los datos de entrada o de salida, accediendo a distancia al ordenador del sujeto pasivo, para extraer del computador de la víctima los suficientes datos, claves de acceso, etc.

a) **Manipulación de datos de entrada o falsificación de datos**: Que no son otra cosa que todas las instrucciones o información que se le da a la computadora, como por ejemplo, teclear algo, dar un click del mouse, escanear una imagen, etc.[20] Esta acción puede darse mediante la manipulación de programas, modificando los ya existentes o insertando nuevos programas.

[19]La Internet Como Nueva Tecnología De La Información Y La Comunicación Y La Delincuencia Informática". (2010). Cuenca: Doctor Jaime Edmundo Andrade Jara(, p. 61)
[20] Computadoras e Internet Hardware Otros - Hardware Ra Castillo. Fecha de consulta: 20:10, febrero 10, 2015 desde <https://espanol.answers.yahoo.com/question/index?qid=20090913123845AAPd0Du >

b) **Manipulación de datos de salida, o sustracción de datos:** Estos datos **se refieren a** toda respuesta que da un ordenador, frente a la orden que se le haya dado, por ejemplo, la imagen que da el monitor, las impresiones que se realizan,etc. El ejemplo más claro en este caso, es el fraude a través de los cajeros automáticos, falsificando las instrucciones de la computadora, en la fase de adquisición de los datos.

Manipulación de programas o Caballos de Troya.- Son programas destructivos enmascarados como juegos utilidades, aplicaciones. Su ejecución genera un daño al sistema del computador aunque parezca hacer algo útil, cuando en realidad se está insertando instrucciones de forma encubierta en un programa informático para que efectuara una función no autorizada; mientras se ejecuta su función normal.

Por ejemplo, un Caballo de Troya seria un código escondido en el interior de un juego. El usuario descarga el juego y lo prueba; en principio no notará ninguna diferencia, sin embargo, al ejecutar el programa; este de modo oculto estaría realizando otro tipo de acciones, tales como: borrar códigos, enviar copias de información por la red, instalar virus informáticos, etc.[21]

Técnica de Salami o redondeo de cuentas.- Al programa bancario se le introduce instrucciones, para que este remita a determinada cuenta, imperceptibles sumas de dinero, provenientes de otras cuentas manejadas por el autor.

Pishing.- Se envían correos electrónicos aparentemente de fuentes confiables, por ejemplo de entidades financieras, creando páginas web falsas, con características similares a la de la institución suplantada; realizando encuestas falsas, paginas falsas de recargas de móviles o ventas de productos, con tarjetas de crédito; en donde una vez obtenida la información deseada, la página presenta algún error o indica que la operación no se ha podido realizar. Otro ejemplo es la aparición de presuntos compradores quienes solicitan al vendedor datos

[21] Cursos de Virus Informáticos. Anónimo. Fecha de consulta: 16:00, febrero 15, 2015 desde<http://manto2k.tripod.com/virus.htm.>

financieros para supuestamente realizar el respectivo pago por el producto comprado.

Otra de las modalidades de esta técnica es el **pharming** que consiste en manipular las direcciones DNS-[22] mediante las cuales el autor conduce a la víctima a sitios virtuales falsos.

El mismo artículo, en el numeral 3 una vez más sanciona la obtención ilegal de datos, pero en esta ocasión específicamente, la obtención de toda información vinculada con datos financieros sin importar la forma o técnica utilizada para su adquisición: Pues para lograr dicho cometido el autor bien puede lograrlo cometiendo otros delitos, o con auxilio de un tercero que le haya brindado las facilidades para tal finalidad.

En este sentido, la mencionada disposición legal reza: **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.**

Ahora bien, en la redacción del COIP, en el último numeral del artículo 230, erróneamente se hace alusión al numeral 3 como un inciso.

Para efecto de comprobación de tal falencia, me permito transcribir a continuación el numeral 4 del artículo en mención

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.

[22] Sistema de Nombres de Dominio.-Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet.
Los seres humanos identificamos los sitios de internet mediante nombres, como son Google.com, Yahoo.es, Apple.com, etc. lo que los hace más fácil de recordar y de escribir, estos nombres es lo que conocemos como nombres de dominio.
Las computadoras identifican los sitios web y se conectan a ellos utilizando el formato numérico, algo parecido a la numeración telefónica.
Ahí es donde entran en acción los servidores DNS, ellos son como enormes y complejas guías telefónicas, que a petición nuestra traducen o convierten los nombres de dominio que le solicitemos, en las direcciones que les corresponden.

2.5.3.- Artículo 231.- Transferencia electrónica de activo patrimonial.

La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

Es pertinente anotar que el COIP en esta disposición legal, da paso a la libre interpretación, en razón de que en su redacción utiliza una terminología bastante subjetiva al referirse **"al activo patrimonial",** de lo cual surge interrogantes como ¿Qué se debe entender por activo patrimonial?, ¿qué tipo de bienes y derechos constituyen este activo patrimonial?, ¿los bienes y derechos que le constituyen que valor deben tener para ser considerados como un activo patrimonial?, ¿ Si el valor del activo patrimonial es mínimo, desde un punto de vista económico, es conveniente la intervención del estado?, etc.

De esta manera podremos darnos cuenta que al no establecerse un parámetro que delimite el daño que debe generarse en el activo patrimonial de una persona, mal podría intervenir el Estado sancionando conductas que no merecen la intervención penal; es decir irrespetando el principio de mínima intervención del Estado; principio recogido por nuestra Constitución en el artículo 195.

Doctrinariamente, este delito es identificado como **SABOTAJE INFORMÁTICO**

Para Rodolfo Herrera, el sabotaje informático es: *"toda acción, típica, antijurídica, y dolosa destinada a destruir o inutilizar el soporte lógico de un sistema computacional, empleando medios computacionales.*

Los métodos más usados para causar daños lógicos, es el uso de programas destructores, con los cuales se puede borrar grandes cantidades de información en un corto tiempo;

1.- Bombas lógicas o cronológicas.- Consiste en un programa o parte de él, que permanece inactivo, hasta que una pieza específica de la lógica del programa es activada. Debido a esas características, una bomba lógica es parecidas a las minas de tierra; en este caso el activador más usual es una fecha; en este evento, los controles de la fecha del sistema de la bomba lógica, no hacen nada hasta que la hora y la fecha lleguen, siendo en ese instante que la bomba lógica se activa y ejecuta su código.

Estas bombas, también, pueden ser programadas para activar una gama variada de condiciones, como cuando una base de datos crece más allá de un cierto tamaño, entonces es eliminada. *La forma más peligrosa de la bomba lógica es aquella que se activa, cuando algo no sucede.*

Por otro lado*, la acción de las bombas lógicas, van dirigida contra una víctima específica para lograr causar algún daño como:* borrar información del disco duro, mostrar un mensaje, reproducir una canción, enviar un correo electrónico, apagar el monitor

La doctrina ha clasificado a las bombas lógicas o cronológicas en las siguientes:

a) Bombas fijas.-Estas son las que toman como referencia una fecha fija en la que se precipitará la reacción esperada.

b) Bombas variables.- El programa se activa en el momento en que se cumplen las condiciones que el programador ha determinado para que se desencadene la reacción esperada.

c) Bombas aleatorias.-Los estudiosos de la Delincuencia Informática les han definido a este tipo de métodos destructivos como mixtos ya que combinan las condiciones de tiempo y de modo; en otras palabras, se cumple la acción de la

bomba en la fecha y hora previstas, si antes se ha cumplido con las condiciones de ejecución.

2.- El virus informático.- Tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o conocimiento del usuario; pudiendo destruir, de manera intencionada, los datos almacenados en un ordenador.

Estos virus informáticos se propagan a través de un software, al ser ejecutado por la víctima; mismos que se caracteriza por afectar a casi todos los sistemas operativos conocidos y usados actualmente, (destacando que el virus, sólo atacará al sistema operativo, para el cual fue desarrollado); pudiendo ocasionar cortes en los sistemas de información, daños a nivel de datos; por diseminarse y propagarse por medio de réplicas y copias; a veces bloquean el ordenador, destruyen la información almacenada en el respectivo dispositivo, unas veces, y otras reducen el espacio en el disco.

Los expertos, advierten que en la actualidad, una de las formas de transmisión de virus se da atreves de la aplicación de WhatsApp, en el momento en el que los usuarios sus usuarios realizan llamadas VolP (es un método por el cual tomando señales de audio analógicas, se las transforma en datos digitales que pueden ser transmitidos a través de internet hacia una dirección determinada.). Posteriormente la aplicación maliciosa activa llamadas WhatsApp, que redirecciona al usuario a un formulario en el que le solicitaba su número de teléfono para inscribirlo en un servicio de SMS Premium (Mensaje corto de texto que se puede enviar entre teléfonos celulares o móviles.)

Otro caso es el envió de correo electrónicos, en los que se informan que, el usuario tiene pendiente escuchar un mensaje de voz. Para escucharlo es necesario hacer click en la opción Auto-play, que en realidad es un enlace a una web maliciosa.

2.5.4.- 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.***

Esta disposición legal resulta ser un tipo penal abierto, por lo tanto genera inseguridad jurídica y atenta al principio de legalidad al introducir la frase ***"de cualquier manera***", con la que se da a entender que no se considera la licitud o, ilicitud de la producción, venta, distribución, creación de los distintos programas informáticos.

2, Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Es evidente que nuestra legislación, se orienta a la protección tanto de los sistemas informáticos como telemáticos; sin dejar de lado la protección a los derechos de propiedad intelectual, tema que ha venido desarrollándose en la legislación ecuatoriana, acorde a las nuevas necesidades que presenta la sociedad, siendo una de ellas la protección de las diferentes creaciones informáticas que son consideradas en la Ley de Propiedad Intelectual en el artículo 8 bajo la denominación de "programas de ordenadores". Por lo tanto sólo el titular de un programa de ordenador, puede autorizar: la reproducción total o

parcial del programa, la traducción o transformación del programa; así como la distribución del mismo.

Sin embargo, se debe indicar que en el numeral dos del artículo referente, si bien es cierto trata de proteger derechos de propiedad intelectual, en atención al artículo 288, de la Ley de Propiedad Intelectual, el que da lugar al ejercicio de acciones civiles, administrativas o penales por la vulneración de derechos de esta índole.

No es menos cierto que estos tipos penales merecen un tratamiento especial en un capitulo plenamente destinado a su tratamiento; puesto que no es lo mismo sancionar a un sujeto que atente contra el derecho a la intimidad, privacidad, que cause daño en el activo patrimonial; que a alguien que destruya, altere, copie, clone, distribuya o realice cualquier otra acción sin la autorización del titular de esos derechos de propiedad intelectual; puesto que los derechos de propiedad intelectual no solo están vinculados con derechos patrimoniales, sino que estos también involucran derechos morales como:

- Reivindicar la paternidad de su obra.
- Mantener la obra inédita o conservarla en el anonimato o exigir que se mencione su nombre o seudónimo cada vez que sea utilizada;
- Oponerse a toda deformación, mutilación, alteración o modificación de la obra que pueda perjudicar el honor o la reputación de su autor;
- Acceder al ejemplar único o raro de la obra que se encuentre en posesión de un tercero, a fin de ejercitar el derecho de divulgación o cualquier otro que le corresponda.
- Reclamar indemnización de daños y perjuicios independientemente de las otras acciones contempladas en la Ley de Propiedad intelectual.

También incluye el derecho exclusivo de explotación, mismo que encierra lo siguiente:

- La reproducción de la obra por cualquier forma o procedimiento.
- La comunicación pública de la obra por cualquier medio que sirva para difundir las palabras, los signos, los sonidos o las imágenes.
- La distribución pública de ejemplares o copias de la obra mediante la venta, arrendamiento o alquiler.
- La importación.
- La traducción, adaptación, arreglo u otra transformación de la obra.

En este punto concluyo indicando que el artículo 289 de la Ley de Propiedad intelectual, a más de los derechos reconocidos, en caso de ser vulnerados los mismos da la posibilidad a demandar:

- La cesación de los actos violatorios.
- El comiso definitivo de los productos u otros objetos resultantes de la infracción, el retiro definitivo de los canales comerciales de las mercancías que constituyan infracción, así como su destrucción.
- El comiso definitivo de los aparatos y medios empleados para el cometimiento de la infracción.
- El comiso definitivo de los aparatos y medios para almacenar las copias.
- La indemnización de daños y perjuicios.
- La reparación en cualquier otra forma, de los efectos generados por la violación del derecho.
- El valor total de las costas procesales.

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.

El Código considera como agravante, el daño cometido a bienes informáticos destinados al servicio público, o, seguridad de la ciudadanía; ya que la primera está orientada a satisfacer necesidades de una colectividad, de interés general, a través de las diferentes entidades públicas o privadas creadas por la Constitución o la Ley. En tanto que la Seguridad Ciudadana, debe ser entendida como la situación de tranquilidad y seguridad en una comunidad, como producto del respeto de las normas de convivencia social y del control de la criminalidad, que permite el desarrollo de las actividades ciudadanas en forma normal.

A esta actividad delictiva la doctrina la denomina **ACCESO NO AUTORIZADO A SERVICIOS INFORMÁTICOS;** que para los autores chilenos **Marcelo Huerta y Claudio Líbano**, consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o passwords, causando daños inmediatos y tangibles en la víctima, o bien por la mera voluntad de curiosear o divertirse de su autor.

Para Claudio Líbano este delito puede clasificarse en: a) hacking directo o acceso indebido, y; b) hacking indirecto o como medio de comisión de otros delitos.

Entre los diferentes métodos preferidos se pueden encontrar:

a) **Puertas falsas.-** Consiste en aprovechar las rutas directas y ocultas de accesos al sistema, que sirven para hacer la revisión o la recuperación de información en caso de errores del sistema.

b) **Llave maestra.-** Uso no autorizado de programas para modificar, destruir, copiar, insertar, utilizar o impedir el uso de datos archivados en un sistema informático.

c) **Pinchado de líneas.-** Se realiza a través de la interferencia de líneas telefónicas o telemáticas a través de las cuales se transmiten la información procesada en las bases de datos informáticas.

2.5.5.- Artículo 233.- Delitos contra la información pública reservada legalmente.

La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años.

La Información clasificada, debe ser comprendida como, toda aquella información que no puede ser divulgada libremente por los distintos medios de comunicación; es así que el artículo 30 de la Ley Orgánica de Comunicación considera como tal la siguiente información:

- Aquella que esté protegida expresamente con una cláusula de reserva previamente establecida en la ley.
- La información acerca de datos personales y la que provenga de las comunicaciones personales, cuya difusión no ha sido debidamente autorizada por su titular, por la ley o por juez competente.
- La información producida por la Fiscalía en el marco de una indagación previa.
- La información acerca de las niñas, niños y adolescentes que viole sus derechos según lo establecido en el Código de la Niñez y Adolescencia, por ejemplo circulación de publicaciones, imágenes, videos, grabaciones, que contengan información inadecuada para subdesarrollo[23].

Por otro lado la Ley Orgánica De Transparencia Y Acceso A La Información Pública en el artículo 17 manifiesta que información reservada comprende:

[23] Artículo 46,52, 54 del Código de la Niñez y Adolescencia.

a) Los documentos calificados de manera motivada como reservados por el Consejo de Seguridad Nacional, por razones de defensa nacional, de conformidad con el artículo 81, inciso tercero, de la Constitución Política de la República y que son:

- Los planes y órdenes de defensa nacional, militar, movilización, de operaciones especiales y de bases e instalaciones militares ante posibles amenazas contra el Estado.

- Información en el ámbito de la inteligencia, específicamente los planes, operaciones e informes de inteligencia y contra inteligencia militar, siempre que existiera conmoción nacional.

- La información sobre la ubicación del material bélico cuando ésta no entrañe peligro para la población.

- Los fondos de uso reservado exclusivamente destinados para fines de la defensa nacional.

b) Las informaciones expresamente establecidas como reservadas en leyes vigentes.

Es importante señalar que esta información se mantendrá bajos estas características durante 15 años contados a partir de la fecha de su clasificación.

Perderá esta categoría cuando desaparezcan las causas que indujeron a la misma.

Este periodo de reserva puede ampliarse, siempre y cuando permanezca y se justifique las causales que dieron lugar a su clasificación.

La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.

Es notorio el vacío que deja este inciso, puesto que, se sanciona directamente tan solo la obtención de información de tales características, y no así la intensión con la cual actuó el servidor público.

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información, que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.

Claramente la protección de información confidencial tiene como fin el amparo de **la** Seguridad del Estado; toda vez que con esta actividad delictiva se pondría en grave riesgo a toda una población.

Nuevamente este artículo hace referencia a delitos informáticos ya vistos en los artículos anteriores, como son: la obtención ilegal de datos, sabotaje, informático, fraude informático, acceso no autorizado a servicios informáticos, revelación ilegal de datos. Con la diferencia de que estos datos están vinculados con información confidencial vinculada al Estado.

2.5.6.- 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.

Por último, este artículo hace mención a la conocida **PIRATERÍA INFORMÁTICA,** que consiste en la comercialización de obras protegidas, sin que exista el consentimiento del autor de los derechos de propiedad intelectual. Más con el desarrollo de la red, se da la transferencia masiva de productos sin previo consentimiento de su propietario.

Doctrinariamente existen cinco tipos de piratería, así:

a.- Piratería por usuario final.- Se presenta cuando un empleado de una empresa, reproduce copias de software sin que tenga autorización para ello;

b.- Uso excesivo del servidor por parte de un cliente.- Esta especie de piratería se presenta cuando varios empleados en una red, usan de manera simultánea una copia central de un programa; en este caso, si hay más usuarios que los que permite la licencia, estamos frente a un uso excesivo.

c.- Carga de uso de disco duro. Se da cuando una empresa que vende ordenadores, los carga con copias ilegales de software en los discos duros, generalmente, para que la compra resulte más atractiva.

d.- Falsificación de software.- Supone la reproducción y la venta ilegal de material protegido por derechos de autor, con la intención y el ánimo de imitar dicho producto protegido.

e.- Piratería por Internet.- Se presenta cuando se descarga software de Internet; en este aspecto, la piratería a través de la red de redes, supone la utilización de variadas fórmulas para atentar contra propiedad intelectual; por ejemplo:

- Cuando los sujetos activos de la infracción ofertan los materiales protegidos por los derechos de autor, mediante páginas web, ya sea mediante el uso de los sistemas de conversación multiusuario, conocido con el nombre de Internet Relay Chat, o simplemente a través del correo electrónico.

- Cuando se proporciona facilidades para que el usuario sea quien acceda y descargue los archivos. En este evento, se ofrece archivos pirateados mediante páginas web o FTP (File Transfer Protocol, que es un protocolo de nivel de aplicación utilizado para copiar archivos a y desde sistemas remotos de computadora en una red, utilizando Internet); en efecto para acceder y realizar la descarga, se utiliza una contraseña.

- El uso de programas, en los que un usuario posibilita el acceso a una porción o a la totalidad de su disco duro a otros usuarios, a raíz de lo cual se estructura un gran caudal común de obras protegidas; en este caso, todos los usuarios acceden fácilmente a través de los buscadores.[24]

Nótese que en los artículos 230, numerales 2 y 4; 231, inciso segundo y 232, numeral 1, también se considera como delito la creación, desarrollo y divulgación de las herramientas necesarias e idóneas para la comisión de los distintos delitos tipificados en los artículos correspondientes; ya que sin el auxilio de esas herramientas, el sujeto activo jamás podría llegar a materializar dichos actos delictivos. Por lo tanto al ser considerados como delitos cada una de estas actividades, es lógico que quien inobserve la respectiva disposición legal será merecedor de una pena, la cual varía de acuerdo al objeto o intensión que consecuentemente impulsa a esas conductas.

Para concluir este tema, debemos ser conscientes que un gran número de la población al menos posee una cuenta en cualquier Red Social On-line, las cuales se han convertido en los medios idóneos para comerte cualquier clase de delitos, y aun mas los ya conocidos delitos convencionales, como por ejemplo; terrorismo, amenazas, divulgación de material pornográfico, injurias, estafa, etc.

[24] La Internet Como Nueva Tecnología De La Información Y La Comunicación Y La Delincuencia Informática". (2010). Cuenca: Doctor Jaime Edmundo Andrade Jara(, p. 45-68)

CAPITULO III

LA PRUEBA PERICIAL INFORMÁTICA EN LA LEGISLACIÓN ECUATORIANA.

3.1.- GENERALIDADES.

La misma naturaleza dinámica del ser humano, en el sentido de que este no puede desenvolverse aisladamente de la sociedad; da como resultado a un sin número de relaciones, ya sean de orden social o jurídico, las cuales en cualquier momento requieren ser demostradas, para realizar aclaraciones, para una mera satisfacción de los interesados, demostrar irresponsabilidad o responsabilidad con respecto a una acción u omisión tal como sucede en el campo del Derecho; y mas situaciones de la vida cotidiana, de las ciencias, el arte y tecnologías.

En este sentido se debe mencionar que la prueba juega un papel preponderante en el ámbito jurídico; puesto que constituye la esencia misma del debido proceso; tanto más que nuestra Carta Magna en el artículo 76, numeral 4 establece que "***En todo proceso en el que se determinen derechos y obligaciones de cualquier orden, se asegurará el derecho al debido proceso que incluirá las siguientes garantías básicas:" "Las pruebas obtenidas o actuadas con violación de la Constitución o la ley no tendrán validez alguna y carecerán de eficacia probatoria.".*** Pues sin ella no sería posible aclarar y demostrar aquellos hechos controvertidos, dudosos.

Por lo tanto se puede decir, al igual que otros autores, la prueba es "***el corazón del problema en juicio",*** cuyo objeto está formado por aquellos hechos individuales o colectivos, voluntarios o involuntarios, provenientes del hombre o de la naturaleza, las cosas materiales o inmateriales, hechos físicos o psíquicos, incluyendo los derechos y excepciones reclamadas y planteadas por las partes litigantes.

Como bien lo establece el Código Orgánico Integral Penal en su artículo 453 que la finalidad de la prueba es "***llevar a la o al juzgador al convencimiento de los hechos y circunstancias materia de la infracción y la responsabilidad de la persona procesada***.", permitiendo de esta manera que la misma cumpla con su

función social y jurídica, que no es otra cosa que el restablecimiento de la paz social y satisfacer el interés de aquella parte que considere que sus derechos han sido violentados.

3.2.- CONCEPTO DE PRUEBA.

Caravantes manifiesta que la etimología puede tener dos criterios estos son:

"Procede del adverbio ***probe,*** que significa honradamente, por considerarse que obra con honradez quien prueba lo que pretende y;

Proviene de ***Probandum,*** de los verbos recomendar, aprobar, experimentar, patentizar, hacer fe, según varias leyes del Derecho Romano.[25]

Ricardo Vaca Andrade**,** en su obra "Manual de Derecho Procesal", tomo I conceptualiza a la prueba como "***el modo de introducir en el proceso la constancia o evidencia de los hechos relacionados con el objeto de cada proceso penal y que se da como consecuencia del esfuerzo de todos los sujetos procesales para conseguir que la producción, recepción y valoración de los elementos de prueba facilite el descubrimiento de la verdad real.***"

3.3- PRINCIPIOS DE LA PRUEBA EN EL ÁMBITO PENAL.

El mismo COIP en el artículo 454 prescribe los principios que regirán a la prueba:

1. Oportunidad.- Es anunciada en la etapa de evaluación y preparatoria de juicio y se practica únicamente en la audiencia de juicio. Los elementos de convicción deben ser presentados en la etapa de evaluación y preparatoria de juicio. Las investigaciones y pericias practicadas durante la investigación alcanzarán el valor de prueba, una vez que sean presentadas, incorporadas y valoradas en la audiencia oral de juicio. Sin embargo, en los casos excepcionales previstos en este Código, podrá ser prueba el testimonio producido de forma anticipada.

[25]El Documento Electrónico: Su Importancia, Trascendencia y Valor Probatorio en la Legislación Ecuatoriana". (2010). Marcia Fernanda Cedillo Díaz (, p. 72)

A través de este principio se genera seguridad procesal a favor de cada una de las partes procesales, en tal virtud garantiza regularidad y temporalidad a los procesos , evitando dilaciones en los mismos, y actuaciones de mala fe de alguna de las partes presentado pruebas en último momento; aunque en este último caso el COIP en el artículo 617 realiza una excepción, permitiendo presentar pruebas en el día de la Audiencia de Juzgamiento siempre y cuando cumpla con dos requisitos a) no tener conocimiento de la prueba, sino hasta ese momento y b) que sea relevante para el proceso.

2 inmediación.- Las o los juzgadores y las partes procesales deberán estar presentes en la práctica de la prueba.

Es tan verdadera y apegada al debido proceso la siguiente frase "***mientras más cerca está el juez de la prueba, más cerca está de la verdad***"; puesto que el juez para poder tener verdadero conocimiento de causa, y resolver con certeza, es necesario que este como actor principal del proceso, tenga una relación directa con todos los momentos de la actividad probatoria; pudiendo de esta manera garantizar un debido proceso.

Por su parte, los sujetos procesales al tener conocimiento de la prueba a practicarse podrán hacer ejercicio de su derecho a la contradicción impugnado, pidiendo aclaraciones de las mismas; principio que además implica el derecho a la defensa.

3 Contradicción.- Las partes tienen derecho a conocer oportunamente y controvertir las pruebas, tanto las que son producidas en la audiencia de juicio como las testimoniales que se practiquen en forma anticipada.

Este principio está vinculado con el anterior; a mas de ser un principio de orden constitucional; en razón de que la Constitución en el artículo 168, numeral 6 señala que "***La administración de justicia, en el cumplimiento de sus deberes y en el ejercicio de sus atribuciones, aplicará los*** **siguientes** ***principios:" " La sustanciación de los procesos en todas las materias, instancias, etapas y diligencias se llevará a cabo mediante el sistema oral, de acuerdo con los***

principios de concentración, contradicción y dispositivo." Por lo tanto ninguna prueba podrá ser evacuada sin conocimiento del juez, tribunal, o de las partes procesales, o cuando esta haya sido enunciada o practicada fuera del momento procesal oportuno.

4. **Libertad probatoria.-** Todos los hechos y circunstancias pertinentes al caso, se podrán probar por cualquier medio que no sea contrario a la Constitución, los instrumentos internacionales de derechos humanos, los instrumentos internacionales ratificados por el Estado y demás normas jurídicas.

Es decir que el objeto de la prueba podrá ser demostrado a través de cualquier medio legalmente permitido, idóneo y conducente para tal fin. En tal caso los sujetos procesales están en la obligación de actuar con apego a la verdad, tal como lo dispone la Constitución como un deber de todos los ciudadano en el artículo 83, numeral 12, "***ejercer la profesión son sujeción a la ética.***" Y el Juez por su parte podrá dictar cualesquier medida que facilite la aplicación de este principio.

5. Pertinencia.- Las pruebas deberán referirse, directa o indirectamente a los hechos o circunstancias relativos a la comisión de la infracción y sus consecuencias, así como a la responsabilidad penal de la persona procesada.

Los medios de prueba utilizados beben ser coherentes y viabilizar la demostración de los hechos discutidos, es decir que deben haber concordancia entre los hechos requeridos de prueba y ,los medios a utilizarse, a fin de evitar dilaciones innecesarias en el desarrollo del proceso, agotando indebidamente recursos económicos, materiales, humanos. Lo que implica una limitante al principio de libertad para evitar que alguna de las partes procesales solicite la práctica de pruebas impertinentes, ajenas al proceso.

6. Exclusión.- Toda prueba o elemento de convicción obtenidos con violación a los derechos establecidos en la Constitución, en los instrumentos internacionales de derechos humanos o en la Ley, carecerán de eficacia probatoria, por lo que deberán excluirse de la actuación procesal. Se inadmitirán aquellos medios de

prueba que se refieran a las conversaciones que haya tenido el fiscal con la persona procesada o su defensa en desarrollo de manifestaciones preacordadas. Los partes informativos, noticias del delito, versiones de los testigos, informes periciales y cualquier otra declaración previa, se podrán utilizar en el juicio con la única finalidad de recordar y destacar contradicciones, siempre bajo la prevención de que no sustituyan al testimonio. En ningún caso serán admitidos como prueba.

Este principio esta íntimamente ligado con el principio de legalidad, pues para que la prueba haga fe en juicio será imprescindible la observancia de las disposiciones legales que regulan tanto los medios de prueba, como el procedimiento a seguirse para la demostración de los hechos controvertidos.

7. Principio de igualdad de oportunidades para la prueba.- Se deberá garantizar la efectiva igualdad material y formal de los intervinientes en el desarrollo de la actuación procesal.

Partamos del hecho de que el Ecuador es un estado Constitucional de Derechos y justicia, que reconoce y garantiza a todos sus habitantes nacionales y extranjeros los derechos y garantías reconocidos por el Ecuador en la misma Constitución, Instrumentos internacionales, siendo una de estas garantías “el debido proceso” regulado en el artículo 75 y 76, en donde se garantiza a las personas el acceso a la justicia en igualdad de condiciones sin discriminación alguna, permitiendo de este modo no favorecer o desfavorecer a las partes procesales en atención a sus diferentes condiciones, en miras a evitar parcialidad en la administración de justicia.

3.4.- FUENTES Y MEDIOS DE PRUEBA.

Al surgir un conflicto jurídico de índole penal, los indicios, evidencias quedan dispersas en varias fuentes, como por ejemplo en un disco duro, en un CD, en la memoria de las personas, en la naturaleza, etc., las cuales necesariamente deberán ser incorporadas en el proceso con auxilio de los medios de prueba permitidos por la ley, que en nuestro caso el COIP en el artículo 498 reconoce tres medios, a saber son: a) el documento, b)el testimonio y c) la pericia.

De lo antes manifestado se colige que no debe haber confusión entre fuente y medios de prueba.

Fuente de prueba.- Es un concepto extraprocesal, es una realidad anterior, exterior e independiente del proceso.[26]

Medios de prueba.- El tratadista mexicano Javier Piña Palacios, enseña que los medios de prueba son "los instrumentos que sirven para obtener los elementos necesarios que, utilizándolos, pueden llevar a la conclusión de si un determinado hecho está o no probado."[27]

Doctrinariamente se han desarrollado múltiples clasificaciones de los medios de prueba en atención al tipo de fuentes de la prueba, aunque en la práctica una u otra clasificación no influya en el desarrollo del proceso. En este sentido la clasificación más tradicional de es la elaborada por Bentham,

Primera:

a) Medios de prueba personales: Son aquellas aportadas por el ser humano.

b) Medios de prueba reales: generalmente deducidas del estado de las cosas.

Segunda:

a) Medios de prueba directos: Por ejemplo el testimonio.

b) Medios de prueba indirectos o circunstanciales: Se refiere a objetos o bien vestigios que permitan acreditar algo.

Tercera:

a) Medios de prueba voluntarios: Es aquella llevada al juzgador a la primera solicitud o sin necesidad de solicitud judicial, sin necesidad de ninguna medida coercitiva.

[26] Fuentes de Prueba. Enciclopedia Jurídica. Fecha de consulta: 10:00, febrero 20, 2015 desde <.http://www.enciclopedia-juridica.biz14.com/d/fuente-de-prueba/fuente-de-prueba.htm>
[27] Manual De Derecho Procesal Penal, tomo II (2010). Ricardo Vaca Andrade (p. 903)

b) Medios de prueba involuntarios: Es aquella presentada ante el juez o tribunal mediante el uso de la coacción.

Cuarta:

a) Medios de prueba por práctica

b) Medios de prueba por documento.

Este carácter dependerá de la producción de éstos, si surgen como consecuencia y durante el proceso o bien de manera independiente y sin la intención de utilizarlos en él.

Quinta:

a) Medios de prueba por documentos ocasionales: Por ejemplo la correspondencia personal, la agenda personal, el diario o cualquier otro documento análogo que no se haya realizado por el autor con la manifiesta intención de utilizarla en un proceso judicial

b) Medios de prueba por documentos preconstituidos. Cuando se trata de un documento auténtico realizado en cumplimiento a ciertas formas legales con el objetivo de ser destinado posteriormente en un proceso.

Sexta:

a) Medios de prueba independiente de cualquier otra causa.

b) Medios de prueba dependientes.

Séptima:

a) Medios de prueba originales: Por ejemplo el testimonio de un testigo presencial.

b) Medios de prueba derivados: como el caso de fotocopias de documentos originales.[28]

3.5.- MOMENTOS DE LA ACTIVIDAD PROBATORIA.

Ricardo Vaca Andrade, en su obra "Manual de Derecho Procesal Penal, tomo II" indica que, al iniciar una acción penal de orden pública, para lograr la práctica de la prueba idónea en el momento procesal oportuno, necesariamente la prueba deberá cumplir con ciertas etapas:

3.5.1.- Proposición.-

Debemos tener claro que en los casos de acción pública, inicialmente deben pasar por una etapa de investigación llamada indagación previa, a fin de obtener los suficientes indicios que determinen la existencia de una infracción, en base a los cuales el Fiscal podrá dar inicio a un proceso penal con la Instrucción Fiscal, etapa en la cual se seguirá recabando indicios y más elementos que determinen la existencia del delito y la responsabilidad de determinada persona/s. una vez culminada dicha etapa el fiscal formulará cargos en la Audiencia Preparatoria de Juicio en base a todos los elementos recopilados. Si el Juez competente considera que hay merito suficiente para continuar con el proceso, dictará el Auto de Llamamiento a Juicio, para lo cual deberá analizar todas las versiones, peritajes, testimonios anticipados, etc., los mismos que servirán para que el tribunal en la Etapa de Juicio obtenga pruebas que les lleve a pronunciarse en uno u otro sentido.

El punto es que todas las diligencias que se hayan sido solicitadas y practicadas con observancia de las disposiciones legales, durante la Indagación previa e Instrucción Fiscal, constituirán el pilar fundamental en el cual apoyaran su decisión, ya sea el Juez de lo penal o el Tribunal.

En este sentido diremos que la prueba puede ser propuesta por:

[28] Los Medios de Prueba en Materia Penal (2011). Instituto de Investigaciones Jurídicas de la UNAM. Fecha de consulta: 14:00, febrero 20, 2015 desde< http://www.juridicas.unam.mx/publica/rev/boletin/cont/83/art/art8.htm.>

Estado: quien actúa a través de los órganos competentes:

- **Fiscal.**-Haciendo uso de sus facultades, dispone que la Policía Judicial realice alguna diligencia, o cuando el Fiscal solicita al Juez la práctica de alguna diligencia.

Se debe tener presente que tanto el juez, como el presidente del tribunal de garantías pénales, no proponen prueba; en este caso sus facultades se limitan a disponer la prueba solicitada por alguno de los sujetos procesales; pero si están en la facultad de interrogar a los testigos, pero tan solo con fines de aclaración de los hechos que declaran.

- **Por iniciativa de parte:** En este caso el procesado, tiene la posibilidad de presentar al Fiscal evidencia que demuestre que no es responsable del delito. Y por otra parte esta prueba puede ser presentada por la victima, a más de las ya obtenidas por Fiscalía.

  Si alguna de los sujetos procesales pide la práctica de alguna diligencia como medio de prueba, es relevante que la misma especifique que es lo que desea que se averigüe.

3.5.2.- Producción.-

Se cumple cuando se realiza la diligencia, que es el medio de prueba, una vez que las partes procesales hayan solicitado la práctica de ciertas diligencias probatorias al Fiscal, Juez de lo Penal, o Tribunal en su caso; quienes aceptarán la producción y por tanto ordenarán la práctica de lo pedido, al considerar que es conveniente, oportuno, relevante y pertinente. Así por ejemplo la victima solicita al fiscal la práctica de una pericia informática, la cual es aceptada y por ende ordenado; mismo que se cumple según la doctrina en las siguientes fases:

Estudio de antecedentes y toma de datos adicionales.- Se recopila toda la documentación necesaria existente sobre el caso, y que sirve para dar respuesta a lo que se está pidiendo averiguar. Se realizará un reconocimiento pericial, es

decir, someter a la revisión técnica los elementos informáticos para obtener determinados datos de comportamiento o detalles técnicos imprescindibles.

Estudio de los datos y hechos observados.- En esta fase se buscan las relaciones entre los datos adquiridos para llegar a conclusiones intermedias que permitan construir los fundamentos del estudio.

Elaboración y entrega del informe pericial.- Se procede a la elaboración del informe, sintetizando las conclusiones.

La defensa del informe.- Por último, la fase de la defensa del informe tiene por objeto ratificar y afianzar el trabajo realizado. Para ello el perito comparece y de forma oral aclara las conclusiones obtenidas y los métodos empleados para conseguirlas.[29]

3.5.3 Valoración De La Prueba.-

Es la operación intelectual destinada a establecer la eficacia conviccional de los elementos de prueba. Tiene por objeto establecer la utilidad jurídica y legal de las diversas pruebas que han sido incorporadas al proceso penal.

Nuestra legislación acoge el sistema de la sana crítica para todo el desarrollo del proceso, y aun más para la valoración de las pruebas.

Este sistema da la posibilidad al juzgador de llegar a sus conclusiones sobre los hechos de la causa, valorando la prueba con total libertad, respetando los principios de la recta razón, esto es con miramiento a las normas de la lógica, de la psicología, de la experiencia común.

Las características más importantes del sistema de la sana crítica son:

- La sentencia tiene que ser debidamente motivada.
- La resolución solo puede fundamentarse en las pruebas oportunas, legalmente incorporadas al proceso.

[29] Reflexiones Técnicas y Jurídicas de la Prueba Pericial Informática" (2008). Doctor Edgar Francisco Cevallos Gualpa (p. 42-44)

- La confortación razonada de todas las pruebas, tanto de cargo como de descargo.

3.6.- EL PERITO INFORMÁTICO

Para Juan Carlos Riofrío “los peritos en general, son personas expertas en una materia, capaces de aportar al juez conocimientos que no posee, con el fin de servir de lentes de aumento para la justicia con el fin de aclarar el asunto litigiosos en revisión.”

Desde un punto de vista muy generalizado se podría decir que las personas calificadas para ser peritos en el área informática, serian los Ingenieros y Tecnólogos en Sistemas y Telemática, quienes deberán contar con vasta experiencia y conocimientos.

Sin embargo se considera que esto no es suficiente; porque para que el perito logre una satisfactoria experticia, es menester que estos estén formados en aéreas complementarias, como son:

Áreas de Tecnologías de Información y Electrónica:

- *Lenguajes de programación*.- Es un lenguaje formal diseñado para expresar procesos que pueden ser llevados a cabo por máquinas como las computadoras.

Pueden usarse para crear programas que controlen el comportamiento físico y lógico de una máquina, para expresar algoritmos con precisión, o como modo de comunicación humana.

- *Teorías de sistemas operacionales y sistemas de archivo*.- Se refiere al software del sistema; conjunto de programas de computadora que permite una administración eficaz de sus recursos.

- *Protocolos e infraestructuras de comunicación.-* Los protocolos son determinadas reglas a cumplir por los dispositivos que desean comunicarse; constituyen la base del Internet, y razón principal de su éxito. Se dividen en varios niveles: de transporte, de internet, direcciones IP, usuarios y dominios, dominios

geográficos, sistema de nombres de dominio, números de puerto, nivel de red/enlace.

- *Fundamentos de circuitos eléctricos y electrónicos*.- Es necesario conocer aspectos sobre la distribución y la transformación de la potencia eléctrica, sobre todo en motores eléctricos; teorías de circuitos básicos; circuitos dinámicos y su relación con la electrónica.

.- *Arquitectura de Computadores*.- En este campo es necesario conocer aspectos sobre: unidad central del sistema, unidad central de proceso, unidad de control (CU), unidad aritmética y lógica (ALU), registros, memoria de acceso aleatorio (RAM), memoria ROM, caché, buses, arquitecturas de bus, reloj, tarjetas de expansión interna, tarjetas controladoras de periféricos, tarjetas de expansión controladoras del modo de video, tarjetas controladoras de comunicaciones, etc.

- *Fundamentos de Bases de Datos*. Las bases de datos almacenan datos, permitiendo manipularlos fácilmente y mostrarlos de diversas formas. El proceso de construir una base de datos es llamado diseño de base de datos. La informatización de una base de datos requiere de un SGBD, es decir de un conjunto de programas encargados de definir, construir y manipular una base de datos, y mantener su integridad. Algunas bases de datos populares son: MS Access, dBase, FoxPro, Paradox, Approach, Oracle y Open Office Base.

- *Áreas de Seguridad de la Información*.- Las áreas se refieren a la confidencialidad, integridad, disponibilidad y fiabilidad de la información con relación a servidores, clientes y dispositivos, gestión de actualizaciones y descargas, seguridad de red y perimetral, protección frente a virus y otras amenazas, correo electrónico, etc.

-*Principios de Seguridad de la Información*.- Es necesario conocer el conjunto de metodologías, prácticas y procedimientos que buscan proteger la información como activo valioso, con el fin de minimizar las amenazas y riesgos continuos a los que está expuesta.

- Políticas, estándares y procedimiento en Seguridad de la Información

- Análisis de vulnerabilidades de seguridad informática.- La vulnerabilidad conocida también como falencias o brechas representa el grado de exposición a las amenazas en un contexto particular, es decir, en este caso dentro de la generación, transmisión, intercambio y almacenamiento de la información.

- Análisis y administración de riesgos informáticos.- Hace alusión al conocimiento sobre análisis y administración tanto de los riesgos físicos como de los riesgos lógicos. Entre los primeros se encontrarían los incendios, inundaciones, sabotajes, vandalismos, accesos indebidos e indeseados, etc. Entre los segundos: fraudes informáticos, espionaje, virus, ataques de intrusión, denegación de servicios, etc.

- Clasificación de la información, técnicas de hacking y vulneración de sistemas de información.- Es fundamental conocer la clasificación de la información tomando como parámetros, su grado de confidencialidad.

En este sentido, como se vio anteriormente, hay de tres niveles de información: pública, restringida, y confidencial o estratégica, las mismas que igualmente tendrán diferentes medidas de seguridad para enfrentar la acción de los crackers.

- Mecanismos y tecnologías de seguridad informática.- Entre las principales se plantean: intercambio de autenticación, cifrado, integridad de datos, firma digital, control de acceso, tráfico de relleno, firewalls (es un sistema diseñado para impedir el acceso no autorizado), gestión de claves seguras.

- Concienciación en seguridad informática.- De esto depende por ejemplo el establecimiento de responsabilidad de una persona en el caso de un delito informático, es decir si actúo con plena conciencia y voluntad a pesar de habérsele concientizado sobre el riesgo que implica el hecho de manejar un ordenador con conexión a Internet, el envío de correo electrónico, la navegación por Internet, los virus, los troyanos, las actualizaciones de seguridad, el spam, el phishing, la ingeniería social, etc.

Área Jurídica:

- Teoría General del Derecho. - Debe conocer la finalidad del derecho, que encierra aspectos sustantivos, positivos como instituciones y normas jurídicas; y además aspectos adjetivos o de procedimiento entre los que se incluye la prueba.

- Formación básica en delito informático.**-** Debe entender al delito informático, como todo acto o conducta ilegal e ilícita considerada como criminal; dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro cualquier bien jurídico protegido; delitos tipificados en el respectivo cuerpo normativo.

*- Formación básica en protección de datos y derechos de autor***.**- Hace referencia al derecho consagrado como garantía constitucional por la mayoría de las legislaciones, acerca de la privacidad y confidencialidad de los datos en estrecha relación con la información sensible y la información privada de los usuarios.

En cuanto a los derechos de autor, y la propiedad intelectual cobran mucha importancia, al adoptar nuevas características con la implementación de los medios informáticos, como las copias digitales, los software libre, propietario, de código abierto etc. , sumado a ello los conflictos por los nombres de dominio, y las marcas registradas.

- *Formación básica en convergencia tecnológica*. Hace referencia a la posibilidad del aprovechamiento al máximo de todas las potencialidades tecnológicas que poseen las nuevas plataformas, a través de los mecanismos de banda ancha para Internet, y la convergencia tecnológica de los teléfonos móviles de nuevas generaciones, de la televisión y radio digitales, etc.

- *Formación básica en evidencia digital y pruebas electrónicas*.- Debe conocer que constituye la evidencia digital, electrónica, telemática, como pueden ser recogidas; que técnicas deben aplicarse, cuáles son las herramientas especiales a utilizarse. Debe saber diferenciar la evidencia digital de la evidencia física, y la relación existente entre las mismas. Tener conocimiento sobre los dispositivos en

los que aquella evidencia se encuentra almacenada; los mecanismos, técnicas y procedimientos para su recolección, resguardo y almacenamiento. Y por último la forma como deben presentarse dentro de un proceso para que sea considerada como medio de prueba.

- Análisis comparado de legislaciones e iniciativas internacionales.- Es básico el conocimiento de la legislación nacional e internacional además de los Tratados y Convenios internacionales sobre temas relacionados con la Ley de Comercio Electrónico, Firmas Digitales, Protección de Datos, Delitos Informáticos, Cyber Delitos, Nombres de Dominio, Propiedad Intelectual, Derechos de Autor, Protección al Consumidor, Protocolos de Internet, etc.

Áreas de Criminalística y Ciencias Forenses:

- Cadenas de custodia y control de evidencias.- Este aspecto tiene como fin encaminar correctamente el tipo de investigación, la obtención de indicios y posteriormente los elementos probatorios necesarios para sostener un caso.

Área de Informática Forense:

- *Análisis de datos.*- Hace referencia al análisis de todo el proceso de envío, recepción y almacenamiento de datos, a través de los diferentes medios tecnológicos e informáticos, y de las diversas fases por las que atraviesa, lo que a su vez permite investigar, el momento en el que los mismos, han sido interceptados, modificados, o bloqueados en su acceso y transmisión.

- *Análisis de registros de auditoría y control.*- El área comprende todo el análisis referente a las auditorías de políticas de seguridad contra amenazas y vulnerabilidades con respecto al talento humano asignado a la función de sistemas de información; plataformas de hardware y software implementadas; sistemas de información utilizadas, producidas y desarrolladas; las actividades de procesamiento de datos ejecutadas; **s**ervicios de procesamiento de datos que son contratados con terceros etc.

- *Correlación y análisis y evidencias digitales*.- La evidencia informática puede encontrarse en el hardware (está constituido por todos los componentes físicos de un sistema informático) o en la información (hace referencia a todos los datos, programas almacenados y mensajes de datos trasmitidos usando el sistema informático). Es por ello que el Doctor Santiago Acurio Del Pino**,** en su manual de Procedimiento de Operaciones Estándar denominado "Manual de Manejo de Evidencias Digitales Entornos Informáticos", hace las siguientes consideraciones:

1.- Se debe saber qué tipo de delito se va a investigar: porque no es igual investigar un delito ordinario, que un delito informático.

2.- Es importante diferenciar entre evidencia digital y evidencia electrónica, lo que orientará al investigador forense a identificar las distintas y diversas fuentes de evidencia de manera que permitirá aplicar el método más idóneo para la recolección y mantenimiento de la correspondiente evidencia.

El autor citado clasifica a las fuentes de evidencia digital en tres grupos:

a) Sistemas De Computación.- Este primer grupo está conformado por los computadores personales y todos sus periféricos como teclados, ratones y monitores, las computadoras, etc.

b) Sistemas De Comunicación**.-** Están compuestos por las redes de telecomunicaciones, la comunicación inalámbrica y el Internet.

c) Sistemas Convergentes De Computación**.-** Están formados por los teléfonos, celulares inteligentes, y cualquier otro aparato electrónico que posea convergencia digital[30] y que puede contener evidencia digital.

3- Se debe determinar el rol que cumple el hardware o la información en la investigación de un delito; en razón de que estos en uno casos pueden presentarse como: resultado, instrumento o evidencia del delito.

[30] Designa la posibilidad de consultar el mismo contenido multimedia desde diferentes dispositivos.

Hardware	**Mercancía ilegal o resultado**	Cuando su posesión no está autorizada por la ley; o Sera resultado del delito cuando este es obtenido de forma ilícita.
	Instrumento	Cuando es utilizado como un arma o herramienta, para la comisión del delito, por ejemplo los snifers que sirven para interceptar comunicaciones.
	Evidencia	Es un elemento físico que se constituye como prueba de la comisión de un delito, por ejemplo el scanner que se usa para digitalizar una imagen de pornografía infantil.
Información	**Mercancía ilegal o resultado**	Cuando su posesión no está permitida por la ley. Será resultado del delito del delito cuando su obtención es ilegal.
	instrumento	Cuando es usada como medio para cometer una infracción, por ejemplo los programas de ordenador.
	Evidencia	Las acciones informáticas dejan evidencias del actuar de los sujetos.

- *Procedimientos de control y aseguramiento de evidencias digitales*.- Cuando se va revisar una escena del crimen del tipo informático es necesario tener en cuenta un procedimiento de operaciones estándar (POE), que es el conjunto de pasos o etapas que deben realizarse de forma ordenada al momento de recolectar o examinar la evidencia digital. Entre una de las principales consta el

aseguramiento físico de la escena, cuyo objetivo básico es prevenir el acceso no autorizado de personal a la misma, evitando así la contaminación de la evidencia o su posible alteración.

Una vez asegurada la escena del delito, se debe proceder a recolectar la evidencia existente con los debidos cuidados según se vayan presentando las circunstancias propias de cada caso. Para el efecto, Santiago Acurio Del Pino formula algunas recomendaciones básicas:

a) Dispositivos electrónicos:

- No tomar los objetos sin guantes de hule, podría alterar, encubrir o hacer desaparecer las huellas dactilares existentes en el equipo o en el área donde se encuentra el sistema informático.
- Asegurar los equipos de cualquier tipo de intervención física o electrónica hecha por extraños.
- Si no está encendido, no lo encienda *(para evitar el inicio de cualquier tipo de programa de autoprotección*
- Si es posible verifique el Sistema Operativo, a fin de iniciar la secuencia de apagado, y evitar pérdida de información.
- Si se cree razonablemente que el equipo informático está destruyendo la evidencia, debe desconectarse inmediatamente.
- Si está encendido, no se lo debe apagar inmediatamente *(para evitar la pérdida de información volátil)*
- A falta de un técnico, se debe proceder de la siguiente manera: no usar el equipo informático que está siendo investigado, ni tampoco buscar evidencias sin el entrenamiento adecuado.
- .Si hay un “Mouse” conectado, se debe movérselo cada minuto para evitar que la pantalla se cierre o se bloqueé.

- Si el aparato está conectado a una red, se deberá anotar los números de conexión, (números IP).
- Fotografiar la pantalla, las conexiones y cables
- Evitar el uso de bolsas plásticas, ya que pueden causar una descarga de electricidad estática[31] que puede destruir los datos.
- Coloque etiquetas en los cables para facilitar reconexión posteriormente
- Anote la información de los menús y los archivos activos (sin utilizar el teclado). *Cualquier movimiento del teclado puede borrar información importante.*
- Si hay un disco, un disquete, una cinta, un CD u otro medio de grabación en alguna unidad de disco o grabación; es necesario retirarlo, protéjalo y guárdelo en un contenedor de papel
- Bloquear toda unidad de grabación con una cinta, un disco o un disquete vacío.
- Sellar cada entrada o puerto de información con cinta de evidencia. De igual manera deben sellarse los tornillos del sistema a fin de que no se puedan remover o reemplazar las piezas internas del mismo.
- Mantener el sistema y medios de grabación separados de cualquier tipo de imán, o campo magnético

b) Teléfonos Inalámbricos, Celulares, Cámaras Digitales: Se puede encontrar evidencia potencial contenida en los teléfonos inalámbricos tal como:

Números marcados.

Números guardados en la memoria y en el marcado rápido,

[31] acumulación de un exceso de carga eléctrica en una zona con poca conductividad eléctrica, un aislante, de manera que la acumulación de carga persiste.

Identificador de llamadas, llamadas entrantes y salientes.

Nombres y direcciones.

Número de acceso al correo de voz.

Contraseña del correo de voz.

Números de tarjetas de crédito.

Números de llamadas hechas con tarjeta.

Información de acceso al Internet y al correo electrónico.

Se puede encontrar en la pantalla del aparato Imágenes. Fotos, grabaciones de voz.

c) Regla Del Encendido “On” Y Apagado “Off**”**

- Si el aparato está encendido "ON", este no debe ser apagado "OFF"; caso contrario puede iniciarse el bloqueo del aparato.
- Transcribir toda la información de la pantalla del aparato, y de ser posible tomar una fotografía.
- Evitar el descargue de la batería del aparato, al ser este transportado.
- Sellar todas las entradas y salidas; así como también todos los puntos de conexión o de admisión de tarjetas o dispositivos de memoria; y todos los tornillos para evitar que se puedan retirar o reemplazar piezas internas.
- Buscar y asegurar el conector eléctrico.
- Colocar en una bolsa de FARADAY, (El material de estas bolsas forman un blindaje alrededor de teléfonos celulares, GPS, netbooks, dispositivos bluetooth, laptops, etc., bloqueando toda señal celular, WIFI o de radio. Una vez dentro de la bolsa de faraday, el dispositivo no

podrá volver a conectarse con la red aunque se encuentre encendido, asegurando que el mismo no pueda ser controlado, localizado o bloqueado remotamente).

- Revisar los dispositivos de almacenamiento removibles.
- Si el aparato está apagado "OFF", debe dejárselo en ese estado. Prenderlo puede alterar evidencia al igual que en las computadoras.
- Es necesario que el investigador busque el manual del usuario relacionado con el aparato encontrado.

d) Máquinas de Fax

- Si la máquina de fax es encontrada prendida “ON”, el apagarla causaría la perdida de la memoria de último número marcados así como de los facsímiles[32] guardados.
- Buscar la concordancia entre el número de teléfono asignado a la máquina de fax y la línea de teléfono a la que está conectada.
- Buscar que el encabezado del mensaje y el número impreso coincidan con el del usuario y la línea telefónica.
- Es necesario que el investigador busque el manual del usuario relacionado con el aparato encontrado.

e) Dispositivos de Almacenamiento

Los dispositivos de almacenamiento son usados para guardar información; los cuales se clasifican en:

1.- Dispositivo magnético: como discos duros o los disquetes.

2.- Dispositivos de estado sólido3 o memoria sólida, como: las memorias flash y dispositivos USB.

[32] Es una copia o reproducción casi idéntica de un documento

3.- Dispositivos ópticos, como: discos compactos y DVD.

Frente a este tipo de evidencias se debe actuar de la siguiente manera:

- Recolectar las instrucciones de uso, los manuales y las notas de cada uno de los dispositivos encontrados.
- Documentar todos los pasos al revisar y recolectar los dispositivos de almacenamiento.
- Alejar a los dispositivos de almacenamiento de cualquier magneto[33], radio trasmisores y otros dispositivos potencialmente dañinos[34].

- *Verificación y validación de procedimientos aplicados en la pericia forense*.- La pericia forense, es una ciencia que se ocupa de la utilización de los métodos científicos aplicables a la investigación de todo tipo de delitos. En lo que respecta a la pericia forense informática, utiliza el análisis forense de las evidencias digitales, y de toda información o datos que se guardan en una computadora o sistema informático. Se encarga de la preservación, identificación, extracción, documentación e interpretación de la evidencia digital a ser presentada en una Corte de Justicia, siguiendo los procedimientos técnicos y legales preestablecidos[35].

3.7.- REQUISITOS PARA SER CALIFICADO COMO PERITO

El Consejo de la Judicatura en su página virtual, el 14 de abril del 2014 dio a conocer los requisitos que deben cumplir los aspirantes a ser calificados como peritos en las distintas áreas: requisitos que están acorde a las exigencias del COIP.

- Ser mayor de edad y estar en ejercicio de su derecho de participación.

[33] Generador eléctrico en el que el inductor está formado por uno o más imanes permanentes

[34] "Manual de Manejo de Evidencias Digitales y Entornos Informáticos". Dr. Santiago Acurio Del Pino. Fecha de consulta: abril 20, 2015 desde < http://www.oas.org/juridico/english/cyb_pan_manual.pdf >

[35] Reflexiones Técnicas y Jurídicas de la Prueba Pericial Informática" (2008). Doctor Edgar Francisco Cevallos Gualpa (p. 20-36)

- Conocer y ser experta (o) en la profesión, arte, oficio, o actividad para la cual solicite calificarse.

- Las y los profesionales, así como también los expertos, deben tener al menos dos años de graduadas (os), o al menos dos años de práctica y experiencia a la fecha de la solicitud de la calificación en su especialidad.

- Los postulantes también podrán presentar hasta 10 informes periciales realizados en los últimos dos años para justificar su conocimiento, los cuales serán analizados por el Consejo de la Judicatura**.**

- No estar inmersos en las inhabilidades o prohibiciones previstas en la Ley y en el Reglamento del Sistema Pericial Integral del Ecuador.

Para que uno o varios peritos intervengan en un proceso, será necesaria la petición de parte interesada, ante la cual el Juez o el Fiscal designarán al perito, de acuerdo a la especialidad requerida. Ésta selección se realizará mediante el sistema informático pericial de la Función Judicial, el que escogerá de forma aleatoria al perito entre los calificados de la circunscripción territorial donde se genera el pedido.

Por otro lado el Código Orgánico Integral Penal en el artículo 511, plasma las obligaciones que debe cumplir un perito debidamente designado; a saber estos son los siguientes:

1. Ser profesionales expertos en el área, especialistas titulados o con conocimientos, experiencia o experticia en la materia y especialidad, acreditados por el Consejo de la Judicatura.

2. Desempeñar su función de manera obligatoria, para lo cual la o el perito será designado y notificado con el cargo.

3. La persona designada deberá excusarse si se halla en alguna de las causales establecidas en este Código para las o los juzgadores.

4. Las o los peritos no podrán ser recusados, sin embargo el informe no tendrá valor alguno si el perito que lo presenta, tiene motivo de inhabilidad o excusa, debidamente comprobada.

5. Presentar dentro del plazo señalado sus informes, aclarar o ampliar los mismos a pedido de los sujetos procesales.

6. El informe pericial deberá contener como mínimo el lugar y fecha de realización del peritaje, identificación del perito, descripción y estado de la persona u objeto peritado, la técnica utilizada, la fundamentación científica, ilustraciones gráficas cuando corresponda, las conclusiones y la firma.

7. Comparecer a la audiencia de juicio y sustentar de manera oral sus informes y contestar los interrogatorios de las partes, para lo cual podrán emplear cualquier medio.

8. El Consejo de la Judicatura organizará el sistema pericial a nivel nacional, el monto que se cobre por estas diligencias judiciales o procesales, podrán ser canceladas por el Consejo de la Judicatura.

De no existir persona acreditada como perito en determinadas áreas, se deberá contar con quien tenga conocimiento, especialidad, experticia o título que acredite su capacidad para desarrollar el peritaje.

Para los casos de mala práctica profesional la o el fiscal solicitará una terna de profesionales con la especialidad correspondiente al organismo rector de la materia.

Cuando en la investigación intervengan peritos internacionales, sus informes podrán ser incorporados como prueba, a través de testimonios anticipados o podrán ser receptados mediante video conferencias de acuerdo a las reglas del presente Código.

3.8 REQUISITOS DEL INFORME PERICIAL.

El artículo 21 del Reglamento del Sistema Especializado Integral de Investigación de Medicina Legal y Ciencias Forenses establece los requisitos que debe cumplir el informe pericial.

1.- Parte de antecedentes.- En donde se debe delimitar el objeto del peritaje, esto es, se debe especificar claramente el tema sobre el que informará en base a lo ordenado por la jueza o el juez, la o el fiscal y/o lo solicitado por las partes procesales.

2.- Parte de consideraciones técnicas o metodológicas a aplicarse.- En donde se debe explicar claramente, como aplican sus conocimientos especializados de una profesión, arte u oficio, al caso o encargo materia de la pericia.

3.- Parte de conclusiones.- Luego de las consideraciones técnicas, se procederá a emitir la opinión técnica, o conclusiones de la aplicación de los conocimientos especializados sobre el caso concreto analizado. La conclusión será clara y directa en relación a la pericia realizada. Se prohíbe todo tipo de juicios ambiguos, así como también cualquier tipo de juicio de valor sobre la actuación de las partes en el informe técnico.

4.- Parte de inclusión de documento de respaldo, anexos, o explicación de criterios técnicos.- Deberá sustentar sus conclusiones ya sea con documentos y objetos de respaldo (Fotos, laminas demostrativas, copias certificadas de documentos, grabaciones de audio y video, etc.) y/o con la explicación clara de cuál es el sustento técnico o científico para obtener un resultado o conclusión especifica. Se debe exponer claramente las razones especializadas del perito para llegar a la conclusión correspondiente. No se cumplirá con este requisito si no se sustenta la conclusión con documentos, objetos, o con la explicación técnica y científica exigida.

El artículo en mención culmina manifestando que a más de los requisitos establecidos, el perito deberá hacer constar en el informe pericial cualquier otro requisito exigido por la ley correspondiente; u otro informe que considere relevante.

3.9.- CONCLUSIONES.

Es innegable que la comunicación, es un elemento indispensable para el desarrollo del ser humano; es por ello que la humanidad siempre se ha preocupado en buscar y desarrollar los mecanismos idóneos para lograr una ágil y eficiente comunicación, pasando desde los simples sonidos hasta llegar a la comunicación a través de la Red, cuyo desarrollo no se detiene; pues se siguen creando diversas herramientas para su perfeccionamiento, generando mayor comodidad, rapidez en la obtención de información, e incluso calidad de la misma.

Sin embargo este gran avance tecnológico presenta sus ventajas y desventajas, por la enorme variedad de servicios que presta, que son aprovechados por ciertos sujetos como una herramienta más para causar algún tipo de daño ya sea por mera diversión, desafío, o por un simple interés personal o a favor de un tercero, violentando derechos fundamentales reconocidos y garantizados en la Constitución y tratados Internacionales, así como derechos de autor, derecho a la intimidad privacidad, seguridad del Estado etc.

Ante tal amenaza, al igual que otros estados del mundo, nuestra legislación ecuatoriana, ha considerado oportuno atender las nuevas necesidades exigidas por la sociedad, tipificando en el Código Orgánico Integral Penal ciertas conductas practicadas por medios informáticos, telemáticos o electrónicos como dolosas.

Aun con los distintos cuerpos normativos que regulen conductas de esta índole, no es suficiente para combatir la *Cyberdelincuencia*; en realidad se requiere de la colaboración de todos los ciudadanos para este fin, creando una concientización a cerca del uso de los distintos servicios que brinda la Red, generando una cultura informática.

Además considero que en las Facultades de Jurisprudencia se bebe empezar a impartir la cátedra de Derecho Informático, o por lo menos dedicarle un espacio a esta rama del Derecho, a fin de que los estudiantes de esta carrera se familiaricen con esa termología técnica y compleja propia del campo informático, lo que les

facilitara una mejor comprensión y análisis de los cuerpos normativos que regulan la actividad informática.

Pues no podemos negar la realidad por la que la sociedad ecuatoriana atraviesa en la actualidad, cada vez su seguridad se ve amenazada en el uso del sistema informático; tanto así que expertos advierten que en el año 2014 se ha incrementado el índice de delitos a través de los medios informáticos, y es posible que el número de víctimas sea mayor por el desarrollo económico que experimenta el país. Este tipo de delitos son cometidos desde los países de Colombia y Perú, atacando preferentemente a aquellas personas que mantienen alguna cuneta en las distintas entidades financieras.

Mas el seguimiento de estos delitos se torna complejo, por la misma facilidad que brinda la misma informática para borrar toda posible evidencia; debiendo sumar a esta desventaja la existencia mínima de peritos informáticos a nivel del país; a manera de ejemplo me permito manifestar que revisado el listado de peritos calificados por el Consejo de la Judicatura del Azuay, en la presente fecha se encuentra registrados tan solo cuatro peritos de esta categoría.

BIBLIOGRAFÍA

Base doctrinaria

ALBÁN GÓMEZ. **ERNESTO** "Manual de Derecho Penal Ecuatoriano". Edicioneslegales S.A. Quito 2012.

ANDRADE JARA JAIME EDMUNDO, "La Internet Como Nueva Tecnología De La Información, La Comunicación Y La Delincuencia Informática". Universidad de Cuenca. Cuenca. 2010.

ARAUJO ASTUDILLO FLAVIO NORBERTO; **"La Prueba Y Su Incorporación Al Proceso En El Juicio Penal**" Universidad de Cuenca; Cuenca; 2010.

CEDILLO DÍAZ MARCIA FERNANDA. "El Documento Electrónico: Su Importancia, Trascendencia y Valor Probatorio en la Legislación Ecuatoriana". 2010.

CEVALLOS GUALPA EDGAR FRANCISCO. "Reflexiones Técnicas y Jurídicas de la Prueba Pericial Informática". Universidad de Cuenca, 2008.

DE CEA JIMÉNEZ ANDREA;´´ Los delitos en las redes sociales: Aproximación a su estudio y clasificación ´´ Universidad de Salamanca; Salamanca; 2012.

HERRERA ÁVILA CRISTIAN;´´ Hacia una Correcta Hermenéutica Penal: Delitos Informáticos vs. Delitos Electrónicos ´´ Universidad de Cuenca; Cuenca; 2010.

PAEZ RIVADENEIRA JUAN JOSE; "Reflexiones Técnicas Y Jurídicas De La Prueba Pericial Informática ´´ Universidad de Cuenca; Cuenca; 2008.

URETA ARREAGA LAURA; 'Retos A Superar En La Administración De Justicia Ante Los Delitos Informativos En El Ecuador'´; Escuela Superior Politécnica del Litoral; Guayaquil; 2009.

VACA ANDRADE RICARDO. "Manual De Derecho Procesal Penal, tomo II" Editorial Corporación de Estudios y Publicaciones- Quito de 2009.

Base Legal

CÓDIGO DE LA NIÑEZ Y ADOLESCENCIA, del arco ediciones, Cuenca, 2014.

CÓDIGO ORGÁNICO INTEGRAL PENAL, del arco ediciones, Cuenca, 2014.

CONSTITUCION DE LA REPUBLICA DEL ECUADOR, del arco ediciones, Cuenca, 2014.

LEY ORGÁNICA DE COMUNICACION, del arco ediciones, Cuenca, 2014.

LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. Del arco ediciones, Cuenca, 2014.

LEYDE PROPIEDAD INTELECTUAL, del arco ediciones, Cuenca, 2014.

REGLAMENTO GENERAL A LA LEY ORGÁNICA DE COMUNICACION, del arco ediciones, Cuenca, 2014.

Sitios web

ACURIO DEL PINO SANTIAGO "Delitos Informáticos: Generalidades." Recuperado de < http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf >

ANDRÉS ABAD. (2013) “10 Características de lo Bueno y lo Malo." Recuperado de <http://fgjhghgh.blogspot.com/>

BLIGOO. (10 de enero del 2010) “Redes Sociales”. Recuperado de <http://redessociales.bligoo.com.mx/content/view/1534653/VentajasyDesventajas-de-las-redes-sociales.html#.VLbvRNKUf5k>

CLAUDIO HERNÁNDEZ. (16 de noviembre del 2010)“Historia y evolución de Hackers y Crackers”. Recuperado de < http://www.monografias.com/trabajos82/historia-evolucion-hackers crackers/historia-evolucion-hackers-crackers2.shtml#ixzz3StOcRb4r.>

D. BOYD Y **B. ELLISON**. “Redes Sociales en internet." Recuperado de <http://www.edukanda.es/mediatecaweb/data/zip/971/page_05.htm>

DEL PINO SANTIAGO ACURIO. “Manual de Manejo de Evidencias Digitales y Entornos Informáticos”. (8 de diciembre del 2009) Recuperado de <http://www.oas.org/juridico/english/cyb_pan_manual.pdf>

EL UNIVERSO NOTICIAS. (17 de noviembre del 20014) “Delitos Informáticos en la Web podrían aumentar en el Ecuador”. Recuperado de <http://www.eluniverso.com/noticias/2014/11/17/nota/4226966/ataques-web-podrian-aumentar.>

ELVIS J BELIALDIAZMARQUIS (26 de abril del 2011) “Redes Sociales." *redes sociales*. Recuperado de <http://www.monografias.com/trabajos84/redes-sociales/redes-sociales.shtml#caracteria>

ENCICLOPEDIA JURÍDICA. (2014) “Fuentes de Prueba”. Recuperado de <.http://www.enciclopedia-juridica.biz14.com/d/fuente-de-prueba/fuente-de-prueba.htm>

INGRID CHAVES Y YANCI VILLALO. (8 de septiembre de 2008). "Hackers y Crackers". Recuperado de <http://hackersycrackers-yi.blogspot.com/.>

ISABEL PONCE. (2012) "Historia de las redes sociales." Recuperado de <http://recursostic.educacion.es/observatorio/web/es/internet/web-20/1043-redes-sociales?start=2>(

I**NSTITUTO DE INVESTIGACIONES JURÍDICAS DE LA UNAM** (2011) "Los Medios de Prueba en Materia Penal". Recuperado de <http://www.juridicas.unam.mx/publica/rev/boletin/cont/83/art/art8.htm.>

MASTER'S DEGREE ONLINE "Cursos de Redes Sociales para padres."*Características Generales de las redes sociales"*. Recuperado de <http://www.adrformacion.com/cursos/redsocp/leccion1/tutorial3.html>

PABLO FERNÁNDEZ BURGUEÑO. "Blog de Derecho." Clasificación de Redes Sociales. (2009) Recuperado de <http://www.pabloburgueno.com/2009/03/clasificacion-de-redes-sociales/>

WIKIPEDIA, LA ENCICLOPEDIA LIBRE. (diciembre, 2014) "Hacker (seguridad informática)". Recuperado de <http://es.wikipedia.org/w/index.php?title=Hacker_(seguridad_inform%C3%A1tica)&oldid=80132007.>

WIKIPEDIA-LA ENCICLOPEDIA LIBRE (diciembre, 2014) "Servicio de Red Social." Recuperado de <http://es.wikipedia.org/wiki/Servicio_de_red_social#Riesgos_en_el_uso_de_las_redes_sociales>

WIKIPEDIA. (Enero del 2015)" Electrónica.". Recuperado de <http://es.wikipedia.org/wiki/Electr%C3%B3nica>

WIKIPEDIA. (enero del 2015) "Imformática." Recuperado de http://es.wikipedia.org/wiki/Inform%C3%A1tica >