ReCIBE, Año 4 No. 3, Noviembre 2015

Estudio cualitativo de la relación de las leyes y la pericia informática en el Ecuador

Francisco Bolaños-Burgos
Facultad de Sistemas, Telecomunicaciones y Electrónica
Universidad Espíritu Santo - Ecuador
fcobolanos@uees.edu.ec

Cristopher Gómez-Giacoman
Facultad de Sistemas, Telecomunicaciones y Electrónica
Universidad Espíritu Santo - Ecuador
cgomezg@uees.edu.ec

Resumen: El presente trabajo analiza cualitativamente las leyes vigentes en el Ecuador relacionadas a los procesos de la pericia informática. Para aquello, se estudia los pasos empleados por un perito de la Policía Nacional en el desarrollo de los casos de delito informático, suscitados en el periodo 2012-2014, que implican la evidencia digital en: disco duros, cuentas de correo electrónico, redes sociales y motor de base datos. Apartir de los casos analizados, se puede concluir que la ley contempla una mayor cantidad de artículos relacionados a las bases de datos. Sin embargo, se tendría que analizar otros tipos de evidencia digital tales como: documentos de ofimática, imágenes digitales, ficheros de registros de actividad, memoria volátil, entre otros.

Palabras Clave: Pericia Informática, evidencia digital, perito informático, Código Orgánico Integral Penal (COIP).

Qualitative study of the relation of the laws and the IT know-how in the Ecuador

Abstract: This paper analyzes qualitatively the current laws in Ecuador related to the computer forensic processes. For this, the steps applied for a computer expert of the Policía Nacional in the development of some computer forensic cases are analyzed, during the years 2012-2014. These cases focuse on digital evidence such as: hard disk, email accounts, social networks and database engine. From the examination of the cases, we concluded that the law provides a greater amount of articles related to database. However, other types of digital evidence would have to be studied which are: offimatic documents, digital images, file activity logs, volatile memory, among others.

Keywords: Computer Forensics, digital evidence, computer expert, Código Orgánico Integral Penal (COIP).

1. Introducción

En el Ecuador las investigaciones realizadas acerca de pericia informática son de bajo interés, una de las causas es el desconocimiento del tema por parte de la sociedad, adicional a la falta de procedimientos registrados de delitos informáticos competentes a las autoridades o entidades gubernamentales. (Ferruzola, 2014). Vizueta (2011) indica que la falencia principal de la pericia informática en el Ecuador es la carencia de peritos que tengan conocimientos informáticos adecuados obteniendo como resultado impunidad de casos debido a la falta de conocimientos, pocas habilidades idóneas para la

utilización de medios tecnológicos en la adquisición de pruebas, y una correcta legislación de acuerdo a los delitos informáticos actuales.

Con los antecedentes se puede observar que, en el país las falencias detectadas tales como la falta de capacitación y conocimiento, una incorrecta legislación, y la falta de procedimientos registrados de los delitos informáticos por parte de las entidades (Ureta, 2015), han producido que la pericia informática no tenga la fortaleza suficiente generando malos procesos los cuales se convierten en casos impunes (López, 2014). Por este motivo es importante realizar un estudio que evidencie si las leyes de delito informático en el Ecuador abarcan toda la perspectiva del mismo. (Ojeda, 2014)

Este estudio tiene como objetivo analizar las leyes vigentes en el Ecuador (COIP) relacionadas a los delitos informáticos y los procesos de pericia informática. Para lo cual se han escogido tres casos reales obtenidos en los archivos del departamento de criminalística de la Policía Nacional, con la finalidad de conocer la cantidad de artículos del COIP que se relacionan con la evidencia digital.

2. Marco Teórico

2.1 Informática Forense

Warren & Heiser (2002) definen la informática forense como la participación de la preservación, la identificación, la extracción, la documentación y la interpretación de los datos informáticos. Igual que (Yasinsac, Erbacher, Marks & Pollitt, 2003) quienes dicen que las técnicas y los conocimientos forenses se utilizan para explicar el estado actual de un artefacto digital; tal sistema informático como medio de prueba. De la misma manera Carroll, Brannon & Song (2008) definen la informática forense como: El uso de métodos científicamente probados y derivados hacia la preservación, recopilación,

validación, identificación, análisis, interpretación, documentación y presentación de evidencia digital derivados de fuentes digitales con el fin de facilitar o promover la reconstrucción de los hechos que son de índole penal. Mientras tanto US-CERT (2008) la define como la disciplina que combina elementos de derecho y ciencias de la computación para recopilar y analizar datos de los sistemas informáticos, redes, comunicaciones inalámbricas y dispositivos de almacenamiento de una manera que es admisible como prueba en un tribunal de justicia. Como se puede ver los cuatro autores coinciden en que la informática forense se basa en una secuencia de procesos que recopilan y analizan los datos con el fin de ser presentados en la Corte, La Figura 1 muestra en detalle este proceso.

2.2 Evidencia Digital

Casey (2004) indica que la evidencia digital, pruebas digitales o pruebas electrónicas son cualquier información probatoria almacenada o transmitida en forma digital que se puede utilizar en la Corte. Así mismo, esta puede ser definida como el conjunto de datos en formato binario que incluye archivos, contenido o referencia a estos (metadatos) que se encuentran en el hardware o el software del sistema violado, la evidencia digital es única en comparación con otras formas de "pruebas documentales" (Accorsi, 2009). Sin embargo, Lin, Chao & Peng (2011) definen la evidencia digital como: toda la información verificable que se encuentra en el sistema electrónico, que proporciona algunos datos para el análisis informático forense posterior el cual puede ser de tipo físico o lógico, está construida de campos magnéticos y pulsos eléctricos que son recogidos y analizados con herramientas y técnicas especiales. A diferencia de los documentos en papel, la evidencia digital es frágil y una copia de un documento almacenado en un archivo es idéntico al original (Osborne & Mata, 2011). Antes de aceptar la evidencia digital, un tribunal determinará si la prueba es pertinente, si es auténtica, si se trata de

rumores y si una copia es aceptable o se requiere el original, esta posee las siguientes características:

1. Volátil.
2. Anónima.
3. Duplicable.
4. Alterable y modificable.
5. Eliminable.

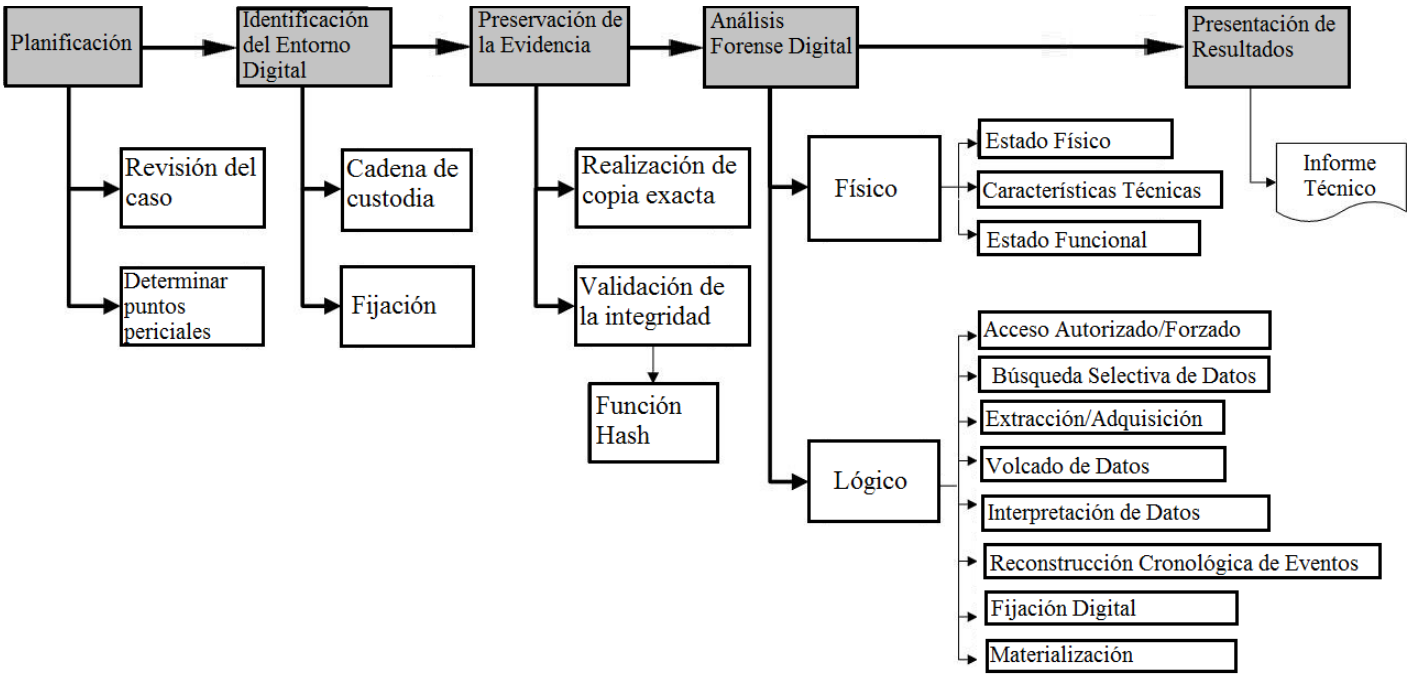

Figura 1.

Procesos de computación forense

Fuente: (Bogen & Dampier, 2005)

2.3 Metadato

Los metadatos son datos sobre los datos (Steinacker, Ghavam, & Steinmetz, 2001). Dick CA (2004) dice que los metadatos son descripciones estructuradas

opcionales que están disponibles públicamente para ayudar de forma explícita en la localización de objetos. Al igual que Wroe et al (2004) quienes dicen que los metadatos facilitan el flujo de trabajo de forma automática convirtiendo datos de un formato a otro, se requiere que los metadatos describan el contenido y la estructura de los mismos. Kosch et al (2005) indican que algunos metadatos permiten una compresión de datos más eficiente. El término es ambiguo, ya que se utiliza para dos conceptos fundamentalmente diferentes, metadatos estructural es sobre el diseño y la especificación de estructuras de datos y está más adecuadamente llamado "datos acerca de los contenedores de datos"; mientras que los metadatos descriptivos, por otro lado, tratan casos individuales de datos de aplicación, el contenido de datos, (Hua et al, 2011). Los autores antes mencionados coinciden en que los metadatos son datos acerca del contenido, ubicación, estructura y la compresión

2.4 Imagen Forense

Creutzburg & Luttenberger (2011) dicen que: "La imagen se copia uno a uno del objeto que se examina, en las imágenes de disco duro y volcados de memoria se buscan datos interesantes, como imágenes, archivos o archivos borrados de registro". Igual que Iqbal, B., Iqbal, A., Guimaraes, Khan & Obaidli (2012) quienes indican que una imagen forense es una copia "bit a bit" del disco duro objeto, en el cual se llevará a cabo todos los análisis pertinentes, búsquedas selectivas de datos o archivos que son de interés para la autoridad competente, la imagen forense se realiza para cumplir con uno de los protocolos de la informática forense que es la preservación de la evidencia digital y el principio de la cadena de custodia para preservar el medio magnético original. Los dos autores coinciden en que la imagen forense es una copia exacta del original.

2.5 Cadena de Custodia

Caloyannide & Grumman (2009) la definen como el procedimiento que debe garantizar que los procesos de recolección de las evidencias se realizaron correctamente, y que la evidencia recolectada en la escena es la misma que se presenta en la corte, el procedimiento a seguir en relación con la evidencia en la escena y durante todo el proceso de investigación es la recolección y almacenamiento de pruebas, las etapas de la cadena de custodia son:

1. Eliminación o la recopilación de pruebas.
2. Conservación y empacado de las pruebas.
3. Transporte de las pruebas.
4. Transferencia, ya sea a los laboratorios o a las diferentes oficinas para su custodia.
5. Se lleva a cabo la custodia y preservación definitiva hasta el debate

Lee, K., Lee, C., Park, Kim, & Won (2011) la definen a la cadena de custodia como el procedimiento de control que se aplica a la evidencia física relacionada con el delito, desde su ubicación para su evaluación por los responsables del análisis que por lo general son los peritos, y con el fin de evitar alteraciones, sustituciones, contaminación o la destrucción desde la ubicación, fijación, recolección, embalaje y transporte de la evidencia en la escena del incidente hasta la presentación al debate.

2.6 Delitos Informáticos

Bojanc & Blažic (2008) definen que un delito informático o ciberdelincuencia es cualquier acción, característica ilícita y culpable, que se da por métodos informáticos o pretende destruir y dañar ordenadores, medios electrónicos y redes de Internet. Mientras que Yen, Lin, & Chang (2011) definen que los delitos informáticos tienen un alcance mayor y puede incluir delitos

tradicionales como el fraude, el robo, chantaje, falsificación y malversación de fondos públicos en los ordenadores y las redes que se han utilizado como medio.

2.7 Ley Informática

Colombia (2009) define que la ley informática tienen como objetivo la protección integral de los sistemas que utilizan tecnología de información, así mismo como la prevención y sanción de delitos cometidos contra tales sistemas o algunos de sus componentes o los cometidos mediante el uso de dicha tecnología. Mientras que Ecuador (2014) define la ley informatica como el conjunto de ordenamientos jurídicos establecidos con el fin de regular el tratamiento de la información.

2.8 Código Penal

El código penal es un conjunto ordenado y sistematizado de normas jurídicas punitivas de un estado o país, en el año 2013, la Asamblea Nacional de la República del Ecuador promulgó el nuevo COIP (Blum, 2010). En la Tabla 1 se muestra un resumen del Código Penal en relación con las penas para delitos informáticos en el país.

Articulo	Area de Estudio
103	Violación a los derechos humanos, diversas formas de explotación.
178,179,180	Delitos contra el derecho a la intimidad personal y Familiar.
182	Delito contra el derecho al honor y buen nombre.
190, 191, 192, 193, 194, 195	Delitos contra el derecho a la propiedad.

221	Delitos contra el derecho a la identidad.
229, 230, 231, 232, 233, 234	Delitos contra la seguridad de los activos de los Sistemas de Información y Comunicación.
298	Delitos contra el Régimen de Desarrollo.
453, 454	Prueba, disposiciones generales.
475, 476, 477	Actuaciones especiales de investigación.
498	Medios de prueba.
499, 500	Documentos, reglas generales.
511	La pericia, reglas generales.

Tabla 1.

Resumen del código penal basado en Código Penal del Ecuador

Fuente: Elaboración propia en base a Código Orgánico Inegral Penal del Ecuador (COIP)

2.9 Mecanismos de seguridad en la evidencia digital

Torres, Rueda, & Cano (2004) dicen que durante la recolección y análisis de la evidencia digital, el perito debe utilizar métodos para verificar y mantener la integridad de los mismo, debido a que es vital la preservación de la evidencia ya que se debe recolectar sin altearla, una manera de garantizar la integridad de la evidencia digital es utilizando algoritmos Message Digest o Función Hash por ejemplo: MD5, SHA1, SHA256, etc.

Una función de hash es un algoritmo usado para producir una secuencia de caracteres de longitud fija, basada en una entrada de longitud variable, cualquier entrada dada siempre produce el mismo resultado, pero si un bit en la entrada cambia, la salida del hash cambiará significativamente y de forma aleatoria (Ke et al, 2011). Por otra parte, Creutzburg & Luttenberger (2011)

dicen que los códigos hashes son muy importantes para la informática forense, porque son la huella digital de los datos. Los dos autores concluyen que los códigos hashes son caracteres que deben tener siempre el mismo valor, caso contrario los códigos han sido alterados.

2.10 Herramientas Forenses

Malek (2008) indica que son dispositivos electrónicos que ayudan a mantener la integridad de los datos y el procesamiento de los mismos, pero se requiere de una especialización y conocimientos avanzados en la materia para la utilización correcta de estas. Mientras que Sánchez (2013) dice que las herramientas forenses son equipos que ayudan a obtener datos de registros como: información del sistema, información de aplicaciones, ficheros ejecutables, y más. Los dos autores indican que con el fin de realizar un correcto levantamiento de información el perito debe contar con herramientas y técnicas especialmente diseñadas para ello.

3. Metodologia

Esta investigación aplicará una metodología con enfoque cualitativo utilizando un muestreo por conveniencia ya que los casos analizados son representativos de la evidencia digital en el ámbito civil los cuales son: discos duros, cuentas de correo electrónico, redes sociales y motor de base datos, en el periodo comprendido entre los años 2012-2014.

La primera fase fue determinar los casos que se analizarán, se incluyeron sólo los tres debido a que el acceso a los mismos no es tan factible, a pesar de que estos una vez sentenciados son de dominio público.

A partir de lo anterior, se realizó una entrevista a un Perito Policial el cual dio la descripción de los equipos y los procesos que utiliza la Policía Nacional para

realizar trabajos de pericia informática, lo siguiente fue establecer los procesos y herramientas que se necesitan para realizar una pericia informática de forma correcta siguiendo las Directrices para la recolección de evidencia, aplicando las buenas prácticas de Request for Comments (RFC). (Instituto Nacional de Ciberseguridad, 2014)

Por consiguiente se clasificó la información considerando cada uno de los casos analizados. Luego, se procedió con el análisis de la información utilizando técnicas de estadística descriptiva tales como: tablas de contraste y gráfico de dispersión que facilitan la exposición de diferencias y similitudes entre los procesos y artículos del COIIP utilizados en cada uno de ellos.

Finalmente, esto llevó a contrastar los resultados examinados y permitó presentar un resumen en el que se muestra si las leyes vigentes en el Ecuador cubren los diferentes tipos de evidencia digital y sus respectivas tipificaciones.

4. Desarrollo

4.1 Caso 1

Adquisición y preservación de imágenes forenses de discos duros operativos en CPUs o equipos portátiles

4.1.1 Descripción

El siguiente es un caso real, tomado de los archivos del Departamento de Criminalística de la zona 8 sobre Lavado de Activos relacionados con la evidencia incautada en un operativo de la Unidad de Lavado de Activos (ULA), las pruebas fueron ingresadas en las bodegas de la Policía Judicial de la Zona 8, de la cual se va a tomar un elemento (laptop) para ilustrar los procedimientos

aplicados por los especialistas del Departamento de informática Forense, al adquirir y preservar un disco duro alojado dentro de un equipo en la pericia.

4.1.2 Proceso

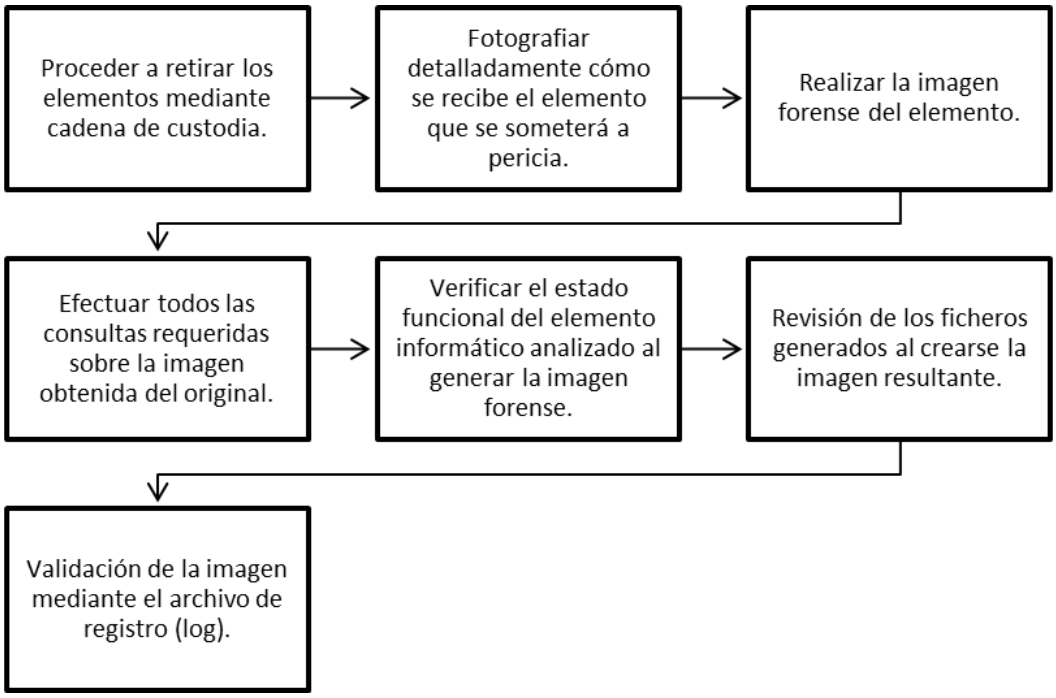

Figura 2.

Diagrama de pasos realizados en la pericia informática Caso 1

Fuente: Elaboración en base al desarrollo del Caso 1

1) Proceder a retirar mediante cadena de custodia, de las Bodegas de la Policía Judicial o Centros de Acopio correspondientes, los elementos que la autoridad competente delega y disponga para que sean sometidos a pericia.
2) Fijar fotográficamente, cómo se recibe el elemento que se someterá a pericia, detallando el envoltorio, puertos y estado de conservación, todo esto referenciado con un testigo métrico.
3) Utilizar el hardware de protección contra escritura y conectarlo, luego con FTK Imager se procede a realizar la imagen forense.

4) La imagen forense debe realizarse en un medio idóneo, a fin de efectuar todos los trabajos de campo y técnicos requeridos sobre la imagen obtenida, nunca sobre el dispositivo original.
5) Al realizar el proceso de generación de la imagen forense se debe verificar el estado funcional del elemento informático analizado, este procedimiento establece si el disco duro al momento de la pericia se encontraba funcionalmente operativo. En todo caso, si el medio magnético tuviera algún daño o desperfecto de índole físico, electrónico o lógico que impide la realización de la imagen, se deberá registrar la novedad e indicar el tipo de daño que presenta el medio magnético en el informe.
6) Conjuntamente con la imagen forense creada por la herramienta FTK Imager, se generan dos ficheros que poseen el mismo nombre asignado al archivo de la imagen resultante, uno con extensión .csv y otro con extensión .txt, el primero contiene siete columnas, con los siguientes encabezados: Filename (nombre del fichero), Full Path (ruta completa de la ubicación del fichero), Size (en bytes), Create (fecha), Modified (fecha), Accessed (fecha) e Is Delete (si/no), en las cuales se listan todos los ficheros contenidos en el disco duro origen.
7) El fichero .txt, es el log con el registro completo del proceso de creación de la imagen forense y el que se utiliza como medio de validación de la imagen, ya que en él se encuentran datos como fecha de inicio, fecha de término, hash MD5 y SHA1 del contenido total del disco duro preservado, una vez obtenido el fichero .txt con su contenido se puede validar la imagen forense adquirida.

   Con la conclusión de estos pasos se puede dar como completado el proceso estandarizado de adquisición y preservación de un disco duro, que debe ser aplicado a fin de garantizar la integridad de la evidencia digital y precautelar el cumplimiento de los principios de cadena de custodia que rigen en todos los elementos de índole informático ingresados como evidencia. Este mismo procedimiento puede ser aplicado a cualquier tipo de medio magnético de almacenamiento, esto es: discos duros internos o externos, memorias USB, memorias SD y microSD.

4.2 Caso 2

Adquisición y preservación de cuentas de correo electrónicos y cuentas de redes sociales.

4.2.1 Descripción

Se expone a continuación dos casos reales, el primero trata de una persona que por acudir a revisar sus cuentas de correos electrónicos (dos cuentas de correo electrónico, una en Hotmail y otra en Yahoo) en cybers con el fin de mantener segura su correspondencia electrónica porque pensaba que la conexión de internet de su domicilio se encontraba intervenida, termina perdiendo el acceso a una de las cuentas (la de Hotmail) por cuanto había sido cambiada su clave de acceso y le era imposible accesar a la misma. La labor pericial se centra en constatar si es posible tener acceso a la cuenta de correo electrónico de Hotmail, con el usuario y contraseña del titular de la misma. El segundo caso estudia las publicaciones de mensajes en un muro de la red social (Facebook), a fin de determinar si la persona denunciada es la titular de la cuenta de Facebook que hizo varias publicaciones.

4.2.2 Proceso

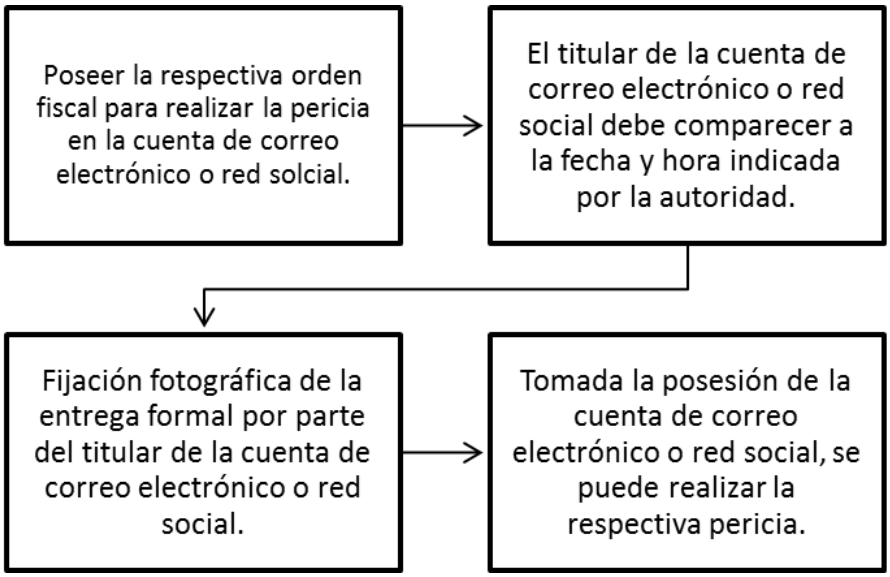

Figura 3. *Diagrama de pasos realizados en la pericia informática Caso 2*
Fuente: Elaboración en base al desarrollo del Caso 2

Para el efecto de realizar este tipo de adquisiciones, a fin de preservar la información obrante en una cuenta de correo electrónico o cuenta de red social, hay que tener presente aspectos muy importantes, para no violar los derechos fundamentales de las personas, existe una clara norma a respetar y que muchas veces fallan los peritos civiles; y es, en el acceso consentido expreso y la entrega libre y voluntaria del nombre de usuario y contraseña, por parte del titular de la cuenta de correo electrónico o red social al perito designado por la autoridad competente. Para el cumplimiento de lo antes dicho, se deben realizar los siguientes pasos:

1) Tener la respectiva orden fiscal para realizar la pericia en torno a la adquisición de la información obrante en un correo electrónico, en el cual se detalle textualmente la cuenta a ser intervenida, así como la delimitación correcta del objeto de pericia, esto es, el mensaje o mensajes específicos que el perito

debe adquirir, preservar y materializar de toda la información que obra dentro de dicha cuenta de correo.

2) Proceder a Oficiar a la autoridad competente a fin de que el titular de la cuenta de correo electrónico o red social, comparezca con fecha y hora, hasta las instalaciones u oficina que el perito señale, a fin de que conjuntamente con el titular de la cuenta el perito acceda a dicha información, desde un equipo con conexión a internet que el experto debe tener para dicha labor.
3) Como todo actuar pericial se debe realizar la respectiva fijación fotográfica, una vez que el titular de la cuenta concurra para la realización de la diligencia, dejando por escrito la entrega formal por parte del titular de la cuenta de correo electrónico o red social de la entrega libre y voluntaria del usuario y contraseña, ya que el perito debe tomar posesión de dicha cuenta de correo o red social, mientras dure la diligencia (pueden ser horas, días o semanas) y asegurarse de la no intrusión de terceras personas que puedan alterar la evidencia ya que se encuentra a cargo del perito (se realizan cambios en las seguridades de la cuenta de correo por parte del perito).
4) Una vez tomada la posesión de la cuenta de correo electrónico o red social, se puede realizar la fijación respectiva y preservación mediante tomas de captura de pantallas, de la información de interés pericial, para su posterior materialización en el informe.

Así como es de suma importancia el procedimiento para la adquisición de la cuenta de correo o red social, mucho más es la devolución del mismo, una vez terminado el procedimiento pericial es importante la devolución de la cuenta a su titular dejando constancia de su recepción satisfactoria, restableciendo sus configuraciones de seguridad anteriores en lo posible o que el titular en presencia del perito ponga nuevos parámetros de seguridad, siempre buscando que la persona tenga una total aceptación y conformidad en la devolución.

4.3 Caso 3

Adquisición y fijación dentro de una pericia que involucra bases de datos.

4.3.1 Descripción

En este caso se tiene el ingreso y modificación de datos no autorizados por parte del operador de un aplicativo que alimenta una base de datos del Ministerio de Agricultura, en el cual se pretendía favorecer a un productor bananero, ingresando datos falsos en cuanto a la real ubicación de las tierras de cultivo de una finca, a fin de que esta obtenga beneficios relacionados a su legalidad e insumos de agricultura.

4.3.2 Proceso

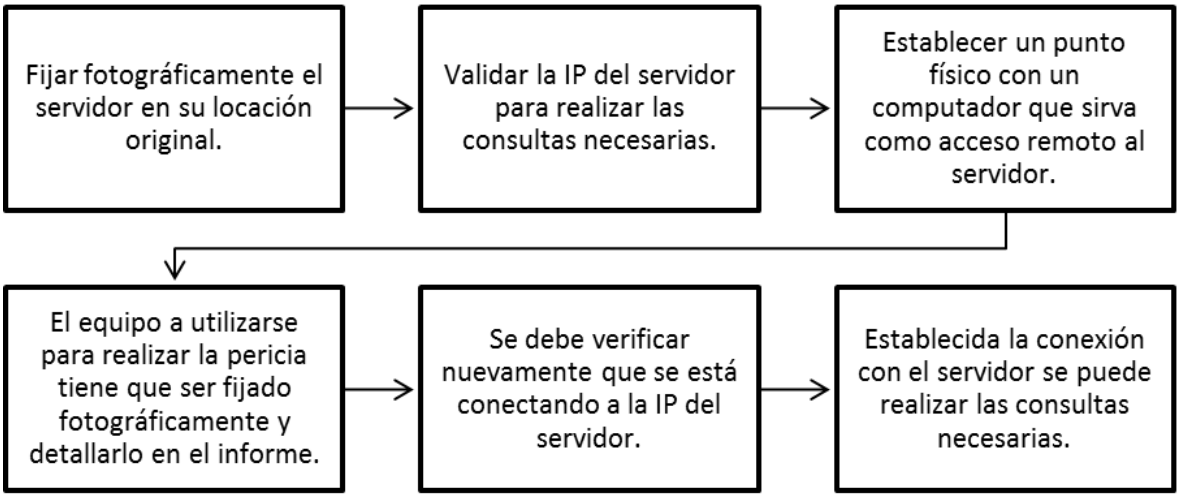

Figura 4.

Diagrama de pasos realizados en la pericia informática Caso 3

Fuente: Elaboración en base al desarrollo del Caso 3

En este tipo de circunstancias, primero se debe entender el entorno legal y las limitaciones en cuanto a la incautación de equipos se refiere en torno a estos

casos, por cuanto al tratarse casi siempre de empresas que manejan un volumen muy elevado de transacciones en sus servidores y que dependen de ellas para su normal desenvolvimiento o instituciones públicas que brindan servicios que no pueden dejar de brindar a la ciudadanía, es poco práctico incautar el disco o discos duros del servidor o servidores a fin de obtener las respectivas imágenes forenses y realizar el análisis en el laboratorio, por lo que es necesario hacer las consultas mientras el aplicativo se encuentra en ejecución. Por tal motivo la colaboración del administrador de base de datos y la facilidad de acceso a toda la información son indispensables en este tipo de casos. Los pasos necesarios para realizar una pericia en este tipo de caso son:

1) A fin de empezar el trabajo de campo, en estos casos se recomienda como primer paso, fijar fotográficamente el servidor, en su locación original.
2) Posterior a esto, es necesario validar la IP del servidor, al cual se conectará desde un acceso remoto, para realizar las consultas pertinentes.
3) Una vez hecho esto, se tiene que establecer un punto físico con un computador, que sirva como acceso remoto al servidor.
4) Dicho equipo a utilizarse para realizar la pericia también tiene que ser fijado fotográficamente y detallar en el informe su modelo y serie.
5) Una vez establecido el acceso remoto, se debe verificar que se está conectando a la IP del servidor.
6) Establecidos los pasos anteriores se puede realizar las consultas necesarias, las cuales serán fijadas mediante capturas de pantallas y materializadas en el informe a presentar.

5. ANÁLISIS DE CASOS

Cumplimiento e incumplimiento con el COIP.

5.1 Caso 1

Como se puede observar en la Tabla 2 cada proceso realizado en la pericia (pasos en el desarrollo del caso) esta llevado a cabo bajo los artículos del COIP que engloban el ámbito informático al momento de realizar un peritaje. En la columna de observación se puede ver información adicional que se debe tener en cuenta cuando se lleva a cabo el proceso en mención con el fin de no violar o faltar algún artículo de la legislación informática y esto a su vez pueda invalidar la información extraída que se pretenda presentar en el informe. En la segunda columna (procesos en la pericia) se evidencia que los pasos están alineados con el artículo que éste utiliza en el proceso, en este caso la mayor utilización de artículos están en los pasos 2,3 y 4 cuyos grupos de artículos se enfocan en: finalidad, principio, medios de prueba, contenido digital y reglas generales, es importante indicar que los pasos anteriormente mencionados están enfocados a la adquisición y preservación de la información en un disco duro de una laptop.

5.2 Caso 2

En la Tabla 3 se visualiza que el mayor número de procesos que se repiten son 2,3 y 4 cuyos grupos de artículos se enfocan en: calumnia, alteración de identidad, información pública reservada, acceso no consentido a un sistema informático, finalidad, retención de correspondencia, intersección de datos, medias de pruebas y contenido digital, en este proceso se hace más énfasis a estos artículos debido a que pertenece a una pericia realizada en una cuenta de correo electrónico y de redes sociales en la cual se debe contar con la

aprobación del afectado de forma escrita para poder realizar la pericia de forma que se cumplan estos artículos.

5.3 Caso 3

La Tabla 4 muestra que el mayor número de pasos que cubren más artículos son 2,5 y 6 debido a que estos enmarcan: revelación ilegal de base de datos, intercesión ilegal de datos, transferencia electrónica de activo patrimonial, ataque a la integridad de sistemas informáticos, delitos contra la información pública reservada legalmente, acceso no consentido a un sistema informático, finalidad, medios de prueba, contenido digital, apropiación fraudulenta por medios electrónicos. Además es importante indicar que este caso se desarrolló en base a una pericia informática realizada a un motor de base de datos del Ministerio de Agricultura del Ecuador que fue intervenida y modificada de forma ilícita.

Articulo	**Procesos en la pericia (aplicación y cumplimiento)**	**Observación**	**Procesos de computación forense**
178 Violación a la intimidad 179 Revelación de secreto 180 Difusión de información restringida	1 y 2		Preservación Identificación
182 Calumnia	1	Se debe contar con los permisos necesarios por parte de la autoridad.	Preservación Identificación

453 Finalidad **454 Principios**	2, 3 y 4	En el artículo 454 los literales 5 y 6 rigen la validez de la prueba.	Extracción
498 Medios de prueba	2, 3, 4 y 5	Se debe tener en claro los únicos medios válidos para presentar alguna evidencia como prueba.	Documentación
499 Reglas generales **500 Contenido digital**	3, 4, 5, 6, 7	El artículo 500 los literales 1, 2, 3 y 4 detallan la forma correcta para materializar la evidencia obtenida.	Documentación
511 Reglas generales	1, 2, 3, 4, 5, 6, 7	La persona asignada para realizar la pericia debe cumplir con los literales del 1 al 9.	Interpretación

Tabla 2.

Cumplimiento del código penal en los procesos forenses del Caso 1.

Fuente: Elaboración propia en base a Código Orgánico Integral Penal del Ecuador (COIP).

Articulo	**Procesos en la pericia (aplicación y cumplimiento)**	**Observación**	**Procesos de computación forense**
178 Violación a la intimidad **179 Revelación de secreto** **180 Difusión de información**	1 y 2		Preservación Identificación

restringida			
182 Calumnia	1, 2, 4	Se debe contar con los permisos necesarios por parte de la autoridad.	Preservación Identificación
221 Supresión, alteración o suposición de la identidad y estado civil	2 y 3	Se debe entregar las cuentas (correo o red social) tal y cual estaban antes de la intervención del perito.	Extracción
233 Delitos contra la información pública reservada legalmente 234 Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	2 y 3	El artículo 234 es vital al momento de materializar la información obtenida.	Extracción
453 Finalidad 454 Principios literales	3 y 4	En el artículo 454 los literales 5 y 6 rigen la validez de la prueba.	Documentación
475 Retención de correspondencia 476 Interceptación de las comunicaciones o datos informáticos 477 Reconocimiento de grabaciones	2 y 3	Se aplica en este caso ya que las cuentas han sido intervenidas (afectación).	Documentación
498 Medios de prueba	4	Se debe tener en claro los únicos medios	Interpretación

		válidos para presentar alguna evidencia como prueba.	
499 Reglas generales 500 Contenido digital	4	El artículo 500 los literales 1, 2, 3 y 4 detallan la forma correcta para materializar la evidencia obtenida.	Interpretación
511 Reglas generales	1, 2, 3, 4	La persona asignada para realizar la pericia debe cumplir con los literales del 1 al 9.	Interpretación

Tabla 3.

Cumplimiento del código penal en los procesos forenses del Caso 2.

Fuente: Elaboración propia en base a Código Orgánico Integral Penal del Ecuador (COIP).

Articulo	**Procesos en la pericia (aplicación y cumplimiento)**	**Observación**	**Procesos de computación forense**
178 Violación a la intimidad 179 Revelación de secreto 180 Difusión de información restringida	1		Preservación Identificación

182 Calumnia	2, 3, 5	Se debe contar con los permisos necesarios por parte de la autoridad.	Preservación Identificación
190 Apropiación fraudulenta por medios electrónicos	2 y 3	Validar que es el servidor correcto al que se le realiza la pericia.	Extracción
229 Revelación ilegal de base de datos **230 Interceptación ilegal de datos** **231 Transferencia electrónica de activo patrimonial** **232 Ataque a la integridad de sistemas informáticos** **233 Delitos contra la información pública reservada legalmente** **234 Acceso no consentido a un sistema informático, telemático o de telecomunicaciones**	5	Cuando se lleva a cabo la pericia en los servidores se debe tener en cuenta estos artículos, para no tener inconvenientes al momento de realizar los procedimientos pertinentes.	Extracción
453 Finalidad **454 Principios**	6	En el artículo 454 los literales 5 y 6 rigen la validez de la prueba.	Documentación
498 Medios de prueba	2, 5 y 6	Se debe tener en claro los únicos medios válidos para presentar alguna evidencia como prueba.	Documentación

499 Reglas generales 500 Contenido digital	2, 5 y 6	El artículo 500 los literales 1, 2, 3 y 4 detallan la forma correcta para materializar la evidencia obtenida.	Interpretación
511 Reglas generales	1, 2, 3, 4, 5, 6	La persona asignada para realizar la pericia debe cumplir con los literales del 1 al 9.	Interpretación

Tabla 4.

Cumplimiento del código penal en los procesos forenses del Caso 3.

Fuente: Elaboración propia en base a Código Orgánico Integral Penal del Ecuador (COIP).

Finalmente, realizado el análisis de los tres casos la Figura 5 muestra que el mayor número de artículos utilizados son relacionados en el caso de base de datos que representa el 75% de uso de los mismos, en cuanto al caso de redes sociales se obtiene un 58% de utilización y por último para discos duros se observa un 29% de uso.

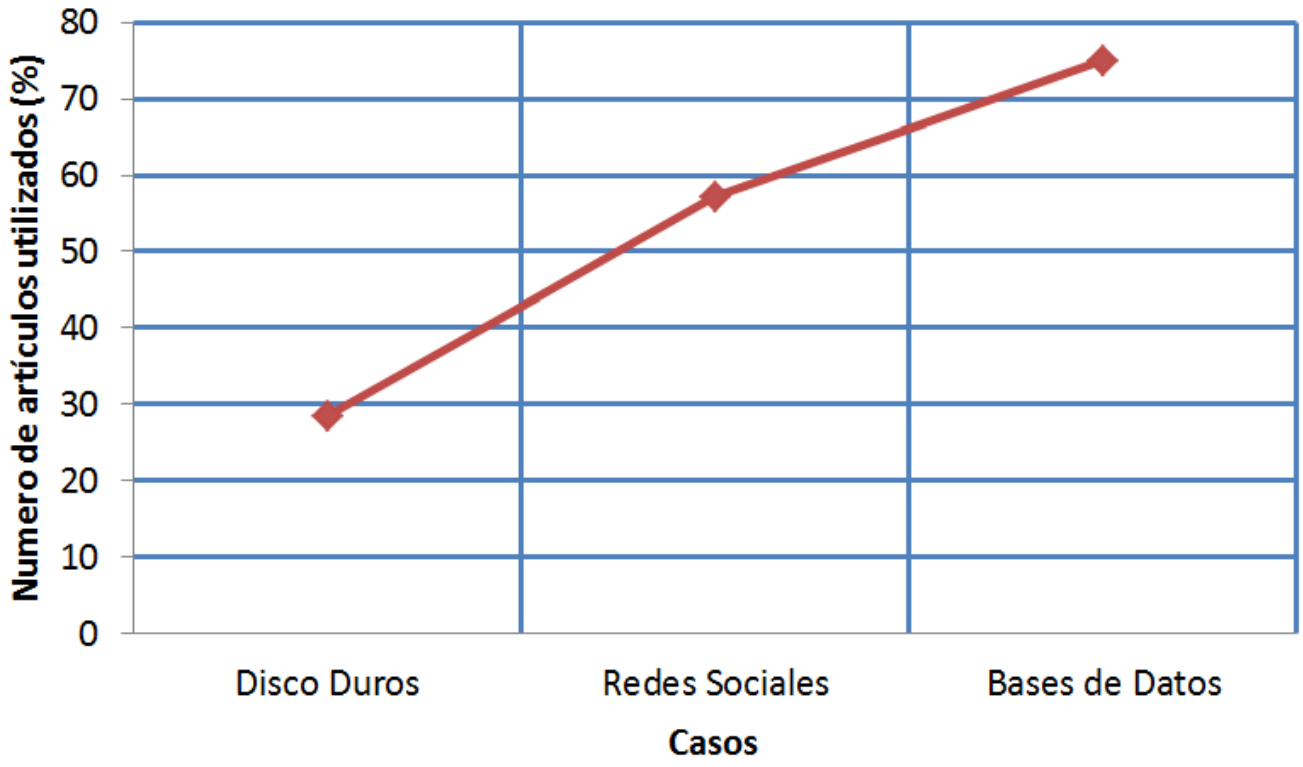

Figura 5.

Gráfico del número de artículos utilizados en los casos desarrollados.

Fuente: Elaboración propia en base al análisis de los datos.

6. CONCLUSIONES, LIMITACIONES Y TRABAJOS FUTUROS.

El Ecuador cuenta con un Código Orgánico Integral Penal (COIP) renovado que tiene vigencia desde el año 2014 en donde se actualizaron los artículos para penalizar los delitos informáticos existentes, se observa en el desarrollado de los tres casos expuestos en este paper que existen una serie de hechos tales como: los artículos resguardan en su totalidad los procesos empleados para efectuar una pericia informática, los equipos usados para realizar una adquisición y preservación de la información están normados bajo algún

artículo. Una vez realizada la investigación se puede determinar que la ley contempla una mayor cantidad de artículos relacionados a las bases de datos tal como se puede evidenciar en la Figura 5 de la sección de análisis de datos. Esto conlleva a que los casos de delito informático que tengan algún tipo de relación con los motores de base de datos serán sancionados no dando cabida a algún vacío legal.

Existen algunas limitaciones en este estudio, el periodo de tiempo empleado en la investigación y la cantidad de casos estudiados (3), teniendo como única fuente los archivos del Departamento de Criminalística del Guayas. Se incluyeron sólo tres casos debido al alto nivel de dificultad que existe en el acceso de los casos sentenciados por parte de las autoridades y establecimientos encargados. Es por ello que se hace un llamado a las autoridades pertinentes para que faciliten la información para fines académicos.

Por ser un estudio exploratorio no se puede ser concluyente con los resultados, sin embargo este análisis muestra un panorama empírico de esta temática en el Ecuador que puede servir como referente para un estudio descriptivo o inferencial. Cabe mencionar que es posible desarrollar varios temas que podrían ser utilizados para futuras investigaciones en base a este artículo. El estudio de otros tipos de evidencia digital tales como: documentos de ofimática, imágenes digitales, ficheros de registros de actividad, memoria volátil, entre otros y su relación con el COIP. Además el rango de años y la fuente de información de los casos podrían ampliarse y así evidenciar si la cobertura de artículos es la misma que contempla este paper. Finalmente, se puede categorizar los casos por provincias para brindar un mejor análisis descriptivo general de la pericia informática en el país.

Referencias

Accorsi, R. (2009, 07 24). IEEE. Retrieved 11 06, 2014, from Log Data as Digital Evidence: What Secure Logging Protocols Have to Offer?: www.ieee.org

Blum, J. (2010). Juez Nacional del Ecuador, Abodago. Guayaquil: Corte Nacional de Justicia.

Bojanc, R., & Blažic, B. (2008, 02 15). IEEE. Retrieved 11 08, 2014, from Standard Approach for Quantification of the ICT Security Investment for Cybercrime Prevention: www.ieee.org

Caloyannide, M., & Grumman, N. (04 de 2009). IEEE. Recuperado el 04 de 12 de 2014, de Forensics Is So "Yesterday": www.ieee.org

Carroll, O., Brannon, S., & Song, T. (2008, 01). The United Stated Departament of Justice. Retrieved 10 01, 2014, from Computer Forensics: Digital Forensic: http://www.justice.gov/usao/eousa/foia_reading_room/usab5601.pdf

Casey, E. (2004, 12). Elsevier. Retrieved 10 01, 2014, from Digital Evidence and Computer Crime, Second Edition: http://books.google.co.uk/books?id=Xo8GMt_AbQsC&hl=en&dq=Digital%20Evidence%20and%20Computer%20Crime,%20Second%20Edition&ei=it1XTMncCMm44gbC_qyFBw&sa=X&oi=book_result&ct=result&resnum=1&ved=0CDQQ6AEwAA

Colombia. (05 de 01 de 2009). Secretaría General de Bogotá. Recuperado el 14 de 03 de 2015, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Creutzburg, R., & Luttenberger, S. (2011). Forensic investigation of certain types of mobile devices. Retrieved 09 30, 2014, from file:///C:/Users/Cristopher/Downloads/Forensic%20investigation%20of%20certain%20types%20of%20mobile%20devices.pdf

Dick C.A., B. (2004, 10). IEEE Multimedia. Retrieved 10 01, 2014, from Is It Time for a Moratorium on Metadata?: http://homepages.cwi.nl/~dcab/PDF/ieeeMM2004.pdf

Ecuador. (02 de 10 de 2014). Asamblea Nacional del Ecuador. Recuperado el 15 de 03 de 2015, de http://www.asambleanacional.gob.ec/: http://www.asambleanacional.gob.ec/es/leyes-aprobadas

Ferruzola, E. (12 de 02 de 2014). Perito Informatico. (C. Gomez, Entrevistador)

Hua, Y., Zhu, Y., Jiang, H., Feng, D., & Tian, L. (2011, 04). IEEE. Retrieved 11 07, 2014, from Supporting Scalable and Adaptive Metadata Management in Ultralarge-Scale File Systems: www.ieee.org

Instituto Nacional de Ciberseguridad. (18 de 06 de 2014). Instituto Nacional de Ciberseguridad. Recuperado el 13 de 02 de 2015, de Gobierno de España: https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/rfc3227

Iqbal, B., Iqbal, A., Guimaraes, M., Khan, K., & Obaidli, H. (2012, 10 12). IEEE. Retrieved 11 07, 2014, from Amazon Kindle Fire from a Digital Forensics Perspective: www.ieee.org

Ke, H.-J., Liu, J., Wang, S.-J., & Goyal, D. (2011, 10 28). IEEE. Retrieved 11 06, 2014, from Hash-Algorithms Output for Digital Evidence in Computer Forensics: www.ieee.org

Kosch, H., Boszormeny, L., Dollers, M., Schojer, P., Kofler, A., & Libsie, M. (2005, 01). IEEE MultiMedia. Retrieved 10 01, 2014, from The life cycle of multimedia metadata: http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?tp=&arnumber=1377106&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1377106

Kuntze, N., & Rudolph, C. (2011, 05 26). IEEE. Retrieved 11 06, 2014, from Secure Digital Chains of Evidence: www.ieee.org

Lee, K., Lee, C., Park, N., Kim, S., & Won, D. (2011, 05 25). IEEE. Retrieved 11 06, 2014, from An Analysis of Multi-function Peripheral with a Digital Forensics Perspective: www.ieee.org

Lin, I.-L., Chao, H.-C., & Peng, S.-H. (2011, 10 28). IEEE. Retrieved 11 06, 2014, from Research of Digital Evidence Forensics Standard Operating Procedure with Comparison and Analysis Based on Smart Phone: www.ieee.org

López, F. (20 de 02 de 2014). Perito Informatico. (C. Gómez, Entrevistador)

Malek, M. (04 de 2008). IEEE. Recuperado el 28 de 11 de 2014, de An overview of IT Security Forensics: www.ieee.org

Ojeda, W. (2014, 09 01). Perito Informatico acreditado por Cosejo Judicatura de Ecuador, Cbo. Segundo de Policia. (C. Gomez, Interviewer)

Osborne, G., & Slay, J. (2011, 8 26). IEEE. Retrieved 11 6, 2014, from Digital Forensics Infovis: An Implementation of a Process for Visualisation of Digital Evidence: www.ieee.org

Sánchez, P. (10 de 09 de 2013). Conexion Inversa. Recuperado el 14 de 03 de 2015, de Security & Pure Forensics: http://conexioninversa.blogspot.com/2013/09/forensics-powertools-listado-de.html

Steinacker, A., Ghavam, A., & Steinmetz, R. (2001, 03). IEEE Multimedia. Retrieved 10 01, 2014, from Metadata Standards for: http://www.dsc.ufcg.edu.br/~garcia/cursos/TEICOPIN/metadataWE.pdf

Torres, D., Rueda, S., & Cano, J. (2004). Avances en criptología y seguridad de la información. Recuperado el 26 de 06 de 2015, de https://books.google.com.ec/books?hl=en&lr=&id=ibSu6896l_YC&oi=fnd&pg=PR7&dq=mecanismos+de+seguridad+de+la+informacion&ots=-GTHhqPn_T&sig=zr_zyoAQJaHzSacYasNOFc_UXb4#v=onepage&q=mecanismos%20de%20seguridad%20de%20la%20informacion&f=false

Ureta, L. (13 de 02 de 2015). Perito Infromatico. (C. Gomez, Entrevistador)

US-CERT. (2008). United Stated Computer Emergency Readiness. Retrieved 09 30, 2014, from https://www.us-cert.gov/

Vizueta, J. (2011). Delitos Informaticos en el Ecuador. Guayaquil: EDINO.

Warren, K., & Heiser, J. (2002). Addison-Wesley. Retrieved 10 01, 2014, from Computer Forensics: Incident Response Essentials: http://books.google.com.ec/books?id=nNpQAAAAMAAJ&redir_esc=y

Wroe, C., Goble, C., Greenwood, M., Lord, P., Miles, S., Papay, J., y otros. (02 de 2004). IEEE Intelligent Systems. Recuperado el 01 de 10 de 2014, de Automating Experiments Using Semantic Data on a Bioinformatics Grid: http://homepages.cs.ncl.ac.uk/phillip.lord/download/publications/seven_kinds.pdf

Yasinsac, A., Erbacher, R., Marks, D., & Pollitt, M. (2003, 08). IEEE Security & Privacy. Retrieved 10 01, 2014, from Computer forensics education: http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?tp=&arnumber=1219052&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F8013%2F27399%2F01219052

Yen, Y.-S., Lin, I.-L., & Chang, A. (2011, 07 2). IEEE. Retrieved 11 08, 2014, from A Study on Digital Forensics Standard Operation Procedure for Wireless Cybercrime: www.ieee.org

AccessData. (2014). Recuperado el 17 de 10 de 2014, de http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk

Acurio, S. (2010). OEA - Organización de los Estados Americanos. Recuperado el 12 de 02 de 2015, de http://www.oas.org/juridico/spanish/cyb_ecu_plan_operativo.pdf

Blum, J. (2010). Juez Nacional del Ecuador, Abodago. Guayaquil: Corte Nacional de Justicia.

Colombia. (05 de 01 de 2009). Secretaría General de Bogotá. Recuperado el 14 de 03 de 2015, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Ecuador. (02 de 10 de 2014). Asamblea Nacional del Ecuador. Recuperado el 15 de 03 de 2015, de http://www.asambleanacional.gob.ec/: http://www.asambleanacional.gob.ec/es/leyes-aprobadas

López, F. (20 de 02 de 2014). Perito Informatico. (C. Gómez, Entrevistador)

Sánchez, P. (10 de 09 de 2013). Conexion Inversa. Recuperado el 14 de 03 de 2015, de Security & Pure Forensics: http://conexioninversa.blogspot.com/2013/09/forensics-powertools-listado-de.html

Ureta, L. (13 de 02 de 2015). Perito Infromatico. (C. Gomez, Entrevistador)

Notas biográficas:

Francisco Bolaños. Es Ingeniero en Computación Especialización Sistemas de Información, tiene una Maestría en Seguridad Informática Aplicada. Es director de la Maestría en Auditoría de Tecnologías de la Información en la Universidad Espíritu Santo. Su línea de investigación es la criptografía aplicada con énfasis en sidechannelattacks.

Cristopher Gómez. Es Ingeniero en Sistemas con mención en Desarrollo. Fue Integrante del departamento de Servicio de Ingeniería de Alcatel-Lucent en Ecuador. A partir mayo de 2015 se desempeña como Analista de Tecnologías de la Información y Comunicaciones en el departamento de seguridad y base de datos de la Comisión de Transito del Ecuador. Sus líneas de investigación: Seguridad Informática y Computación Forense.