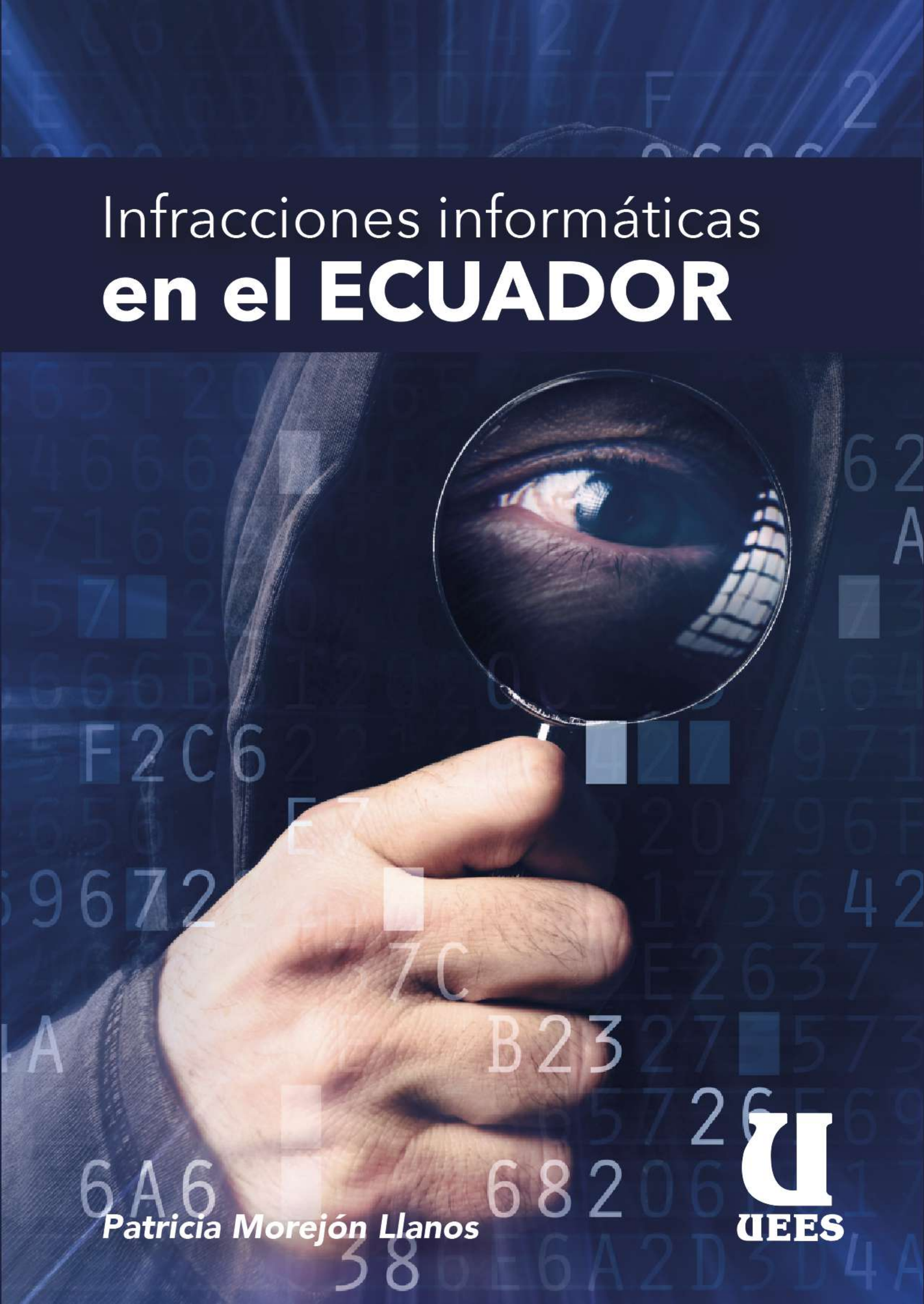
Infracciones informáticas en el ECUADOR



Patricia Morejón Llanos

UEES

UEES
UNIVERSIDAD ESPÍRITU SANTO

Infracciones Informáticas en el Ecuador

Patricia Morejón Llanos
2018

Universidad Espíritu Santo – Ecuador

Autor:
Patricia Morejón Llanos

Editores:
Fernando Espinoza Fuentes
Alexandra Portalanza Chavarría

Asistente editorial:
Natascha Ortiz Yánez

Cita:
(Morejón, 2018)

Referencia Bibliográfica:
Morejón P. (2018) Infracciones Informáticas en el Ecuador. Universidad Espíritu Santo, Samborondón - Ecuador

Portada:
Centro de Investigaciones, Universidad Espíritu Santo.

Diagramación e impresión:
Impgraficorp S.A.

ISBN-E:
978-9978-25-225-3

DEDICATORIA

A Dios, por estar conmigo en cada paso que doy,
por fortalecer mi corazón e iluminar mi mente.

A mis hijas, porque son mi luz, mi gran felicidad
y mi mayor regocijo.

A mis alumnos de quienes recibo un aprendizaje diario,
quienes han causado a mi corazón alegría descomunal,
contagiándome ser parte de su mundo incomparable,
extraordinario y sublime.

"Porque todas las cosas proceden de Él,
y existen por Él y para Él.
¡A Él sea la gloria por siempre! Amén".
(Romanos11:36)

Índice

PRÓLOGO

Los libros han sido, y serán los fieles amigos de los científicos, filósofos y estudiantes. Desde la curiosidad natural que tenemos los seres humanos para aprender y entender cómo funcionan las cosas, hasta las más complejas obras han sido creadas, entre otros orígenes, gracias a la armonía que resulta de la conjugación de una información con otra. Así hemos dado a luz una nueva definición o teoría que, a su vez, origina otras. Es una dinámica sin fin. Cuando se escribe un libro el autor se adentra a protagonizar esa dinámica. Con agrado escribo este prólogo que intenta recoger la visión de la autora.

La justicia es un anhelo de todas las sociedades. ¿Cómo lograrla? Pues no siempre contamos con los elementos para identificar una infracción, ni tampoco para llegar al final de un exitoso proceso.

El Derecho Penal es una de las ciencias del Derecho que intenta progresar al son de la modernidad. No siempre lo alcanza. Y es allí donde importa mucho el detenerse, observar lo sucedido, anotar lo que hace falta y seguir avanzando. Con esa información en la mano es cuando se puede empujar a esta ciencia del derecho, a identificar al infractor, determinar el modo y castigarlo, teniendo en cuenta el derecho a la igualdad ante la ley y el debido proceso.

La autora nos brinda este libro para mostrarnos la realidad compleja de un tipo especial de infracciones, los llamados delitos informáticos.

Cuando el derecho a la vida, a la propiedad y otros, es dañado con las herramientas que nos trajo la tecnología informática, contamos gracias este libro, con un análisis que nos permitirá avanzar en ese citado anhelo de la justicia.

La autora nos recuerda las características de los delitos y el impacto internacional que tienen los delitos informáticos. Sabemos que no resulta difícil que la persona que penetre en nuestras cuentas, de correo o financieras, necesariamente no reside cerca de nosotros, es más, puede que no lo conozcamos, ni él a nosotros, pues pudo ser contratado para cometer la infracción o solo parte de ella. Por ejemplo, espiar algo y entregar lo espiado a otra persona. El autor o autores pueden estar en otro continente y cometer la infracción, solos o en conjunto, mediante un solo acto o en sucesivos.

Otro terrible ejemplo, es aquel que involucra a quien desde muy lejos solicita fotos y videos pornográficos y otros que aquí, en nuestro país, los filme, grabe y envíe a otro, quien a su vez los comercia como pornografía. Abundan titulares de medios de comunicación que nos han informado de

importantes cantidades de dinero sustraídas de modo virtual. Alguien pudo acceder a lo supuestamente impenetrable.

El secreto y las claves en la comunicación no son nuevas en la historia de la humanidad, existieron siempre, así como siempre existió quien pudo acceder a lo que nadie podía saber y claves que abrían tesoros. Lo nuevo es el conjunto de elementos que la tecnología tiene y que nos obliga a reflexionar sobre dónde se cometió la infracción, quién y cómo; sin jurisdicción y tipicidad no habrá juicio.

Lo nuevo, en todo caso, está representado por la estructura de esas violaciones a nuestros derechos que los agiliza y, en algunos casos logra invisibilidad a los infractores.

Dentro de ese contexto, la autora nos brinda un camino a seguir y unas propuestas por realizar. Gentilmente la autora nos lleva a muchas reflexiones para poder comprender en su integridad lo que significan los delitos informáticos, los obstáculos procesales y sobretodo la exigencia que debe tener la pericia y la evidencia.

La experiencia como Agente Fiscal y hoy como Fiscal Provincial, su dedicación a los estudios que han caracterizado su aporte en áreas especializadas, también son un elemento importante en la redacción de los capítulos de este libro. Pues bien sabemos de la sabiduría que se genera cuando se estudia y se practica a la vez, lo cual es incalculable.

La cercanía con los protagonistas, la coordinación con los peritos, la colaboración que brindan resoluciones y sentencias especiales le brinda a la autora la autoridad necesaria para presentar esta obra.

Siento agradecimiento por haber sido elegida para escribir este prólogo y cómo justa contraprestación sugiero y recomiendo la lectura del mismo. Estoy segura que aportará en grado valioso al crecimiento profesional de quienes estamos llamados a trabajar por la justicia y provocar que el Derecho abrace la realidad de nuestras sociedades y que nos deje la seguridad jurídica que necesitamos.

María Josefa Coronel

Infracciones Informáticas
En El Código Orgánico Integral Penal

Introducción

Estudiar en el Instituto Normal No. 5, en mi natal San Miguel de Bolívar, era la "opción" más conveniente para cumplir mi anhelado sueño: ¡ser abogada!, razón por la que consentí no con mucho agrado, pero si resuelta a continuar con mis ideales. Lo que nunca sospeché es que en los años posteriores de estudio, me enamore de la carrera de docente, tuve el alto honor de ser alumna-maestra del afamado, temido y amado maestro Cervantes Ángulo, quien en el transcurso de las prácticas pre-profesionales me enseñó, no solo a pararme frente al alumno en punta de un triángulo para poder mirar a todos; que error de concepto no se debe dejar pasar, que no podemos llegar a clases a improvisar, entre mil y un enseñanzas que perennemente están en mi memoria y corazón; y ya en el ejercicio profesional de profesora de educación primaria y universitaria por 27 años, aprendí que el maestro no solo enseña y que el alumno aprende, sino inverso, los alumnos enseñan, mejoran, corrigen y que cada uno transitan por nuestras vidas dejando vestigios de amor entrañable, pues sus fisonomías, necesidades, gestos, entusiasmo, se hacen nuestras. Cada grupo de alumnos ha comprimido mi corazón de alegría descomunal, me han contagiado de su mundo diferente, maravilloso y único. Amo enseñar, porque entendí que ser maestro no es una "elección" como pensé, sino una vocación.

Y es justamente por esta aptitud y apego, que decidí recoger en el presente libro, las experiencias como docente de Derecho Informático, que ha merecido que la mayoría de los alumnos universitarios me identifiquen como tal, por lo tanto, el mismo es realizado fundamentalmente con la obtención de información de bibliografía relacionada con el tema, tratando de copar todos los escenarios posibles y el poco conocimiento adquirido en los años de cátedra impartidos en las Universidades Espíritu Santo y Católica Santiago de Guayaquil, así como Fiscal de la Unidad de Delitos Informáticos y Telecomunicaciones en la Fiscalía Provincial del Guayas.

En el texto intento establecer las diferentes particularidades dentro de la gama de los mencionados delitos informáticos, explicando términos usuales y básicos con el fin de contribuir a los lectores a la mejor comprensión de aquellas figuras delictivas mediante la representación pictórica, en tanto se examina la variedad y analogía en la normativa jurídica penal anterior, como la del Código Orgánico Integral Penal vigente, como respuesta a la inaplazable y urgente revisión del nuevo sistema jurídico en la que surgieron tipos penales ignorados por el Código Penal anterior, que era arcaico, inconcluso y modificado en más de cuatro décadas, desde octubre de 1971.

Entre las nuevas conductas penalmente relevantes se encuentran las citadas infracciones informáticas, que de alguna manera vienen adaptarse a las normas internacionales, y por ello es importante diferenciarlas de las tradicionales, sobre todo porque las mismas se cometen mediante un ordenador, en el ciberespacio, siendo necesario por parte de la ciudadanía y autoridades, una acción eficaz para evitar la impunidad, tanto en la esfera nacional como internacional, en la que los delincuentes informáticos utilizan nuevos medios o instrumentos.

Anhelo llevar al lector a una observación breve de las nuevas infracciones de carácter informático, en las que se ubicará el bien jurídico protegido y características propias de las mismas, y que llegue a convertirse en material de consulta y de apoyo perceptible y didáctico, pudiendo inclusive de ser el caso, aplicarse en los ámbitos de nuestra vida diaria, ya sea de forma directa o indirecta, debido a las necesidades actuales de la información, que reclaman conocimiento y estudio inmediato.

Finalmente, es necesario indicar que las concepciones, opiniones y tendencias planteadas en el texto, deben ser reforzadas y consolidadas con las lecturas de soporte vistas en cada uno de los temas, que han sido resguardadas por distintas fuentes de información para mejorar los conocimientos y atesorar la perspectiva, no solo en nuestro acervo jurídico sustantivo, sino también adjetivo.

Capítulo I

Infracciones Penales

Breves Consideraciones

En nuestro país, en el Código Penal Ecuatoriano vigente hasta el 10 de agosto del 2014, el Art. 10 definía a las infracciones de la siguiente forma:

"Son infracciones los actos imputables sancionados por las leyes penales, y se dividen en delitos y contravenciones, según la naturaleza de la pena peculiar"; a partir de la fecha antes referida con el nacimiento del actual Código Orgánico Integral Penal, el artículo18 las define como *"actos típicos, antijurídicos y culpables cuya sanción se encuentra prevista en este Código*".

Conservando en el artículo posterior (19 COIP), la estructura bipartita compuesta de delitos y contravenciones; lo que implica enfocarnos en los tres elementos asociados entre sí, como aquellos que establecen una conducta penalmente relevante y por consiguiente, alcanzan la consideración de delito; siendo ineludible precedentemente a desarrollar el tema central, tener claro qué es un delito informático.

En el mundo inconstante encontramos multiplicidad de definiciones de delito, con variedad de doctrinas y pensamientos sobre el mismo; existen grandes juristas con diferentes corrientes o razonamientos sobre su concepto y elementos, lo que hace improbable consolidar un concepto universal de DELITO; juristas de disímiles enfoques ideológicos y teóricos dan un concepto del mismo, apoyados en estudios serios y originales, solo por mencionar referiré algunos de ellos.

Francisco Carrara, uno de los grandes representantes de la Escuela Clásica, consideró que el delito no es un ente de hecho, sino un ente jurídico, cuya esencia debe consistir en la violación de un derecho; mantuvo que el derecho es connatural en el hombre, porque Dios lo dio a la humanidad desde su creación para que pueda cumplir sus deberes en la vida terrenal….." (Carrara, 1944).

Como reacción o rivalidad a la Escuela Clásica, Cesare Lombroso, Enrico Ferri y Rafael Garófalo, instituyen la célebre Escuela Positiva del siglo XIX,

la que establece que en la naturaleza debe estudiarse al delito como un ente real, actual y existente.

Ernst Von Belin, definió al delito como la acción, típica, antijurídica y culpable sometida a una adecuada sanción penal y que llena las condiciones objetivas de penalidad.

Edmundo Mezger por su parte dijo, que el delito es la acción típicamente antijurídica, personalmente imputable y conminada a una pena.

Pellegrino Rossi precisa al delito como la infracción de un deber exigible por un cometido a la sociedad o a los particulares.

Etimológicamente, la palabra "delito" se deriva del latín DELINQUERE, que significa: desviarse, resbalar o abandonar el camino señalado.

Instauramos entonces que sin un concepto universal de delito, tampoco existe generalidad de tipos penales en los países del mundo, mucho menos legislaciones o normas penales puntuales; cada país ajusta las conductas a un tipo penal existente, y si no concurre en el catálogo de delitos, se lo hace mediante los organismos legales correspondientes para poder sancionar, pues algunos delitos dejan de ser punibles y otros van surgiendo en la sociedad de forma paulatina, y en muchos casos surgen con la aparición de la modernización o globalización, como el caso preciso de los delitos ambientales, tributarios, informáticos entre otros.

ACCIÓN es la conducta manifestada, sometida o flexible a la voluntad del ser humano, por tanto, solo el hombre es capaz de ejecutar una acción. Esta corriente nos dirige a la certeza de que los pensamientos o actitudes internas del ser humano, como la intención no manifestada en su forma física, no son penados o sancionados como conductas antijurídicas o en contra de la ley.

Los tipos penales son las normas constantes en el Código Orgánico Integral Penal, y por tanto, la **TÍPICIDAD** viene a constituirse en la acción de adecuar un determinado tipo penal a la conducta del ser humano antes referida, dicho de otra manera, es el ajuste o encuadramiento de un hecho en relación a lo que determina la ley. Por otra parte, la tipicidad tiene una relación bastante estrecha con principios como el de legalidad que en el Código Orgánico

Integral Penal se encuentra en el artículo 5, #1 el cual menciona que "no hay infracción penal, pena, ni proceso penal sin ley anterior al hecho", también conocido con el aforismo latino "*nulum crimen, nulum pena, sine lege"*, no existe crimen, ni pena, sin ley previa, dado por Anselm Von Feuerbach, quien no perteneció a ninguna escuela, como tampoco hizo alarde de una equivalencia de opiniones, solo escribió de forma corriente bajo el dominio de la filosofía idealista de Kant, preocupándose por enunciar una concepción del delito y dar un cimiento eficaz a la pena y a la responsabilidad penal y continúa, siendo aplicado en el moderno Derecho Penal y continúa de igual forma, en nuestro actual ordenamiento jurídico penal. Es importante mencionar que una conducta no puede ser considerada como penalmente relevante, ni se le podrán aplicar sanciones a la persona que realice determinada acción, si previo a su cometimiento, esta acción no fue establecida como un tipo penal, es decir, una conducta no puede sancionarse como delito, sin antes ser establecido en la ley como tal, que es lo que describe lo antes referido.

El principio de irretroactividad de la ley, también tiene relación con la tipicidad, en el sentido de que no basta que una conducta esté tipificada en la ley para que se puedan aplicar las sanciones correspondientes a la infracción, para ello es necesario que además, la acción se encuadre con un tipo penal, y que este tipo penal haya existido con anterioridad al cometimiento de la acción.

Esta acción debe ser **ANTIJURIDICA,** prohibida, contraria a derecho, desaprobada, un juicio de desvalor que recae sobre un hecho. Sin olvidar que la antijuridicidad tiene excluyentes, eximentes o causas de justificación que también provienen de la misma sistematización jurídico-penal, es decir, una conducta está prohibida pero si hay causas de justificación está consentido. La acción es típica pero no antijurídica. El ejemplo más tradicional es el homicidio cometido en legítima defensa.

La acción típica y antijurídica ha de ser **CULPABLE,** es decir, atribuir el incumplimiento de la norma para atribuirle o hacerle responsable del mismo, ya sea en grado de autor, o cómplice; obviamente que dicha culpabilidad o responsabilidad deberá probarse, y sobre todo no deberá existir ausencia de exculpación.

Con estas puntualizaciones, podemos caminar al análisis sobre qué es un delito informático, pues no cabe duda, que los elementos del delito en forma general, están inmersos en este tipo de infracciones, ya que lo único que cambia son las características, las herramientas o la dirección del sujeto activo al quebrantar la norma.

Como podemos apreciar en la gráfica, los delitos informáticos tiene una implicación internacional, de tal manera que el delincuente puede estar en el continente americano y mediante comunicación inalámbrica, o por medios de transmisión física, puede cruzar con la ayuda de modulación de ondas electromagnéticas a través de servicios de comunicaciones públicas y privadas, y llegar a otro continente y alcanzar a su víctima, convirtiéndose las infracciones informáticas, en un delito transnacional transgredido por un grupo criminal organizado y estructurado, para obtener beneficio propio o de terceros, mediante acciones peligrosas que tienen un dominio evidente fuera del ámbito nacional, que requieren del auxilio universal, para un seguro seguimiento estén o no, en convenios internacionales, como sucede en nuestro país, que aún no somos suscriptores de ninguno.

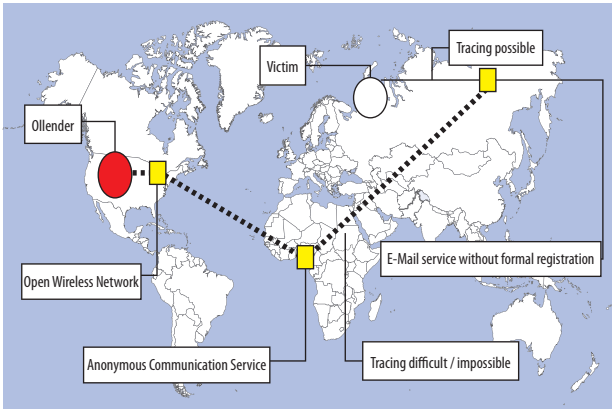


Figura 1.

Reglas de Competencia. Principio de Ubicuidad.

En los delitos informáticos, es tradicional que se planteen problemas a la hora de determinar el lugar de la comisión de los mismos, pues proceden de lugares inicialmente desconocidos, ejecutados a través de ordenadores

o cualquier medio electrónico, que cuente con servicio de internet y que en ciertos casos pueden ocasionar efectos delictivos en distintos lugares, es decir, que la acción puede realizarse en una zona geográfica distinta de la que se logre obtener consecuencias de violaciones jurídicas.

Si bien es cierto, que a través de la informática forense se puede determinar la dirección IP, acrónimo de Internet Protocol, que son series de números que identifican un dispositivo de conexión de cualquier computadora dentro de una red, es imposible determinar irrefutablemente quien es el usuario, y si bien, en nuestro país como en otros, la dirección IP sean fijas o dinámicas, son considerados datos de carácter sumamente particular, no es menos cierto que surge la pregunta ¿cómo sustentamos una acusación punible en estos casos?; la respuesta en Ecuador se respaldaba en el principio de territorialidad, que se sostiene en el razonamiento de la soberanía del Estado que representa a la ley penal, adaptable a los hechos punibles ejecutados dentro del territorio del Estado, sin miramiento de la ciudadanía del autor y los participantes, siendo en nuestra legislación sumamente extenso, pues se contemplaba en el Art. 21 del Código de Procedimiento Penal, numeral 8, las conocidas REGLAS DE COMPETENCIA TERRITORIAL que dice: *"Cuando la infracción hubiese sido preparada o comenzada en un lugar y consumada en otro, el conocimiento de la causa corresponderá al juez de garantías penales de este último",* y que vislumbra ahora sin mucha variación, como REGLAS DE COMPETENCIA, en el artículo 404 del Código Orgánico Integral Penal, numeral 8 de la siguiente manera *"cuando la infracción hubiese sido preparada o comenzada en un lugar y consumada en otro, el conocimiento de la causa corresponderá al juez de garantías penales de este último",* por tanto, si se determina que en nuestro país se consumó el delito, a pesar de ser ejecutado fuera de territorio nacional, serán los jueces del lugar donde se consuma el competente, para resolver el mismo, que es aplicable como parte de la Función Judicial a los Fiscales investigadores.

Esta regla de competencia territorial, intrínsecamente está ligada con el principio de justicia universal o principio de universalidad, que fundamenta el estudio del derecho de cualquier Estado, independientemente del lugar de comisión y de la nacionalidad del autor, cimentado en el criterio de resguardar los bienes supranacionales que concierne a todos los Estados en común,

lo que es afinado por el principio o teoría de la ubicuidad diseñada por Karl Binding, en su positivismo jurídico, cuando señalaba que el lugar de comisión es tanto el de la acción, como del resultado, y que el fundamento de esta teoría está en la unidad que constituyen la acción y el resultado, lo que impediría su consideración aislada, que concibe cometido el delito en todos los lugares en los que ha tenido lugar, tanto la iniciación como el resultado, es decir, la competencia de investigar y juzgar, será a la autoridad del lugar donde se producen los efectos como se mencionaron, concordante con lo establecido en el Artículo 14 del COIP, del ámbito espacial de aplicación, numeral 2, que indica: "*Las infracciones cometidas fuera del territorio ecuatoriano, en los siguientes casos: a) Cuando la infracción produzca efectos en el Ecuador o en los lugares sometidos a su jurisdicción…".*

Se explica con claridad los conceptos relativos al principio de jurisdicción universal y al de ubicuidad:

a) Principio de jurisdicción universal.- Llamado también de justicia universal, conlleva la ampliación del sistema de excepciones a la territorialidad de la ley penal, aplicada a ciertos delitos cuyo bien jurídico protegido obliga a esta persecución forzada fuera del ámbito del territorio nacional, para que los responsables del ciberdelito no queden en la impunidad. Partiendo de la llamada "teoría de la acción", habría que considerar que el lugar de origen del delito informático es aquel en que se encuentra ubicado el servidor informático, desde el cual, el responsable del ciberdelito lanza el ataque a través de las redes informáticas, o bien, es el espacio físico o virtual en el que almacena datos o información obtenida ilícitamente. En cambio, partiendo de la denominada "teoría del resultado", se considera que cualquier estado puede invocar su jurisdicción para perseguir el delito informático originado en otro estado, si se establece la existencia de elementos de convicción del resultado del ciberdelito, en su territorio.

b) Principio de ubicuidad.- Respecto de esta tesis, que goza de mayor aceptación doctrinaria en la actualidad, debemos decir que para la misma no es relevante el lugar de origen o del resultado del delito informático. Existe ubicuidad cuando la jurisdicción de un estado actúa tanto en el caso de que la acción delictiva se lleve a cabo en su territorio y el resultado se

produjo fuera de él, tanto como si el ilícito se originó fuera de su territorio y tuvo su resultado dentro de su territorio. El delito se entenderá cometido en cualquiera de los lugares en que se despliega la actividad del autor del hecho o donde se manifiesta el resultado típico, que de formar parte del territorio nacional permitirán la competencia de éste. Solo la atención al lugar en que se despliega la acción y al lugar en que se ejecuta el resultado, pueden aportar los elementos necesarios para el correcto enjuiciamiento del hecho (énfasis añadido).

Situada de forma incuestionable la regla de competencia, se requiere comprender con mayor detalle, que los medios electrónicos son todos los instrumentos establecidos para adquirir información a través de redes de forma computarizada y eficaz, tales como: el internet, correos electrónicos, fax, telefonía, entre otros, y que un computador se compone principalmente del *software,* que representa el conjunto de programas, instrucciones y reglas informáticas, y el *hardware* que es el conjunto de los componentes físicos de los que está hecho el equipo. Para mayor claridad hablaremos de cada uno de ellos.

Figura 2.

Hardware

Proviene del inglés “hard” el cual significa “duro” y es el término usado para referirse a toda la parte tangible y “permanente” de la informática; es la máquina que permite que se almacenen datos y se procese información, compuesta por elementos o partes con funciones principales y otras con

funciones secundarias o auxiliares, por ejemplo: el CPU en su traducción del inglés al español significa “Unidad Central de Procesamiento”, que viene a constituirse en la parte principal de todo el sistema computacional, debido a que el mismo es el encargado de manejar el procesamiento y almacenamiento de datos y de programas del computador; en cambio, el micrófono, scanner, parlantes, impresora, audífono, cámara, etc., son las partes secundarias del computador que no siempre son necesarias para el funcionamiento del mismo, sino más bien tienen la función de apoyo.

La computadora, ordenador o hardware, se ha convertido en un medio para la realización de los delitos informáticos, pues es la: *“Máquina capaz de efectuar una secuencia de operaciones mediante un programa, de tal manera, que se realice un procesamiento sobre un conjunto de datos de entrada, obteniéndose otro conjunto de datos de salida…”.*

Pablo A. Palazzi, en su obra “Delitos Informáticos” (2010), pág.33., plantea el argumento de que lo imprescindible al analizar los delitos informáticos es lograr determinar cuál es el papel que los ordenadores realizan dentro de un hecho ilícito. A su vez, el autor menciona que los delitos comunes y los delitos informáticos comparten una regla genérica, esto nos lleva a enfrentar la necesidad de delimitar los elementos que diferencian a un delito informático de los delitos comunes. Por su parte se puede entender que la computadora puede ser usada como “(…) *instrumento delictivo donde no importa aplicar analogía de alguna especie, sino adaptar la figura penal a los avances de la técnica…”* (PALAZZI, 2010)

Figura 3.

SOFTWARE

Corresponde a la parte intangible de la computadora, la cual realiza la función más transcendental que tiene el computador, esto es, la del procesamiento de información y almacenamiento de datos. De igual forma se debe recordar que el software es la parte que le da sentido al hardware puesto que sin esta, únicamente contaríamos con una estructura física, la cual estará conformada por un conjunto de elementos y compuestos electrónicos, de tal manera que el hardware por sí solo, no pueda realizar función o tarea alguna.

Siendo el delito informático cada vez más usual, abundante e innovador, realizado en su generalidad a través de ordenadores o redes de Internet, que incluye conductas nuevas del delincuente, destinadas a obtener datos o programas de computación de forma ilegítima en un sistema de información a través de espionaje, destrucción de sistemas de seguridad, apropiación de dinero por medios electrónicos, saboteando y dañando programas, apuntalando al terrorismo, violentando claves, entre otros, se considera que dichas conductas punibles van en aumento, pues cada día aparecen nuevas figuras delictuosas cometidas de forma virtual; cuando en la sociedad se tiene conocimiento de una modalidad, el delincuente informático crea o innova otra; así del phishing vamos al pharming por ejemplo, en términos que podamos entender los que no somos informáticos, cuando la singularidad de solicitar claves por internet en páginas clonadas es un descalabro, porque ya no las suministramos debido a varios ingredientes, como aquella publicidad de la entidad financiera insistiendo a los usuarios de no entregar claves por ningún medio electrónico, o porque los delincuentes informáticos conocen que la mayoría de la población contamos con un teléfono en el que se ha instalado un sistema de alarma, por lo que excluyen la circunstancia de requerir claves en páginas creadas o clonadas y diseñan programas informáticos maliciosos, para que la información entregada de manera efectiva en páginas reales sean desviadas con fines reprochables a los mismos.

Vicente Vallejo Delgado (2010), indicó que delito informático *"es el acto típico, antijurídico, imputable y culpable, sancionado por una pena y cometido mediante ordenadores y demás recursos electrónicos y cibernéticos. Por lo tanto, el acto que utilice recursos materiales como ordenadores, módems, fax,*

telefax, filmadoras, entre otros, tipificados como delito y sancionado con una pena, es delito Informático...". (Vallejo, 2010)

Acurio Del Pino, quien cita a Davara Rodriguez, define al Delito informático como *"la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software* **...**" (Acurio, 2010)

Julio Téllez Valdés define a los delitos informáticos en su forma típica y atípica, como "*las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin*". (TELLEZ VALDEZ, 2008)

Concluimos entonces con el concepto de infracciones informáticas reproduciendo el contenido con la siguiente ampliación ***Art. 18.- Infracción Penal.*** *Infracción penal es la conducta típica, antijurídica y culpable,* ***ya sean cometidos en forma tradicional o por cualquier medio electrónico o informático,*** *cuya sanción se encuentra prevista en este Código".* Ahora es necesario encauzar el hecho, que no todas las personas pueden llegar a ejecutar una infracción informática, debido a que solo un explícito número de ciudadanos poseen conocimientos en procesamiento de datos con los que infringirían los sistemas de seguridad con el fin de cometer estos ilícitos, entonces es poco factible que personas sin conocimientos en la materia cometan delitos informáticos, a menos que éste sea ejecutado sin intención sino más bien, escudriñando algún sistema operativo, y como resultado de aquello ocasione algún tipo de daño, lo que en nuestro país no sería considerado infracción penal debido al elemento indispensable para que una conducta sea punible, como lo es el dolo, que lo define el Artículo 26, a quien actúa con dolo la persona que tiene el designio de causar daño. Responde por delito preterintencional la persona que realiza una acción u omisión de la cual se produce un resultado más grave que aquel que quiso causar, y será sancionado con dos tercios de la pena, consecuentemente contar con conocimientos elementales o desarrolladas en el área informática no necesariamente consiste una "conditio sine qua non" para delinquir

y que, con el avance tecnológico y la gran habilidad con la que se puede compartir instrucciones e información a través de tutoriales, blogs, etc.; solo por mencionar existe una sección de la web conocida como la "infra net", un sitio donde distintas personas comparten información y ofertan todo tipo de productos pertenecientes a fuentes ilícitas, que facilita a una persona, que si bien no cuenta con los conocimiento de experticia necesarios para cometer un delito de este tipo, con la persistencia y el propósito positivo de quebrantar la ley, son aptos a través de guías y recomendaciones de convertirse en lo suficientemente idóneos para realizar este tipo de delitos y estar acorde a lo dispuesto en el Artículo 22, que señala que son penalmente relevantes las acciones u omisiones que ponen en peligro o producen resultados lesivos, descriptibles y demostrables.

El mismo mexicano **Dr. Julio Téllez Valdés,** indica algunas de las características sobre el modo de operar de estos ilícitos y menciona las siguientes: (TELLEZ VALDEZ, 2008)

Conductas criminógenas de cuello blanco (white collar crimes), en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.

- Acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando.
- Acciones de oportunidad, en cuanto que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios de más de cinco cifras a aquellos que los realizan.
- Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar.

- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- En su mayoría son imprudenciales y no necesariamente se cometen con intención.
- Ofrecen facilidades para su comisión a los menores de edad.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
- Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Por lo antes referido, es necesario clarificar al sujeto activo del delito enfocando en la intención de causar daño como lo veremos a continuación.

Delincuente Informático

Hacking, cracking y delitos informáticos son temas significativos en la actualidad y seguirán siéndolo con mayor énfasis en un futuro previsible, debido al progreso imponente de la know-how (conocimientos) en materia informática. "*Para algunos autores el sujeto activo de "estos delitos se encuentra conformado por un grupo de personas con una inteligencia y educación que superan el común, con vastos conocimientos informático…"* (PALAZZI, 2010)

En nuestro ordenamiento jurídico, la persona natural es el SUJETO ACTIVO del delito a quien se le proporciona una sanción. En materia de delitos informáticos no cambia esta generalidad, tras un ordenador siempre debe haber una persona natural quien será responsable por el cometimiento del delito, ya sea que ésta haya sido realizada de forma directa o que se trate de la persona que proyectó un programa para que se ejecute por su cuenta.

Hacking y Craking: Definición y Diferencias

Hacking

Utiliza técnicas de ingenio, programadas para acceder a un sistema informático, que necesariamente en esta penetración no son autorizadas, puede ser que lo que haya examinado es un ingreso a tales sistemas sin dirigir sus actos a la afectación de la integridad o disponibilidad de la información, incluso puede ocurrir el caso que quien vulnera el sistema no busca en lo absoluto causar daños al sistema y mucho menos apropiarse de información, simplemente busca el poner a prueba sus habilidades y en algunos casos trabajar para la seguridad informática para tal o cual compañía o entidad, cuya seguridad fue vulnerada, delitos que son descubiertos fortuitamente, otros por el desconocimiento en la forma de operar o curiosidad para experimentar conocimientos adquiridos, como fue el caso del norteamericano Robert Tappan Morris, quien en su época de estudiante en la Universidad de Cornell, aproximadamente en el año 1988, creó un programa que con el tiempo se conocería con el nombre de "gusano gris", el primer gusano de ordenador de la era de la Internet y que a decir de Robert Tappan, su única intención al crear este gusano fue la de conocer la capacidad o tamaño del Internet, de esta forma realizó un envío del gusano desde el conocido Instituto Tecnológico de Massachussets (MIT), a fin de ocultar su verdadera procedencia, sin contar que el mismo trascendiera de forma tan rápida, lo cual causó un daño fulminante y a gran escala; entre los perjuicios ocasionados se registró que las computadoras infectadas comenzaban a ponerse lentas hasta llegar al punto donde se caían los sistemas y las máquinas dejaban de funcionar. Otro punto que incrementó la magnitud de los daños es que entre las computadoras infectadas con ese gusano, se encontraban equipos de agencias como la NASA y el Pentágono, incluyendo a universidades como Berkeley y Stanford. Al ser descubierto, Robert Tappan Morris fue enjuiciado y condenado en la corte de Syracuse, estado de Nueva York, a 4 años de prisión y al pago de US $10,000 de multa, pena que fue conmutada a libertad bajo palabra y condenado a cumplir 400 horas de trabajo comunitario, lo que nos permite colegir que vulnerar la seguridad del sistema de cualquier entidad o empresa sin autorización, pero sin la intención de contravenir normas, puede

llegar a ser considerado como vulneración a la intimidad del titular de aquella información o como un delito mayor en otras legislaciones y en la nuestra también merece sanción penal.

Cracking

Ahora bien, para los casos donde el sujeto activo no tiene como principal objetivo probar sus conocimientos o dar seguridad a un sistema informático, sino que la intención del sujeto activo es la de vulnerar de forma directa un sistema, con la principal finalidad de ocasionar daños al sistema informático u obtener beneficios ilícitos para sí o para terceros, podemos definir al cracking como el sujeto de activo de la infracción, que dirige una conducta punible contraria a derecho por medio de la creación de programas o rutinas, inutiliza, destruye y se apropia de información que se pueda encontrar tanto en sistemas de cómputo o telefónicos. Estudiosos en la materia señalan inclusive que dentro de los mismos crackers existe una subdivisión, que son: piratas, lamer, phreakers entre otros.

- Piratas: Son aquellos cuya actividad consiste en realizar copias ilegales de programas por medio de la vulneración de la seguridad de los sistemas de protección informáticos que cada entidad tiene para la protección de sus datos. Los piratas también se caracterizan por generar una indeterminada cantidad de copias de esta información y distribuirlas de forma clandestina.
- Lamer: Son un tipo de cracker que no poseen conocimientos propios sobre informática, pero que por medio de la ayuda de personas que sí cuentan con este conocimiento, obtienen programas y todo tipo de herramientas que les permite atacar ordenadores. Los lamer se definen en pocas palabras como “sujetos que ejecutan aplicaciones sin saber mucho de ellas y causan grandes daños”.
- Phreakers: Se trata de crackers cuyas actividades de causar daño se centran en las líneas telefónicas. Los phreakers se dedican a atacar y romper la seguridad de los sistemas telefónicos, ya sea para causar daños en el mismo o realizar llamadas de forma gratuita.

En conclusión, el cracker es aquel que rompe sistemas de seguridad en computadoras, colapsa servidores, entra a zonas restringidas, infecta redes o se apodera de ellas, altera, suprime o daña la información, obstaculiza, deja inoperante o menoscaba el funcionamiento de un sistema o dato informático, se apropia de información privilegiada, transfiere fondos entre cientos de modalidades más, a sabiendas de que lo que está haciendo no es permitido o es ilícito; con el designio de causar daño, es ahí donde estamos frente al SUJETO ACTIVO DE UN DELITO DOLOSO, como ya se mencionó.

Delincuente de Cuello Blanco

Es menester mencionar que los delitos informáticos son asociados con el "delito de cuello blanco", que fuera mencionado por Edwin H. Sutherland, como crimen realizado por personas de supuesta respetabilidad y un estatus social alto; además indicaba, que los delincuentes contravienen por varias motivaciones, pero que en general no se caracterizan por ubicarse en situación de pobreza, sino que se encuentran con cierta estabilidad económica y que entre las actividades que realizan, se determinan los delitos de desfalco, ventas de propiedades, etc., los mismos suelen no contar con antecedentes delictivos y cuando son identificados, en la mayoría de los casos, se determina que son apuestos, frecuentemente hombres que funcionan solos y que a criterio personal, a nivel internacional podemos mencionar a varios delincuentes con éste perfil, mencionándose para mejor comprensión, la descripción de Edward Snowden, de quien indicaron los Congresistas Norteamericanos, que trabajó en la Agencia de Seguridad Nacional de EE.UU. (NSA), y es desde ahí que supuestamente descargó 1,7 millones de archivos de inteligencia de las agencias estadounidenses, que significó mérito suficiente para que EEUU considere al robo de esta información, como el más grande realizado en la historia, donde se hayan sustraído documentos e información reservada.

De tal manera que el perfil dado por Sutherland, se asocia al delincuente informático en algunas particularidades, tales como que gozan de una inteligencia y talentos rimbombantes, con gran capacidad en el manejo de la computadora, no necesita ser mayor de edad, por lo general los niños de ésta generación vienen con un chip incorporado, pues desde muy pequeños

tienen acceso a ordenadores y desarrollan *fácilmente práctica, destrezas* para dominar sistemas computacionales. A nivel internacional se cita como ejemplo de aquello a Jonathan James, mejor conocido como "C0MRADE", quien llamó la curiosidad de todo el mundo, por ser el primer adolescente condenado a seis meses de arresto por cometer delitos como hacker, cuando apenas tenía 16 años. James instaló un programa que se introdujo en el ordenador y que estableció una puerta trasera a través de la cual fue posible controlar el sistema afectado sin conocimiento por parte del usuario, programa que fue instalado en los servidores de la Agencia de Reducción de Amenazas de la Defensa (Defense Threat Reduction Agency, DRTA), que le permitió ver correos electrónicos de asuntos delicados con el fin de capturar los nombres de usuarios y contraseñas de esta organización, que se encargaba de reducir las amenazas a Estados Unidos y sus aliados en materia de armas nucleares, biológicas, químicas, convencionales y especiales, a esto se sumó la apropiación de un software de la NASA, que según el Departamento de Justicia de Estados Unidos, contenía "un programa utilizado para controlar el medio ambiente, temperatura y humedad, de la Estación Espacial Internacional". Debido a este ataque, la NASA tuvo que paralizar sus computadoras por tres semanas, lo que generó una pérdida de US$ 41,000.[1]. Jonathan James fue arrestado el 26 de enero del año 2000 y tuvo que permanecer en arresto domiciliario por seis meses, tiempo durante el cual estuvo prohibido de acercarse a una computadora para uso recreacional. El 19 de mayo de 2008, James fue encontrado muerto en la ducha de su casa, luego de haberse disparado a sí mismo en la cabeza. Su suicidio habría sido motivado porque se sentía perseguido por la justicia por delitos que no cometió, como el del ataque a la cadena de tiendas por departamento TJX. James dejó una nota antes de suicidarse, en la que decía lo siguiente: *"Honestamente, de verdad, no tengo nada que ver con TJX. No tengo confianza en el sistema 'justicia'. Quizás mis acciones hoy, así como esta carta, le envíen un mensaje más fuerte al público. De todos modos, ya perdí el control de la situación y esta es mi única manera de recuperarlo".* (Derecho Informático, 2010)

Otro caso con mucha notoriedad fue el de Adrián Lamo, quien logró insertar su nombre dentro de la lista de expertos que podían ver información personal de los contribuidores del diario, en la que también se encontraban los números del seguro social. Además, Adrián Lamo también hackeó las cuentas en LexisNexis que tenía The Times, para posteriormente realizar investigaciones de temas de interés. El Diario "The New York Times" presentó una denuncia en contra de Lamo que se publicó en 2003, con su orden de captura. Fue declarado culpable del cargo de delitos informáticos contra Microsoft, Lexis Nexis y The New York Times, el 8 de enero de 2004, por lo que tuvo que permanecer con arresto domiciliario por seis meses y pagar 65,000 dólares en restitución por sus delitos.

Se puede claramente diferenciar al sujeto activo del delito en materia informática: el cracking actúa con dolo, por el designio de causar daño y en algunos casos el hacker con culpa por infringir el deber objetivo de cuidado, que personalmente le corresponde, produciendo un resultado dañoso.

Capítulo 2

Análisis de las Infracciones Informáticas Observadas en el Código Penal Anterior y Código Orgánico Integral Penal.

ANTECEDENTES:

Se mencionó que nuestra legislación divide a las infracciones en delitos y contravenciones; evidentemente que la contravención también es una ACCIÓN TÍPICA, ANTIJURÍDICA Y CULPABLE, pues no debe variar la estructura elemental general ya descrita en la división de INFRACCIÓN que hace el Código Orgánico Integral Penal. A su vez, la única distinción que se hace, exclusivamente es en función de la amenaza y con el fin de diferenciar los delitos de las contravenciones como lo prevé al segundo y tercer párrafo del Art 19 del Código Orgánico Integral Penal, en el que podemos distar uno del otro, *"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",* por consiguiente se ratifica que la diferencia entre los delitos y las contravenciones, se centra principalmente en la gravedad de la infracción cometida y por consiguiente, la diferencia radica en la aplicación de la pena o la sanción de estas conductas conforme a la hecho antijurídico consumado.

Ahora bien, las infracciones informáticas, nacen en nuestro país, el 17 de abril del 2002, con la creación de la Ley 67, publicada en el Registro Oficial Suplemento 557, en la que el Congreso Nacional de ese entonces, consideró que el uso de sistemas de información y de redes electrónicas, incluida la internet, ha adquirido importancia para el desarrollo del comercio y la producción, permitiendo la realización y concreción de múltiples negocios de trascendental importancia, tanto para el sector público como para el sector privado. Que es necesario impulsar el acceso de la población a los servicios electrónicos que se generan por y a través de diferentes medios electrónicos, entre otros considerandos, y crea la LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS, estableciendo en el Art. 57, en cuanto a las Infracciones Informáticas, lo siguiente: *"Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley…"*, es decir, que en el

artículo 10, que se conceptuaba las infracciones en forma general estaban incluidas las de carácter informático, y ya en el año 2014, derogado el anterior Código Penal junto con el Código de Procedimiento Penal, con la aparición del Código Orgánico Integral Penal, el cual empezó a tener vigencia desde Agosto del 2014, donde se fortaleció el concepto de infracciones en forma general a todos los tipos penales contemplados en el mismo, con la inclusión de nuevas tipologías en las que se le otorgó mayor importancia a las infracciones con modalidades informáticas.

En Viena, del 10 al 17 de abril del 2014, se efectúo el Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, en el que se concluyó de forma unánime la coexistencia de dos prototipos de delitos cibernéticos:

a) Delito cibernético en sentido estricto ("delito informático"): Todo comportamiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas informáticos y los datos procesados por ellos; y,

b) Delito cibernético en sentido lato ("delito relacionado con computadoras"): Todo comportamiento ilícito realizado por medio de un sistema o una red informáticos, o en relación con ellos; incluidos los delitos como la posesión, el ofrecimiento o la distribución ilegales de información por medio de un sistema o una red informáticos.

Bien Jurídico Protegido o Tutelado por El Estado

Nos encontramos en un Estado Constitucional de Derechos y Justicia, desde el cual se observa al bien jurídico protegido o tutelado por el mismo, como una de las piedras angulares para la limitación de la potestad punitiva del Estado hacia al ciudadano, con la implementación en materia penal de tipos punitivos que auxilien, defiendan los derechos de los ciudadanos y logren el bien común, no solo con la intención de crear aquellas conductas reprochables que merezcan sanción, sino que efectivamente resguarden un interés individual y social, acorde con lo establecido en el artículo Art. 11, que señala que el ejercicio de los derechos se regirá por los siguientes principios,

numeral *4. "Ninguna norma jurídica podrá restringir el contenido de los derechos ni de las garantías constitucionales"*, en armonía con los artículos 3 y 4 del Código Orgánico Integral Penal, relacionando al principio de mínima intervención en el derecho penal también llamado *"principio de ultima ratio"*, que tiene más de una observación, pero que se concluye en que las represiones penales son restringidas al círculo de lo necesario, en gracia de sanciones para los ilícitos más leves, es decir, el derecho penal una vez consentido su necesidad de aplicación, no ha de castigar todas las conductas lesivas a los bienes jurídicos que preliminarmente se ha considerado merecedores de protección, sino únicamente las conductas de ataque más peligrosas para ellos, reflexiones análogas con las demás GARANTÍAS Y PRINCIPIOS RECTORES DEL PROCESO PENAL, como el dignidad humana y titularidad de derechos, en que *"los intervinientes en el proceso penal son titulares de los derechos humanos reconocidos por la Constitución de la República y los instrumentos internacionales...*" conexo a lo establecido en el artículo 5 Ibídem, que determina aquellos principios procesales como el derecho al debido proceso penal, de legalidad, favorabilidad, inocencia, igualdad entre otros, que incorporado el de lesividad y de última ratio ya mencionado, imponen la demanda de no abarcar todos los altercados sociales, sino directamente aquellas alteraciones indispensables para la armónica convivencia social y general, y que la afectación a un bien jurídico protegido por el Estado tenga un castigo correccional y eficiente como ubica el *ius puniendi.*

En materia de delitos informáticos tenemos diversidad de bienes jurídicos tutelados que vienen a ser pluriofensivos, que pueden ser violentados a través de comportamientos inadecuados que quebrantan la sistémica coexistencia general que germinan de un delito tradicional, pues no existe bien jurídico distinto en materia informática que constitucionalmente son resguardados, afectan la intimidad, el patrimonio, la propiedad intelectual, la seguridad, etc. Por ejemplo los derechos de libertad contemplados en el Art. 66, establece el numeral 26 *"El derecho a la propiedad en todas sus formas, con función y responsabilidad social y ambiental…",* que es quebrantado con la amplia gama de fraudes informáticos y las manipulaciones de datos; por su parte el numeral 21 establece el " *derecho a la inviolabilidad y al secreto de la correspondencia*

física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación", que son abiertamente violentados en la obtención de forma ilícita de bancos de datos de usuarios en alguna institución o la publicación de información de circulación restringida, interceptación ilegal, etc., distribución de material pornográfico que vulnera el derecho a la integridad personal, que incluye entre otros, la integridad física, psíquica, moral y sexual; solo por aludir algunos.

Tipos Penales en el Código Orgánico Integral Penal

El Código Orgánico Integral Penal, **en adelante** llamado **(COIP),** desde su vigencia destinó nuevas y mejoradas infracciones penales, percibidas desde el punto de vista de casos acontecidos en la sociedad durante años y que no pudieron ser incluidos en el Código Penal anterior, a pesar de existir variadas reformas en la vigencia del mismo; lo propio en temas de procedimientos y rehabilitación social de las personas sentenciadas, así como la reparación integral de las víctimas.

Sustituir la normativa vigente desde 1971, con 730 artículos, proyectó no solo la optimización de tiempos procesales, garantizar los derechos de las víctimas directas o indirectas, sino también 306 tipos penales, dentro de los cuales se consideraron conductas nuevas y existentes a la realidad nacional e internacional, como en el caso de los delitos por violaciones a los derechos humanos y de lesa humanidad, con el fin de perfeccionar la aplicación de un sistema jurídico justo y equitativo basado en el respeto a los Derechos Humanos, la Constitución y las leyes conexas, honrando compromisos internacionales, dejando atrás la multiplicidad y coexistencia de diversos textos penales y no penales, para acertar en un solo cuerpo de leyes normalizado y agrupado lo sustantivo, adjetivo y objetivo del derecho penal.

Entre los nuevos delitos penales se consideran aquellos mecanismos trascendentales, para comenzar esparciendo en la sociedad ecuatoriana una nueva cultura penal, como es el caso de los delitos cometidos a través de

medios informáticos; injustos no tradicionales que permitirán no impunidad y fortalecimiento de la justicia penal existente.

A continuación revisaremos los tipos penales asociados con infracciones informáticas o utilizando medios informáticos.

Graves Violaciones a los Derechos Humanos y Delitos Contra el Derecho Internacional Humanitario.

DIVERSAS FORMAS DE EXPLOTACIÓN

Art. 103 COIP:

Pornografía con utilización de niñas, niños o adolescentes.

"La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual; será sancionada con pena privativa de libertad de trece a dieciséis años…".

Figura 4

En el articulado se observa que una de las modalidades al momento de establecer éste censurable delito es mediante soportes informáticos y electrónicos, lo que no precisamente lo hace un "delito informático"; sin embargo,

siendo la pornografía infantil no una figura penal nueva, tradicionalmente la misma se lo ejecutaba a través de revistas, videos, películas de video, lo que en la actualidad resulta obsoleto acorde con la globalización que trajo consigo un incremento del uso de internet, para la descarga y propagación de la pornografía infantil en páginas web, correos electrónicos, redes sociales, etc., debido a que su comercialización es más efectiva por la habilidad de negociar y lo dificultoso de detectar de donde proviene o quien la realiza, pues son creados con métodos de evasiva y encriptación, que sin regulación en el uso de internet, el control y el rastreo del origen de los archivos se convierte en un trabajo muy arduo para los peritos especializados, que a diferencia de quienes la producen, pueden ser sujetos sin conocimientos que solo necesitan de víctimas y cualquier medio de los que contempla la norma.

La conducta delictiva de pornografía infantil de niños, niñas y adolescentes, incluida en el artículo 103 del COIP, como una de las peores formas de violación a los derechos humanos de la niñez y adolescencia, logra que los Jueces sancionen con el mayor rigor de la ley, evitando impunidad, además de salvaguardar la dignidad humana y el derecho al sano desarrollo de la sexualidad que violentados afectan todas las dimensiones de la vida de éste grupo vulnerable, considerados actos de violencia que interrumpen su desarrollo integral tanto cognoscitivo, físico, emocional y psicológico de manera concluyente, provocando daños irreparables en su vida, y que si bien no cuenta con una definición absoluta a nivel mundial, es uno de los injustos penales más imperturbables para el derecho internacional, razón por la que Naciones Unidas lo define como cualquier representación de un niño dedicado a actividades sexuales explicitas reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales, mientras que el Consejo de la UE lo define como: *"niño real practicando o participando en una conducta sexualmente explicita, incluida la exhibición lasciva de los genitales o de la zona púbica del niño".* (PENAL C. O., 2014)

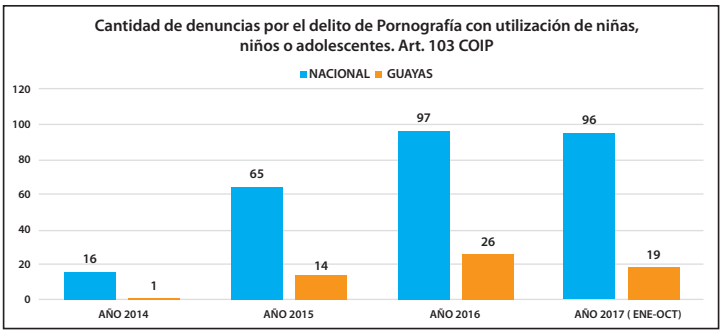


Figura 5.

Fuente: *Fiscalía del Guayas/octubre 2017*

En todo caso, nuestra normativa enfoca en la representación visual, por parte del transgresor a través de cualquiera de las formas idónea para ser contemplado, acrecentando la sanción de acuerdo a la edad de la víctima, que será de hasta veintiséis años, pues va implícita la conducta sexual como particularidad del tipo penal, incluido el soporte informático y electrónico.

Concluyendo, se puede expresar que delito informático en sí de pornografía infantil, no existe; las modalidades delictivas históricas, hoy son cometidas a través de soportes informáticos, por lo tanto lo que cabe en este tipo penal es resaltar el enfoque actualizado del asambleísta en el libro segundo, título IV, Art. 500 de la norma sustantiva ecuatoriana, al considerar como medio de prueba documental el contenido digital, que en el anterior Código de Procedimiento Penal no constaba, y que en el año 2004, cuando en el archipiélago de Galápagos fuera descubierto, investigado y sancionado el caso denominado “Burdet Cedeño”, que a nivel nacional e internacional causó conmoción social, pues los sentenciados cometieron concurrencia de delitos sexuales, tales como violaciones masivas contra menores de edad, abuso sexual entre otros delitos incalificables, sin poder vincular la investigación al delito conexo de pornografía infantil, pues además del delito mayor se hallaron fotos e imágenes de más de 70 niños, que eran difundidas a una página web, como pornografía infantil, lo que desató la necesidad inminente de contar con una normativa relacionada; así la Ministra Fiscal del Estado de la época,

Doctora Mariana Yépez, elevó un proyecto de Ley al Congreso Nacional, con la necesidad de reprimir a redes internacionales de pornografía infantil; además de estar acorde al artículo 34 de la Convención de Derechos del Niño, en las que nuestro país es suscriptor; se concluyó entonces con reformas al Código Penal anterior, para evitar la impunidad y la ausencia de sanciones posteriores proporcionales al daño que este tipo de violaciones causan en las víctimas, los delitos de proxenetismo y corrupción de menores, como reforma los delitos de explotación sexual que fue la base para la ejecución final del articulado vigente en el COIP, el que en uno de los innumerados decía así:

Art.104.- *Quien produjere, publicare o comercializare imágenes pornográficas, materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato, u organizare espectáculos en vivo, con escenas pornográficas en que participen los mayores de catorce y menores de dieciocho años, será reprimido con la pena de seis a nueve años de reclusión menor ordinaria, el comiso de los objetos y de los bienes producto del delito, la inhabilidad para el empleo, profesión u oficio.*

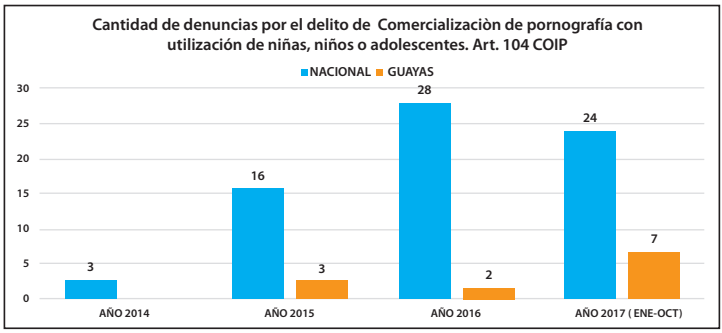


Figura 6.

Fuente: *Fiscalía del Guayas/octubre 2017*

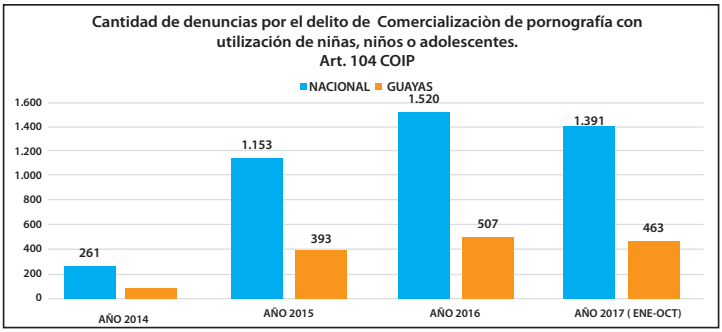


Figura 7.

Fuente: *Fiscalía del Guayas/octubre 2017*

Delitos Contra los Derechos de Libertad.

Delitos Contra Integridad Sexual y Reproductiva

Art. 173 Coip.- Contacto con finalidad sexual con menores de dieciocho años por medios Electrónicos.-

"La persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años".

Figura 8.

La conducta anteriormente contemplada, se conoce en el mundo cibernético como “grooming”, palabra de origen inglés “groom” que significa acicalar o limpiar, considerado como un nuevo problema referente a la seguridad de los niños, niñas y adolescentes en internet, que reside en la ejecución de tareas proyectadas por un adulto, con la intención de establecer lazos de amistad con un niño o niña por esa vía, con el objetivo de lograr contentamiento sexual mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual, donde los delincuentes se escudan en el anonimato o falsas identidades y prevaliéndose de la inocencia de los menores y la fácil accesibilidad al internet, que sin ningún control de padres, madres, curadores o representantes, son utilizados por los mismos y que tiene como característica primordial, establecer con el adulto perseguidor una “amistad” para ganar su confianza y luego involucrarlos en actividades sexuales reales o en redes de pornografía infantil, conducta readaptada a las viejas prácticas de pederastas con la tecnología. Una vez abordadas a sus víctimas en la red, suelen propagarse al mundo físico, resultando en muchos casos en delitos de tráfico de pornografía infantil, abuso sexual, violación y hasta asesinatos.

En Colombia, en febrero del 2016, se hizo público el caso denominado “El imitador de cantantes”, que consistía en un hombre de 23 años, quien manejaba dos perfiles falsos en Facebook, a nombre del cantante Maluma, sujeto que se ganaba la confianza de niñas entre 9 y 12 años, a quienes que solicitaba fotografías y videos en que aparecieran desnudas o en ropa interior; cuando ya era enviado el material solicitado, las amenazaba con publicar las imágenes o enviárselas a sus padres a menos que accedieran a sostener relaciones sexuales con él. Fue capturado con 15 discos duros, 5 tabletas, 9 celulares, 15 memorias micro SD y 2 memorias USB, que utilizaba para almacenar y distribuir las imágenes. Si bien fue sentenciado con la máxima pena en el país vecino, no todos los agresores son capturados debido a la problemática para investigar y sancionar como son la falta de denuncia de la víctima y la dificultad de identificar el lugar de enlace.

El grooming online ajusta la conducta a la propuesta de un contacto sexual online, por lo general vía “webcam”, cámara de vídeo miniaturizada con la

que se obtiene vínculo con un ordenador para grabar imágenes o emitirlas en directo a través de internet, material que más tarde es compartido con otros, ocasionado graves traumas en la víctima y que puede ser utilizado con amenazas para que germinen delitos mayores, que pueden ser cometidos en diversos lugares, desde domicilios particulares, salas de chat, redes sociales online entre otros. Las estadísticas de estudiosos en la materia establecen que un groomer módico puede tener hasta 200 menores en sus listas de amigos, en tiempos indeterminados, quienes emplean la seducción para obtener sus morbos o mienten sobre su edad, rostro, profesión o sexo, para encajar en un caso de relación de consentimiento, que en nuestra legislación es considerado irrelevante.

Como se ha referido, en la sociedad de la información en la que nos encontramos, los delitos cometidos en contra y por lo menores, han aumentado, debido al universo que se maneja con las Tecnologías de la Información y Comunicación (TIC´s) que están al alcance de los niños, niñas y adolescentes, donde el ingrediente esencial es que los adultos responsables no están al pendiente de sus hijos para orientarlos acerca del uso adecuado de estas (TIC's).

Queda por lo menos la satisfacción jurídica de contar con el tipo penal de "grooming" para que en el caso de sancionar, no dejar en la impunidad este tipo de transgresiones.

Delitos Contra Los Derechos De Libertad

Delitos contra integridad sexual y reproductiva

Art. 174 COIP: Oferta de servicios sexuales con menores de 18 años por medios informáticos

"La persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, foto blogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad, será sancionada con pena privativa de libertad de siete a diez años…" (PENAL C. O., 2014)

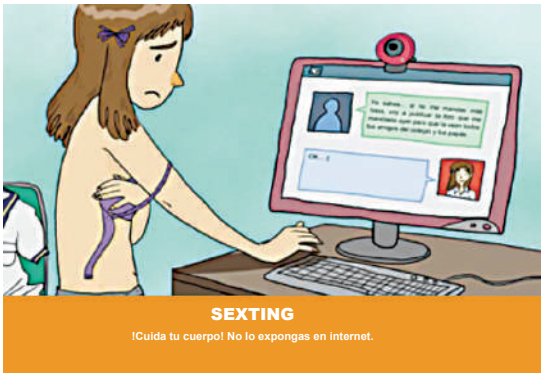


Figura 9.

La figura penal castiga al adulto que "**ofrezca"** mediante cualquier soporte informático servicios sexuales con niños, niñas y adolescentes, no el contacto sexual, no el exhibicionismo, no material con contenido sexual, entre otras funestas figuras penales, simplemente aquel que prometa por cualquier medio transgredir los límites intrínsecos y propios de menores de 18 años, buscando el agresor diversas maneras, siendo una de las más usuales en el mundo cibernético e identificada como "sexting", palabra en inglés sex (sexo) y texting (mensajes de texto), que inicialmente fuera identificada en Estados Unidos en el año 2005, modalidad que consiste en la acción de intercambiar mediante internet, teléfono, redes sociales, fotografías tomadas con algún contenido sexual, que bien puede darse dentro de una relación sentimental o amorosa consentida, mas no con la intervención de niños, niñas y adolescentes, aunque cuenten con el anuencia de los mismos, pues como ya se mencionó, el consentimiento en este tipo de delitos es irrelevante por la edad, y peor aún si dicha oferta se la hace en función de la amenaza como suele suceder.

Los niños, niñas y sobre todo en este tipo penal se encasillan con mayor facilidad los adolescentes, por falta de discernimiento o exceso de confianza, no dimensionan el grado de sus actos, que luego les puede traer consecuencias, no solo emocionales, sino sicológicas también, por la impiedad y degradación pública a la que se ven sometidos, ya que una vez en manos del agresor, las fotografías o videos de contenido sexual, lo que sigue es la "Sextorsión", que es el elemento para extorsionar o chantajear al protagonista de las imágenes

que puede desencadenar en la pérdida inclusive de su vida. En México, en el Distrito Federal se hizo notorio el caso de un joven que había sido víctima de violación por siete de sus compañeros de escuela, cinco de ellos eran menores de edad. Estos jóvenes videograbaron la violación para luego ser renviada vía bluetooth a través de los celulares.

Existe un segundo enfoque al analizar el artículo 174 del COIP y es que el Estado a través de sus legisladores, decidió predominar el interés superior de niños, niñas y adolescentes, respetando el mandato constitucional contemplado en el Art. 44, garantizando la integridad física, psicológica y sexual de los más pequeños ciudadanos, de conductas antijurídicas de individuos que *utilicen de forma directa o faciliten a terceros*, cualquier medio electrónico para OFRECER servicios de naturaleza sexual, que puedan asociarse con la explotación sexual comercial infantil (ESCI), debido a que la norma en estudio no sanciona la ejecución de los actos sexuales, sino la solo oferta, que bien este tipo de delitos ha sido considerado por el derecho internacional como una grave violación de los derechos humanos de niños, niñas y adolescentes que originó a que la Organización Internacional de Trabajo (OIT), como el organismo especializado de la ONU para promoción de la justicia social y el reconocimiento de las normas fundamentales del trabajo, vea la explotación sexual comercial infantil como análoga a la esclavitud y al trabajo forzoso, relacionando este grupo sensible de la sociedad en actividades sexuales remuneradas, en efectivo o en especie, (conocida comúnmente como prostitución infantil) en las calles o en el interior de establecimientos, en lugares como burdeles, discotecas, salones de masaje, bares, hoteles y restaurantes, entre otros.

Es importante resaltar que por primera vez en la legislación ecuatoriana se manejan glosarios como blogs y foto blogs, utilizadas continuamente por los cibernautas, que significa bitácora dentro de un sitio web personal, que contiene galería de imágenes o fotografías, de fácil acceso por quienes son parte de la red, abarcando no solo lo usual como fotografías y videos.

Siendo un problema social que adquiere derivaciones en la vida de los niños, niñas y adolescentes, en su ambiente y en todos y cada uno de los contextos en los que se desarrollan, los asambleístas tipificaron el solo hecho

del ofrecimiento, como prevención, que indiscutiblemente incluyen a la familia, ámbito educativo, entorno social, autoridades, en sí toda la sociedad.

Delitos contra los Derechos de Libertad

Delitos contra el Derecho a la Intimidad Personal y Reproductiva

Art. 178 del COIP: Violación a la Intimidad:

"*La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.*

No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley". (PENAL C. I., 2014)

Figura 10.

La nueva figura delictiva descrita en líneas anteriores puede parecerse particularmente a la contemplada en el libro II, Titulo II, capítulo V, "De los delitos contra la inviolabilidad de secreto", enumerados del Art. 202 del Código Penal anterior que establecía:

Art. ...- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener

información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

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

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica. Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art. ...- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.

La intimidad en múltiples ocasiones es confundido con privacidad, incluso con la confidencialidad, por lo que se hace necesario en primer lugar, esclarecer que la intimidad poseec onceptualmente un alcance minúsculo comparado con la privacidad y la confidencialidad; sin embargo, a título personal considero que es el más pernicioso e incómodo, para decirlo de alguna manera, tratándose que el derecho a la intimidad resguarda la parte más inseparable, intrínseca de un ser humano por estar vinculado a la esfera esencial, personal e íntima, de ahí el nombre “intimidad”, que no solo abarca los sentimientos sino los dogmas de cualquier tipo, sean políticas, religiosas, inclinaciones, tendencias sexuales y de género, pensamientos, fundamentos, entre otros, que en muchos de los casos, la persona se niega a compartirlos

con los demás por la motivación que tenga o crea tener; peor aún quiere proveer a otro individuo el conocimiento de manera autónoma y consciente, por varios motivos, entre los que destaca la vulneración de su propia imagen, es decir, el derecho a la intimidad corresponde con la psique del individuo.

Siendo entonces un derecho asociado a la información, en el tipo penal en estudio, se sanciona la vulneración del mismo utilizando varias herramientas informáticas, y es por eso que contemplar una figura nueva en el COIP, en la trasgresión del mismo, constituye una manera de protección.

La disposiciones dadas en el Art. 178 del COIP, van inmersas en la desobediencia del bien jurídico protegido por el derecho constitucional como el secreto, la confidencialidad de la información y la jerarquía de los datos, con la imperiosa reserva establecida en nuestra Constitución, Título II, capítulo sexto referente a los Derechos de LIBERTAD, en su Art. 66, numeral 19, como el derecho a la protección de datos de carácter personal; derecho compuesto por el poder de atesorar la intimidad, reserva y privacidad de la información exclusiva de cada uno de los ciudadanos ecuatorianos, obviamente excluyendo las requeridas por autoridad competente y con las formalidades que el caso amerite, y que si bien en ninguna parte de los articulados se menciona el término “Espionaje”, mucho menos “Espionaje informático”, paradójico al bien jurídico protegido, se describen situaciones bastantes similares como es la ilegalidad del acceso o intromisión informática ilícita, asentada en la particularidad de ingresar en un sistema informático ajeno, con la intención de acceder a información intangible y particular, forzando el mandato constitucional referido en líneas anteriores, que va en perjuicio de la víctima y en beneficio de los malhechores, con mayor sanción se consideró en el Código Penal anterior, cuando el espionaje afectaba a la seguridad del Estado y que ahora es contemplado como parte de este articulado en el Art. 354 del COIP, dentro del capítulo de los Delitos contra la Estructura del Estado Constitucional, y si bien el vocablo ESPIONAJE está incorporado al romanticismo o a nombres como Mata Hari que dio al fisgoneo un aura romántica, hoy en día existen diversas maneras de espiar, ya sea empleando micrófonos de miniatura, modernos aparatos fotográficos independientes o que vienen incorporados en los celulares, en plumas, reloj,

sensores, detectores en aparatos electrónicos, todos ellos para espiar u obtener información de diverso tipo, pero sobre todo de datos corporativos, secretos comerciales e industriales, datos personales de empleados, clientes de compañías, información personal, etc, que de acuerdo al Derecho Internacional viene a constituirse en una actividad delictiva que está tipificada como delito de especial gravedad, merecedora de máximas penas, incluidas las privativas de libertad. Es necesario mencionar que la pena es acorde a un delito de menor gravedad, capaz de aplicarse cualquier procedimiento que beneficie al agresor, lo que a la larga seria desproporcionado al daño que probablemente se cause, y que si bien posee un enfoque más breve y categórico, por ningún motivo innova un nuevo bien jurídico, por el contrario mantiene incólume el derecho a la reserva y el secreto, lo que es mejor aún, se aprecia que en el Art. 178 del COIP, donde se perfeccionó evidentemente el mandato constitucional, del artículo 66, numeral 21, que establece*: "El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación*", ampliándolo y restableciéndole al campo virtual y como ya se mencionó especificando que debe darse bajo la intervención judicial, como peculiaridad ideológica y estructural bajo la tendencia de la reglamentación de la normatividad, patente al principio de aplicación inmediata de los preceptos que invoque el ciudadano y aun sin la necesidad de su exhortación o fundamentación; lo que constituye un avance en el desarrollo del Derecho Penal Ecuatoriano, sobresaliendo los intereses superiores de la sociedad en su conjunto. El tipo penal en mención sanciona la transgresión a la esfera más íntima del ciudadano respecto de aquella información que contenga aspectos relativos a lo particular que no debe ser conocido por un tercero bajo ningún acontecimiento resaltando una vez más el consentimiento o la autorización legal, anuencia dada por la persona titular de la información y la autorización legal en las circunstancias que la ley permite procesalmente en el COIP, analizando además el ánimo de hacer daño, de menoscabar el derecho de las personas violentando diversos derechos, pero en particular el de la intimidad.

Encuadrar la conducta en cualquiera de los verbos rectores constantes en la norma, tales como acceder, interceptar, examinar, retener, grabar, reproducir, difundir o publicar no solo que es sancionado al que delinque, sino que ocasiona al sujeto pasivo una grave afectación, por consiguiente, quien contraviene deberá enfrentar ante la justicia delitos adyacentes como violencia psicológica, daño moral en el ámbito civil o lo que es peor, incitación al suicidio como ya sucedió en Italia por un asunto de violación a la intimidad.

En el segundo inciso excluye a quien es interviene personalmente, cuando "***divulgue*** *grabaciones de audio y vídeo",* pero no excluye cuando "*acceda, intercepte, examine, retenga, grabe, reproduzca o publique…",* por tanto aplicando el Art. 13 del COIP no sería aplicable la exclusión, si revisamos diligentemente el mismo dice:

"Artículo 13.- Interpretación.-

Las normas de este Código deberán interpretarse de conformidad con las siguientes reglas:

1. La interpretación en materia penal se realizará en el sentido que más se ajuste a la Constitución de la República de manera integral y a los instrumentos internacionales de derechos humanos.

2. Los tipos penales y las penas se interpretarán en forma estricta, esto es, respetando el sentido literal de la norma.

3. Queda prohibida la utilización de la analogía para crear infracciones penales, ampliar los límites de los presupuestos legales que permiten la aplicación de una sanción o medida cautelar o para establecer excepciones o restricciones de derechos.

Lo que si se prevalece es la exclusión a personas que divulguen audios o videos de información pública de acuerdo con lo previsto en la ley, que tiene lógica considerando que quienes somos parte de redes sociales sabemos que las mismas no nos pertenecen de forma personal, pues así establece la aceptación contractual al momento de crear una cuenta pública, por solo mencionar un ejemplo, lo que conlleva a la reflexión de saber manejar la información que compartimos de forma prudente, protegiendo no solo a la persona titular sino a su entorno.

Delitos contra los Derechos de Libertad

Delitos contra el Derecho a la Propiedad

ARTÍCULO 186.- Estafa.-

La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años. La pena máxima se aplicará a la persona que:

1. *Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.*
2. *Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares.*

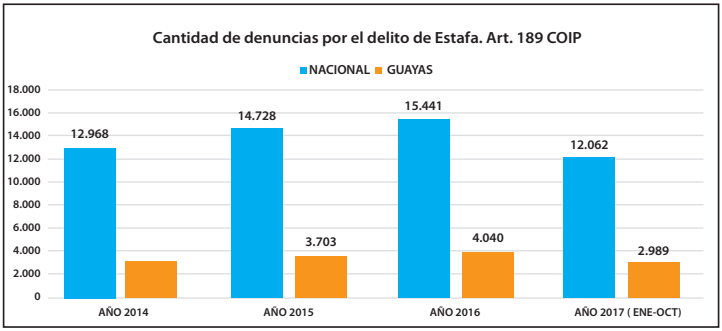


Figura 11.

Fuente: *Fiscalía del Guayas / Octubre 2017*

La estafa es un delito que vulnera como bien jurídico el patrimonio, es decir, el ánimo de apoderarse de algo impropio o engañar con fines de lucro, cometido con el propósito de apropiarse de una cosa perteneciente a otro. La anterior figura penal establecía al engaño como fundamento esencial del tipo,

haciéndose entregar fondos, muebles, obligaciones, finiquitos, recibos, uso de nombres falsos, o de falsas calidades, empleando manejos fraudulentos para hacer creer en la existencia de falsas empresas, de un poder, o de un crédito imaginario, para infundir la esperanza o el temor de un suceso, accidente, o cualquier otro acontecimiento quimérico, o para abusar de otro modo de la confianza o de la credulidad, reprimiendo dichas conductas con prisión de seis meses a cinco años y multa de ocho a ciento cincuenta y seis dólares de los Estados Unidos de Norte América, y considerada la sanción con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, *el que cometiere el delito utilizado medios electrónicos o telemáticos*… Art. 563 del Código Penal.

La norma actual no considera al engaño como componente fundamental en la configuración del tipo penal como lo era en la antigua disposición legal, sino con la inducción al error de su víctima, con el fin de tener por efecto un acto conector con el derecho de propiedad, y que por ende patrimonialmente perjudicial, cambiando la verdad a través de la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, como bien lo instituye, sino más bien incorpora las modalidades a través de las que se comete este delito, dentro de la dogmática y criterios interpretativos propios de la estafa, convirtiéndolo en una nueva figura penal, guiada por la manipulación informática, con la orientación al engaño de la víctima para concretar el ánimo de lucro como elemento subjetivo completado con los elementos objetivos del hecho punible.

Si analizamos la estafa cometida por medios informáticos nos encontramos con indiscutibles divergencias entre la contemplada en el Art. 186 del COIP numerales 1 y 2, y la que recogía el Art. 563 del Código Penal, penúltimo inciso, pues en la norma actual se recogen las muchas modalidades estudiadas desde el proceder de las conductas delictivas en el país encuadrando en el tipo penal, siendo como ya se mencionó, el error que genera el acto de disposición en perjuicio de la propia víctima o de un tercero; en cambio subsisten los elementos subjetivos del dolo y el ánimo de lucro, incorporando en los numerales 1 y 2, las tarjetas de crédito como dispositivos electrónicos, como nuevas herramientas de la tecnologías para apoderarse de información.

Figura 12.

En materia de sistematización, una de las modalidades que se puede establecer en el primer inciso del artículo en mención, es a través de los SPAM, volviéndose sumamente difícil llegar a los delincuentes; por lo general, los spam o correos no deseados aparecen desde servidores que trascienden las fronteras de nuestro país, utilizando inclusive nombres falsos, direcciones obtenidas de forma ilícita, o bien recogidas en la web o tomadas de cadenas de mail que pueden llegar a ser la puerta de ingreso para un viable desfalco.

Figura 13.

De hecho en la web se concreta el scamming, proveniente del inglés Scam que significa “estafa” a través de correos electrónicos, con el fin de obtener dinero de la víctima de cualquier manera; una de las modalidades

más utilizadas es donde *"el escenario de estafa de viaje, donde un supuesto servicio de pareja ofrece contactos con mujeres de Europa del Este, los cuáles comienzan en el sitio y pasan rápidamente por contacto directo con la mujer deseada por correo electrónico, para más adelante continuar por teléfono, ella dice que no tiene teléfono, así que utilizarán un servicio de voz por internet o ella lo llamará a él". Finalmente la mujer solicita 1000 o 2000 euros para viajar al país de la víctima, estas estafas pueden durar varias semanas o meses, desde el primer contacto hasta el pedido del dinero, estableciendo el marco psicológico de credibilidad en la víctima…"* (Ramiro, 2010)

Figura 14.

SHUTTER: Conocido como el programa de captura de pantalla más avanzado, que radica en el manejo de cajeros automáticos, ocasionando en los mismos un estado de error en el software; los delincuentes informáticos implantan una lámina en la ranura de la salida del dinero y lo maniobran mediante un sensor, el cajero automático interpreta dicha condición de error, paraliza la transacción, y luego de abandonar la víctima el lugar observado por el delincuente, este acude al sitio de forma inmediata, recoge las bandas transportadoras y cumple el propósito de obtener dinero de forma ilícita.

Figura 15.

Se pueden mencionar un sinnúmero de modalidades al momento de buscar estafar a una víctima, desde la nueva concepción del tipo penal de estafa, así como también los instrumentos utilizados para el efecto, que ventajosamente el artículo 186 lo abarca, incluidos los realizados por medios telemáticos y de comunicaciones. A continuación se comparte información brindada por la Ingeniera Mirka Lorena León Álvarez, quien con su vasta experiencia como Jefe de Control de Fraude en el ámbito de telefonía móvil, resume los tipos de fraudes por telecomunicaciones que se encuadran en este tipo penal.

TIPOS DE FRAUDE

1. Fraude por suscriptor
2. Fraude Roaming
3. Fraude Refiling
4. Fraude By Pass
5. Fraude Dealer
6. Fraude Smishing
7. Fraude Reciclaje
8. Fraude Reventa
9. Fraude Interno
10. Control de Equipos robados

FRAUDES POR SUSCRIPCIÓN

Contratación de servicios sin intención de pago por bienes y servicios.

Tipos de fraude por suscripción

11. Uso de información personal de identificación falsa
12. Uso de identidad de otra persona/robo de identidad
13. Uso de la identidad de personas jurídicas
14. Presta nombres
15. Motivaciones:
    - Tiempo aire
    - Equipo
    - Comisión / bonificación

Algunos cambios comunes de la información personal son:

- El nombre está mal escrito
- Dirección ficticias
- Números telefónicos no coinciden con el lugar de trabajo o domicilio
- Referencias personales no existen

Figura 16.

PRESTA NOMBRES

- Préstamo del nombre a un tercero (defraudador) para acceder a los productos o servicios, sin intención de pago o de ocultar identidad real.
- Presta nombre recibe pago por parte del defraudador.
- Personas de difícil acceso domiciliario (rural, zonas peligrosas)
- Personas perfil crediticio Do E (bajos recursos) o tercera edad

Figura 17.

Figura 18.

Fraude por suscripción

Quiénes lo hacen

1. Clientes individuales/Gestores de cuentas
2. Delincuentes profesionales
3. Vendedores/Distribuidores
4. Empleados de la Operadora

Vulnerabilidades

- En aquellas áreas geográficas que tienen una concentración de actividad delictiva.
- En los mercados donde el nivel de competencia entre los operadores es muy alta.

- Donde el canal de distribución es ¨fragmentado¨ con proveedores de servicios y sub-agentes.
- Inaplicabilidad de sanciones
- Operadores de nuevos por la ausencia de experiencia en control y falta de datos históricos parqa la gestión de fraude.

Fraude Refilling

Proceso mediante el cual el país que origina el tráfico lo enruta hacia un país puente que no es el destino final y es este país quien re-enruta la llamada hacia el país destino.

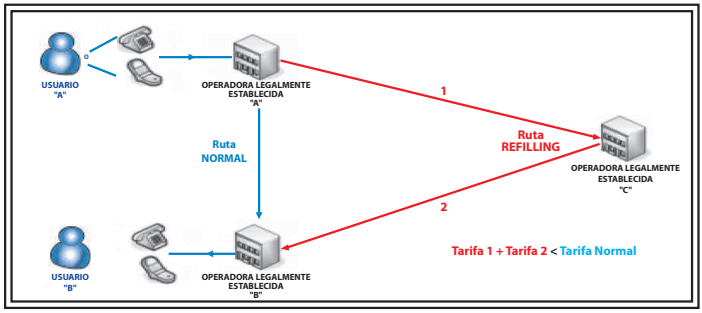


Figura 19.

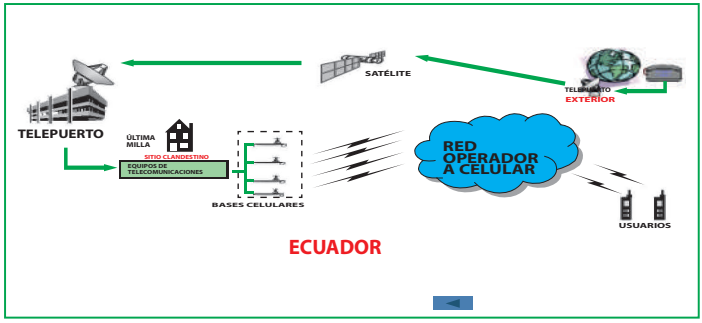


Figura 20.

Fraude Dealer

Se refiere a las actividades fuera del marco regular comercial de la cadena de ventanas para obtener beneficio propio, causando pérdidas a la compañía.

Tipos de Fraude Dealer

- Alteración de inventario

- Preativación de líneas
- Up Grandes/ Renovación ficticias

Fraude a través de mensajes de texto/Smishing

Es el uso del servicio de mensaje de texto de un operador, con el obejetivo de conseguir códigos de tiempon aire para su reventa y/o utilización.

La modalidad también se da para poder obtener datos personales de los abonados revelando claves, accesos, direcciones que ayudan al estafador para perpetrar nuevos fraudes.

Fraude a través de mensajes de texcto/Smishing

Quiénes lo hacen ?

- Reclusos
- Estafadores
- Personas naturales
- Vulnerabilidad
- Tecnología
- Falta de controles

Reventa

- Uso del servicios para comercialización a terceros. Esto es debido a que usualmente la oferta comercial de empresas es más atractiva que para personas naturales; esto promueve a que personas activen planes empresariales para la reventa individual.
- Otro tipo de reventa es usando líneas de prepago para revender en locutorios clandestinos.
- La reventa también se da cuando activan líneas a nombre de distribuidores o vendedores para a su vez revender a terceros.

Control de equipos robados

Las operadoras mantienes estrictos controles que aseguran que equipos reportados como robados con el mismo IMEI no se puedan activar, tales como:

- Línea directa sin costo para reporte de equipos robados.
- Manejo de lista negras.
- Limitaciones tecnológicas para la activación de equipos robados.
- Registo del IMEI en el EIR (Equipment Identity Register).

Es necesario indicar que la suplantación de identidad se encuentra ubicada en el capítulo de delitos contra el derecho a la identidad, bien jurídico protegido diferente al de la estafa, puesto que en nuestro país, tanto en los delitos de telecomunicaciones, delitos tradicionales y sobre todo en todo tipo de fraudes, el delito primario es suplantar identidad, es decir, primero habrá el fraude primario para luego proceder con los secundarios; por ejemplo, primero se suplantará identidad para obtener una línea pre-pago y posteriormente ejecutar delitos tradicionales como la extorsión, secuestros, intimidación, asesinatos, etc., o se suplanta identidad para beneficiarse ilícitamente de equipos de terminales móviles o servicios de telefonía e internet de manera ilícita; secuestro de cuentas con cambios de chip como nueva modalidad en nuestro país adoptada de otros estados. De hecho a nivel latinoamericano la suplantación de identidad es el primer fraude que afecta a la ciudadanía y directamente a las operadoras móviles, pues se evitan pagos después de la venta de equipos o se evade pasar por los controles que limitan a ciertos clientes de telefonía de obtener equipos de gama alta que son subsidiados. De igual manera, los tipos de fraudes detallados en líneas anteriores como roaming, relifing, by pass, en nuestro país el delito primario en la mayoría de los casos, será a través de la suplantación de identidad, adquiriendo chips con planes post pago, para evitar responsabilidades económicas y penales. Ventajosamente el artículo 212 del COIP, determina “cualquier forma” en la que estas nuevas peculiaridades informáticas, que aunque no estén tipificadas, sean parte de las innovaciones de delincuentes informáticos en la sociedad.

Artículo 212.- Suplantación de identidad.- La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años. (Penal C. O., 2014)

Delitos contra los Derechos del Buen Vivir

Delitos contra la Seguridad de los Activos de los Sistemas de Información y Comunicación

Art 230.- Interceptación Ilegal De Datos.-

Será sancionada con pena privativa de libertad de tres a cinco años:

1. *La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.*

2. *La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.*

3. *La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.*

4. *La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.*

Figura 21.

Según la Real Academia de la Lengua Española, interceptación significa *"detención o apropiación de algo antes que llegue a su destino"*, en cambio, ilegal expresa *"Que no está permitido por la ley",* es decir, que el tipo penal de interceptación ilegal refiere a apropiarse de forma ilícita de algo.

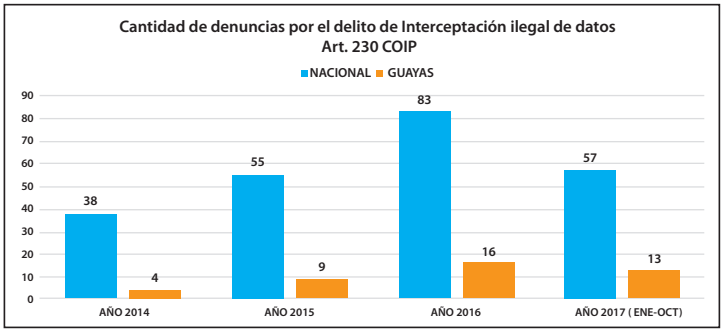


Figura 22.

Fuente: *Fiscalía del Guayas/Octubre 2017*

El articulado empieza indicando la sanción penal y luego en cuatro numerales resume qué tipo de conductas son las que serán castigadas, alude a "la persona" refiriéndose al sujeto activo, quien deberá ajustar el suceso de seguridad más dificultoso de descubrir, por producir una alteración en determinado sistema que va en contra de la confiabilidad, por ello es que las cuatro circunstancias se refieren a interrupción, apropiación, clonación y diseño o desarrollo de programas informáticos, como los vocablos primordiales más viables.

En general, el artículo protege el quebrantamiento a la seguridad informática lógica (software), como los contenidos y la información contenida en soportes informáticos y la física aplicada a los equipos como tal, la infraestructura informática (hardware).

El numeral 1 enfoca a la ilegalidad por falta de autorización (judicial), que va en contra de derecho, a pesar que en nuestra legislación, la interceptación es permitida con la autorización de un juez, tal como se señala en el artículo 456 del Código Orgánico Integral Penal, para atacar primordialmente el crimen organizado, con tiempos determinados. El tipo penal también está relacionado al Intrusismo Informático, pues la redacción se refiere a procedimientos efectuados por el delincuente consistente en el ingreso a sistemas de información o computadoras quebrantando medidas de seguridad reservadas a la protección de datos.

En general, se sanciona a "la persona" que acceda sin autorización a un ordenador de forma improcedente, a través de cualquier medio de forma virtual, ya sea dentro de un "espacio" que pertenece a otro como bien intangible, y el acceso no autorizado a un sistema cuya información es aprehendida y probablemente acopiada, para el posible cometimiento de un injusto penal, convirtiéndose en ataques que no solo vulneran bienes jurídicos protegidos por el Estado como la confidencialidad, la intimidad o reserva, sino aquellos delitos contra la seguridad de los activos de los sistemas de información y comunicación, que son de efectiva gravedad contra el conglomerado social.

Desde esa perspectiva, la filmación o la grabación de las conversaciones y comunicaciones telefónicas, se constituyen en una herramienta de investigación cuya autorización corresponde a miembros de la función jurisdiccional, con las debidas motivaciones del porque dicha solicitud, que habitualmente tiene la finalidad de obtener pruebas para la comprobación de hechos punibles graves y por consiguiente la vinculación de los presuntos responsables.

Los restantes numerales refieren a la variedad de modalidades existentes para la configuración del tipo penal, entre las que se mencionan las siguientes:

SKIMMING Es el robo de información de tarjetas de crédito utilizado en el

momento de la transacción, con la finalidad de reproducir o clonar la tarjeta de crédito o débito para su posterior uso engañoso. Consiste en el copiado de la banda magnética de dichas tarjetas.

Los escenarios comunes en los que se realiza skimming son restaurantes, bares, gasolineras o en cajeros electrónicos donde un sujeto está en posesión de la tarjeta de crédito de la víctima o en un lugar en el que se ha instalado un dispositivo que puede copiar la información.

En el caso de un cajero automático, el delincuente informático pone un dispositivo a través de la ranura para tarjetas, que tiene como objetivo leer la información de la banda magnética y la copia para su uso posterior. Estos dispositivos se utilizan a menudo en combinación con una microcámara que graba el código de seguridad del usuario. Lo único que hace el delincuente, es pasar la tarjeta por el lector.

Figura 23.

PHARMING es la explotación de una vulnerabilidad en el software de los servidores o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio.

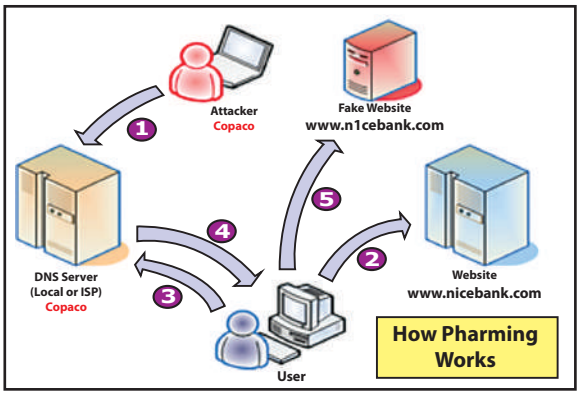


Figura 24.

SNIFFEO es la práctica de poder capturar tramas de información que viajan sobre la red. Toda la información que viaja sobre el internet y que llega a una terminal, como lo es una computadora, es capturado y analizado por dicho dispositivo. Sin embargo, un sniffer captura dicha información a la cual se le llama trama, y mediante una técnica llamada "inyección de paquetes" puede llegar a modificar, corromperla y reenviar dicha información. Con esto se logra engañar a los servidores que proveen servicios en internet.

Figura 25.

PHISING.- es utilizado como uno de los métodos para estafar, el término proviene de la unión de los vocablos en inglés: *password, harvesting* y *fishing*, "cosecha y pesca de contraseñas", pero la información confidencial obtenida

de forma fraudulenta, no solo se refiere a claves, sino también a números de tarjetas de crédito, de cuentas, entre otros, con la clara intención de apropiarse de dinero de cuentas bancarias, y si bien en la actualidad la modalidad persiste, ya no tiene el mismo efecto que hace años atrás, debido a la publicidad de las entidades bancarias, como a las alertas que llegan a través de diversos medios informáticos, como correos y mensajes de texto.

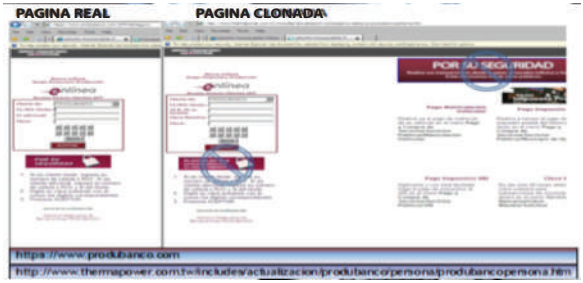


Figura 26.

Diferenciar un mensaje proveniente de phishing no resulta fácil para un usuario que haya recibido un correo de tales características, especialmente cuando efectivamente es cliente de la entidad financiera de la que supuestamente proviene el envío, ya que el mensaje de correo electrónico presenta logotipos o imágenes que han sido recogidas del sitio web real al que el mensaje fraudulento hace referencia.

De lo analizado se observa que el punto de vista de la función legislativa radicó en articular tipos penal detectados desde la realidad social, que se encuentran incorporados a las TIC (Tecnologías de la Información y Comunicación), concentrando notables modalidades o subtipos de figuras penales específicas ya existentes y concibiendo nuevas categorías de los denominados ciberdelitos, que de forma acelerada se propagan en nuestro país.

Delitos contra los Derechos del Buen Vivir

Delitos contra la Seguridad de los Activos de los Sistemas de Información y Comunicación

Art. 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:

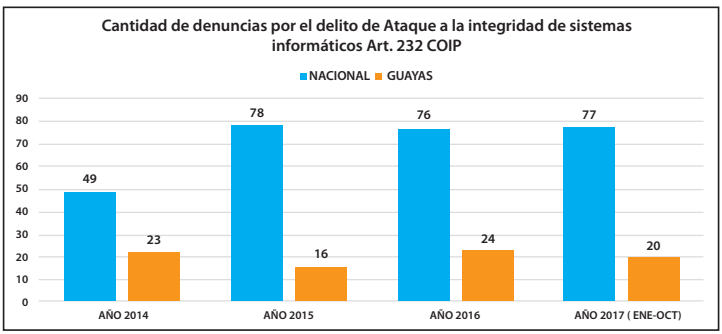


Figura 27.

Fuente: *Fiscalía del Guayas/Octubre 2017*

1. *Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.*

2. *Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.*

3. *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.*

Figura 28.

El artículo va asociado de forma directa al sabotaje informático, así el primer inciso lo conceptualiza de forma categórica a las operaciones criminales inmateriales, no visibles de forma física, sino virtual, que una vez verificadas las consecuencias, son muy difíciles de valorar. La presente tipificación en los numerales 1) y 2) enfocan dos aristas: primero describe el objeto de la destrucción congruente al software, a la destrucción de datos, programas o documentos, interrupción del funcionamiento de sistemas, que pude ir desde labores muy naturales como desconectar el ordenador de la electricidad, hasta diseñar un programa para tal fin, y el segundo ahora sí, a la destrucción de la parte física, hardware.

El numeral tercero recoge en cambio la gravedad de la sanción, cuando cualquiera de las dos conductas de los numerales precedentes se refiera a *bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana,* gravedad de daños informáticos que deberá evaluarse a través del valor de pérdida de funcionalidad del objeto del delito, asociada con la conducta desplegada por el autor, evidentemente el legislador pretendió imputar conductas asociadas a técnicas que permiten cometer sabotajes informáticos, desde un virus informático como un "malware", que tiene por objeto alterar la normal marcha de la computadora, sin el permiso o el conocimiento del usuario, dadas a través de una serie de instrucciones de programación que pueden adherirse inclusive a programas

legítimos, y propagarse a otros programas informáticos que destruyen de manera intencional los datos almacenados en una computadora.

Uno de los primeros virus transferidos vía correo electrónico, fue el MELLISA, creado el 26 de marzo de 1999, por David L. Smith, quien fue condenado a 10 años de prisión, pasando 20 meses en prisión y multado con 5.000 dólares, el que consistía en trasmitir en un correo electrónico como archivo adjunto, denominado "list.doc" y utilizando técnicas de ingeniería social que llegaban con el mensaje *"aquí está el documento que me pediste… no se lo enseñes a nadie*", que en poco tiempo protagonizó una infección masiva causando más de 80 millones de dólares de pérdidas.

Gusano informático. Tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

Bomba lógica o cronológica. Aquella que exige conocimientos especializados, ya que requiere la programación de la destrucción o modificación de datos. Es importante destacar, que a diferencia de los virus o gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; es por esta razón, que de todos los dispositivos informáticos criminales, la bomba lógica es la que más daño hace dentro del sistema informático. Es difícil saber cuál es el sujeto, por cuanto se puede programar la detonación para que tenga lugar mucho tiempo después de que se haya marchado el criminal informático.

El delito de sabotaje puede contener pérdidas económicas, tanto en empresas, instituciones públicas, privadas y gubernamentales, etc.

En el Código Penal anterior se contemplaban dos tipos penales que eran muy parecidos, pero con características propias, como la Destrucción Maliciosa de Información, recogido en el Art. 262 reformado del Código Penal decía:

"*Será reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiera maliciosa y fraudulentamente, destruido o suprimo documentos, títulos, programas,*

datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo… ”. (Penal C. I., 2014)

La importancia del bien jurídico protegido, la integridad de la administración pública, que constaba en el artículo anterior y en el actual, la vulneración a la seguridad de los activos de los sistemas de información y comunicación, justifica la agravada sanción contra el pésimo empleado público, que incurre en este delito calificado como destructor de la información, conocimiento y de la verdad en determinado aspecto o caso, así como el perjuicio causado en bienes destinados a la prestación de un servicio público.

De igual forma la Comisión de Codificación del Congreso Nacional de ese entonces (2002), consideró que la destrucción maliciosa de documentos ya referido en el 202 CP, no era lo mismo que daño informático y por ello consideró a continuación del 415 del Código Penal establecer otro tipo penal:

Art. ...- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica. La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculado con la defensa nacional.

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

Se diferenciaban entonces los daños informáticos de la destrucción maliciosa de información, en la calificación del sujeto activo, pues en el último mencionado debía necesariamente ser funcionario público, mientras que el primero cualquier ciudadano, además de que dicha destrucción de información en el 415 CP, no solo podía ser al software como parte lógica de la máquina, sino también a la parte tangible, como el disco duro o hardware.

Hoy por hoy, el artículo en estudio incluye las dos modalidades referidas.

Delitos contra los Derechos del Buen Vivir

Delitos contra la Seguridad de los Activos de los Sistemas de Información y Comunicación.

Art 190.- Apropiación Fraudulenta por Medios Electrónicos.-

La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para ***facilitar la apropiación*** *de un bien ajeno o que procure la* ***transferencia*** *no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona* ***alterando, manipulando o modificando*** *el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.*

La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.

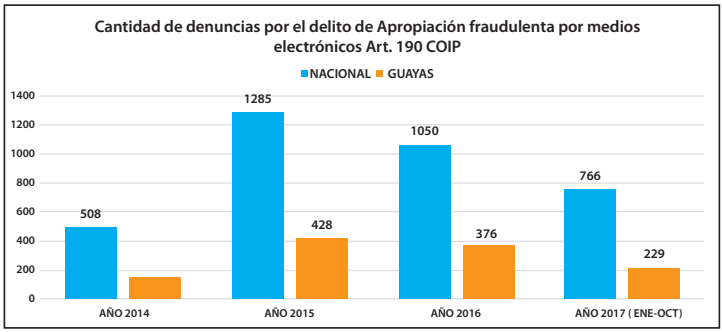


Figura 29.

Fuente: *Fiscalía del Guayas/Octubre 2017*

Art 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.

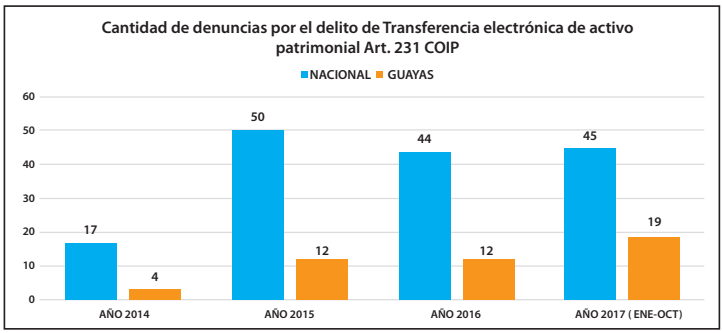


Figura 30.

Fuente: *Fiscalía del Guayas/Octubre 2017*

Los dos artículos en una lectura rápida son similares, sin embargo, hay diferencias entre el uno y el otro; el bien jurídico protegido es distinto, el uno afecta el legítimo derecho al patrimonio consagrado en la Carta Magna, considerado como el conjunto de los bienes de una persona visto desde un punto subjetivo y objetivo, por ser inalienable durante su vida, pero transmisible por causa de muerte conforme el Código Civil, encaminado el artículo a sancionar los actos premeditados e ilegítimos que causen menoscabo al patrimonio de otra persona, complementado con la utilización con el término "fraudulentamente", y el otro, la vulneración de la seguridad de los activos de los sistemas de información y comunicación; en los dos se habla de bienes materiales e inmateriales, en el 190 debe configurarse el traspaso, pues en este se refiere a la apropiación, mientras que en el 231 del funcionamiento para "procurar", que si bien tiene el mismo fin, una vez hecha la transferencia se configura el 190, que tiene un contexto virtual en el que se enfatiza como lugar de origen de los ataques a las computadores o servidores informáticos como instrumentos para consumación del delito, y las cuentas de las víctimas, la mayoría clientes de instituciones financieras, como destino de los embates en los que obtienen dineros entregados a los bancos, sin la desconfianza de recibir afectación a su patrimonio, lo que hace que socave la confianza de la ciudadanía.

Se puede aseverar de forma fehaciente, que la mayoría de las infracciones informáticas van encaminadas a la apropiación ilícita por medios informáticos, por ser el injusto penal de mayor periodicidad, existiendo numerosos modos para el efecto; Se puede mencionar la conocida circunstancia de SALLAMI, aprovechada por el delincuente en las reproducciones inconscientes de los procesos de cómputo y que se configura con la trasferencia mediante rodajas muy finas (céntimos de dinero), limitadamente visibles de transacciones financieras de una cuenta a otra, a través de ingreso ilegítimo a programas, dando instrucciones implícitas a una determinada cuenta desde varias de ellas.

Figura 31.

El Art. 231 refiere los verbos alterar, manipular o modificar, relacionados a cambiar las características, la esencia o la forma en el funcionamiento de programa o sistema informático o telemático, o mensaje de datos, perturbando o trastornando el estado normal del mismo, haciendo cambios o alteraciones en una cosa interesadamente, para conseguir un fin determinado, esto es procurarse o encaminar la conducta al traspaso o incautación no consentida de un activo patrimonial, modificando programas existentes en el sistema de computadoras o insertando nuevos programas o nuevas rutinas, manipulando, modificando o cambiando un dispositivo electrónico que concebirá la variación de alguna característica sin alterar sus cualidades o características esenciales, refiriéndose ya no a la posesión de una cosa en particular como lo hace el 190, sino a los bienes patrimoniales, bienes, derechos y obligaciones, que se agrupan en dos conjuntos de elementos patrimoniales o grandes masas patrimoniales, que en materia contable se habla de activos y pasivos, asociados al conjunto de bienes que tienen un mismo propietario y que si bien de alguna manera la transferencia afecta al patrimonio, el articulo 231 adquiere un carácter pluriofensivo concomitantemente a la apropiación no consentida que también transgrede el sistema informático, la libertad e intimidad personal, la titularidad del derecho intelectual, entre otros, y que sanciona además al sujeto pasivo actuante, de forma posterior a dicha vulneración que presta su cuenta o crea una falsa para que el delito de trasferencia se consuma a pesar de ser quien provoca ni la alteración, ni la manipulación peor las modificaciones.

En el Art. 231 COIP, la acción material no incurre sobre el ordenador o computador, denominado hardware (que como aparato físico, ya se encuentra protegido en otras figuras delictivas: hurto, robo, apropiación ilícita, daños, etc.), como ya se mencionó, sino sobre su aspecto específico, que contiene su sistema de soporte lógico, identificado con el concepto del software que se consuma cuando el infractor afecta los datos informáticos o el funcionamiento de un sistema informático de tercero, con el ánimo de apropiarse o lucrarse de forma personal o para terceros, una de aquellas modalidades factiblemente sería la modalidad de **CASH MANAGEMENT.**

Fuente: Fiscalía del Guayas /Octubre 2017

CASH MANAGEMENT: Servicios que tiene las instituciones para las transferencias bancarias de clientes empresariales, de la que los delincuentes informáticos se aprovechan para generar órdenes de pago no autorizadas, transfiriendo fondos de forma ilícita.

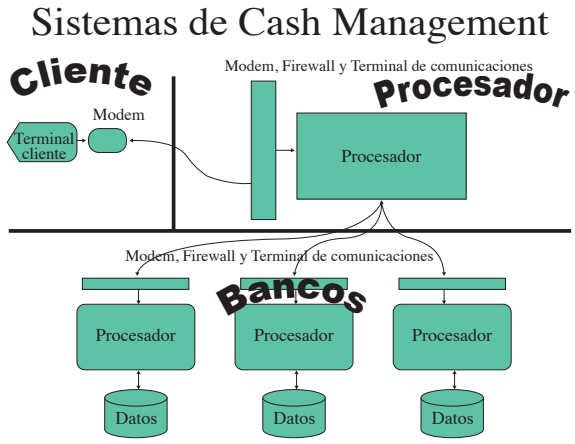


Figura 32.

El Art. 190 es muy afín al que había primariamente en el Código Penal, a continuación del Art. 553

Art. ...- Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información

o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1. Inutilización de sistemas de alarma o guarda;

2. Descubrimiento o descifrado de claves secretas o encriptados;

3. Utilización de tarjetas magnéticas o perforadas;

4. Utilización de controles o instrumentos de apertura a distancia; y,

5. Violación de seguridades electrónicas, informáticas u otras semejantes.

En todo caso la apropiación indebida no requiere un beneficio del sujeto activo, sino un perjuicio del sujeto pasivo, que rige en el tipo penal de apropiación fraudulenta, que conlleva a la distracción del dinero y la transferencia electrónica de activo patrimonial, que hace referencia al traspaso de bienes de un patrimonio a otro.

Delitos contra la Seguridad de los activos de los Sistemas de Información y Comunicación

Art 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.

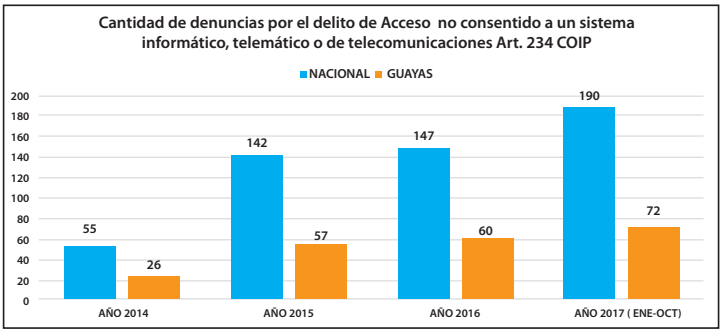


Figura 33.

Fuente: *Fiscalía del Guayas/Octubre 2017*

El bien jurídico vulnerado en esta norma penal es la transgresión en la seguridad de los activos de los sistemas de información y comunicación, especialmente desde el punto de vista de la privacidad, la cual puede ser observada desde la representación informativa y comercial.

Cuando analizamos la norma legal de acceso no consentido a un sistema informático, telemático o de telecomunicaciones, es necesario primero enfocar que existe acceso consentido, que va ubicado en la acción realizada por usuarios internos y externos dentro de un sistema de información, los que hacen uso del acceso con el permiso concedido por el dueño del sistema, como el caso de las redes sociales públicas, en las que el ingreso es plenamente permisible. En cambio, el artículo en examen sanciona el acceso en contra de la voluntad de quien tenga el legítimo derecho, precautelando en la sociedad la relación entre las personas en todos los niveles existentes, porque enfoca sistemas telemáticos que encierra amplia gama de las comunicaciones originadas con el internet, todo dispositivo electrónico (software y hardware) y los sistemas de telecomunicaciones que incluyen infraestructura física y lógica, que consiente un transporte adecuado de la información, en cualquier medio (sea mensajes de datos, de voz, etc.).

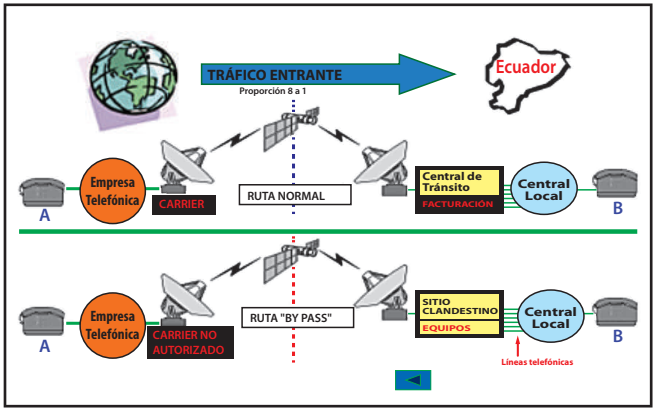
"…Debe entenderse que un sistema informático es un valor en sí mismo. La dimensión *informática se configura como un nuevo espacio social, político y económico, que tiene como característica esencial su incorporeidad. En la red telemática lo esencial es el acceso y la información que suministra, de manera que la dificultad o la negación a este acceso puede suponer una limitación vital para las interrelaciones humanas…"22*

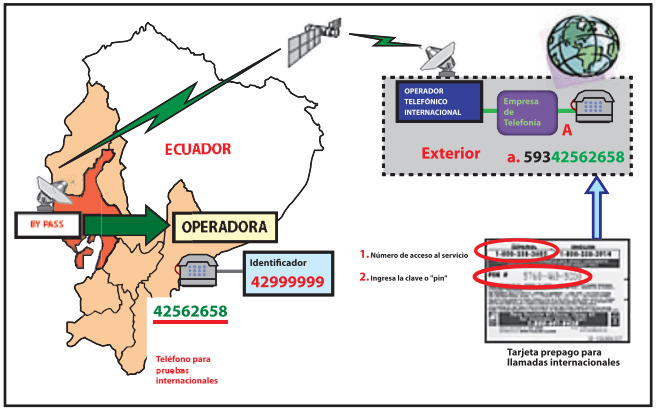
El aprovechamiento ilegítimo radica en la obtención de beneficios diferentes por los que fuera desarrollado el sistema, utilizado para obtener varias ventajas a través de manipulación de bases de datos y como consecuencia obtener o alterar información contenida en ellas, tratando de perjudicar o beneficiar a terceros, redireccionando el código fuente o de la interfaz de usuario de cualquier sistema con acceso al internet, para alterar su funcionamiento o su diseño, y hacer que la misma se dirija a un receptor completamente diferente que legítimamente sea designado.

Aprovecharse de los servicios sin pagar a los proveedores legítimos, es ejecutar acciones inclinados a obtener réditos económicos; un ejemplo claro y frecuente en nuestro país es la conocida modalidad de delito de "by pass", que constaba en el artículo 422 del antiguo Código Penal, definido como aquel sistema conformado por un enlace internacional, una instalación de equipos de telecomunicaciones y **líneas telefónicas; cuya interconexión permite establecer una ruta ilegal por la cual se cursa tráfico telefónico internacional, prestando así un servicio de telecomunicaciones sin contar con** la correspondiente autorización y toman posesión clandestina de instalaciones que, por su configuración y demás datos técnicos, hagan presumir que entre sus finalidades, está la de destinarlos a ofrecer los servicios señalados en el inciso anterior, aún cuando no estén siendo utilizados, de alguna manera puede situarse dentro de este tipo penal, a pesar que las sanciones penales deben ser aplicadas sin perjuicio de las responsabilidades administrativas y civiles previstas en la Ley Especial de Telecomunicaciones y sus reglamentos.

En la singularidad expresada, el acceso se efectúa desde un lugar exterior, ubicado en la red de telecomunicaciones, aprovechado por el delincuente debido a la falta de severidad de las medidas de seguridad, ausencias de

medidas modernas de seguridad haciéndose pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de sustento que están en el propio sistema.





En nuestro país, las operadoras de telefonía y comunicación móvil, disponen de un registro de cada uno de sus usuarios del servicio celular, que empezó en el 2009, con el denominado “empadronamiento”, como parte de un convenio estatal a través de las instituciones encargadas de vigilar las telecomunicaciones en Ecuador y los representantes de las proveedoras de servicios en calidad de empresas privadas. El empadronamiento consiste en conocer la identificación real del propietario de la línea telefónica, quien debe

someterse al respectivo registro de forma ágil y dinámica a fin de garantizar la continuidad de los servicios, tanto en la modalidad de la línea contratada en el plan tarifario, como de las líneas prepago, obviamente que en dicho compromiso, las operadoras no serán responsables de la autenticidad de la información que sus usuarios les proporcionen, pero deberán garantizar la confidencialidad de la misma a excepción de peticiones de juez competente.

Las figuras penales que se van analizar consecutivamente se encuentran dentro del capítulo de conductas que contravienen el derecho a la propiedad, entendiendo que las mismas una vez efectuadas, tiene como propósito apropiarse de cosa ajena. Sin embargo, es bueno establecer que la telefonía celular puede en ocasiones ser el medio para la consumación de delitos tradicionales como: asesinatos, secuestros, intimidación, apropiaciones indebidas, etc.

Se considera que el espíritu de las normas penales antes referidas, fueron proteger a las personas individuales o jurídicas que se dedican a la venta al público de equipos terminales nuevos o usados, quienes a más de cumplir con los requerimientos de ley, tanto para el registro como para la comercialización, ya sea distribución y/o venta previstos en la ley con la respectiva documentación, marca, modelo, forma de pago etc., son víctimas de las diversas formas de evadir dichos controles y dedicarse a la venta libre de teléfonos, o lo que es peor, comercializar aparatos hurtados dentro y fuera del territorio nacional. Es por ello la importancia de contar con tipos penales que sanciona conductas de idemación, compra, modificación, utilización, porte, adquisición o cualquier forma de propiedad de equipo terminal móvil, que asome en la Base de Datos Negativa.

Artículo 191.- Reprogramación o modificación de información de equipos terminales móviles.- La persona que reprograme o modifique la información de identificación de los equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años.

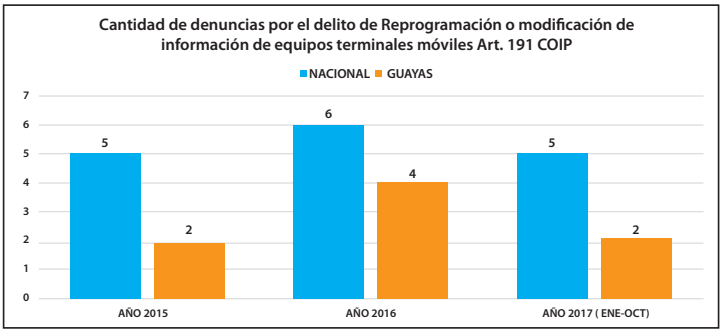


Figura 34.

Fuente: *Fiscalía del Guayas /Octubre 2017*

El tipo penal en análisis, consiste en la tarea de reformular los programas a través de la comprobación y examen de procesos de sistematización ilegítimos, que al igual que la modificación, cambia su disposición o alguna característica, alterando sus condiciones o características originales.

Una de las más habituales y destacadas modalidades de reprogramación o modificación de información de celulares es mediante el flasheo, que trasforma el software interno del mismo con el ingreso de códigos que se ajusta a otra versión. **Reflexeo,** modificación o blanqueo de los terminales, que viene a constituirse en el cambio o alteración del IMEI original con el que viene del fabricante, que contiene la identificación del equipo. La peculiaridad del reflexeo es blanquearle o cambiarle su identidad original para que sea utilizable, recordando que el IMEI es único por cada terminal, tiene un código único pregrabado en los teléfonos móviles que identifica al aparato de forma exclusiva a nivel mundial, que es trasferido por dicho aparato a la red cuando se conecta a esta, de tal manera que las operadoras cuando el cliente denuncia el bloqueo sea por robo o hurto proceden con el bloqueo a nivel de red, teniendo como efectos la inhabilitación del IMEI, y por consiguiente no se podrá utilizar. En el mercado negro se utiliza el reflexeo o modificación del IMEI original por uno genérico, o por otro, que este liberado con lo cual el equipo va a tener las funcionalidades operativas para tener voz, datos, SMS, pero con otro IMEI.

El gobierno y el estado están impulsando el Programa de "Listas positivas" que se refieren a un registro a nivel nacional de todos los IMEI que son autorizados e importados legalmente, para que puedan ser usados dentro de la red de tres operadoras móviles autorizadas: CONECEL, OTECEL Y CNT; así como las operadoras y el Estado poseen programas muy severos de "listas negativas", que consisten en incluir información sobre los equipos que han sido bloqueados por robo o hurto a los clientes, para evitar que se continúen comercializando, siempre y cuando el cliente lo denuncie. Debido a que en nuestro país no existe la obligación de denunciar, pues simplemente se puede llamar a la operadora móvil para solicitar el bloqueo.

También se puede asociar como modalidad, el utilizar bajo la ingeniería social, cuando el delincuente informático, conociendo los datos básicos llame o solicite a la operadora por cualquier vía, sea call center u otro medio, solicitando la liberación de los equipos, y a pesar de no estar reprogramando o modificando el equipo como tal, al valerse de la ingeniería social proceder a liberar el equipo y como resultado, poder utilizarlo.

Artículo 192.- Intercambio, comercialización o compra de información de equipos terminales móviles.- La persona que intercambie, comercialice o compre bases de datos que contengan información de identificación de equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años.

Debido al sinfín de delitos como robo, venta, contrabando, activación de equipos móviles de forma ilegal, hurto, transferencias ilícitas, entre otros; deben ser las consideraciones de los asambleístas para contemplar dentro de los delitos contra la propiedad el precedente artículo, pues hoy en día, el instrumento para obtener información confidencial de bases de datos de millones de personas, se pueden conseguir con mucha facilidad; si bien es cierto que las bases como tales son legales e instituidas por asociaciones, compañías, empresas serias que quieren o deben almacenar información financiera, comercial etc., el inconveniente radica en dos elementos esenciales: cómo se consigue dicha información y el uso que se las dé, debido a que información privilegiada puede pasar a manos de organizaciones criminales para de forma posterior negociarlas con fines delictivos.

En nuestro país la apoderada de conservar el listado consolidado de la base de datos que contiene información de identificación de equipos terminales móviles es la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), adscrita al Ministerio rector de las Telecomunicaciones y de la Sociedad de la Información, entidad encargada de la administración, regulación y control de las telecomunicaciones y del espectro radioeléctrico y su gestión, así como de los aspectos técnicos de la gestión de medios de comunicación social que usen frecuencias del espectro radioeléctrico o que instalen y operen redes.

Partiendo de este concepto, es necesario establecer que solo, ARCOTEL, contiene el consolidado de la base de datos con la información de identificación de equipos terminales móviles y de todas las operadoras de servicios de internet, como OTECEL (Movistar), CONECEL (Claro), y CNT, que de alguna manera se denomina "lista blanca" y por tanto, cualquier persona natural o jurídica que intercambie, comercialice o compre estos equipos, encuadran su conducta en el tipo penal examinado.

Artículo 193.- Reemplazo de identificación de terminales móviles.- La persona que reemplace las etiquetas de fabricación de los terminales móviles que contienen información de identificación de dichos equipos y coloque en su lugar otras etiquetas con información de identificación falsa o diferente a la original, será sancionada con pena privativa de libertad de uno a tres años.

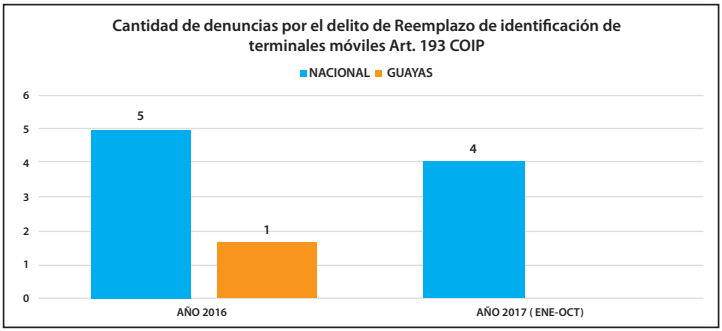


Figura 35.

Fuente: *Fiscalía del Guayas /Octubre 2017*

Artículo 194.- Comercialización ilícita de terminales móviles.- La persona que comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

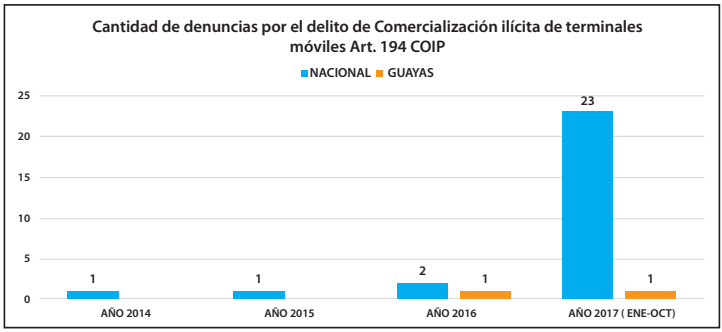


Figura 36.

Fuente: *Fiscalía del Guayas /Octubre 2017*

Los artículos antepuestos se relacionan, no con información, sino con el reemplazo de la identificación, a través de etiquetas falsas, así como la comercialización de los mismos.

Artículo 195.- Infraestructura ilícita.- La persona que posea infraestructura, programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil, será sancionada con pena privativa de libertad de uno a tres años.

Finalmente, el artículo 195 recoge los anteriores articulados, ubicando a la posesión ilegal de infraestructura con equipos electrónicos, celulares, programación, para modificar o alterar la información de conductas conducentes de manera indiscutible al cometimiento de un injusto penal.

Capítulo 3

CONSIDERACIONES GENERALES SOBRE LA OBTENCIÓN DE PRUEBAS EN INFRACCIONES INFORMÁTICAS CONTEMPLADAS EN EL COIP

La comunicación se ha definido como el intercambio de información de todo tipo, *pública privada, confidencial,* opiniones, sentimientos, etc., comunicación que puede darse a través de correos electrónicos, pizarra compartida, foros de debate, tablón de anuncios, videoconferencias, chat, etc. La información es resguardada tanto por el marco constitucional, como el procesal. De tal manera, que la comunicación no puede ser ni utilizada, ni intervenida por personas impropias a su dueño. Y si las mismas tienen orden judicial, deben estar sujetas a intervenciones adecuadas, siguiendo los correctos procedimientos.

Dentro de las actuaciones y técnicas especiales de investigación, se contempla un articulado relacionado con comunicaciones o datos informáticos que de ningún modo trasgrede principios, derechos y garantías constitucionales, sino más bien vislumbra instrucciones en favor de tales principios, derechos y garantías, con la finalidad de impedir delitos mayores, relacionado con convenios supra nacionales, como el Convenio de la Unión Europea sobre asistencia judicial en materia penal de 2000, que regula intervención de toda clase de comunicaciones de última generación, como las de satélite y telemáticas, a efectos de una investigación penal correcta y eficaz.

En el Código Orgánico Integral Penal se establecen, técnicas especiales de investigación, que se emplean como un instrumento necesario para examinar delitos a través de sistemáticas generales de indagación en la típica delincuencia ordinaria, entre las que estarían versiones, reconocimientos de lugar, experticias de evidencias, psicológicas, médicas, sociológicas, reconstrucción de los hechos, interceptaciones, etc., y técnicas específicas como reconocimiento en un entorno virtual, electrónico como una de las características de la investigación de los delitos informáticos, distinguiéndose accesos sistemáticos de ataques a bienes jurídicos tradicionales y nuevos como interceptación ilegal, transferencia de bienes, sabotaje, espionaje entre otras, a la vez que pueden utilizar algunas diligencias que hasta la

promulgación del COIP, no eran utilizadas, como se observa en el artículo 476, numeral 4) COIP, en lo que tiene que ver con soportes informáticos que contribuyeron a mantener una Política Penal relacionada con el desarrollo de la Sociedad de la Información y la masificación del uso de las Tecnologías de la Comunicación y la Información.

Artículo 476.- Interceptación de las comunicaciones o datos informáticos.-

La o el juzgador ordenará la interceptación de las comunicaciones o datos informáticos previa solicitud fundamentada de la o el fiscal cuando existan indicios que resulten relevantes a los fines de la investigación, de conformidad con las siguientes reglas:

4. Previa autorización de la o el juzgador, la o el fiscal, realizará la interceptación y registro de los datos informáticos en transmisión a través de los servicios de telecomunicaciones como: telefonía fija, satelital, móvil e inalámbrica, con sus servicios de llamadas de voz, mensajes SMS, mensajes MMS, transmisión de datos y voz sobre IP, correo electrónico, redes sociales, videoconferencias, multimedia, entre otros, cuando la o el fiscal lo considere indispensable para comprobar la existencia de una infracción o la responsabilidad de los partícipes.

Por otro lado, se conoce que con el cometimiento de un delito penal, lo primero que surge en el procedimiento es identificar la materialidad de la infracción, con más énfasis cuando ya se encuentra en etapa de juicio, en la 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, debiendo tener un nexo causal entre la prueba y sus elementos que se sintetiza en la dependencia entre la infracción y la persona procesada, basados en hechos reales introducidos o que puedan ser introducidos a través de un medio de prueba y nunca, en presunciones, conforme los artículos 474 y 475 del COIP, razón por la que en los sistemas procesales es imposible prescindir de la identificar del cuerpo del delito o la exteriorización del acto reprochable con todas las condiciones que lo acompañaron en su realización.

En materia informática existe multiplicidad de dificultades al momento de obtener pruebas tales como:

- Facilidad para maniobrar, simular o cambiar la evidencia.
- Manipulación de la existencia, origen y contenido de prueba
- No se respeta cadena de custodia desde que se extrae y recaba hasta su aportación en juicio.
- Problemas al momento de asegurar y garantizar la autenticidad e integridad de las pruebas.
- Eliminación de datos, así como su modificación, distorsión o manipulación.
- Desconocimiento de la materia y de las herramientas y posibilidades técnicas.
- Complejidad del uso de medios o dispositivos electrónicos o telemáticos.
- Falta de comprensión unos conocimientos técnicos especializado, entre otros.

Medios De Prueba

Conforme el artículo 498 del COIP, se establecen tres medios de prueba:

1. El documento
2. El testimonio
3. La pericia

Perito

- El vocablo perito proviene de latín peritus y significa "sabio, experimentado, hábil", *"el que poseyendo especiales conocimientos teóricos y prácticos, informa bajo juramento al juzgador sobre puntos litigiosos en cuanto se relacionan con su especial saber o experiencia"*

Los peritos son terceras personas, competentes en una ciencia, arte, industria o cualquier forma de la actividad humana, que dan conocimientos

respecto de alguno de los hechos que se investigan en la causa y se relacionan con su actividad.

Con la aparición de la tecnología en la sociedad, como herramienta fundamental de la comunicación, también surge la imperiosa necesidad de instituir nuevos perfiles profesionales en materias nuevas como las infracciones informáticas, versados en el plano de las nuevas tecnologías, que realicen análisis de los diversos elementos informáticos, así como en la exploración de datos que alcancen la categoría de evidencia y luego prueba digital para esclarecer los hechos dentro de un proceso penal, que proveerá conocimientos y razonamientos a Fiscales, Jueces de primer nivel, tribunales penales, jueces de salas provinciales o nacionales, que ciertamente requieren precisar información específica que usualmente es inexplorado.

El peritaje es el examen y estudio que realiza el perito sobre el problema encomendado para luego entregar su informe o dictamen pericial con sujeción a lo dispuesto por la ley.

El Art. 76 Constitución del Ecuador, Numeral 7 literal j): Quienes actúen como testigo o peritos están obligados a comparecer ante la jueza, juez, o autoridad y a responder al interrogatorio respectivo.

Principios Básicos del Peritaje son:

- Objetividad
- Autenticidad y conservación
- Legalidad
- Idoneidad
- Inalterabilidad
- Documentación

El campo investigativo de los delitos informáticos, no excluye de ninguna manera “un cuerpo del delito”, todo lo contrario, sin éste no habría injusto penal, razón por la que la utilización de la ciencia y de la tecnología en la recopilación de evidencias, se ha desarrollado en forma progresiva, examinar

la escena del crimen o lugar donde se halla el resultado de la infracción, se lo hace mediante reconocimiento y un estudio eficaz.

El COIP en el artículo 500, añadió en la parte adjetiva, el contenido digital, lo que es de gran importancia para la legislación ecuatoriana, no solo porque ya contamos con normas sustantivas en materia de delitos informáticos que requieren de análisis analógico, sino porque estamos sintonizados con la tecnlobalizacion, si consideramos que hoy en día la información se almacena, se copia, se divulgada y se utilizada mediante redes de telecomunicación y herramientas TIC, en amplio contenido digital, como: imágenes, vídeos, audios, textos, software, aplicaciones, videojuegos, portales, blogs, foto blogs, redes sociales, por lo que es significativa la figura procesal mencionada, más aun cuando la Informática Forense, como herramienta y técnica, es la más utilizada para la ejecución de análisis forense en los diversos dispositivos de carácter informático.

Art. 500 COIP:*"El contenido digital es todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí. En la investigación se seguirán las siguientes reglas:*

1. *El análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de técnicas digitales forenses.*
2. *Cuando el contenido digital se encuentre almacenado en sistemas y memorias volátiles o equipos tecnológicos que formen parte de la infraestructura critica del sector público o privado, se realizará su recolección, en el lugar y en tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.*
3. *Cuando el contenido digital se encuentre almacenado en medios no volátiles, se realizará su recolección, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.*

4. *Cuando se recolecte cualquier medio físico que almacene, procese o transmita contenido digital durante una investigación, registro o allanamiento, se deberá identificar e inventariar cada objeto individualmente, fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará mediante cadena de custodia a un centro de acopio especializado para este efecto.*

Figura 37.

El articulado mencionado va de la mano con la informática forense que en el Código de Procedimiento Penal anterior no estaba contemplado. El COIP lo aprecia como respuesta a aquellas necesidades específicas y acopladas al nuevo marco jurídico sustantivo penal, tales como la obtención de pruebas electrónicas mediante el análisis forense consistente en el conjunto de técnicas reservadas a la extracción de información única de cualquier soporte informático, sin alterar el estado de los mismos, que permitirá buscar y recabar datos, y sobre todo establecer un patrón de comportamiento para descubrir información que probablemente estaría encriptada y que servirá para comprobar la materialidad de la infracción.

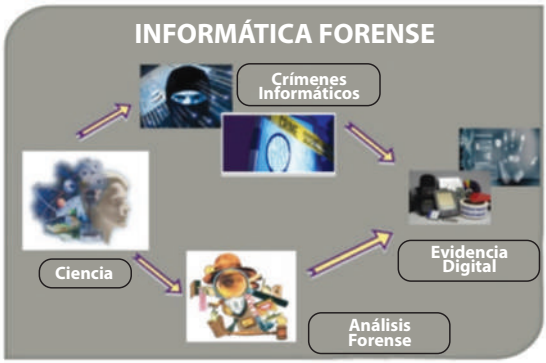


Figura 38.

Extracto conceptual de Informática Forense

La ciencia informática data de los años 40, es una de las más recientes.

- Su evolución e integración en la sociedad ha sido muy rápida.
- 40s: Se investiga para saber qué es computable.
- 60s: Se investiga para reducir costos y potencia.
- 80s: Se investiga para hacer fiable y robusta.
- 00s: Se investiga cómo controlar qué hacen los usuarios con los ordenadores y qué sucede dentro de estos.
- 01s hasta la actualidad. Control total. Se quiere investigar y monitorizar la actividad en los Sistemas de Información e Internet.

La Informática Forense no aparece a causa de Internet.

- "Al principio no había redes".
- LOS VIRUS FUERON LOS PRIMEROS "INVESTIGADOS": 90S.
- La I.F. se inicia con la Ingeniería Inversa,
- Con la apertura de las redes a los usuarios cambia la casuística.
- A finales de los 90 y principios del milenio, la cantidad de redes interconectadas facilita delitos informáticos.

- Ahora sí existen delitos propios sólo de Internet (Intrusiones en sistemas, robo mundo físico).
- La gente miente, roba, falsifica, escucha, ataca, destruye y hasta organiza asesinatos y actos terroristas.

El Objetivo de la Informática Forense, es recobrar registros y mensajes de datos existentes dentro de un equipo informático, de tal manera que toda esa información digital, pueda ser usada como prueba en juicio, siendo la ciencia de: adquirir, preservar, obtener, presentar datos que hayan sido procesados electrónicamente y almacenados en soportes informáticos, y cuando los mismos hayan sido instrumentos del cometimiento de injustos penales informáticos necesitan ser recuperarlos y legalizarlos para poder utilizarlos en investigaciones y procesamientos penales como prueba legalmente conseguida, sobre todo porque no es una tarea fácil, dada la naturaleza volátil y la facilidad de manipulación, falsificación, protección tecnológica o eliminación de los datos electrónicos como ya se mencionó, y por tanto deben ser realizados por forenses informáticos, quienes desarrollando y utilizando protocolos científicos y procedimientos para investigar ordenadores, analizan y mantienen la autenticidad de los datos recuperados.

A petición de los expertos del G8, la Organización Internacional de Prueba Informática (OIPI), acordó entre los países miembros, elaborar recomendaciones sobre normas, incluida la definición de métodos, técnicas de identificación y términos comunes, que deben utilizarse para descubrir infracciones informáticas con el establecimiento de un formato común para las peticiones forenses.

La Informática Forense admite solución de conflictos tecnológicos conexos con seguridad informática y protección de datos, en los que la ciudadanía obtiene contestación a violación de privacidad, competencia desleal, fraude, robo de información confidencial y/o espionaje, apropiación ilícita, surgidos a través de uso indebido de las tecnologías de la información, ya que mediante sus procedimientos se identifican, aseguran, extraen, analizan y presentan pruebas generadas y guardadas electrónicamente, para que puedan ser aceptadas en un proceso de forma legal.

"Una de éstas herramientas es la Informática Forense, ciencia criminalística que, sumada al impulso y utilización masiva de las tecnologías de la información y de la comunicación en todos los ámbitos del quehacer del hombre, está adquiriendo una gran importancia, debido a la globalización de la sociedad de la información. Pero a pesar de esto esta ciencia no tiene un método estandarizado, razón por la cual su admisibilidad dentro de un proceso judicial podría ser cuestionada, pero esto no debe ser un obstáculo para dejar de lado esta importante clase de herramienta, la cual debe ser manejada en base a rígidos principios científicos, normas legales y de procedimiento…". (Santiago, 2010)

Es necesario dentro de la investigación a los sistemas de información, conseguir la detección inmediata de evidencias que han vulnerado los sistemas informáticos, mediante metodologías forenses que incluyen el almacenamiento seguro de datos en diferentes medios y evidencias digitales, sin alterar los datos de origen. Cada fuente de información se cataloga preparándola para su posterior análisis y se documenta cada prueba aportada. Las evidencias digitales recabadas permiten elaborar un pronunciamiento claro, conciso, fundamentado y con justificación, para elevar de ser el caso, de indicios de convicción a pruebas legítimamente operadas.

Cabe señalar que la informática forense también tiene finalidad preventiva, como la auditoría a través de la práctica de numerosas ensayos sistemáticos, en que los mecanismos de protección son situados para la seguridad de métodos de información, que permitirán detectar las vulnerabilidades del sistema de seguridad, con el fin de corregirlas.

Al igual que en cualquier otro delito estipulado en el Código Orgánico Integral Penal, los delitos informáticos también poseen un mecanismo muy específico para el reconocimiento de pruebas que certifiquen lo que en realidad sucedió; la diferencia del delito tradicional radica en que la evidencia es digital y por tanto, se convierte en la herramienta con la que se vulnera un bien jurídico; asemejando con características de un delito habitual, para un asesinato el puñal o la pistola pueden ser útiles para la ejecución del hecho, en cambio para un hacker o cracker, la computadora o cualquier soporte electrónico serán el medio o el fin de delinquir, razones suficientes para determinar que en

investigaciones donde existen medios informáticos no puede ser realizada por cualquier persona sino por aquellos que posean conocimientos sobre materia electrónica, que sigan pasos relacionados y concretos como: identificación del incidente, recopilación y preservación de evidencias, análisis de la evidencia o análisis forense.

Análisis Forense

Es la técnica utilizada generalmente para la prevención y detección de fraudes de una manera técnica mediante un proceso estructurado, donde intervienen peritos especializados como contadores, auditores, abogados, investigadores, informáticos entre otros.

En el caso de informáticos, su finalidad por lo general será obtener mediante la reproducción exacta de un disco, que subsiguientemente le permitirá acceder a los sistemas de archivos vulnerados, inspeccionar todo tipo de información almacenada tales como: cuentas de usuario, documentos, programas, entre otros, logrando la recuperación inclusive de archivos borrados o datos incompletos, provenientes de chat, correos electrónicos, redes sociales, que se convertirán en evidencia para el Fiscal o las partes y posteriormente, en prueba que será expuesta en etapa de juicio.

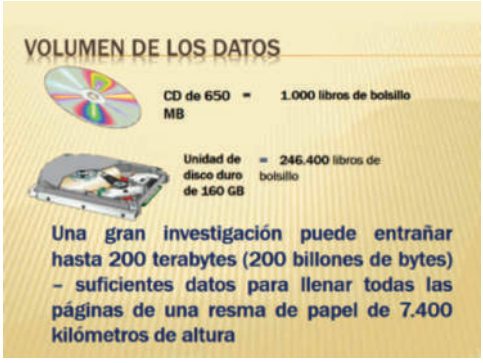


Figura 39.

Evidencia Digital (software)

Cuando su posesión no está autorizada por la Ley, como por ejemplo, pornografía infantil, copias pirateadas de programas de ordenador, secretos industriales robados.

Es un instrumento o herramienta usada como medio para cometer infracción, como por ejeplo los programas de ordenador que se utilizan para romper las seguridades de un sistema informático, romper contraseñas o brindar acceso no autorizado.

Información almacenada digitalmente que puede llegar a ser utilizada como prueba en un proceso judicial.

Para que esto sea viable, será necesario seguir procedimientos en su recuperación, almacenamiento y análisis. Es muy importante seguir una cadena de custodia lo suficientemente robusta y que permita asegurar la conservación de la evidencia digital.

Evidencia Electrónica (Hardware)

Cuando su posesión no está autorizada por la ley, por ejemplo: Decodificadores de la señal de televisión por cable, robo hurto, fraude.

La evidencia electrónica es usada como un arma o herramienta y pueden ser:

Snifers, Skimming, Scanner, Computador de escritorio, Computador portátil, Estación de trabajo, Hardware de red, Servidor, Teléfono celular, Aparato para identificar llamadas, Localizados beeper, GPS, Cámaras, videos, Sistemas de seguridad, Memoria flash, Palm, Juegos electrónicos, Sistemas en vehículos, Impresora, Copiadora, Grabadora, Videograbadora DVD, Duplicadora de discos, Discos, disquetes, cintas magnéticas, Aparatos lícitos (sniffers, decodificadores, etc.).

Figura 40.

Cadena de Custodia

Esta expresión es un término legal que se refiere a la capacidad de garantizar la identidad e integridad de un espécimen o evidencia, desde su obtención durante su análisis, hasta el final del proceso.

En la práctica, consiste en salvaguardar la evidencia, de forma documentada, de forma que se eviten alegaciones de que la evidencia ha sido modificada o alterada durante el proceso de la investigación. La cadena de custodia es un conjunto de pasos o procedimientos seguidos para preservar la prueba digital, que permita convertirla y usarla como evidencia digital en un proceso judicial. El COIP, consideró como nueva figura procesal a la cadena de custodia

Artículo 456.- Cadena de custodia.- *Se aplicará cadena de custodia a los elementos físicos o contenido digital materia de prueba, para garantizar su autenticidad, acreditando su identidad y estado original; las condiciones, las personas que intervienen en la recolección, envío, manejo, análisis y conservación de estos elementos y se incluirán los cambios hechos en ellos por cada custodio. La cadena inicia en el lugar donde se obtiene, encuentra o recauda el elemento de prueba y finaliza por orden de la autoridad competente. Son responsables de su aplicación, el personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, el personal competente en materia de tránsito y todos los servidores públicos y particulares que tengan relación con estos elementos, incluyendo el personal de servicios de salud que tengan contacto con elementos físicos que puedan ser de utilidad en la investigación.*

La cadena de custodia evidencia lo siguiente:

- Quién obtuvo la evidencia.
- Dónde y cuándo la evidencia fue obtenida.
- Quién protegió la evidencia.
- Quién ha tenido acceso a la evidencia.

Cooperación Internacional, Convenio de Budapest

El convenio de Budapest, es el primer Tratado Internacional que trata en particular las infracciones de derechos de autor, fraude informático, pornografía infantil, los delitos de odio y violaciones de seguridad de red.

Su principal objetivo, que figura en el preámbulo, es aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional.

Fue elaborado por el Consejo de Europa en Estrasburgo, con la participación activa de los estados observadores de Canadá, Japón y China.

El Convenio y su Informe Explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa, el 8 de noviembre de 2001. El 23 de noviembre de 2001 se abrió a la firma en Budapest y entró en vigor el 1 de julio de 2004.

A partir del 28 de octubre de 2010, 30 estados firmaron, ratificaron y se adhirieron a la Convención, mientras que otros 16 estados firmaron la Convención, pero no la ratificaron.

El Convenio es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, también contiene una serie de competencias y procedimientos, tales como la búsqueda de las redes informáticas y la interceptación legal.

En el 2001, 30 países firmaron el convenio de Budapest; con este convenio pretenden coordinar la lucha para erradicar el terrorismo, que a su vez será el primer instrumento jurídico que incorpora a internet como objeto de obligaciones y sanciones.

La convención de Budapest del 2001, tuvo como principal objetivo establecer reglas claras y coordinadas entre los estados, para hacer frente a la lucha contra el cybercrimen. Los firmantes han sido solo 54, ratificándola solo 42 y 17 reglamentándola a su derecho interno.

En la siguiente tabla se detalla los países que han firmado y ratificado la firma del convenio:

	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Albania	23/11/2001	20/6/2002	1/7/2004				X			
Andorra	23/4/2013									
Armenia	23/11/2001	12/10/2006	1/2/2007				X			
Austria	23/11/2001	13/6/2012	1/10/2012		X	X	X			
Azerbaijan	30/6/2008	15/3/2010	1/7/2010		X	X	X	X		
Belgium	23/11/2001	20/8/2012	1/12/2012		X	X	X			
Bosnia and Herzegovina	9/2/2005	19/5/2006	1/9/2006				X			
Bulgaria	23/11/2001	7/4/2005	1/8/2005		X	X	X			
Croatia	23/11/2001	17/10/2002	1/7/2004				X			
Cyprus	23/11/2001	19/1/2005	1/5/2005				X			
Czech Republic	9/2/2005	22/8/2013	1/12/2013		X	X	X			
Denmark	22/4/2003	21/6/2005	1/10/2005		X		X	X		
Estonia	23/11/2001	12/5/2003	1/7/2004				X			
Finland	23/11/2001	24/5/2007	1/9/2007		X	X	X			
France	23/11/2001	10/1/2006	1/5/2006		X	X	X			
Georgia	1/4/2008	6/6/2012	1/10/2012			X				
Germany	23/11/2001	9/3/2009	1/7/2009		X	X	X			
Greece	23/11/2001									
Hungary	23/11/2001	4/12/2003	1/7/2004		X	X	X			
Iceland	30/11/2001	29/1/2007	1/5/2007		X		X			
Ireland	28/2/2002									
Italy	23/11/2001	5/6/2008	1/10/2008				X			
Latvia	5/5/2004	14/2/2007	1/6/2007		X		X			
Liechtenstein	17/11/2008									
Lithuania	23/6/2003	18/3/2004	1/7/2004		X	X	X			
Luxembourg	28/1/2003									
Malta	17/1/2002	12/4/2012	1/8/2012			X				
Moldova	23/11/2001	12/5/2009	1/9/2009			X	X	X		
Monaco	2/5/2013									
Montenegro	7/4/2005	3/3/2010	1/7/2010	55	X		X			
Netherlands	23/11/2001	16/11/2006	1/3/2007				X	X		
Norway	23/11/2001	30/6/2006	1/10/2006		X	X	X			
Poland	23/11/2001									
Portugal	23/11/2001	24/3/2010	1/7/2010			X	X			
Romania	23/11/2001	12/5/2004	1/9/2004				X			
Russia										
San Marino										
Serbia	7/4/2005	14/4/2009	1/8/2009	55			X			
Slovakia	4/2/2005	8/1/2008	1/5/2008		X	X	X			
Slovenia	24/7/2002	8/9/2004	1/1/2005				X			
Spain	23/11/2001	3/6/2010	1/10/2010			X	X			
Sweden	23/11/2001									
Switzerland	23/11/2001	21/9/2011	1/1/2012		X	X	X			
The former Yugoslav Republic of Macedonia	23/11/2001	15/9/2004	1/1/2005				X			
Turkey	10/11/2010									
Ukraine	23/11/2001	10/3/2006	1/7/2006		X		X			
United Kingdom	23/11/2001	25/5/2011	1/9/2011		X		X			

Non-members of the Council of Europe

	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Argentina										
Australia		30/11/2012 a	1/3/2013		X		X			
Canada	23/11/2001									
Chile										
Colombia										
Costa Rica										
Dominican Republic		7/2/2013 a	1/6/2013			X	X			
Israel										
Japan	23/11/2001	3/7/2012	1/11/2012		X	X	X			
Mauritius		15/11/2013 a	1/3/2014				X			
Mexico										
Morocco										
Panama		5/3/2014 a	1/7/2014				X			
Philippines										
Senegal										
South Africa	23/11/2001									
United States of America	23/11/2001	29/9/2006	1/1/2007		X	X	X			

Los objetivos principales del convenio son:

1. La armonización de los elementos nacionales de derecho penal de fondo de infracciones y las disposiciones conectados al área de los delitos informáticos.
2. La prevención de los poderes procesales del derecho penal interno es necesaria para la investigación y el enjuiciamiento de esos delitos, así como otros delitos cometidos por medio de un sistema informático o pruebas en formato electrónico.
3. Establecimiento de un régimen rápido y eficaz de la cooperación internacional.

Son varios los beneficios que en materia informática se obtendria al firmar el Convenio de Budapest, y se procede a mencionar solo dos en la parte adjetiva o procesal que subjetivamente se considera que son significativos en el avance en la materia:

1. Teniendo en marcha un COIP, que en la parte sustantiva si contempla delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, acceso ilícito, pornografía infantil, entre otros de carácter informático; así como diferentes delitos cometidos por medio de un sistema informático que están tipificados en la norma sustantiva penal,

(primer libro COIP), mediante la cooperación internacional, se alcanzaria que tanto en la investigación y el enjuiciamiento de esos delitos, con mucha rapidez se obtengan elementos de convicción que será elevada en el momento procesal oportuno a categoría de prueba, y considerándose el contenido digital del Art. 500 COIP, se podría recibir mediante formato electrónico, que evitará impunidad por falta de la misma, cumpliendo no solo los principios básicos del proceso penal, sino también principios constitucionales, pues se lograría llegar a sentencias que en los últimos años por la falta de información, sobre todo de aquellas conductas que han sido realizadas utilizando redes electrónicas, no solo en nuestro país sino fuera de las fronteras ecuatorianas, son de dificultosa obtención, habida consideración que la asistencia penal internacional se demora mucho tiempo por los trámites inherentes a la aplicación de la misma, que esperando llegue el resultado, ocasiona en algunos casos, que los tipos penales prescriban por el paso del tiempo.

2. Se tendría de forma directa el beneficio de poder controlar de mejor manera la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos en el Código Orgánico Integral Penal, o una contraseña, un código de acceso o datos informáticos similares, que permitan tener acceso a la totalidad o a una parte de un sistema informático, que en forma conjunta con todos los países se pudieran trasladar informaciones conjuntas para prevención de delitos, esto debido a que cuando éste tipo de infracciones son cometidas fuera de la esfera nacional, se corre el riesgo que dichos actos deliberados e ilegítimos que causan un perjuicio patrimonial a otra persona mediante cualquier introducción, alteración, borrado o supresión de datos informáticos, o mediante cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona, sean utilizados para el cometimiento de concurrencia de delitos, pues siendo suscriptores del Convenio

de Budapest nos garantizará entre países miembros, la conservación rápida de datos informáticos almacenados, mantenimiento y revelación parcial rápidas de los datos relativos, el registro y confiscación de datos almacenados, la obtención en tiempo real de datos relativos al tráfico así como la interceptación de datos relativos al contenido, que no solo servirá como punto de partida para la obtención de pruebas, sino que se evitará el cometimiento de más delitos penales.

Capítulo I - Terminología

Artículo 1.- Definiciones a los efectos del presente Convenio:

a) Por sistema informático se entiende todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa;

b) Por datos informáticos se entiende cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función;

c) Por proveedor de servicios se entiende a toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático, y cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio; y por datos sobre el tráfico se entiende cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente.

El capítulo II ofrece un resumen de la gama de delitos que deben ser considerados en las legislaciones nacionales de los estados partes, mencionando en primer lugar a los códigos penales (leyes sustantivas penales)

Capítulo II –

Medidas que deberán adoptarse a nivel nacional

Sección 1 - Derecho penal sustantivo

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

Artículo 2.- Acceso ilícito: Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático.

Artículo 3.- Interceptación ilícita. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artículo 4.- Interferencia en los datos.

1) Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

2) Cualquier Parte podrá reservarse el derecho a exigir que los actos definidos en el apartado 1 provoquen daños graves.

Artículo 5.- Interferencia en el sistema. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito

en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 6.- Abuso de los dispositivos

1) Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

i. Un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5;

ii. Una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados en los artículos 2 a 5; y

b) La posesión de alguno de los elementos contemplados en los anteriores apartados a.i) o ii) con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Cualquier Parte podrá exigir en su derecho interno que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2) No podrá interpretarse que el presente artículo impone responsabilidad penal en los casos en que la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición mencionadas en el apartado 1 del presente artículo no tengan por objeto la comisión de un delito previsto de conformidad con los artículos 2 a 5 del presente Convenio, como es el caso de las pruebas autorizadas o de la protección de un sistema informático.

3) Cualquier Parte podrá reservarse el derecho a no aplicar lo dispuesto en el apartado 1 del presente artículo, siempre que la reserva no afecte a la venta, la distribución o cualquier otra puesta a disposición de los elementos indicados en el apartado 1.a.ii) del presente artículo. Título 2 Delitos informáticos

Artículo 7.- Falsificación informática. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal.

Artículo 8.- Fraude informático. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:

a) Cualquier introducción, alteración, borrado o supresión de datos informáticos;

b) Cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

Capítulo 4.

Delitos relacionados con el contenido

Artículo 9.- Delitos relacionados con la pornografía infantil

1) Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) La producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;

b) La oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;

c) La difusión o transmisión de pornografía infantil por medio de un sistema informático;

d) La adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;

e) La posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

2) A los efectos del anterior apartado 1, por "pornografía infantil" se entenderá todo material pornográfico que contenga la representación visual de:

a) Un menor comportándose de una forma sexualmente explícita;

b) Una persona que parezca un menor comportándose de una forma sexualmente explícita;

c) Imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.

3) A los efectos del anterior apartado 2, por menor se entenderá toda persona menor de 18 años. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de 16 años.

4) Cualquier Parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2.

Título 4.- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines **Artículo 10.-** Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

1) Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual, según se definan en la legislación de dicha

Parte, de conformidad con las obligaciones asumidas en aplicación del Acta de París de 24 de julio de 1971 por la que se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre la propiedad intelectual, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

2) Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en la legislación de dicha Parte, de conformidad con las obligaciones que ésta haya asumido en aplicación de la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre las obras de los intérpretes y ejecutantes y los fonogramas, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

3) En circunstancias bien delimitadas, cualquier Parte podrá reservarse el derecho a no exigir responsabilidad penal en virtud de los apartados 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos.

En último lugar, el capítulo IV dedica a las Disposiciones Finales, que tienen la forma y utilidad de este tipo de disposiciones en los otros Convenios del Consejo de Europa, consagradas a resaltar la aplicación territorial, efectos del Convenio y otras cláusulas de este tipo.

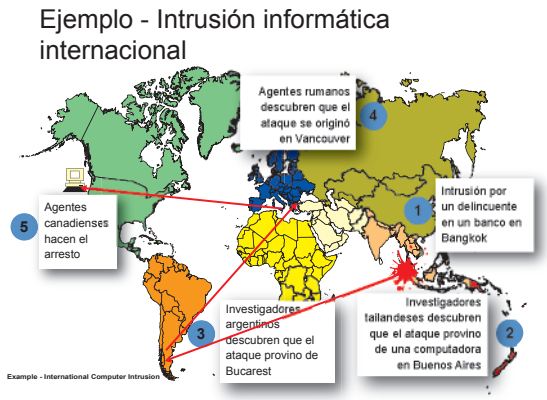


Figura 41.

Definición de términos Básicos:

Adware: Se trata de programas que recogen o recopilan información acerca de los hábitos de navegación del usuario en cuestión. Se suele utilizar con fines publicitarios o marketing para determinar qué, cómo, cuánto, todo tipo de datos que indiquen la conducta de los internautas o sea todas las personas que tenemos acceso al internet.

Análisis Forense: Es la identificación de rastros digitales que evidencien que cierto suceso ha ocurrido en el dispositivo. Estas evidencias pueden ser usadas en un juicio.

Blog o Bitácora: es un sitio web que incluye, a modo de diario personal de su autor o autores, contenidos de su interés, actualizados con frecuencia y a menudo comentados por los lectores.

Bomba Lógica: Una bomba es una parte de código insertada intencionalmente en un programa informático que permanece oculto hasta cumplir una o más condiciones preprogramadas, en ese momento se ejecuta una acción maliciosa.

Caballos de Troya: programa que una vez instalado en el ordenador provoca daños o pone en peligro la seguridad del sistema.

Carting o Cambiazo: Se denomina a aquella modalidad utilizada para apropiarse con engaños, de la tarjeta de crédito o de débito, cuando las personas están haciendo fila en un cajero automático, para después apropiarse del dinero.

Ciberterrorismo: También llamado "terrorismo electrónico" se refiere al uso de medios de tecnologías de información, comunicación, informática, electrónica o similar, con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno, causando con ello una violencia a la libre voluntad de las personas. Los fines pueden ser económicos, políticos o religiosos principalmente.

Comercio Electrónico: Es toda transacción comercial realizada en parte o en su totalidad, a través de redes electrónicas de información.

Computadora: Máquina electrónica capaz de almacenar información y tratarla automáticamente mediante operaciones matemáticas y lógicas controladas por programas informáticos.

Cracker: Es cualquier persona que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

Desmaterialización Electrónica de Documentos: Es la transformación de la información contenida en documentos físicos o mensajes de datos.

Delito Informático: Es toda aquella acción, típica, antijurídica y culpable que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet.

Dialers: Técnica que consiste en la instalación de un marcador que provoca que la conexión a internet se realice a través de un número de tarificación especial y no a través de modo indicado por el operador, con el que se haya contratado dicha operación.

Dispositivo Electrónico: Instrumento físico o lógico utilizado independientemente para iniciar o responder mensajes de datos, sin intervención de una persona al momento de dicho inicio o respuesta.

Espionaje Informático: Este tipo de espionaje se refiere a entrar a fisgar en datos computarizados, en búsqueda de información sigilosa que de rédito económico del que se tratara de beneficiar el agente. El espionaje informático en la actualidad pasó de ser un concepto de solo un acopio de información, a un concepto más complejo que comprende todo el proceso inmanente a él, es decir, asimilado dentro de su contenido el proceso de almacenamiento, tratamiento y transmisión de datos. Los programas mediante los cuales se puede efectivizar este tipo de operaciones se denominan "spywares", que son espiones que constantemente monitorean los pasos del usuario de un computador conectado a la red de internet, sin su consentimiento, a fin de trazar un perfil comercial completo, tal es el caso de proveedores de productos de tiendas virtuales, las que intentan captar información que tenga utilidad para el agente. Es decir, spyware es un programa encargado de registrar todo lo que se realiza en un PC, por lo que hasta un sencillo clic en el ratón queda almacenado. Se obtiene información confidencial o también se puede obtener o conocer cuál es el funcionamiento que una persona le está dando a la máquina.

Evidencia Digital: Es aquella que abarca cualquier información en formato digital que pueda establecer una relación entre un delito y su autor.

Evidencia Electrónica: Son datos que de manera digital se encuentran almacenada o fueron transmitidos mediante equipos informáticos y que son recolectados mediante herramientas técnicas especializadas, empleadas por un perito en una investigación informática. Tiene la función de servir como prueba física (por encontrarse dentro un soporte) de carácter intangible (no modificables) en la investigación informática.

Equipo Terminal Móvil: Equipo electrónico por medio del cual el usuario accede a las redes de telecomunicaciones móviles para recibir servicios de telefonía.

Firma Digitalizada: Es aquella firma que se utiliza tanto en actos públicos como privados, y que puede ser escaneada en forma informática y transferida vía internet.

Foto Blog: Es un blog al cual se le agrega una fotografía por entrada o artículo. La palabra *fotolog* en español tiene dos orígenes: derivada del inglés *photoblog* y derivada del sitio.

Gusano Informático: Es un malware que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

Hacking. Sujeto que ingresa a un sistema informático con conocimientos básicos, quien puede violentar o fortalecer sistemas de seguridad.

Imei: Identificador internacional del Equipo Terminal Móvil (por sus siglas en inglés) o sus equivalentes en el futuro, código variable pregrabado en los equipos terminales móviles que los identifica de manera específica.

Informática Forense: Es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permite identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Información: Conjunto de datos acerca de algún suceso, hecho, fenómeno o situación privada o pública.

Infracción: Es toda trasgresión, quebrantamiento de una ley, pacto o tratado, o de una norma moral, lógica o doctrinal.

Ingeniería Inversa: Es obtener información o un diseño a partir de un producto accesible al público, con el fin de determinar de qué está hecho, qué lo hace funcionar y cómo fue fabricado.

Ingeniería Social: Es una técnica que pueden utilizar ciertas personas, tales como investigadores privados, criminales, o delincuentes informáticos, para obtener información, acceso o privilegios en sistemas de información, que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

IP: Conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, la cual garantiza que las redes

físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.

Intimidad: El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta Ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados.

Lazo Libanés: Consiste en introducir un plástico negro con la medida de la tarjeta en la ranura del cajero y se pega a sus extremos afuera, para que la tarjeta se quede trabada y el ladrón luego la recupere.

Mensaje de Datos: Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio.

Pharming: Es una explotación de una vulnerabilidad en el software de los servidores DNS o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio a otra máquina distinta. De esta forma un usurario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página que el atacante haya especificado para ese nombre de dominio.

Phising: Llamado también suplantación de identidad, es un término informático que determina un tipo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

Principio de Ubicuidad: Es cuando al cometer un delito, el mismo es comenzado en un lugar y concluido en otro, según reglas de competencia territorial es competente el Juez del lugar en que el delito se consumó.

Sabotaje Informático: Es un Delito Informático tipificado como el acto de borrar, suprimir o modificar sin autorización funciones o datos de un sistema informático con intención de obstaculizar su funcionamiento normal. Resulta

especialmente aplicable a quien, deliberadamente, introduzca un virus informático en dichos sistemas.

Seguridad de la Información.- Conjunto de medidas preventivas y reactivas de los sistemas tecnológicos, que permiten resguardar y proteger la información, buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

Tecnologías de Información.- Aquellas herramientas y métodos empleados para recabar, retener, manipular o distribuir información.

Virus Informático: Es un programa o código que provoca daños en el sistema como alteración o borrado de datos; se propaga a otros computadores haciendo uso de la red, del correo electrónico, etc.

RECOMENDACIONES

Al redactar el presente libro, me propuse al final presentar algunas **recomendaciones que en** explícito **momento pueden servir de algo** al lector**; a pesar que en el mundo de la** informática, los cracking detectan con mucha facilidad las vulnerabilidades de los sistemas, en general, es fundamental estar al día de la aparición de nuevas técnicas que amenazan la **seguridad de su equipo informático**, para tratar de evitarlas o de aplicar la solución más efectiva posible. A continuación planteo lo siguiente:

1. Se debe actualizar el sistema operativo y el software instalado en su equipo, poniendo especial atención a las actualizaciones de su navegador web, aplicar los parches de seguridad recomendados por los fabricantes. Esto le ayudará a prevenir la posible intrusión de hackers.
2. Es recomendable tener instalado en su equipo algún tipo de software anti-spyware, para evitar que se introduzcan en su equipo programas espías destinados a recopilar información confidencial sobre el usuario.
3. Utilice contraseñas seguras, es decir, aquellas compuestas por ocho caracteres, como mínimo, y que combinen letras, números y símbolos. Es conveniente además, que modifique sus contraseñas con frecuencia, no se debe compartir con otras personas la clave de seguridad para acceder a páginas webs y así evitar que pueda ser suplantado por otra persona.
4. Navegue por páginas web seguras y de confianza. Para diferenciarlas identifique si dichas páginas tienen algún sello o certificado que

garanticen su calidad y fiabilidad, Desconfíe de aquellos e-mails en los que entidades bancarias, compañías de subastas o sitios de venta online, le solicitan contraseñas, información confidencial, etc.

5. Sea cuidadoso al utilizar programas de acceso remoto. A través de internet y mediante estos programas, es posible acceder a un ordenador, desde otro situado a kilómetros de distancia.
6. Para proteger la identidad, tenemos que hacer buen uso de la información que publicamos en internet, para así no ser un blanco fácil para los delincuentes informáticos.
7. No creer en las ofertas ni en los premios que algunas páginas ofrecen, pues son engaños para cometer delitos informáticos.
8. No aceptar ni divulgar los sitios virtuales que promueven la autodestrucción, la xenofobia, la exclusión, la pornografía de menores, la trata de personas, la intolerancia o cualquier actividad al margen de la ley.
9. Denunciar las páginas que cometan delitos informáticos.
10. Tener cuidado con las personas que se conozcan por el ambiente tecnológico y no dar información personal.
11. Hablar con nuestros hijos sobre el peligro de contactarse con personas virtuales que no conozcan; y sobre todo nunca citarse a escondidas con éstos; pues no siempre el perfil expuesto públicamente es el verdadero.

Bibliografía

Acurio, P. (2010). *DELITOS INFORMÁTICOS.*

Carrara, F. (1944). *PROGRAMA DEL CURSO DE DERECHO CRIMINAL.*

Derecho Informático. (2010). *PC WORLD EN ESPAÑOL*.

PALAZZI, P. A. (2010). *DELITTOS INFORMÁTICOS.* BUENOS AIRES: ABELEDO PERROT S.A.

PENAL, C. I. (2014). *Artículo 178.* QUITO.

Penal, C. I. (2014). *Artículo 262.*

PENAL, C. O. (2014). *ARTÍCULO 103.* QUITO.

PENAL, C. O. (2014). *Artículo 174.* (C. d. Publicaciones, Ed.) Quito, Ecuador.

Penal, C. O. (2014). *Artículo 212.*

Ramiro, A. (2010). *Delitos Informáticos.*

Santiago, P. (2010). *Derechos y Nuevas TEcnologías.*

TELLEZ VALDEZ, J. (2008). *Derecho Informatico.* México.

Vallejo, V. (2010). *DELITOS INFORMÁTICOS.*

En el libro se explica los términos usuales y básicos del derecho informático; así como también de manera concisa y práctica los diferentes tipos de delitos en esta área, que se cometen desde un ordenador, en el ciberespacio, lo que debe ser punible por la normativa del Estado para evitar la impunidad de los delincuentes cibernéticos.

Es un texto que permite contribuir, ante la falta de cultura informática en el Ecuador, con las diferentes variedades entre la norma jurídica penal anterior y el nuevo Código Orgánico Integral Penal.
Ante la falta de información conceptual en este ámbito, esta obra permite explicar concepciones, opiniones, tendencias sobre las conductas penales de carácter informático adaptadas de la legislación internacional y diferenciándolas de los conceptos tradicionales.

Cada uno de sus capítulos permite al lector comprender el bien jurídico protegido, los obstáculos procesales y sobre todo la importancia de la pericia y evidencias para una correcta aplicación del derecho sustantivo al adjetivo.

UEES | Centro de Investigaciones

ISBN: 978-9978-25-225-3

uees_ec
universidadespiritusanto
www.uees.edu.ec
Km. 2,5 La Puntilla,
Samborondón

ceninv@uees.edu.ec
Teléfono: (593-4) 283 5630 Ext: 208 - 209